在AWS上部署身份服务引擎(ISE)3.4版

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 第一部分：生成一组SSH密钥对
- 第 2 部分：使用CloudFormation模板(CFT)配置ISE
- 第 3 部分：使用Amazon机器映像(AMI)配置ISE

验证

- 访问使用CFT构建的ISE实例
- 访问使用AMI构建的ISE实例
- 访问ISE GUI
- 从终端通过SSH访问CLI
- 使用PuTy通过SSH访问CLI

故障排除

- 用户名或密码无效
  - 解决方案

已知缺陷

简介

本文档介绍如何在AWS上配置思科ISE，使用：

- CloudFormation模板(CFT)
- Amazon计算机映像(AMI)

先决条件

要求

思科建议您在继续此部署之前了解以下主题：

- 思科身份服务引擎(ISE)
- AWS EC2实例管理和网络
- SSH密钥对生成和使用
- 基本了解AWS中的VPC、安全组和DNS/NTP配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎 (ISE)
- Amazon Web Services(AWS)云控制台

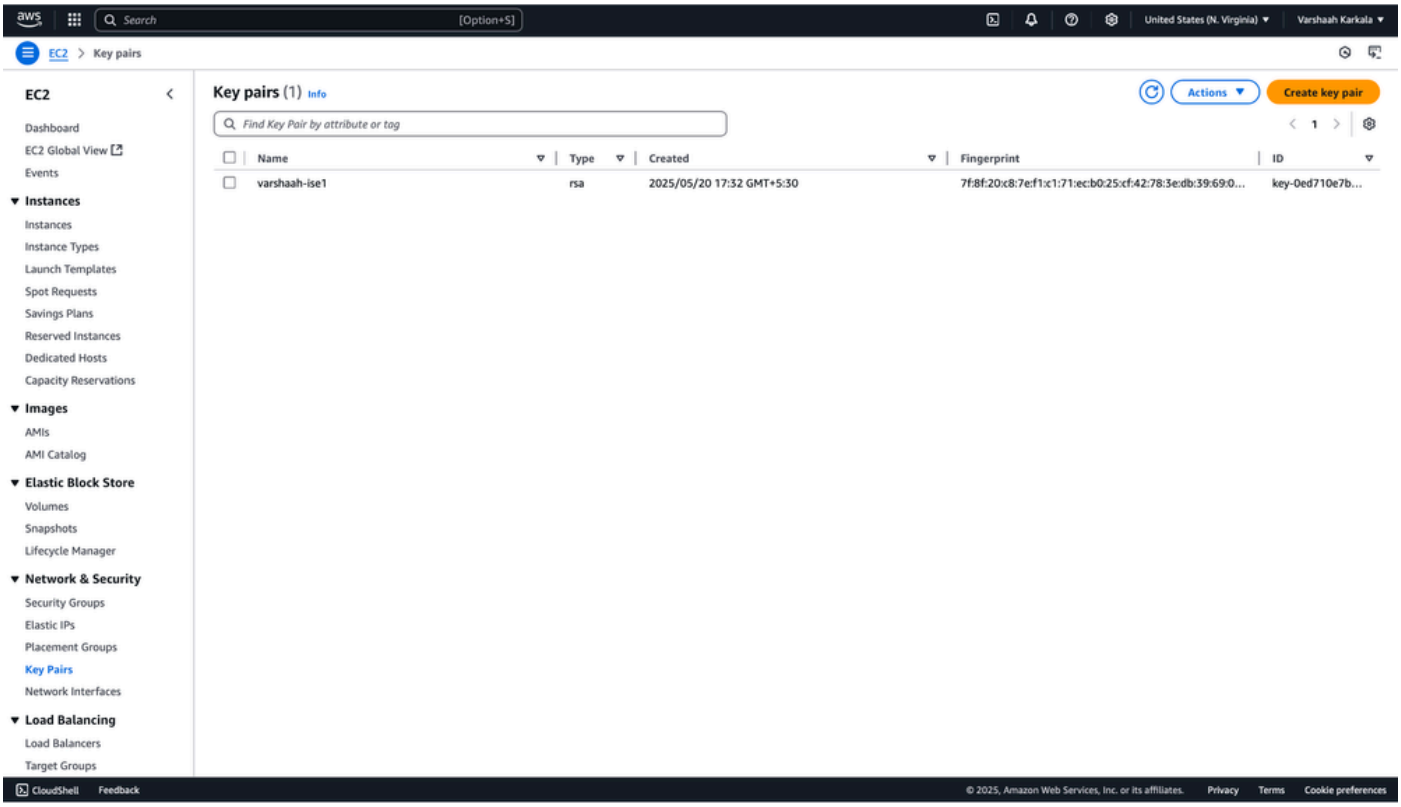
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

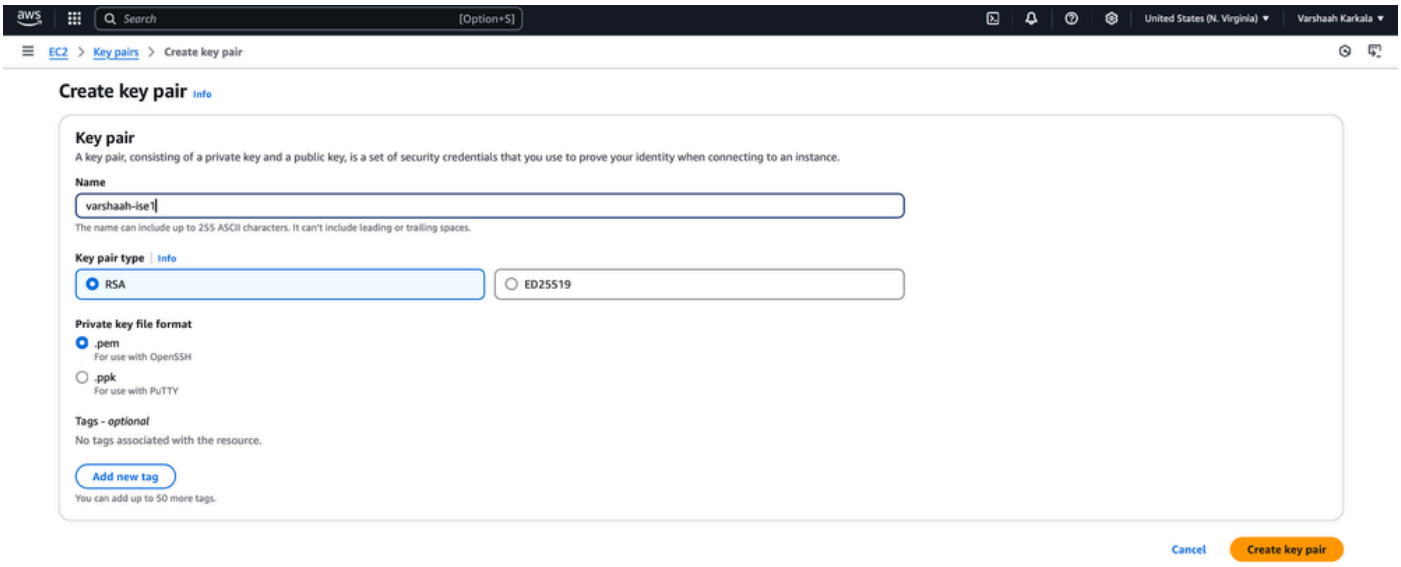
第一部分：生成一组SSH密钥对

1.对于此部署，您可以使用预先存在的密钥对，也可以创建新密钥对。

2.要创建新密钥对，请导航到EC2 > Network and Security > Key Pairs，然后单击“创建密钥对”。



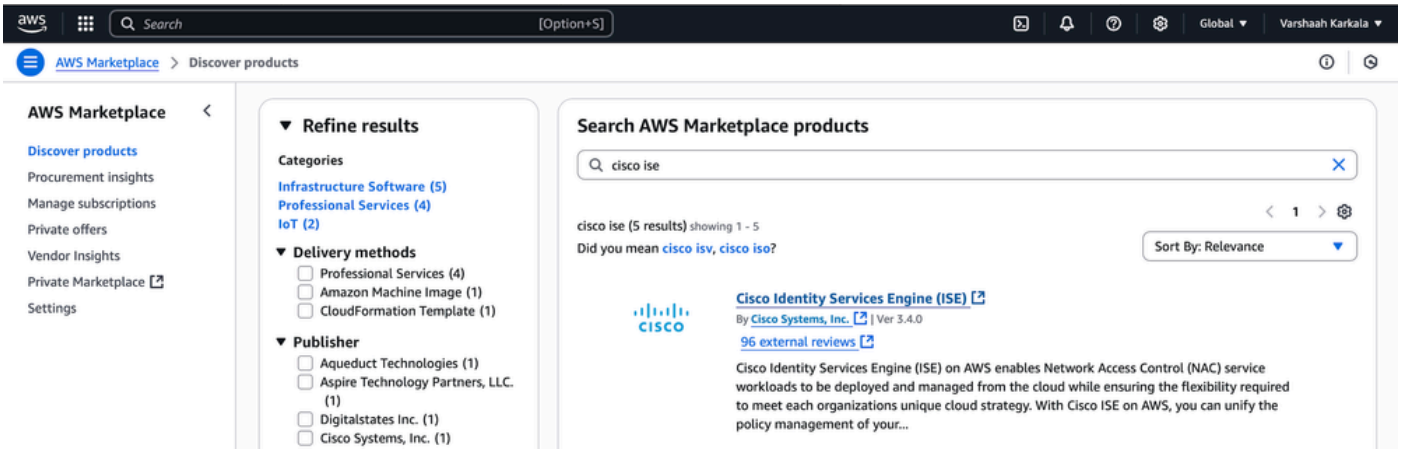
3.输入密钥对名称，然后单击“创建密钥对”。

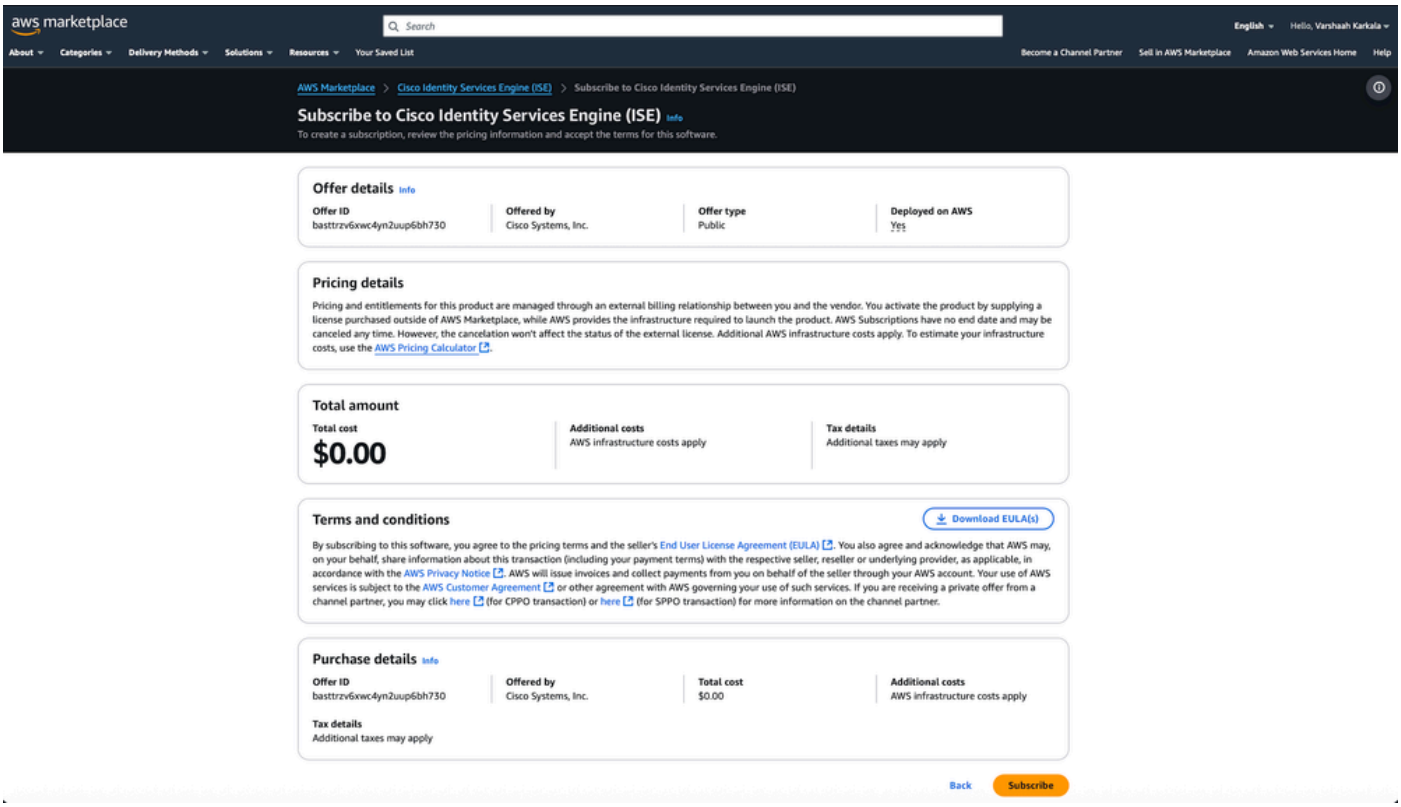


密钥对文件(.pem)会下载到本地计算机上。确保此文件是安全的，因为这是启动EC2实例后可以访问它的唯一方法。

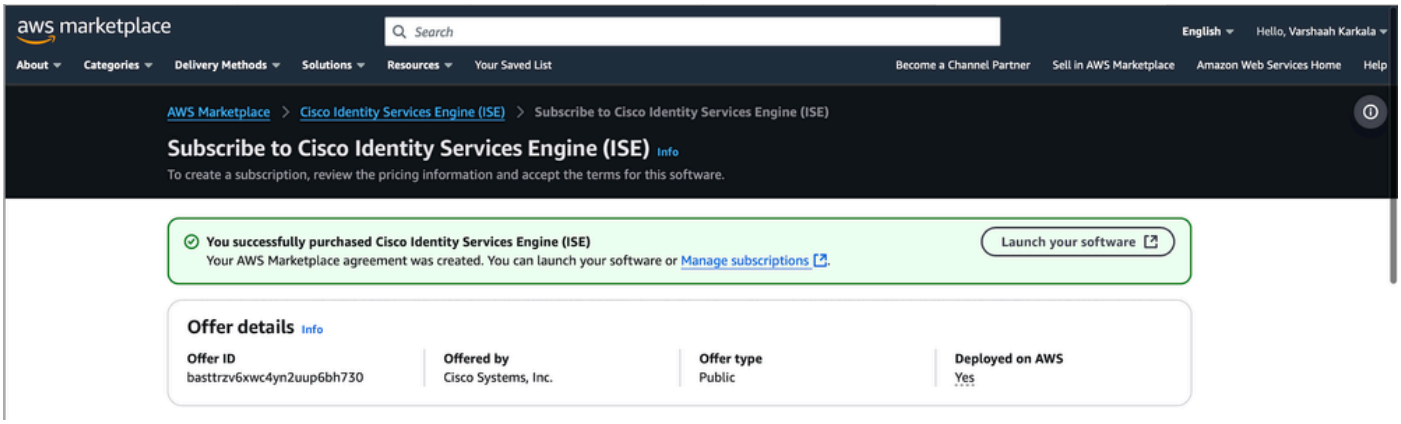
第 2 部分：使用CloudFormation模板(CFT)配置ISE

1. 登录AWS管理控制台并搜索AWS Marketplace订用。
2. 在搜索栏中，键入cisco ise，然后从结果中选择Cisco Identity Services Engine(ISE)。单击Subscribe。

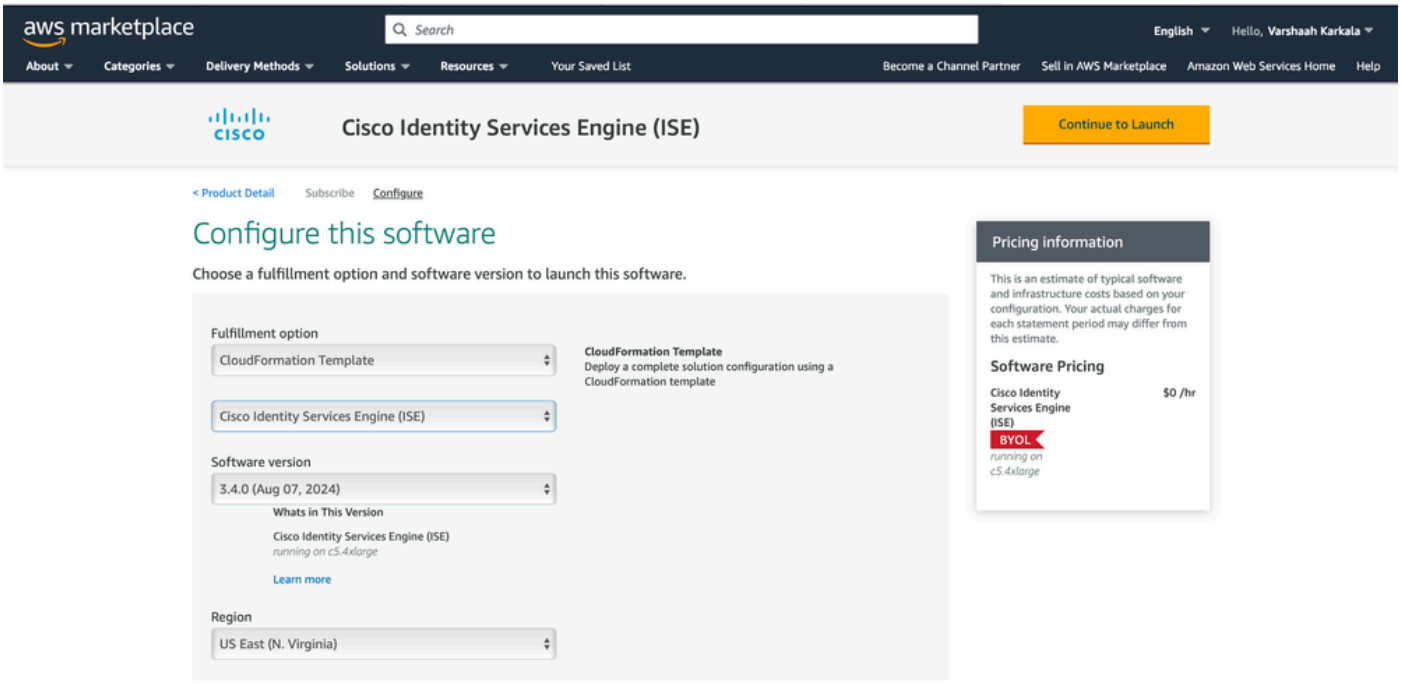




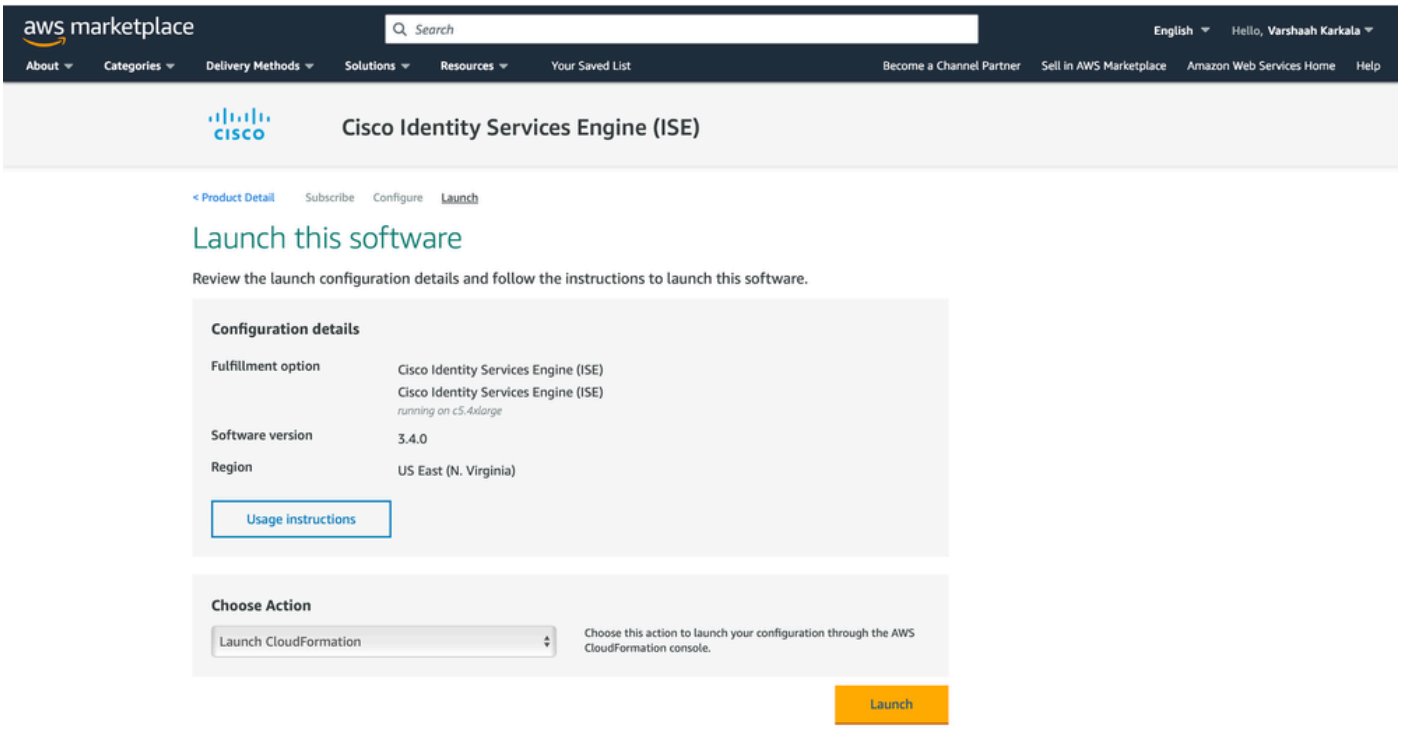
3.订购后，选择启动软件。



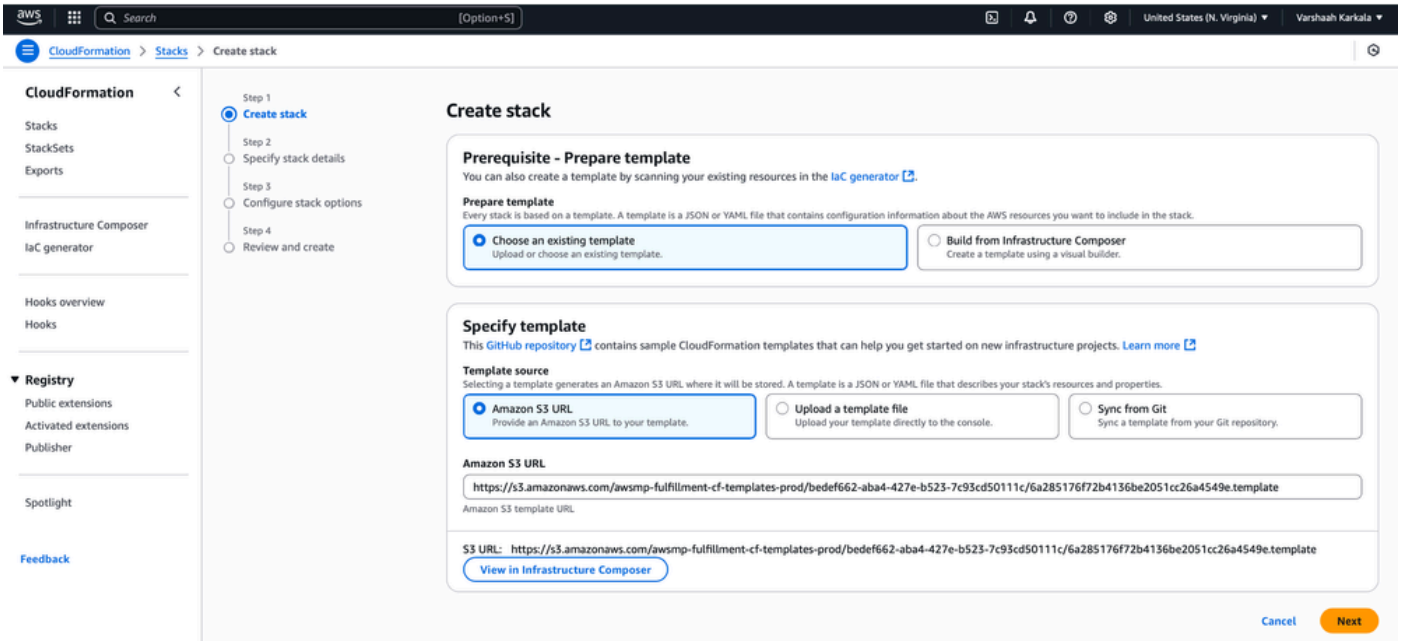
4.在“执行”选项下，选择“CloudFormation模板”。选择软件版本（ISE版本）、要部署实例的区域，然后点击继续启动。



5.在下一页上，选择Launch CloudFormation作为操作。

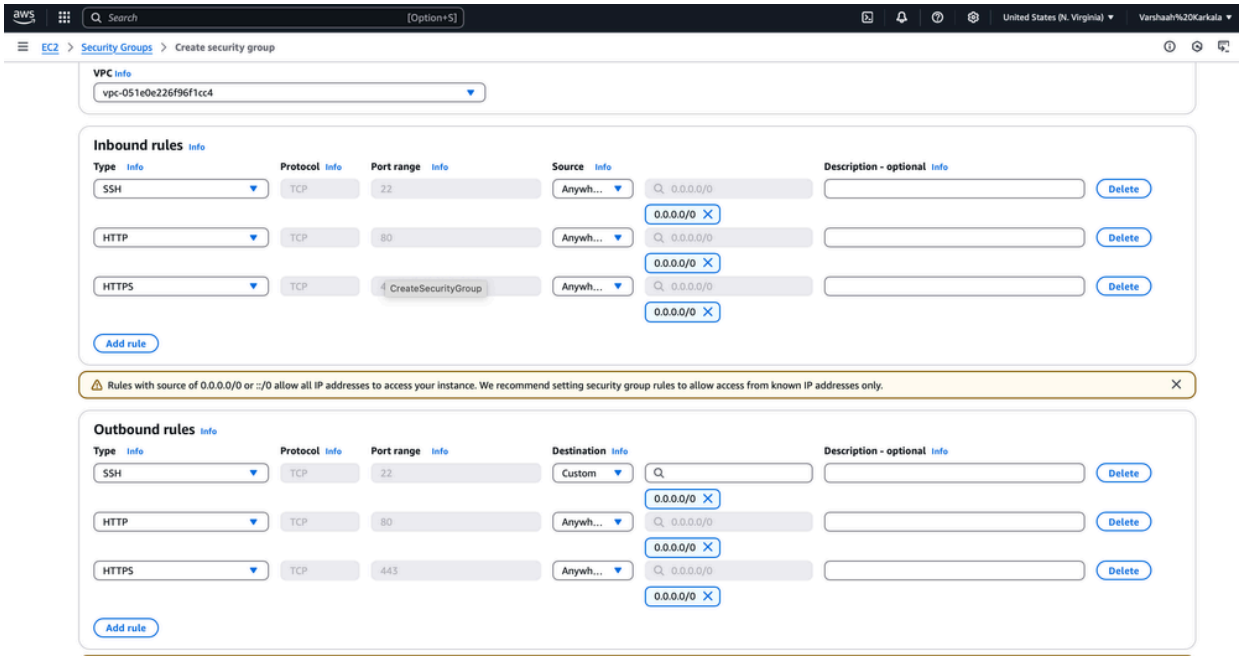


6.在“堆栈设置”下，保留默认设置，然后单击“下一步”。



7.输入所需的参数：

- 堆栈名称:为堆栈提供唯一名称。
- 主机名:为ISE节点分配主机名。
- Key pair:选择生成的密钥对或预先存在的密钥对，以便以后访问EC2实例。
- 管理安全组:
  - 使用默认安全组（如下所示）或通过EC2控制面板创建自定义安全组。
  - 要创建新的安全组，请导航到EC2 Dashboard，然后转到Network and Security > Security Groups以创建新的安全组。
  - 点击创建安全组并输入所需的详细信息。
  - 确保将安全组配置为允许所需的入站和出站流量。例如，从IP地址启用SSH（端口22）访问以进行CLI访问。

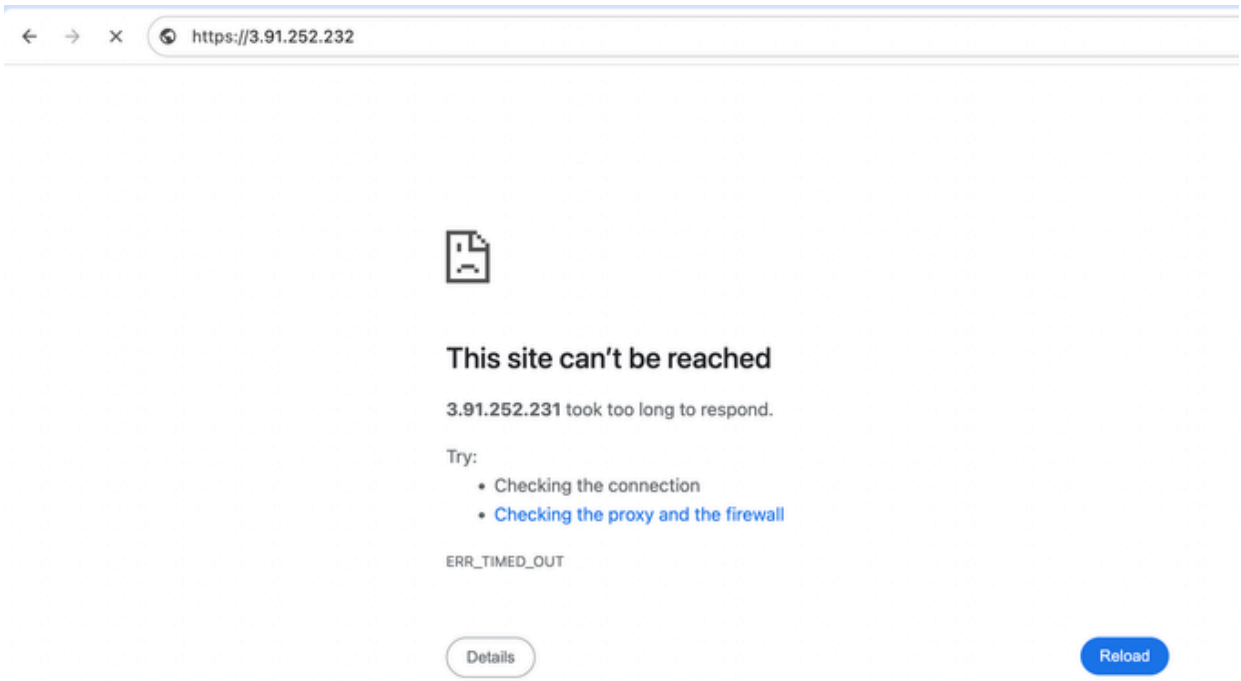


- 如果SSH访问配置不正确，则尝试通过SSH连接时可能会遇到“操作超时”错误。

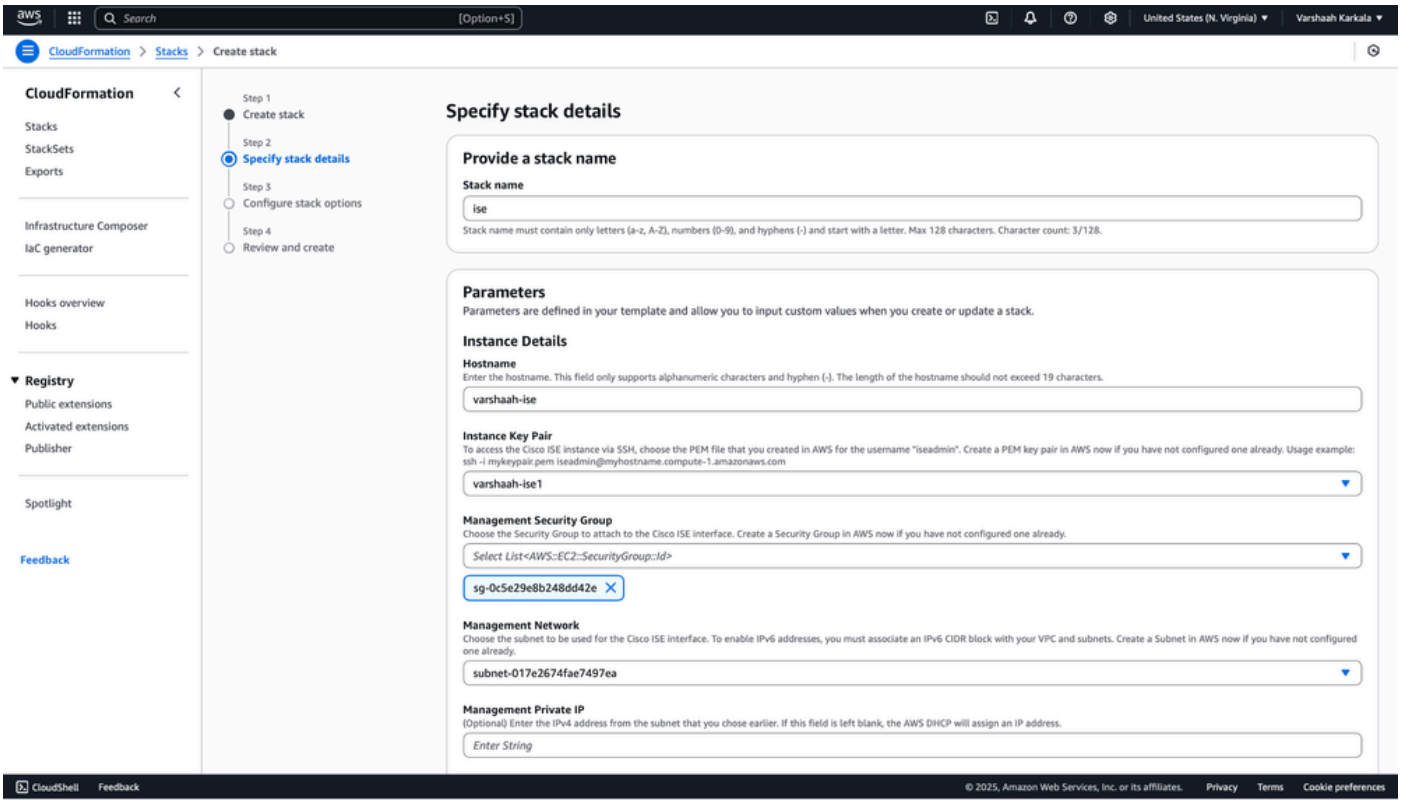
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

ssh: connect to host 3.91.252.232 port 22: Operation timed out
```

- 如果未配置HTTP/HTTPS访问，则在尝试访问GUI时，您可能会看到“无法到达此站点”错误。



- 管理网络：已选择某个预先存在的子网。



如果您的设计需要分布式部署，其中有些节点托管在AWS中，而有些节点则托管在内部部署中，请使用私有子网配置专用VPC，并建立到内部VPN前端设备的VPN隧道，以启用AWS托管和内部ISE节点之间的连接。

有关配置VPN头端设备的详细步骤，请参阅本指南。

8. EBS加密

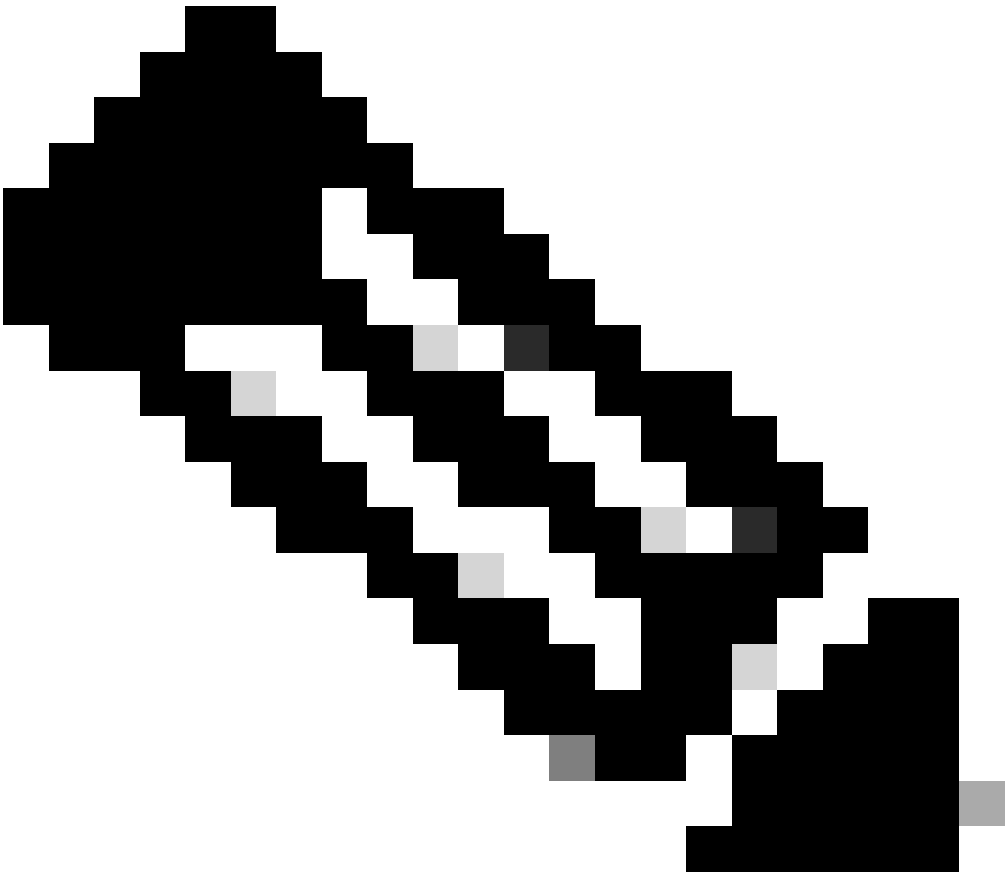
- 向下滚动以查找EBS加密设置。
- 将EBS Encryption设置为False，除非您有特定的加密需求。



9.网络配置：

- 向下滚动以访问配置网络设置的选项，例如DNS域、主名称服务器和主NTP服务器。

  确保正确输入这些值。



注意：此处的语法不正确可能会阻止ISE服务在部署后正确启动。



10.服务和用户详细信息：

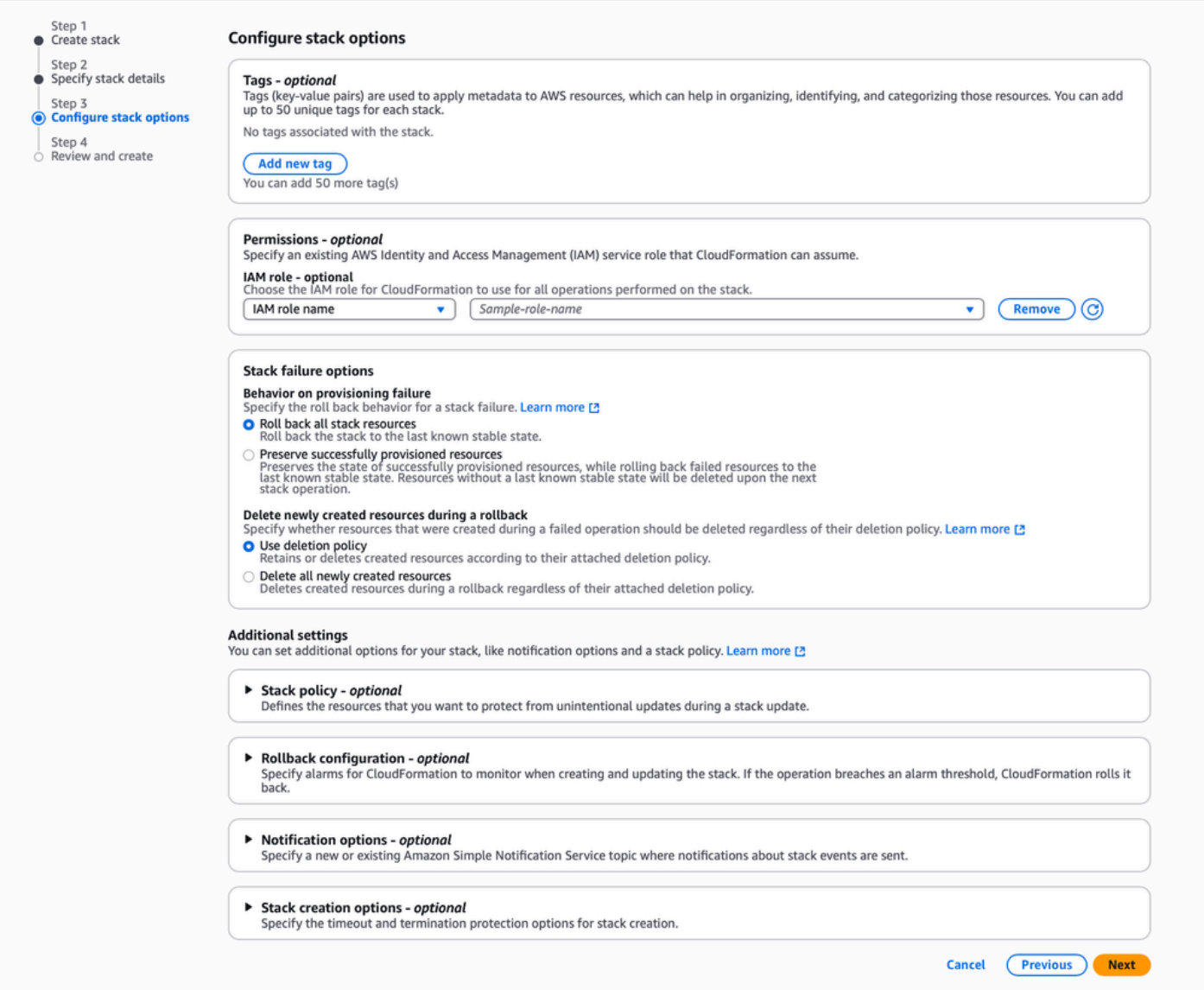
- 向下滚动以找到用于启用ERS和pxGrid服务的选项
- 选择yes或no，选择是否启用ERS和pxGrid。
- 在User Details下，设置默认admin用户的密码。



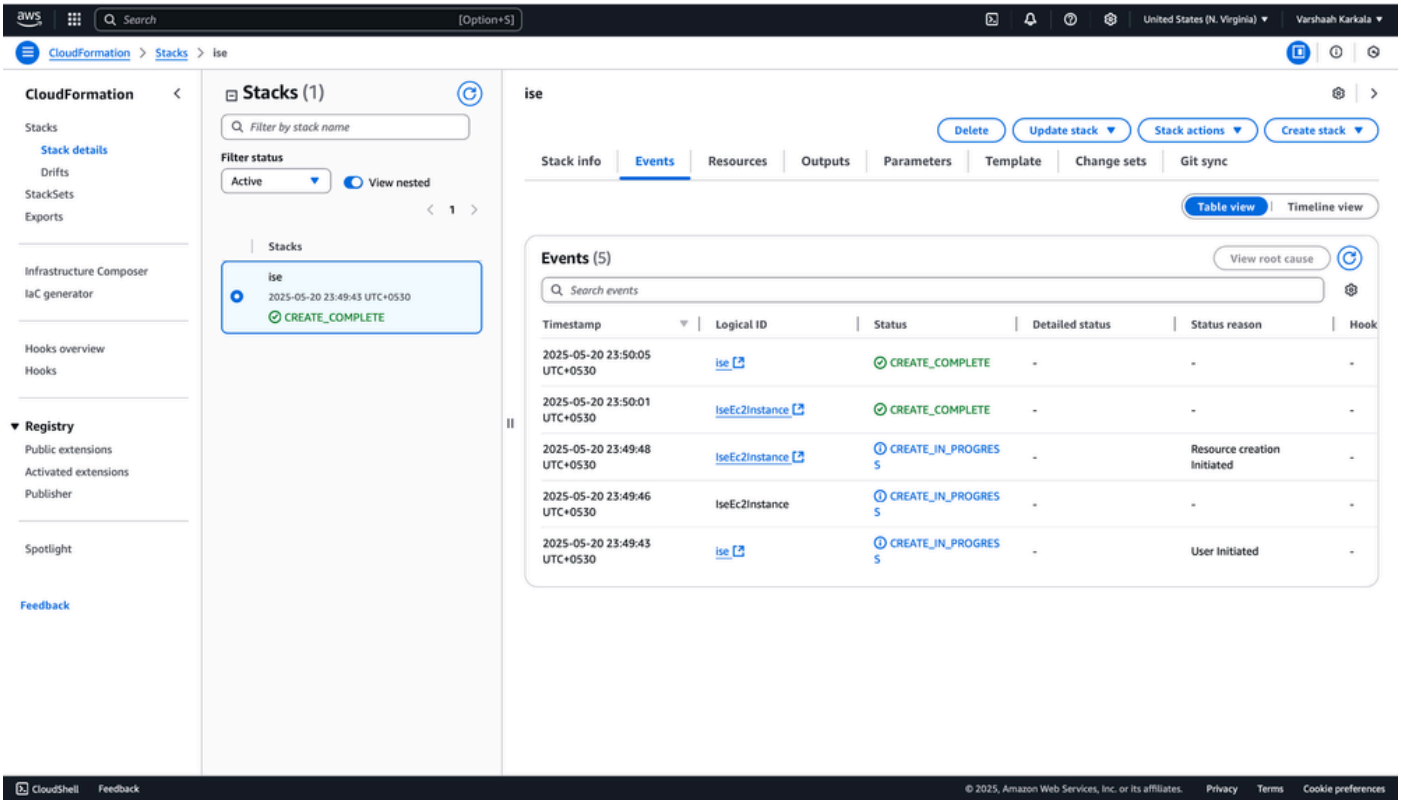
- 单击 Next。

11.配置堆栈选项：

- 保留所有默认选项，然后单击Next。



12.复查模板以确保所有配置均正确，然后单击Submit。模板构建完成后，其类似于以下示例：



13.访问堆栈详细信息：
导航到AWS管理控制台中的CloudFormation服务，然后转到Stacks部分。从列表中找到已部署的堆栈。

十四、“查看输出”选项卡:

选择堆栈并打开输出选项卡。在这里，您可以找到在部署过程中生成的重要信息，例如：

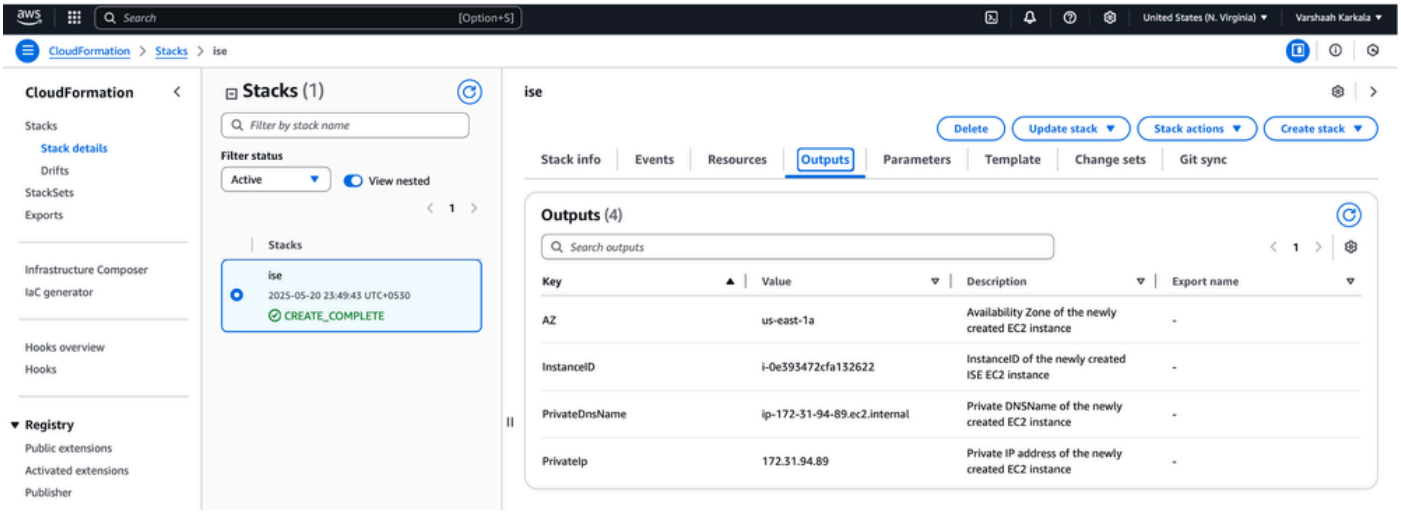
·可用区:部署资源的区域。

•实例 Id:已部署实例的唯一标识符。

· DNS名称:实例的专用DNS名称，可用于远程访问。

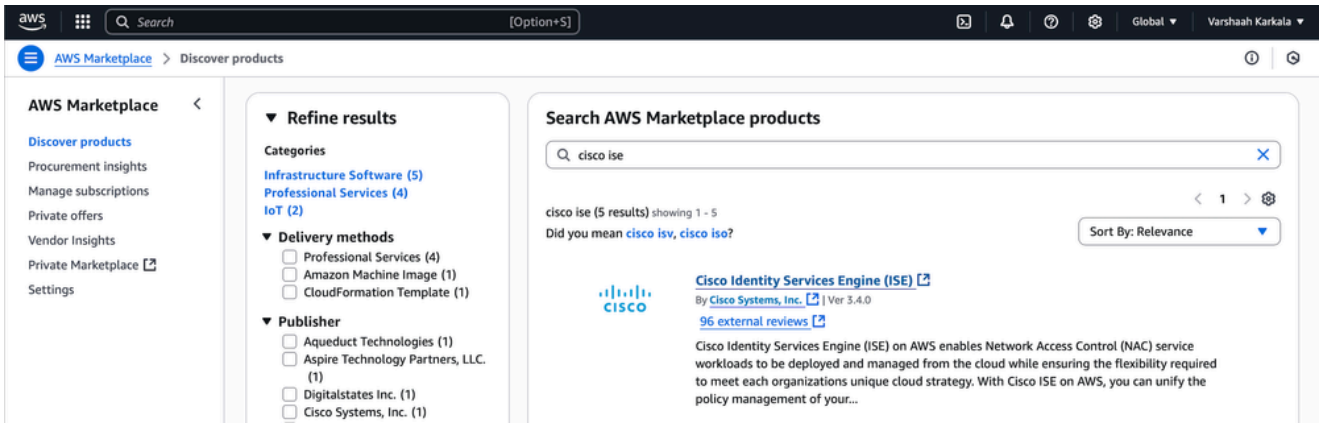
•IP 地址：实例的公有IP地址或私有IP地址，具体取决于您的配置。

此信息可帮助您连接到实例并验证其可用性。“输出”选项卡与以下示例类似：



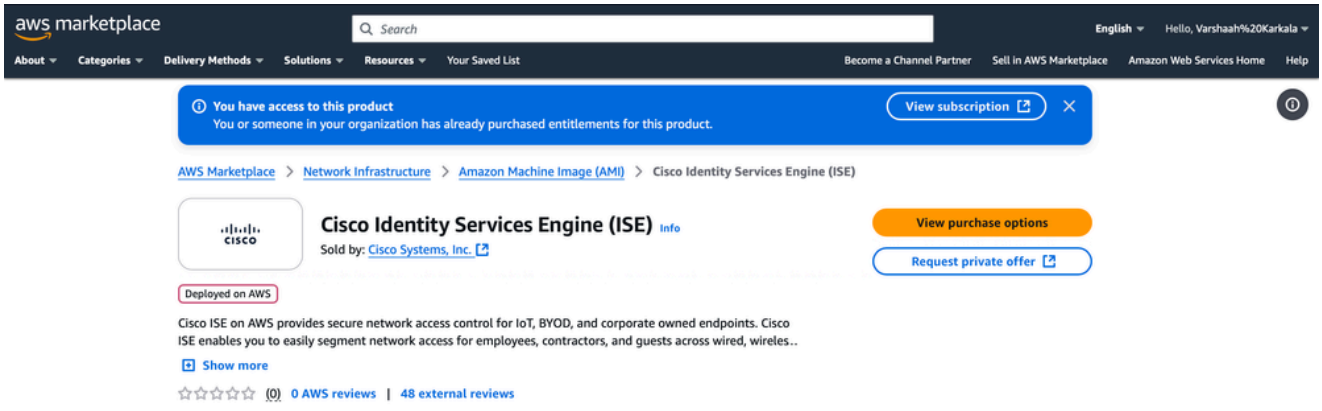
第 3 部分：使用Amazon机器映像(AMI)配置ISE

1. 登录AWS Management Console并搜索AWS Marketplace订用。
2. 在搜索栏中，键入cisco ise，然后从结果中选择Cisco Identity Services Engine(ISE)。

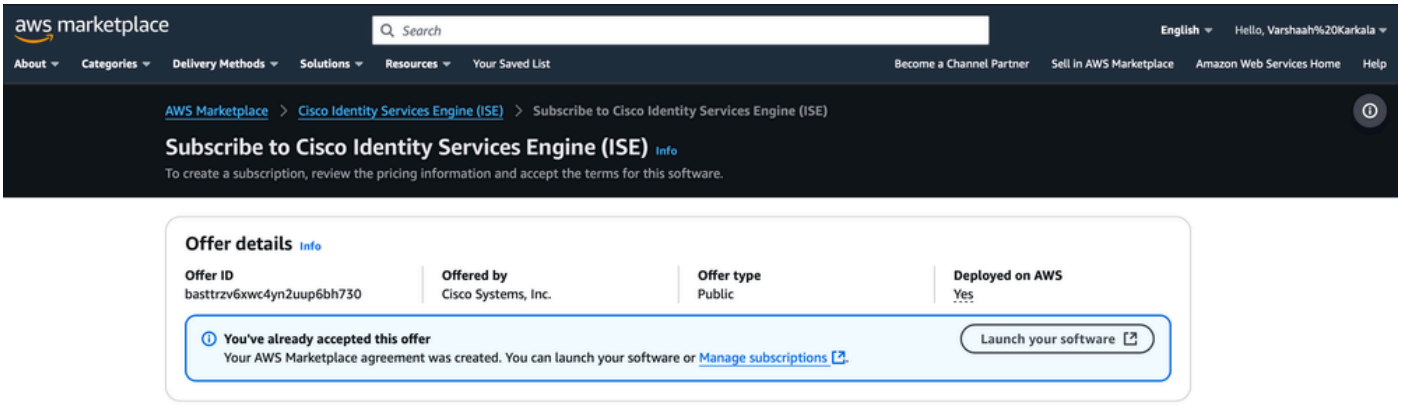


AWS Marketplace上的ISE

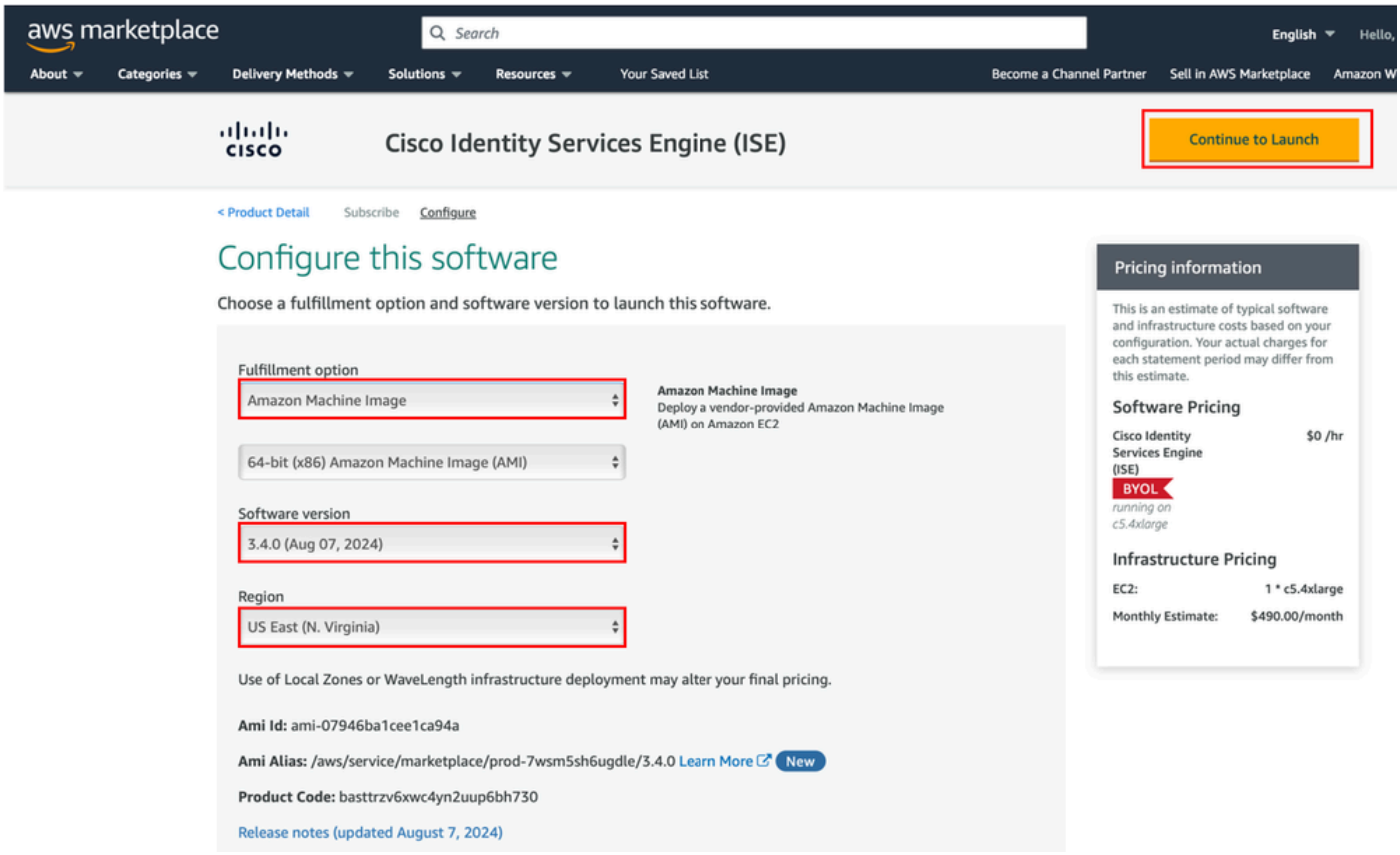
3. 单击View purchase options。



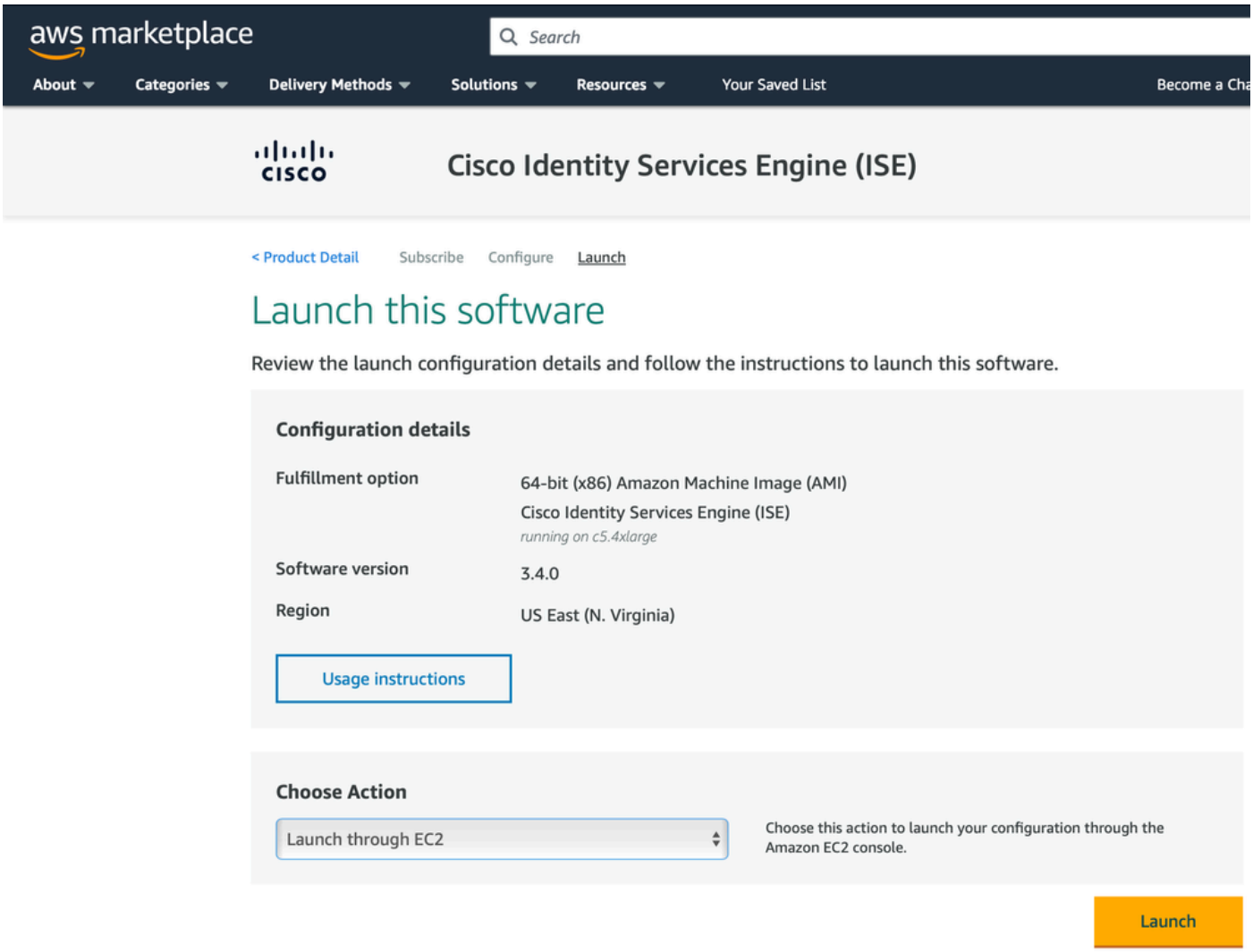
4.单击启动软件。



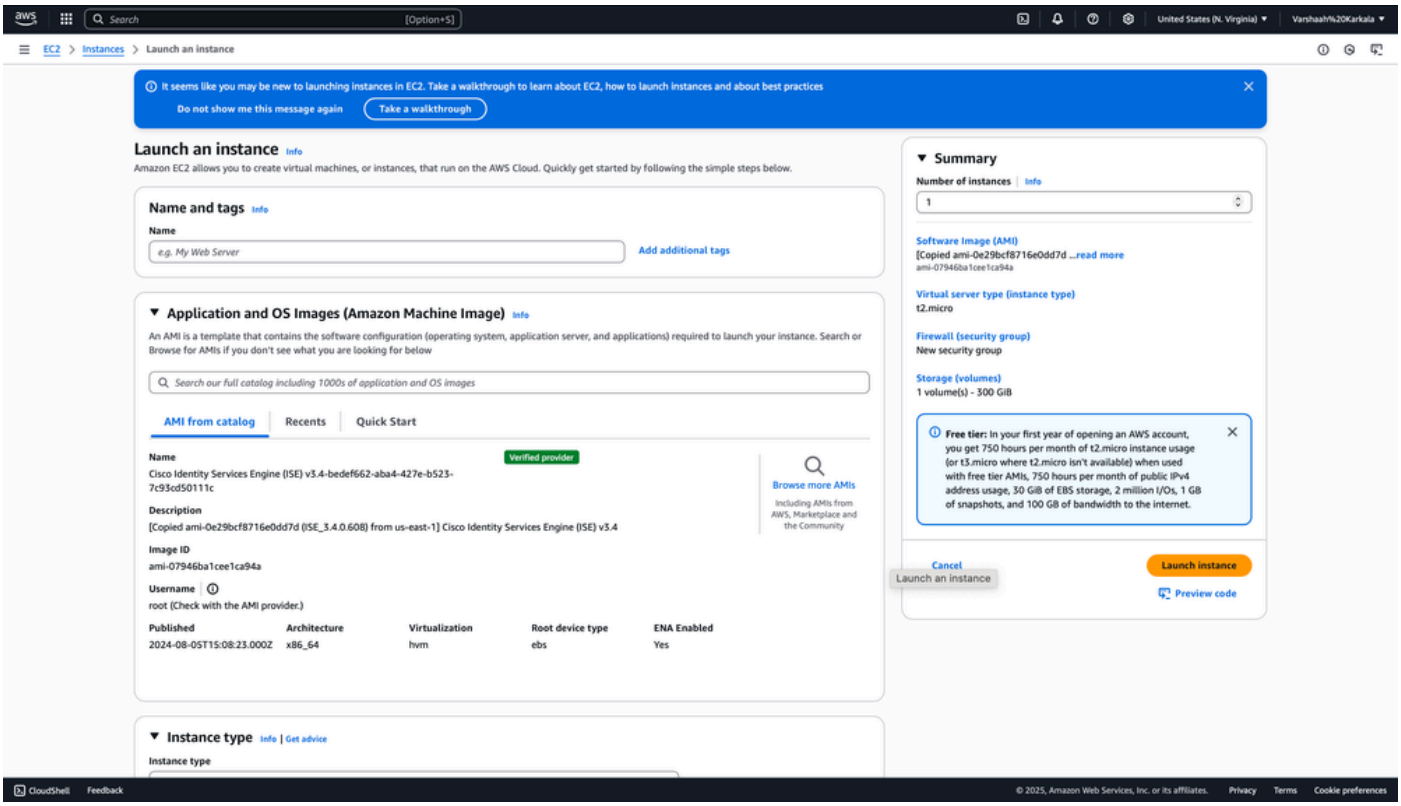
5.在“实施选项”下，选择Amazon Machine Image。选择所需的软件版本和AWS区域，然后单击Continue to Launch。



6.在Choose Action下拉列表中，选择Launch through EC2，然后单击Launch继续。



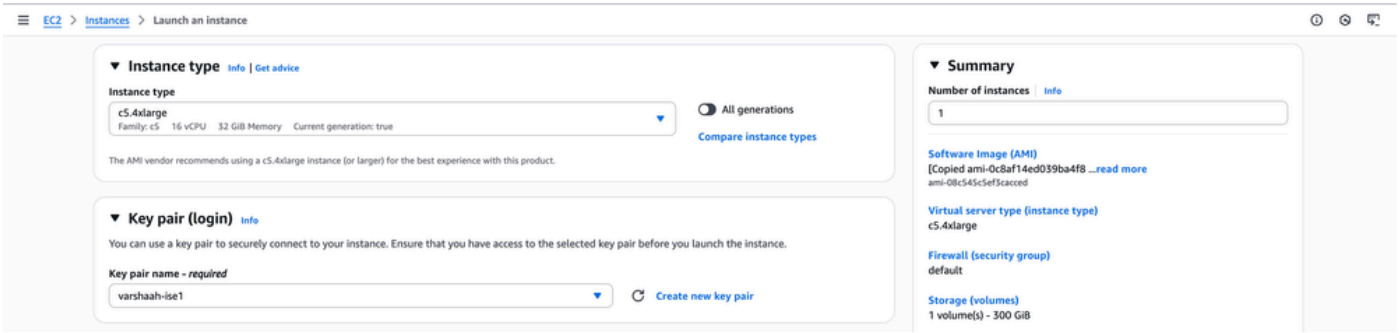
7. 您将被重定向到EC2启动实例页面以配置您的实例设置。



8.向下滚动到实例类型部分，并根据您的部署要求选择适当的实例类型。

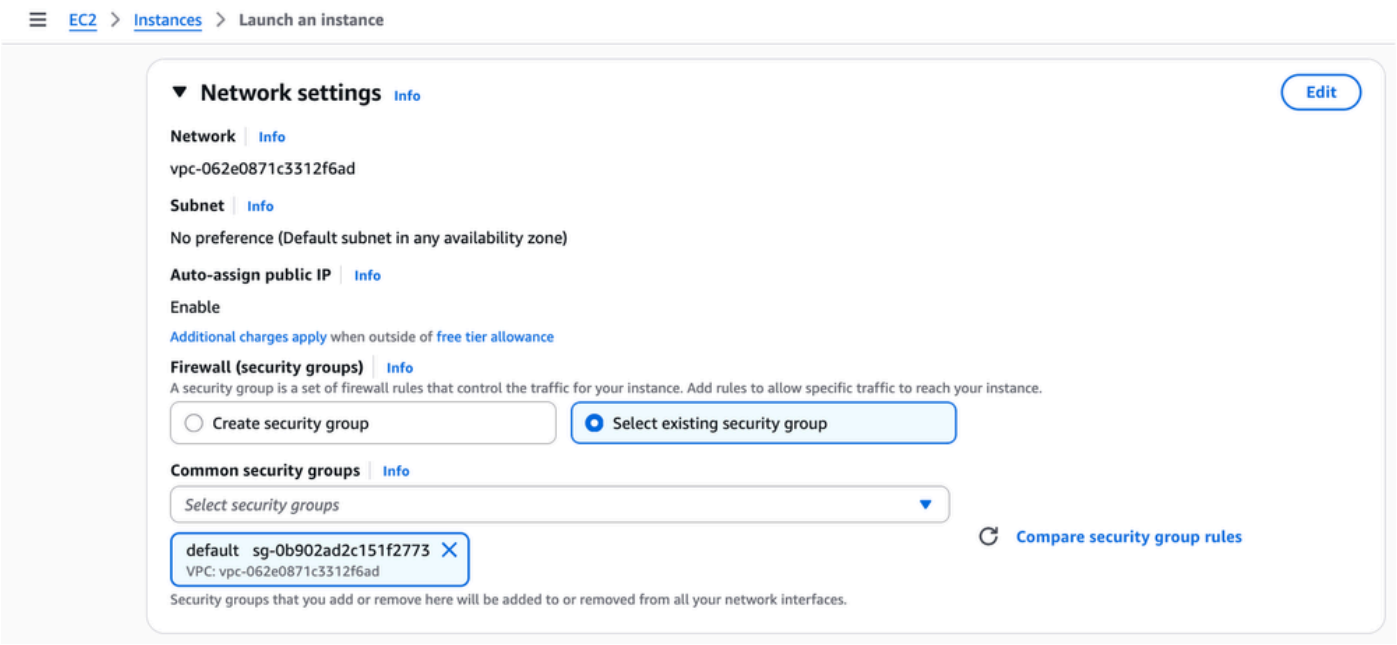
在密钥对（登录）下，选择之前生成的密钥对或创建一个新的密钥对（请参阅前面提供的密钥对创建步骤）。

将Number of Instances设置为1。



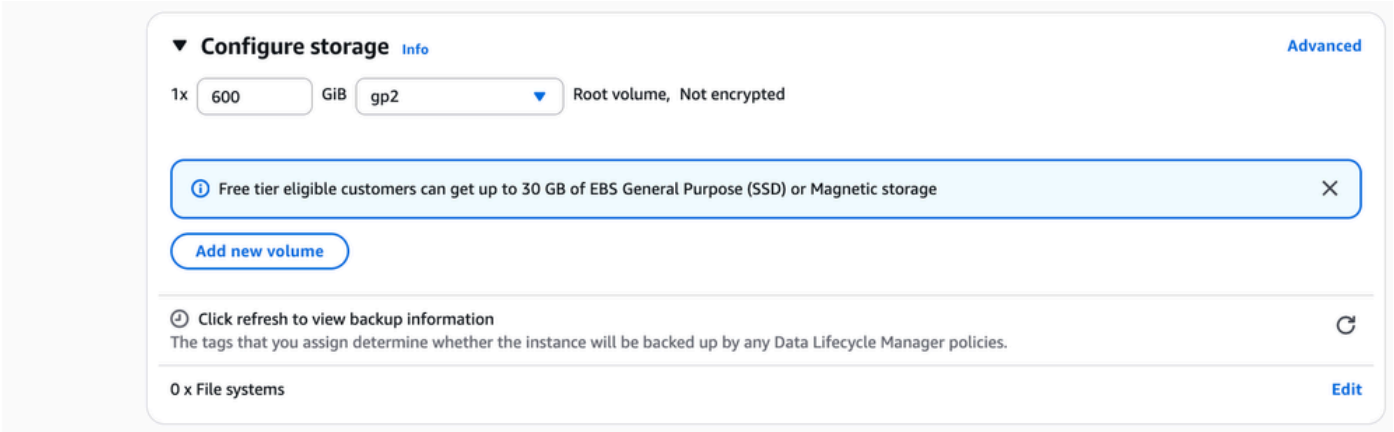
9.在网络设置部分：

- 根据需要配置VPC和子网。
- 对于Security Group，请选择现有组或创建新组（如示例所示）。



10.在配置存储部分，配置所需的卷大小。

示例：600 GiB，使用gp2卷类型。



11.在高级详细信息部分中，配置部署所需的任何其他设置，例如IAM实例配置文件、用户数据或关闭行为。

▼ **Advanced details** Info

Domain join directory | Info

Select ▼ Create new directory

IAM instance profile | Info

Select ▼ Create new IAM profile

Hostname type | Info

IP name ▼

DNS Hostname | Info

- Enable IP name IPv4 (A record) DNS requests
- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | Info

Default ▼

Shutdown behavior | Info

Stop ▼

Stop - Hibernate behavior | Info

Disable ▼

Termination protection | Info

Disable ▼

Stop protection | Info

Select ▼

Detailed CloudWatch monitoring | Info

Disable ▼

Credit specification | Info

Standard ▼

Placement group | Info

Select ▼ Create new placement group

EBS-optimized instance | Info

Disable ▼

Instance bandwidth configuration | Info

Default ▼

Purchasing option | Info

- (●) None
- ( ) Capacity Blocks
  Launch instances for your active capacity blocks
- ( ) Spot instances
  Request Spot Instances at the Spot price, capped at the On-Demand price

Capacity reservation | Info

None ▼

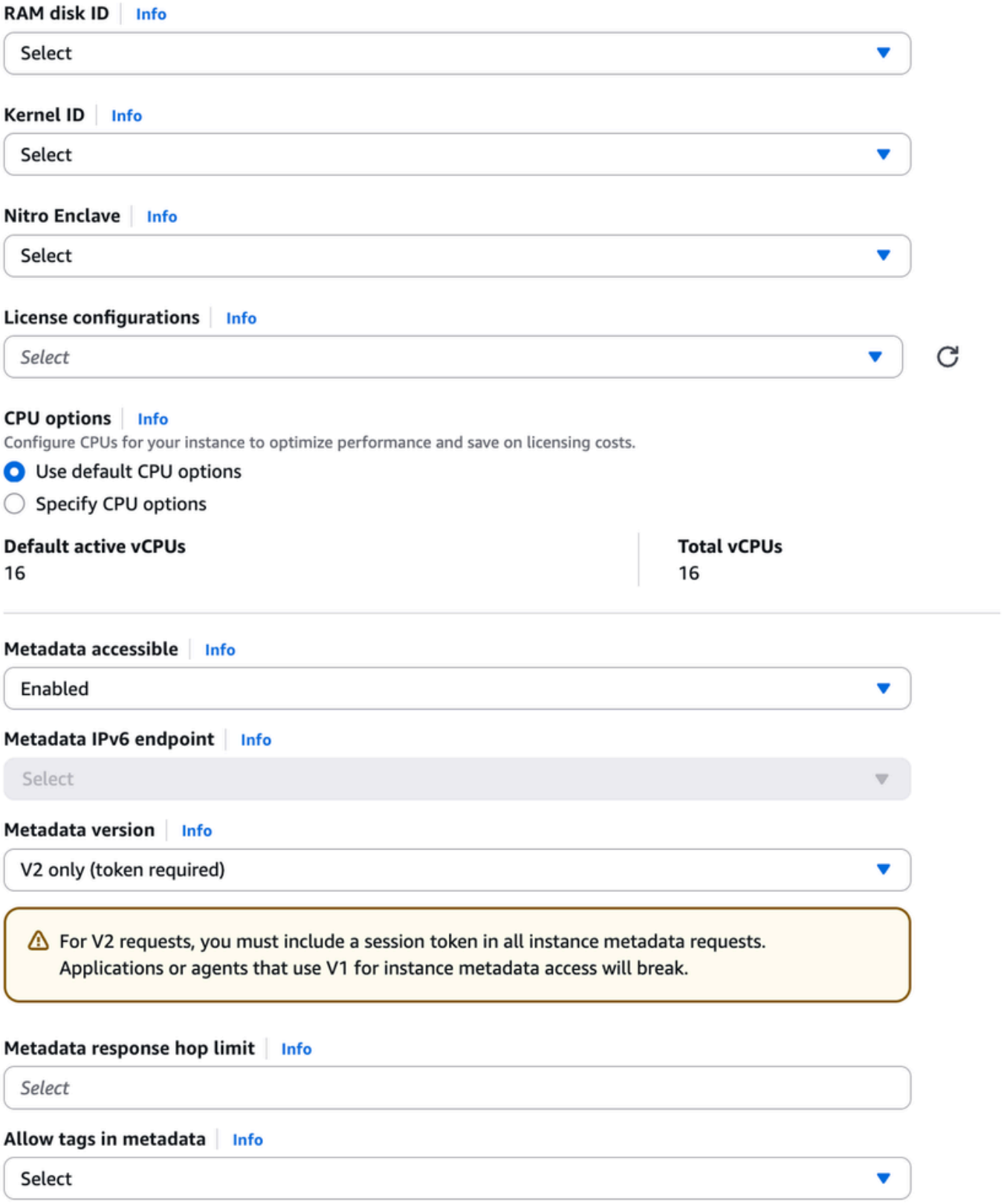
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12.在“元数据版本”部分：

- 对于ISE版本3.4及更高版本，请选择V2 only（需要令牌）— 这是推荐的选项。
- 对于低于3.4的ISE版本，请选择V1和V2（可选令牌）以确保兼容性。



13.在用户数据字段中，为ISE实例提供初始配置参数，包括主机名、DNS、NTP服务器、时区、ERS和管理员凭证。

示例：
hostname=varshaahise2

primarynameserver=x.x.x.x

dnsdomain=varshaah.local

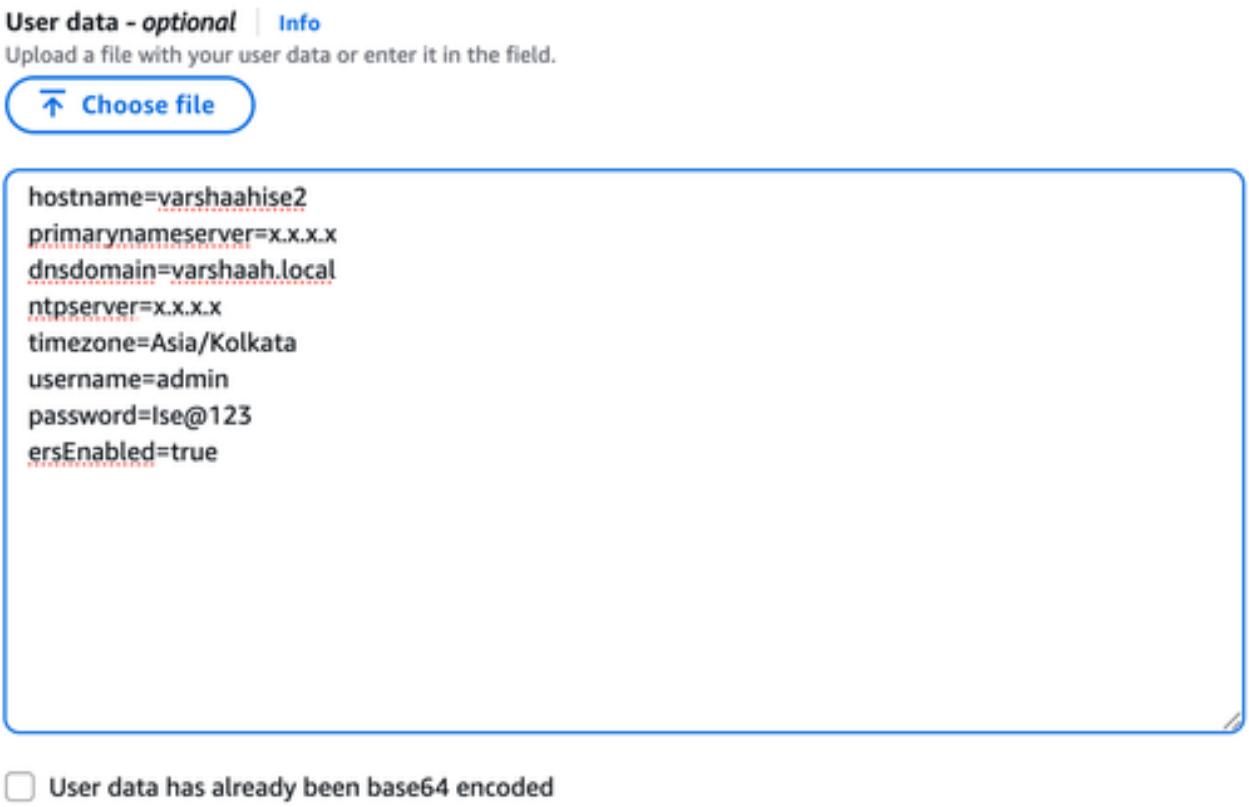
ntpserver=x.x.x.x

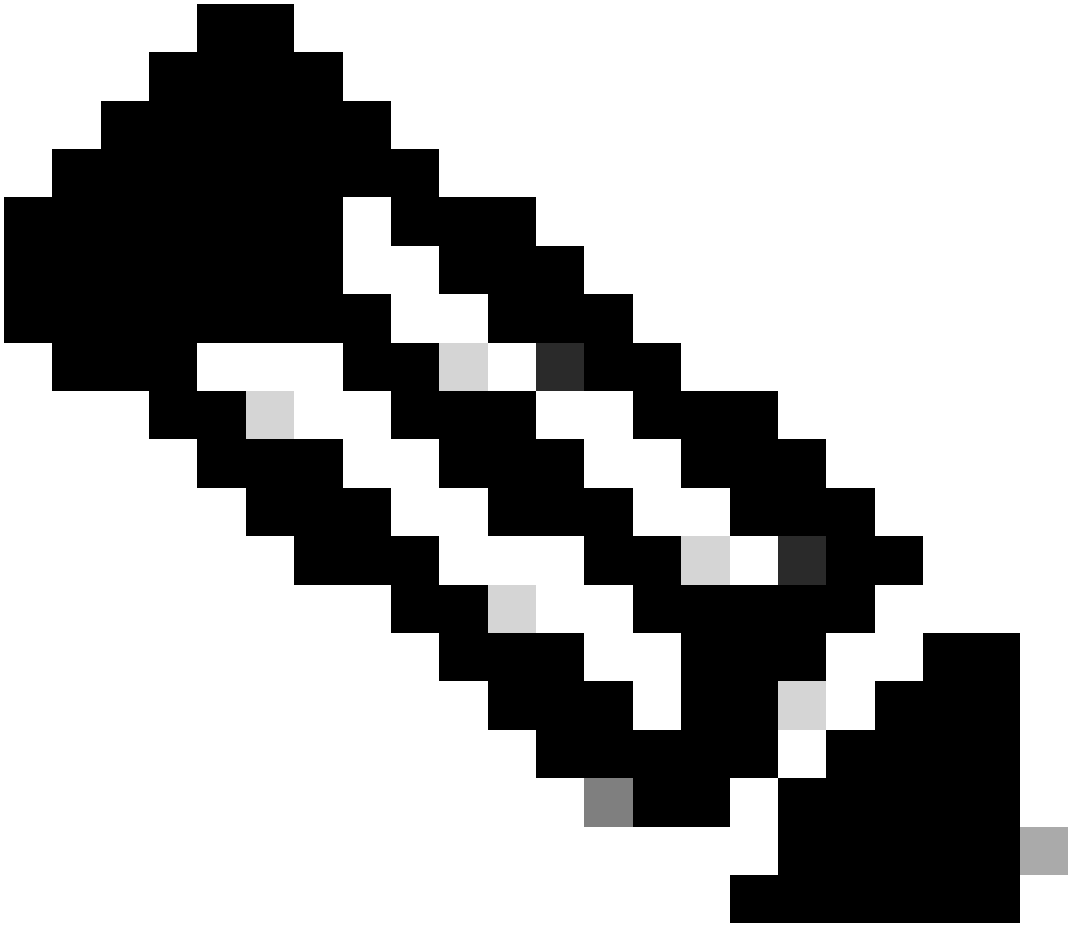
时区=亚洲/加尔各答

username=admin

password=Ise@123

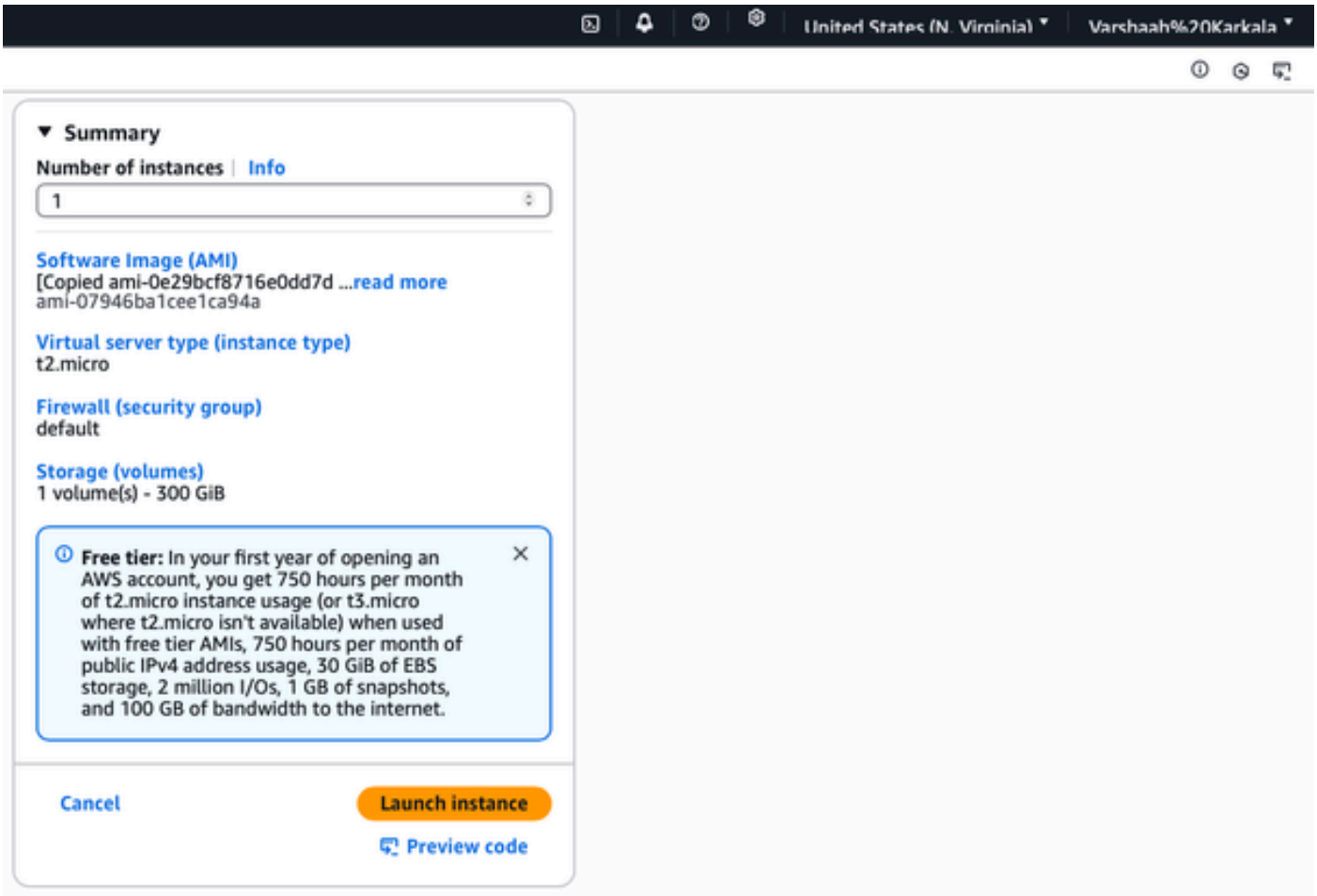
ersEnabled=true



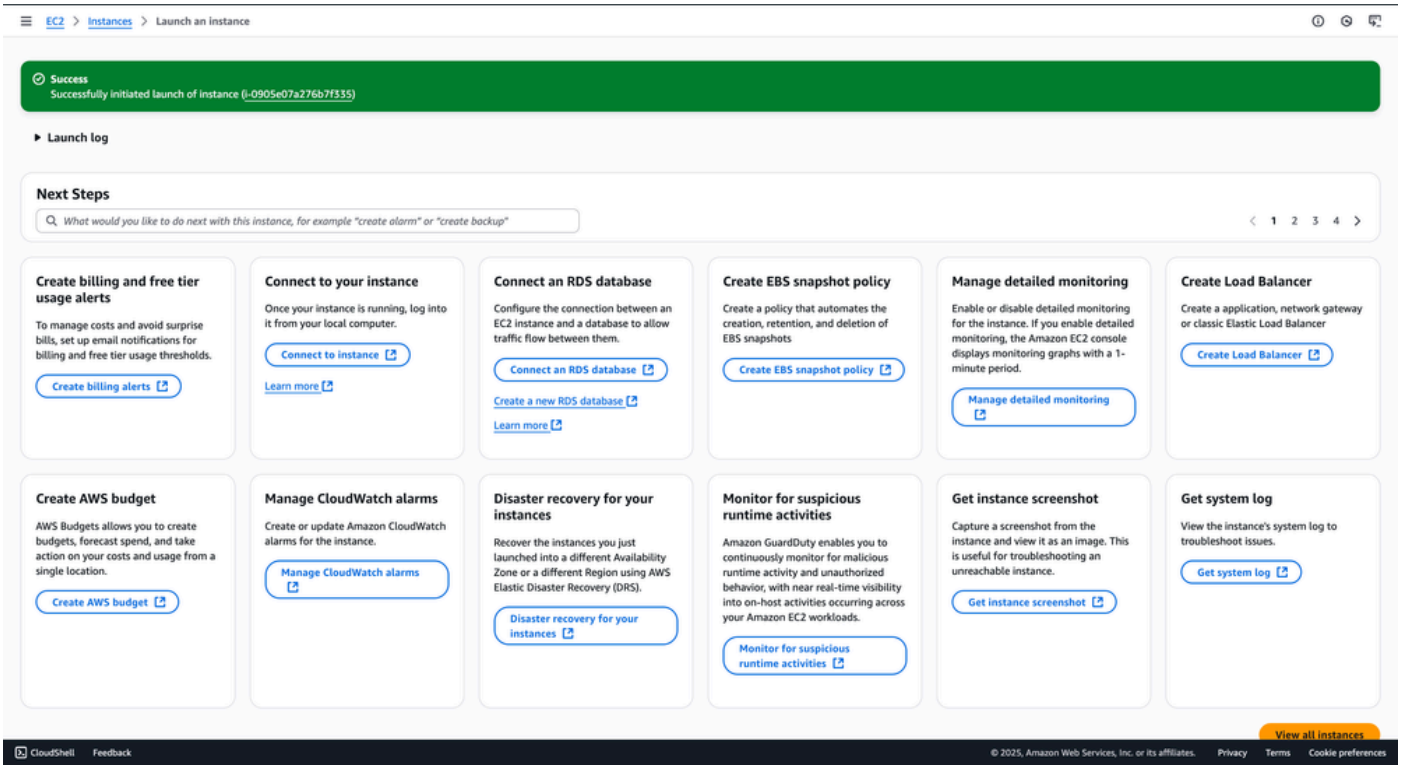


注意：确保密码符合思科ISE密码策略。

输入用户数据并完成配置后，点击启动实例。



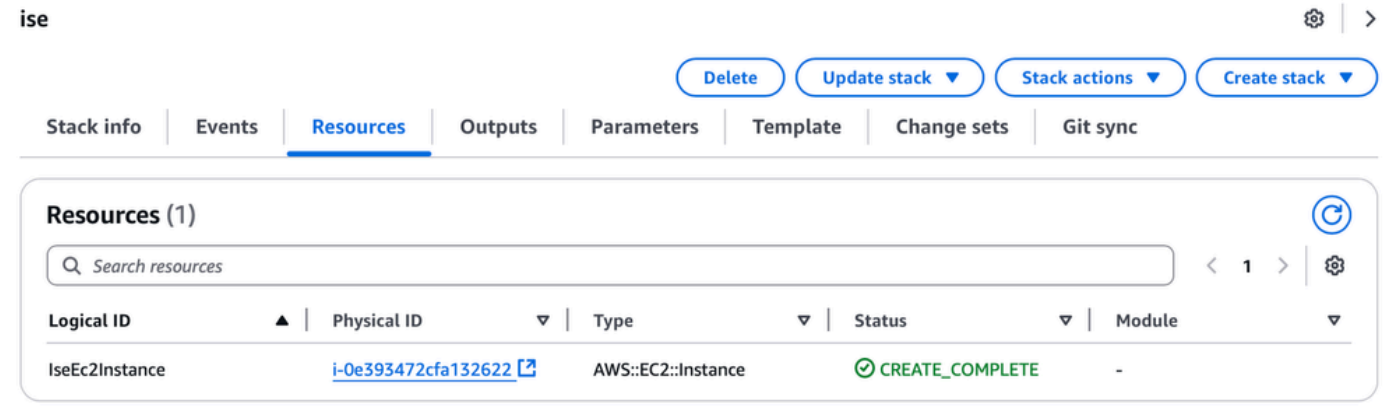
14.启动实例后，系统会显示确认消息，说明：'已成功启动实例<instance_name>'。 这表示启动过程已成功启动。

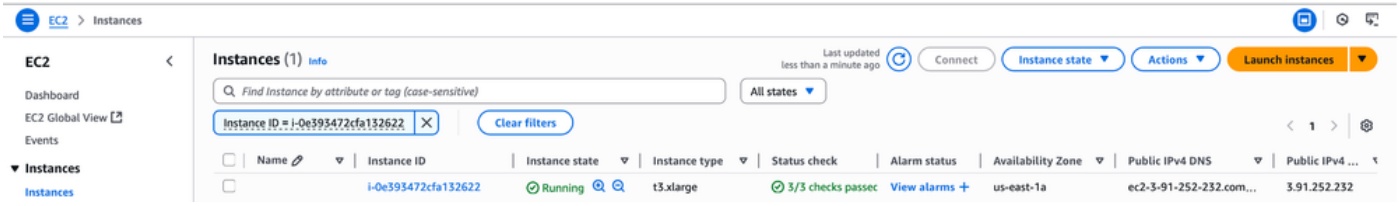


验证

访问使用CFT构建的ISE实例

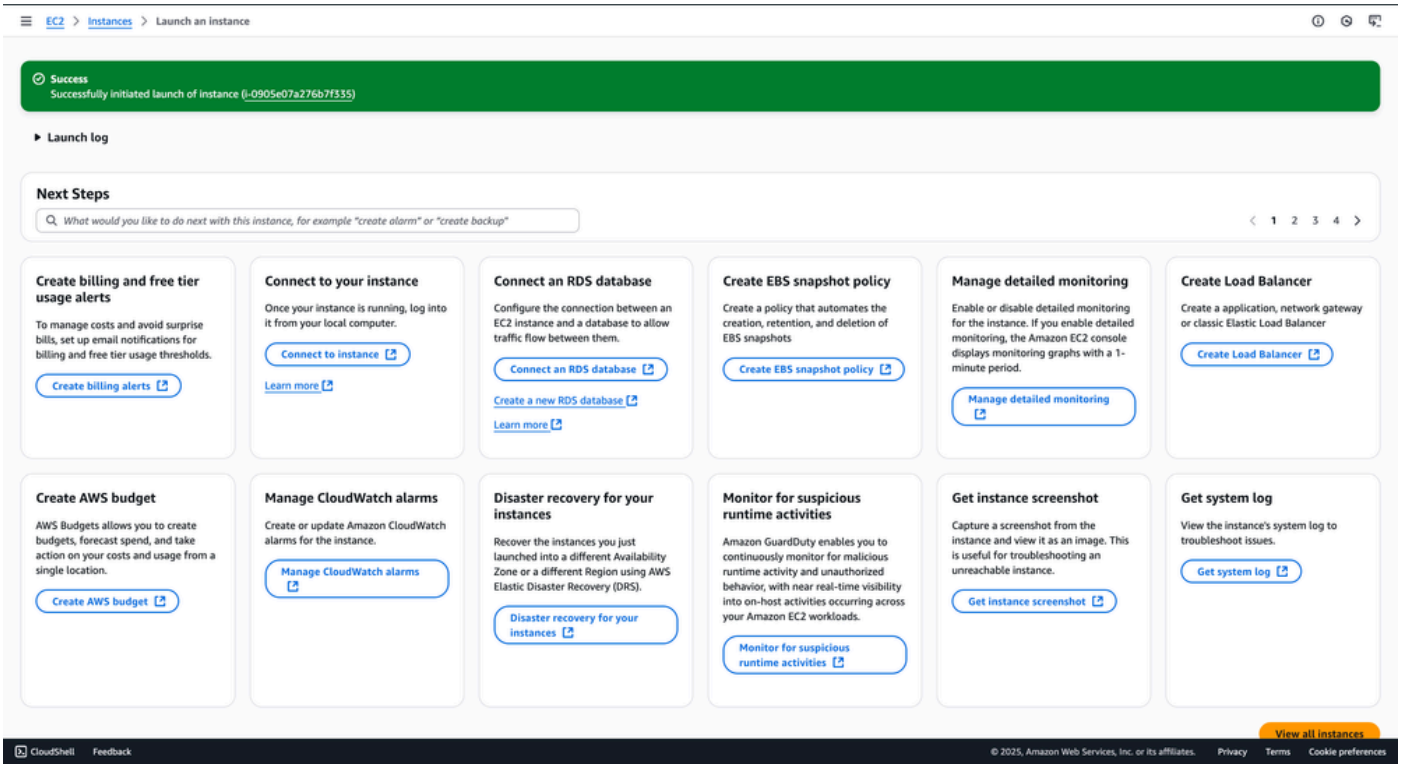
转至CloudFormation堆栈中的Resources选项卡，然后单击Physical ID。它将您重定向到EC2控制面板，您可以在其中看到实例。

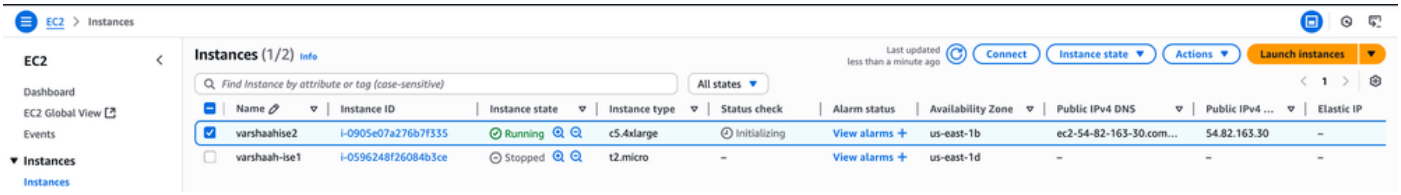




访问使用AMI构建的ISE实例

单击查看所有实例可导航到EC2实例页。在此页上，验证状态检查显示为3/3检查通过，表明实例运行正常且运行正常。





访问ISE GUI

ISE服务器现在已成功部署。

要访问ISE GUI，需要在浏览器中使用实例的IP地址。由于默认IP是专用的，因此不能直接从Internet访问。

检查公共IP是否与实例相关联：

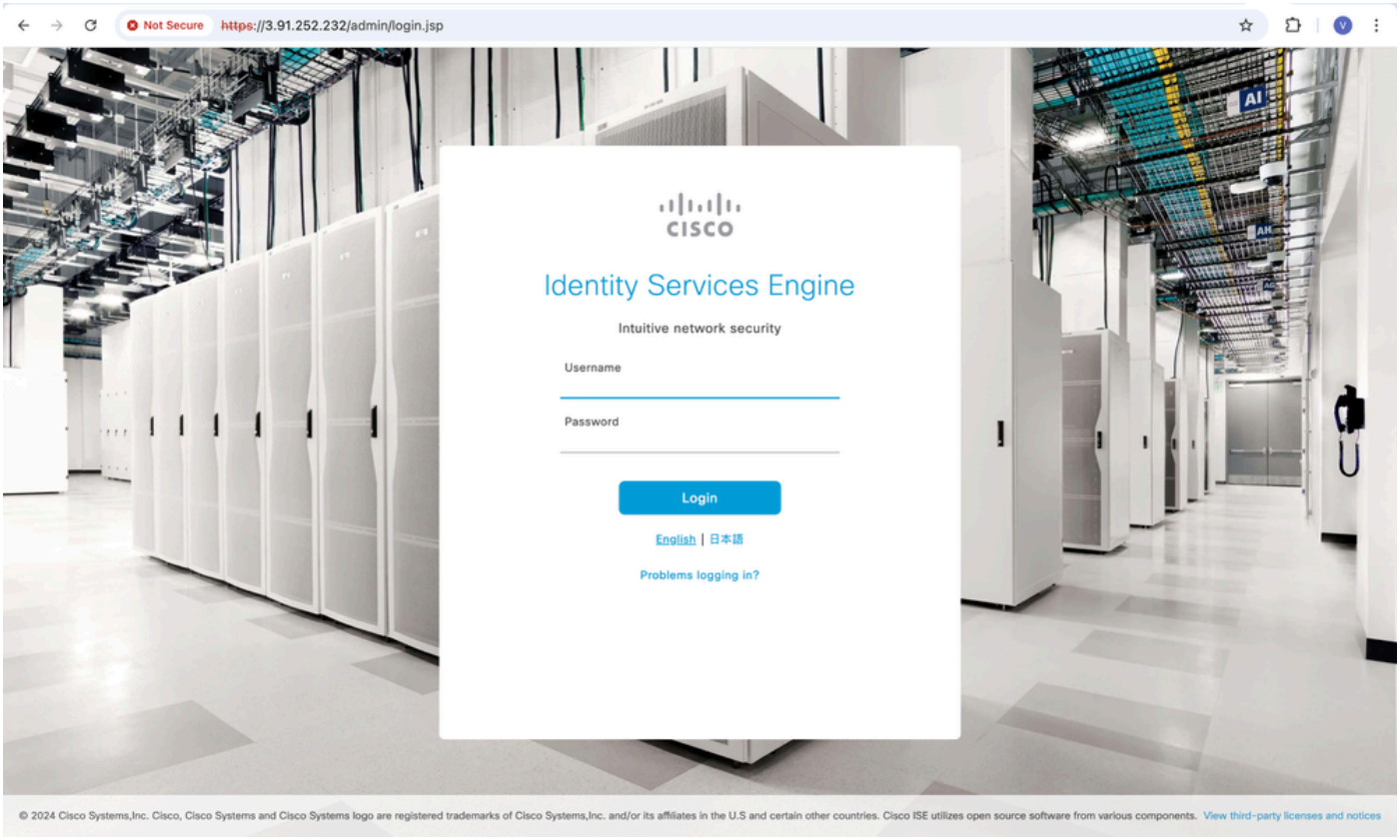
- 导航到EC2 > Instances，然后选择您的实例。
- 查找Public IPv4 address字段。

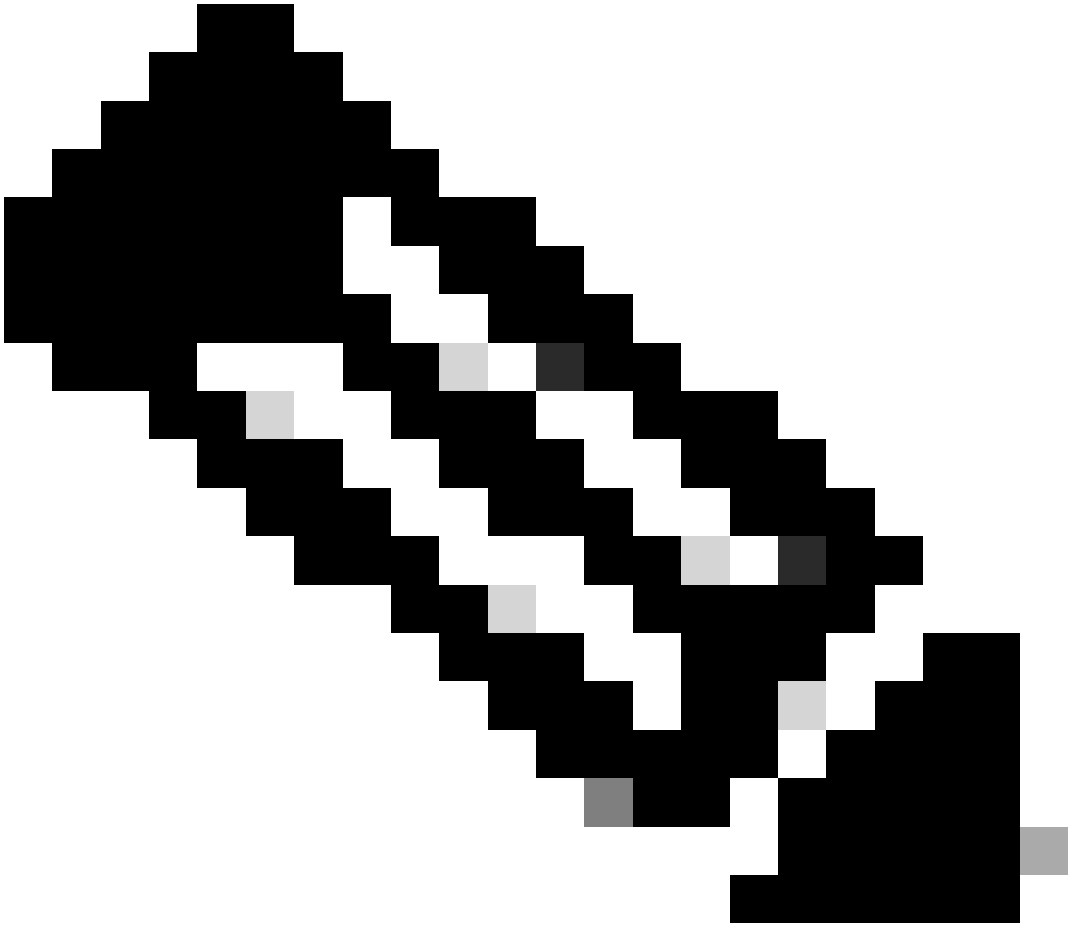
在这里，我们可以看到一个可用于访问ISE GUI的公共IP地址。



打开受支持的浏览器（例如Chrome或Firefox），然后输入公共IP地址。

系统将显示ISE GUI登录页面。





注意：SSH访问可用后，ISE服务通常需要10-15分钟才能完全转换到运行状态。

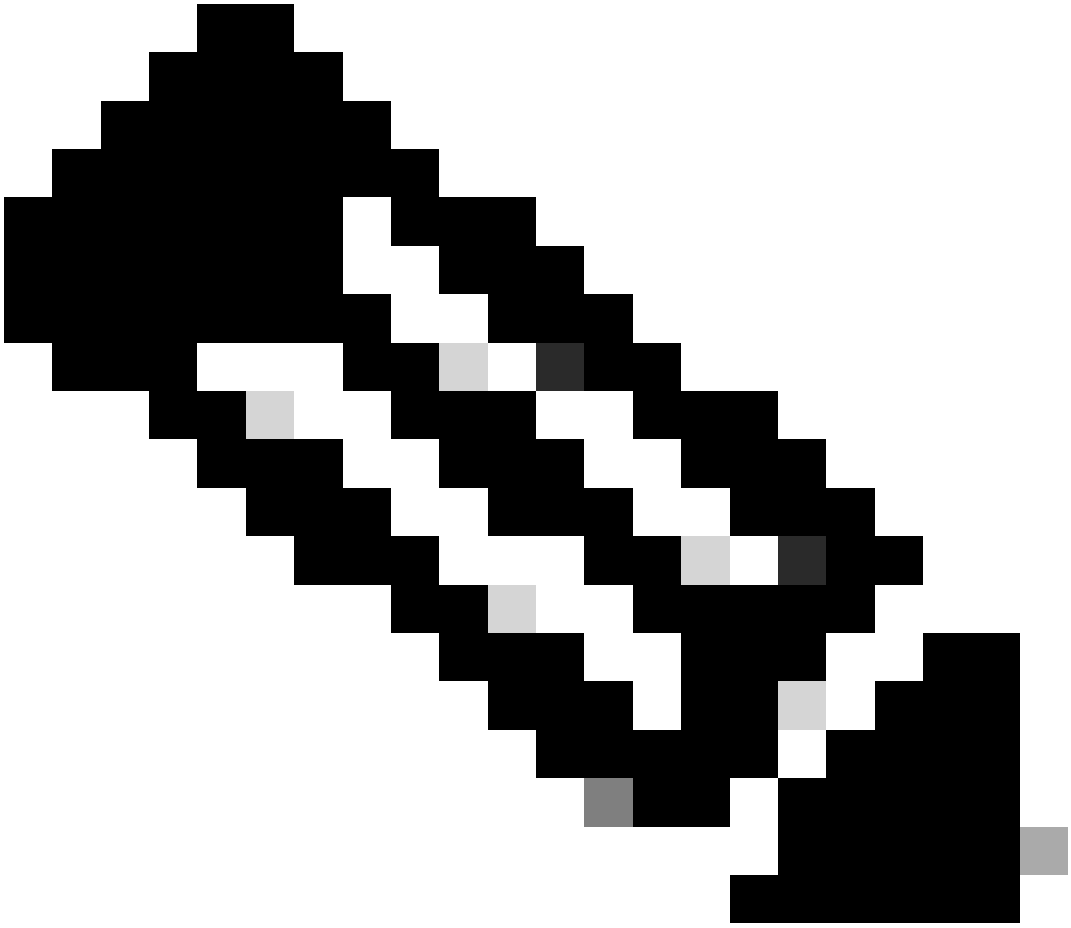
从终端通过SSH访问CLI

在EC2控制台中，选择您的实例，然后单击Connect。

在SSH客户端选项卡下，请执行以下步骤：

- 导航到包含已下载的.pem密钥文件的文件夹。
- 运行以下命令：

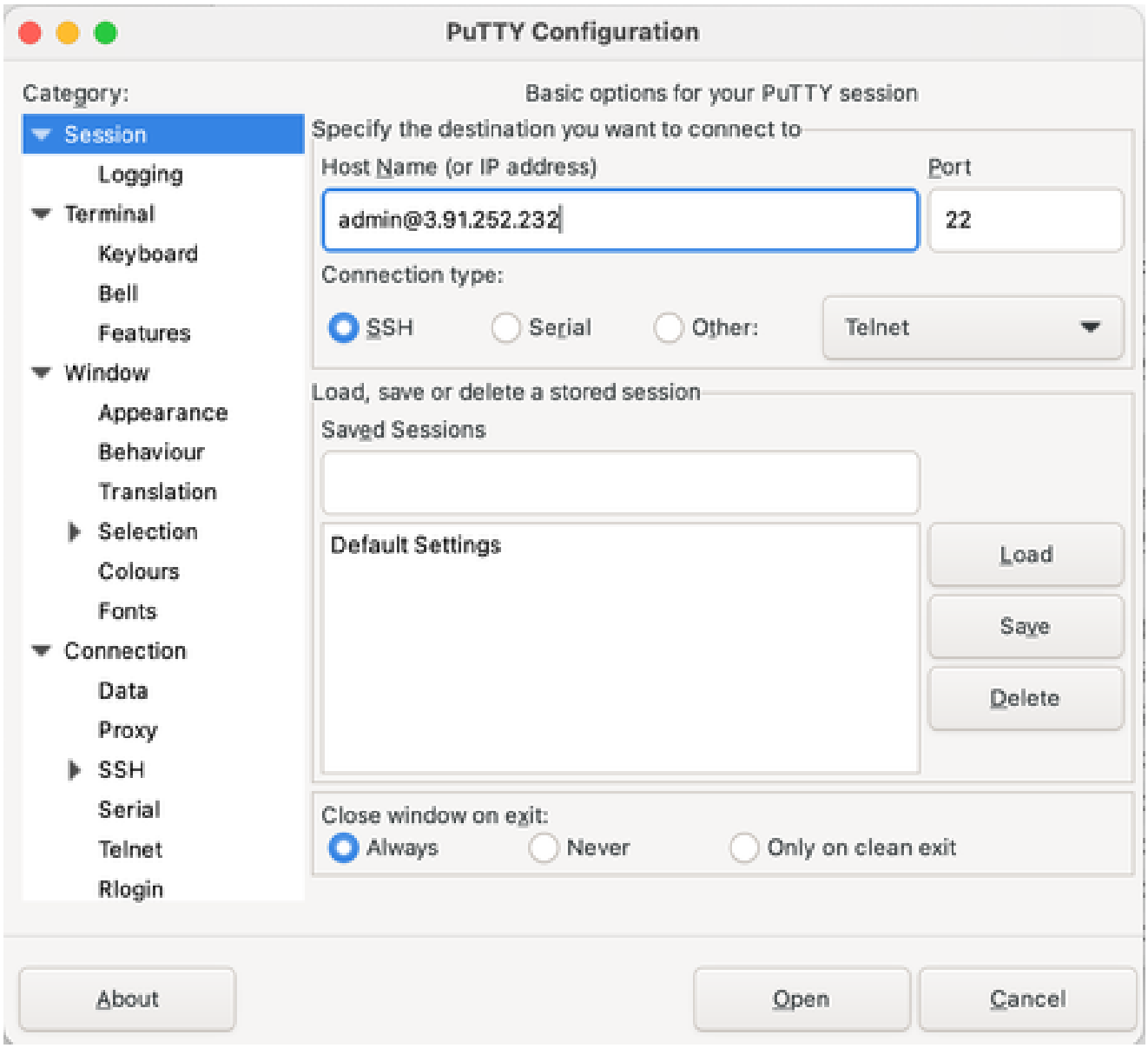
- cd <路径到密钥文件>
- chmod 400 <您的密钥对名称>.pem
- ssh -i "<your-key-pair-name>.pem" admin@<public-ip-address>



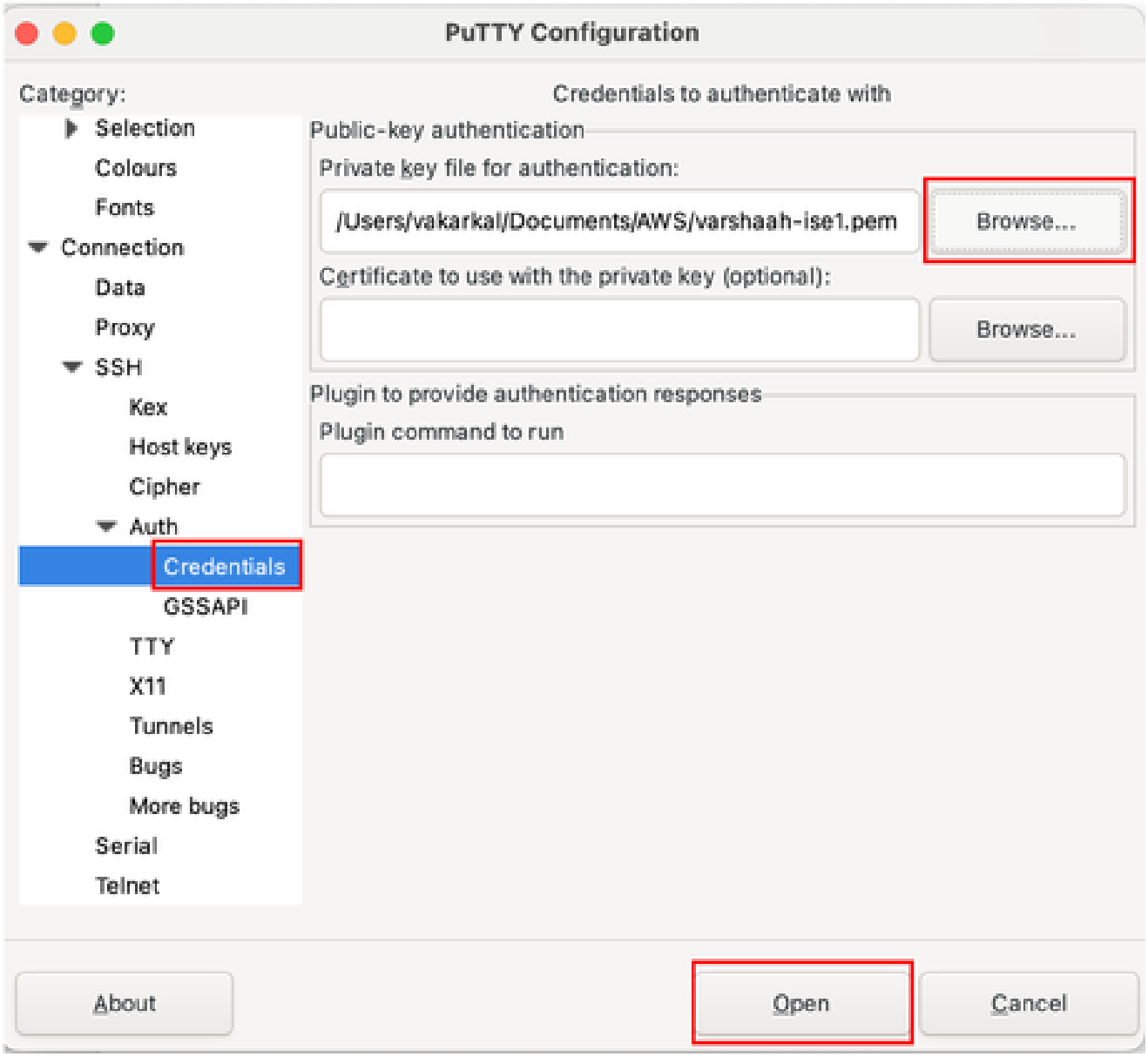
注意：使用admin作为SSH用户，因为思科ISE通过SSH禁用根登录。

使用PuTy通过SSH访问CLI

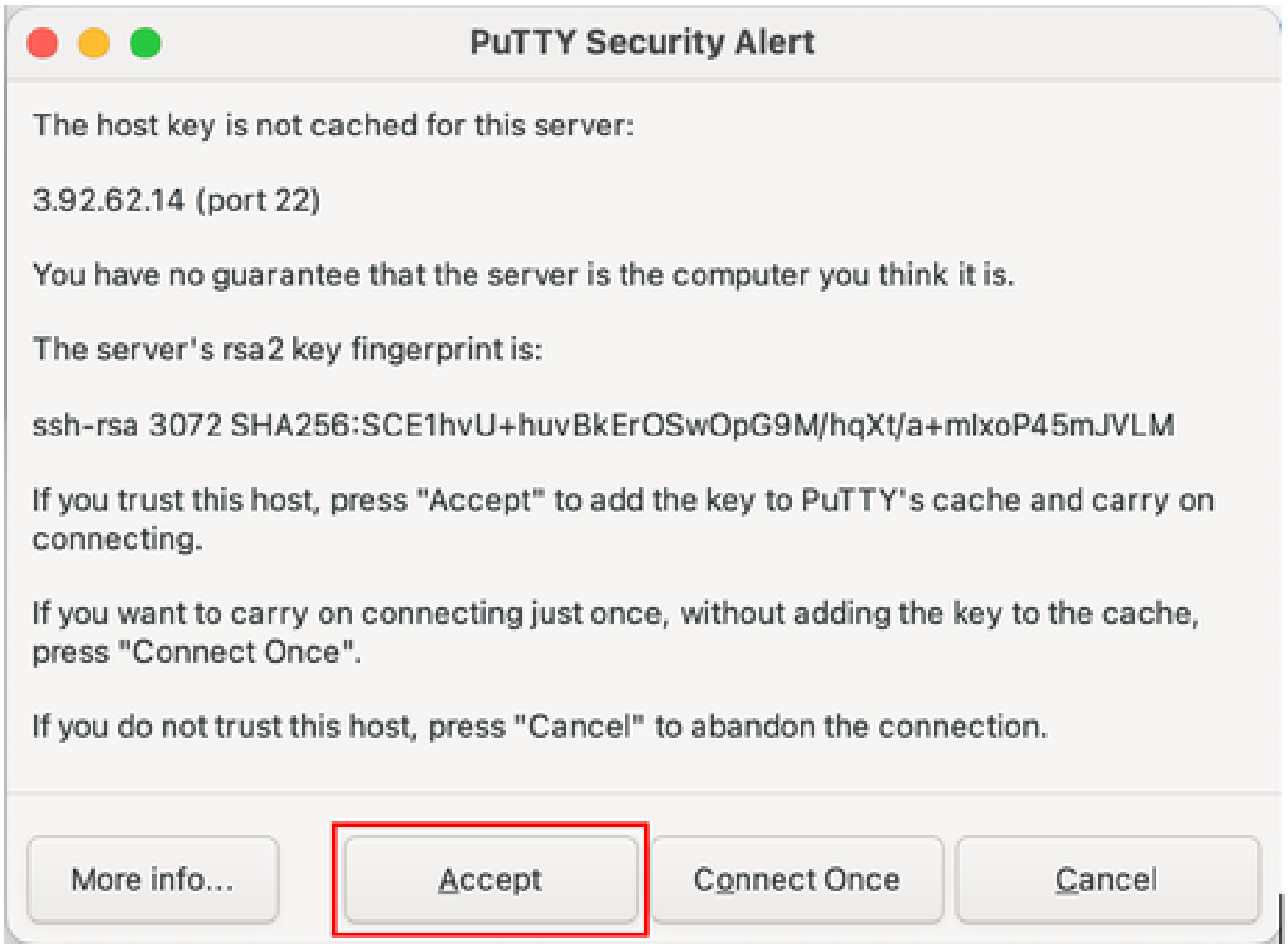
- 打开PuTTY。
- 在Host Name字段中，输入：admin@<public-ip-address>



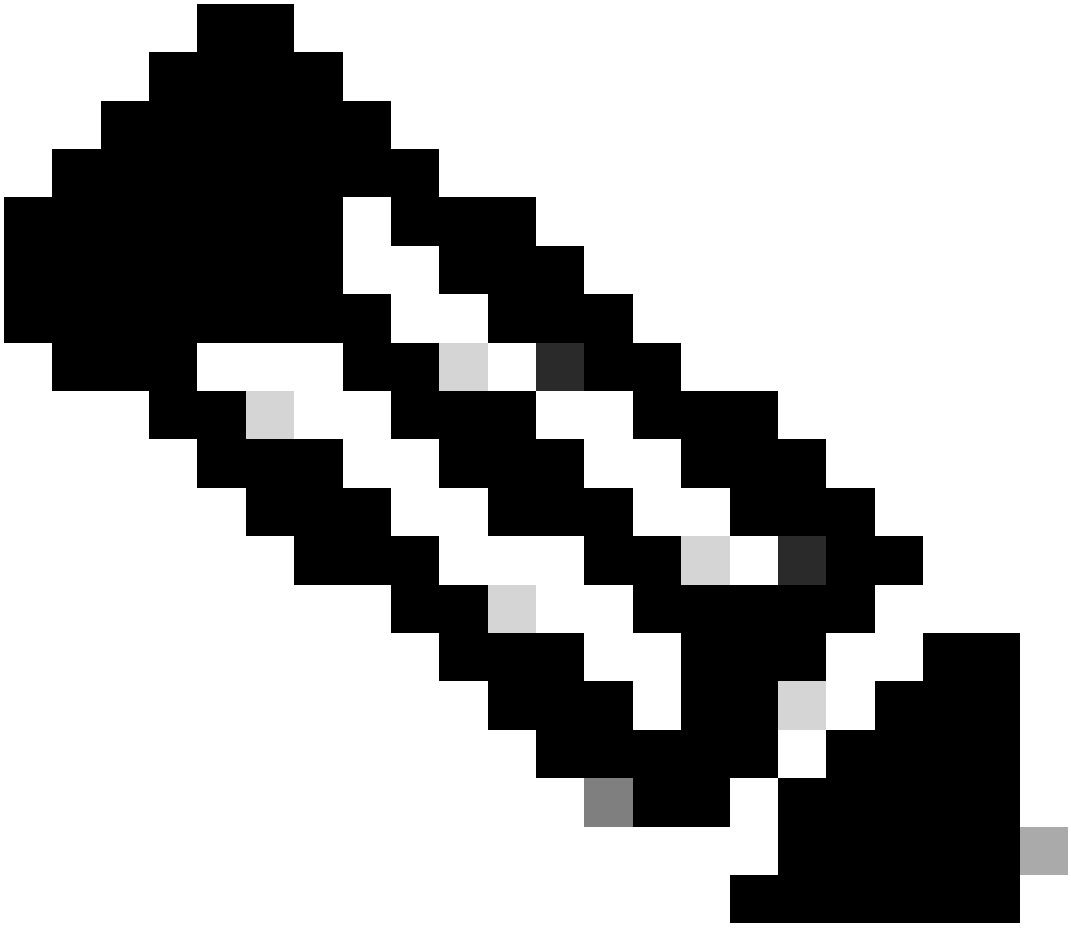
- 在左侧窗格中，导航到连接> SSH >身份验证>凭证。
- 点击Private key file for authentication旁边的Browse，然后选择您的SSH私钥文件。
- 单击Open启动会话。



- 出现提示时，单击Accept确认SSH密钥。



- 您的PuTTY会话现在连接到ISE CLI。

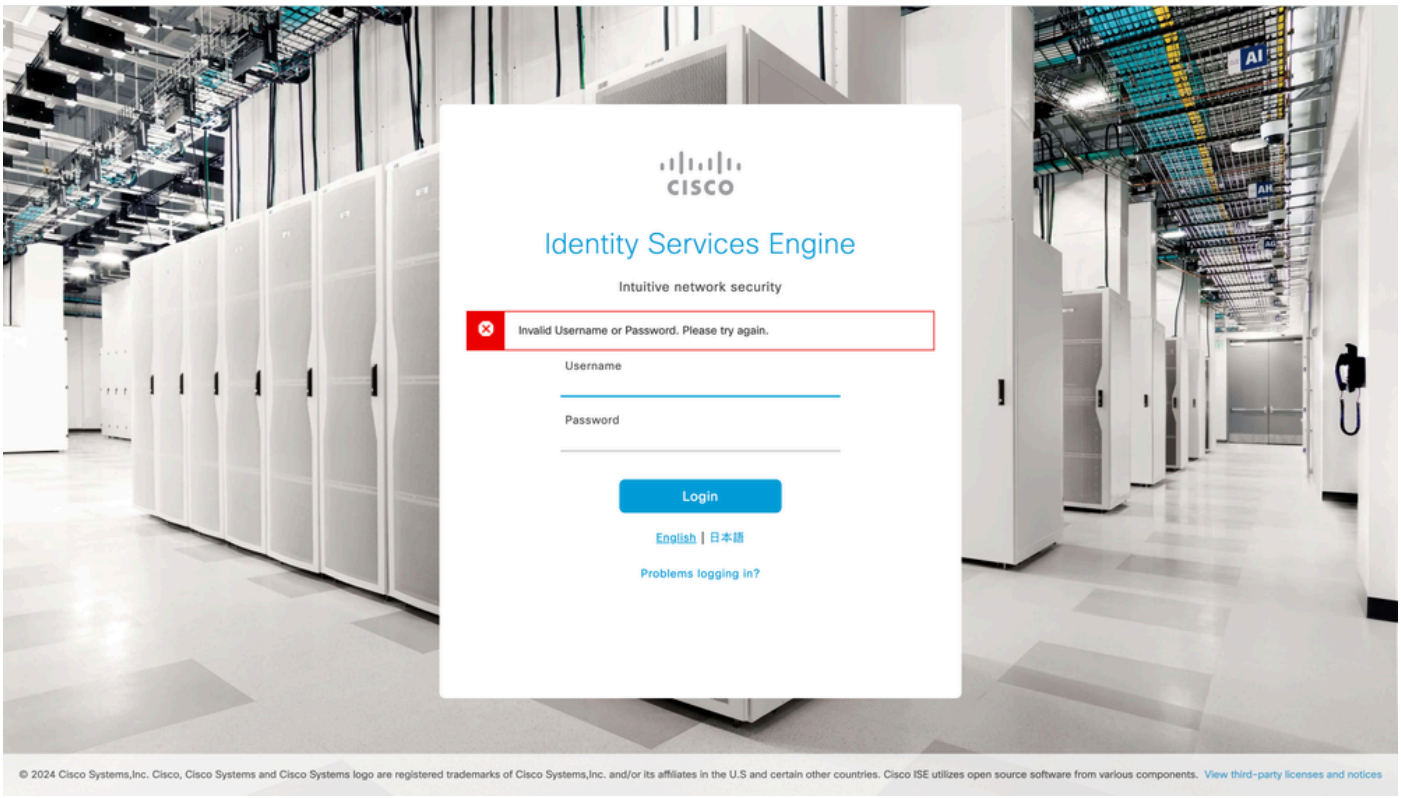


注意：通过SSH访问ISE可能需要20分钟。在此期间，连接尝试可能会失败，错误如下：“权限被拒绝(publickey)。”

故障排除

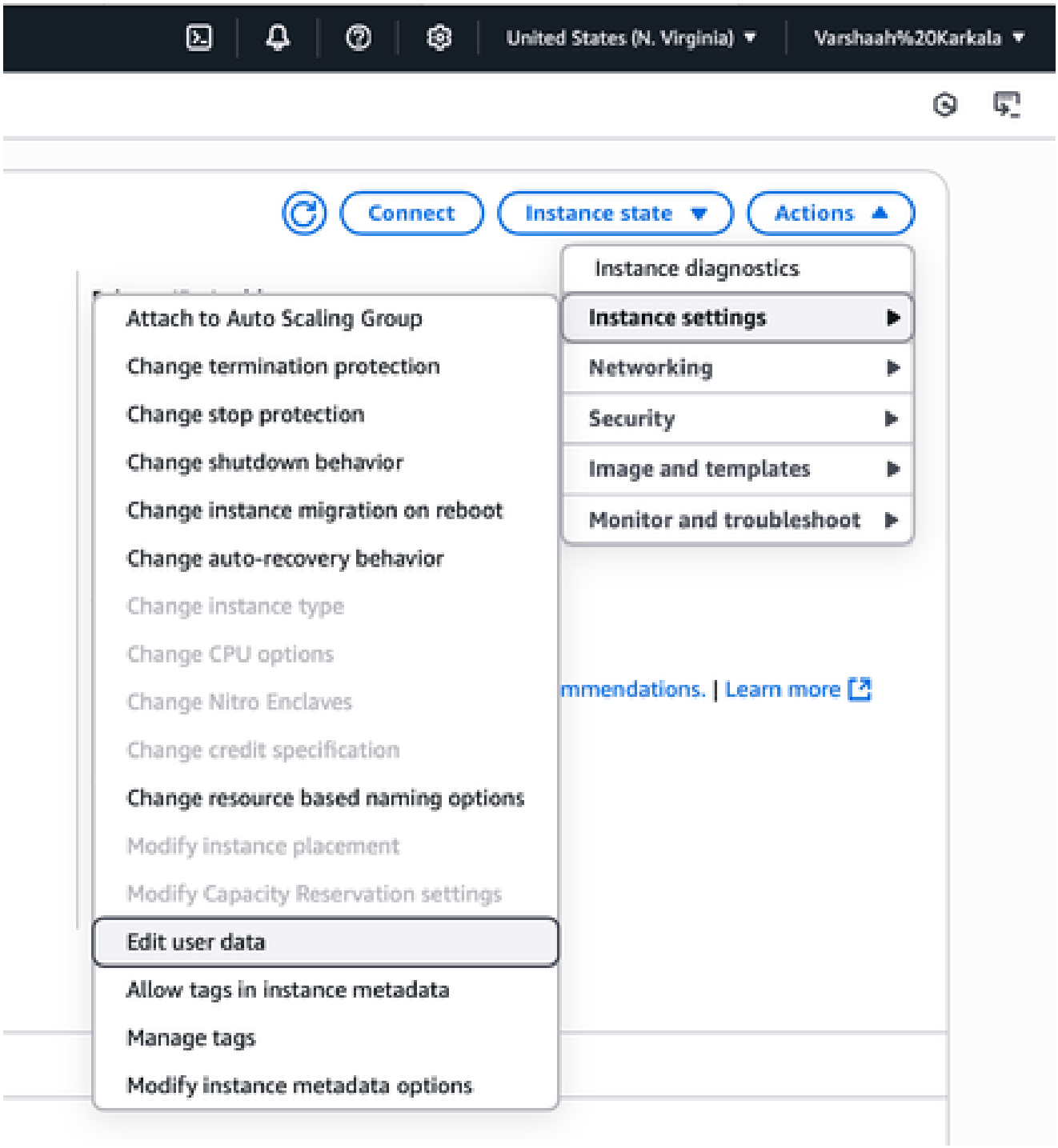
用户名或密码无效

身份验证问题通常是由实例创建期间不正确的用户输入引起的。这会产生错误信息“用户名或密码无效”。请重试。 尝试登录到GUI时出错。

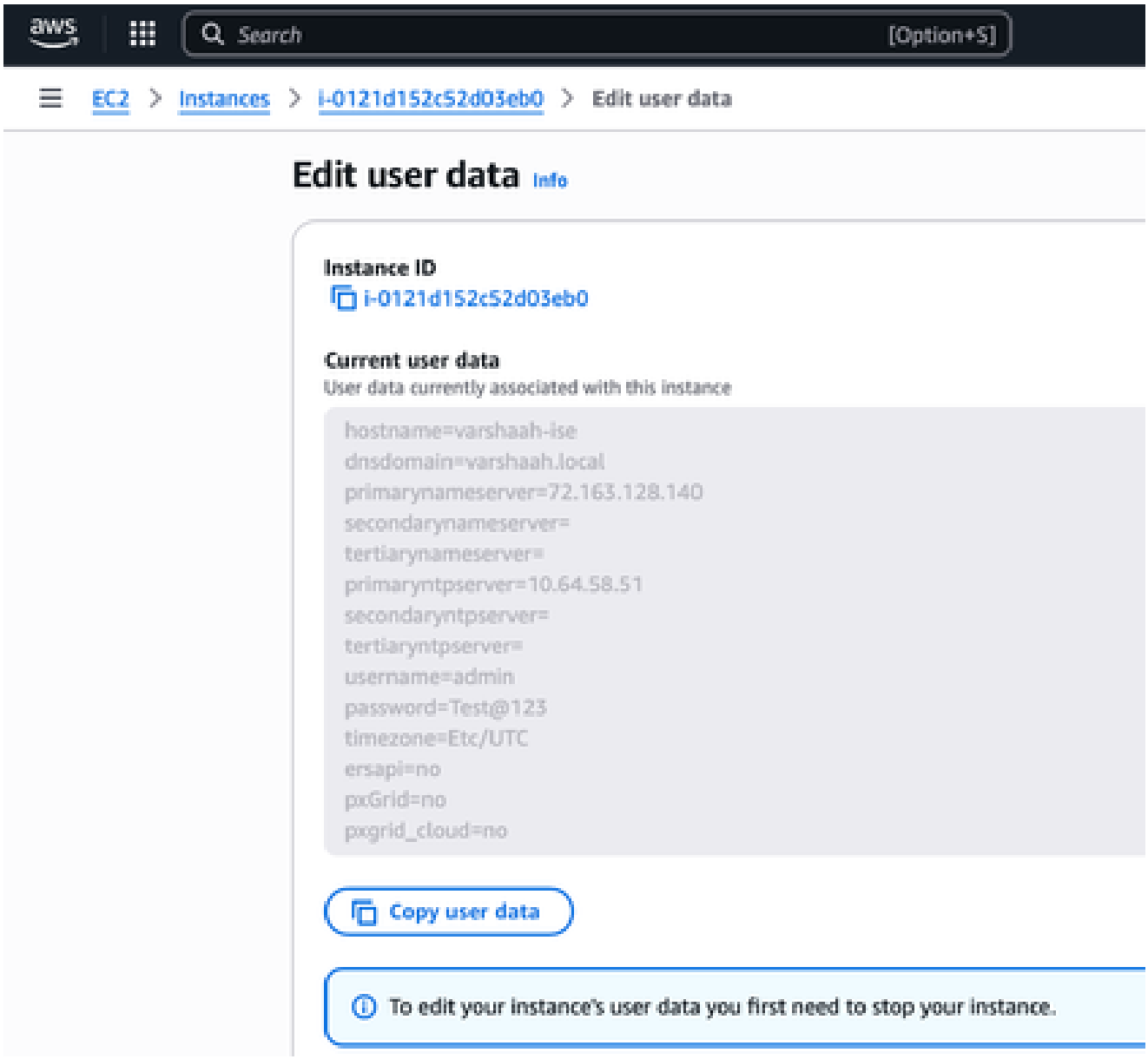


解决方案

- 在AWS EC2控制台中，导航到EC2 >实例> your_instance_id
- 点击 “操作”(Actions)>“实例设置”(Instance settings)>“编辑用户数据”(Edit user data)。



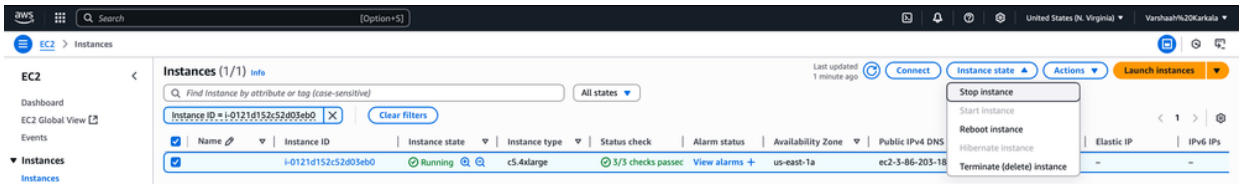
- 您可以在此处找到实例启动期间设置的特定用户名和密码。这些凭证可用于登录到ISE GUI。



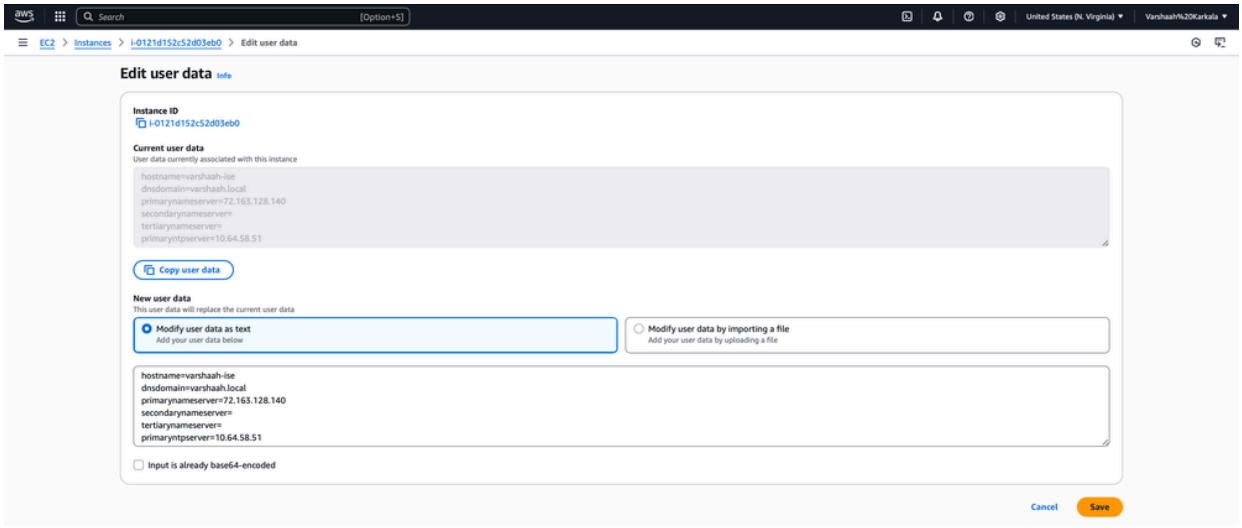
- 设置主机名和密码时验证主机名和密码：
  - 主机名
    - 仅允许字母数字符和连字符(-)。
    - 长度不得超过19个字符。
  - 密码
    - 必须符合Cisco ISE密码策略。
    - 请参阅官方ISE管理员指南：[ISE 3.4密码策略 — 思科管理员指南]
- 如果配置的密码不符合ISE密码策略，登录尝试将失败；即使使用正确的凭证。

- 如果您怀疑密码配置错误，请按照以下步骤进行更新：

1. 在EC2控制台中，转到EC2 > Instances > your_instance_id
2. 单击Instance state > Stop instance。



3. 实例停止后，单击操作>实例设置>编辑用户数据。



4. 修改用户数据脚本以相应地更新密码。
5. 保存更改，然后通过Instance state > Start instance重新启动实例。

已知缺陷

Bug ID	描述
思科漏洞ID 41693	如果元数据版本设置为“仅V2”，AWS上的ISE无法检索用户数据。 ISE 3.4之前的版本仅支持IMDSv1。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。