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：

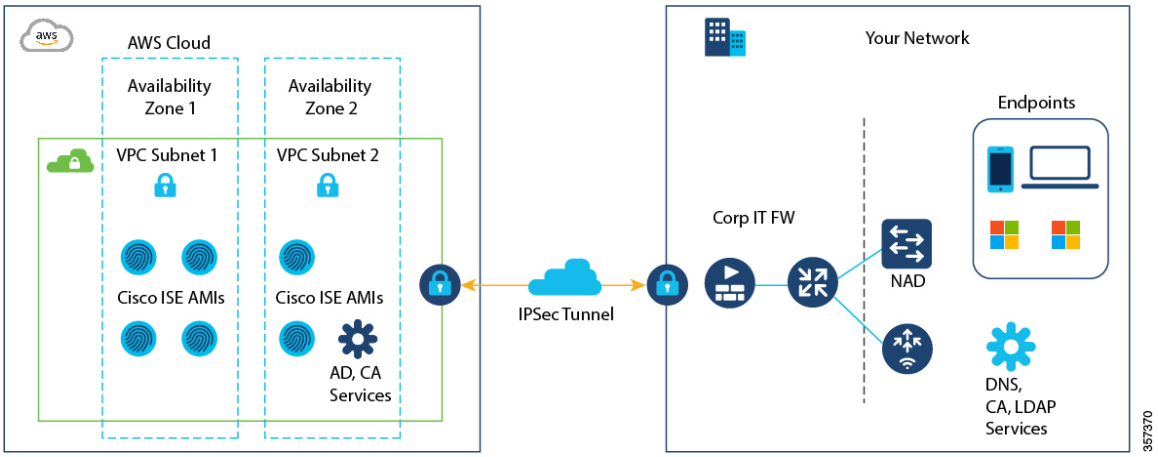
- 通过 AWS 市场启动思科 ISE CloudFormation 模板， 第 5 页
- 通过云计算组建模板启动思科 ISE ， 第 7 页
- 启动思科 ISE AMI

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 *1:* 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 *1:* 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。

- 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。

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。