Implante o Identity Services Engine (ISE) versão 3.4 no AWS

Contents

Introdução

Este documento descreve como configurar o Cisco ISE no AWS usando o modelo CloudFormation (CFT) e a Amazon Machine Image (AMI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos antes de prosseguir com esta implantação:

- Cisco Identity Services Engine (ISE)
- Gerenciamento de instâncias e rede AWS EC2
- Geração e uso do par de chaves SSH
- Compreensão básica de VPCs, grupos de segurança e configuração DNS/NTP no AWS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity services engine (ISE)
- Console de nuvem da Amazon Web Services (AWS)

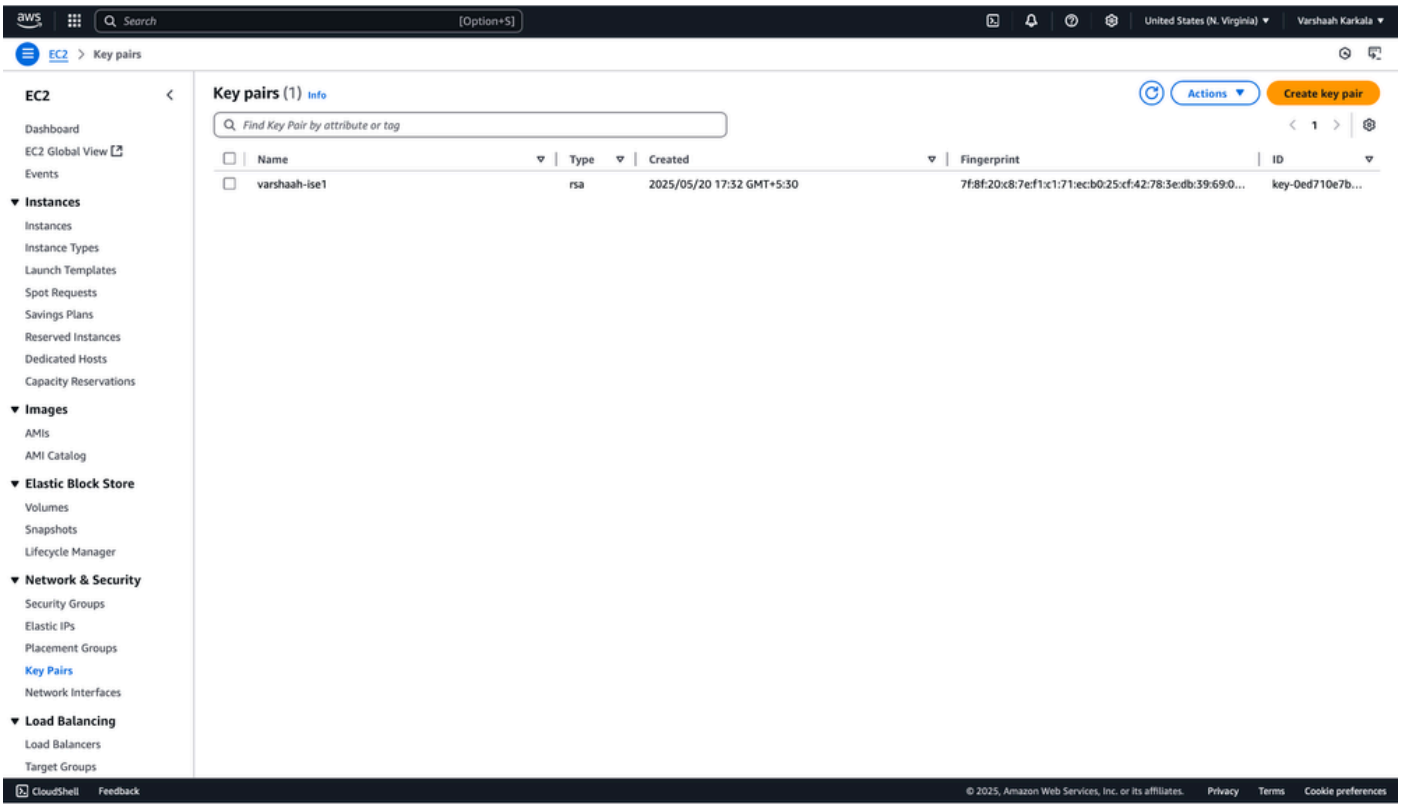
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

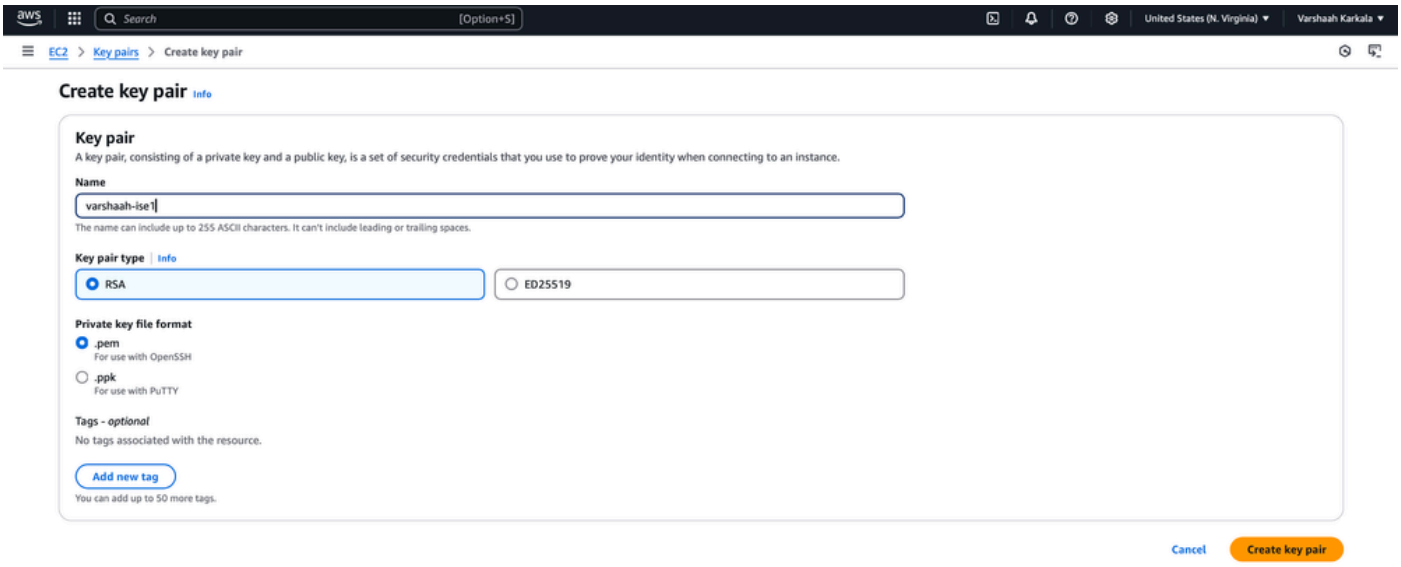
Parte 1: Gerando um par de chaves SSH

1. Para esta implantação, você pode usar um par de chaves pré-existente ou criar um novo.

2. Para criar um novo par, navegue para EC2 > Rede e Segurança > Pares de Chaves e clique em Criar par de chaves.



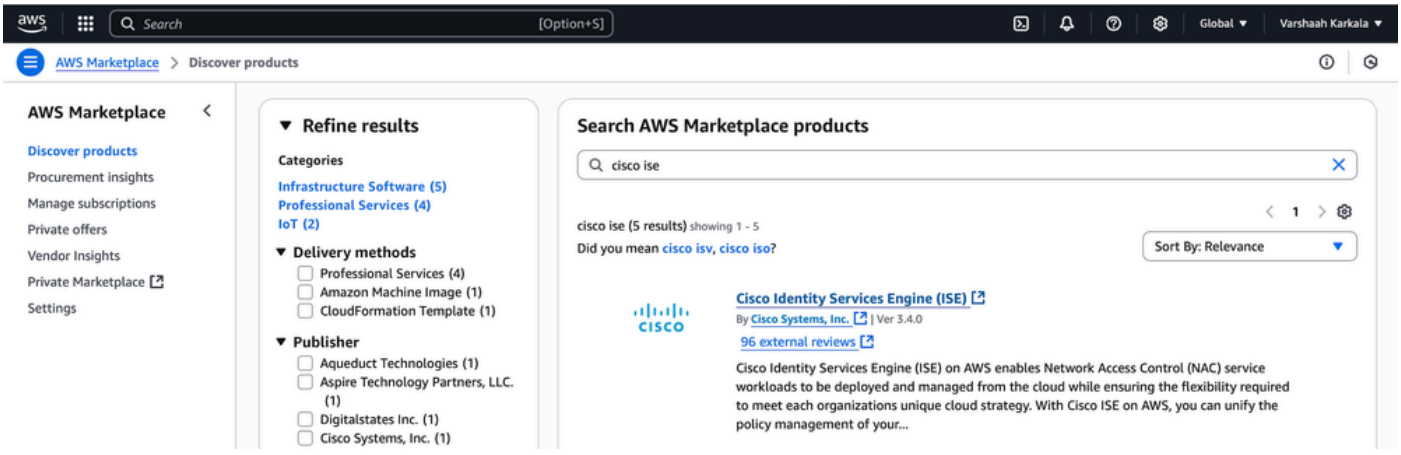
3. Insira o nome do par de chaves e clique em Criar par de chaves.

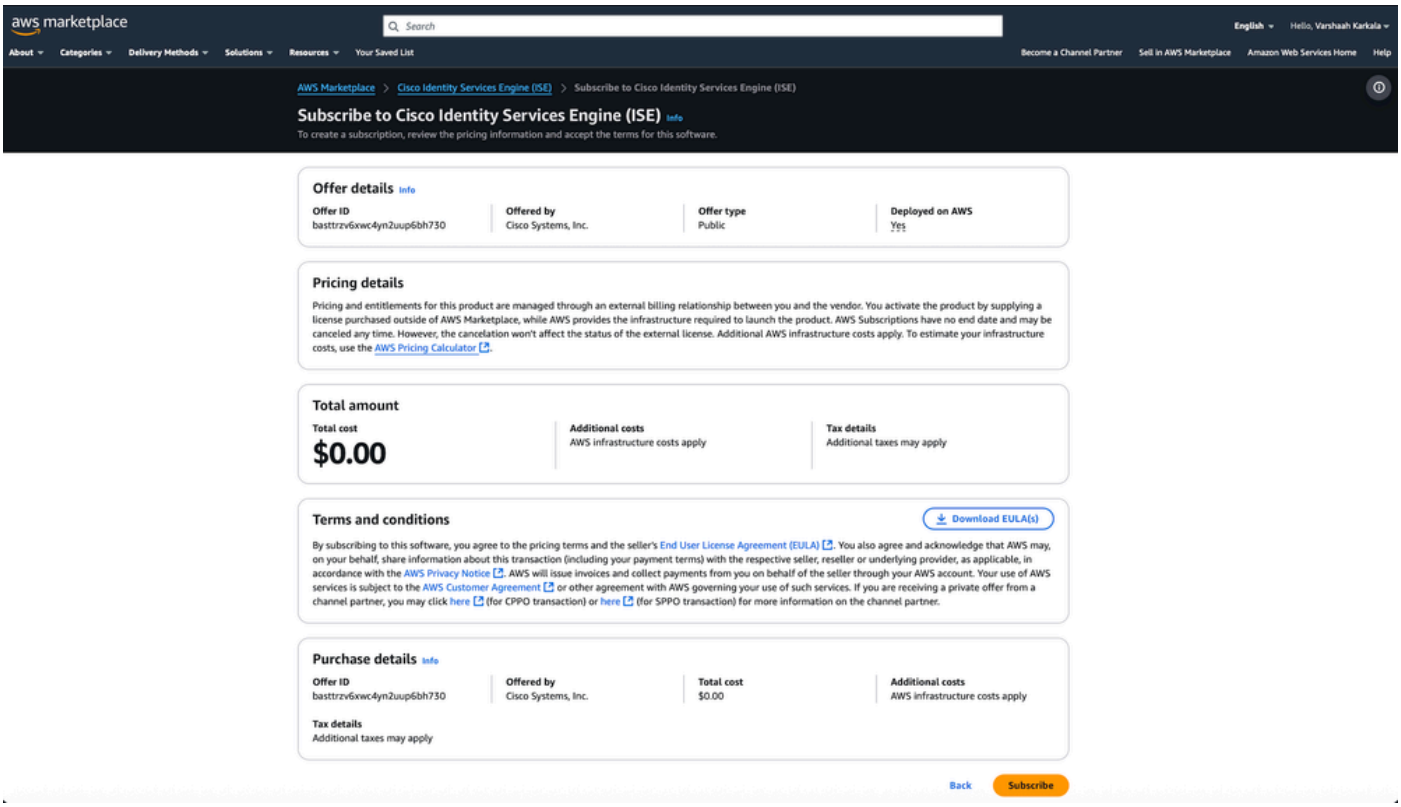


O arquivo de par de chaves (.pem) é baixado na sua máquina local. Certifique-se de manter esse arquivo seguro, pois essa é a única maneira pela qual você pode acessar sua instância EC2 depois que ela for iniciada.

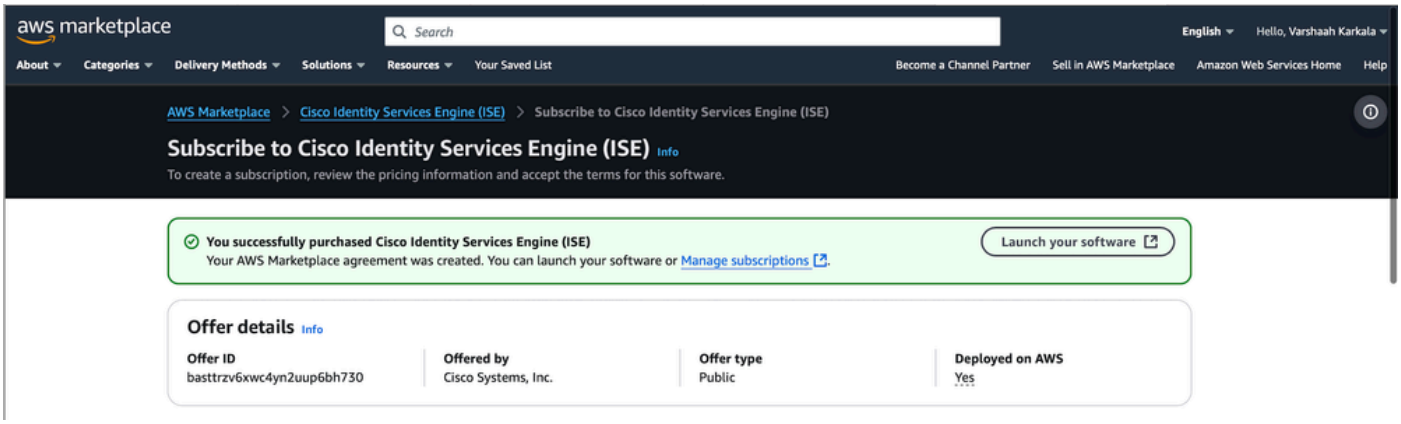
Parte 2: Configuração do ISE usando um modelo de formação de nuvem (CFT)

1. Faça login no AWS Management Console e procure AWS Marketplace Subscriptions.
2. Na barra de pesquisa, digite cisco ise e clique em Cisco Identity Services Engine (ISE) nos resultados. Clique em Assinar.

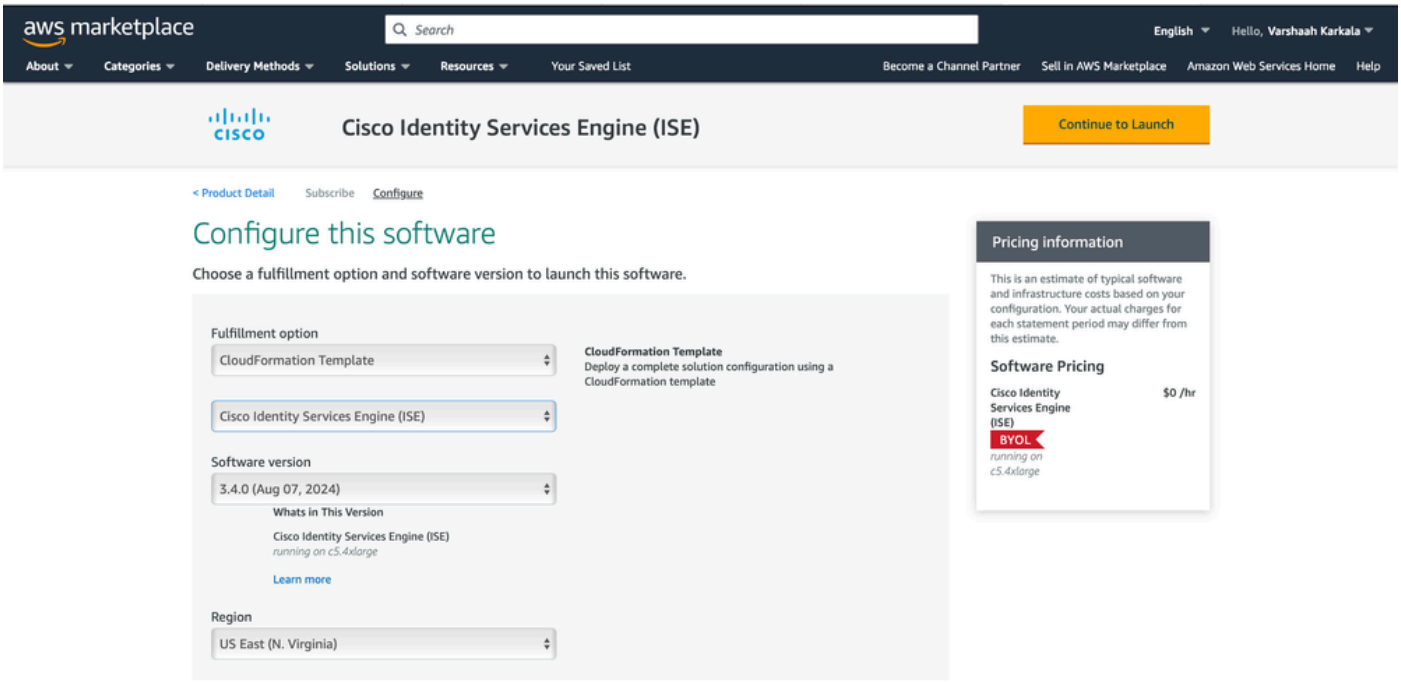




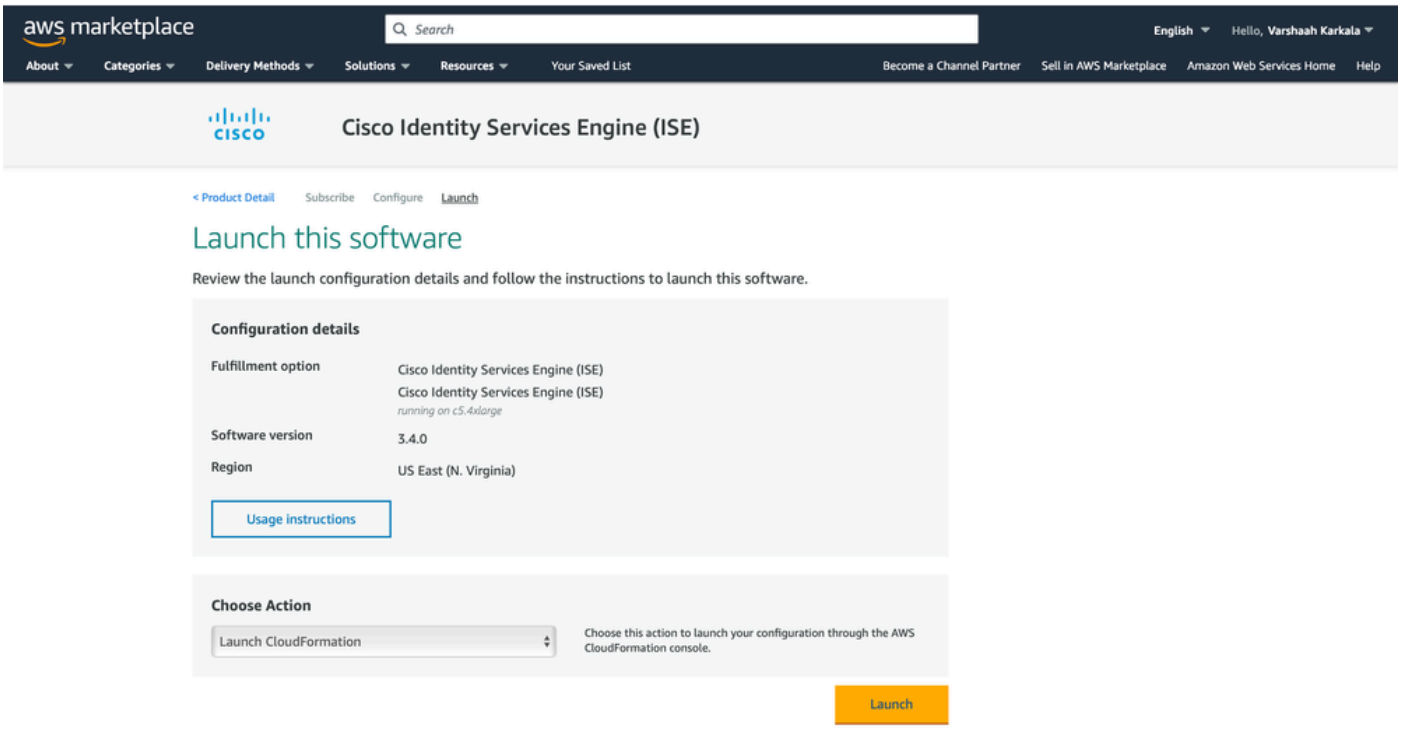
3. Após a assinatura, clique em Iniciar o Software.



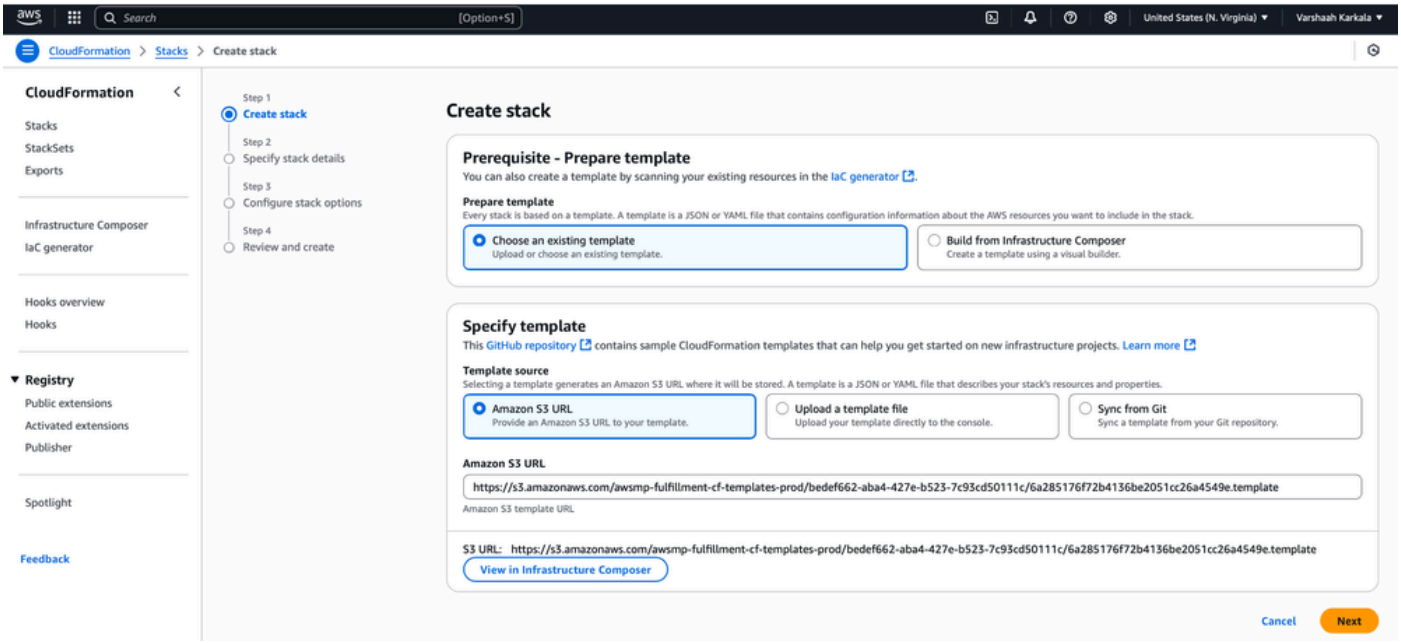
4. Em Opção de Preenchimento, escolha Modelo de Formação em Nuvem. Escolha a versão do Software (versão do ISE) e a Região onde deseja implantar a instância. Clique em Continuar para iniciar.



5. Na próxima página, escolha Iniciar CloudFormation como a ação e clique em Iniciar.

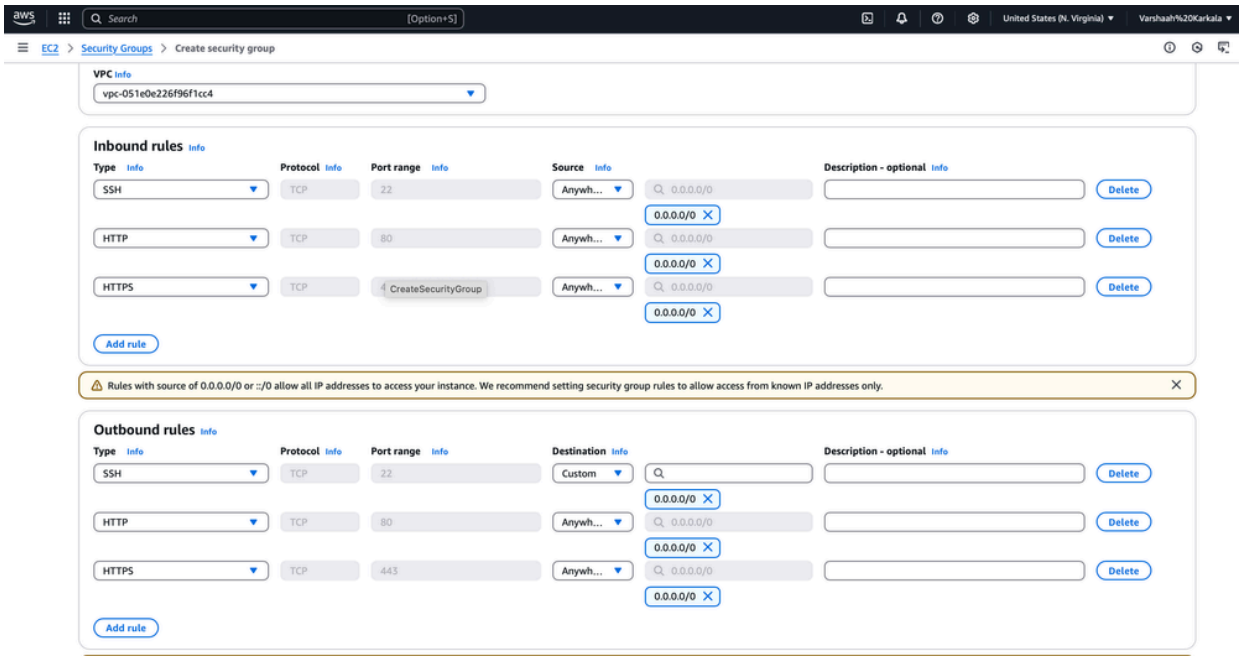


6. Nas configurações da pilha, mantenha as configurações padrão e clique em Avançar.



7. Informe os parâmetros necessários:

- Nome da pilha: Forneça um nome exclusivo para sua pilha.
- Hostname: Atribua o nome de host para o nó do ISE.
- Par de chaves: Selecione o par de chaves gerado ou pré-existente para acessar a instância EC2 posteriormente.
- Grupo de segurança de gerenciamento:
    - Use o grupo de segurança padrão (como mostrado) ou crie um personalizado por meio do painel EC2.
    - Para criar um novo grupo de segurança, navegue até o painel EC2 e navegue até Rede e segurança > Grupos de segurança para criar um novo grupo de segurança.
    - Clique em Create security group e insira os detalhes necessários.
    - Verifique se o grupo de segurança está configurado para permitir o tráfego de entrada e saída necessário. Por exemplo, habilite o acesso SSH (porta 22) do seu endereço IP para acesso CLI.

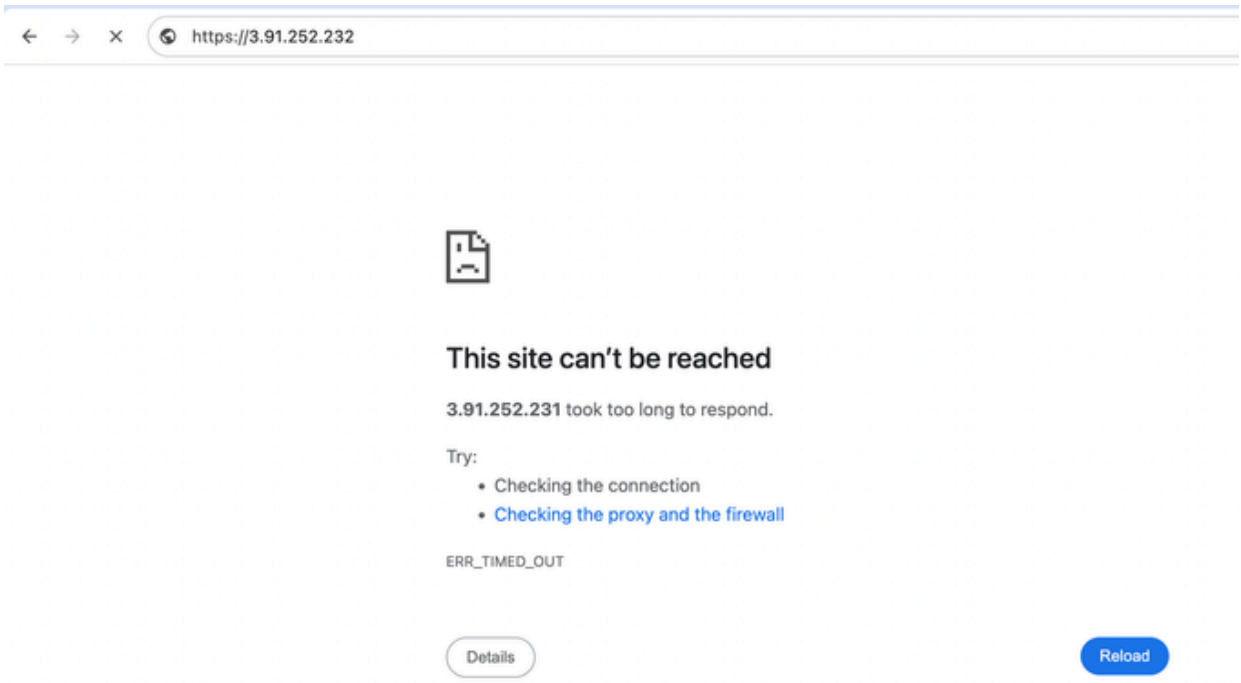


- Se o acesso SSH não estiver configurado corretamente, você pode encontrar um erro "Operation timed out" ao tentar se conectar via SSH.

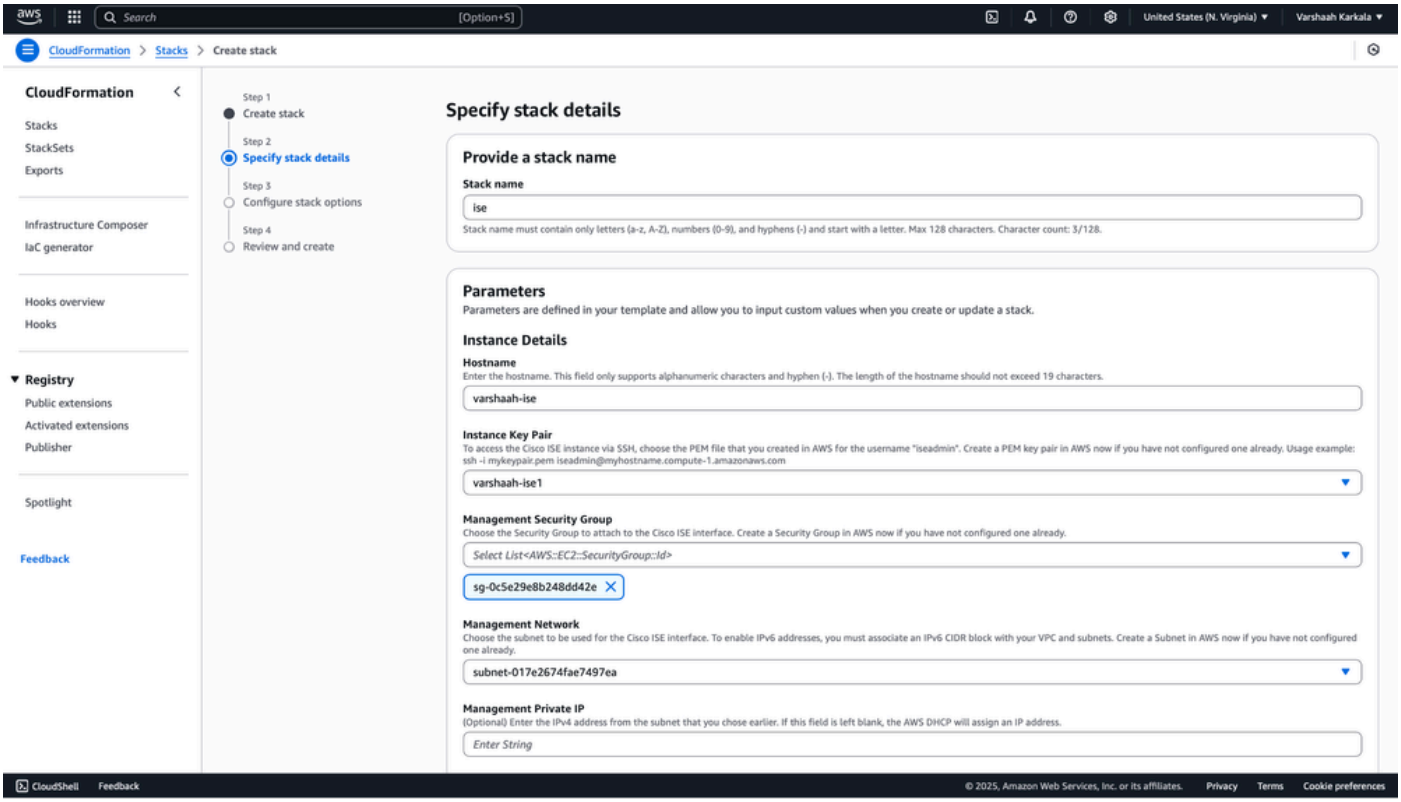
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

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

- Se o acesso HTTP/HTTPS não estiver configurado, você poderá ver um erro "Este site não pode ser acessado" ao tentar acessar a GUI.



- Rede de gerenciamento: uma das sub-redes preexistentes é selecionada.



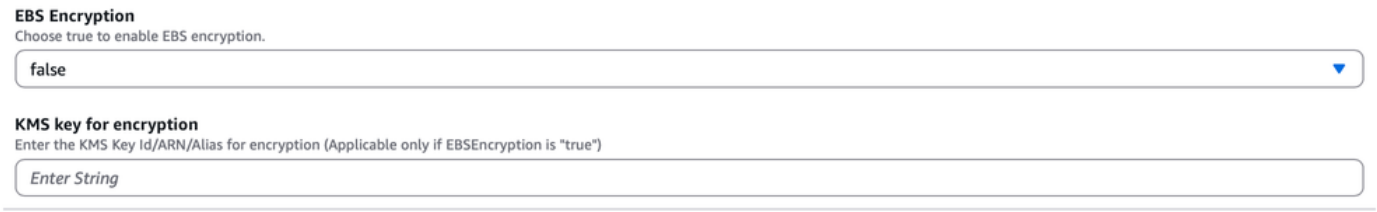
Se o seu projeto exigir uma implantação distribuída com alguns nós hospedados no AWS e outros no local, configure um VPC dedicado com uma sub-rede privada e estabeleça um túnel VPN para o dispositivo de headend da VPN no local para permitir a conectividade entre os nós do ISE hospedados no AWS e no local.

Para obter etapas detalhadas sobre como configurar o dispositivo VPN Headend, consulte [este]

guia.

8. Criptografia EBS

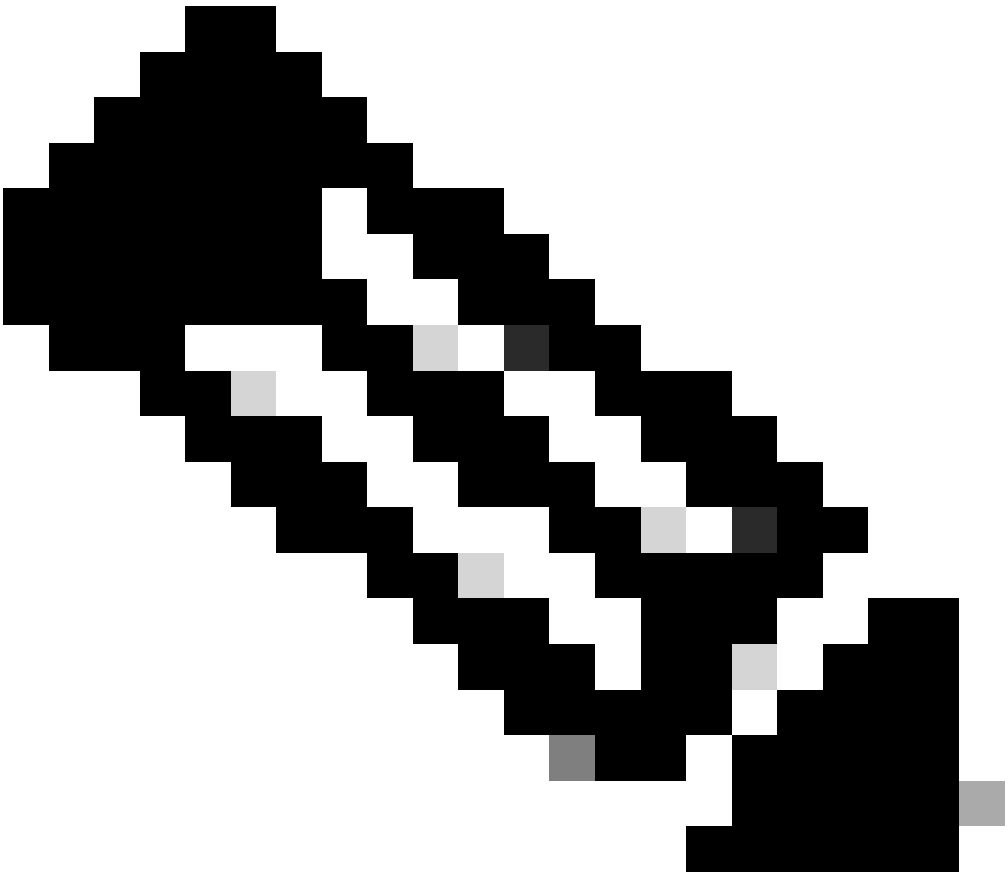
- Role para baixo para localizar as configurações de criptografia EBS.
- Defina Criptografia EBS como False, a menos que você tenha necessidades de criptografia específicas.



9. Configuração de Rede:

- Role para baixo para acessar as opções de configuração de rede, como domínio DNS, Servidor de nome primário e Servidor NTP primário.

  Certifique-se de que esses valores sejam inseridos corretamente.



Note: A sintaxe incorreta aqui pode impedir que os serviços do ISE sejam iniciados corretamente após a implantação.

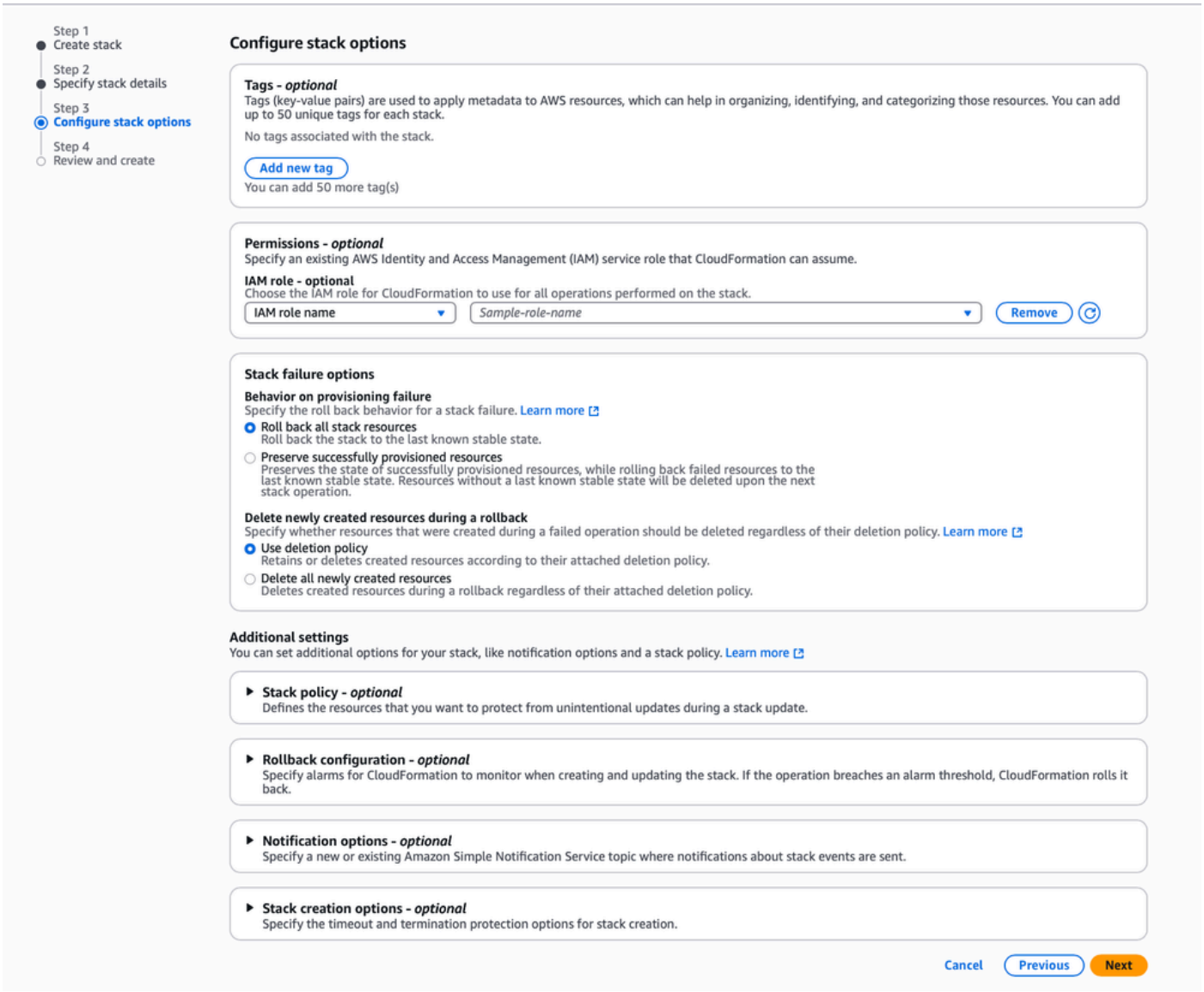
10. Detalhes do Serviço e do Usuário:

- Role para baixo para localizar a opção para ativar os serviços ERS e pxGrid
- Escolha se deseja habilitar os serviços ERS e pxGrid selecionando yes ou no.
- Em Detalhes do usuário, defina a senha do usuário admin padrão.

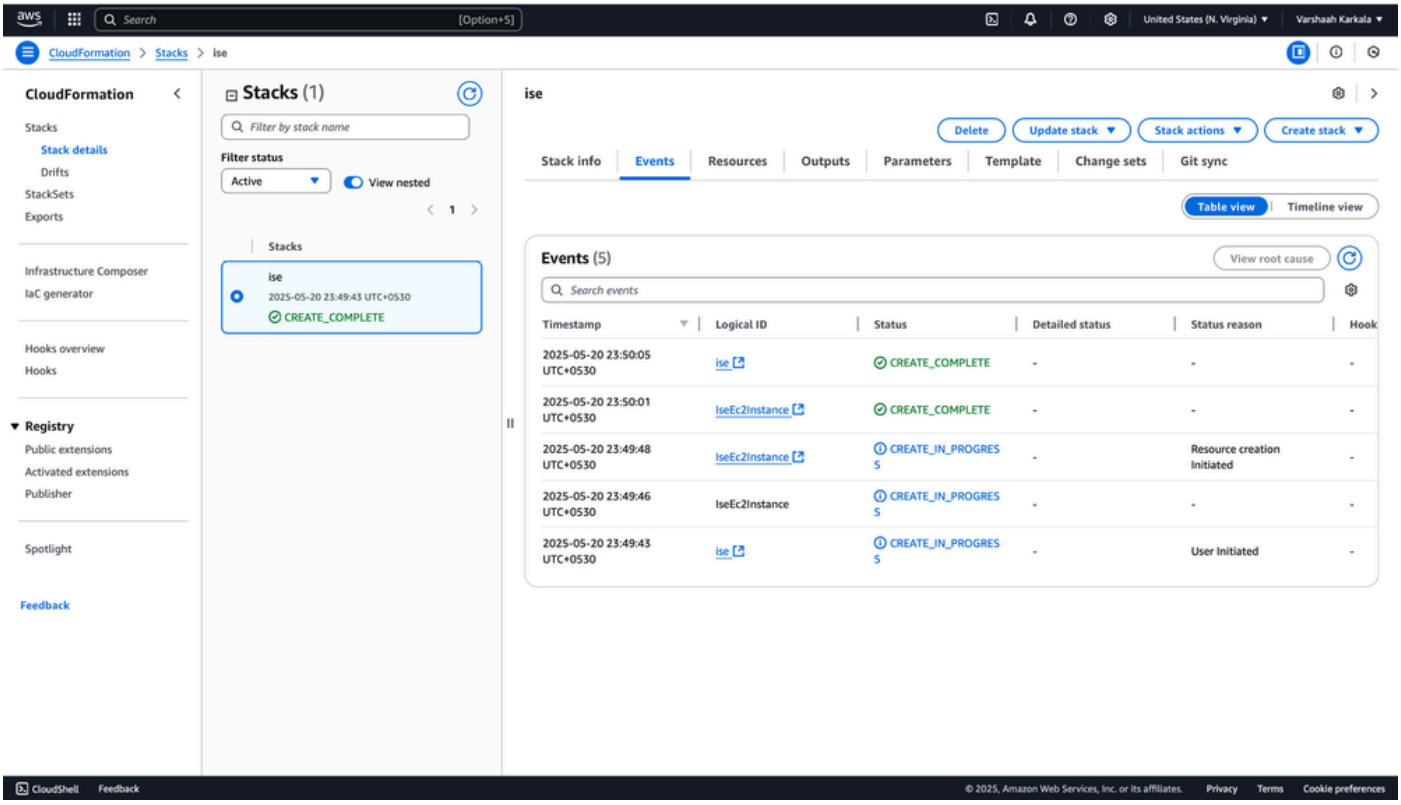
- Clique em Next.

11. Configurar Opções de pilha:

- Deixe todas as opções padrão como estão e clique em Avançar.



12. Revise o modelo para garantir que todas as configurações estejam corretas e clique em Enviar. Depois de criado, o modelo se parece com o exemplo mostrado abaixo:



13. Acesse os detalhes da pilha:
Navegue até CloudFormation > Stacks e localize sua pilha implantada.

14. Guia Exibir Saídas:

Selecione sua pilha e abra a guia Saídas. Aqui, você encontrará informações importantes geradas durante o processo de implantação, como:

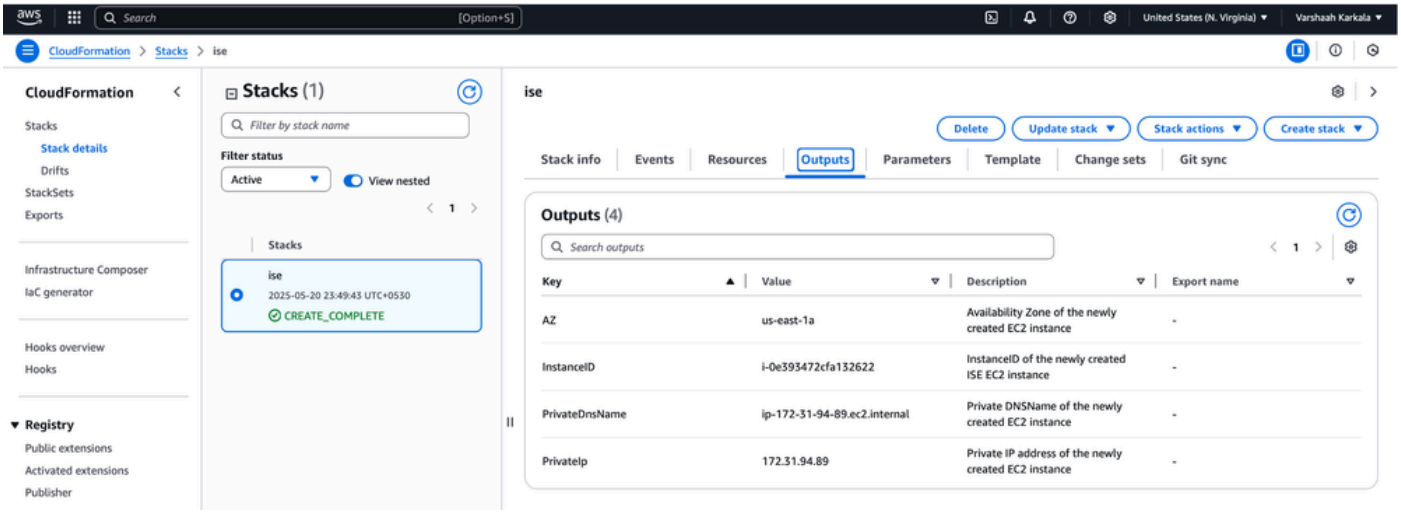
· Zona de disponibilidade: A região onde os recursos são implantados.

· ID da instância: O identificador exclusivo da instância implantada.

· Nome DNS: O nome DNS privado da instância, que pode ser usado para acesso remoto.

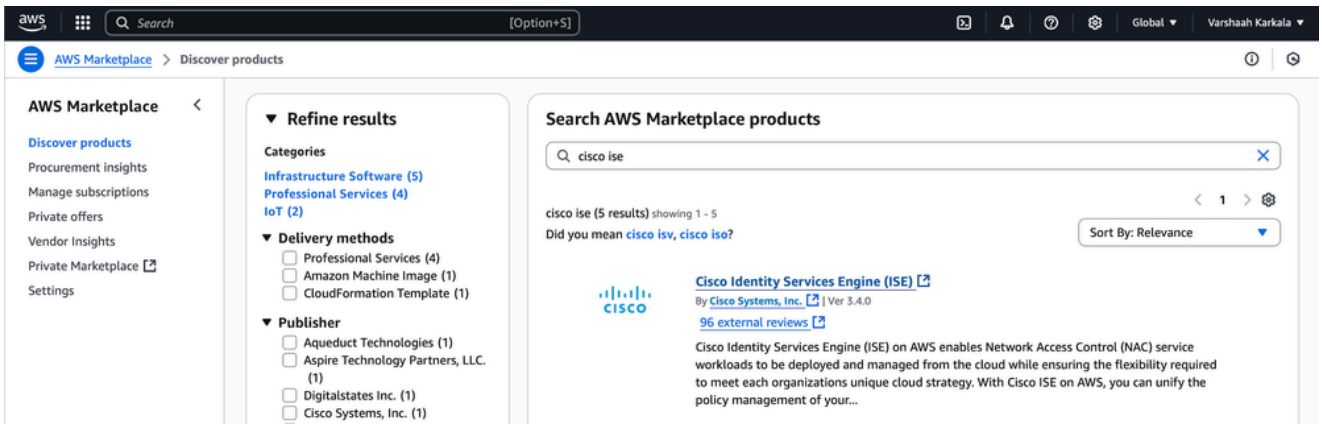
•Endereço IP: O endereço IP público ou privado da instância, dependendo da sua configuração.

Essas informações ajudam você a se conectar à instância e verificar sua disponibilidade. A guia Saídas se parece com este exemplo:



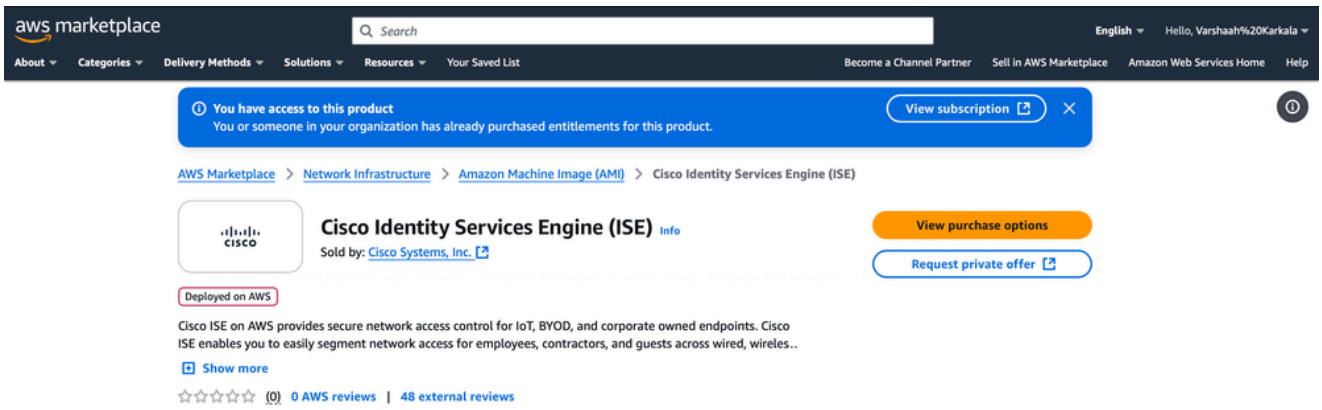
Parte 3: Configurando o ISE usando uma Amazon Machine Image (AMI)

1. Faça login no AWS Management Console e procure Assinaturas do AWS Marketplace.
2. Na barra de pesquisa, digite cisco ise e clique em Cisco Identity Services Engine (ISE) nos resultados.

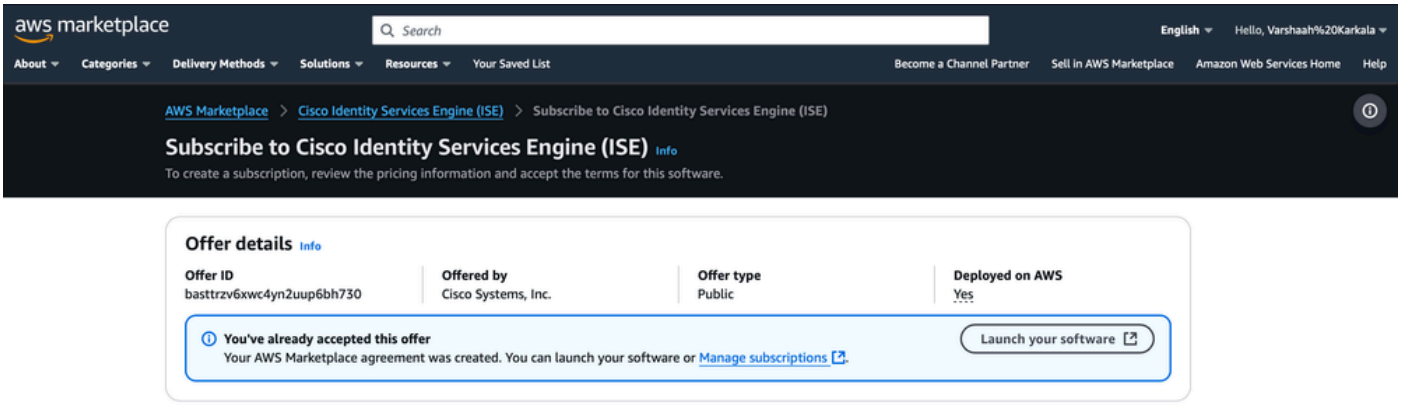


ISE no AWS Markeplace

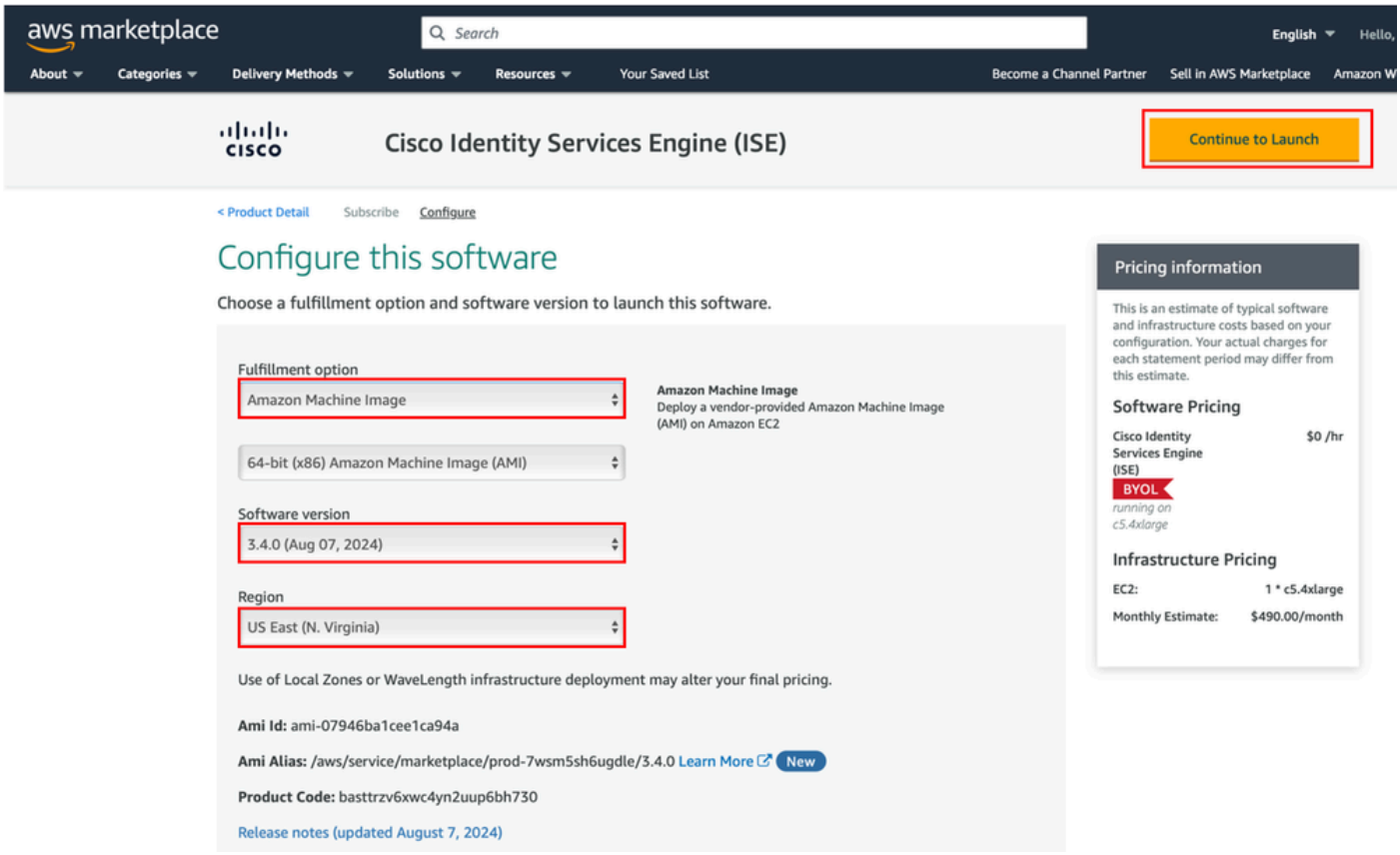
3. Clique em Exibir opções de compra.



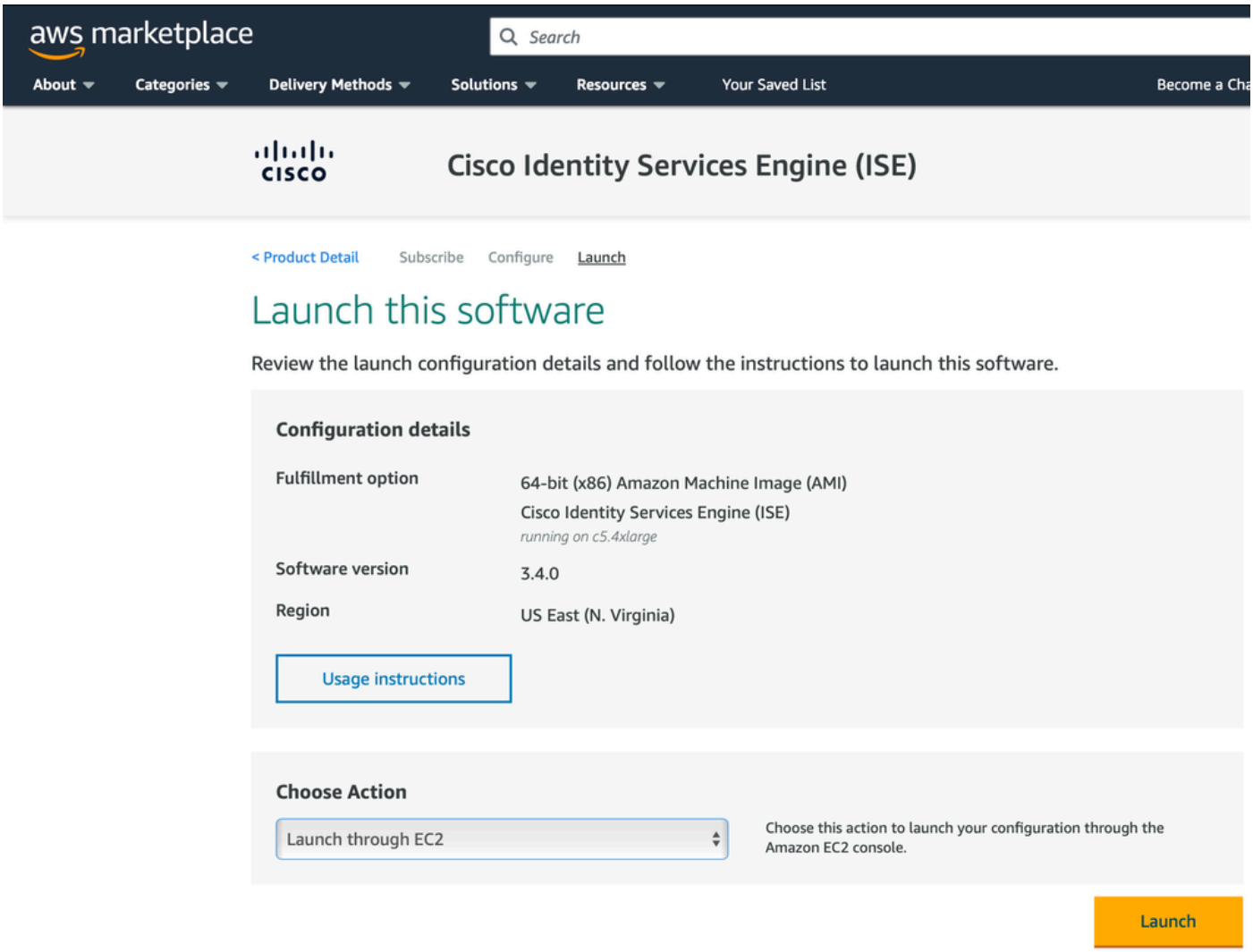
4. Clique em Iniciar seu software.



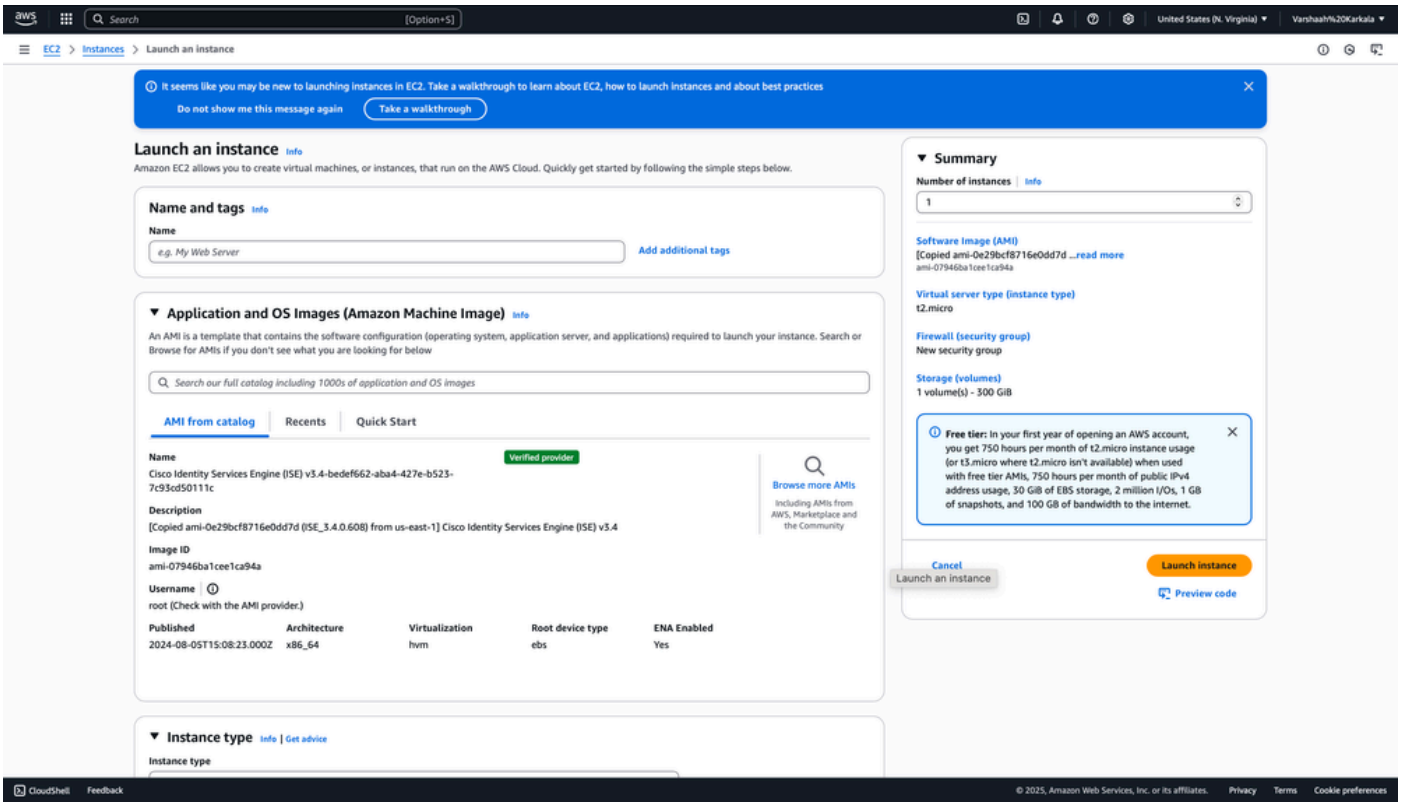
5. Sob a Opção de Preenchimento, escolha Amazon Machine Image. Escolha a versão de Software desejada e Region. Clique em Continuar para iniciar.



6. Em Escolher Ação, escolha Iniciar através de EC2. Clique em Iniciar para continuar.



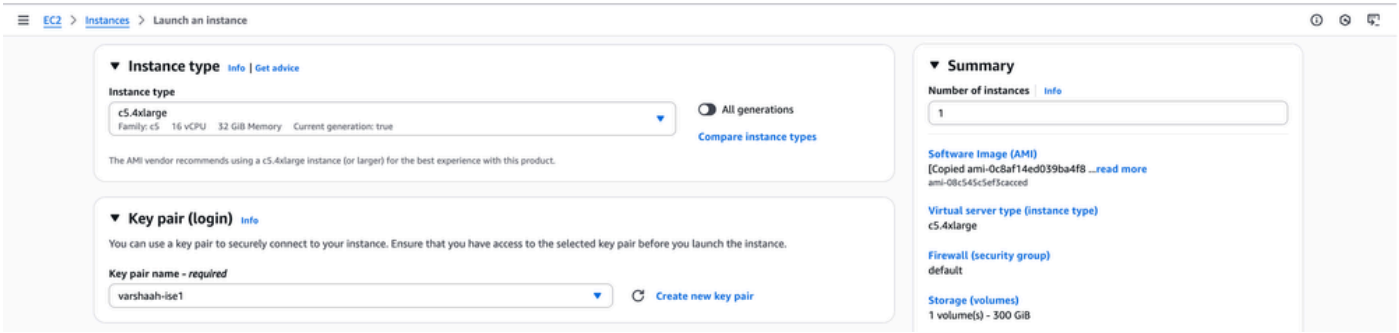
7. Você é redirecionado para a página EC2 Launch an Instance para definir as configurações da instância.



8. Role para baixo até a seção Tipo de Instância e escolha um tipo de instância apropriado com base em seus requisitos de implantação.

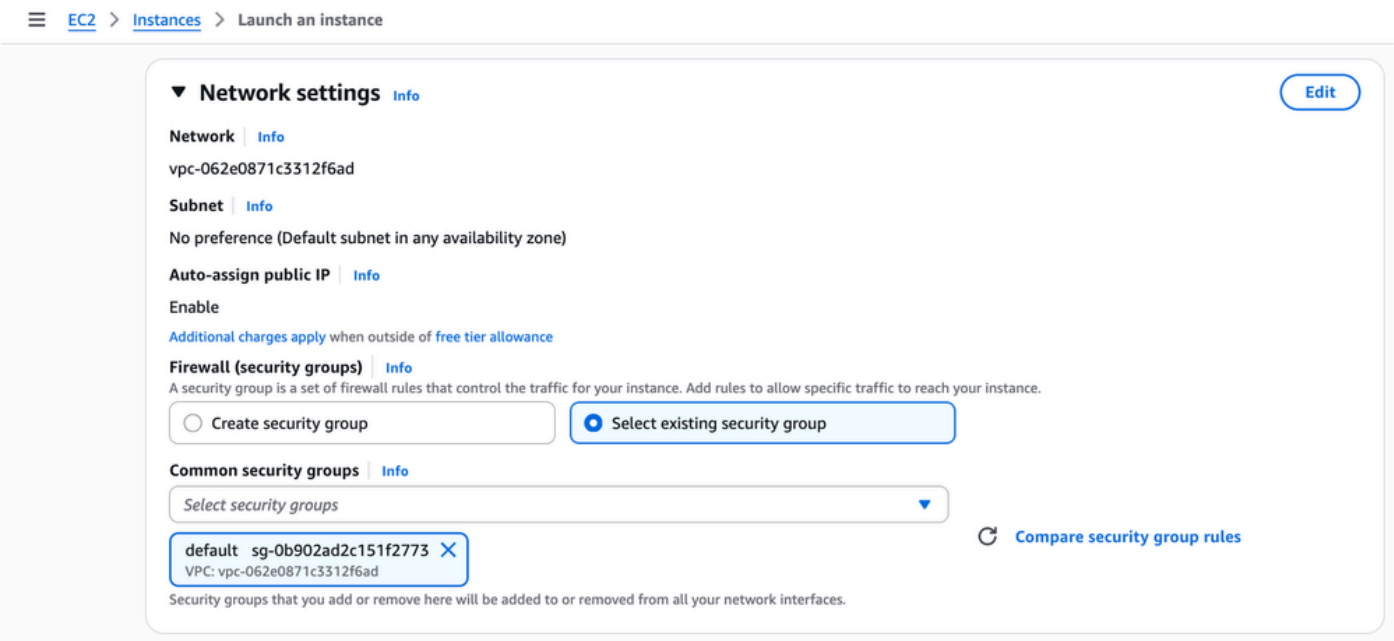
Em Par de chaves (login), selecione o par de chaves que foi gerado anteriormente ou crie um novo um (consulte as etapas de criação de pares de chaves fornecidas anteriormente).

Defina Number of Instances como 1.



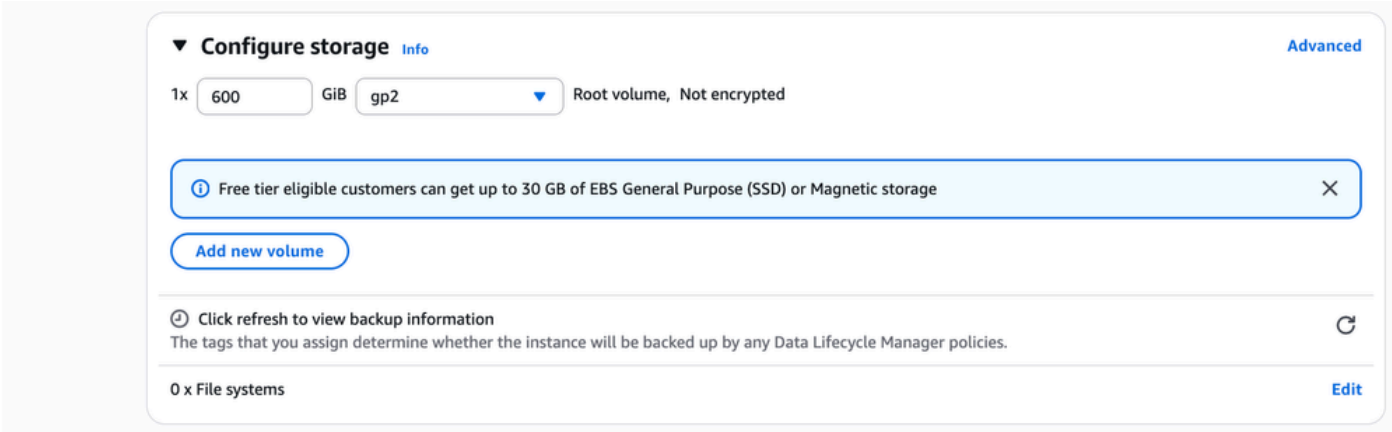
9. Na seção Configurações de rede:

- Configure o VPC e a sub-rede conforme necessário.
- Para o Grupo de segurança, selecione um existente ou crie um novo grupo (como mostrado no exemplo).



10. Na seção Configurar Armazenamento, configure o volume size desejado.

Exemplo: 600 GiB usando o tipo de volume gp2.



11. Na seção Detalhes Avançados, configure as definições adicionais necessárias para sua implantação, como perfil da instância do IAM, dados do usuário ou comportamento de desligamento.

▼ **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 ▼

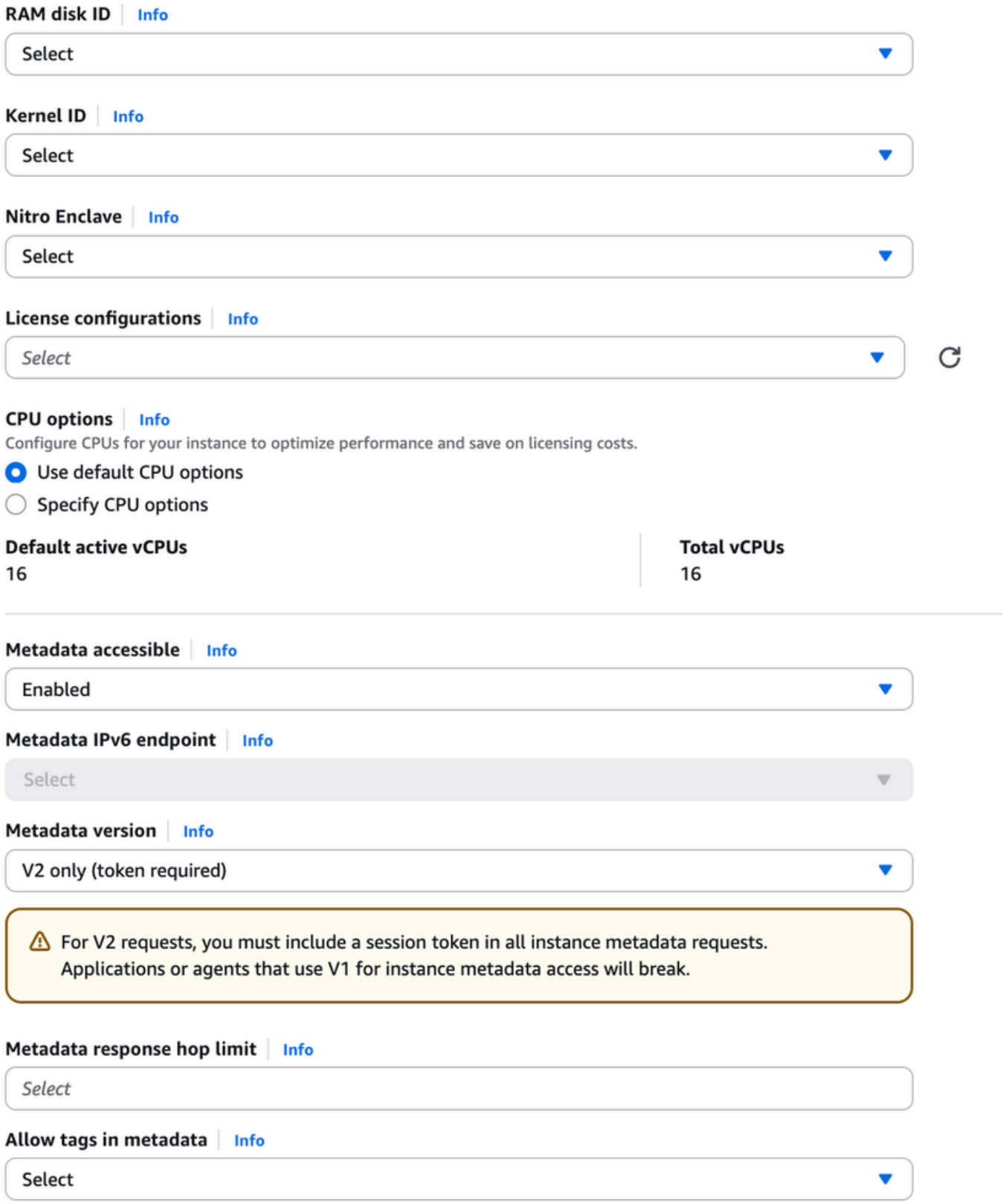
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. Na seção Versão de Metadados:

- Para o ISE versão 3.4 e posterior, escolha Somente V2 (token necessário) — esta é a opção recomendada.
- Para versões do ISE anteriores à 3.4, escolha V1 e V2 (token opcional) para garantir a compatibilidade.



13. No campo Dados do usuário, forneça os parâmetros de configuração inicial para a instância do ISE, incluindo as credenciais nome do host, DNS, servidor NTP, fuso horário, ERS e admin .

Exemplo:
hostname=varshahise2

primary nameserver=x.x.x.x

dnsdomain=varshaah.local

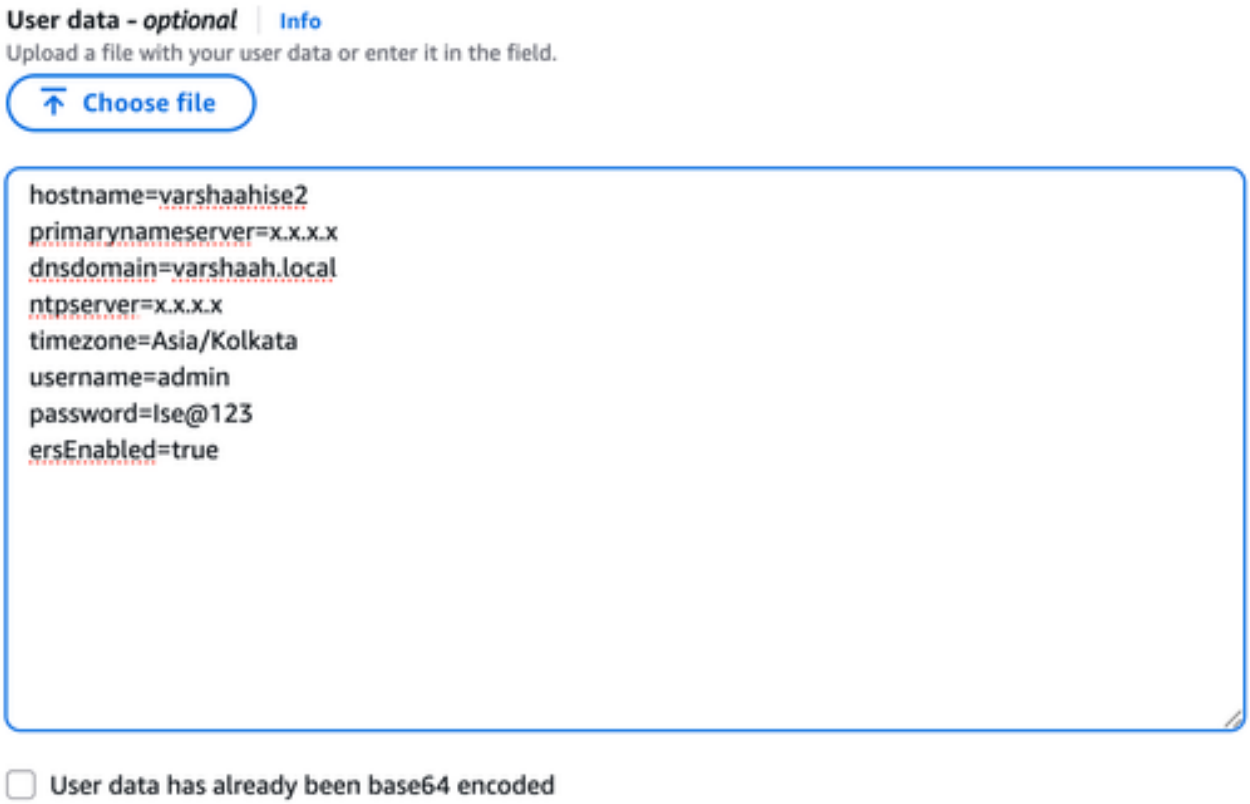
ntpserver=x.x.x.x

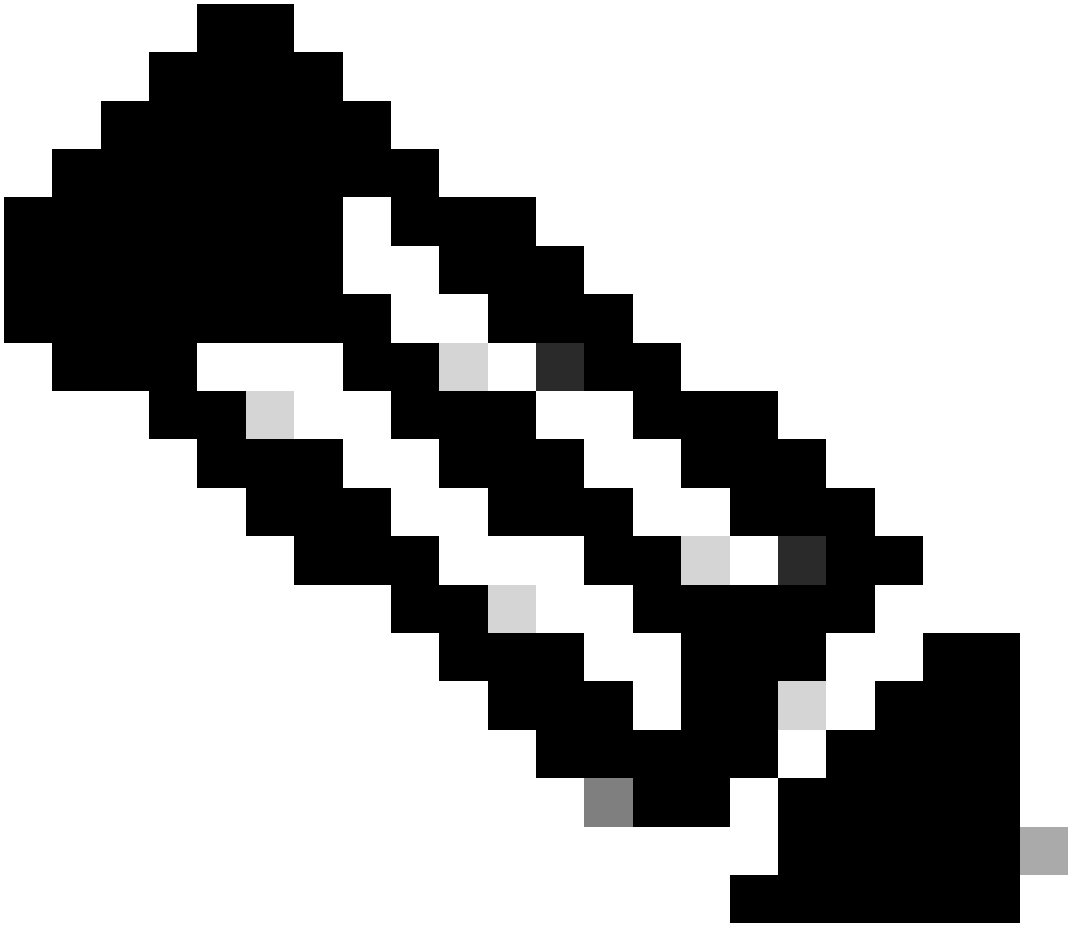
timezone=Ásia/Kolkata

username=admin

password=Ise@123

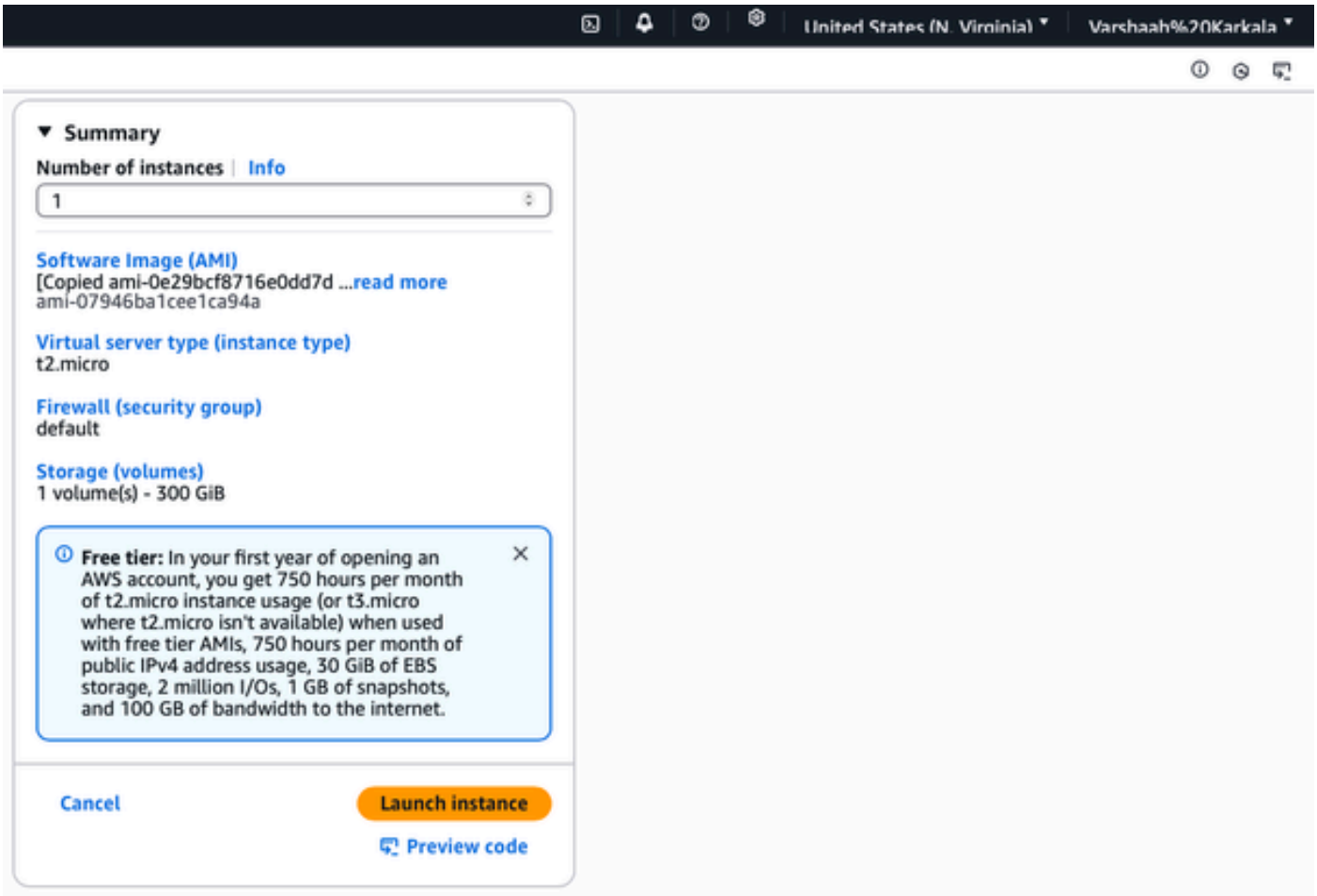
ersEnabled=true



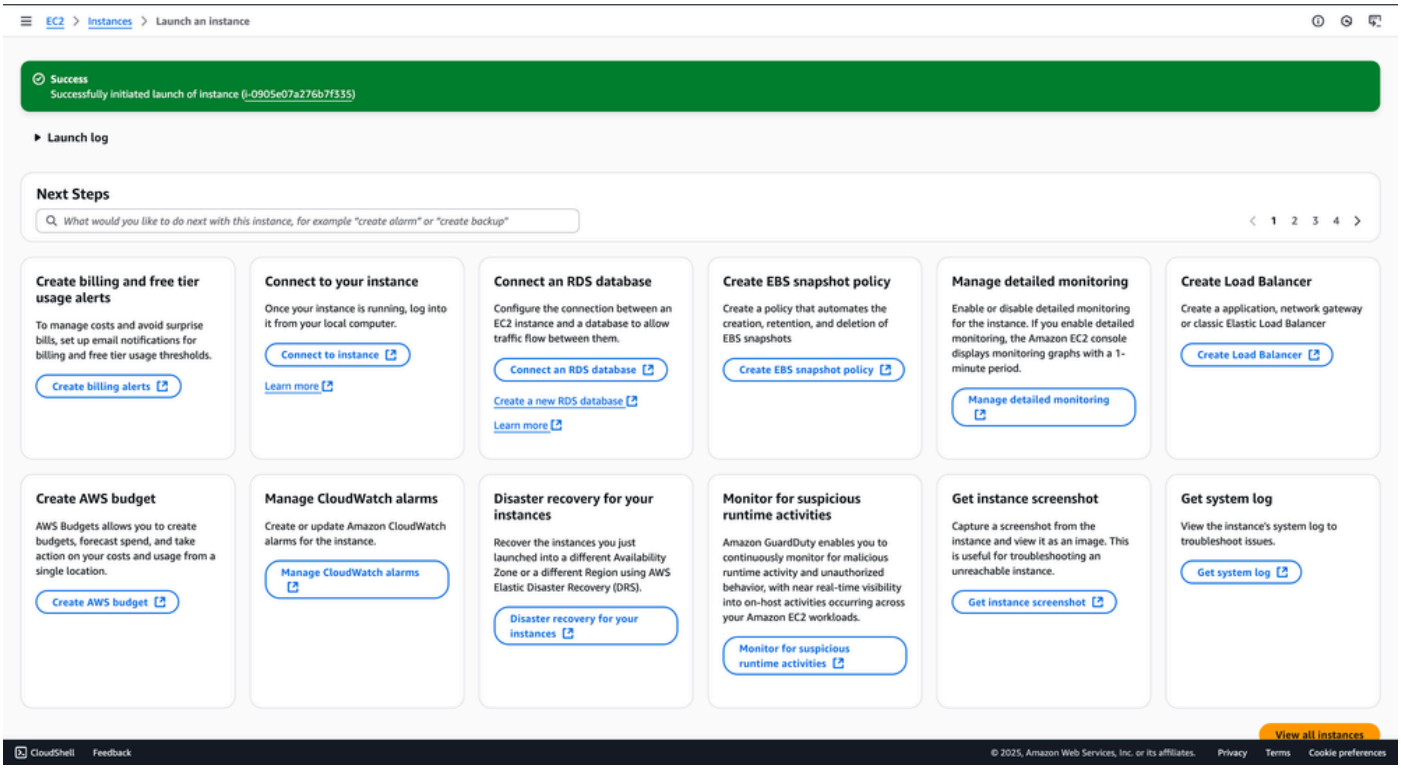


Note: Verifique se a senha está em conformidade com a política de senha do Cisco ISE.

Após inserir os dados do usuário e concluir a configuração, clique em Iniciar instância.



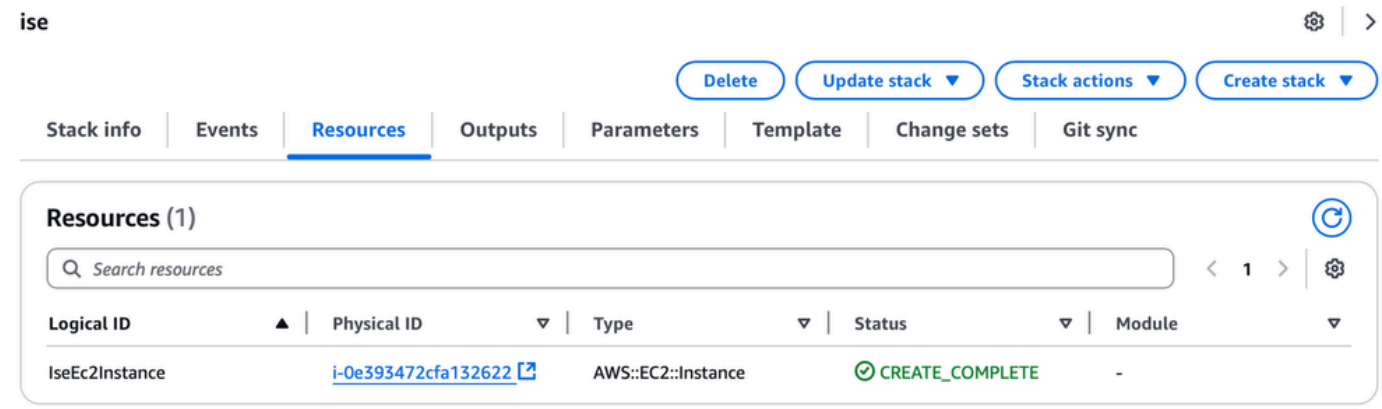
14. Depois que a instância é iniciada, uma mensagem de confirmação é exibida informando: 'Inicialização da instância <nome_da_instância> iniciada com êxito'. Isso indica que o processo de inicialização foi iniciado com êxito.

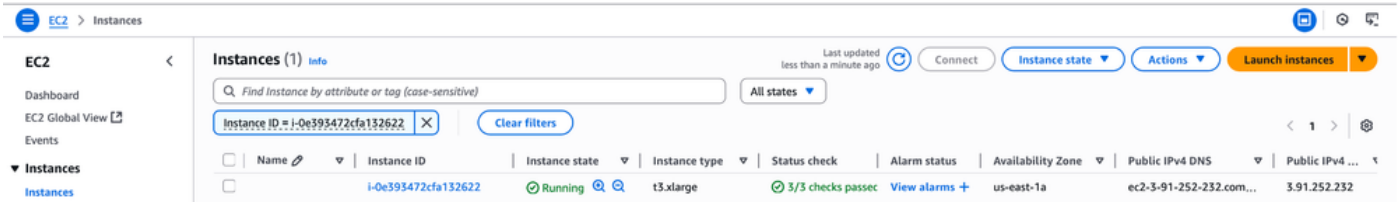


Verificar

Acesse a instância do ISE criada usando o CFT

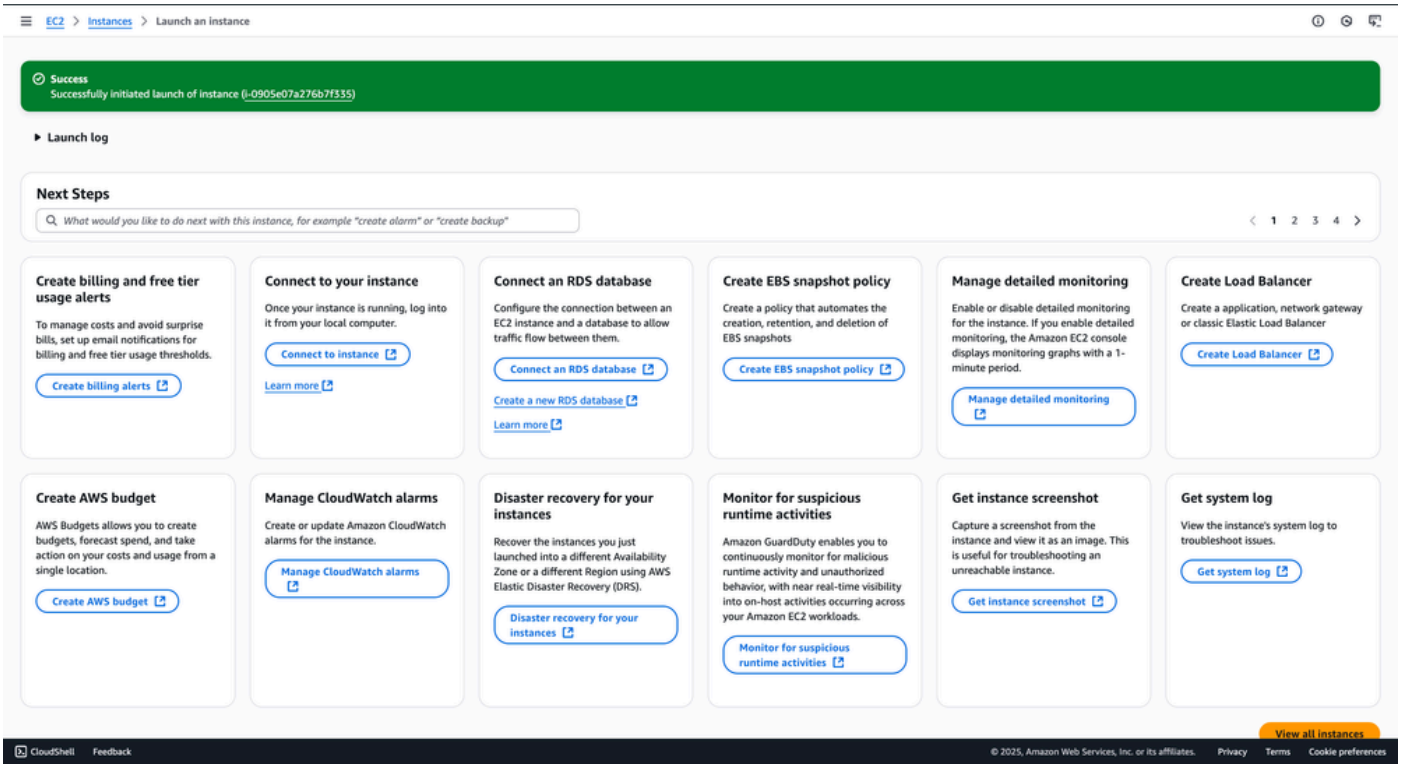
Navegue até a guia Resources em sua pilha CloudFormation e clique no Physical ID. Ele o redireciona para o painel EC2, onde você pode ver a instância.

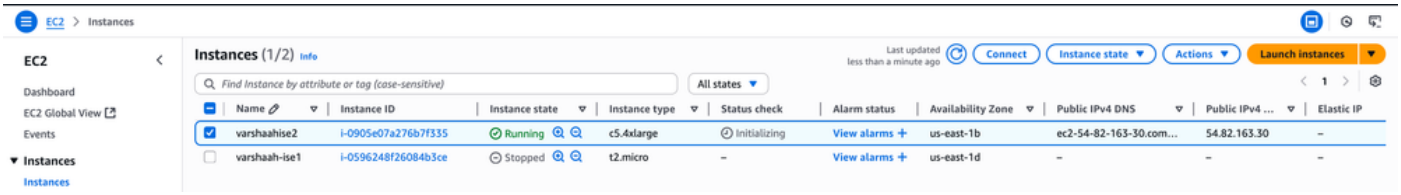




Acesse a instância do ISE criada usando o AMI

Clique em Exibir Todas as Instâncias para navegar até a página de instâncias do EC2. Nessa página, verifique se a Verificação de Status é mostrada como verificações de 3/3 aprovadas, indicando que a instância está ativa e íntegra.





Acessar a GUI do ISE

O servidor ISE foi implantado com êxito.

Para acessar a GUI do ISE, você precisa usar o endereço IP da instância em seu navegador. Como o IP padrão é privado, ele não pode ser acessado diretamente da Internet.

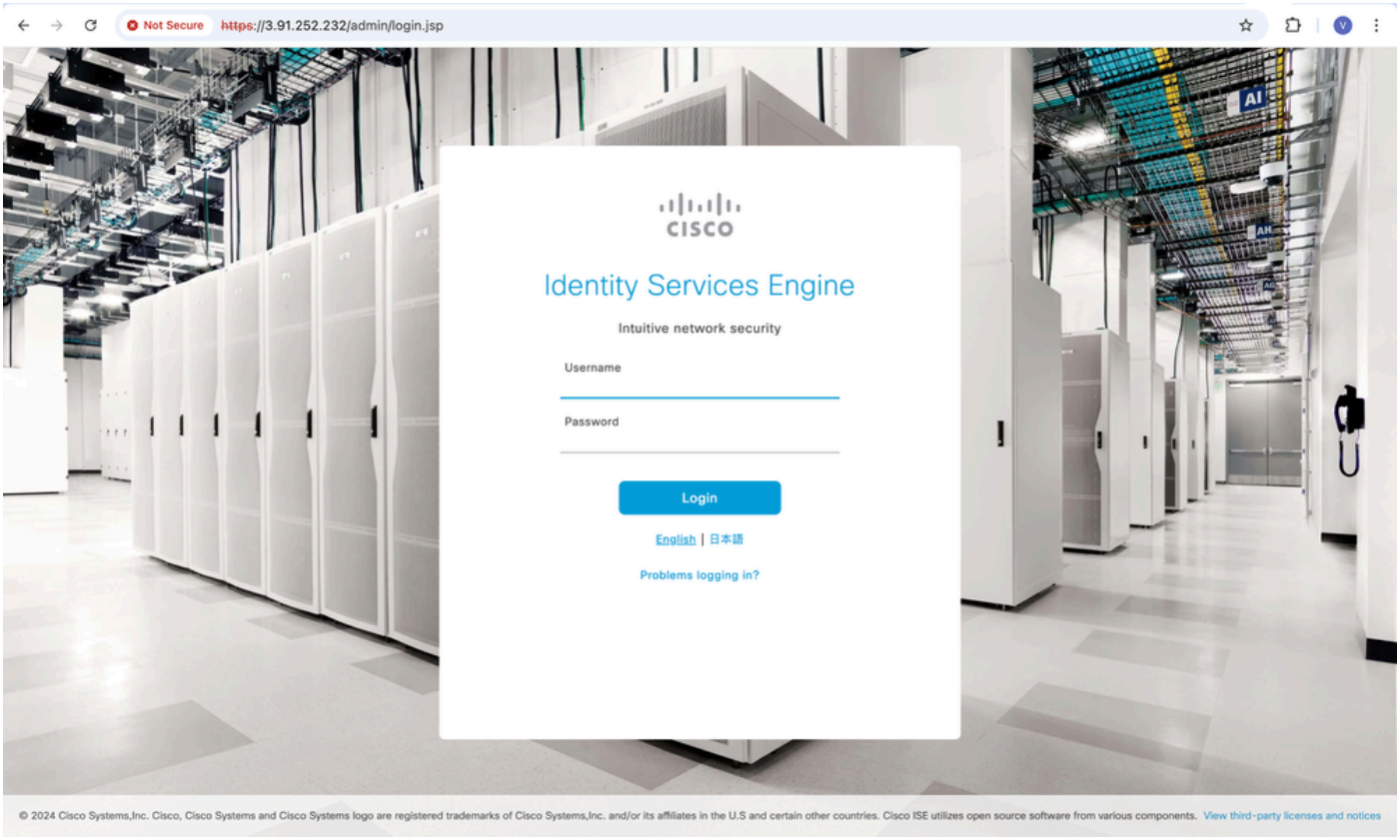
Verifique se um IP público está associado à instância:

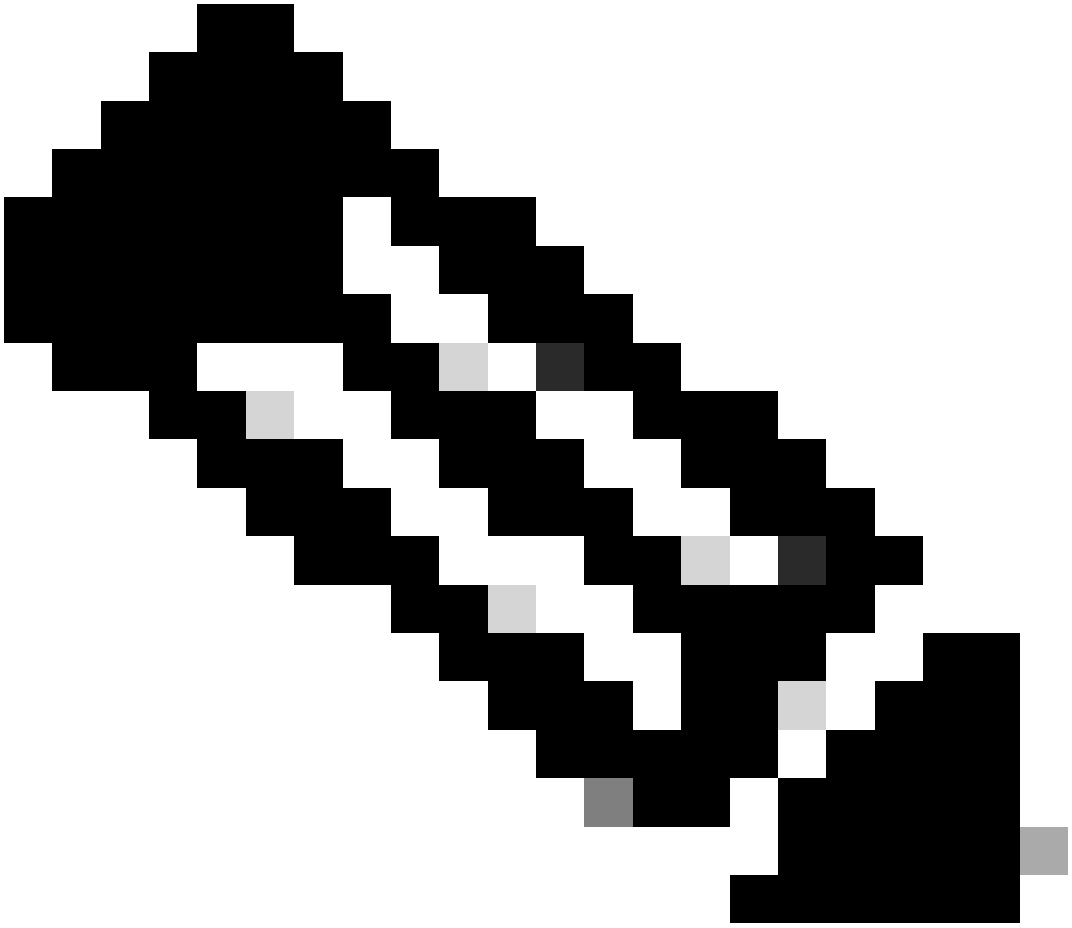
- Navegue até EC2 > Instâncias e selecione sua instância.
- Procure o campo endereço IPv4 público.

Aqui, você pode ver um endereço IP público que pode ser usado para acessar a GUI do ISE.

Abra um navegador compatível (por exemplo, Chrome ou Firefox) e insira o endereço IP público.

A página de login da GUI do ISE é exibida.





Note: Depois que o acesso SSH se torna disponível, geralmente leva de 10 a 15 minutos para que os serviços do ISE façam a transição completa para um estado de execução.

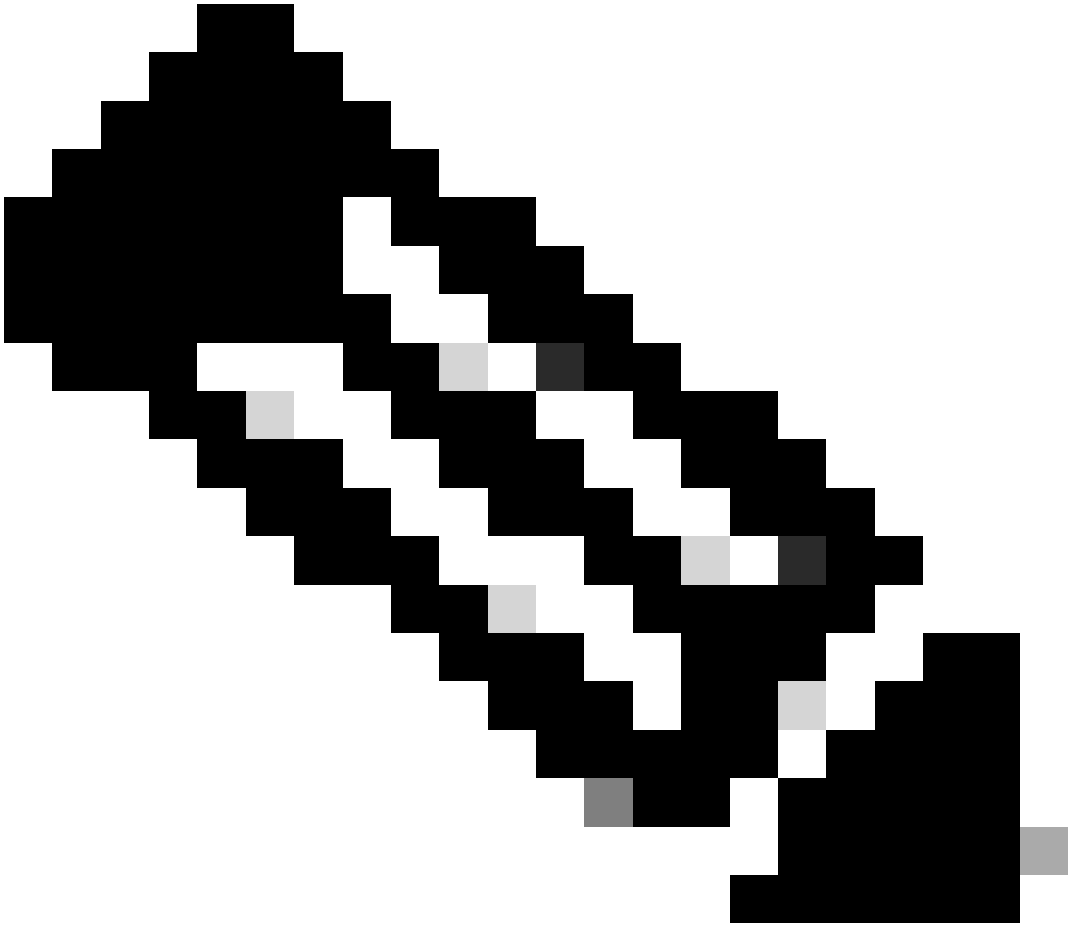
Acessar CLI via SSH a partir do terminal

No console EC2, selecione sua instância e clique em Connect.

Na guia SSH client, siga estas etapas:

- Navegue até a pasta que contém o arquivo de chave .pem baixado.
- Execute estes comandos:

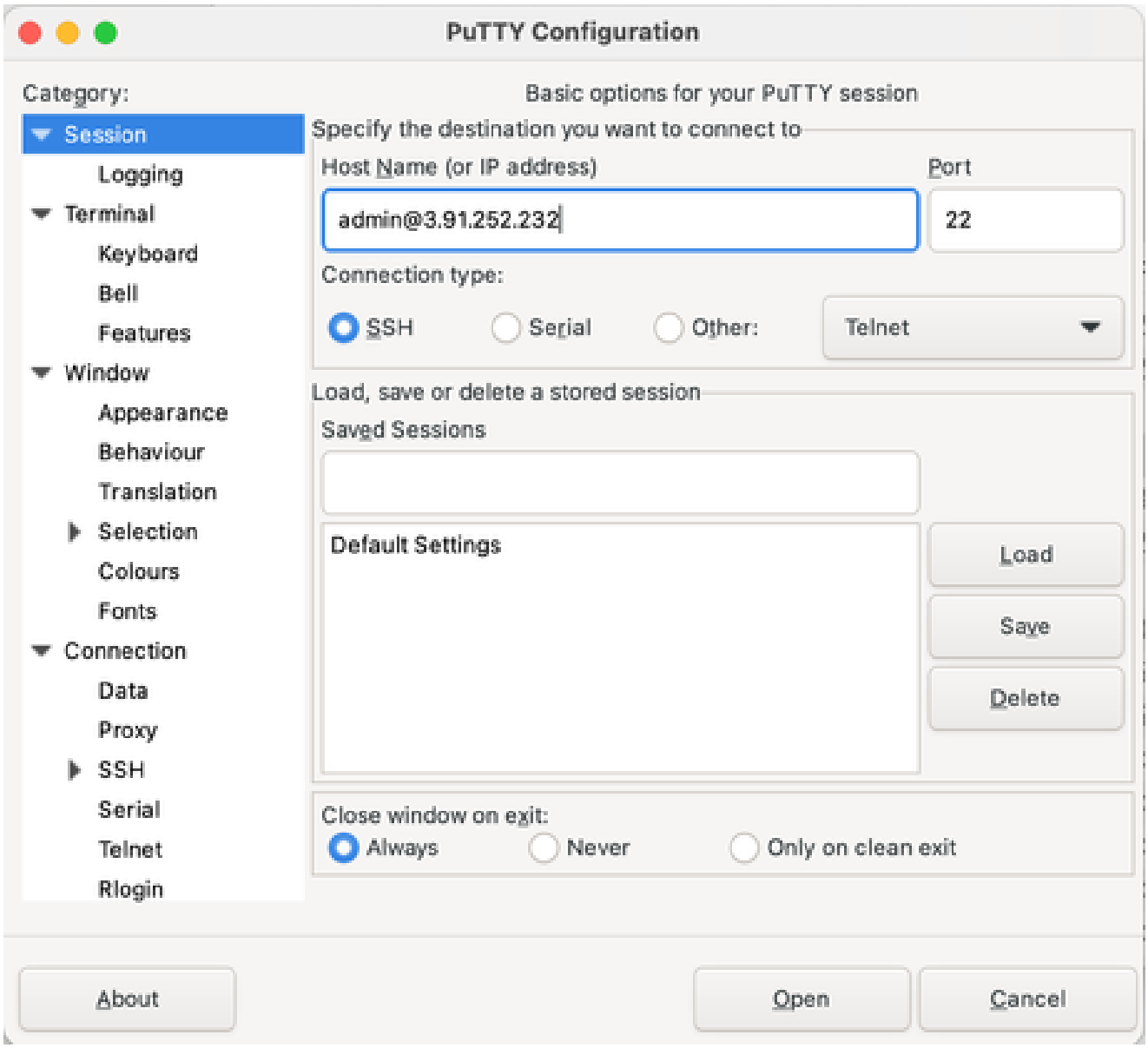
- cd <path-to-key-file>
- chmod 400 <nome-do-par-de-chaves>.pem
- ssh -i "<your-key-pair-name>.pem" admin@<public-ip-address>



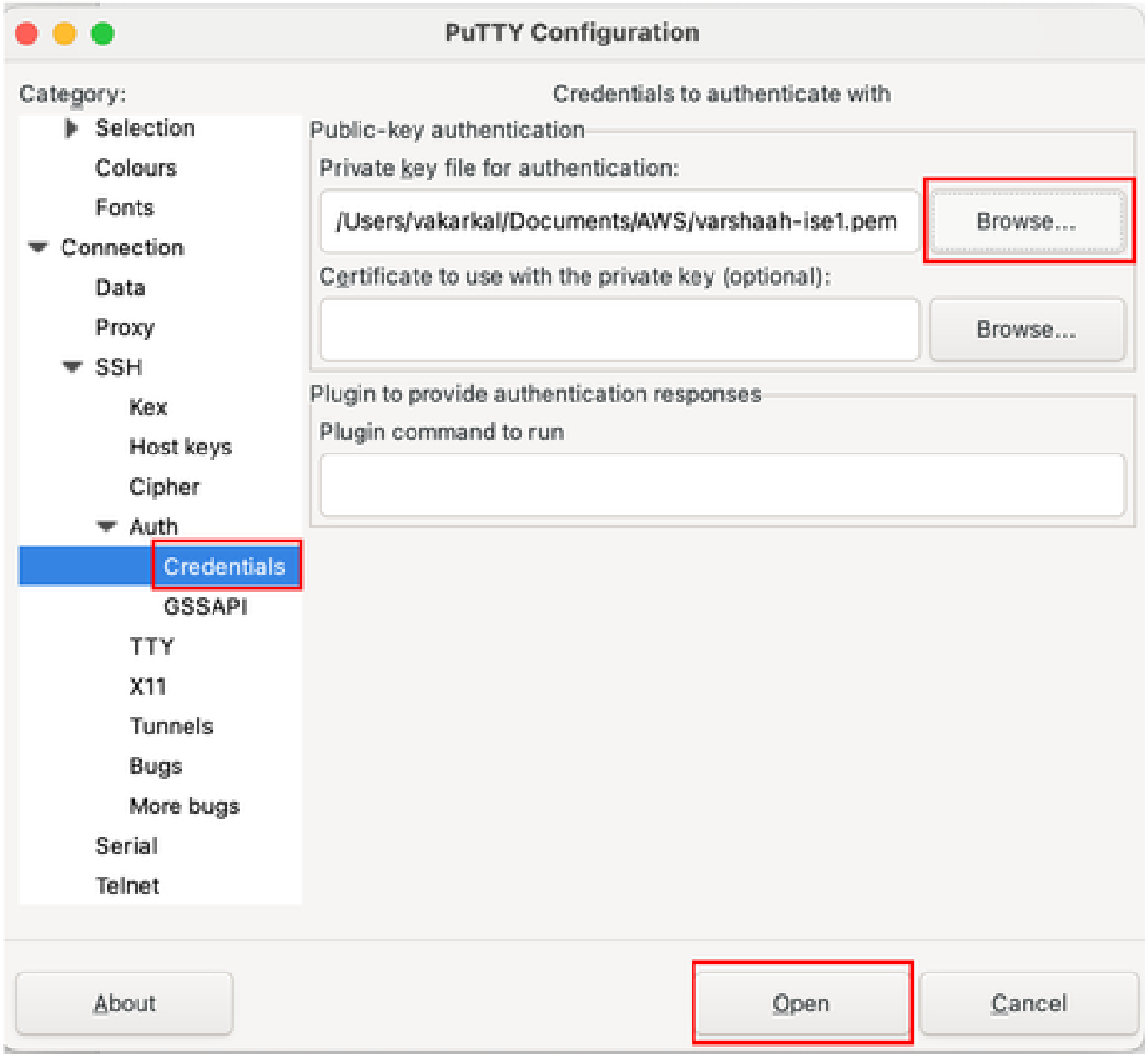
Note: Use admin como o usuário SSH, já que o Cisco ISE desabilita o login raiz via SSH.

Acessar CLI via SSH usando PuTTy

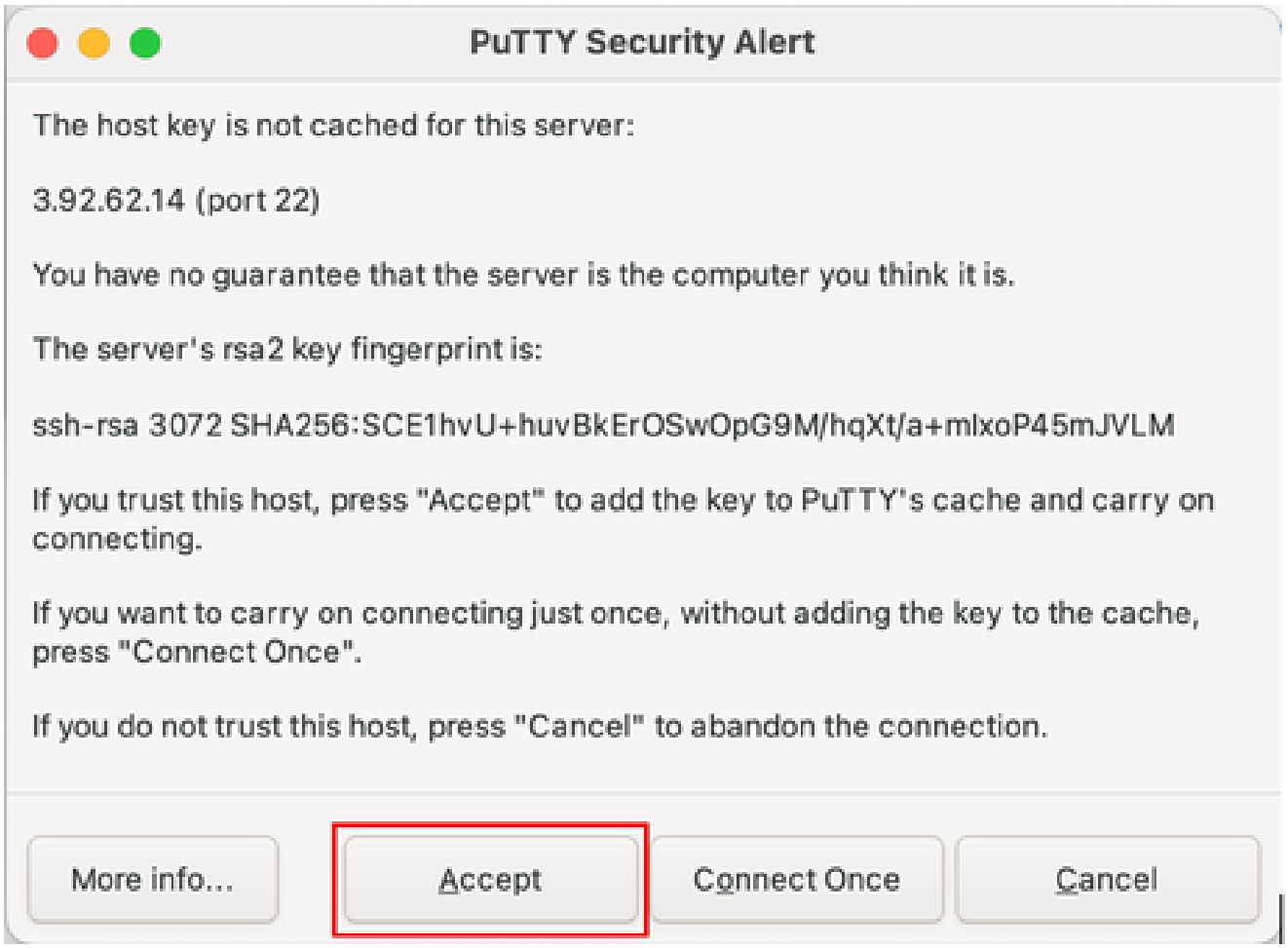
- Abra o PuTTY.
- No campo Host Name, insira: admin@<public-ip-address>



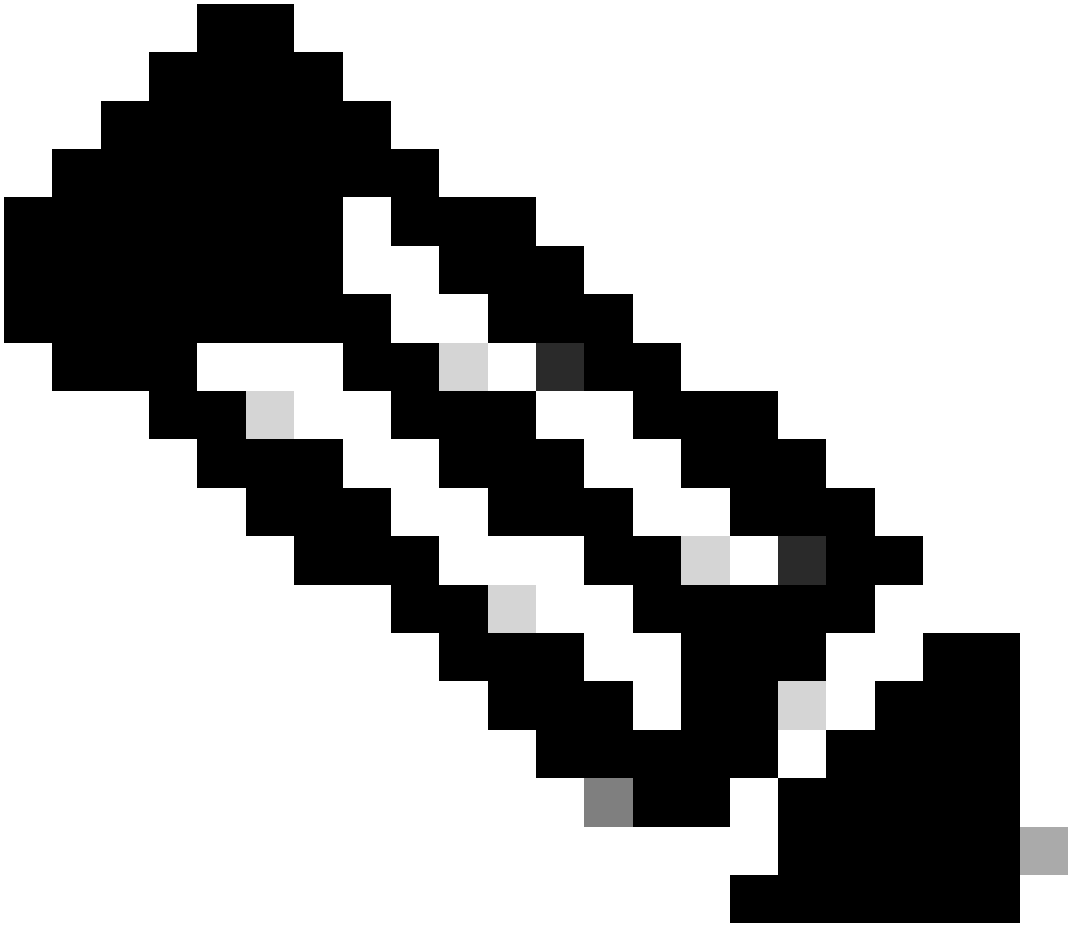
- No painel esquerdo, navegue até Connection > SSH > Auth > Credentials.
- Clique em Browse ao lado de Private key file for authentication e selecione seu arquivo de chave privada SSH.
- Clique em Abrir para iniciar a sessão.



- Quando solicitado, clique em Aceitar para confirmar a chave SSH.



- Sua sessão PuTTY agora se conecta à CLI do ISE.

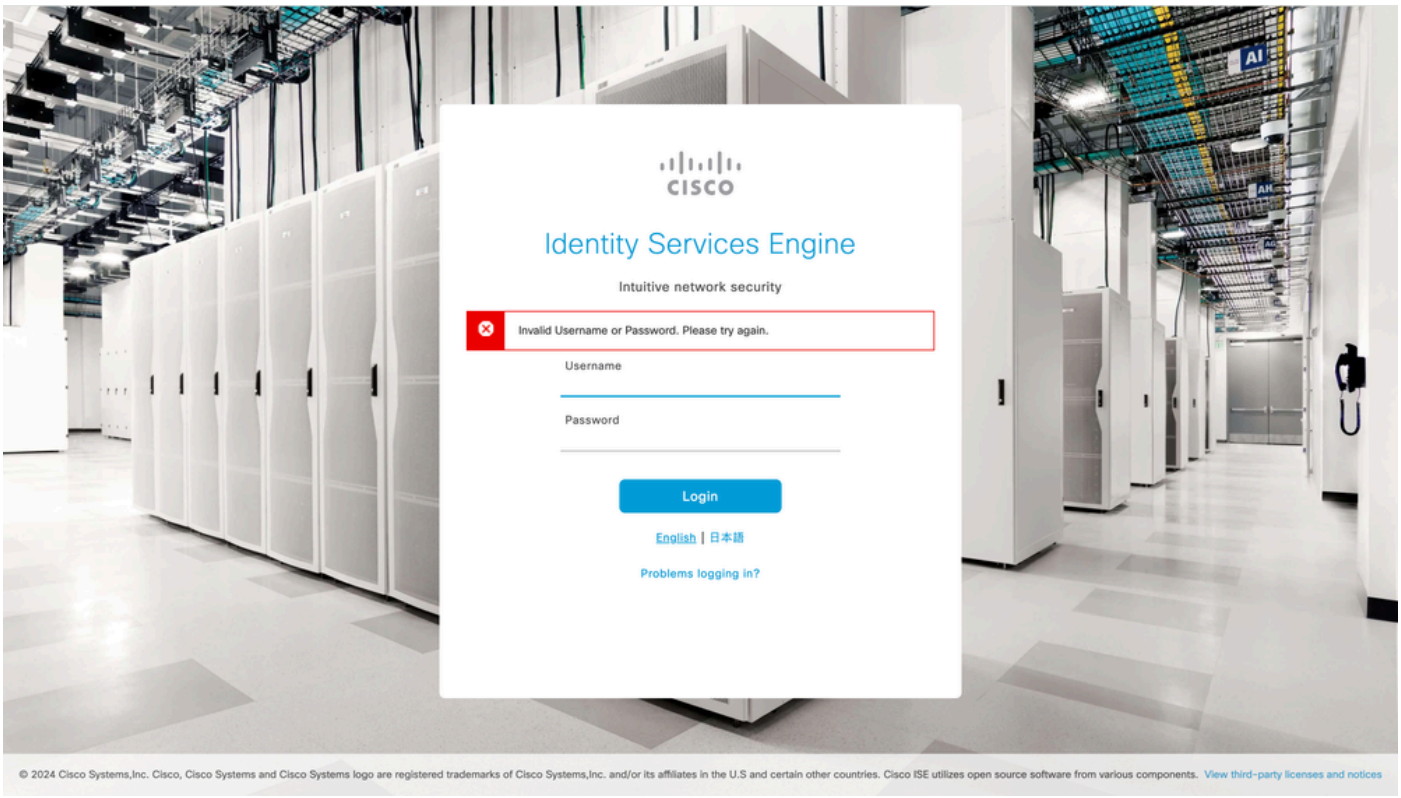


Note: Pode levar até 20 minutos para que o ISE se torne acessível via SSH. Durante esse período, as tentativas de conexão podem falhar com o erro: "Permissão negada (chave pública)."

Troubleshooting

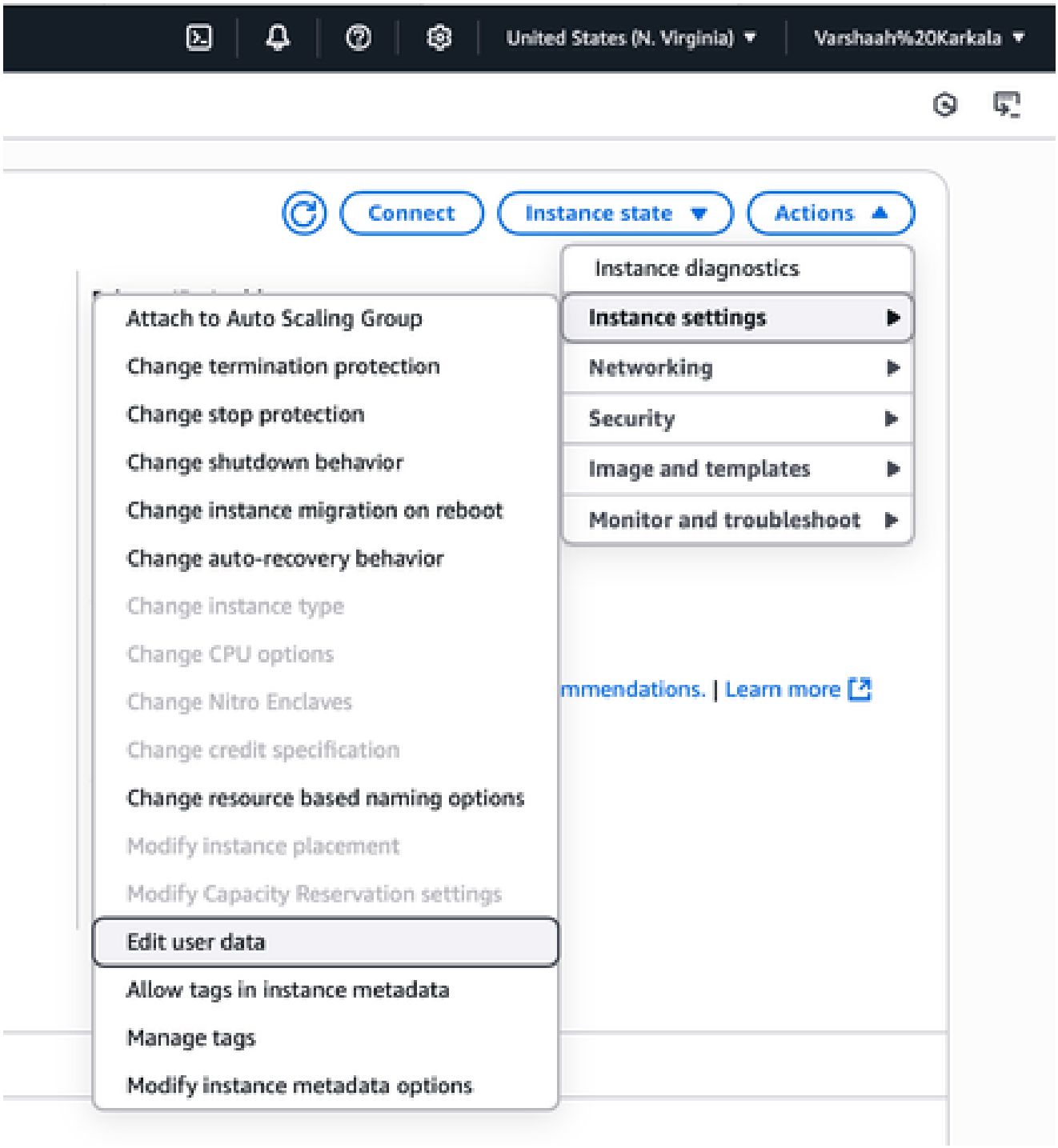
Nome de usuário ou senha inválidos

Os problemas de autenticação geralmente são causados por entrada incorreta do usuário durante a criação da instância. Isso produz uma mensagem de erro como "Nome de Usuário ou Senha Inválidos. Tente novamente." erro ao tentar fazer login na GUI.

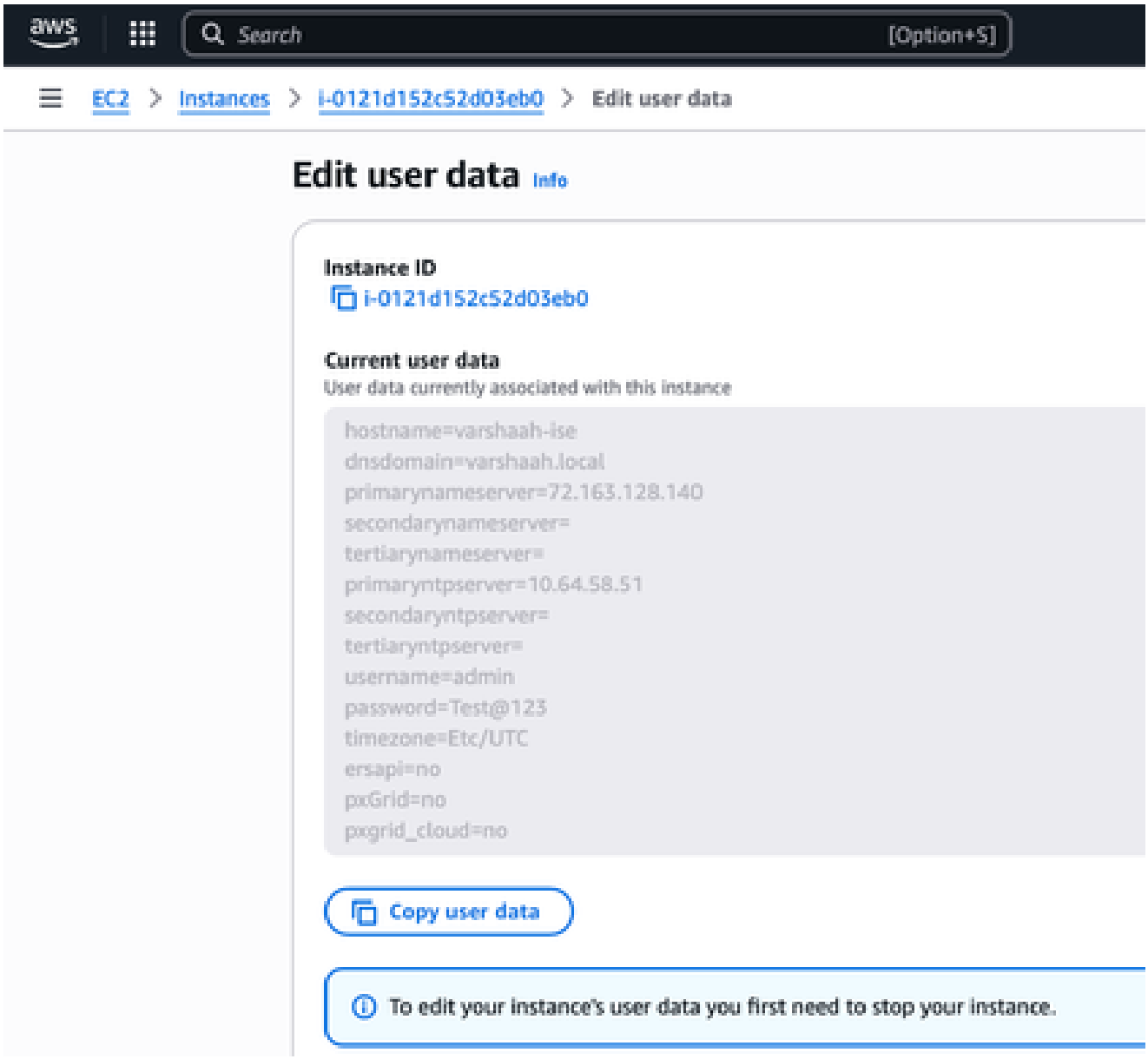


Solução

- No AWS EC2 Console, navegue para EC2 > Instâncias > your_instance_id.
- Clique em Actions e escolha Instance settings > Edit user data.



- Você pode encontrar aqui o nome de usuário e a senha específicos que foram definidos durante a inicialização da instância. Essas credenciais podem ser usadas para fazer login na GUI do ISE.



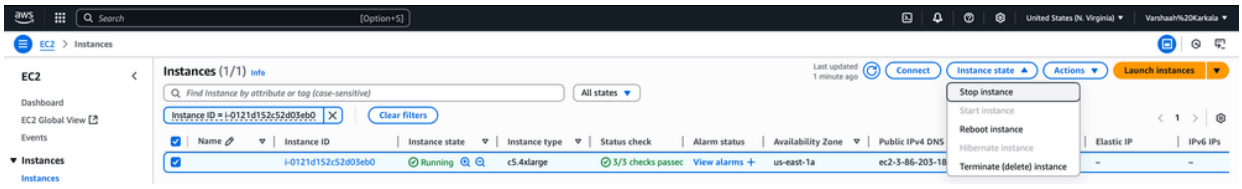
- Verifique o nome de host e a senha ao configurar o nome de host e a senha:
  - Hostname
    - Somente caracteres alfanuméricos e hífens (-) são permitidos.
    - Não deve exceder 19 caracteres de comprimento.
  - Senha
    - Deve estar em conformidade com a política de senha do Cisco ISE.
    - Consulte o Guia de administração oficial do ISE: Política de senha do ISE 3.4 - Guia do administrador da Cisco

- Se a senha configurada não atender à política de senha do ISE, as tentativas de login falharão; mesmo com as credenciais corretas.

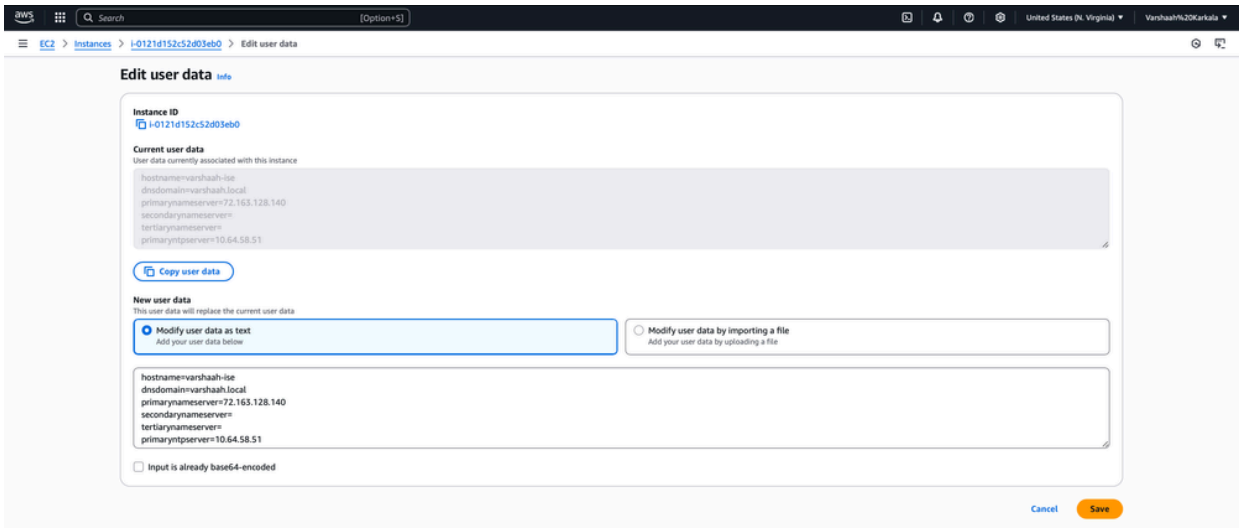
- Se você suspeitar que a senha foi configurada incorretamente, siga estas etapas para atualizá-la:

    1. No Console EC2, navegue para EC2 > Instâncias > your_instance_id

    2. Clique em Estado da instância > Parar instância.



    3. Depois que a instância for interrompida, clique em Ações > Configurações da instância > Editar dados do usuário.



    4. Modifique o script de dados do usuário para atualizar a senha de acordo.

    5. Clique em Salvar para salvar suas alterações. Clique em Estado da instância > Iniciar instância para reiniciar a instância.

Defeitos conhecidos

ID do bug	Descrição
ID de bug da Cisco 41693	O ISE no AWS não recupera os dados do usuário se a versão dos metadados estiver definida apenas como V2. Somente o IMDSv1 é

	suportado nas versões anteriores ao ISE 3.4.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.