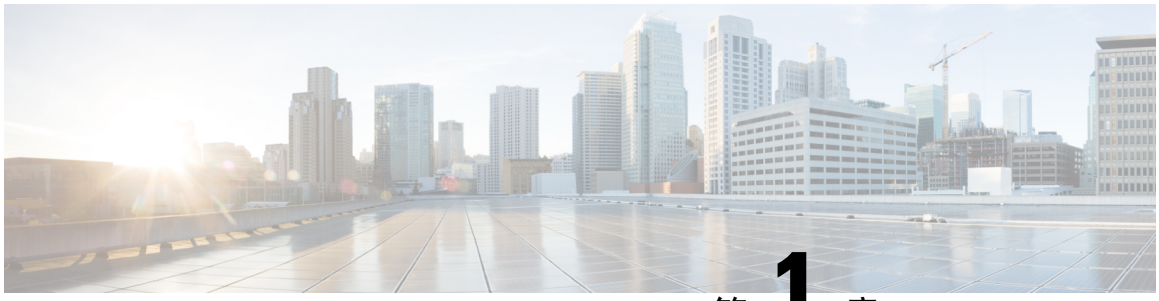
思科身份服务引擎安装指南，版本 3.1

首次发布日期: 2021 年 8 月 3 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

目录



第 1 章

思科 ISE 中的网络部署

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

其他参考资料 (Additional References)

以下链接包含在使用思科 ISE 时可供使用的其他资源：https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册思科配置文件管理器。

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

思科漏洞搜索工具

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

文档反馈

要提供有关思科技术文档的反馈，请使用每个在线文档右窗格中提供的反馈表。

思科 ISE 网络架构

思科 ISE 架构包括以下组件：

- 节点和角色类型
  - 思科 ISE 节点 - 思科 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。

思科 ISE 部署术语

本指南在讨论思科 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。

术语	定义
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

思科 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、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

具有监控角色的思科 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。通过思科 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思科 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》中的安全组标记交换协议部分。

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

具有单个思科 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。

具有多个思科 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思科 ISE 节点的部署。在思科 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。思科 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

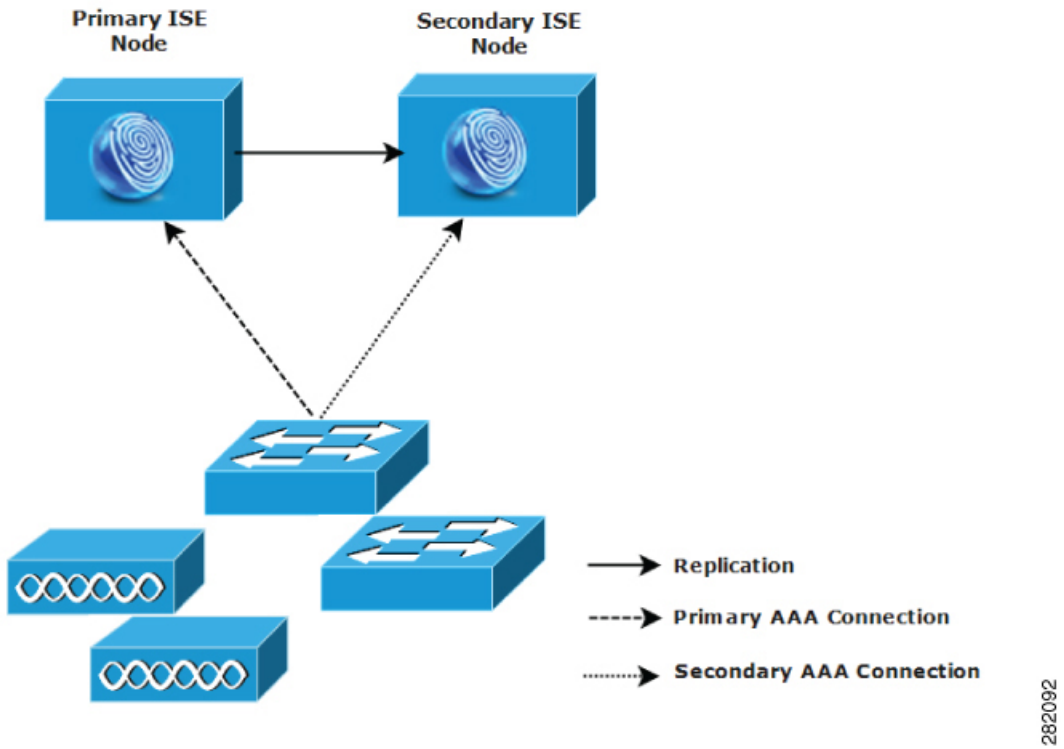
小型网络部署

最小的思科 ISE 部署包含两个思科 ISE 节点，其中一个思科 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思科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。思科ISE会将驻留在主要思科ISE节点上的所有内容与辅助思科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:* 思科 *ISE* 节点的小型网络部署



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

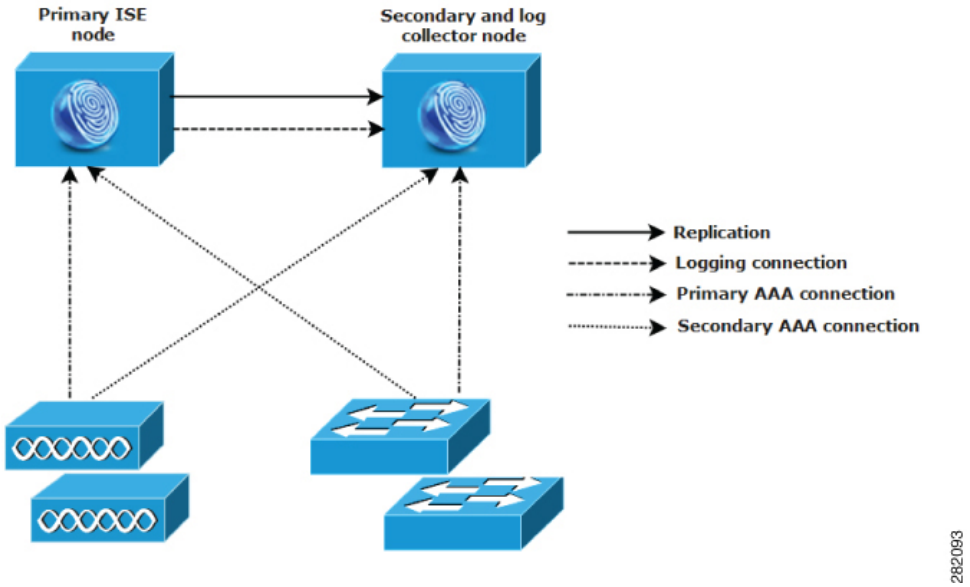
在分离式思科ISE部署中，您将按照小型思科ISE部署中所述继续维护主要节点和辅助节点。但是，AAA 负载会在两个思科 ISE 节点之间进行拆分，以优化 AAA 工作流程。如果 AAA 连接有任何问题，则每个思科 ISE 设备（主要或辅助）需要能够处理全部工作负载。主要节点和辅助节点在正常网络操作过程中均不处理任何 AAA 请求，因为此工作负载分布在两个节点之间。

以此方式拆分负载的功能会直接减少系统中每个思科 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。

在分离式思科 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。如果您有两个思科 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思科 ISE 节点设置为用作日志收集器。

此外，分离式思科 ISE 部署设计具有优势，因为它允许增长。

图 *2:* 思科 *ISE* 中的拆分网络部署



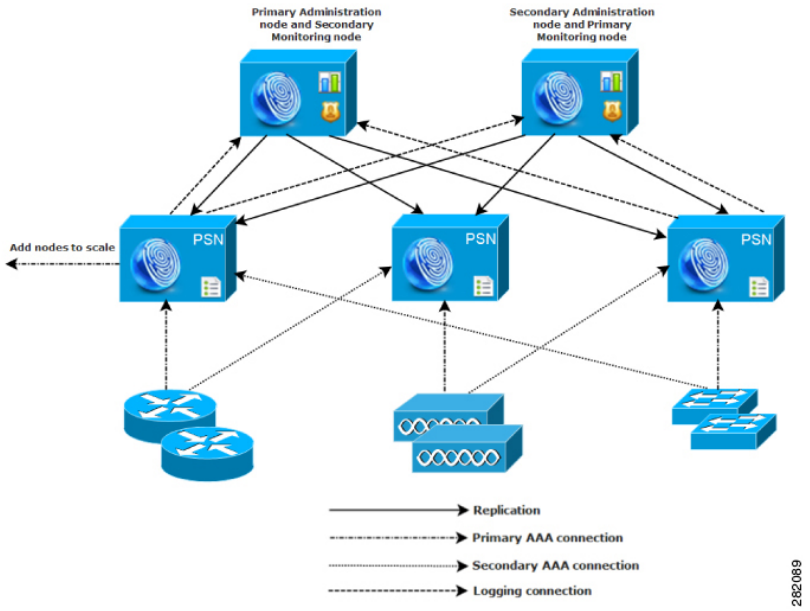
中型网络部署

随着小型网络的增长，您可以通过添加思科 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。

注释 在中型网络部署中，不能在运行管理角色和/或监控角色的节点上启用策略服务角色。需要专用策略服务节点。

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思科 ISE 节点专用于网络中的日志收集。

图 *3:* 思科 *ISE* 中的中型网络部署



大型网络部署

集中日志记录

我们建议您对大型思科 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RFC3164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，您可以使用思科 ISE 中提供的报告和警报功能支持所有思科 ISE 节点。

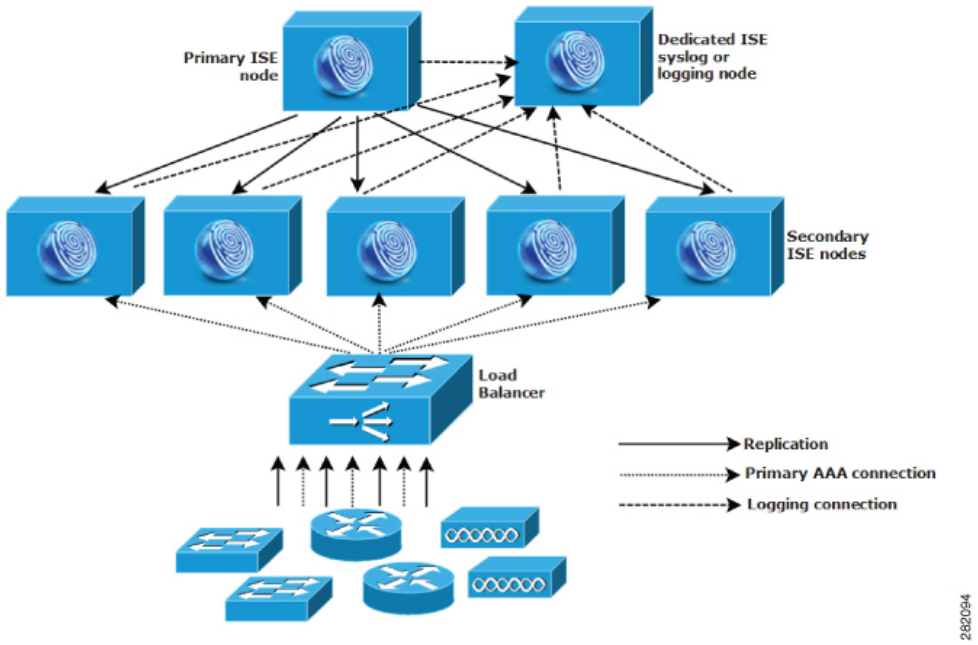
您也可以考虑使用设备将日志发送到思科 ISE 节点上的监控角色以及通用系统日志服务器。如果思科 ISE 节点上的监控角色关闭，则添加通用日志服务器可提供冗余备份。

在集中式网络中使用负载均衡器

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:* 思科 *ISE* 中使用负载均衡器的大型网络部署

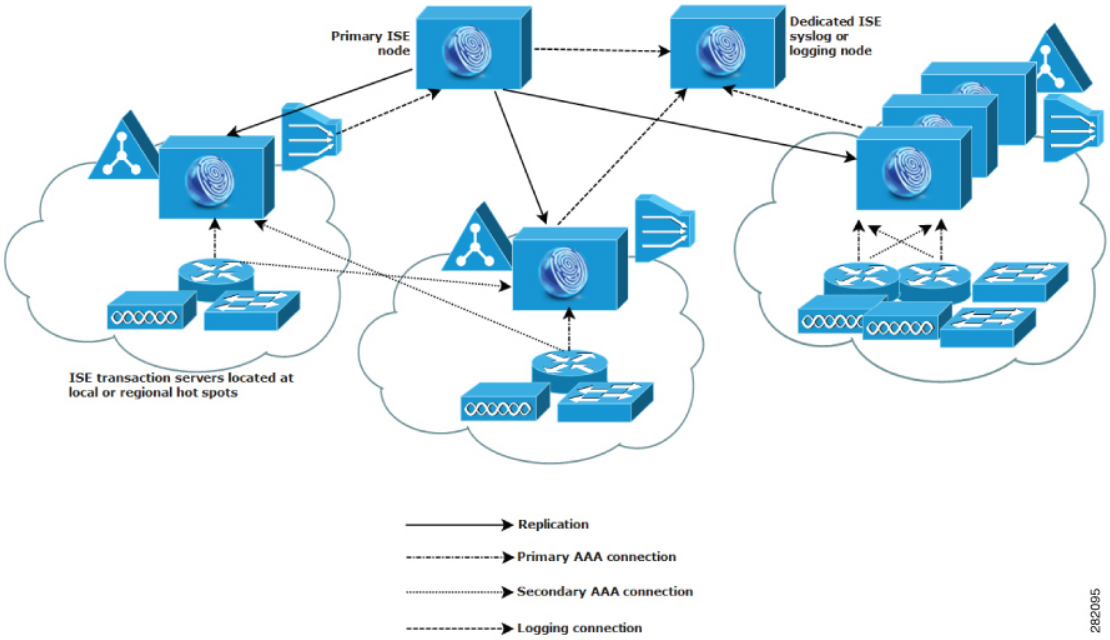


思科 ISE 中的离散网络部署

离散思科 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思科 ISE 节点与辅助思科 ISE 节点结合使用。我们仍建议您在思科 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:* 思科 *ISE* 中的离散部署



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，可供思科 ISE 访问以优化 AAA 性能。
- AAA 客户端的位置非常重要。您应使思科 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。
- 思科 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，请考虑使用思科 ISE 节点作为本地站点的备份以提供冗余。
- 应在所有思科 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。

思科 ISE 中的每个部署模式的最大支持会话数

下表列出了每个部署模式的最大支持会话数。

表 *1:* 每个部署模式支持的最大会话数

部署模式	平台	最大会话数
独立（所有角色位于单个节点上）	3615	10,000
	3655	25,000
	3695	50,000
	3595	20,000
基本 2 节点部署（冗余）	3615	10,000
	3655	25,000
	3695	50,000
	3595	20,000
混合分布式部署（管理和 MnT 位于同一设备上；策略服务位于专用设备上）	3615 作为 PAN 和 MnT	10,000
	3655 作为 PAN 和 MnT	25,000
	3695 作为 PAN 和 MnT	50,000
	3595 作为 PAN 和 MnT	20,000
专用（PAN、MnT、PXG 和 PSN 节点）	3595 作为 PAN 和 MnT	500,000
	3655 作为 PAN 和 MnT	500,000
	3695 作为 PAN 和 MnT	2,000,000

表 *2:* 每个专用 ***PSN*** 的最大活动会话数

按 **PSN** 扩展	最大活动会话数
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3595	40,000

SNS 3500/3600 系列设备的部署规模和扩展建议

表 *3: SNS 3500/3600* 系列设备的最大 *RADIUS* 扩展

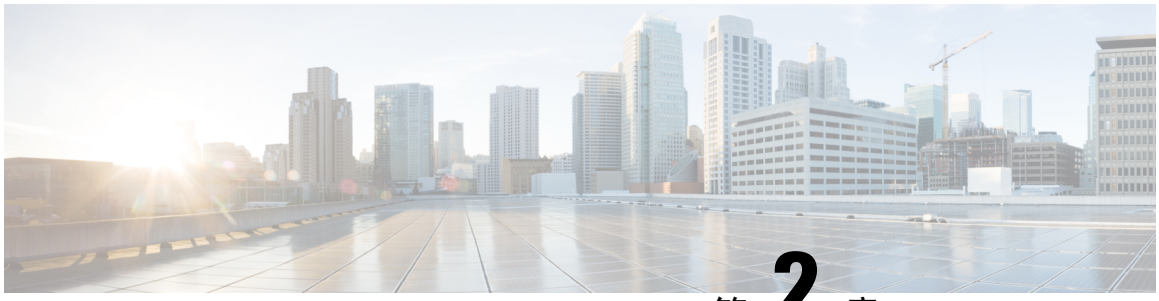
部署模式	平台	专用 PSN 的最大数量	每个部署的最大 RADIUS 会话数
独立	3595	0	20,000
	3615	0	10,000
	3655	0	25,000
	3695	0	50,000
PAN 和 MnT 位于同一节点和专用 PSN 上	3595 作为 PAN 和 MnT	6	20,000
	3615 作为 PAN 和 MnT	6	10,000
	3655 作为 PAN 和 MnT	6	25,000
	3695 作为 PAN 和 MnT	6	50,000
专用（PAN、MnT、PXG 和 PSN 节点）	3595 作为 PAN 和 MnT	50	500,000
	3655 作为 PAN 和 MnT	50	500,000
	3695 作为 PAN 和 MnT	50	2,000,000

支持思科 ISE 功能所需的交换机和无线局域网控制器配置

要确保思科 ISE 能够与网络交换机互操作，并且来自思科 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

思科安全网络服务器 3500/3600 系列设备和虚拟机要求

思科 ISE 的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思科 SNS 3500 或 3600 系列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。

注释 强化您的虚拟环境，并确保所有安全更新都是最新的。思科对于虚拟机监控程序中发现的任何安全问题概不负责。

思科安全网络服务器 3500 和 3600 系列设备

有关思科安全网络服务器 (SNS) 硬件设备规范，请参阅思科安全网络服务器产品手册中的“表 1：产品规范”。

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

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

注释 思科 ISE 3.1 不支持思科 SNS 3515 设备。有关思科 ISE 3.1 支持的硬件平台的信息，请参阅支持的硬件。

思科 ISE 的 VMware 虚拟机要求

思科 ISE 支持以下 VMware 服务器和客户端：

- 适用于 ESXi 6.5 及更高版本的 VMware 版本 11（默认）
- 适用于 ESXi 7.*x* 的 VMware 版本 13（默认）

您可以使用 VMware 迁移功能在主机之间迁移虚拟机 (VM) 实例（运行任何角色）。思科 ISE 支持热迁移和冷迁移。

- 热迁移也称为实时迁移或 vMotion。热迁移期间无需关闭或关闭思科 ISE。您可以在不中断其可用性的情况下迁移思科 ISE VM。
- 思科 ISE 必须关闭并关闭电源才能进行冷迁移。思科 ISE 不允许在迁移期间停止或暂停数据库操作。因此，请确保思科 ISE 在冷迁移期间未运行且未处于活动状态。

注释 您必须先使用 application stop 命令，然后再使用 halt 命令或关闭虚拟机，以便防止出现数据库损坏问题。

注意 如果在 VM 上启用了快照功能，可能会损坏 VM 配置。如果发生此问题，您需要重新映像 VM 并禁用 VM 快照。

注释 VMware 快照用于保存 VM 在给定时间点的状态，因此思科 ISE 不支持使用 VMware 快照备份 ISE 数据。在多节点思科 ISE 部署中，所有节点中的数据都与当前数据库信息保持同步。恢复快照可能会导致数据库复制和同步问题。建议您使用思科 ISE 中包含的备份功能来存档和恢复数据。使用 VMware 快照备份 ISE 数据将导致停止思科 ISE 服务。需要重启才能激活 ISE 节点。

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：

- ISE-3.x.x.xxx-virtual-SNS3615-SNS3655-300.ova
- ISE-3.x.x.xxx-virtual-SNS3615-SNS3655-600.ova
- ISE-3.x.x.xxx-virtual-SNS3655-SNS3695-1200.ova
- ISE-3.x.x.xxx-virtual-SNS3695-2400.ova

300 GB OVA 模板足以用于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#unique_31。

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。

表 *4: OVA* 模板预留

OVA 模板类型	CPU 数量	CPU 预留 (MHz)	内存 (GB)	内存预留 (GB)
评估	4	无预留。	16	无预留。
小型	16	16,000	32	32
中	24	24,000	96	96
大型	24	24,000	256	256

强烈建议您保留 CPU 和内存资源以匹配资源配置。否则可能会严重影响 ISE 的性能和稳定性。

有关支持的操作系统的信息，请参阅虚拟机支持的操作系统。

有关思科 SNS 设备的产品规格的信息，请参阅思科安全网络服务器产品手册。

下表列出了 VMware 虚拟机要求。

表 *5: 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：4 个 CPU 核心 • 生产 • 时钟速度：2.0 GHz 或更快 • 核心数量： • **SNS 3500 系列设备：** • 中型：16 • 大型：16 注释 由于超线程，核心数量相当于思科安全网络服务器 3500 系列中核心数量的两倍。 • **SNS 3600 系列设备：** • 小型：16 • 中型：24 • 大型：24 注释 由于超线程，核心数量相当于思科安全网络服务器 3600 系列中核心数量的两倍。例如，对于小型网络部署，您必须分配 16 个 vCPU 核心才能满足 SNS 3615（包含 8 个 CPU 核心或 16 个线程）的 CPU 规格。
内存	• 评估：16 GB • 生产 • 小型：32 GB (SNS 3615) • 中型：64 GB (SNS 3595) 和 96 GB (SNS 3655) • 大型：256 GB，用于 SNS 3695

要求类型	规范
硬盘	• 评估：300 GB • 生产 300 GB 至 2.4 TB 磁盘存储（大小取决于部署和任务）。 请在以下链接查看 VM 的建议磁盘空间：磁盘空间要求。 建议您的虚拟机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#unique_32。 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。 注释 将 ISE VM 的磁盘 SCSI 控制器从其他类型更新为 VMware Paravirtual 可能会导致其无法引导。
网卡	需要 1 个 NIC 接口（建议使用两个或更多 NIC；支持六个 NIC）。思科 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。
VMware 虚拟硬件版本/虚拟机监控程序	ESXi 6.5 和更高版本以及 ESXi 7.*x* 上的 VMware 虚拟机硬件版本 11 或更高版本。

思科 ISE 的 Linux KVM 要求

表 *6: 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：4 个 CPU 核心 • 生产 • 时钟速度：2.0 GHz 或更快 • 核心数量： • **SNS 3500 系列设备：** • 中型：16 • 大型：16 注释 由于超线程，核心数量相当于思科安全网络服务器 3500 系列中核心数量的两倍。 • **SNS 3600 系列设备：** • 小型：16 • 中型：24 • 大型：24 注释 由于超线程，核心数量相当于思科安全网络服务器 3600 系列中核心数量的两倍。例如，对于小型网络部署，您必须分配 16 个 vCPU 核心才能满足 SNS 3615（包含 8 个 CPU 核心或 16 个线程）的 CPU 规格。

要求类型	最低要求

内存	• 评估：16 GB
	• 生产
	  • 小型：32 GB (SNS 3615)
	  • 中型：64 GB (SNS 3595) 和 96 GB (SNS 3655)
	  • 大型：256 GB

硬盘	• 评估：300 GB • 生产 300 GB 至 2.4 TB 磁盘存储（大小取决于部署和任务）。 请在以下链接查看 VM 的建议磁盘空间：磁盘空间要求。 建议您的虚拟机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 个 NIC 接口（建议使用两个或更多 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	QEMU 2.12.0-99 上的 KVM

思科 ISE 的 Microsoft Hyper-V 要求

表 *7: 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：4 个 CPU 核心
	• 生产
	  • 时钟速度：2.0 GHz 或更快
	  • 核心数量：
	  • **SNS 3500 系列设备：**
	  • 中型：16
	  • 大型：16
	  由于超线程，核心数量相当于思科安全网络服务器 3500 系列中核心数量的两倍。
	  • **SNS 3600 系列设备：**
	  • 小型：16
	  • 中型：24
	  • 大型：24
	  注释 由于超线程，核心数量相当于思科安全网络服务器 3600 系列中核心数量的两倍。例如，对于小型网络部署，您必须分配 16 个 vCPU 核心才能满足 SNS 3615（包含 8 个 CPU 核心或 16 个线程）的 CPU 规格。

内存	• 评估：16 GB
	• 生产
	  • 小型：32 GB (SNS 3615)
	  • 中型：64 GB (SNS 3595) 和 96 GB (SNS 3655)
	  • 大型：256 GB

要求类型	最低要求
硬盘	• 评估：300 GB • 生产 300 GB 至 2.4 TB 磁盘存储（大小取决于部署和任务）。 请在以下链接查看 VM 的建议磁盘空间：磁盘空间要求。 建议您的虚拟机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 个 NIC 接口（建议使用两个或更多 NIC；支持六个 NIC）。
虚拟机监控程序	Hyper-V (Microsoft)

思科 ISE 的 Nutanix AHV 要求

思科 ISE 必须使用标准思科 ISE.iso 映像在 Nutanix AHV 上部署。Nutanix AHV 不支持使用 OVA 模板部署思科 ISE。

下表指定在 Nutanix AHV 上为不同类型的部署建议的资源预留：

类型	CPU 数量	CPU 预留 (MHz)	内存 (GB)	内存预留 (GB)	硬盘
评估	4	无预留	16	无预留	200 GB
小型	16	16,000	32	32	600 GB
中	24	24,000	96	96	1.2 TB
大型	24	24,000	256	256	2.4 TB（拆分为 4*600 GB）

在继续安装思科 ISE 之前，您必须在 Nutanix AHV 上执行以下配置：

- 在 Nutanix AHV 上创建虚拟机 (VM) 并关闭 VM 电源。
- 使用 ssh login 访问 Nutanix CVM 并运行以下命令：
  - $acli
  - <acropolis> vm.serial_port_create <*Cisco ISE VM Name*> type=kServer index=0

- <acropolis> vm.update <*Cisco ISE VM Name*> disable_branding=true
- <acropolis> vm.update <*Cisco ISE VM Name*> extra_flags=”enable_hyperv_clock=False”

- 退出 Acropolis CLI 并打开 VM 电源，以便使用 standard.iso 映像继续安装思科 ISE。

表 *8: Nutanix AHV* 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 • 小型 - 12 个处理器（6 个启用了超线程的核心） • 大型 - 16 个处理器（8 个启用了超线程的核心） 6 个核心；2.0 Ghz 或更快。 思科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。

要求类型	最低要求
内存	• 评估： • 基本 - 4 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 对于 2.4 TB 硬盘支持，必须使用 4*600 GB。
KVM 磁盘设备	磁盘总线 - SCSI
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	AOS - 5.20.1.1 LTS, Nutanix AHV - 20201105.2096

Amazon Web 服务和 Azure VMware 解决方案上 VMware 云的思科 ISE 支持

在 VMware 云上安装思科 ISE 的过程与在 VMware 虚拟机上安装思科 ISE 的过程完全相同。

- 部署在 Amazon Web 服务 (AWS) 上 VMware 云中的思科 ISE 虚拟机：思科 ISE 可以托管在 AWS 上 VMware 云提供的软件定义的数据中心 (SDDC) 上。确保在 VMware 云上配置适当的安全组策略（在**网络和安全 (Networking & Security) > 安全 (Security) > 网关防火墙设置 (Gateway Firewall Settings)** 下）以支持访问现场部署、必需设备和服务。

- 部署在 Azure VMware 解决方案 (AVS) 上的思科 ISE 虚拟机：AVS 在 Microsoft Azure 上本地运行 VMware 工作负载，思科 ISE 可从中托管为 VMware 虚拟机。

思科 ISE 的虚拟机设备大小建议

用于监控节点的大型 VM 在思科 ISE 2.4 中引入。 在大型 VM 上部署监控角色可提高对实时日志查询和报告完成的响应速度，从而改进性能。

注释 此外形规格仅可在版本 2.4 及更高版本中用作 VM，并需要大型 VM 许可证。

虚拟机 (VM) 设备规格应可与生产环境中运行的物理设备相当。

为设备分配资源时，请记住以下准则：

- 未能分配指定的资源可能会导致性能降级或服务故障。强烈建议您部署专用 VM 资源，不要在多个访客 VM 之间共享或超订用资源。使用 OVF 模板部署思科 ISE 虚拟设备可确保为每个 VM 分配足够的资源。如果不使用 OVF 模板，请确保在使用 ISO 映像手动安装思科 ISE 时分配同等的资源预留。

注释 如果您选择手动部署思科 ISE 而没有分配建议的预留，则必须负责密切监控设备的资源利用率，并根据需要增加资源，以确保思科 ISE 部署正常运行。

注释 OVF 模板不适用于 Linux KVM。OVF 模板仅适用于 VMware 虚拟机。

- 如果使用 OVA 模板进行安装，请在安装完成后检查以下设置：
  - 确保分配资源预留，此预留在思科 ISE 的 VMware 虚拟机要求，第 14 页部分的 CPU/内存 **预留 (Reservation)** 字段（**编辑设置 (Edit Settings)** 窗口的**虚拟硬件 (Virtual Hardware)** 选项卡下）指定，以确保思科 ISE 部署正常运行。
  - 确保 **CPU 限制 (CPU Limit)** 字段（**编辑设置 (Edit Settings)** 窗口的**虚拟硬件 (Virtual Hardware)** 选项卡下）中的“CPU 使用”(CPU usage) 设置为**无限制 (Unlimited)**。设置 CPU 使用限制（例如将 CPU 使用限制设置为12000 MHz）会影响系统性能。如果已设置限制，则必须关闭 VM 客户端，删除限制，然后重新启动 VM 客户端。
  - 确保**内存限制 (Memory Limit)** 字段（**编辑设置 (Edit Settings)** 窗口的**虚拟硬件 (Virtual Hardware)** 选项卡下）中的“内存使用”(memory usage) 设置为**无限制 (Unlimited)**。设置内存使用限制（例如将限制设置为 12000 MB）会影响系统性能。

- 确保在**硬盘 (Hard Disk)** 区域中将**共享 (Shares)** 选项设置为**高 (High)**（**编辑设置 (Edit Settings)** 窗口的**虚拟硬件 (Virtual Hardware)** 选项卡下）。

  管理和 MnT 节点很大程度上依赖磁盘使用率。使用共享磁盘存储 VMware 环境可能会影响磁盘性能。必须增加分配给节点的磁盘共享数，才能提高节点的性能。

- 在 VM 上部署策略服务节点时，其磁盘空间可以少于管理或监控节点。任一生产思科 ISE 节点的最小磁盘空间为 300 GB。有关各种思科 ISE 节点和角色所需的磁盘空间的详细信息，请参阅 #unique_31。
- VM 可配置有 1 至 6 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、访客服务或 RADIUS。

注释 VM 上的 RAM 和 CPU 调整不需要重新映像。

思科 ISE 部署中的虚拟机磁盘空间要求

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。

注释 必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

表 *9:* 建议的虚拟机磁盘空间

思科 ISE 角色	用于评估的最小磁盘空间	用于生产的最小磁盘空间	用于生产的建议磁盘空间	最大磁盘空间
独立 ISE	300 GB	600 GB	600 GB 至 2.4 TB	2.4 TB
分布式思科 ISE，仅管理	300 GB	600 GB	600 GB	2.4 TB
分布式思科 ISE，仅监控	300 GB	600 GB	600 GB 至 2.4 TB	2.4 TB
分布式思科ISE，仅策略服务	300 GB	300 GB	300 GB	2.4 TB
分布式思科 ISE，仅 pxGrid	300 GB	300 GB	300 GB	2.4 TB
分布式思科ISE，管理和监控（以及可选的 pxGrid）	300 GB	600 GB	600 GB 至 2.4 TB	2.4 TB
分布式思科ISE，管理、监控和策略服务（以及可选的 pxGrid）	300 GB	600 GB	600 GB 至 2.4 TB	2.4 TB

注释 当主管理节点临时成为监控节点时，需要额外的磁盘空间来存储本地调试日志、暂存文件以及在升级期间处理日志数据。

思科 ISE 的磁盘空间准则

在决定思科 ISE 的磁盘空间时，请记住以下准则：

- 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% 的虚拟机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 360 GB 将分配用于日志存储。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 76 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 60 GB 用于日志存储。

如果在初始安装后增加虚拟机磁盘大小，请执行思科 ISE 全新安装。全新安装有助于正确检测和利用完整的磁盘分配。

下表根据分配的磁盘空间以及连接至网络的终端数，列出了 RADIUS 日志可以在监控节点上保留的天数。天数基于以下假设：启用日志记录抑制后，每个终端每天进行十次或更多身份验证。

表 *10:* 监控节点日志存储 - *RADIUS* 的保留期（天）

终端数	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

下表根据分配的磁盘空间以及连接至网络的终端数，列出了 TACACS+ 日志可以在监控节点上保留的天数。天数基于以下假设：脚本针对所有 NAD 运行，每天运行 4 个会话，每个会话运行 5 个命令。

表 *11:* 监控节点日志存储 - *TACACS+* 保留期（天）

终端数	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

增加磁盘大小

如果发现情景与可视性功能较慢，或者日志空间不足，则必须分配更多磁盘空间。

要计划更多的日志存储，每增加 100 GB 磁盘空间，就有 60 GB 可用于日志存储。

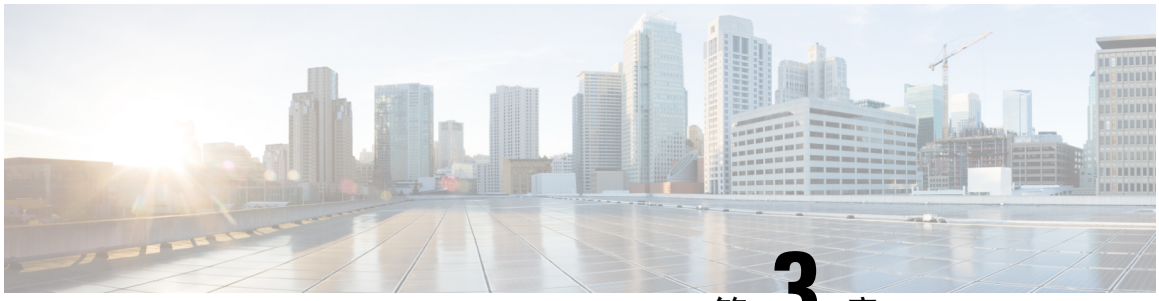
要让 ISE 检测和利用新磁盘分配，您必须取消注册节点，更新 VM 设置，然后重新安装 ISE。一种方法是在更大的新节点上安装ISE，并将此节点作为高可用性添加到部署中。节点同步后，将新VM设置为主 VM，并取消注册原有 VM。

减小磁盘大小

在 VM 上安装思科 ISE 后，您不得减少 VM 预留。如果将 VM 内存减少到低于思科 ISE 服务的要求，则思科 ISE 服务会因为资源不足而无法启动。

在安装思科 ISE 后，如果必须重新配置 VM，请执行以下步骤：

1. 执行思科 ISE 备份。
2. 根据需要使用更改后的 VM 配置来重新映像思科 ISE。
3. 恢复思科 ISE。



第 3 章

安装思科 ISE

使用 CIMC 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：

开始之前

- 确保您已满足本指南中指定的系统要求。
- （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：
  - #unique_43
  - #unique_44
  - 在 Hyper-V 上创建思科 ISE 虚拟机， 第 67 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) 配置实用工具以管理设备并配置 BIOS。有关详细信息，请参阅以下文档：
  - 有关 SNS 3500 系列设备，请参阅 Cisco SNS-3500 系列设备硬件安装指南。
  - 有关 SNS-3600 系列设备，请参阅思科 SNS-3600 系列设备硬件安装指南。

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。

步骤 2 下载思科 ISE ISO 映像。

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**为此产品下载软件 (Download Software for this Product)**。

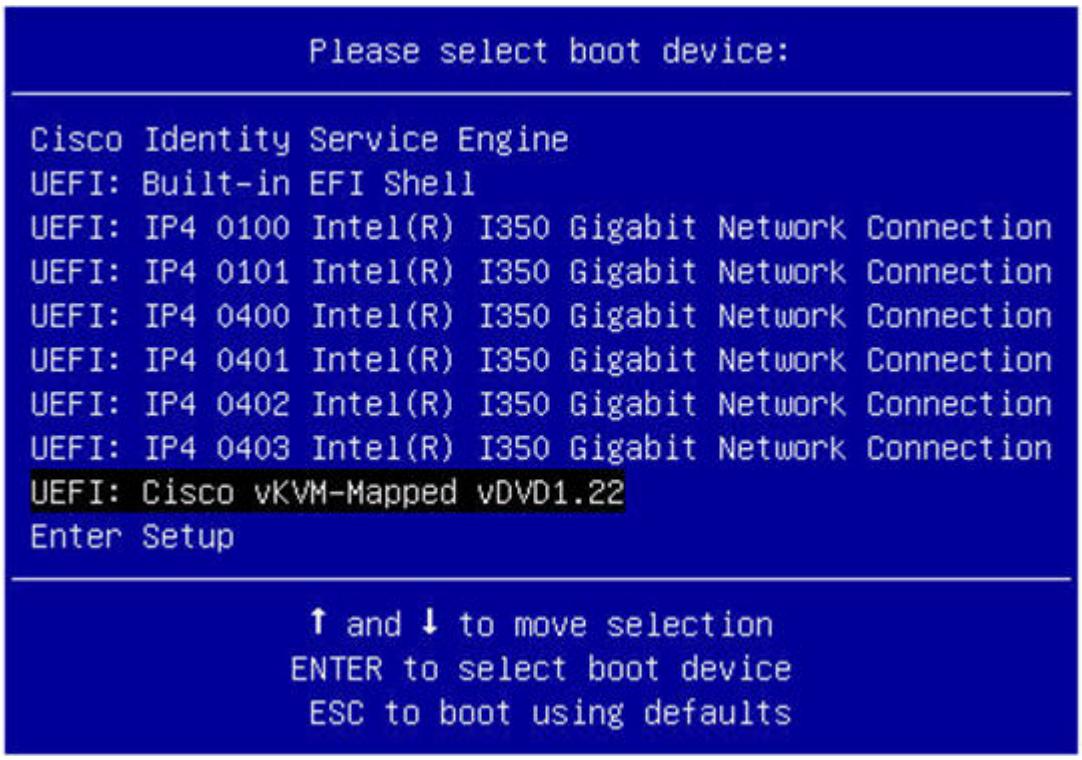
思科 ISE 映像上已经安装 90 天的评估许可证，因此在完成安装和初始配置后，可以对所有思科 ISE 服务进行测试。

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“虚拟媒体”(Virtual Media) > “激活虚拟设备”(Activate Virtual Devices)。
4. 选择“虚拟媒体”(Virtual Media) > “映射 CD/DVD”(Map CD/DVD)，并选择 ISE ISO 映像，然后点击“映射设备”(Map Device)。
5. 选择“宏”(Macros) > “静态宏”(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:* 启动设备的选择



注释　如果 SNS 设备位于您没有任何物理访问权限的远程位置（如数据中心），并且您需要从远程服务器执行 CIMC 安装，则安装可能需要较长时间。建议您将 ISO 文件复制到 USB 驱动器，并在远程位置使用此文件以加快安装过程。

- 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: 3.0.0.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，请参阅思科 ISE 的运行设置程序，第 31 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 继续执行验证思科 ISE 安装过程，第 34 页。

思科 ISE 的运行设置程序

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。此设置流程是一次性配置任务。

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

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

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

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

建议在运行安装脚本时与 NTP 服务器和 DNS 服务器建立网络连接。

要运行设置程序，请执行以下操作：

步骤 1 打开指定用于安装的设备。

系统随即会显示以下设置提示：

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

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

控制台随即会显示一组参数。您必须按照下表中的说明输入参数。

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

表 *12:* 思科 *ISE* 设置程序参数

提示	说明	示例
Hostname	不得超过 19 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。第一个字符必须是字母。 注释 我们建议您使用小写字母，以确保思科 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 或全局 IPv6 地址。	10.12.13.14/ 2001:420:54ff:4::458:121:119
Netmask	必须是有效的 IPv4 或 IPv6 网络掩码。	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
Default gateway	必须是默认网关的有效 IPv4 或全局 IPv6 地址。	10.12.13.1/ 2001:420:54ff:4::458:1

提示	说明	示例
DNS domain name	不能是 IP 地址。有效字符包括 ASCII 字符、任意数字、连字符 (-) 和句点 (.)。	example.com
Primary name server	必须是主域名服务器的有效 IPv4 或全局 IPv6 地址。	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	必须是主域名服务器的有效 IPv4 或全局 IPv6 地址。	（可选）允许您配置多个域名服务器。要执行此操作，请输入 **y** 继续。
Primary NTP server	必须是网络时间协议 (NTP) 服务器的有效 IPv4 或全局 IPv6 地址或主机名。 **注释** 确保主 NTP 服务器可访问。	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	必须是有效的 NTP 域。	（可选）允许您配置多个 NTP 服务器。要执行此操作，请输入 **y** 继续。
System Time Zone	必须是有效时区。例如，对于太平洋标准时间 (PST)，System Time Zone 为 PST8PDT（或协调世界时 (UTC) 减 8 小时）。 **注释** 确保系统时间和时区与 CIMC 或虚拟机监控程序主机操作系统时间和时区匹配。如果时区之间存在任何不匹配，系统性能可能会受到影响。 要获得受支持时区的完整列表，您可以从思科 ISE CLI 运行 **show timezones** 命令。 **注释** 建议您将所有思科 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）

提示	说明	示例
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。由于没有默认密码，您必须创建此密码才能继续。密码长度必须至少为六个字符，并且至少包含一个小写字母 (a - z)、一个大写字母 (A - Z) 和一个数字 (0 - 9)。	MyIseYPass2

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

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

运行设置程序后，系统会自动重新引导。

现在，您可以用设置过程中配置的用户名和密码登录到思科 ISE。

验证思科 ISE 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 输入新密码

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：

```
ise/admin# show application
<name>          <Description>
ise             Cisco Identity Services Engine
```

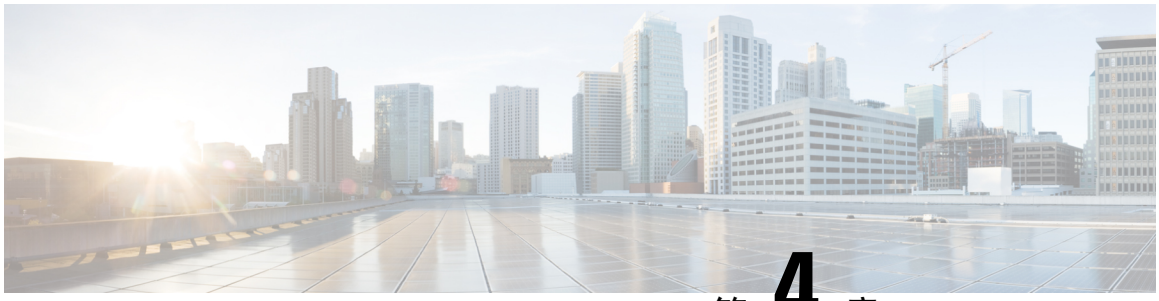
注释 此次发布的不同版本的版本和日期可能会因版本不同而各不相同。

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          14890
Database Server                        running          70 PROCESSES
Application Server                     running          19158
Profiler Database                      running          16293
ISE Indexing Engine                    running          20773
AD Connector                           running          22466
M&T Session Database                   running          16195
M&T Log Collector                      running          19294
M&T Log Processor                      running          19207
Certificate Authority Service          running          22237
EST Service                            running          29847
SXP Engine Service                     disabled
Docker Daemon                          running          21197
TC-NAC Service                         disabled
Wifi Setup Helper Container            not running
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

ise/admin#
```



第 4 章

Amazon Web 服务上的思科 ISE

Amazon Web 服务上的思科 ISE

通过 Amazon Web 服务 (AWS) 安全地将本地网络中的思科 ISE 策略扩展到新的远程部署。

您可以通过 CloudFormation 模板 (CFT) 或 Amazon 计算机映像 (AMI) 在 AWS 中配置和启动思科 ISE。我们建议通过以下列表中的两种方式之一来使用 CFT。要在 AWS 上启动思科 ISE，请：

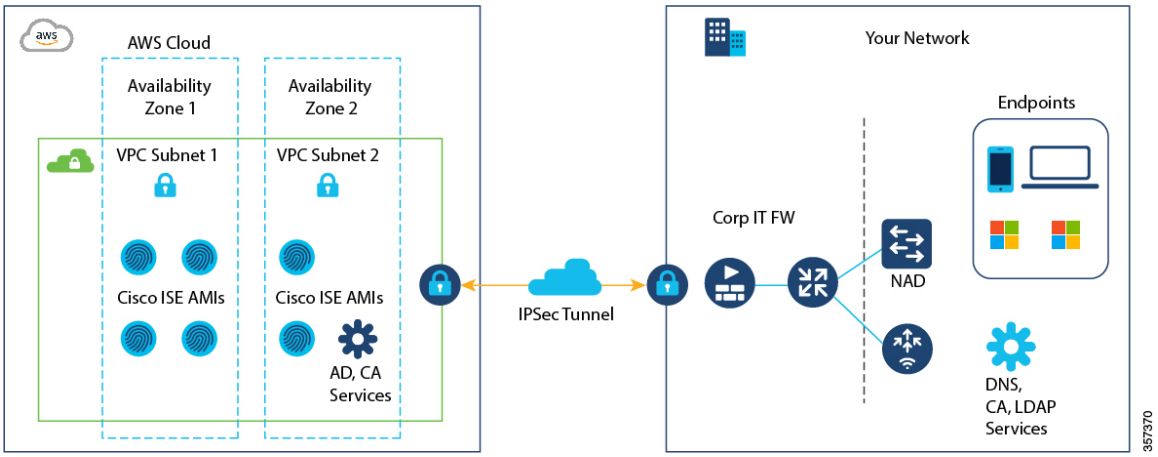
- 通过 AWS 市场启动思科 ISE CloudFormation 模板， 第 41 页
- 通过云计算组建模板启动思科 ISE ， 第 43 页
- 启动思科 ISE AMI

CFT 是让您能够轻松创建和管理云部署的 AWS 解决方案。通过在 AWS 中创建虚拟私有云将您的网络扩展到云中，同时配置虚拟私有网关，以便通过 IPsec 隧道与您的组织网络进行通信。

下图仅为示例。您可以根据组织的需求，在现场或 AWS 中放置证书颁发机构 (CA)、Active Directory (AD)、域名系统 (DNS) 服务器以及轻量级目录访问协议 (LDAP) 等常用服务。

Amazon Web 服务上的思科 ISE

图 *7:* 连接到 ***AWS*** 云的部署示例



有关在 AWS 中使用 CFT 的信息，请参阅《AWS CloudFormation 用户指南》。

下表包含了当前可用的思科 ISE 实例的详细信息。您必须购买思科 ISE VM 许可证才能使用以下任何实例。有关满足您特定要求的 EC2 实例定价的信息，请参阅 Amazon EC2 按需定价。

表 *13:* 思科 ***ISE*** 实例

思科 ISE 实例类型	CPU 核心	RAM（GB）
t3.xlarge 此实例支持思科 ISE 评估使用案例，并受思科 ISE 版本 3.1 补丁 1 及更高版本的支持。支持 100 个并发活动终端。	4	16
c5.4xlarge 建议用于 PSN。	16	32
m5.4xlarge 建议用于 PAN 和 MnT 节点。	16	64
c5.9xlarge 建议用于 PSN。	36	72

有关 AWS 实例类型的规模和性能数据的信息，请参阅《思科身份服务引擎性能和可扩展性指南》。

您可以利用 AWS S3 存储服务来轻松存储备份和恢复文件、监控和故障排除报告等。请参阅 使用 AWS S3 配置思科 ISE 版本 3.1 存储库。

AWS 上的 Cisco ISE 评估实例

如果您不熟悉 Cisco ISE 并希望评估 Cisco ISE 功能，可以使用评估实例 t3.xlarge。在启动新的思科 ISE 实例时，会自动启用评估许可证，有效期为 90 天。 t3.xlarge 实例在评估模式下支持 Cisco ISE。在评估模式下，思科 ISE 支持 100 个并发活动终端，允许您在 90 天内访问所有思科 ISE 功能。

实例类型	CPU 核心	RAM（GB）
t3.xlarge	4	16

t3.xlarge 实例仅在评估模式下支持 Cisco ISE。当您选择使用适当的许可证在网络中完全部署 Cisco ISE 时，必须使用 C 或 M 实例类型来安装和设置 Cisco ISE。t3.xlarge 实例支持 Cisco ISE 版本 3.1 补丁 1 及更高版本。

创建思科 ISE AWS 实例的前提条件

- 您必须熟悉 AWS 解决方案，例如 Amazon Elastic Compute Cloud（EC2) 实例和 Amazon Elastic Block Store (EBS) 卷，以及区域、可用性区域、安全组、虚拟私有云 (VPC) 等概念。有关这些解决方案的信息，请参阅 AWS 文档。

  您还必须熟悉管理 AWS 服务配额。

- AWS 中的 VPC 配置

  请参阅具有公共和专用子网以及 AWS 站点间 VPN 访问权限的 VPC。

- 要创建加密的 EBS 卷，您的 AWS 身份和访问管理 (IAM) 策略必须允许访问密钥管理服务 (KMS) 资源。请参阅 IAM 中的策略和权限。

- 首先在 AWS 中创建安全组、子网和密钥对，然后再配置思科 ISE 实例。

  为思科 ISE 创建安全组时，必须为要使用的思科 ISE 服务的所有端口和协议创建规则。请参阅思科 ISE 端口参考，第 115 页。

- 要为网络接口配置 IPv6 地址，子网必须具有在 AWS 中启用的 IPv6 CIDR 池。

- 您在思科 ISE CloudFormation 模板的**管理网络 (Management Network)** 字段中输入的 IP 地址不能是作为网络接口对象而存在于 AWS 中的 IP 地址。

- 您可以在部署中将静态 IP 配置为专用 IP。但是，必须为静态 IP 配置一个 DNS 可解析主机名。

在 AWS 上使用思科 ISE 的已知限制

以下是在 AWS 中使用思科 ISE 的已知限制：

- 您无法创建思科 ISE 实例的 Amazon EBS 快照，然后再使用该快照创建另一个 EBS 卷。

- Amazon VPC 仅支持第 3 层功能。AWS 实例上的思科 ISE 节点不支持依赖于第 1 层和第 2 层功能的思科 ISE 功能。例如，目前不支持同时使用 DHCP SPAN 分析器探头和使用思科 ISE CLI 的 CDP 协议。
- 不支持 NIC 绑定。
- 双网卡仅支持两个网卡 - 千兆以太网 0 和千兆以太网 1。要在思科 ISE 实例中配置辅助 NIC，必须先在 AWS 中创建网络接口对象，然后将该网络接口对象附加到思科 ISE。安装并启动 AWS 上的思科 ISE 后，通过思科 ISE CLI 将网络接口对象的 IP 地址手动配置为辅助 NIC。
- 思科 ISE 升级工作流程在 AWS 上的思科 ISE 中不可用。仅支持全新安装。但是，您可以执行配置数据的备份和恢复。当您在思科 ISE AWS 实例中恢复数据时，数据会升级到思科 ISE 版本 3.1。
- AWS 中不支持使用基于密码的身份验证对思科 ISE CLI 进行 SSH 访问。您只能通过密钥对来访问思科 ISE CLI，并且必须安全地存储此密钥对。

  如果您使用私钥（或 PEM）文件，而该文件已丢失，那么您将无法访问思科 ISE CLI。

  不支持使用基于密码的身份验证方法来访问思科 ISE CLI 的任何集成，例如思科全数字化网络架构 (DNA) 中心版本2.1.2 及更早版本。
- 当思科 ISE 处于空闲状态时，您可能会收到虚拟机资源不足警报。您可以忽略该警报，因为 CPU 频率保持低于有效节能所需的基准频率 (2 GHz)。
- 对于 Cisco ISE 3.1 软件版本，当您通过由 AWS 启动的 Cisco ISE 实例来运行 **show inventory** CLI 命令时，该命令的输出不会在输出中显示 AWS 上 Cisco ISE 的实例类型。软件版本 Cisco ISE 3.1 补丁 1 及更高版本不会发生此问题。
- 在通过 AWS 启动思科 ISE时，不能将 IPv6 服务器配置为 NTP 服务器。
- 不支持串行控制台监控。
- 默认情况下会生成初始管理员用户账号名称 admin。此用户账号名称用于在安装过程完成后对思科 ISE 进行 SSH 和 GUI 访问。
- 您无法调整 EC2 实例的大小。
- 您无法将思科 ISE 磁盘 EBS 卷转换为 AMI，然后再使用该 AMI 重新启动另一个 EC2 实例。
- 您可以集成位于现场的外部身份源。但是，由于延迟的原因，使用现场身份源时的思科 ISE 性能与使用 AWS 托管的身份源或思科 ISE 内部用户数据库时的思科 ISE 性能不相上下。
- 支持以下部署类型，但必须确保节点间延迟低于 300 毫秒：
  - 混合部署，在现场部署一些思科 ISE 节点，并在 AWS 中部署一些节点。
  - 通过 VPC 对等连接进行区域间部署。
- 不支持 Amazon EC2 用户数据脚本。

- 在配置的思科 ISE CFT 中，您可以定义卷大小 (GB)。但是，AWS 会以千兆字节 (GiB) 来创建 EBS 存储卷。因此，当您在思科 ISE CFT 中输入 600 作为卷大小时，AWS 会创建 600 GiB（即 644.25 GB）的 EBS 卷。
- 在通过思科 ISE CLI 或 GUI 在配置数据备份期间运行恢复操作时，请勿包含 ADE-OS 参数。
- 使用 Cisco ISE AMI 配置的 Cisco ISE 主服务器会自动注册为 Cisco ISE 中的 Cisco TrustSec AAA 服务器，且主机名和 IP 地址值不正确。您必须使用正确的详细信息注册 Cisco ISE 服务器，并从 Cisco TrustSec AAA 服务器列表中删除自动添加的服务器。有关配置 Cisco TrustSec AAA 服务器的信息，请参阅 《*Cisco ISE* 管理员指南》中“分段”章节中的“配置 Cisco TrustSec AAA 服务器”主题。
- 用户数据检索仅适用于元数据版本 V1 (IMDSv1)，但不适用于 V2 版本。

注释

- 从本地设备到 VPC 的通信必须是安全的。
- 在思科 ISE 版本 3.1 补丁 3 中，思科 ISE 会通过 IP 地址 169.254.169.254 将流量发送到 AWS 云，以便获取实例详细信息。这是为了检查它是否为云实例，以及是否可以在本地部署中忽略。

通过 AWS 市场启动思科 ISE CloudFormation 模板

您只能通过 CFT 配置来设置独立节点。要创建思科 ISE 部署，请参阅适用于您的版本的《思科 *ISE* 管理员指南》中“部署”一章。

您不能通过 CFT 添加多个 DNS 或 NTP 服务器。创建 Cisco ISE 实例后，您可以通过 Cisco ISE CLI 来添加更多 DNS 或 NTP 服务器。您也无法通过 CFT 来配置 IPv6 DNS 或 NTP 服务器。使用思科 ISE CLI 来配置 IPv6 服务器。

思科 ISE CFT 会创建卷类型通用 SSD (gp2) 的实例。

开始之前

在 AWS 中，创建要包含在思科 ISE CFT 配置中的安全组和管理网络。

步骤 1 通过以下网址登录到 Amazon 管理控制台：https://console.aws.amazon.com/，然后搜索 **AWS 市场订用 (AWS Marketplace Subscriptions)**。

步骤 2 在显示的**管理订用 (Manage Subscriptions)** 窗口中，点击左侧窗格中的**发现产品 (Discover Products)**。

步骤 3 在搜索栏中输入 **Cisco Identity Services Engine (ISE)** 。

步骤 4 点击产品名称，然后在显示的新窗口中点击**继续订用 (Continue to Subscribe)**。

步骤 5 点击**继续配置 (Continue to Configuration)**。

步骤 6 在**配置此软件 (Configure this software)** 区域中，点击**了解更多 (Learn More)**，然后点击**下载 CloudFormation 模板 (Download CloudFormation Template)** 将思科 ISE CFT 下载到本地系统。您可以根据需要使用此模板来自动配置其他思科 ISE 实例。

您还可以点击**了解更多 (Learn More)** 信息对话框中的**查看模板 (View Template)**，以查看 CFT 的 AWS CloudFormation Designer。

步骤 7 从**软件版本 (Software Version)** 和 **AWS 区域 (AWS Region)** 下拉列表中选择所需的值。

步骤 8 点击**继续启动 (Continue to Launch)**。

步骤 9 从**选择操作 (Choose Action)** 下拉列表中选择**启动 CloudFormation (Launch CloudFormation)**。

步骤 10 点击**启动**。

步骤 11 在**创建堆栈 (Create Stack)** 窗口中，点击**模板就绪 (Template Is Ready)** 和 **Amazon S3 URL** 单选按钮。

步骤 12 点击**下一步 (Next)**。

步骤 13 在新窗口中，在**堆栈名称 (Stack Name)** 字段中输入值。

步骤 14 在**参数 (Parameters)** 区域的下列字段中输入所需的详细信息：

- **主机名 (Hostname)**：此字段仅支持字母数字字符和连字符 (-)。主机名的长度不应超过 19 个字符。
- **实例密钥对 (Instance Key Pair)**：要通过 SSH 访问思科 ISE 实例，请选择您在 AWS 中为用户名 iseadmin 创建的 PEM 文件（在思科 ISE 版本 3.1 中用户名为 admin）。如果尚未配置，请立即在 AWS 中创建一个 PEM 密钥对。此场景中的 SSH 命令示例：**ssh -i mykeypair.pem iseadmin@myhostname.compute-1.amazonaws.com**。
- **管理安全组 (Management Security Group)**：从下拉列表中选择安全组。在配置此 CFT 之前，您必须在 AWS 中创建安全组。

  注释　在此步骤中，只能添加一个安全组。您可以在 Cisco ISE 安装后添加其他安全组。确保在您在此处添加的安全组中配置您希望在设置时在 Cisco ISE 中可用的网络流量规则。

- **管理网络 (Management Network)**：选择要用于思科 ISE 接口的子网。要启用 IPv6 地址，您必须将 IPv6 CIDR 块与 VPC 和子网相关联。如果尚未配置子网，请立即在 AWS 中创建一个子网。
- **管理专用 IP (Management Private IP)**：输入您之前选择的子网中的 IPv4 地址。如果将此字段留空，则 AWS DHCP 会分配一个 IP 地址。

  创建思科 ISE 实例后，从**实例摘要 (Instance Summary)** 窗口复制专用 IP 地址。然后，在创建思科 ISE 部署之前，将该 IP 映射到您的 DNS 服务器的主机名。

- **时区 (Timezone)**：从下拉列表中选择系统时区。
- **实例类型 (Instance Type)**：从下拉列表中选择思科 ISE 实例类型。
- **EBS 加密 (EBS Encryption)**：从下拉列表中选择 **True** 以启用加密。该字段的默认值为 **False**
- **卷大小 (Volume Size)**：指定卷大小 (GB)。可接受的范围为 300 GB 到 2400 GB。我们建议在实际使用中选择 600 GB。配置小于 600 GB 的卷大小仅用于评估目的。当您终止实例时，该卷也会被删除。

  注释　AWS 以十亿字节 (GiB) 创建 EBS 存储卷。当您在**卷大小 (Volume Size)** 字段中输入 600 时，AWS 会创建 600 GiB（或 644.25 GB）的 EBS 卷。

- **DNS 域 (DNS Domain)**：此字段接受的值为 ASCII 字符、数字、连字符 (-) 和句点 (.)。

- **名称服务器 (Name Server)**：以正确的语法输入名称服务器的 IP 地址。

  注释　在此步骤中，您只能添加一个 DNS 服务器。在安装后，您可以通过思科 ISE CLI 来添加其他 DNS 服务器。

- **NTP 服务器 (NTP Server)**：以正确的语法输入 NTP 服务器的 IP 地址或主机名，例如 **time.nist.gov**。您的条目在提交时未得到验证。如果使用错误的语法，思科 ISE 服务可能无法在启动时出现。

  注释　如果您在此处输入的 IP地址或主机名不正确，则思科 ISE无法与NTP服务器同步。使用 SSH 终端登录思科 ISE，然后使用思科 ISE CLI 来配置正确的 NTP 服务器。

  在此步骤中，您只能添加一个 NTP 服务器。在安装后，您可以通过思科 ISE CLI 来添加其他 NTP 服务器。

- **ERS**：要在思科 ISE 启动时启用 ERS 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **OpenAPI**：要在思科 ISE 启动时启用 OpenAPI 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **pxGrid**：要在思科 ISE 启动时启用 pxGrid 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **pxGrid 云 (pxGrid Cloud)**：此字段的默认值为**否 (no)**。
- **输入密码 (Enter Password)**：输入必须用于 GUI 的管理密码。密码必须符合思科 ISE 密码策略。密码会在 AWS 控制台实例设置窗口的**用户数据 (User Data)** 区域中以纯文本显示。请参阅适用于您版本的《思科 *ISE* 管理员指南》“基本设置”一章中的“用户密码策略”部分。
- **确认密码 (Confirm Password)**：重新键入管理密码

步骤 15　点击**下一步 (Next)** 启动实例创建过程。

通过云计算组建模板启动思科 ISE

您只能通过 CFT 配置来设置独立节点。要创建思科 ISE 部署，请参阅适用于您的版本的《思科 *ISE* 管理员指南》中“部署”一章。

您不能通过 CFT 添加多个 DNS 或 NTP 服务器。创建思科 ISE 实例后，您可以通过思科 ISE CLI 来添加其他 DNS 或 NTP 服务器。您也无法通过 CFT 来配置 IPv6 DNS 或 NTP 服务器。使用思科 ISE CLI 来配置 IPv6 服务器。

思科 ISE CFT 会创建卷类型通用 SSD (gp2) 的实例。

开始之前

在 AWS 中，创建要包含在思科 ISE CFT 配置中的安全组和管理网络。

步骤 1　通过以下网址登录到 Amazon 管理控制台：https://console.aws.amazon.com/，然后搜索 **AWS 市场订用 (AWS Marketplace Subscriptions)**。

步骤 2 在显示的**管理订用 (Manage Subscriptions)** 窗口中，点击左侧窗格中的**发现产品 (Discover Products)**。

步骤 3 在搜索栏中输入 **Cisco Identity Services Engine (ISE)**。

步骤 4 点击产品名称，然后在显示的新窗口中点击**继续订用 (Continue to Subscribe)**。

步骤 5 点击**继续配置 (Continue to Configuration)**。

步骤 6 在**配置此软件 (Configure this software)** 区域中，点击**了解更多 (Learn More)**，然后点击**下载 CloudFormation 模板 (Download CloudFormation Template)** 将思科 ISE CFT 下载到本地系统。您可以根据需要使用此模板来自动配置其他思科 ISE 实例。

您还可以点击**了解更多 (Learn More)** 信息对话框中的**查看模板 (View Template)**，以查看 CFT 的 AWS CloudFormation Designer。

步骤 7 在 AWS 搜索栏中，搜索 **CloudFormation**。

步骤 8 从**创建堆栈 (Create Stack)** 下拉列表中，选择**使用新资源（标准）(With new resources [standard])**。

步骤 9 在**创建堆栈 (Create Stack)** 窗口中，选择**模板就绪 (Template Is Ready)** 和**上传模板文件 (Upload a Template File)**。

步骤 10 点击**选择文件 (Choose File)** 并上传您在第 7 步中下载的 CFT 文件。

步骤 11 点击**下一步 (Next)**。

步骤 12 在新窗口中，在**堆栈名称 (Stack Name)** 字段中输入值。

步骤 13 在**参数 (Parameters)** 区域的下列字段中输入所需的详细信息：

- **主机名 (Hostname)**：此字段仅支持字母数字字符和连字符 (-)。主机名的长度不应超过 19 个字符。
- **实例密钥对 (Instance Key Pair)**：要通过 SSH 访问思科 ISE 实例，请选择您在 AWS 中为用户名 admin 创建的 PEM 文件。如果尚未配置，请立即在 AWS 中创建一个 PEM 密钥对。此场景中的 SSH 命令示例：**ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com**。
- **管理安全组 (Management Security Group)**：从下拉列表中选择安全组。在配置此 CFT 之前，您必须在 AWS 中创建安全组。

  注释　在此步骤中，只能添加一个安全组。您可以在 Cisco ISE 安装后添加其他安全组。确保在您在此处添加的安全组中配置您希望在设置时在 Cisco ISE 中可用的网络流量规则。

- **管理网络 (Management Network)**：选择要用于思科 ISE 接口的子网。要启用 IPv6 地址，您必须将 IPv6 CIDR 块与 VPC 和子网相关联。如果尚未配置子网，请立即在 AWS 中创建一个子网。
- **管理专用 IP (Management Private IP)**：输入您之前选择的子网中的 IPv4 地址。如果将此字段留空，则 AWS DHCP 会分配一个 IP 地址。

  创建思科 ISE 实例后，从**实例摘要 (Instance Summary)** 窗口复制专用 IP 地址。然后，在创建思科 ISE 部署之前，将该 IP 地址映射到您的 DNS 服务器的主机名。
- **时区 (Timezone)**：从下拉列表中选择系统时区。
- **实例类型 (Instance Type)**：从下拉列表中选择思科 ISE 实例类型。
- **EBS 加密 (EBS Encryption)**：从下拉列表中选择 **True** 以启用加密。该字段的默认值为 **False**。
- **卷大小 (Volume Size)**：指定卷大小 (GB)。可接受的范围为 300 GB 到 2400 GB。我们建议在实际使用中选择 600 GB。配置小于 600 GB 的卷大小仅用于评估目的。当您终止实例时，该卷也会被删除。

注释　AWS 以十亿字节 (GiB) 创建 EBS 存储卷。当您在**卷大小 (Volume Size)** 字段中输入 600 时，AWS 会创建 600 GiB（或 644.25 GB）的 EBS 卷。

- **DNS 域 (DNS Domain)**：此字段接受的值为 ASCII 字符、数字、连字符 (-) 和句点 (.)。
- **名称服务器 (Name Server)**：以正确的语法输入名称服务器的 IP 地址。

  注释　在此步骤中，您只能添加一个 DNS 服务器。在安装后，您可以通过思科 ISE CLI 来添加其他 DNS 服务器。

- **NTP 服务器 (NTP Server)**：以正确的语法输入 NTP 服务器的 IP 地址或主机名，例如 **time.nist.gov**。您的条目在提交时未得到验证。如果使用错误的语法，思科 ISE 服务可能无法在启动时出现。

  注释　如果您在此处输入的 IP地址或主机名不正确，则思科 ISE无法与NTP服务器同步。使用 SSH 终端登录思科 ISE，接着使用思科 ISE CLI 来配置正确的 NTP 服务器。

  在此步骤中，您只能添加一个 NTP 服务器。在安装后，您可以通过思科 ISE CLI 来添加其他 NTP 服务器。

- **ERS**：要在思科 ISE 启动时启用 ERS 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **OpenAPI**：要在思科 ISE 启动时启用 OpenAPI 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **pxGrid**：要在思科 ISE 启动时启用 pxGrid 服务，请输入**是 (yes)**。此字段的默认值为**否 (No)**。
- **pxGrid 云 (pxGrid Cloud)**：此字段的默认值为**否 (no)**。

  注释　pxGrid 云功能当前不可用，因为对补充产品版本存在依赖关系。不启用 pxGrid 云服务。

- **输入密码 (Enter Password)**：输入必须用于 GUI 的管理密码。密码必须符合思科 ISE 密码策略。密码会在 AWS 控制台实例设置窗口的**用户数据 (User Data)** 区域中以纯文本显示。请参阅适用于您版本的《思科 *ISE* 管理员指南》“基本设置”一章中的“用户密码策略”部分。
- **确认密码 (Confirm Password)**：重新键入管理密码

步骤 14　点击**下一步 (Next)** 启动实例创建过程。

启动思科 ISE AMI

步骤 1　通过 https://console.aws.amazon.com/ec2/ 登录 Amazon EC2 控制台。
步骤 2　从左侧窗格中，选择**实例 (Instances)**。
步骤 3　在显示的**实例 (Instances)** 窗口中，点击**启动实例 (Launch Instances)**。
步骤 4　在显示的**第 1 步：选择 AMI (Step 1: Choose AMI)** 窗口中，点击左侧菜单中的 **AWS 市场 (AWS Marketplace)**。
步骤 5　在搜索字段中，输入**思科身份服务引擎 (Cisco Identity Services Engine)**。
步骤 6　在显示的**思科身份服务引擎 (ISE) (Cisco Identity Services Engine [ISE])** 选项中，点击**选择 (Select)**。

步骤 7 系统将显示**思科身份服务引擎 (ISE) (Cisco Identity Services Engine [ISE])** 对话框，其中包含 AMI 的各种详细信息。查看信息，然后点击**继续 (Continue)** 以继续。

步骤 8 在显示的**第 2 步：选择实例类型 (Step 2: Choose an Instance Type)** 窗口中，点击要使用的实例类型旁边的单选按钮。 支持的实例类型包括：

- c5.4xlarge
- m5.4xlarge
- c5.9xlarge

步骤 9 点击**下一步：配置实例详细信息 (Next: Configure Instance Details)**。

步骤 10 在**第 3 步：配置实例详细信息 (Step 3: Configure Instance Details)** 窗口中，在以下字段中输入所需的详细信息：

- **实例数量 (Number of Instances)**：您必须在此字段中输入 **1**。
- **网络 (Network)**：从下拉列表中选择要在其中启动思科 ISE 实例的 VPC。
- **子网 (Subnet)**：从下拉列表中选择要在其中启动思科 ISE 实例的子网。
- **网络接口 (Network Interfaces)**：默认情况下，下拉列表会显示**新网络接口 (New Network Interface)**，这意味着 IP 地址会由连接的 DHCP 服务器自动分配给思科 ISE。您可以选择在此字段中输入 IP 地址，以便为思科 ISE 分配一个固定 IP 地址。您还可以从**网络接口 (Network Interfaces)** 下拉列表中选择同一子网中的现有网络接口。在设置过程中，您只能配置一个接口。安装思科 ISE 后，您可以通过思科 ISE 添加更多接口。

步骤 11 在**高级详细信息 (Advanced Details)** 区域中，点击**用户数据 (User Data)** 字段中的**作为文本 (As Text)** 单选按钮，然后按以下格式输入键值对：

hostname=<hostname of Cisco ISE>

primarynameserver=<IPv4 address>

dnsdomain=<example.com>

ntpserver=<IPv4 address or FQDN of the NTP server>

timezone=<timezone>

username=<admin>

password=<password>

ersapi=<yes/no>

openapi=<yes/no>

pxGrid=<yes/no>

pxgrid_cloud=<yes/no>

您必须为通过用户数据条目配置的每个字段使用正确的语法。您在用户数据字段中输入的信息在输入时不会经过验证。如果使用错误的语法，启动 AMI 时可能就不会显示思科 ISE 服务。以下是您通过用户数据字段提交的配置的说明：

- hostname：输入的主机名只能包含字母数字字符和连字符 (-)。主机名的长度不能超过 19 个字符，并且不能包含下划线。

- primarynameserver：输入主名称服务器的 IP 地址。只有 IPv4 地址受支持。
- dnsdomain：输入 DNS 域的 FQDN。条目可以包含 ASCII 字符、数字、连字符 (-) 和句点 (.)。
- ntpserver：输入必须用于同步的 NTP 服务器的 IPv4 地址或 FQDN。例如，time.nist.gov。
- timezone：输入时区。例如，“Etc/UTC”。我们建议将所有思科 ISE 节点均设置为协调世界时 (UTC) 时区，特别是在您的思科 ISE 节点都安装于分布式部署中的情况下。此程序可确保来自您的部署中各个节点的报告和日志的时间戳始终同步。
- username：您配置的默认用户名必须是 **admin**。如果配置的用户名不是 **admin**，则启动 AMI 时将无法访问思科 ISE CLI。
- password：为基于 GUI 的思科 ISE 登录配置密码。您输入的密码必须符合思科 ISE 密码策略。例如，密码必须至少包含 8 个字符，并且至少包含一个小写字母、一个大写字母和一个数字。密码不得包含某些词典条目，例如 admin、cisco、password 等。请参阅适用于您版本的《思科 ISE 管理员指南》“基本设置”一章中的“用户密码策略”。
- ersapi：输入 **yes** 以启用 ERS，或输入 **no** 以禁止 ERS。
- openapi：输入 **yes** 以启用 OpenAPI，或输入 **no** 以禁用 OpenAPI。
- pxGrid：输入 **yes** 以启用 pxGrid，或输入 **no** 以禁用 pxGrid。
- pxgrid_cloud：输入 **yes** 以启用 pxGrid 云，或输入 **no** 以禁用 pxGrid 云。要启用 pxGrid 云，则必须启用 pxGrid。如果禁用 pxGrid 但启用 pxGrid 云，则在启动时不会启用 pxGrid 云服务。

步骤 12 点击**下一步：添加存储 (Next: Add Storage)**。

步骤 13 在**第 4 步：添加存储 (Step 4: Add Storage)** 窗口中：

a) 在**大小 (GiB) (Size [GiB])** 列中输入值。

此字段的有效范围为 279.4 至 2235.2 GiB。在生产环境中，存储必须配置为等于或大于 558.8 GiB。小于 558.8 GiB 的存储仅支持评估环境。请注意，思科 ISE 以 GB 为单位来创建存储。此处输入的 GiB 值会在思科 ISE 映像创建过程中自动转换为 GB 值。以 GB 为单位，有效存储范围为 300 – 2400 GB，其中 600 GB 是思科 ISE 在生产环境下使用的最小值。

b) 在**卷类型 (Volume Type)** 字段中，从下拉列表中选择**通用 SSO (gp2) (General Purpose SSO [gp2])**。

c) 要启用 EBS 加密，请在**加密 (Encryption)** 字段的下拉列表中选择加密密钥。

注释 不要点击此窗口中显示的**添加新卷 (Add New Volume)** 按钮。

步骤 14 点击**下一步：添加标记 (Next: Add Tags)**。

步骤 15 （可选）在**第 5 步：添加标签 (Step 5: Add Tags)** 窗口中，点击**添加标签 (Add Tag)**，然后在**键 (Key)** 和**值 (Value)** 字段中输入所需信息。**实例 (Instances)**、**卷 (Volumes)** 和**网络接口 (Network Interfaces)** 列中的复选框会被默认选中。如果您在**第 3 步：配置实例详细信息 (Step 3: Configure Instance Details)** 窗口中选择了特定网络接口，则必须取消选中此窗口中添加的每个标记的**网络接口 (Network Interfaces)** 复选框。

步骤 16 点击**下一步：配置安全组 (Next: Configure Security Group)**。

步骤 17 在**第 6 步：配置安全组 (Step 6: Configure Security Group)** 窗口的**分配安全组 (Assign a security group)** 区域中，您可以选择创建新的安全组，或者或通过点击相应的单选按钮来选择现有的安全组。

a) 如果选择**创建新安全组 (Create a new security group)**，请在**类型 (Type)**、**协议 (Protocol)**、**端口范围 (Port Range)**、**源 (Source)** 和**说明 (Description)** 字段中输入所需的详细信息。

b) 如果选择**选择现有安全组 (Select an existing security group)**，请选中要添加的安全组旁边的复选框。

步骤 18 点击**检查和启动 (Review and Launch)**。

步骤 19 在**第 7 步：查看实例启动 (Step 7: Review Instance Launch)** 窗口中，查看您在此工作流程中创建的所有配置。您可以通过点击相应的**编辑 (Edit)** 链接来编辑这些部分的值。

步骤 20 点击**启动 (Launch)**。

步骤 21 在显示的**选择现有密钥对或创建新密钥对 (Select an existing key pair or create a new key pair)** 对话框中，从下拉列表中选择以下选项之一：

- **选择现有密钥对 (Choose an existing key pair)**
- **创建新密钥对 (Create a new key pair)**

注释 要使用 SSH 登录思科 ISE，请使用用户名为 **iseadmin** 的密钥对。密钥对必须保持完整。如果密钥对丢失或损坏，则无法恢复思科 ISE，因为无法将新的密钥对映射到现有的实例。

步骤 22 选中确认语句的复选框，然后点击**启动实例 (Launch Instances)**。

步骤 23 **启动状态 (Launch Status)** 窗口会显示实例的创建进度。

安装后备注和任务

要检查实例启动的状态，请在 AWS 控制台的左侧窗格中点击**实例 (Instances)**。在配置实例时，实例的**状态检查 (Status Check)** 列显示**正在初始化 (Initializing)**。当实例就绪且可用时，该列HUI 显示**完成 x 个检查 (x checks done)**。

在构建思科 ISE EC2 实例大约 30 分钟后，您便可以访问思科 ISE GUI 或 CLI。您可以使用 AWS 为您的实例提供的 IP 地址来访问思科 ISE 的 CLI 和 GUI，并登录到思科 ISE 管理门户或控制台。

当思科 ISE 实例准备就绪并可供使用时，请执行以下步骤：

1. 在 AWS 中创建密钥对时，系统会提示您将密钥对下载到本地系统中。下载密钥对，因为它包含必须更新的特定权限，这样才能从 SSH 终端成功登录到思科 ISE 实例。

   如果使用 Linux 或 macOS 操作系统，请在 CLI 应用中运行以下命令：

   sudo chmod 0400 mykeypair.pem

   如果使用的 Windows 操作系统：

   1. 右键点击本地系统中的密钥文件。
   2. 选择**属性 (Properties)** > **安全 (Security)** > **高级 (Advanced)**。
   3. 在**权限 (Permissions)** 选项卡中，通过点击相应选项将完全控制分配给相应用户，然后点击**禁用继承 (Disable Inheritance)**。

4. 在**阻止继承 (Block Inheritance)** 对话框中，点击**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
5. 在 **权限 (Permissions)** 选项卡的**权限条目 (Permissions entries)** 区域中，通过点击相应条目选择系统和管理员用户，然后点击**删除 (Remove)**。
6. 点击**应用 (Apply)**，然后点击**确定 (OK)**。

2. 通过在 CLI 程序应用中运行以下命令来访问思科 ISE CLI：

   ssh -i mykeypair.pem admin@<*Cisco ISE Private IP Address*>
3. 在登录提示后，输入 **admin** 作为用户名。
4. 在系统提示时，输入 **show application version ise** 并按 **Enter**。
5. 要查看思科 ISE 进程的状态，请输入 **show application status ise** 并按 **Enter**。

   如果输出显示应用服务器处于运行状态，则思科 ISE 可供使用。
6. 然后，您可以登录到思科 ISE GUI。
7. 然后，执行安装后任务列表，第 103 页中列出的安装后任务。

AWS 上的思科 ISE 兼容性信息

本节详细介绍 AWS 上思科 ISE 特有的兼容性信息。有关思科 ISE 的一般兼容性详细信息，请参阅《Cisco 身份识别服务引擎网络组件兼容性，版本 3.1》。

思科全数字化网络架构 (DNA) 中心集成支持

您可以将思科 ISE 连接到思科全数字化网络架构 (DNA) 中心版本 2.2.1 及更高版本。

负载均衡器集成支持

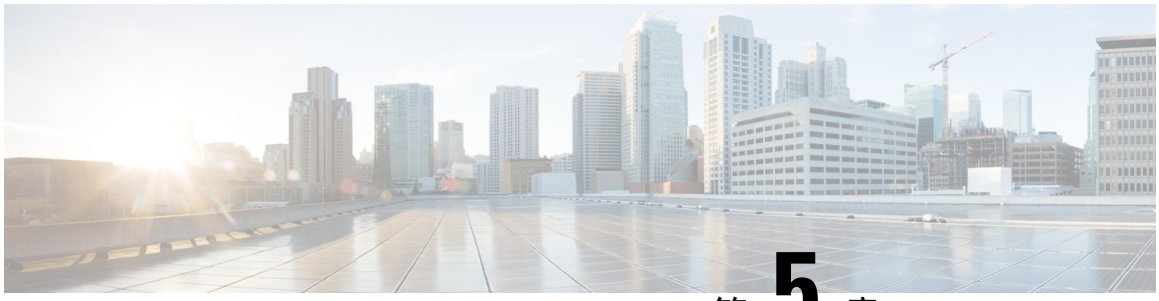
您可以将 AWS 本地网络负载均衡器 (NLB) 与思科 ISE 集成，以实现 RADIUS 流量的负载均衡。但以下警告适用：

- 仅当您在 NLB 中启用客户端 IP 保留时，才会支持授权更改 (CoA) 功能。
- 由于 NLB 仅支持源 IP 关联而不支持基于呼叫站 ID 的粘滞会话，因此可能会出现不均衡的负载均衡。
- 流量可以发送到思科 ISE PSN，即使 RADIUS 服务在节点上未处于活动状态，因为 NLB 不支持基于 RADIUS 的运行状况检查。

您可以将 AWS 本地网络负载均衡器 (NLB) 与思科 ISE 集成，以实现 TACACS 流量的负载均衡。但是，即使 TACACS 服务在节点上未处于活动状态，也可能会将流量发送到思科 ISE PSN，因为 NLB 不支持基于TACACS+ 服务的运行状况检查。

NIC 巨帧支持

思科 ISE 支持巨帧。思科 ISE 的最大传输单位 (MTU) 为 9,001 字节，而网络接入设备的 MTU 通常为 1,500 字节。思科 ISE 支持并接收标准和巨帧，而不会出现问题。您可以在配置模式下通过思科 ISE CLI 根据需要来重新配置思科 ISE MTU。



第 5 章

其他安装信息

SNS 设备参考

创建一个可引导 USB 设备以安装思科 ISE

使用 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 https://github.com/lmacken/liveusb-creator/releases/tag/3.12.0LiveUSB-creator 下载到本地系统。
- 将思科 ISE 安装 ISO 文件下载至本地系统。
- 使用 16 GB 或 32 GB USB 设备。

步骤 1 使用 FAT16 或 FAT32 重新格式化 USB 设备以释放所有空间。

步骤 2 将 USB 设备插入本地系统，然后启动 **LiveUSB-creator**。

步骤 3 从**使用现有 Live CD (Use existing Live CD** 区域中点击**浏览 (Browse)**，并选择思科 ISE ISO 文件。

步骤 4 从**目标设备 (Target Device)** 下拉列表中选择 USB 设备。

如果本地系统只连接了一个 USB 设备，会自动选择该设备。

步骤 5 点击**创建 Live USB (Create Live USB)**。

进度条会指示可引导 USB 创建的进度。完成此过程后，即可在用于运行 USB 工具的本地系统访问 USB 驱动器的内容。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：

- isolinux/*isolinux.cfg* or 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 3595、3615、3655 或 3695 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。

重新映像思科 SNS 3500/3600 系列设备

思科 SNS 3500/3600 系列设备没有内置 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 3500 和 3600 系列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 3500 和 3600 系列设备上，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。

- 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#unique_64。
- 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#unique_65和#unique_64。

VMware 虚拟机

注释 本文档提供的 VMware 外形规格说明也适用于安装在思科 Hyperflex 上的思科 ISE。

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思科 ISE 安装的情况下运行 。您可以从思科 ISE 启动菜单执行此测试。

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 服务器的必备条件

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必备条件：

- 务必要以具有管理权限的用户身份（根用户）登录 ESXi 服务器。
- 思科 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)。
- 确保在 VMware 虚拟机上分配建议的磁盘空间量。请参阅 #unique_31 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思科 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 1.999 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虚拟化技术，无需重新引导设备。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 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思科 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 **高级(Advanced)** > **处理器配置 (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**配置 (Configuration)** > **网络 (Networking)** > **属性 (Properties)** > **VMNetwork**（VMware 服务器实例的名称）**VMswitch0**（其中一个 VMware ESXi 服务器接口） **属性 (Properties)** **安全 (Security)**。

步骤 2 在**安全 (Security)** 选项卡上的“策略例外”(Policy Exceptions) 窗格中，选中**混合模式 (Promiscuous Mode)** 复选框。

步骤 3 在“混合模式”(Promiscuous Mode) 下拉列表中，选择**接受 (Accept)**，然后点击 **确定 (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**编辑 (Edit)**。

步骤 3 点击“硬件”(Hardware) 选项卡上的**添加 (Add)**。

步骤 4 选择**串行端口 (Serial Port)**，然后点击**下一步 (Next)**。

步骤 5 在“串行端口输出”(Serial Port Output) 区域中，点击 **在主机上使用物理串行端口 (Use physical serial port on the host)** 或**通过网络连接 (Connect via Network)** 单选按钮，然后点击**下一步 (Next)**。

- 如果选择“通过网络连接”(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“使用物理串行端口”(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**下一步 (Next)**。

步骤 7 在“设备状态”(Device Status) 区域中，选中相应的复选框。默认值为“已连接”(Connected)。

步骤 8 点击**确定 (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 服务器的必备条件。

步骤 1 登录 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**新虚拟机 (New Virtual Machine)**。

步骤 3 在“配置”(Configuration) 对话框中，针对 VMware 配置选择**自定义 (Custom)**，然后点击**下一步 (Next)**。

步骤 4 输入 VMware 系统的名称，然后点击**下一步 (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数据存储，然后点击**下一步 (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**下一步 (Next)**。

步骤 7 从**版本 (Version)** 下拉列表中选择 **Linux**，然后选择支持的 Red Hat Enterprise Linux 版本。

步骤 8 从“虚拟插槽数量”(Number of virtual sockets) 和“每个虚拟插槽的内核数量”(Number of cores per virtual socket) 下拉列表中选择一个值。核心总数应为：

SNS 3600 系列设备：

- 小型 - 16
- 中型 - 24
- 大型 - 24

由于超线程，核心数量相当于思科安全网络服务器3600系列中核心数量的两倍。例如，对于小型网络部署，您必须分配 16 个 vCPU 核心才能满足 SNS 3615（包含 8 个 CPU 核心或 16 个线程）的 CPU 规格。

注释 强烈建议您保留 CPU 和内存资源以匹配资源配置。否则可能会严重影响 ISE 的性能和稳定性。

步骤 9 选择内存量，然后点击**下一步 (Next)**。

步骤 10 从“适配器”(Adapter) 下拉列表中选择 **E1000** NIC 驱动程序，然后点击**下一步 (Next)**。

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。

步骤 11 选择 **Paravirtual** 作为 SCSI 控制器，然后点击**下一步 (Next)**。

步骤 12 选择**创建新虚拟磁盘 (Create a new virtual disk)**，然后点击**下一步 (Next)**。

步骤 13 在“磁盘调配”(Disk Provisioning) 对话框中，点击**密集调配 (Thick Provision)** 单选按钮，然后点击**下一步 (Next)** 继续。

思科 ISE 同时支持详细和精简调配。但是，我们建议您选择密集调配快速归零以获取更好的性能，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**支持群集功能，例如容错能力 (Support clustering features such as Fault Tolerance)** 复选框。

步骤 15 选择高级选项，然后点击**下一步 (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。

步骤 17 点击**完成 (Finish)**。

系统现已安装 VMware 系统。

下一步做什么

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**电源 (Power)** > **开启电源 (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**编辑设置 (Edit Settings)**。

步骤 2 点击**选项 (Options)** 选项卡。

步骤 3 选择 **高级(Advanced)** > **引导选项 (Boot Options)**。

步骤 4 从**开机引导延迟 (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**强制 BIOS 设置 (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**确定 (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，则思科 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) 下载思科 ISE 软件并将其刻录在 DVD 上。您将需要提供 Cisco.com 凭证。
- （可选；仅当您在 VMware 云上安装思科 ISE 时适用）在 VMware 云上安装思科 ISE 的过程与在 VMware 虚拟机上安装思科 ISE 的过程完全相同。

- 部署在 Amazon Web 服务 (AWS) 上 VMware 云中的思科 ISE 虚拟机：思科 ISE 可以托管在 AWS 上 VMware 云提供的软件定义的数据中心 (SDDC) 上。确保在 VMware 云上配置适当的安全组策略（在**网络和安全 (Networking & Security) > 安全 (Security) > 网关防火墙设置 (Gateway Firewall Settings)** 下）以支持访问现场部署、必需设备和服务。
- 部署在 Azure VMware 解决方案 (AVS) 上的思科 ISE 虚拟机：AVS 在 Microsoft Azure 上本地运行 VMware 工作负载，思科 ISE 可从中托管为 VMware 虚拟机。

步骤 1 登录到 VMware 客户端。

步骤 2 要使 VM 进入 BIOS 设置模式，请右键点击 VM，然后选择**编辑设置 (Edit Settings)**。

步骤 3 点击**选项 (Options)** 选项卡。

步骤 4 点击**引导选项 (Boot Options)**，然后在**强制 BIOS 设置 (Force BIOS Setup)** 区域中选中 **BIOS** 复选框，以便在 VM 引导时进入 BIOS 设置屏幕。

注释 您必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

步骤 5 点击**确定 (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 VM 已开启，请关闭系统。

b) 打开 VM。

系统进入 BIOS 设置模式。

c) 在主 **BIOS** 菜单中，使用箭头键导航到**日期和时间 (Date and Time)** 字段，然后按 **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“退出”(Exit) 菜单，并选择**退出并保存更改 (Exit Saving Changes)**。

h) 选择**是 (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：

```
Automatic installation starts in 150 seconds.
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)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

步骤 8 使用箭头键选择**思科 ISE 安装（串行控制台）(Cisco ISE Installation [Serial Console])** 或**思科 ISE 安装（键盘/监视器）(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 系统上启动思科 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**。

注释 从思科 ISE 版本 3.0 开始，托管 ISE 虚拟机的虚拟化平台的 CPU 必须支持（流传输 SIMD 扩展）SSE 4.2 指令集。否则，某些 ISE 服务（例如 ISE API 网关）将无法工作，并且无法启动思科 ISE GUI。Intel 和 AMD 处理器自 2011 年以来一直支持 SSE 4.2 版本。

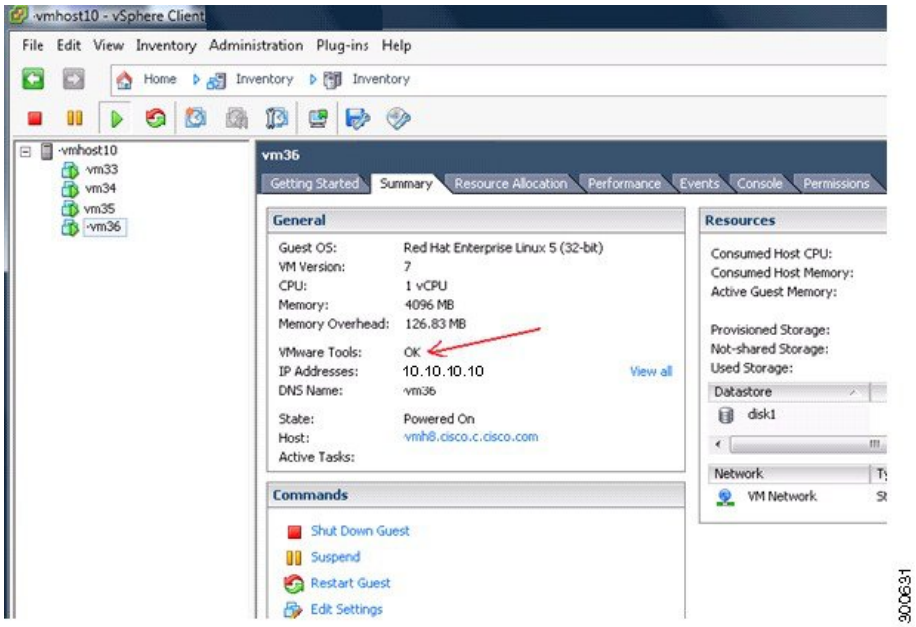
系统随即会显示安装向导并引导您完成初始配置。

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 *8:* 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。

```
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9       , VID: A0  , SN: FCH184X9XXX
Total RAM Memory: 65700380 kB
CPU Core Count: 16
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 4: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 5: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 6: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 7: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 8: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 9: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 10: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 11: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 12: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 13: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 14: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 15: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /xxx/abc
Disk 0: Capacity: 1198.00 GB
NIC Count: 6
NIC 0: Device Name: eth0:
NIC 0: HW Address: xx:xx:xx:xx:xx:xx
NIC 0: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 1: Device Name: eth1:
NIC 1: HW Address: xx:xx:xx:xx:xx:xx
NIC 1: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: HW Address: xx:xx:xx:xx:xx:xx
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: HW Address: xx:xx:xx:xx:xx:xx
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: HW Address: xx:xx:xx:xx:xx:xx
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
NIC 5: HW Address: xx:xx:xx:xx:xx:xx
NIC 5: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

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

对升级 VMware 工具的支持

思科 ISE ISO 映像（常规、升级或补丁）包含受支持的 VMware 工具。思科 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思科 ISE（常规、升级或补丁版本）提供支持。

克隆思科 ISE 虚拟机

您可以克隆思科 ISE VMware 虚拟机 (VM) 来创建与思科 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思科 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

- 确保关闭您要克隆的思科 ISE 虚拟机。在 vSphere 客户端中，右键点击即将克隆的思科 ISE 虚拟机，然后选择**电源 (Power)** > **关闭访客 (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 右键点击要克隆的思科 ISE，然后点击**克隆 (Clone)**。

步骤 3 在“名称和位置”(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**下一步 (Next)**。

这不是正在创建的新思科 ISE VM 的主机名，而是供参考的描述性名称。

步骤 4 选择要运行新思科 ISE VM 的主机或集群，然后点击**下一步 (Next)**。

步骤 5 为正在创建的新思科 ISE VM 选择 datastore，然后点击**下一步 (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“磁盘格式”(Disk Format) 对话框中的**与源格式相同 (Same format as source)** 单选按钮，然后点击**下一步 (Next)**。

此选项会复制正在从其克隆新计算机的思科 ISE VM 中使用的同一格式。

步骤 7 点击“访客自定义”(Guest Customization) 对话框中的**不要自定义 (Do not customize)** 单选按钮，然后点击**下一步 (Next)**。

步骤 8 点击**完成 (Finish)**。

下一步做什么

- 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 模板克隆思科 ISE 虚拟机 (VM)。您可以将思科 ISE 节点克隆到模板并使用该模板创建多个新的思科 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 #unique_85

步骤 2 #unique_86

创建虚拟机模板

开始之前

- 确保关闭您要克隆的思科 ISE 虚拟机。在 vSphere 客户端中，右键点击即将克隆的思科 ISE 虚拟机，然后选择 **电源 (Power) > 关闭访客 (Shut Down Guest)**。
- 我们建议您从刚安装且未运行设置程序的思科 ISE 虚拟机创建模板。然后，您可以在已创建的每个单独的思科 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 右键点击要克隆的思科 ISE VM，然后选择**克隆 (Clone) > 要克隆的模板 (Clone to Template)**。

步骤 3 输入模板的名称，在“名称和位置”(Name and Location) 对话框中选择用于保存模板的位置，然后点击**下一步 (Next)**。

步骤 4 选择您要在其上存储模板的 ESXi 主机，然后点击**下一步 (Next)**。

步骤 5 选择要用于存储模板的数据存储区，然后点击**下一步 (Next)**。

确保此 datastore 具有所需的磁盘空间量。

步骤 6 点击“磁盘格式”(Disk Format) 对话框中的 **与源格式相同 (Same format as source)** 单选按钮，然后点击**下一步 (Next)**。

系统将显示“准备完成”(Ready to Complete) 对话框。

步骤 7 点击**完成**。

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 右键点击已创建的思科 ISE VM 模板，然后选择**从该模板部署虚拟机 (Deploy Virtual Machine from this template)**。

步骤 2 输入新思科 ISE 节点的名称，在“名称和位置”(Name and Location) 对话框中选择该节点的位置，然后点击**下一步 (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**下一步 (Next)**。

步骤 4 选择要用于新思科 ISE 节点的数据存储区，然后点击**下一步 (Next)**。

确保此 datastore 具有所需的磁盘空间量。

步骤 5 点击“磁盘格式”(Disk Format) 对话框中的 **与源格式相同 (Same format as source)** 单选按钮，然后点击**下一步 (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“准备完成”(Ready to Complete) 对话框。

步骤 7 选中**编辑虚拟硬件 (Edit Virtual Hardware)** 复选框，然后点击**继续 (Continue)**。

系统将显示“虚拟机属性”(Virtual Machine Properties) 页面。

步骤 8 选择 **Network adapter**，取消选中**已连接 (Connected)** 和 **启动时连接 (Connect at power on)** 复选框，然后点击 **OK**。

步骤 9 点击**完成 (Finish)**。

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

下一步做什么

- 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

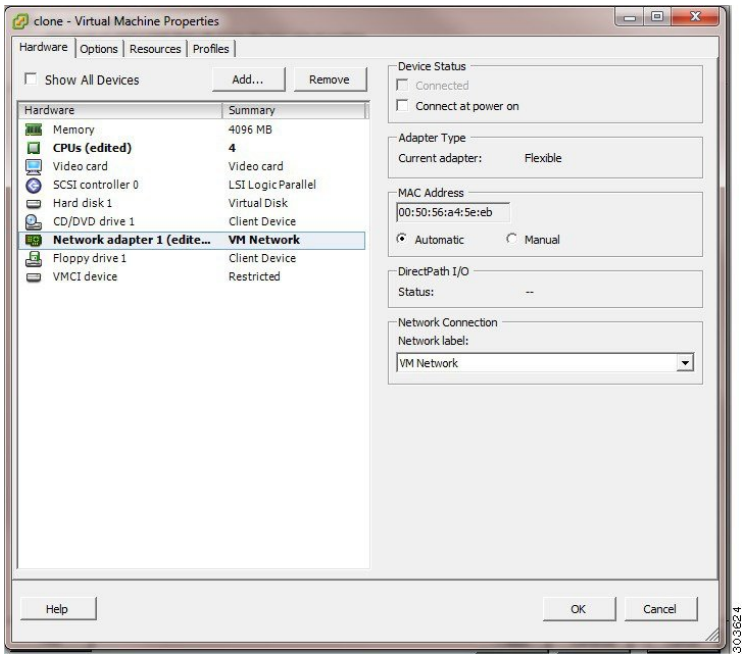
更改克隆虚拟机的 IP 地址和主机名

在您克隆思科 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

- 确保思科 ISE 节点处于独立状态。
- 确保在打开计算机电源时，最近克隆的思科 ISE VM 上的网络适配器未连接。取消选中 **已连接 (Connected)** 和**启动时连接 (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 地址或主机名的思科 ISE 节点的证书。

操作步骤

步骤 1 右键点击最近克隆的思科 ISE VM，然后选择**电源 (Power)** > **开启电源 (Power On)**。

步骤 2 选择最近克隆的思科 ISE VM，然后点击**控制台 (Console)** 选项卡。

步骤 3 在思科 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。系统会重新启动思科 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思科 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** 重新启动思科 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，必须将思科 ISE 节点连接到网络。

步骤 1 右键点击最近克隆的思科 ISE 虚拟机 (VM)，然后点击 **编辑设置 (Edit Settings)**。

步骤 2 点击“虚拟机属性”(Virtual Machine Properties) 对话框中的**网络适配器 (Network adapter)**。

步骤 3 在“设备状态”(Device Status) 区域中，选中**已连接 (Connected)** 和**启动时连接 (Connect at power on)** 复选框。

步骤 4 单击**确定 (OK)**。

将思科 ISE VM 从评估环境迁移至生产环境

评估思科 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，请务必将思科 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 2.4 TB）。
- 请注意，无法将数据从所创建的磁盘空间小于 300 GB 的 VM 迁移至生产 VM。只能将数据从所创建的具有 300 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。

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
```

从思科 ISE 启动菜单检查虚拟机资源

您可以在不依赖于思科 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**系统实用程序（串行控制台）(System Utilities [Serial Console])** 或**系统实用程序（键盘/监视器）(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** 以检查 VM 资源。输出将类似于如下：

```
*****
***** Virtual Machine host detected…
***** Hard disk(s) total size detected: 600 Gigabyte
***** Physical RAM size detected: 16267516 Kbytes
***** Number of network interfaces detected: 6
***** Number of CPU cores: 12
***** 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-3.1.0.x.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-3.0.0.x.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**新建 (New)**。

“创建新虚拟机”(Create a new virtual machine) 窗口随即会显示。

步骤 2 点击**本地安装媒体（ISO 媒体或 CDROM）(Local install media [ISO media or CDROM])**，然后点击**继续 (Forward)**。

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

a) 取消选中**基于安装介质自动检测操作系统 (Automatically detect operating system based on install media)** 复选框，选择“Linux”作为“操作系统类型”(OS type)，选择支持的 Red Hat Enterprise Linux 版本，然后点击**继续 (Forward)**。

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

步骤 5 选中**为此虚拟机启用存储 (Enable storage for this virtual machine)** 复选框，并选择存储设置。

a) 点击**选择托管或其他现有存储 (Select managed or other existing storage)** 单选按钮。
b) 点击**浏览 (Browse)**。
c) 从左侧的“存储池”(Storage Pools) 导航窗格中，点击**磁盘文件系统目录 (disk FileSystem Directory)**。
d) 点击**新建卷 (New Volume)**。

“创建存储卷”(Create storage volume) 窗口随即显示。

e) 为存储卷输入名称。
f) 从**格式 (Format)** 下拉列表中选择**原始 (raw)**。

g) 输入最大容量。
h) 点击**完成 (Finish)**。
i) 选择您创建的卷，然后点击**选择卷 (Choose Volume)**。
j) 点击**继续 (Forward)**。

“准备开始安装”(Ready to begin the installation) 屏幕随即会显示。

步骤 6 选中**安装前自定义配置 (Customize configuration before install)** 复选框。

步骤 7 在“高级”(Advanced)选项下，选择 macvtap 作为接口源，在“源模式”(Source mode) 下拉列表中选择“桥接”(Bridge)，然后点击**完成 (Finish)**。

a) （可选）点击**添加硬件 (Add Hardware)** 可添加其他 NIC。

选择 macvtap 作为网络源，选择 virtio 作为设备型号。

b) 点击**完成 (Finish)**。

步骤 8 在“虚拟机”(Virtual Machine) 屏幕中，选择磁盘设备，并在“高级”(Advanced) 和“性能”(Performance) 选项下，选择以下选项，然后点击**应用 (Apply)**。

字段	值
Disk bus	VirtIO
Cache mode	none
IO mode	native

步骤 9 点击**开始安装 (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。

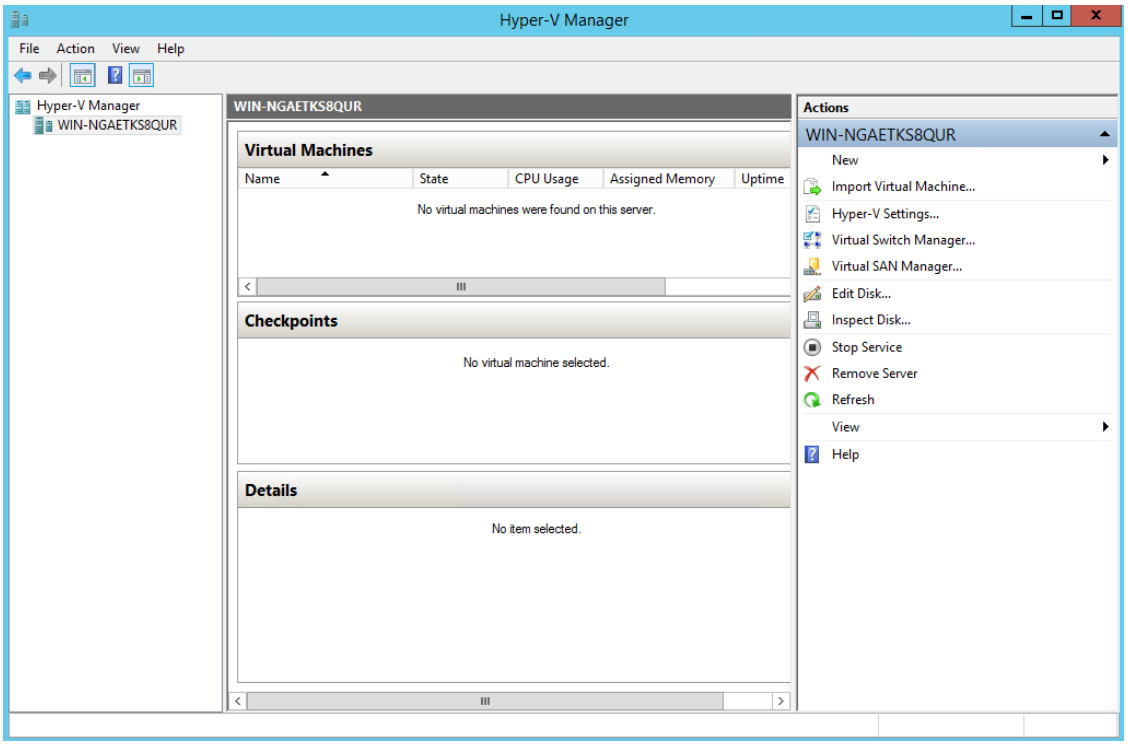
注释 思科 ISE 不支持使用多路径 I/O (MPIO)。因此，如果您为 VM 使用了 MPIO，则安装将失败。

开始之前

将思科 ISE ISO 映像文件从 cisco.com 下载至本地系统。

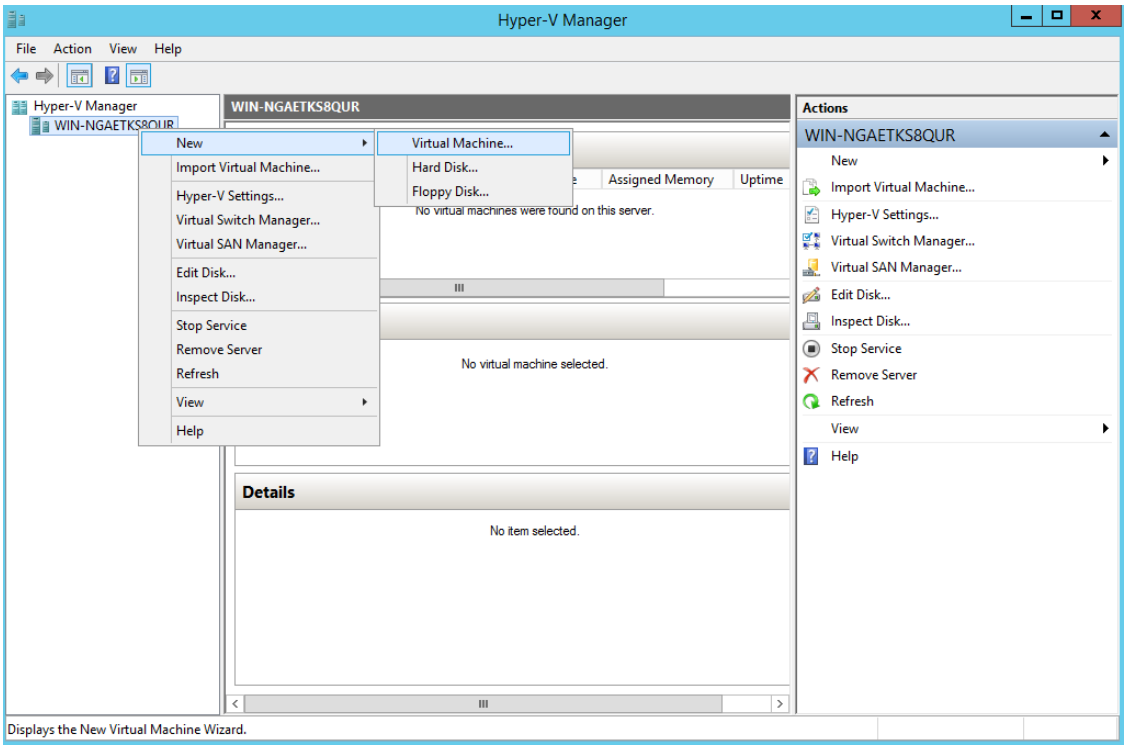
步骤 1 在受支持的 Windows 服务器上启动 Hyper-V Manager。

图 *10: Hyper-V* 管理器控制台



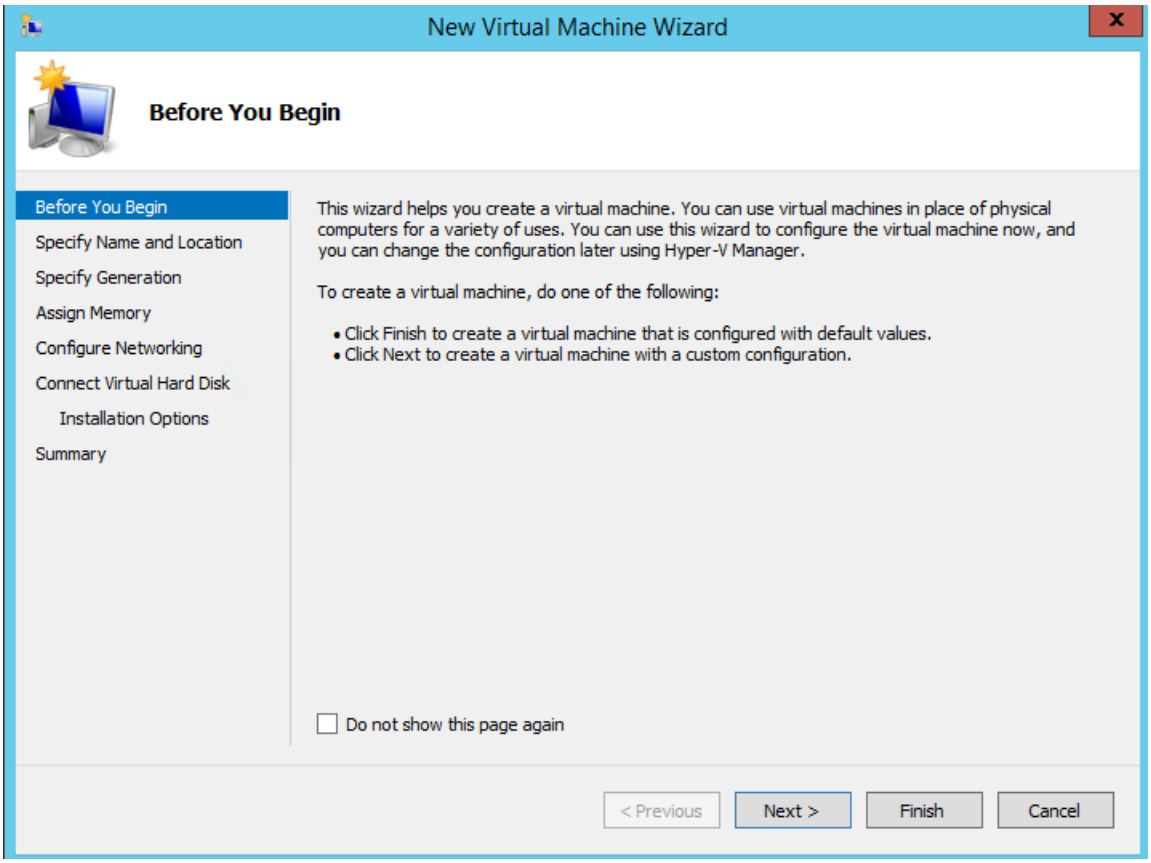
步骤 2 右键点击 VM 主机，然后点击 **新建 (New) > 虚拟机 (Virtual Machine)**。

图 *11:* 创建新的虚拟机



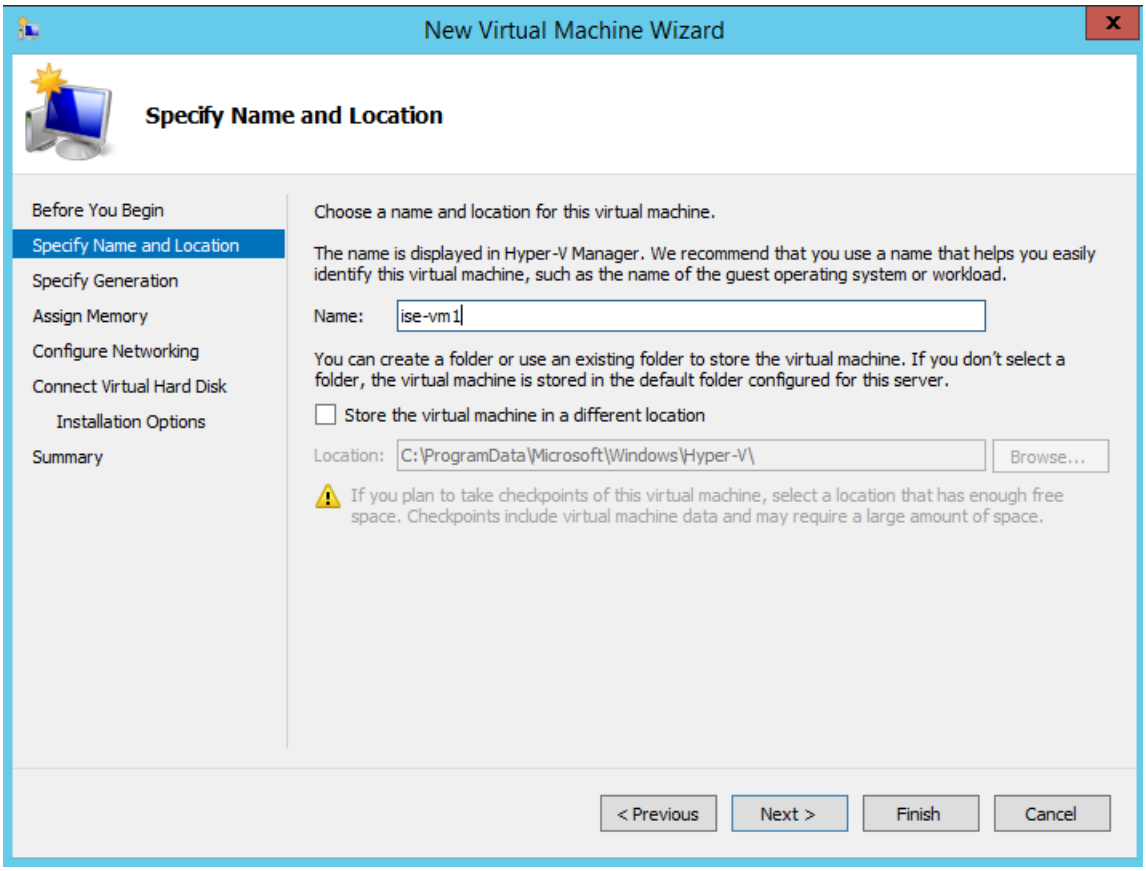
步骤 3 点击下一步 **(Next)** 以自定义 VM 配置。

图 *12: New Virtual Machine Wizard*



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**下一步 (Next)**。

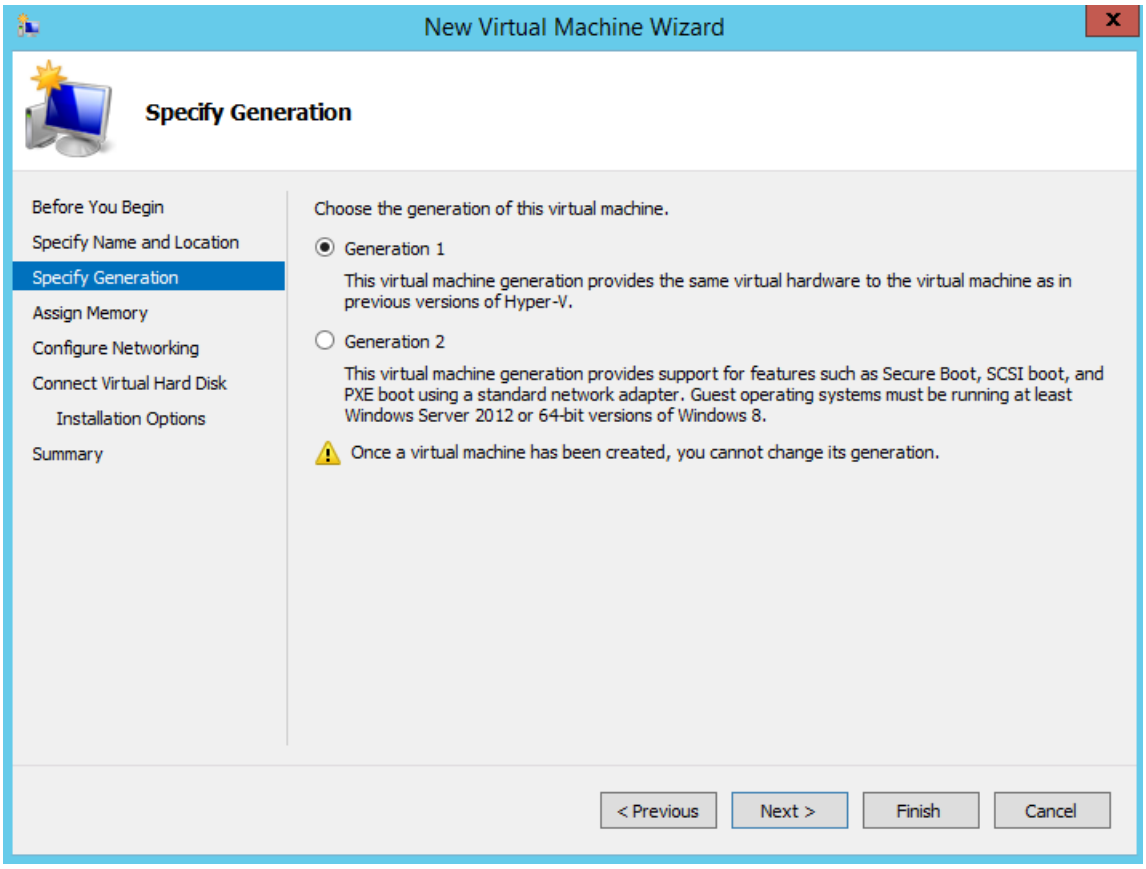
图 *13:* 指定名称和位置



步骤 5 点击**第一代 (Generation 1)** 单选按钮，然后点击**下一步 (Next)**。

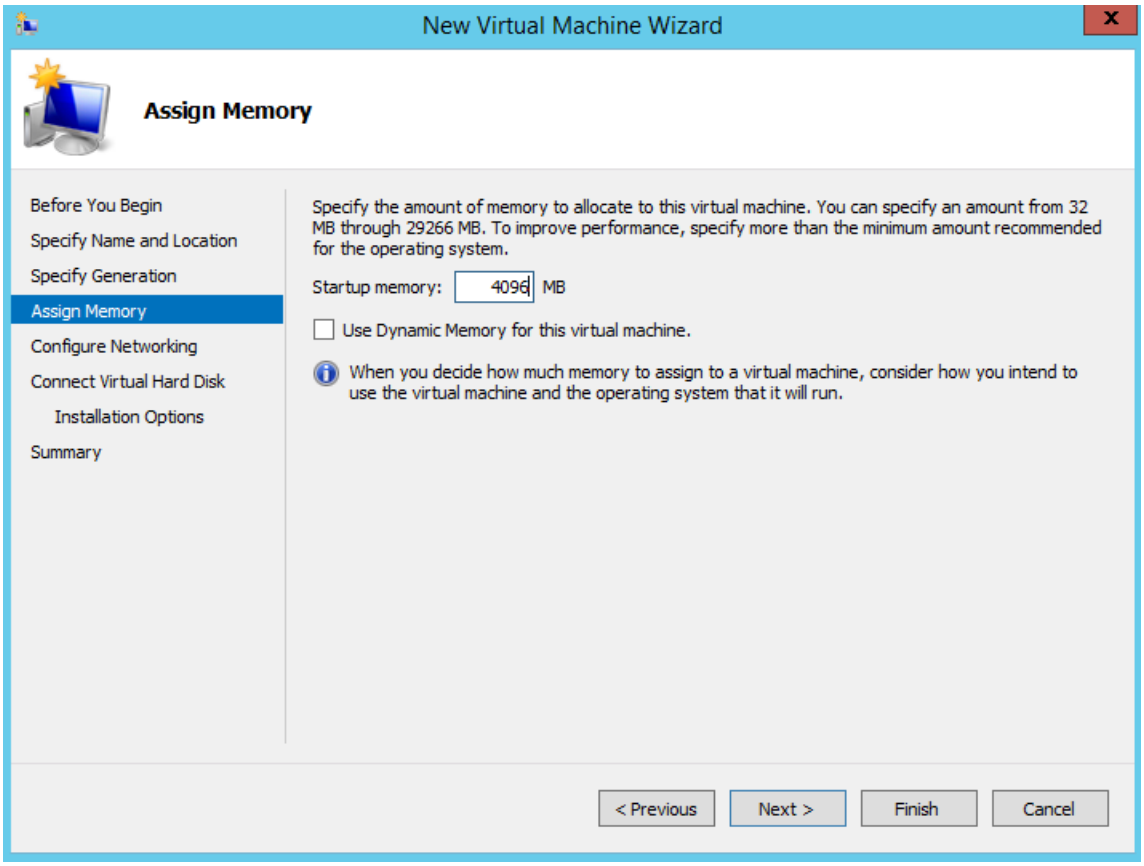
如果选择创建第 2 代 ISE VM，请确保在 VM 设置中禁用**安全引导 (Secure Boot)**。

图 *14:* 指定代数



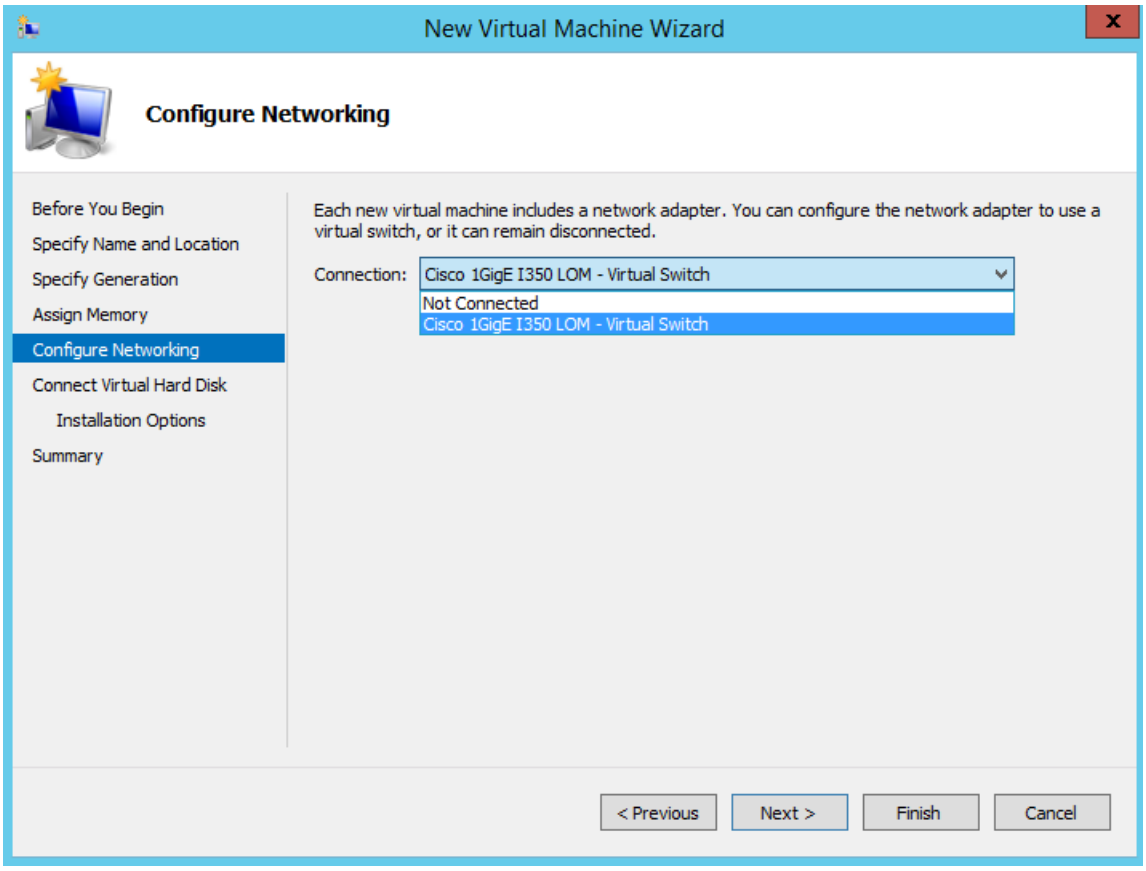
步骤 6 指定分配给此 VM 的内存量（例如 16000 MB），然后点击**下一步 (Next)**。

图 *15:* 分配内存



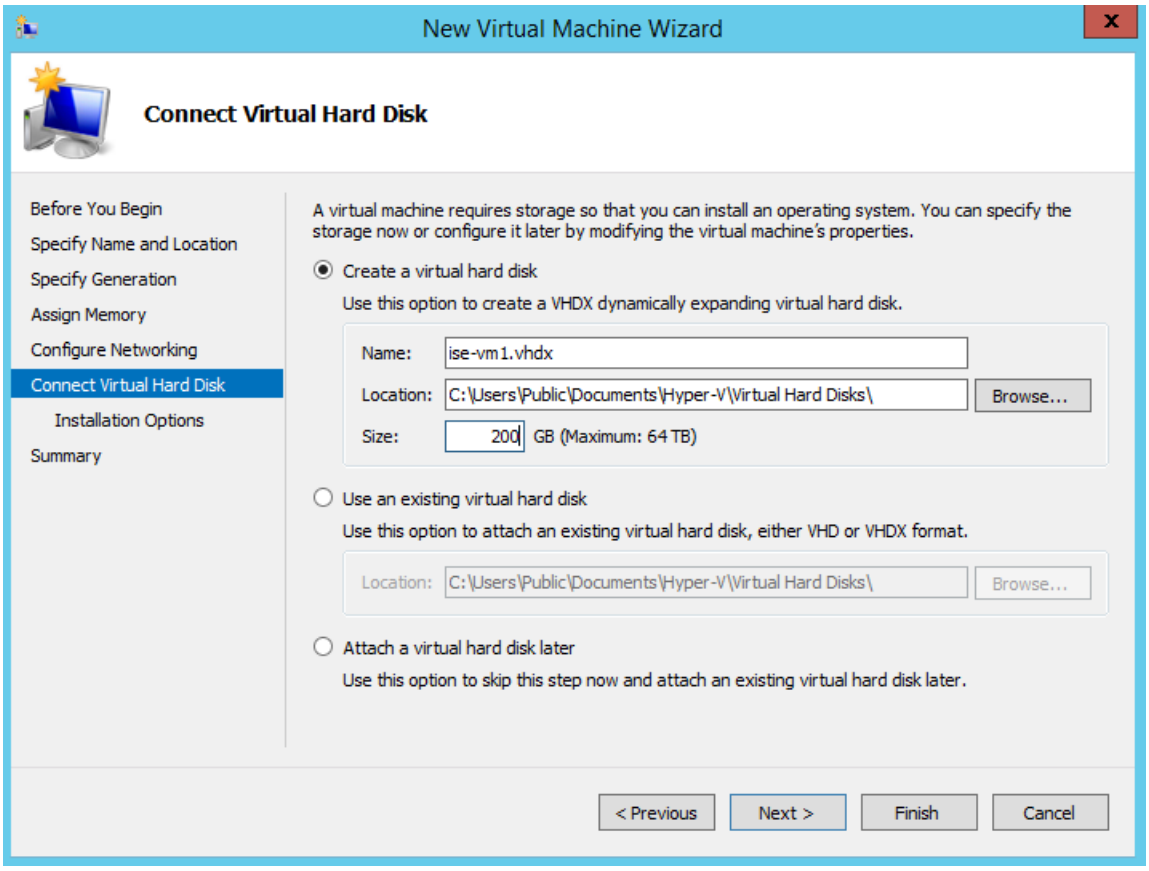
步骤 7 选择网络适配器，然后点击下一步 **(Next)**。

图 *16:* 配置网络



步骤 8 点击创建虚拟硬盘 **(Create a virtual hard disk)** 单选按钮，然后点击下一步 **(Next)**。

图 *17:* 连接虚拟硬盘

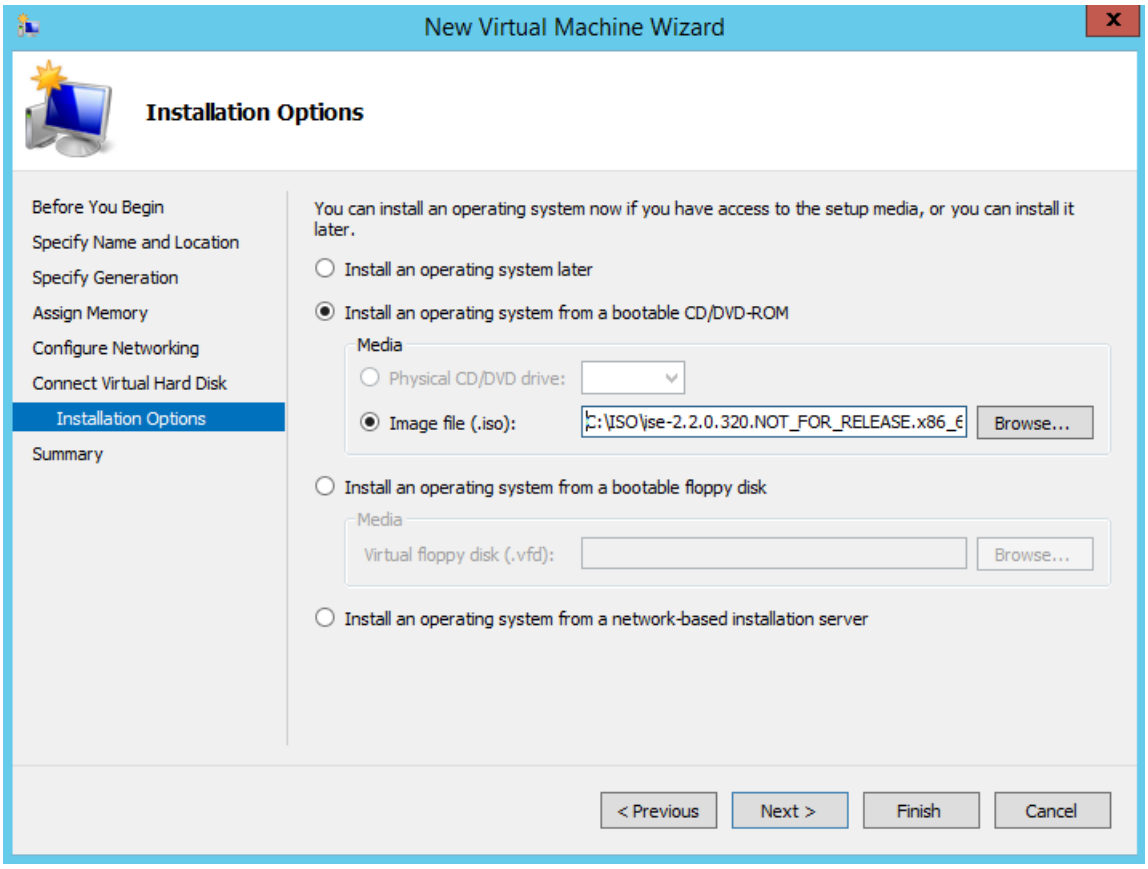


步骤 9 点击从可启动的 **CD/DVD-ROM** 安装操作系统 **(Install an operating system from a bootable CD/DVD-ROM)** 单选按钮。

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

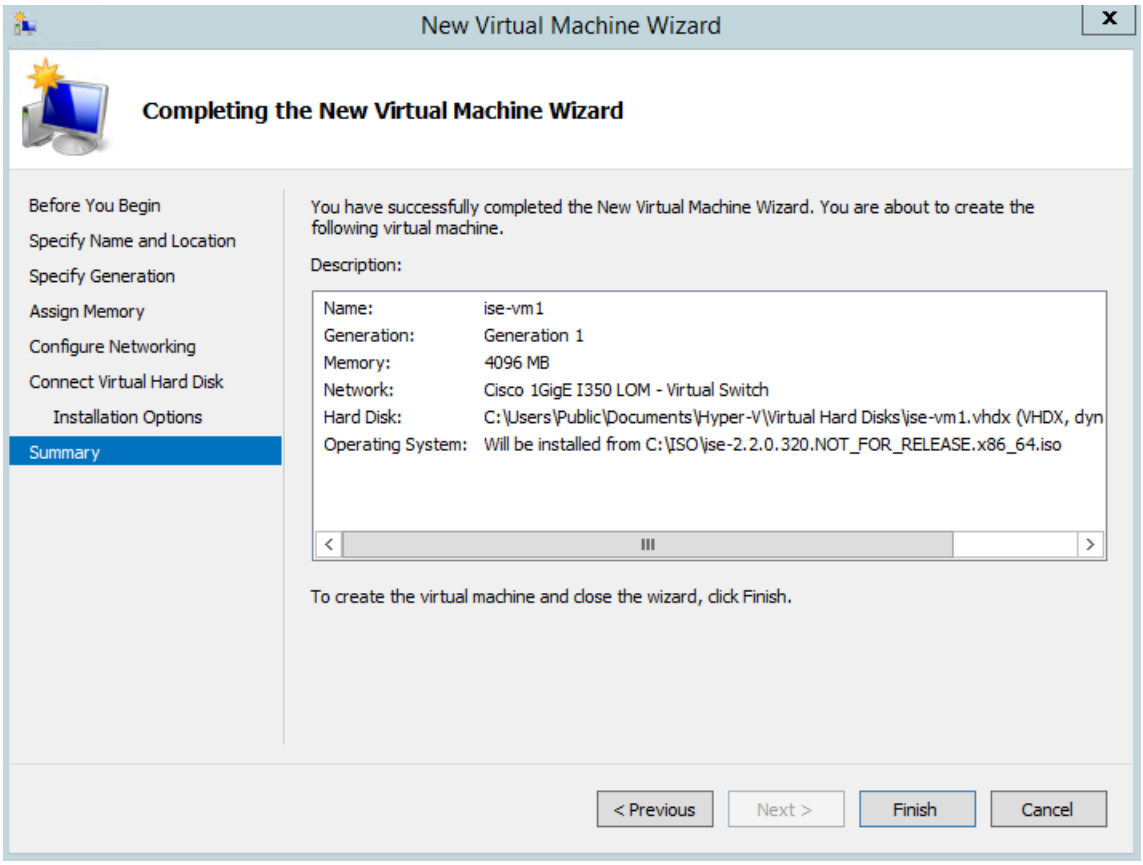
b) 点击浏览 **(Browse)** 以从本地系统选择 ISE ISO 映像，然后点击下一步 **(Next)**。

图 *18:* 安装选项



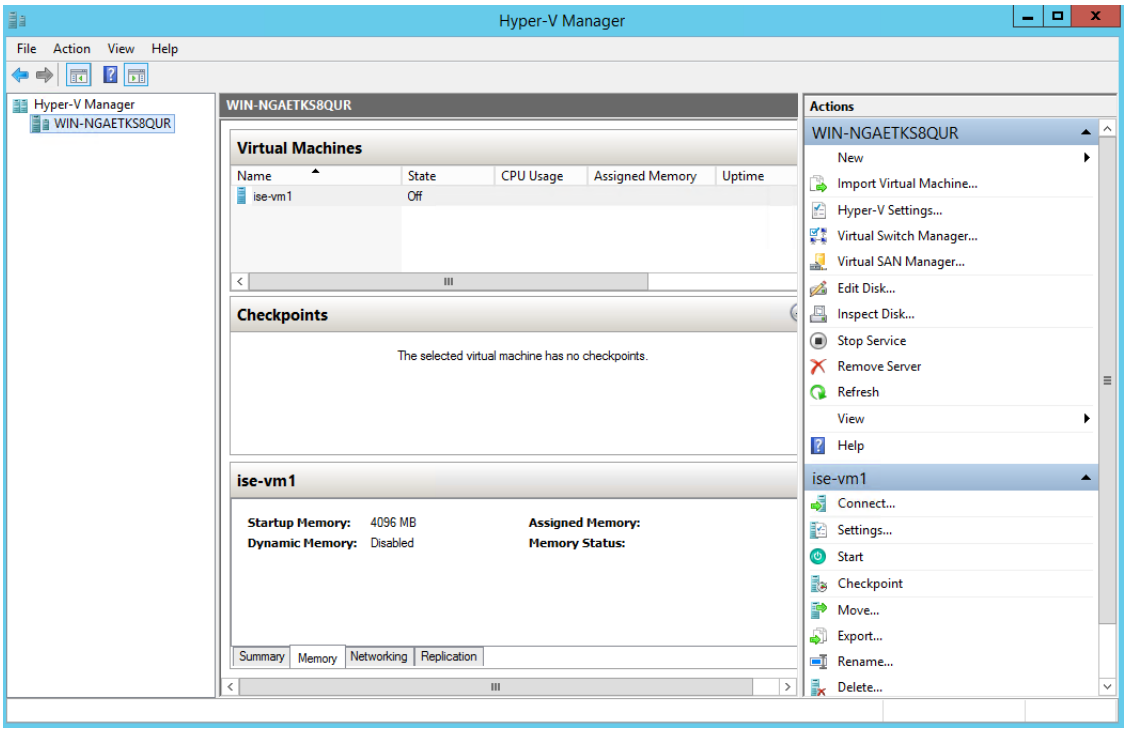
步骤 **10** 点击完成 **(Finish)**。

图 *19:* 完成新虚拟机向导



思科 ISE VM 已在 Hyper-V 上创建完成。

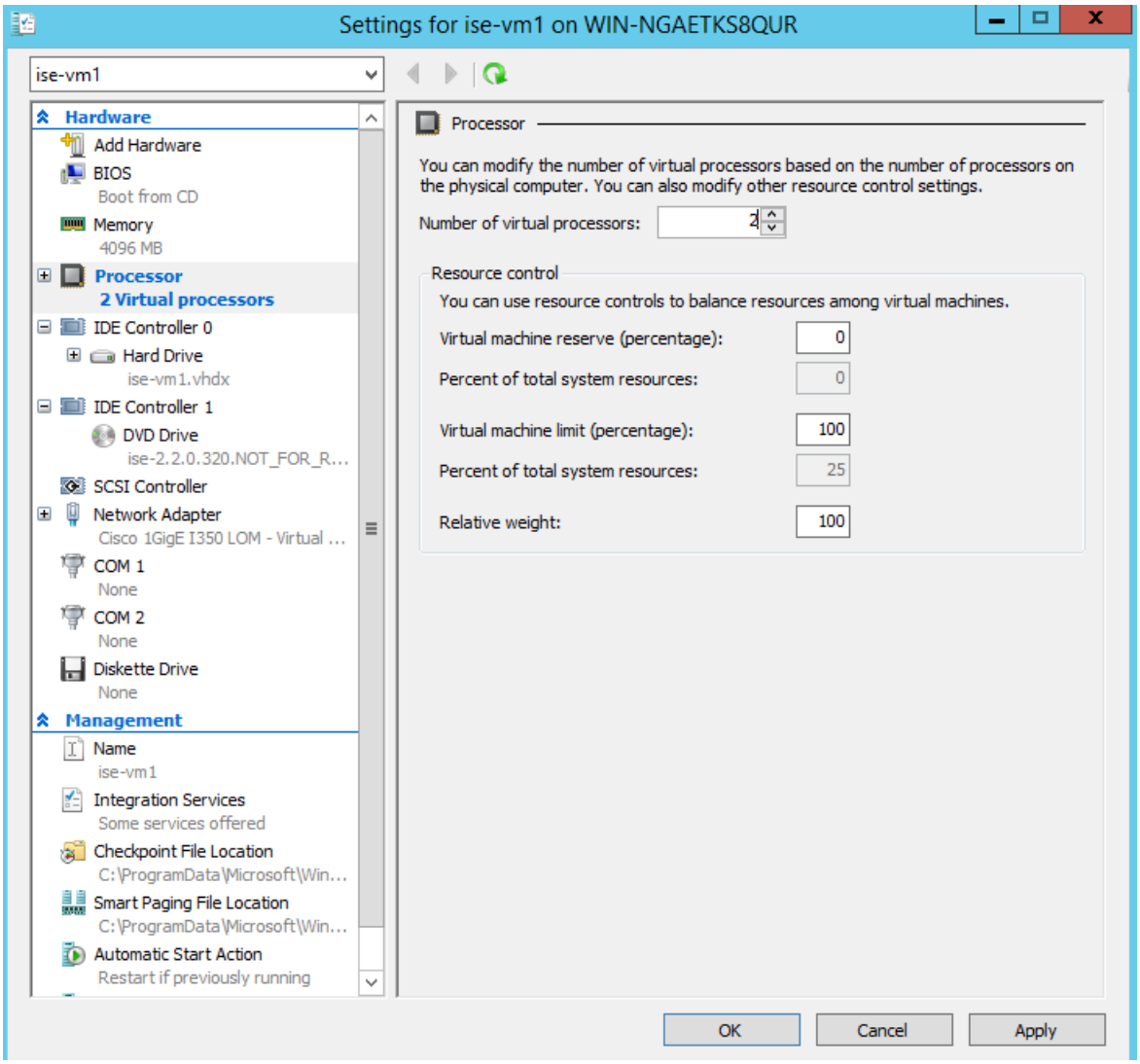
图 *20:* 创建的新虚拟机



步骤 11 选择虚拟机并编辑虚拟机设置。

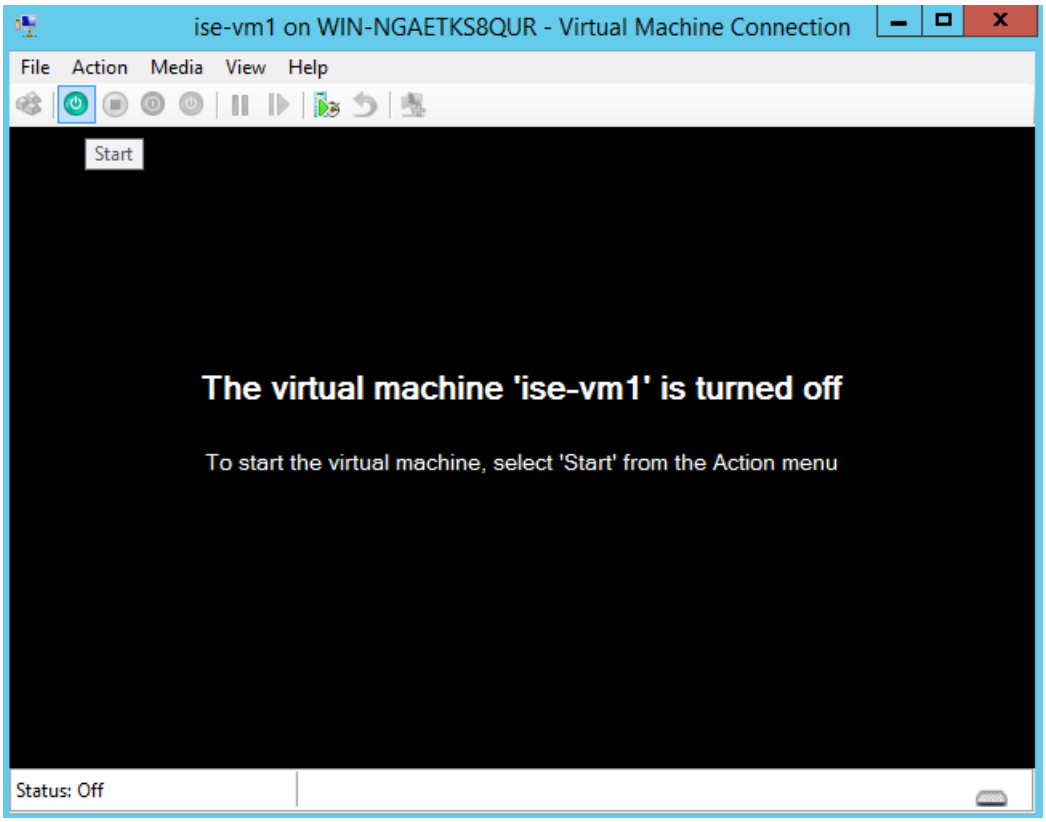
a) 选择**处理器 (Processor)**。输入虚拟处理器的数量（例如 6），然后点击**确定 (OK)**。

图 *21:* 编辑 *VM* 设置



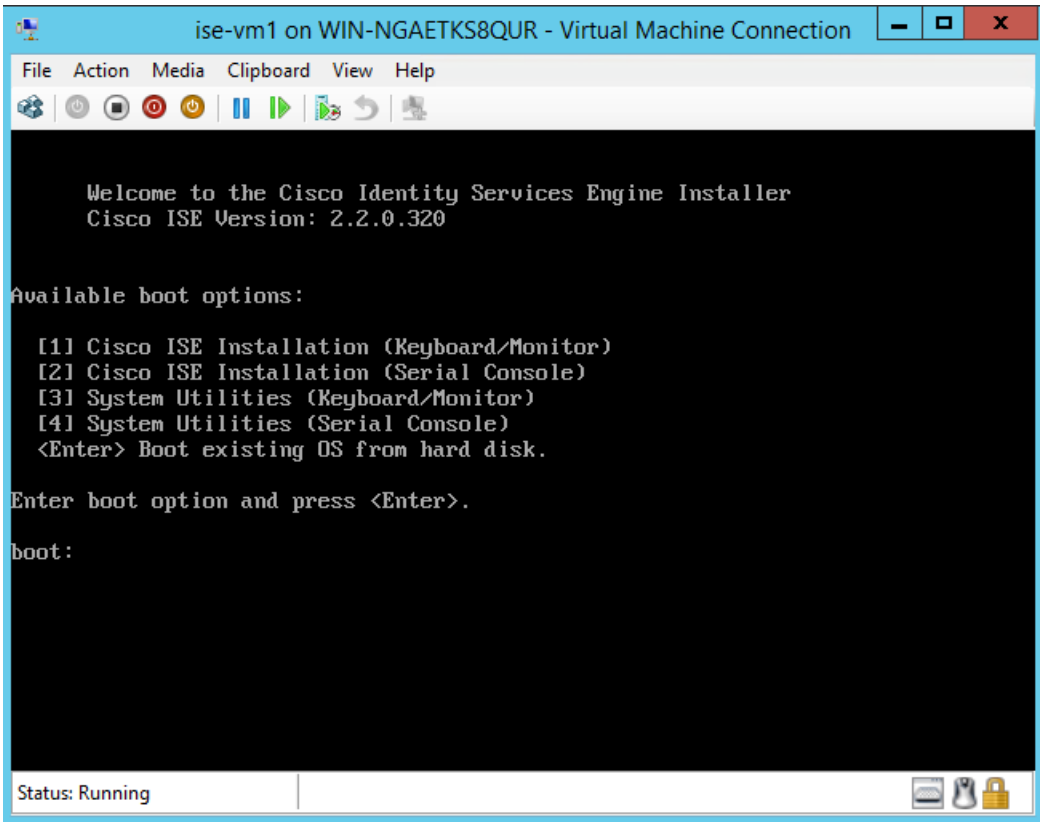
步骤 12 选择 VM，然后点击**连接 (Connect)** 启动 VM 控制台。点击启动按钮以打开思科 ISE VM。

图 *22:* 启动思科 *ISE VM*



思科 ISE 安装菜单随即会显示。

图 *23:* 思科 *ISE* 安装菜单



步骤 13 输入 **1** 使用键盘和显示器安装思科 ISE。

非接触调配

零接触调配 (ZTP) 是一种不间断的调配机制，它可自动执行思科 ISE 安装、修补、热补丁和基础设施服务启用，而无需进行手动干预。

ZTP 可用于思科 ISE 版本 3.1 及更高版本。ZTP 中有两个可用选项：

- **Mapping.img 文件 (Mapping .img file)**：虚拟机 (VM) 自动安装，设备和 OVA 安装支持此方法。它需要配置强制参数，例如主机名、IP 地址、IP 网络掩码、IP 默认网关、DNS 域、主域名服务器、NTP 服务器、系统时区、SSH、用户名和密码。还可以配置可选参数，例如 IPV6、补丁、热补丁、服务和存储库详细信息。有关详细信息，请参阅 ZTP 配置映像文件。

注释 您无法在 Microsoft Hyper-V 上将 .img 文件用于 ZTP。您必须使用 .iso 文件。

- **VM 用户数据 (VM User Data)**：OVA 和 VM 自动安装支持此方法 。如果配置了用户数据，并且需要配置强制参数，例如主机名、IP 地址、IP 网络掩码、IP 默认网关、DNS 域、主域名服务器、NTP 服务器、系统时区、SSH、用户名和密码。还可以配置可选参数，例如 IPV6、补丁、热补丁、服务和存储库详细信息。有关详细信息，请参阅 VM 用户数据。

注释
- 要在 ZTP 过程中跟踪安装进度，则应为虚拟机和设备启用串行控制台。
- 需要使用 ZTP 配置映像文件。

注释 TFTP、HTTP、HTTPS 和 NFS 存储库支持作为 ZTP 流程的一部分在思科 ISE 上安装热补丁和补丁。在 ZTP 流程中创建的存储库在思科 ISE GUI 中不会显示或无法使用。这些存储库必须具有匿名访问权限（无用户名/密码），ZTP 进程才能使用它们。

在虚拟机中自动安装

以下小节提供有关在 VM 中自动安装的信息。

使用 ZTP 配置映像文件在虚拟机中自动安装

步骤 1 登录到 VMware 客户端。

注释 如果您已有现有的VM设置，请继续执行第2步并继续执行第6步。对于新的虚拟机设置，请直接转到第 8 步。

步骤 2 要使 VM 进入 BIOS 设置模式，请右键点击 VM，然后选择**编辑设置 (Edit Settings)**。

步骤 3 点击**选项 (Options)** 选项卡。

步骤 4 点击**引导选项 (Boot Options)**。

步骤 5 在**强制 BIOS 设置 (Force BIOS Setup)** 区域中选中 **BIOS** 复选框，以便在 VM 引导时进入 BIOS 设置屏幕。

注释 您必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

步骤 6 点击**确定 (OK)**。

步骤 7 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 VM 已开启，请关闭系统。

b) 打开 VM。

系统进入 BIOS 设置模式。

c) 在主 **BIOS** 菜单中，使用箭头键导航到**日期和时间 (Date and Time)** 字段，然后按 **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) 使用箭头键导航到引导菜单，然后按 **Enter**。
f) 使用箭头键选择 CD-ROM 驱动器，然后按 **+** 将 CD-ROM 驱动器的启动顺序向上移动。
g) 使用箭头键导航到**退出 (Exit)** 菜单，并选择**退出并保存更改 (Exit Saving Changes)**。（按 Enter 或 Return 键进行选择）。
h) 选择**是 (Yes)** 保存更改并退出。

步骤 8 将思科 ISE 软件 DVD 插入 VMware ESX 主机的 CD/DVD 驱动器。

步骤 9 将 ZTP 配置映像文件插入辅助 CD/DVD 驱动器。

步骤 10 打开虚拟机。

当 DVD 启动时，控制台会显示以下信息：

```
Automatic installation starts in 150 seconds.
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)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

注释 从思科 ISE 3.1 开始，按 **Enter** 键而不输入引导选项将不会使用硬盘选项来触发安装。相反，它会触发 ZTP。

步骤 11 150 秒后，如果满足前提条件，启动过程会自动开始。

注释
- 由于 ZTP 只能通过串行控制台工作，因此安装日志只能通过串行控制台进行监控。在显示设置提示后，可以从 VM 控制台对其进行监控。
- 思科 ISE 服务启动后，您必须从 CD/DVD 手动卸载 ZTP 配置映像文件。

要在设置提示中使用 ZTP（使用键盘执行 ZTP，直到设置提示正确），请执行此程序：

1. 手动安装思科 ISE，直到设置完成（使用引导选项 1 或 2），然后按照上述程序中所述的步骤来创建 ZTP 配置映像文件。

2. 关闭虚拟机电源并将 ZTP 配置映像文件映射到 CD/DVD 驱动器。

3. 启动 VM。

设置详细信息将从映射到 CD/DVD 驱动器的 ZTP 配置文件中提取。

故障排除

问题：如果在 VM 中触发自动安装而未映射 .img 文件，则安装会在 150 秒后失败并显示以下消息：

```
***** The ZTP configuration image is missing or improper. Automatic installation flow
 exited.
```

```
***** Power off and attach the proper ZTP configuration image or choose manual boot to
 proceed.
```

解决方案：此错误消息仅通过串行控制台显示，而不会在VM控制台上显示。如果在已安装思科ISE的现有 VM 中出现此类情况，则硬盘不会在该状态下格式化。现有 VM 可通过执行以下步骤恢复：

1. 关闭 VM。
2. 打开 VM。
3. 按选项 5，在 150 秒内从硬盘启动以便加载现有 VM。

问题：如果设置详细信息在配置文件中无效，则 ZTP 安装将停止，并且 VM 控制台上会显示以下消息：

```
================================================================================

Cisco ISE Installation Failed

================================================================================

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

================================================================================
```

解决方案：

1. 使用有效的详细信息来创建新的 configuration.img 文件。
2. 关闭 VM 电源。
3. 将新的有效映像映射到 CD/DVD 驱动器。
4. 启动 VM。

安装会从设置开始。

使用 VM 用户数据在虚拟机中自动安装

步骤 1 登录到 VMware 客户端。

注释 如果您已有现有的VM设置，请继续执行第2步并继续执行第6步。对于新的虚拟机设置，请直接转到第 8 步。

步骤 2 要使 VM 进入 BIOS 设置模式，请右键点击 VM，然后选择**编辑设置 (Edit Settings)**。

步骤 3 点击**选项 (Options)** 选项卡。

步骤 4 点击**引导选项 (Boot Options)**。

步骤 5 在**强制 BIOS 设置 (Force BIOS Setup)** 区域中选中 **BIOS** 复选框，以便在 VM 引导时进入 BIOS 设置屏幕。

注释 您必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

步骤 6 点击**确定 (OK)**。

步骤 7 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 VM 已开启，请关闭系统。

b) 打开 VM。

系统进入 BIOS 设置模式。

c) 在主 **BIOS** 菜单中，使用箭头键导航到**日期和时间 (Date and Time)** 字段，然后按 **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) 使用箭头键导航到引导菜单，然后按 **Enter**。

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

g) 使用箭头键导航到**退出 (Exit)** 菜单，然后选择**退出并保存更改 (Exit Saving Changes)**（按 Enter 或 Return 键以选择对应的选项）。

h) 选择**是 (Yes)** 保存更改并退出。

步骤 8 将思科 ISE 软件 DVD 插入 VMware ESX 主机的 CD/DVD 驱动器。

步骤 9 配置 VM 用户数据 (VM user data) 选项。

注释 如果在 VM 中同时配置了 .img 文件和 VM 用户数据选项，则会考虑用户数据选项。

步骤 10 打开 VM。

当 DVD 启动时，控制台会显示以下信息：

```
Automatic installation starts in 150 seconds.
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)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

注释 从思科 ISE 3.1 开始，按 **Enter** 键而不输入引导选项将不会使用硬盘选项来触发安装。相反，它会触发 ZTP。

步骤 11 150 秒后，如果满足前提条件，启动过程会自动开始。

注释

- 由于 ZTP 只能通过串行控制台工作，因此安装日志只能通过串行控制台进行监控。在显示设置提示后，可以从 VM 控制台对其进行监控。
- 思科 ISE 服务启动后，您必须从 CD/DVD 手动卸载 ZTP 配置映像文件。

要在设置提示中使用 ZTP（使用键盘执行 ZTP，直到设置提示正确），请执行此程序：

1. 手动安装思科 ISE 直到设置完成（使用引导选项 1 或 2）。\

2. 关闭 VM 电源。

3. 配置上述用户数据选项。

4. 打开 VM 电源。

设置详细信息将从 VM 选项中选取。

故障排除

问题：如果在用户数据选项中输入了无效的设置详细信息，则 ZTP 安装将停止，并且 VM 控制台上会显示以下消息：

```
================================================================================

Cisco ISE Installation Failed

================================================================================

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

================================================================================
```

解决方案：

1. 关闭 VM 电源。
2. 使用有效的数据来更新用户数据详细信息。
3. 启动 VM。

安装会从设置开始。

在设备中自动安装

以下小节提供有关在设备中自动安装的信息。

使用 ZTP 配置映像文件在设备中自动安装

步骤 1 登录 SNS 设备。

步骤 2 关闭主机电源。

步骤 3 选择**计算 (Compute)** > **远程管理 (Remote Management)** > **虚拟介质 (Virtual media)**。

步骤 4 将思科 ISE 软件 ISO 和 ZTP 配置映像文件映射到主 CD/DVD 驱动器和辅助 CD/DVD 驱动器。

步骤 5 开启主机电源。

当设备启动时，控制台会显示以下消息：

```
Please select boot device:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
```

```
[4] System Utilities (Serial Console)
[5] Cisco ISE Installation Through ZTP Configuration (Serial Console)
```

步骤 6 150 秒后，如果满足前提条件，启动过程会自动开始。

注释

- ZTP 只有通过虚拟介质在 SNS 设备上运行。
- 在映射 ISO 文件之前，必须先在虚拟介质中映射 .img 文件。

  由于ZTP要通过串行控制台工作，因此安装日志只能通过串行控制台进行监控。在显示设置提示后，可以从 KVM 控制台监控日志。
- 只有 .img 文件支持设备中的自动安装。

要在设置提示中使用 ZTP（使用键盘完成 ZTP，直到设置提示正确），请执行以下步骤：

1. 手动安装思科 ISE，直到设置完成（使用引导选项 1 或 2），并按照上述步骤来创建 ZTP 配置映像文件。

2. 关闭主机电源并将创建的 ZTP 配置映像文件映射到 CD/DVD 驱动器。

3. 开启主机电源。

设置详细信息将从映射到 CD/DVD 驱动器的 ZTP 配置文件中提取。

故障排除

问题：如果在设备中触发自动安装而未映射映像文件，则安装会在 150 秒后失败并显示以下消息：

```
***** The ZTP configuration image is missing or improper. Automatic installation flow
 exited.
***** Power off and attach the proper ZTP configuration image or choose manual boot to
 proceed.
```

解决方案：

1. 关闭 VM。

2. 打开 VM。

3. 按选项 5，在 150 秒内从硬盘启动以便加载现有 VM。

问题：如果配置详细信息在配置文件中无效，则 ZTP 安装将停止，并且 KVM 控制台上会显示以下消息：

```
================================================================================

Cisco ISE Installation Failed

================================================================================

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

================================================================================
```

解决方案：

1. 使用有效的详细信息来创建新的 configuration.img 文件。
2. 关闭 VM 电源。
3. 将新的有效映像映射到 CD/DVD 驱动器。
4. 启动 VM。

安装会从设置开始。

使用 UCS XML API 触发自动安装

要触发自动安装，请执行以下操作：

注释 所有方法的 API URL 和请求标头均相同：

API URL

```
https://<ucs_server_ip>/nuova
```

标题

```
 headers["Accept"] = "application/xml"
headers["Content-Type"] = "application/xml"
```

步骤 1 获取用于身份验证的登录会话 Cookie。

aaaLogin 方法是登录过程，并且是开始会话所必需的。此操作会在客户端和思科 IMC 之间建立 HTTP（或 HTTPS）会话。此会话 Cookie 会在即将到来的请求中用于维护登录会话。

请求

```
<aaaLogin inName='admin' inPassword='password'/>
```

回答

```
<aaaLogin cookie="" response="yes" outCookie="<real_cookie>" outRefreshPeriod="600" outPriv="admin"
outSessionId="17" outVersion="3.0(0.149)"> </aaaLogin>
```

步骤 2 映射思科 ISE ISO。

这样会将思科 ISE ISO 文件配置为虚拟介质卷。

请求

```
<configConfMo cookie='<real_cookie>' dn='sys/svc-ext/vmedia-svc/vmmap-ISE_ISO' inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmap-ISE_ISO'
 map=' nfs'
 remoteFile= '<ise_iso_file>'
 remoteShare= '<nfs_server_path>'
 status='created' volumeName='ISE_ISO' />
</inConfig>
</configConfMo>
```

回答

```
<configConfMo dn="sys/svc-ext/vmedia-svc/vmmap-ISE_ISO"
 cookie="<real_cookie>" response="yes">
<outConfig>
 <commVMediaMap volumeName="ISE_ISO" map=“nfs”
  remoteShare= ‘<nfs_server_path>'
  remoteFile="<ise_iso_file>"
  mappingStatus="In Progress"
  dn="sys/svc-ext/vmedia-svc/vmmap-ISE_ISO" status="created"/>
  </outConfig>
</configConfMo>
```

步骤 3 映射配置映像文件。

这会将配置映像配置为 vMedia 卷。

请求

```
<configConfMo cookie='<real_cookie>'
dn='sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG’ inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG'
  map=’ nfs’
  remoteFile= ‘<config_img_file>’
  remoteShare= ‘<nfs_server_path>'
  status='created' volumeName='CONFIG-IMG' />
</inConfig>
</configConfMo>
```

回答

```
<configConfMo dn="sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG"
 cookie="<real_cookie>" response="yes">
<outConfig>
 <commVMediaMap volumeName="CONFIG-IMG" map=“nfs”
  remoteShare= ‘<nfs_server_path>'
  remoteFile="<config_img_file>"
  mappingStatus="In Progress"
  dn="sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG" status="created"/>
  </outConfig>
</configConfMo>
```

步骤 4 将 CD-ROM 设为启动顺序中的第一位。

这样将映射在电源重启期间为安装选择的思科 ISE ISO 文件。

请求

```
<configConfMo cookie="<real_cookie>"
inHierarchical="true" dn="sys/rack-unit-1/boot-policy">
  <inConfig>
    <lsbootDef dn="sys/rack-unit-1/boot-policy"  rebootOnUpdate=“yes”>
      <lsbootVirtualMedia access="read-only" order=“1” dn="sys/rack-unit-1/boot-policy/vm-read-only"/>

     </lsbootDef>
  </inConfig>
</configConfMo>
```

回答

```
<configConfMo dn="sys/rack-unit-1/boot-policy" cookie="<real_cookie>" response="yes">
<outConfig>
```

```
  <lsbootDef dn="sys/rack-unit-1/boot-policy" name="boot-policy" purpose="operational" rebootOnUpdate="no"
 status="modified" >
  </lsbootDef>
</outConfig>
</configConfMo>
```

步骤 5 启用 SoL（LAN 上串行）。

这使得 SoL 能够通过 Telnet 来查看安装日志。

请求

```
<configConfMo cookie='<real_cookie>'
dn='sys/rack-unit-1/sol-if'>
<inConfig>
  <solIf dn='sys/rack-unit-1/sol-if' adminState= ‘enable'/>
 </inConfig>
</configConfMo>
```

回答

```
<configConfMo dn="sys/rack-unit-1/sol-if" cookie="<real_cookie>" response="yes">
<outConfig>
<solIf dn="sys/rack-unit-1/sol-if" adminState="enable" name="SoLInterface" speed="115200" comport="com0"
 sshPort="2400" status="modified" ></solIf></outConfig>
</configConfMo>
```

步骤 6 电源重启。

这样会在自动模式下触发思科 ISE 安装。

请求

```
<configConfMo cookie='<real_cookie>' dn='sys/rack-unit-1'>
<inConfig><computeRackUnit
dn='sys/rack-unit-1'
adminPower='cycle-immediate'/>
</inConfig>
</configConfMo>
```

回答

```
<configConfMo dn="sys/rack-unit-1" cookie="<real_cookie>" response="yes">
<outConfig>
   <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="262144" model="SNS-3695-K9"
 memorySpeed="2400" name="SNS-3695-K9" numOfAdaptors="0" numOfCores="12" numOfCoresEnabled="12"
numOfCpus="1" numOfEthHostIfs="0" numOfFcHostIfs="0" numOfThreads="24" operPower="on"
originalUuid="1935836B-B968-4031-8A98-7984F1D35449" presence="equipped" serverId="1" serial="WZP2228085W"
 totalMemory="262144" usrLbl="" uuid="1935836B-B968-4031-8A98-7984F1D35449" vendor="Cisco Systems Inc"
cimcResetReason="graceful-reboot
" assetTag="Unknown" adaptorSecureUpdate="Enabled" resetComponents="components" storageResetStatus="NA"
 vicResetStatus="NA" bmcResetStatus="NA" smartUsbAccess="disabled" smartUsbStatus="Disabled"
biosPostState="completed" status="modified" >
  </computeRackUnit>
</outConfig>
</configConfMo>
```

步骤 7 注销以退出会话。

请求

```
<aaaLogout
    cookie="<real_cookie>"
    inCookie="<real_cookie>"
</aaaLogout>
```

回答：

```
<aaaLogout cookie="" response="yes" outStatus="success"> </aaaLogout>
```

有关详细信息，请参阅 UCS API 方法。

OVA 自动安装

以下各节提供有关使用 OVA 进行自动安装的信息。

使用 ZTP 配置映像文件自动安装 OVA

步骤 1 登录到 VMware 客户端。

注释 如果您已有现有的VM设置，请继续执行第2步并继续执行第6步。对于新的虚拟机设置，请直接转到第 8 步。

步骤 2 要使 VM 进入 BIOS 设置模式，请右键点击 VM，然后选择**编辑设置 (Edit Settings)**。

步骤 3 点击**选项 (Options)** 选项卡。

步骤 4 点击**引导选项 (Boot Options)**。

步骤 5 在**强制 BIOS 设置 (Force BIOS Setup)** 区域中选中 **BIOS** 复选框，以便在 VM 引导时进入 BIOS 设置屏幕。

注释 您必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

步骤 6 点击**确定 (OK)**。

步骤 7 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 VM 已开启，请关闭系统。

b) 打开 VM。

系统进入 BIOS 设置模式。

c) 在主 **BIOS** 菜单中，使用箭头键导航到**日期和时间 (Date and Time)** 字段，然后按 **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) 使用箭头键导航到引导菜单，然后按 **Enter**。

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

g) 使用箭头键导航到**退出 (Exit)** 菜单，然后选择**退出并保存更改 (Exit Saving Changes)**（按 Enter 或 Return 键以选择对应的选项）。

h) 选择**是 (Yes)** 保存更改并退出。

步骤 8 将思科 ISE OVA 文件导入 VMware ESXi。

步骤 9 将 ZTP 配置映像文件插入 VMware ESXi 主机的主 CD/DVD 驱动器。

步骤 10 打开虚拟机。

当 DVD 启动时，控制台会显示以下信息：

```
Automatic installation starts in 150 seconds.
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)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

注释　从思科 ISE 3.1 开始，按 **Enter** 键而不输入引导选项将不会使用硬盘选项来触发安装。相反，它会触发 ZTP。

步骤 11　150 秒后，如果满足前提条件，启动过程会自动开始。

注释
- 由于 ZTP 只能通过串行控制台工作，因此安装日志只能通过串行控制台进行监控。在显示设置提示后，可以从 VM 控制台监控日志。
- 思科 ISE 服务启动后，您必须从 CD/DVD 手动卸载 ZTP 配置映像文件。

要在设置提示中使用 ZTP（使用键盘完成 ZTP，直到设置提示正确），请执行此程序：

1. 手动安装思科 ISE，直到设置完成（使用引导选项 1 或 2），然后按照上述程序中所述的步骤来创建 ZTP 配置映像文件。

2. 关闭 VM 电源。

3. 将 ZTP 配置映像文件映射到 CD/DVD 驱动器。

4. 启动 VM。

设置详细信息将从映射到 CD/DVD 驱动器的 ZTP 配置文件中提取。

故障排除

问题：如果设置详细信息在配置文件中无效，则 ZTP 安装将停止，并且 VM 控制台上会显示以下消息：

```
================================================================================

Cisco ISE Installation Failed

================================================================================

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

================================================================================
```

解决方案：这可以通过执行以下步骤来加以解决：

1. 使用有效的详细信息来创建新的 configuration.img 文件。
2. 关闭 VM 电源。
3. 将新的有效映像映射到 CD/DVD 驱动器。
4. 启动 VM。

安装会从设置开始。

使用 VM 用户数据进行 OVA 自动安装

步骤 1 登录到 VMware 客户端。

注释 如果您已有现有的VM设置，请继续执行第2步并继续执行第6步。对于新的虚拟机设置，请直接转到第8 步。

步骤 2 要使 VM 进入 BIOS 设置模式，请右键点击 VM，然后选择**编辑设置 (Edit Settings)**。

步骤 3 点击**选项 (Options)** 选项卡。

步骤 4 点击**引导选项 (Boot Options)**。

步骤 5 在**强制 BIOS 设置 (Force BIOS Setup)** 区域中选中 **BIOS** 复选框，以便在 VM 引导时进入 BIOS 设置屏幕。

注释 您必须在 VM 设置的引导模式下将固件从 **BIOS** 更改为 **EFI**，才能引导 2 TB 或更大容量的 GPT 分区。

步骤 6 点击**确定 (OK)**。

步骤 7 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 VM 已开启，请关闭系统。
b) 打开 VM。

系统进入 BIOS 设置模式。

c) 在主 **BIOS** 菜单中，使用箭头键导航到**日期和时间 (Date and Time)** 字段，然后按 **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) 使用箭头键导航到引导菜单，然后按 **Enter**。
f) 使用箭头键选择 CD-ROM 驱动器，然后按 **+** 将 CD-ROM 驱动器的启动顺序向上移动。
g) 使用箭头键导航到**退出 (Exit)** 菜单，然后选择**退出并保存更改 (Exit Saving Changes)**（按 Enter 或 Return 键以选择对应的选项）。
h) 选择**是 (Yes)** 保存更改并退出。

步骤 8 将思科 ISE OVA 文件导入 VMware ESXi。

步骤 9 配置 VM 用户数据 (VM user data) 选项。

注释 如果在 VM 中同时配置了 .img 文件和 VM 用户数据选项，则会考虑用户数据选项。

步骤 10 打开 VM。

当 DVD 启动时，控制台会显示以下信息：

```
Automatic installation starts in 150 seconds.
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)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

注释　从思科 ISE 3.1 开始，按 **Enter** 键而不输入引导选项将不会使用硬盘选项来触发安装。相反，它会触发 ZTP。

步骤 11　150 秒后，如果满足前提条件，启动过程会自动开始。

注释
- 由于 ZTP 只能通过串行控制台工作，因此安装日志只能通过串行控制台进行监控。在显示设置提示后，可以从 VM 控制台对其进行监控。
- 思科 ISE 服务启动后，您必须从 CD/DVD 手动卸载 ZTP 配置映像文件。

要在设置提示中使用 ZTP（使用键盘执行 ZTP，直到设置提示正确），请执行此程序：

1. 手动安装思科 ISE 直到设置完成（使用引导选项 1 或 2）。\
2. 关闭 VM 电源。
3. 配置上述用户数据选项。
4. 打开 VM 电源。

设置详细信息将从 VM 选项中选取。

故障排除

问题：如果在用户数据选项中输入了无效的设置详细信息，则 ZTP 安装将停止，并且 VM 控制台上会显示以下消息：

```
================================================================================

Cisco ISE Installation Failed

================================================================================

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

================================================================================
```

解决方案：这可以通过执行以下步骤来加以解决：

1. 关闭 VM 电源。

2. 使用有效的数据来更新用户数据详细信息。

3. 启动 VM。

安装会从设置开始。

创建 ZTP 配置映像文件

使用 **./create_ztp_image.sh ise-ztp.conf ise-ztp.img** 命令来创建 ZTP 配置映像文件。该脚本可以在 RHEL、CentOS 或 Ubuntu 上执行。

要跳过 ICMP、DNS 和 NTP 检查，请在配置映像文件中将以下标志设为 True：

- **ICMP**：SkipIcmpChecks=true
- **DNS**：SkipDnsChecks=true
- **NTP**：SkipNtpChecks=true

create_ztp_image.sh 脚本创建

```
#!/bin/bash
############################################################
# This script is used to generate ise ztp image with ztp
# configuration file.
#
# Need to pass ztp configuration file as input.
#
# Copyright (c) 2021 by Cisco Systems, Inc.
# All rights reserved.
# Note:
# To mount the image use below command
# mount ise_ztp_config.img /ztp
# To mount the image from cdrom
# mount -o ro /dev/sr1 /ztp
############################################################
if [ -z "$1" ];then
echo "Usage:$0 <ise-ztp.conf> [out-ztp.img]"
exit 1
elif [ ! -f $1 ];then
echo "file $1 not exist"
exit 1
else
conf_file=$1
fi
if [ -z "$2" ] ;then
image=ise_config.img
else
image=$2
fi
mountpath=/tmp/ise_ztp
ztplabel=ISE-ZTP
rm -fr $mountpath
mkdir -p $mountpath
dd if=/dev/zero of=$image bs=1k count=1440 > /dev/null 2>&1
if [ `echo $?` -ne 0 ];then
echo "Image creation failed\n"
exit 1
fi
```

```
mkfs.ext4 $image -L $ztplabel -F > /dev/null 2>&1
mount -o rw,loop $image $mountpath
cp $conf_file $mountpath/ise-ztp.conf
sync
umount $mountpath
sleep 1
# Check for automount and unmount
automountpath=$(mount | grep $ztplabel | awk '{print $3}')
if [ -n "$automountpath" ];then
umount $automountpath
fi
echo "Image created $image"
```

ise-ztp.conf 示例配置文件创建

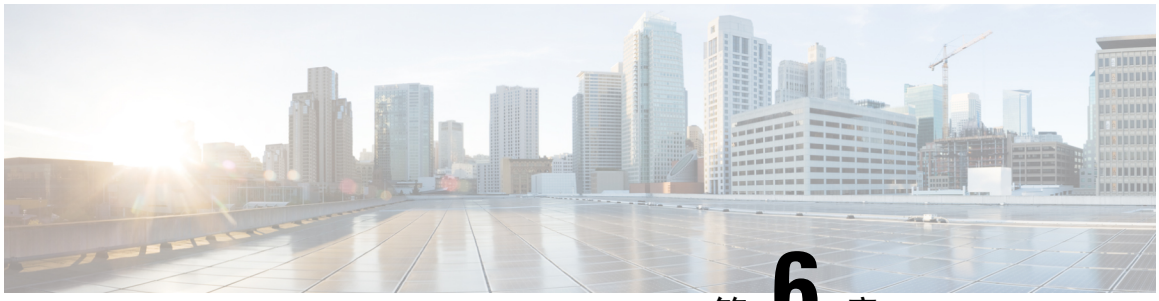
```
hostname=ISETEST-80
ipv4_addr=10.126.68.80
ipv4_mask=255.255.255.0
ipv4_default_gw=10.126.68.1
#IPv6 optional
ipv6_addr=2001:420:54ff:4::455:91/119
ipv6_default_gw=2001:420:54ff:4::455:1
domain=cisco.com
primary_nameserver=72.163.128.140
# secondary and tertiary are optional
secondary_nameserver=72.163.128.141
tertiary_nameserver=72.163.128.142
primary_ntpserver=ntp.esl.cisco.com
# secondary and tertiary are optional
secondary_ntpserver=ntp1.esl.cisco.com
tertiary_ntpserver=ntp2.esl.cisco.com
timezone=Asia/Kolkata
ssh=true
username=admin
password=Test123
#Repository Configuration are optional
repository_name=nfs_repo
repository_protocol=nfs
repository_server_name=10.77.124.11
repository_path=/volume1/vms/infra/patchHotpatch
#Patch Information - optional
patch=ise-patchbundle-3.1.0.367-Patch1-21050400.SPA.x86_64.tar.gz
#HotPatches Information - optional
hotpatches=ise-apply-CSCvo87602_2.x_MemoryDiagnostics_3-SPA.tar.gz,ise-apply-
CSCvo87602_2.x_MemoryDiagnostics_4-SPA.tar.gz
#services - optional
ers=true
openapi=true
pxgrid=true
pxGrid_Cloud=true
# Skipping specific checks
SkipIcmpChecks=true
SkipDnsChecks=true
SkipNtpChecks=true
```

VM 用户数据

思科 ISE 安装支持 ESXi 6.5 及更高版本的 VM 用户数据。

在 base64encode 工具中粘贴 **ise-ztp.conf** 文件的内容。使用 base64encode tool 以获取编码字符串。

您必须在 VM 中输入编码的 base64 字符串以及 VM 用户数据。在 VMware ESXi 中，前往 **VM 选项 (VM Options) > 高级 (Advanced) > 配置参数 (Configuration Parameters) > 编辑配置 (Edit Configuration) > guestinfo.ise.ztp = [Value] Base 编码的 ZTP 配置 (guestinfo.ise.ztp = [Value] Base Encoded ZTP Configuration)** 以输入字符串。



第 6 章

安装验证和安装后任务

登录到思科 ISE 基于 Web 的界面

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

注释 我们建议您使用思科 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， 则思科 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。

有关经过验证的浏览器的信息，请参阅 《Cisco ISE 版本说明》中的“验证的浏览器”部分。

步骤 1 在思科 ISE 设备重新启动完成后，启动其中一种受支持的网络浏览器。

步骤 2 在“地址”(Address) 字段中，通过使用以下格式输入思科 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**登录 (Login)**。

CLI 管理员和基于 Web 的管理员的用户任务差异

使用思科 ISE 设置程序时设置的用户名和密码旨在用于对思科 ISE CLI 和思科 ISE Web 界面进行管理访问。具有思科 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思科 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思科 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。

思科 ISE CLI 管理员用户具有与思科 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	• 备份思科 ISE 应用数据。 • 显示思科 ISE 设备上的所有系统、应用或诊断日志。 • 应用思科 ISE 软件补丁、维护版本和升级。 • 设置 NTP 服务器配置。
仅限 CLI 管理员	• 启动和停止思科 ISE 应用软件。 • 重新加载或关闭思科 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。

创建 CLI 管理员

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

您可以在配置模式下使用以下命令来添加 CLI 管理员用户：

```
username <username> password [plain/hash] <password> role admin
```

创建基于 Web 的管理员

首次对思科 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。

添加管理员用户：

1. 在思科 ISE GUI 中，点击**菜单** 图标 (☰)，然后选择**管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员用户 (Admin Users)**。
2. 选择**添加 (Add) > 创建管理员用户 (Create an Admin User)**。
3. 输入名称、密码、管理员组及其他所需的详细信息。
4. 点击**提交**。

因管理员锁定而重置禁用的密码

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。。

思科 ISE 在**管理员登录 (Administrator Logins)** 窗口中添加了一条日志条目。要查看此处窗口，请点击**菜单** 图标 (☰)，然后选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 审核 (Audit) > 管理员登录 (Administrator Logins)**。此管理员 ID 的凭证将暂停，直至您重置与此 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
```

思科 ISE 配置验证

共有两种验证方法，它们分别通过网络浏览器和 CLI 使用一组不同的用户名和密码凭证来验证思科 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思科 ISE 中不同。

使用网络浏览器验证配置

步骤 1 在思科 ISE 设备重新启动完成后，启动其中一种受支持的网络浏览器。

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

步骤 3 在“思科 ISE 登录”(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**登录 (Login)**。

例如，输入 https://10.10.10.10/admin/ 会显示思科 ISE 登录 (Cisco ISE Login) 页面。

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

注释 首次对思科 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 使用思科 ISE 控制面板验证设备是否正常工作。

下一步做什么

通过使用思科 ISE 基于 Web 的用户界面菜单和选项，您可以配置思科 ISE 系统以满足您的要求。有关配置思科 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

下载并安装最新的思科 ISE 补丁，以便让思科 ISE 保持最新状态。

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

步骤 2 在“主机名称”(Host Name)（或 IP 地址 (IP Address)）字段中，输入主机名（或思科 ISE 设备的点分十进制格式的 IP 地址），然后点击**打开 (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 在提示符后，输入 **show application version ise** 并按 **Enter** 键。

步骤 6 要检查思科 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          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
```

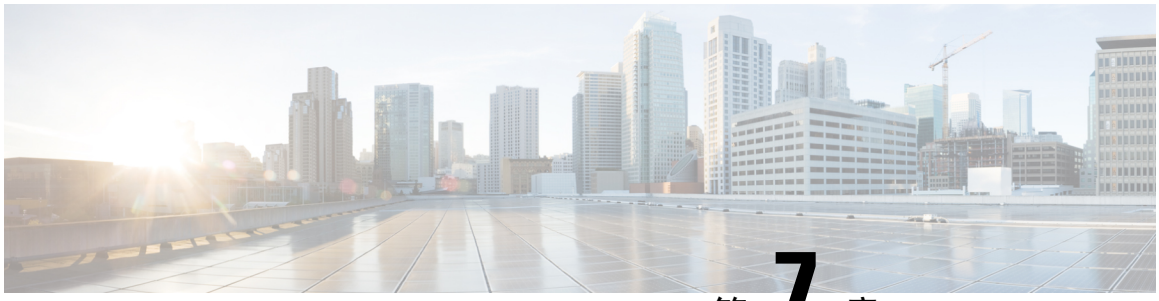
安装后任务列表

安装思科 ISE 后，您必须执行以下必要任务：

表 *15:* 强制安装后任务

任务	管理指南中的链接
应用最新补丁（如果有）	请参阅适用于您的版本的《思科 *ISE* 管理员指南》中“维护和监控”一章中的“软件补丁安装指南”部分。
安装许可证	有关详细信息，请参阅《思科 ISE 订购指南》。请参阅适用于您的版本的《思科 *ISE* 管理员指南》中的“许可”一章。
安装证书	请参阅适用于您的版本的《思科 *ISE* 管理员指南》中“基本设置”一章中的“思科 ISE 中的证书管理”部分。

任务	管理指南中的链接
创建备份存储库	请参阅适用于您的版本的《思科*ISE*管理员指南》中“维护和监控”一章中的“创建存储库”部分。
配置备份计划	请参阅适用于您的版本的《思科*ISE*管理员指南》中“维护和监控”一章中的“计划备份”部分。
部署思科 ISE 角色	请参阅适用于您的版本的《思科*ISE*管理员指南》中“部署”一章中的“思科 ISE 分布式部署”部分。



第 7 章

常见系统维护任务

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聚合功能。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。

表 *16:* 绑定在一起形成接口的物理 *NIC*

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 3500 和 3600 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，了解有关哪些 NIC 可以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 interface** 命令查看已绑定的接口。

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,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,SUBORDINATE,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=6211<UP,BROADCAST,RUNNING,SUBORDINATE,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** 并按 Enter 键。

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。在 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)#
```

使用 DVD 重置丢失、忘记或泄漏的密码

开始之前

确保您了解在尝试使用思科 ISE 软件 DVD 启动思科 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 的思科 ISE 设备的串行控制台连接相关联。通过将其设置为 *no exec*，您可以使用键盘和视频显示器连接以及串行控制台连接。
- 您具有到思科ISE设备的键盘和视频显示器连接（它可以是远程键盘和视频显示器连接或VMware vSphere 客户端控制台连接）。
- 您具有到思科 ISE 设备的串行控制台连接。

步骤 1 确保思科 ISE 设备已接通电源。

步骤 2 插入思科 ISE 软件 DVD。

步骤 3 使用箭头键进行选择，如果使用本地串行控制台端口连接，请选择**系统实用程序（串行控制台）(System Utilities [Serial Console])**，如果使用键盘和视频显示器连接至设备，请选择**系统实用程序（键盘/监视器）(System Utilities [Keyboard/Monitor])**，然后按 **Enter**。

系统会显示 ISO 实用工具菜单，如下所示。

```
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:
```

步骤 4 输入 **1** 以恢复管理员密码。

控制台会显示：

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.

[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4

Enter choice between [1 - 4] or q to Quit: 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。

因管理员锁定而重置禁用的密码

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。。

思科 ISE 在**管理员登录 (Administrator Logins)** 窗口中添加了一条日志条目。要查看此处窗口，请点击**菜单** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **管理员登录 (Administrator Logins)**。此管理员 ID 的凭证将暂停，直至您重置与此 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
```

退货许可

对于退货授权 (RMA)，如果要更换 SNS 服务器上的单个组件，请务必先重新映像设备，再安装思科 ISE。如需帮助，请与 Cisco TAC 联系。

更改思科 ISE 设备的 IP 地址

开始之前

- 在更改 IP 地址之前，请确保思科 ISE 节点处于独立状态。如果该节点是分布式部署的一部分，请从部署中取消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 登录到思科 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

思科 ISE 提供一个命令行界面 (CLI) 命令来查看思科 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 - 思科 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 - 从其安装思科 ISE 应用捆绑包的存储库。不适用于卸载。

步骤 1 登录到思科 ISE CLI。

步骤 2 输入以下命令：**show version history**。

系统将显示以下输出：

```
ise/admin# show version history
-------------------------------------------
Install Date: Fri Nov 30 21:48:58 UTC 2018
Application: ise
Version: 3.0.0.xxx
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

执行系统清除

您可以执行系统清除以安全地清除思科 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思科 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思科 ISE 软件 DVD 启动思科 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 的思科 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。
- 您具有到思科 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）。
- 您具有到思科 ISE 设备的串行控制台连接。

步骤 1 确保思科 ISE 设备已接通电源。

步骤 2 插入思科 ISE 软件 DVD。

步骤 3 使用箭头键选择**系统实用程序（串行控制台）(System Utilities [Serial Console])**，并按 Enter。

系统随即会显示 ISO 实用工具菜单，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：

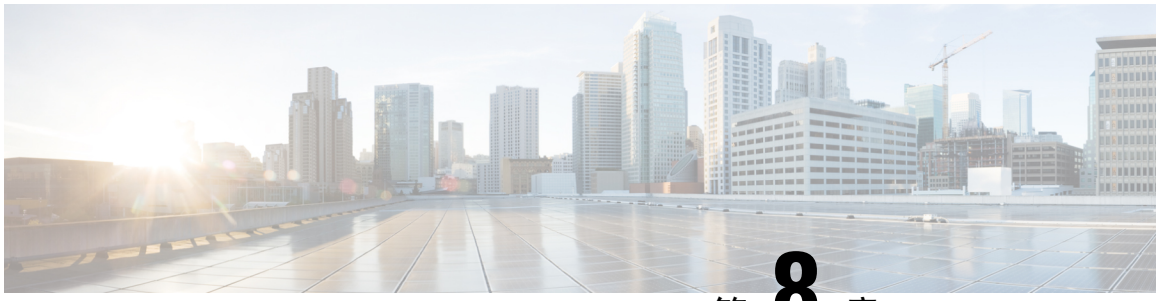
```
THIS IS YOUR LAST CHANGE TO CANCEL. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

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，则必须使用思科 ISE DVD 启动系统并从启动菜单中选择安装选项。



第 8 章

思科 ISE 端口参考

思科 ISE 所有角色节点端口

表 *17:* 所有节点使用的端口

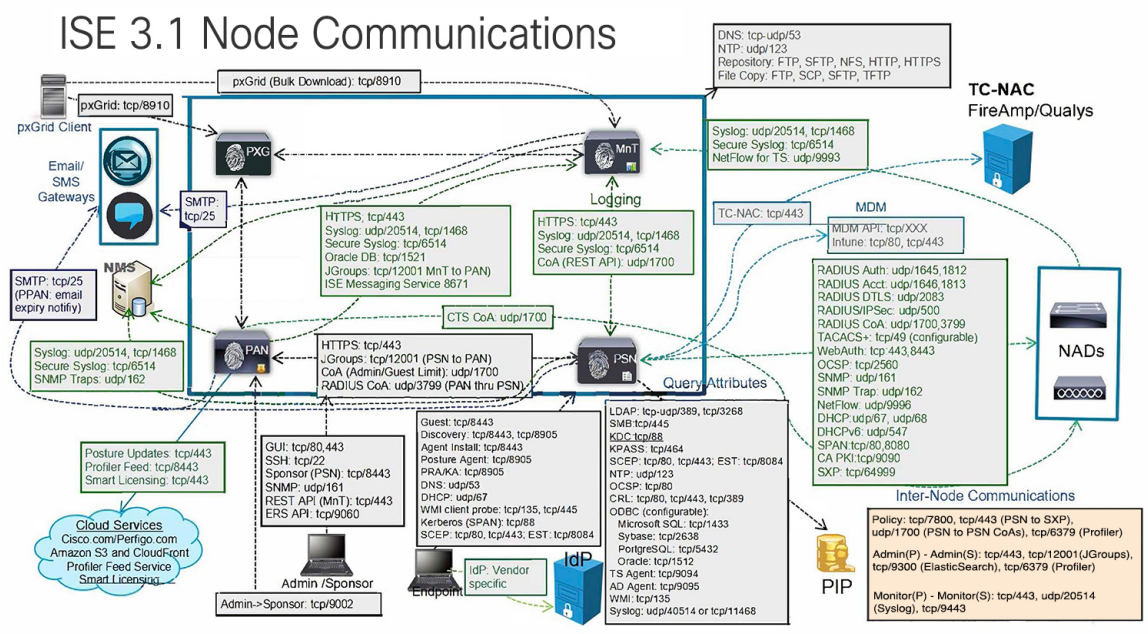
思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
复制和同步	• HTTPS (SOAP)：TCP/443 • 数据同步/复制 (JGroups)：TCP/12001（全局） • ISE 消息服务：SSL：TCP/8671 • 分析器终端所有权同步/复制：TCP/6379	—

思科 ISE 基础设施

本附录列出思科 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。此附录中列出的思科 ISE 端口在对应的防火墙上必须处于打开状态。

在思科 ISE 网络上配置服务时，请记住以下信息：

- 端口将基于您的部署中启用的服务而启用。除了由ISE中运行的服务打开的端口之外，思科ISE将拒绝访问所有其他端口。
- 思科 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。如果在硬件设备上安装，请确保在用于连接到思科 ISE 节点的交换端口上禁用 VLAN 中继，并将这些端口配置为接入层端口。
- 临时端口范围为 10000 到 65500。这在思科 ISE 版本 2.1 及更高版本中保持不变。
- 站点间 VPN 网络配置支持 VMware 云。因此，必须建立从网络访问设备和客户端到思科 ISE 的 IP 地址或端口可访问性，而无需进行 NAT 或端口过滤。
- 所有 NIC 都可以配置有 IP 地址。
- 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。



相关概念

分布式部署中的节点类型和角色，第 3 页

注释 ISE 上的 TCP 保持连接时间为 60 分钟。如果 ISE 节点之间存在防火墙，请在防火墙上相应调整 TCP 超时值。

思科 ISE 管理节点端口

下表列出了管理节点使用的端口：

表 *18:* 管理节点使用的端口

思科 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		-

思科 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
	• 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 • CoA • 外部 RESTful 服务 (ERS) REST API：TCP/9060 注释 ERS 和 OpenAPI 服务是仅通过端口 443 运行的 HTTPS REST API。目前，ERS API 也通过端口 9060 运行。但是，在更高版本的思科 ISE 中，ERS API 可能不支持端口 9060。我们建议您仅将端口 443 用于 ERS API。 • • 从管理员 GUI 管理访客帐户：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。 对思科 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	

思科 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
	点上对传入流量开放。 注释 对于 SAML 管理员登录，应从管理员尝试执行 SAML 登录的设备访问 PSN 的端口 8443。	
监控	• SNMP 查询：UDP/161 注释 此端口因路由表而异。 • ICMP	
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	

思科 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 • 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/1521 • 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。	
邮件	访客帐户和用户密码到期电子邮件通知：SMTP：TCP/25	
智能许可	通过 TCP/443 连接至思科云 通过 TCP/443 和 ICMP 连接到 SSM 本地服务器	

思科 ISE 监控节点端口

下表列出了监控节点使用的端口：

表 *19:* 监控节点使用的端口

思科 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	-
监控	简单网络管理协议 [SNMP]：UDP/161 注释 此端口因路由表而异。 • ICMP	
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 用于警报电子邮件 • SNMP 陷阱：UDP/162	

思科 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/1521，15723，16820 • 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。	
用于入站通信的端口	• 源自启用了 ISE API 网关以路由 MnT REST API 的 ISE 节点的 MnT 入站通信：TCP/9443 • 来自 PAN 的全局搜索：TCP/1521 注释 无论是现场还是云，这些端口在所有类型的部署中均为必需。	
pxGrid 批量下载	SSL：TCP/8910	

思科 ISE 策略服务节点端口

思科 ISE 支持 HTTP 严格传输安全 (HSTS) 以提高安全性。思科 ISE 发送 HTTPS 响应，以向浏览器指示只能使用 HTTPS 访问 ISE。如果用户随后尝试使用 HTTP 而不是 HTTPS 访问 ISE，则浏览器会

在生成任何网络流量之前将连接更改为 HTTPS。此功能可防止浏览器使用未加密的 HTTP 向思科 ISE 发送请求，避免服务器重定向这些请求。

下表列出了策略服务节点使用的端口：

表 *20:* 策略服务节点使用的端口

思科 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	思科 ISE 管理只限于千兆以太网 0。
集群（节点组）	节点组/JGroups：TCP/7800	—
SCEP	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。	
TrustSec	使用 HTTP 和思科 ISE REST API 通过端口 9063 将 TrustSec 数据传输到网络设备。	
SXP	• PSN（SXP 节点）到 NAD：TCP/64999 • PSN 到 SXP（节点间通信）： TCP/9644	
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	

思科 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/1521
	• 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	

思科 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 - 阻止列表门户	HTTPS（必须为思科 ISE 中的服务启用接口）： • 阻止列表门户：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/8445） • 来自访客和发起人门户的 SMTP 访客通知：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。 从思科 ISE 3.1开始，非策略服务节点上已默认禁用端口 8905。要启用此端口，请在**常规设置 (General Settings)** 窗口（**管理 (Administration) > 系统 (System) > 设置 (Settings) > 安全评估 (Posture) > 一般设置 (General Settings)**）中选中**在非政策服务节点上为安全评估服务启用 8905 端口 (Enable Port 8905 on non-Policy Service Nodes for Posture Services)** 复选框。 • 发现（策略服务节点端）：TCP/8443 和 8905 (HTTPS) 从思科 ISE 版本 2.2 或更高版本以及 AnyConnect 版本 4.4 或更高版本开始，此端口可配置。 • 评估 - 状态协商和代理报告：TCP/8905 (HTTPS) • 双向安全评估流程 - TCP/8000-8999（默认端口为 TCP/8449）	

思科 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”。 • 对于使用 EST 身份验证的 Android 设备：TCP/8084。对于 Android 设备，端口 8084 必须添加到重定向 ACL。 • 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 - 从思科 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	
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。	

思科 ISE pxGrid 服务端口

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

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

下表列出了 pxGrid 服务节点使用的端口：

表 *21: pxGrid* 服务节点使用的端口

思科 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
pxGrid 用户	TCP/8910	

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。思科 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。

思科 ISE 进程

下表列出了思科 ISE 进程及其服务影响：

进程名称	说明	服务影响
数据库侦听程序	Oracle 企业数据库侦听程序	必须处于运行状态，所有服务才能正常工作
数据库服务器	Oracle 企业数据库服务器。存储配置数据与操作数据。	必须处于运行状态，所有服务才能正常工作
应用服务器	ISE 的主 Tomcat 服务器	必须处于运行状态，所有服务才能正常工作

分析器数据库	用于 ISE 分析服务的 Redis 数据库	必须处于运行状态，ISE 分析服务才能正常工作
AD 连接器	Active Directory 运行时	必须处于运行状态，ISE 才能执行 Active Directory 身份验证
MnT 会话数据库	用于 MnT 服务的 Oracle TimesTen 数据库	必须处于运行状态，所有服务才能正常工作
MnT 日志收集器	用于 MnT 服务的日志收集器	必须处于运行状态才能获取 MnT 操作数据
MnT 日志处理器	用于 MnT 服务的日志处理器	必须处于运行状态才能获取 MnT 操作数据
证书颁发机构服务	ISE 内部 CA 服务	如果已启用 ISE 内部 CA，则必须处于运行状态

所需互联网 URL

下表列出了会使用某些 URL 的功能。配置网络防火墙或代理服务器，这样 IP 流量才能在思科 ISE 和这些资源之间传输。如果无法访问下表中列出的任何 URL，则表明相关功能可能已损坏或无法运行。

表 *22:* 所需 *URL* 访问权限

特性	URL
安全评估更新	https://www.cisco.com/ https://iseservice.cisco.com
分析源服务	https://ise.cisco.com
智能许可	https://tools.cisco.com

交互式帮助功能需要使用思科 ISE 才能使用管理门户浏览器连接到以下 URL：

- * .walkme.com
- * .walkmeusercontent.com

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。