Déployer Identity Services Engine (ISE) version 3.4 sur AWS

Table des matières

Introduction

Ce document décrit comment configurer Cisco ISE sur AWS à l'aide du modèle CloudFormation (CFT) et d'Amazon Machine Image (AMI).

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance de ces sujets avant de procéder à ce déploiement :

- Cisco Identity Services Engine (ISE)
- Gestion et mise en réseau des instances AWS EC2
- Génération et utilisation de paires de clés SSH
- Compréhension de base des VPC, des groupes de sécurité et de la configuration DNS/NTP dans AWS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Moteur du service de vérification des identités (ISE)
- Console cloud Amazon Web Services (AWS)

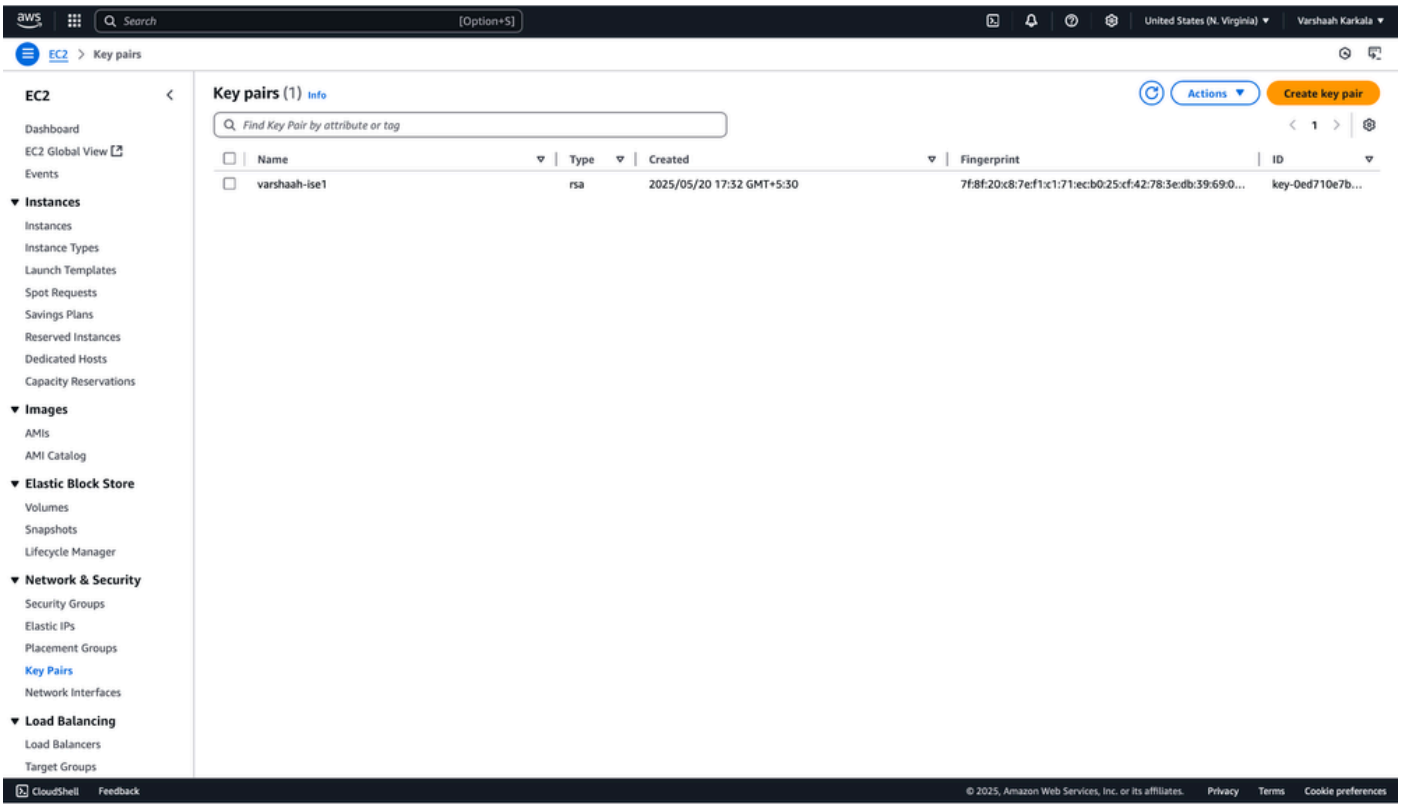
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

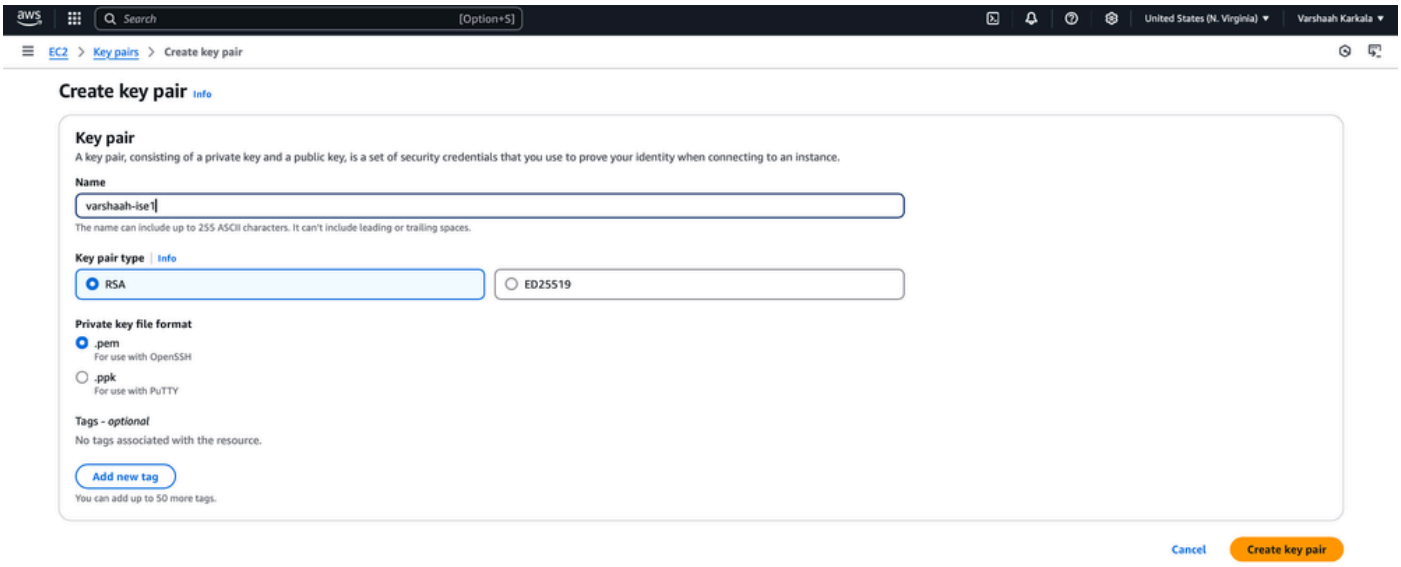
Partie 1 : Génération d'une paire de clés SSH

1. Pour ce déploiement, vous pouvez utiliser une paire de clés préexistante ou en créer une nouvelle.

2. Pour créer une nouvelle paire, accédez à EC2 > Réseau et sécurité > Paires de clés et cliquez sur Créer une paire de clés.



3. Entrez le nom de la paire de clés et cliquez sur Créer une paire de clés.

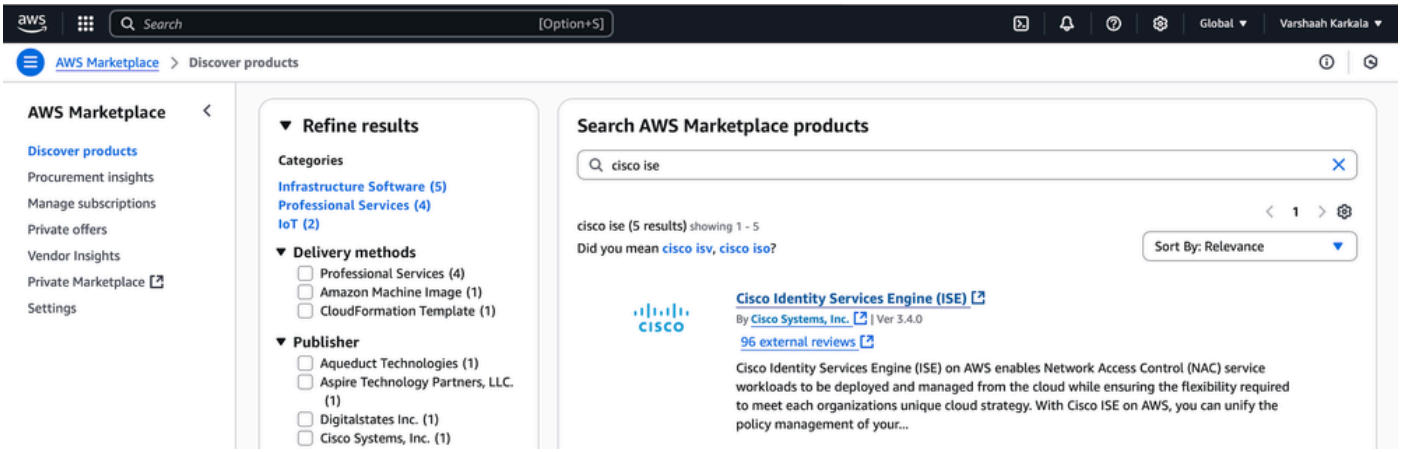


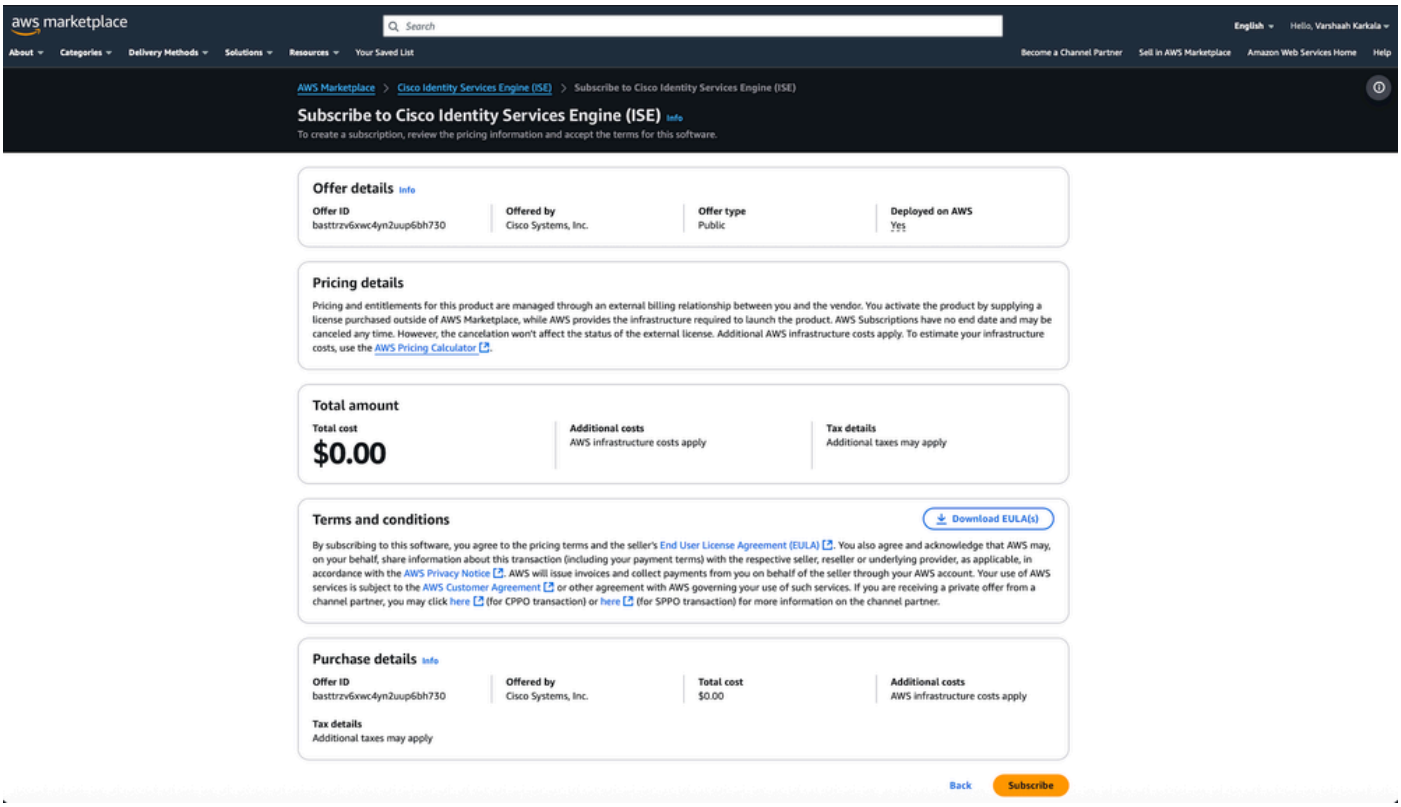
Le fichier de paire de clés (.pem) est téléchargé sur votre ordinateur local. Assurez-vous que vous protégez ce fichier, car c'est la seule façon d'accéder à votre instance EC2 une fois qu'elle est lancée.

Partie 2 : Configuration d'ISE à l'aide d'un modèle CloudFormation (CFT)

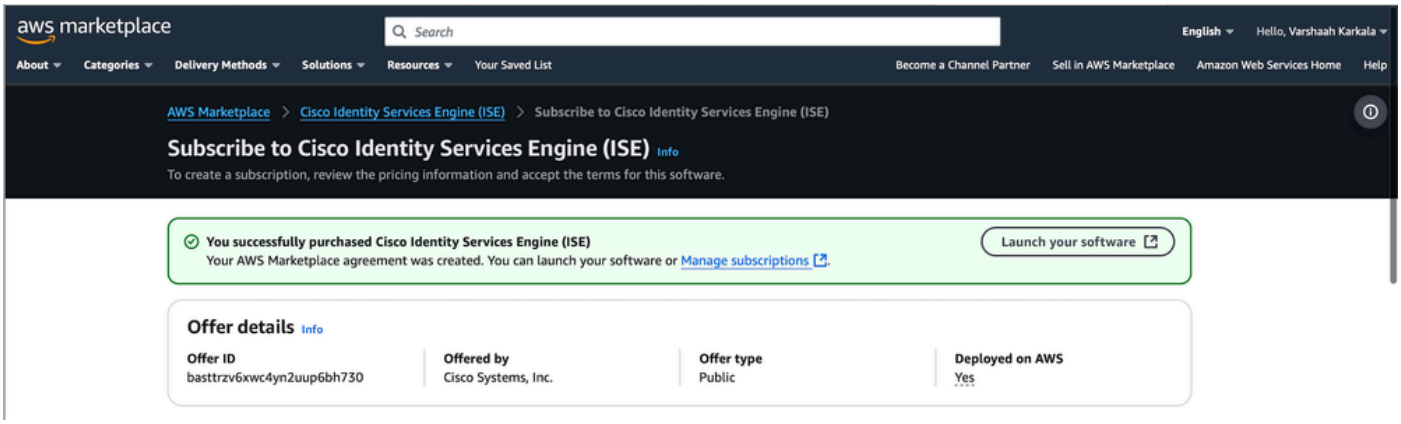
1. Connectez-vous à la console de gestion AWS et recherchez les abonnements AWS Marketplace.

2. Dans la barre de recherche, tapez cisco ise et cliquez sur Cisco Identity Services Engine (ISE) dans les résultats. Cliquez sur Subscribe.

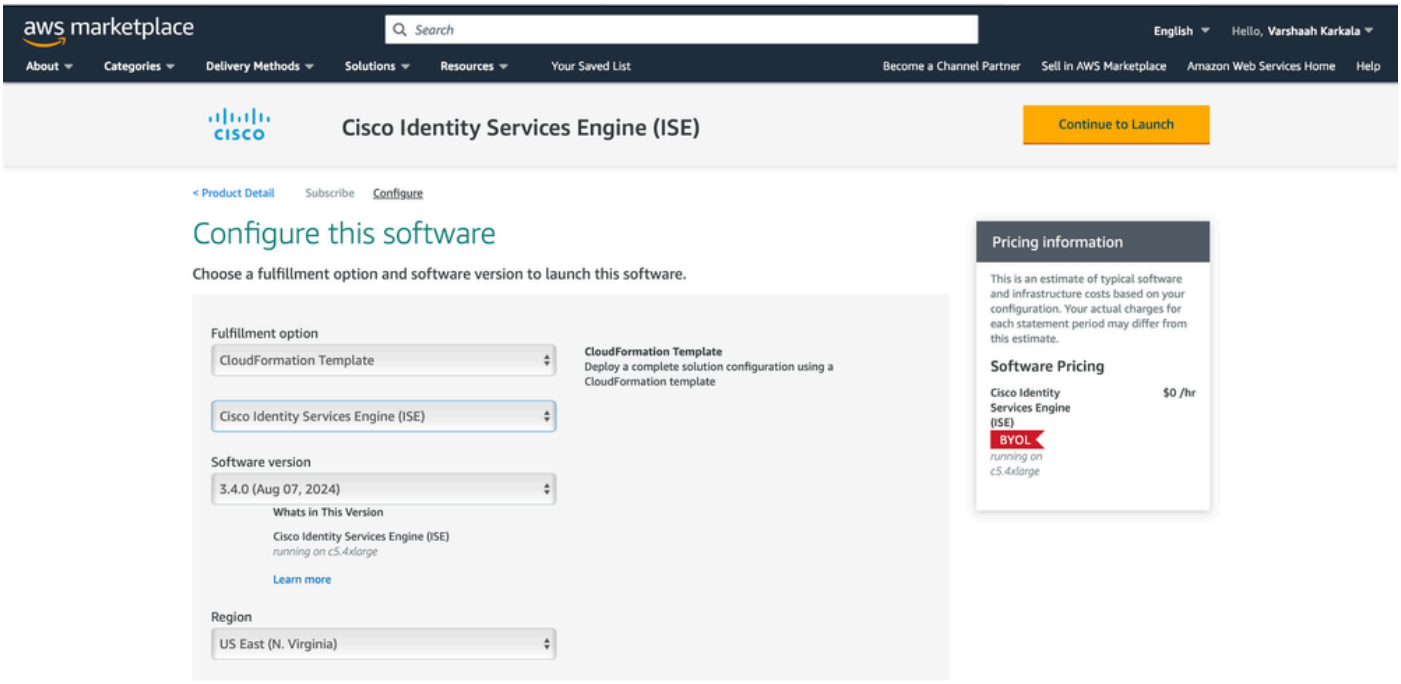




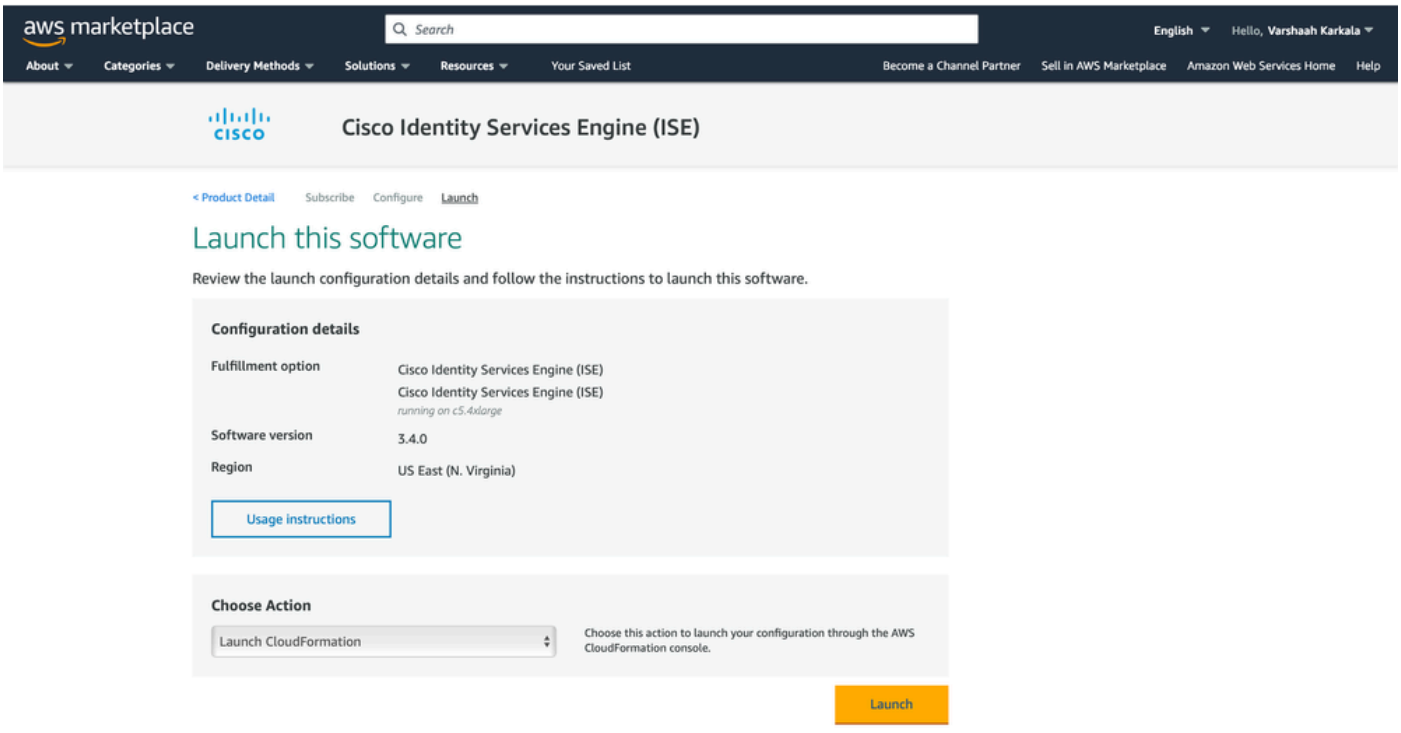
3. Après l'abonnement, cliquez sur Launch Your Software.



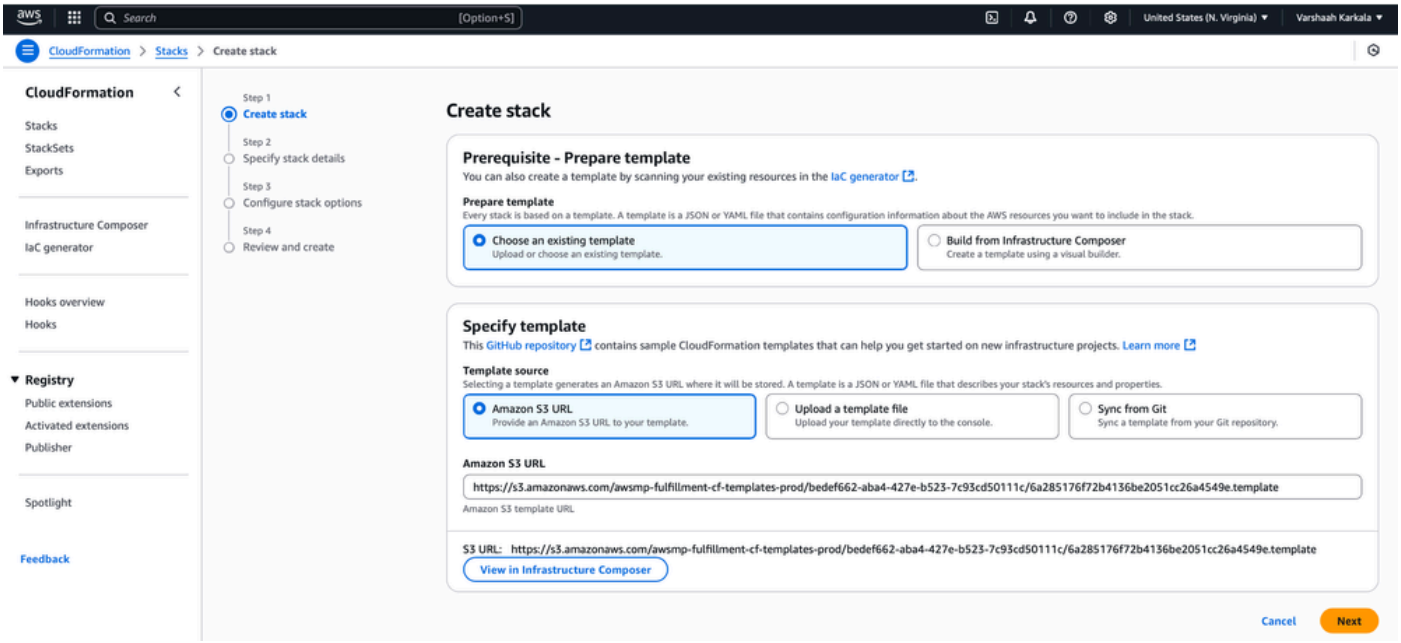
4. Sous Fulfillment Option, sélectionnez CloudFormation Template. Sélectionnez la version du logiciel (version ISE) et la région où vous souhaitez déployer l'instance. Cliquez sur Continuer pour lancer.



5. Sur la page suivante, choisissez Launch CloudFormation comme action et cliquez sur Launch.

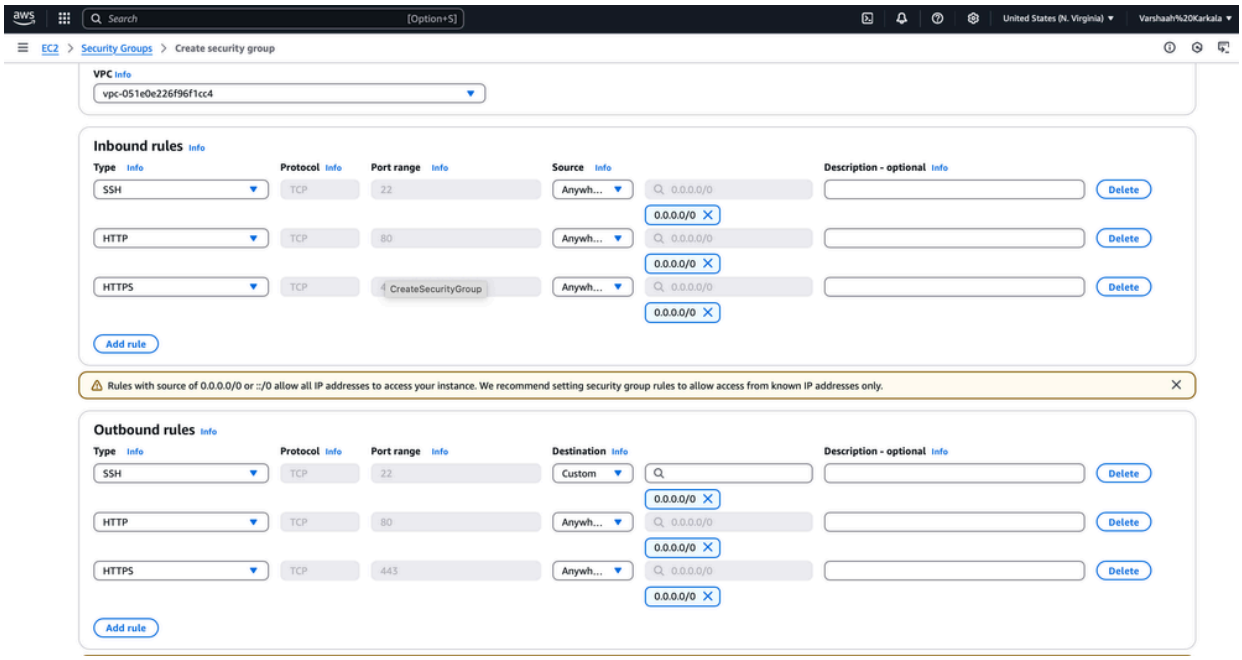


6. Sous les paramètres de la pile, conservez les paramètres par défaut et cliquez sur Suivant.



7. Entrez les paramètres requis :

- Nom de la pile : Entrez un nom unique pour votre pile.
- Nom de l'hôte: Attribuez le nom d'hôte du noeud ISE.
- Paire de clés : Sélectionnez la paire de clés générée ou préexistante pour accéder ultérieurement à l'instance EC2.
- Groupe de sécurité de gestion :
    - Utilisez le groupe de sécurité par défaut (comme illustré) ou créez-en un personnalisé via le tableau de bord EC2.
    - Pour créer un nouveau groupe de sécurité, accédez au tableau de bord EC2 et à Réseau et sécurité > Groupes de sécurité pour créer un nouveau groupe de sécurité.
    - Cliquez sur Create security group et entrez les détails requis.
    - Assurez-vous que le groupe de sécurité est configuré pour autoriser le trafic entrant et sortant requis. Par exemple, activez l'accès SSH (port 22) à partir de votre adresse IP pour l'accès CLI.

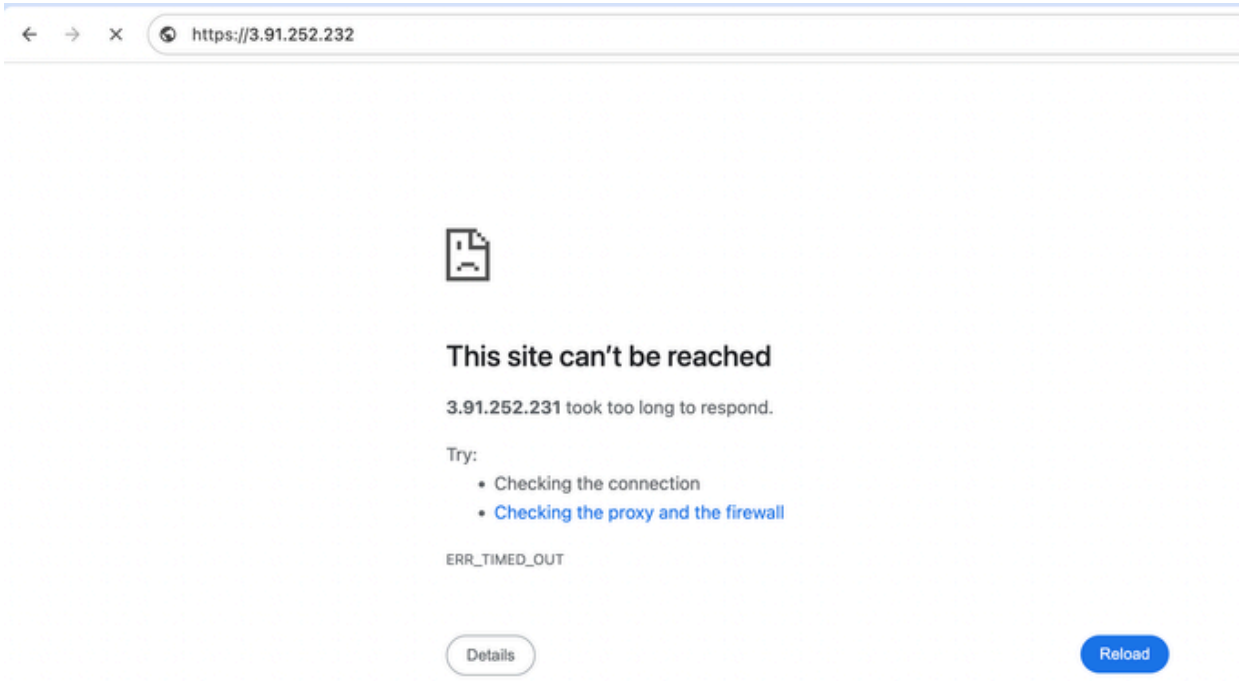


- Si l'accès SSH n'est pas correctement configuré, vous pouvez rencontrer une erreur « Operation timed out » lors de la tentative de connexion via SSH.

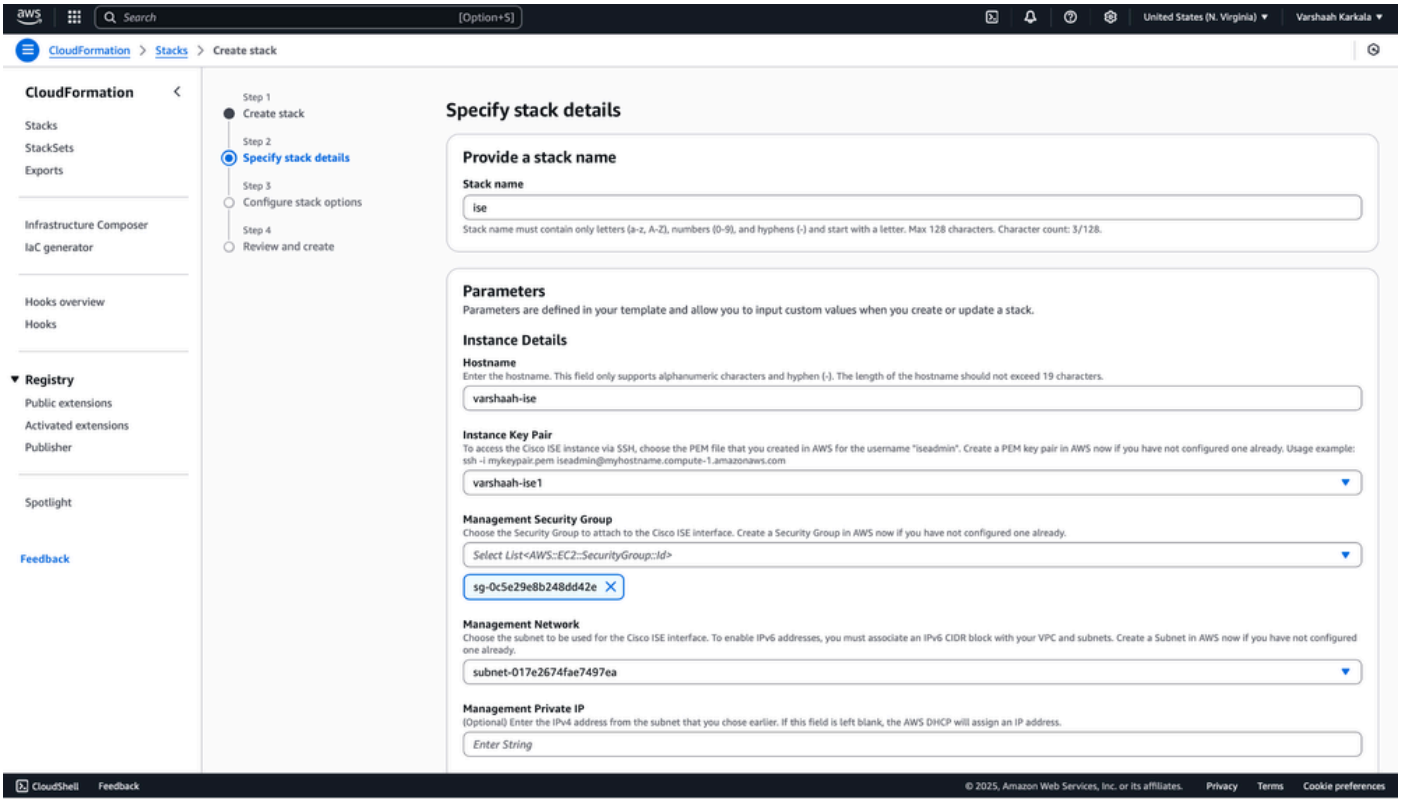
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

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

- Si l'accès HTTP/HTTPS n'est pas configuré, une erreur « Ce site n'est pas accessible » peut s'afficher lors de la tentative d'accès à l'interface utilisateur graphique.



- Management Network : l'un des sous-réseaux préexistants est sélectionné.



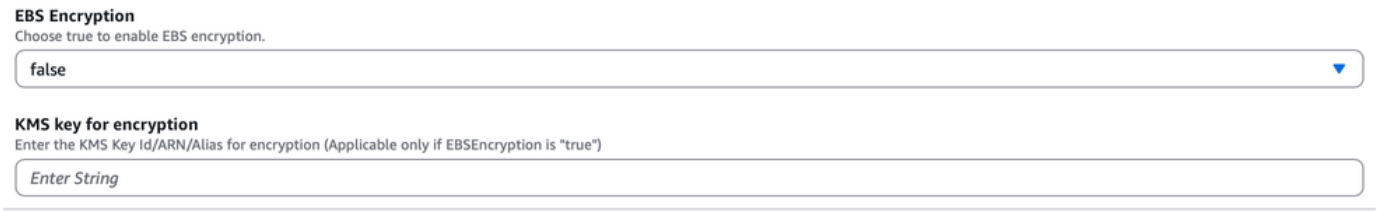
Si votre conception nécessite un déploiement distribué avec certains noeuds hébergés dans AWS et d'autres sur site, configurez un VPC dédié avec un sous-réseau privé et établissez un tunnel VPN vers le périphérique de tête de réseau VPN sur site pour permettre la connectivité entre les noeuds ISE hébergés par AWS et sur site.

Pour connaître les étapes détaillées de configuration du périphérique de tête de réseau VPN,

reportez-vous à ce guide.

8. Cryptage EBS

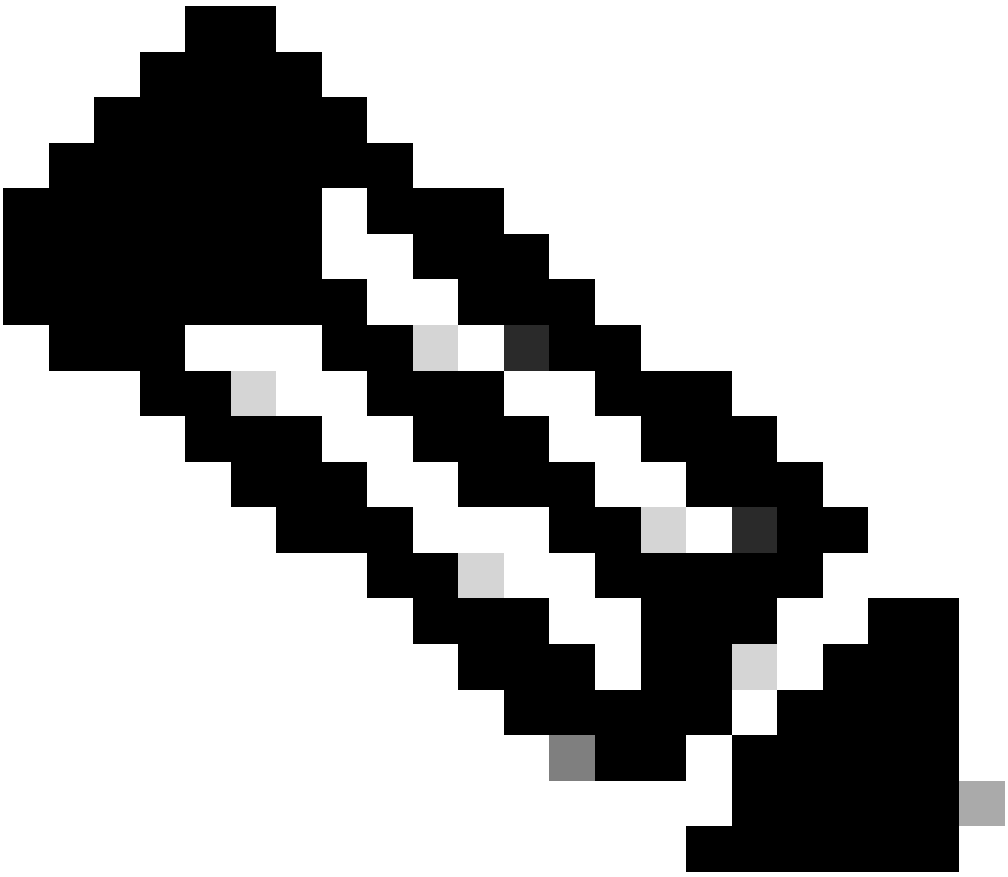
- Faites défiler vers le bas pour localiser les paramètres de cryptage EBS.
- Définissez EBS Encryption sur False, sauf si vous avez des besoins spécifiques en matière de cryptage.



9. Configuration du réseau :

- Faites défiler vers le bas pour accéder aux options de configuration des paramètres réseau, tels que le domaine DNS, le serveur de noms principal et le serveur NTP principal.

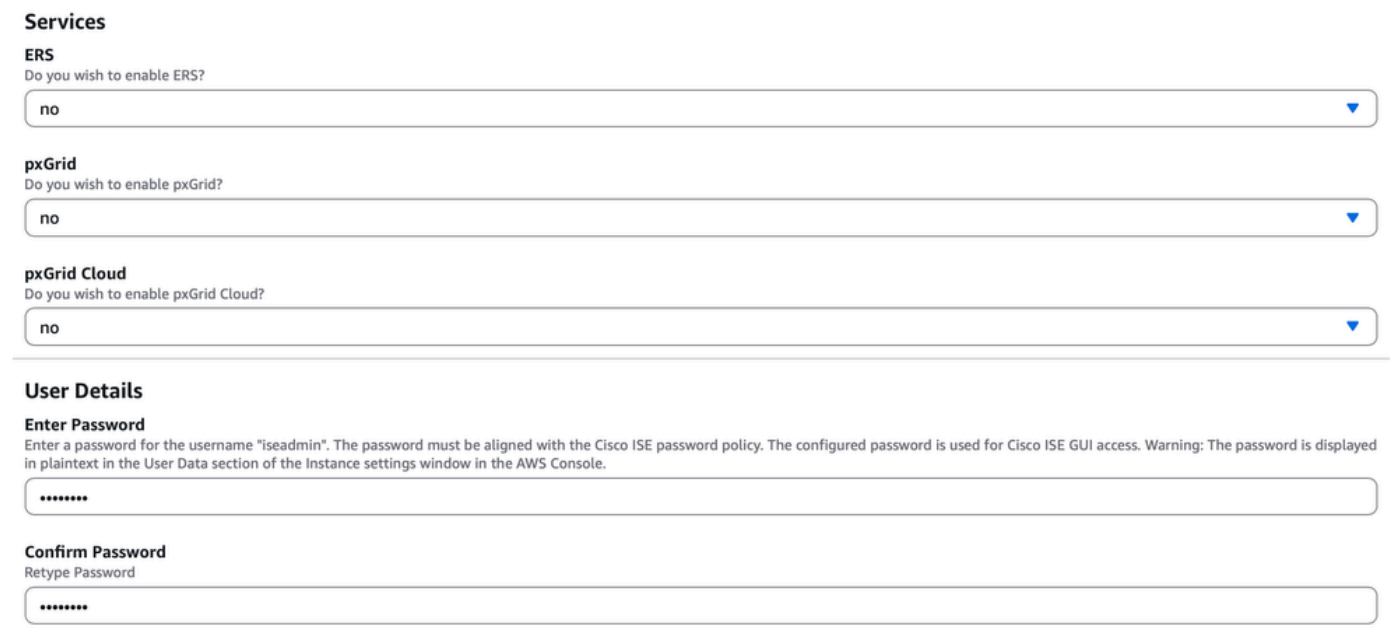
  Assurez-vous que ces valeurs sont saisies correctement.



Remarque : Une syntaxe incorrecte peut empêcher le démarrage correct des services ISE après le déploiement.

10. Détails du service et de l'utilisateur :

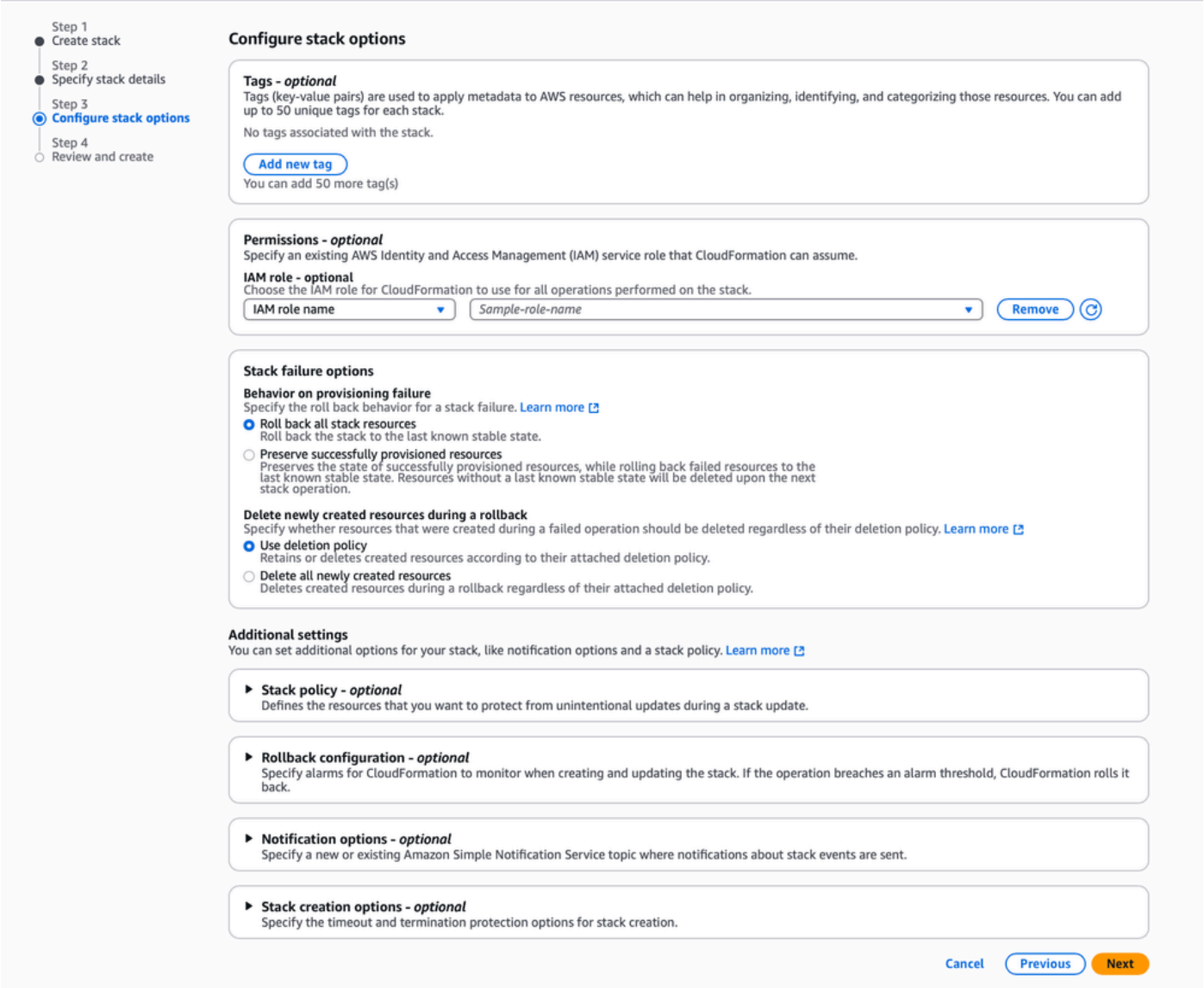
- Faites défiler vers le bas pour localiser l'option permettant d'activer les services ERS et pxGrid
- Choisissez d'activer les services ERS et pxGrid en sélectionnant yes ou no.
- Sous User Details, définissez le mot de passe de l'utilisateur admin par défaut.



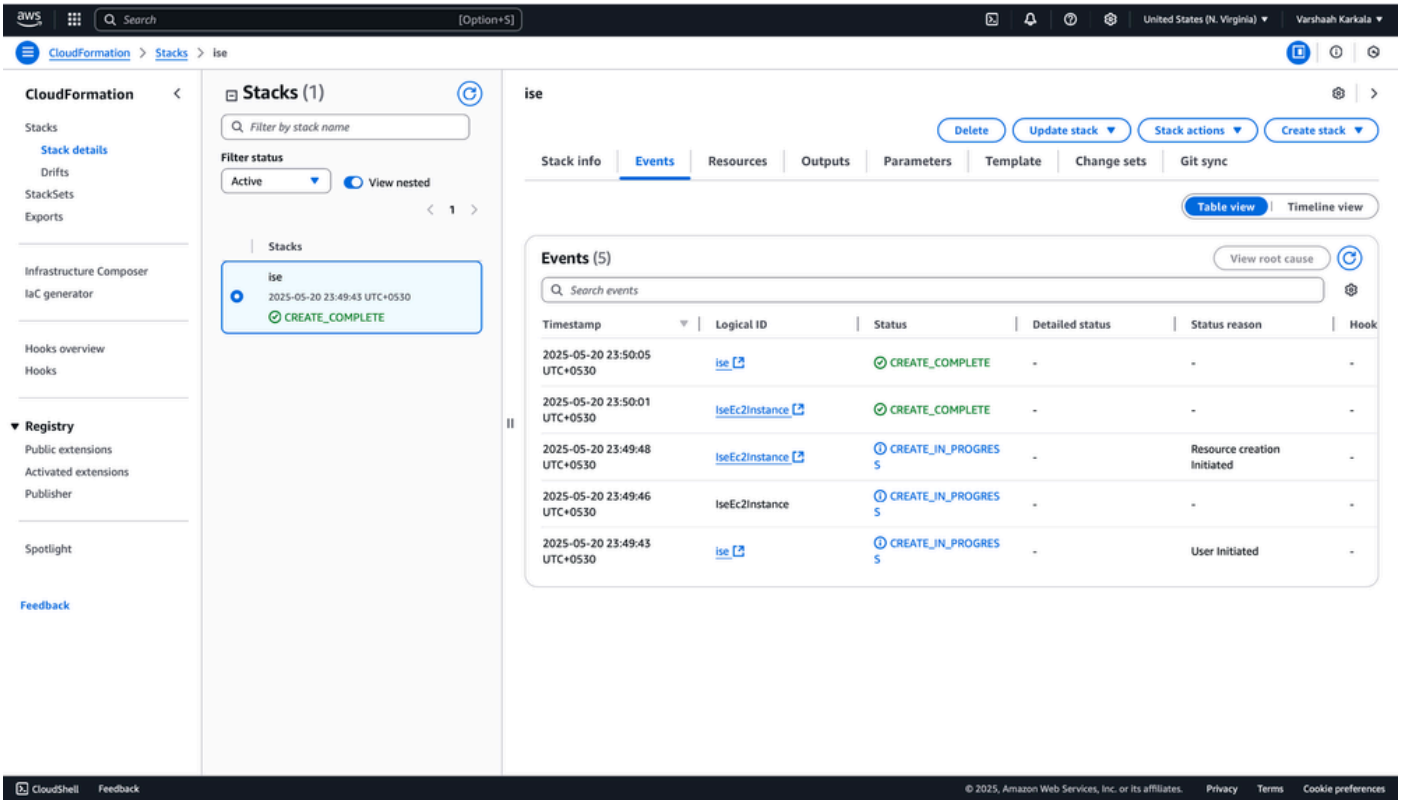
- Cliquez sur Next (Suivant).

11. Configurez les options de la pile :

- Conservez toutes les options par défaut et cliquez sur Next.



12. Vérifiez le modèle pour vous assurer que toutes les configurations sont correctes, puis cliquez sur Soumettre. Une fois le modèle créé, il ressemble à l'exemple ci-dessous :



13. Accédez aux détails de la pile :
Accédez à CloudFormation > Stacks et localisez votre pile déployée.

14. Onglet Afficher les résultats :

Sélectionnez votre pile et ouvrez l'onglet Sorties. Vous y trouverez des informations importantes générées au cours du processus de déploiement, telles que :

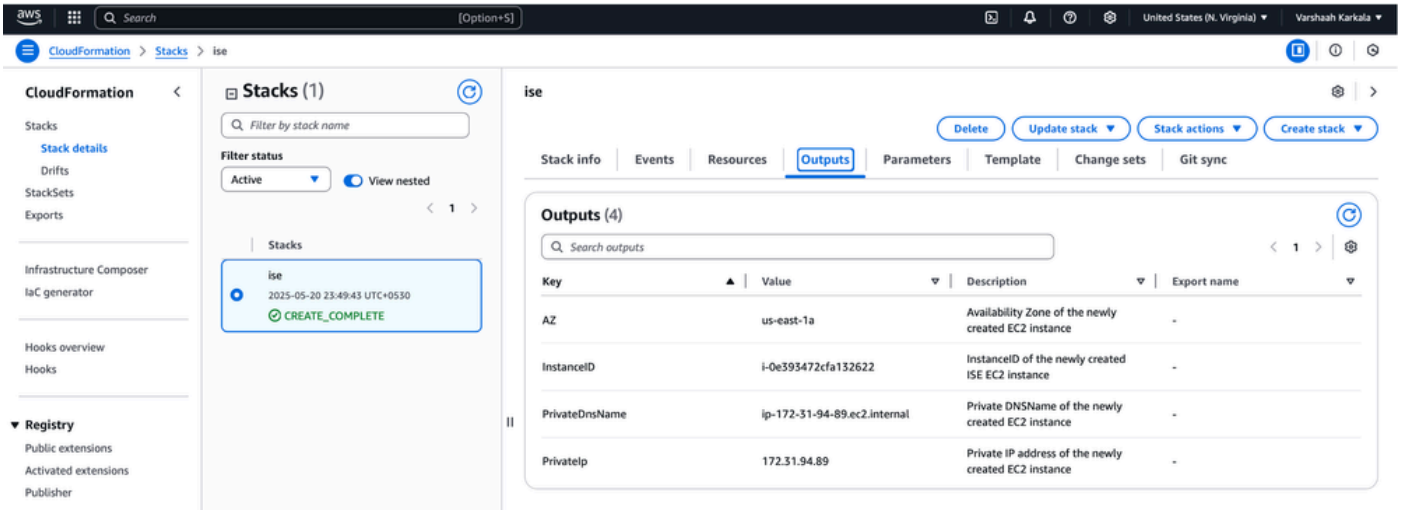
· Zone de disponibilité : Région dans laquelle les ressources sont déployées.

· ID d'instance : Identificateur unique de l'instance déployée.

· Nom DNS : Nom DNS privé de l'instance, qui peut être utilisé pour l'accès à distance.

•Adresse IP : Adresse IP publique ou privée de l'instance, selon votre configuration.

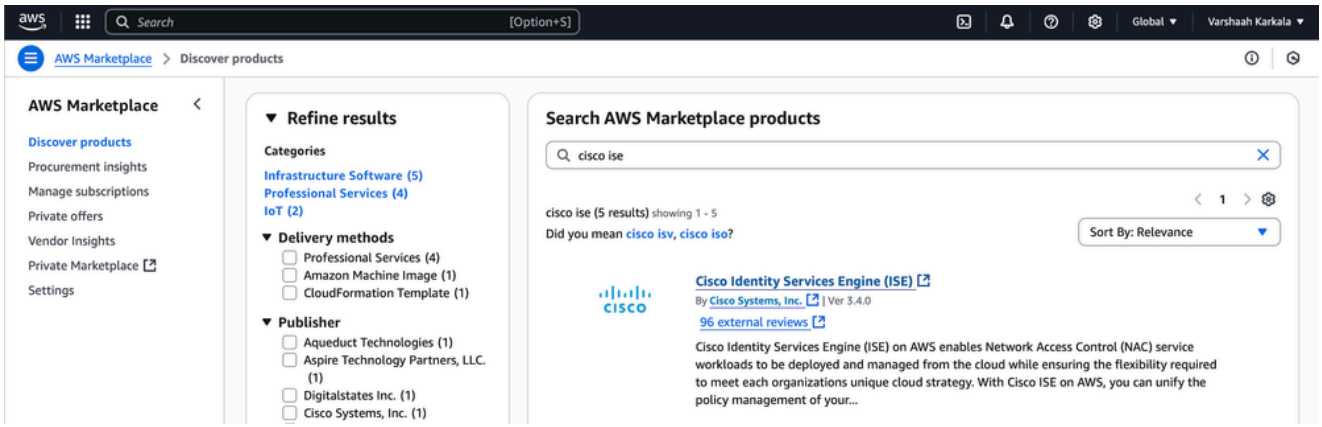
Ces informations vous aident à vous connecter à l'instance et à vérifier sa disponibilité. L'onglet Sorties ressemble à cet exemple :



Partie 3 : Configuration d'ISE à l'aide d'une image de machine Amazon (AMI)

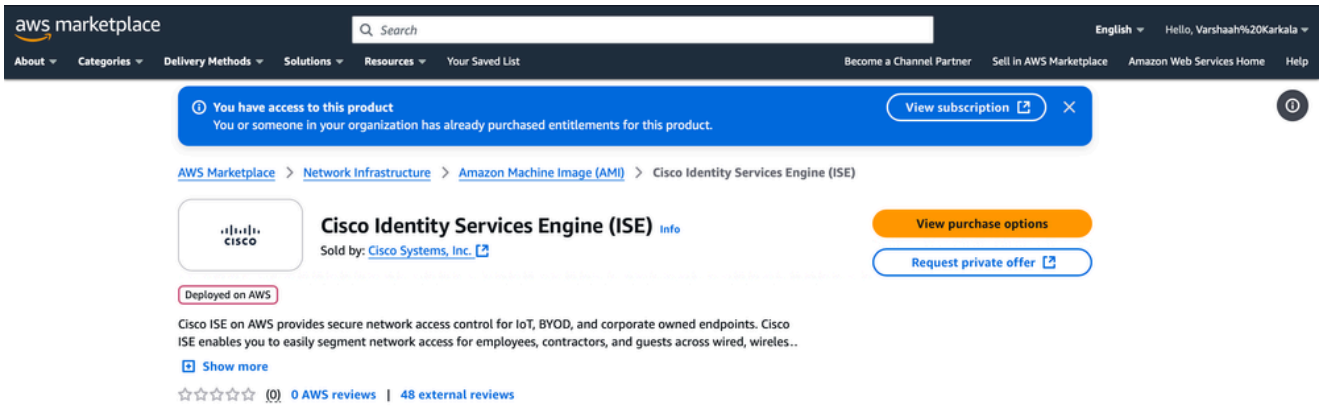
1. Connectez-vous à la console de gestion AWS et recherchez les abonnements AWS Marketplace.

2. Dans la barre de recherche, tapez cisco ise et cliquez sur Cisco Identity Services Engine (ISE) dans les résultats.

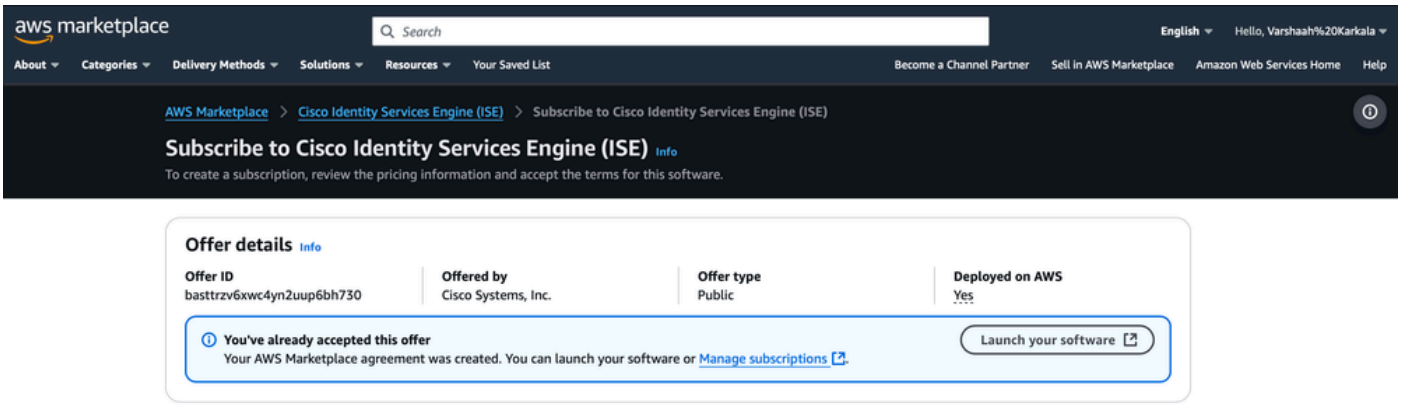


ISE sur AWS Marketplace

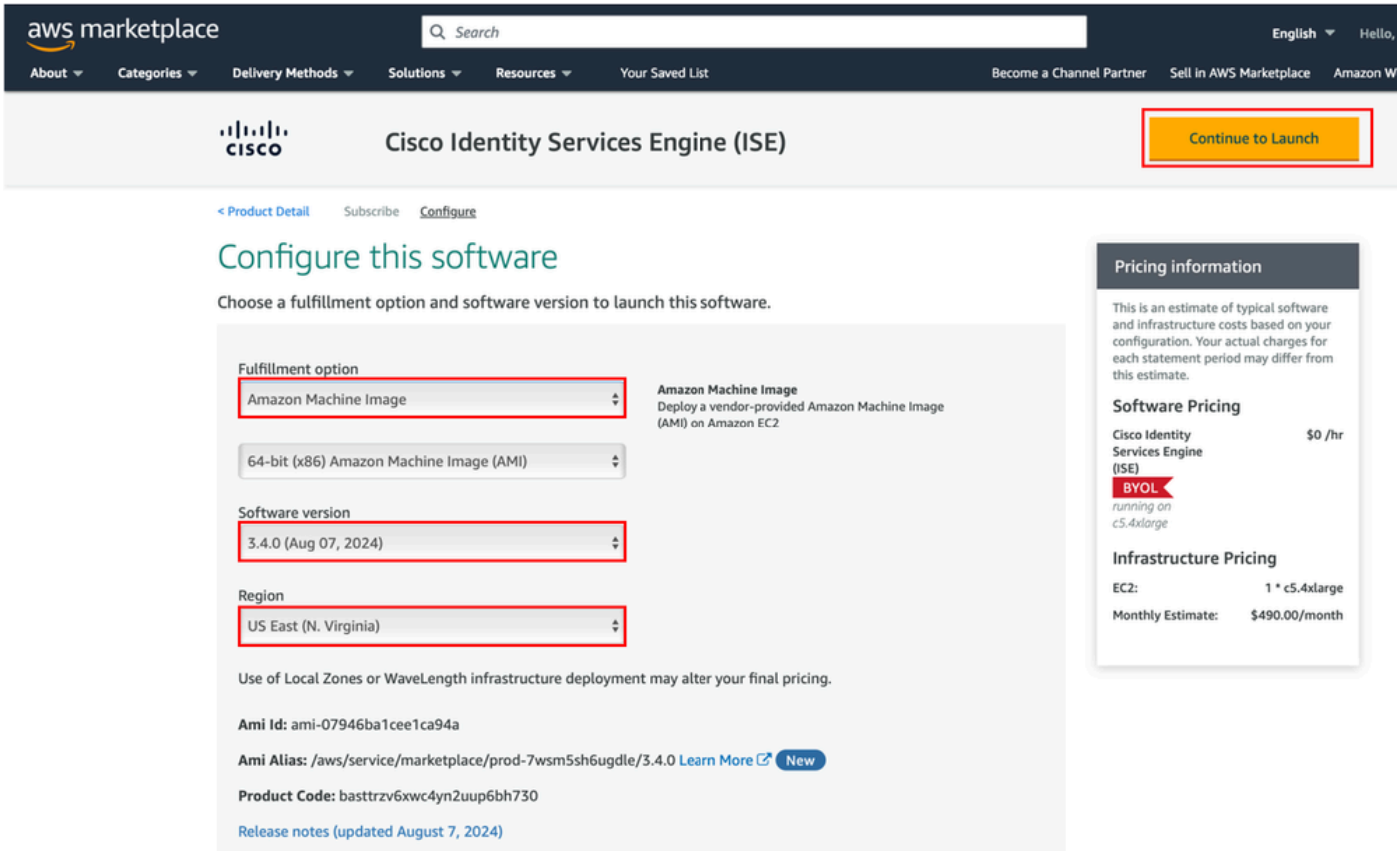
3. Cliquez sur Afficher les options d'achat.



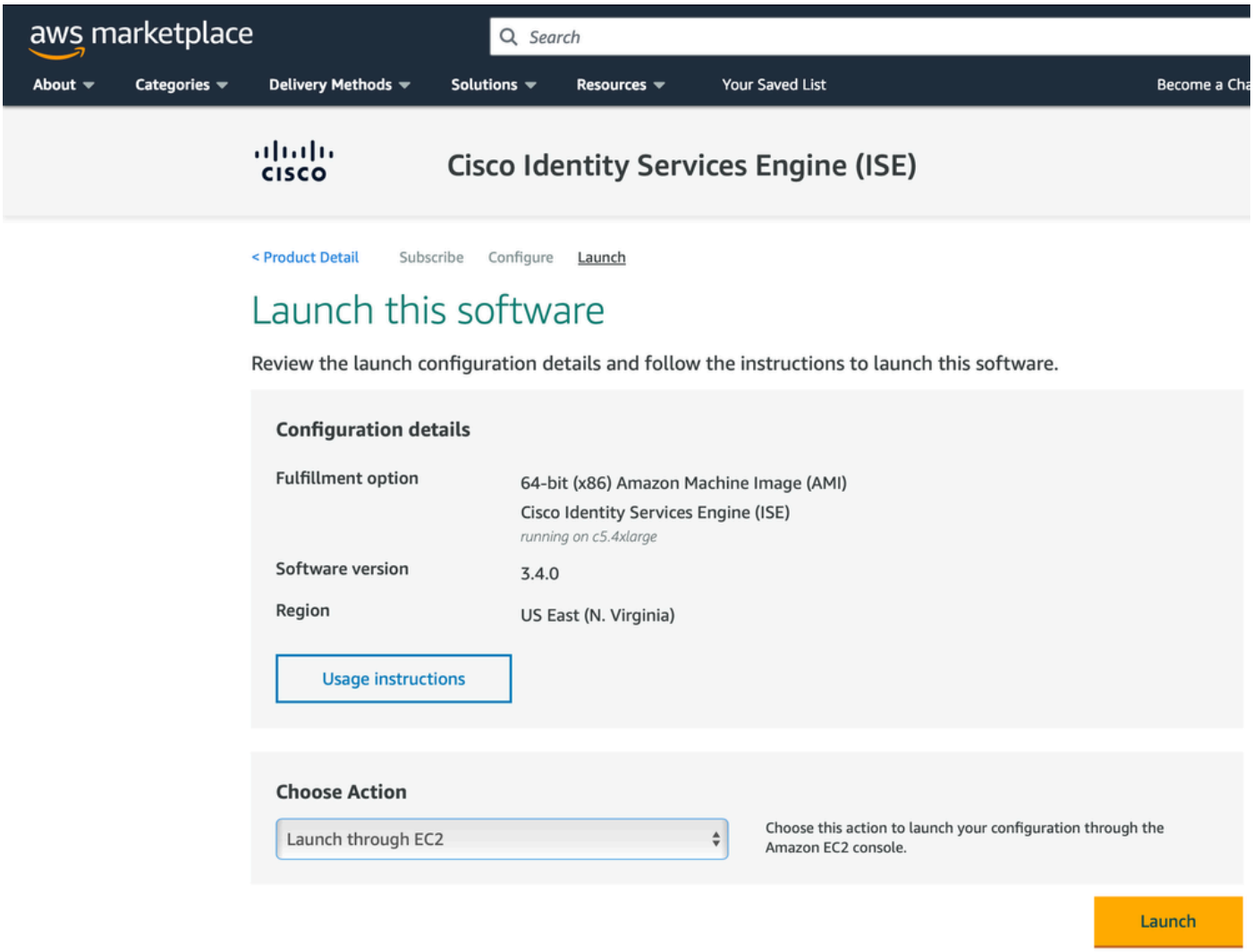
4. Cliquez sur Launch your software.



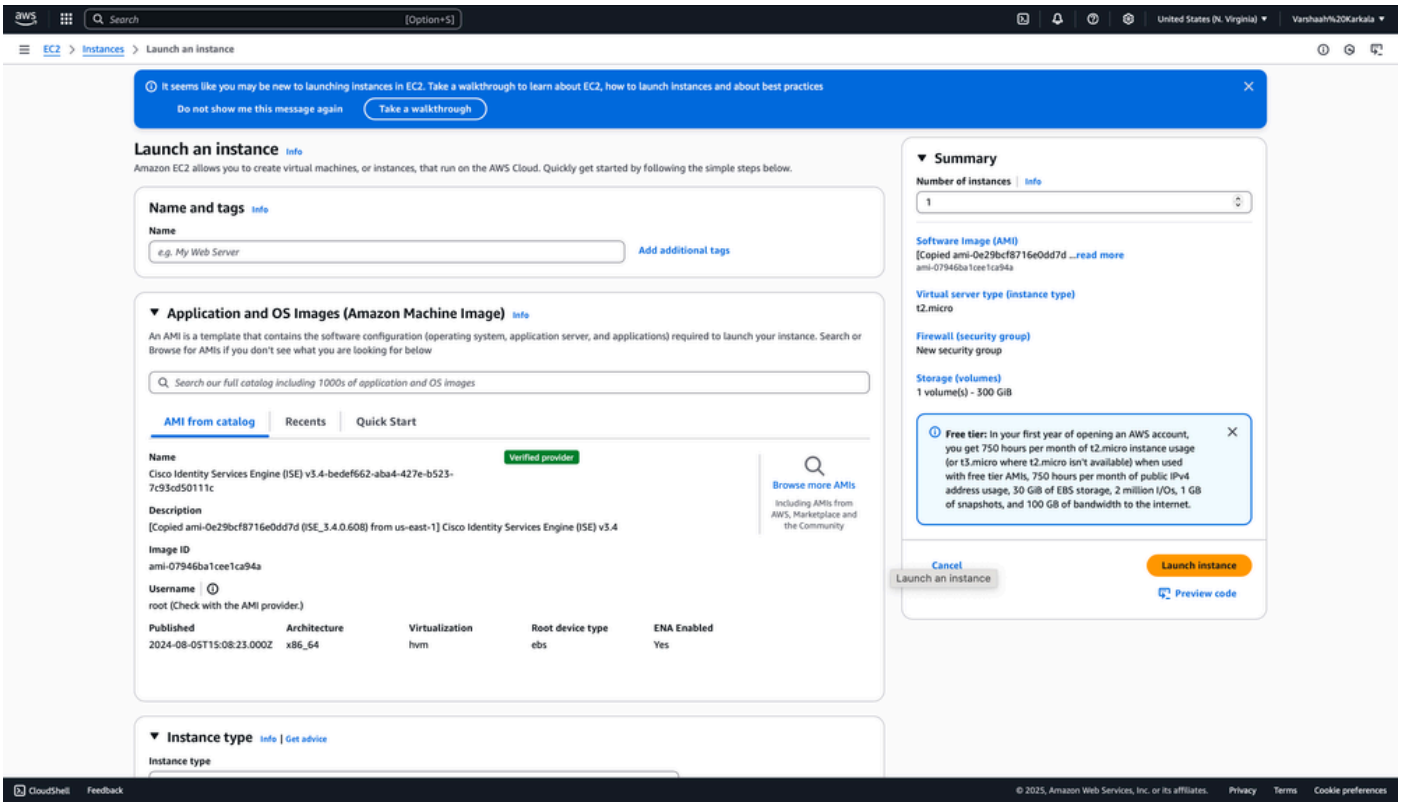
5. Sous l'option d'exécution, choisissez Amazon Machine Image. Choisissez la version et la région du logiciel souhaitées. Cliquez sur Continuer pour lancer.



6. Sous Choisir une action, choisissez Lancer via EC2. Cliquez sur Lancer pour continuer.



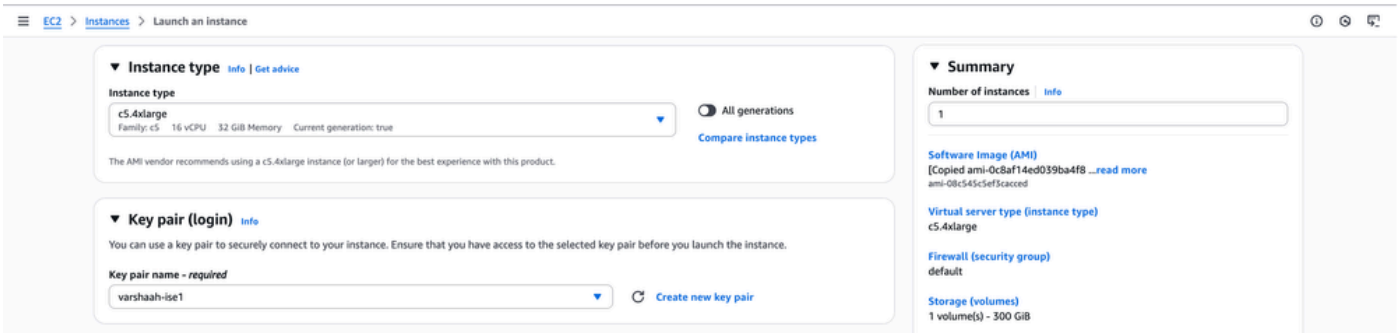
7. Vous êtes redirigé vers la page EC2 Launch an Instance pour configurer vos paramètres d'instance.



8. Faites défiler jusqu'à la section Type d'instance et choisissez un type d'instance approprié en fonction de vos besoins de déploiement.

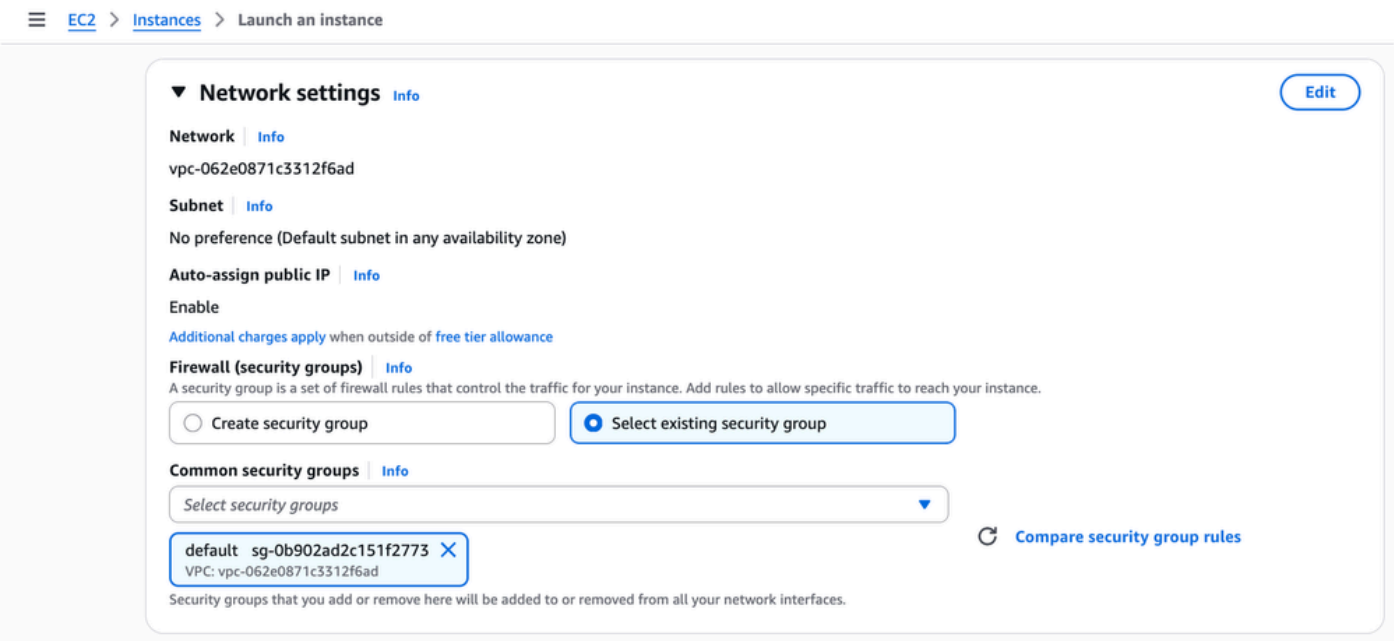
Sous Paire de clés (connexion), sélectionnez la paire de clés qui a été générée précédemment ou créez-en une nouvelle (reportez-vous aux étapes de création de paires de clés fournies précédemment).

Définissez le nombre d'instances sur 1.



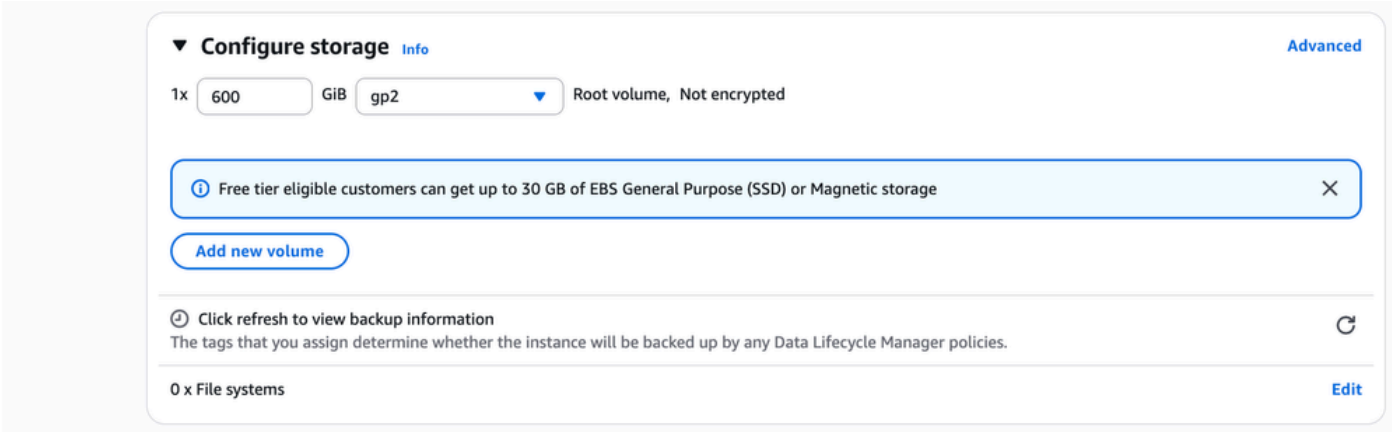
9. Dans la section Paramètres réseau :

- Configurez votre VPC et votre sous-réseau selon les besoins.
- Pour le groupe de sécurité, sélectionnez un groupe existant ou créez un nouveau groupe (comme indiqué dans l'exemple).



10. Dans la section Configurer le stockage, configurez la taille de volume souhaitée.

Exemple : 600 Go en utilisant le type de volume gp2.



11. Dans la section Détails avancés, configurez les paramètres supplémentaires requis pour votre déploiement, tels que le profil d'instance IAM, les données utilisateur ou le comportement d'arrêt.

▼ **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 ▼

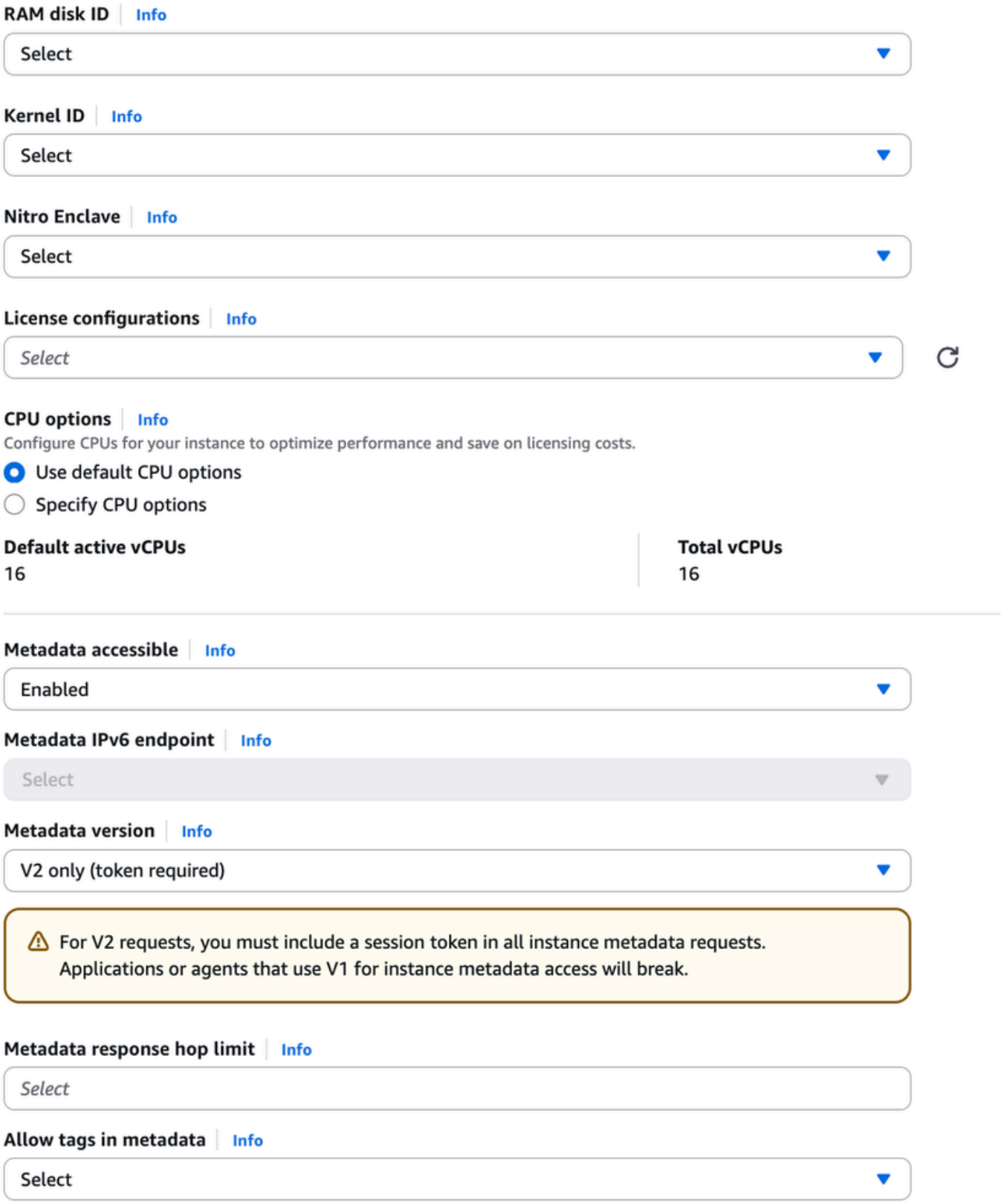
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. Dans la section Version des métadonnées :

- Pour ISE version 3.4 et ultérieure, choisissez V2 only (token required) - c'est l'option recommandée.
- Pour les versions d'ISE antérieures à 3.4, choisissez V1 et V2 (jeton facultatif) pour assurer la compatibilité.



13. Dans le champ Données utilisateur, fournissez les paramètres de configuration initiale pour l'instance ISE, notamment le nom d'hôte, le DNS, le serveur NTP, le fuseau horaire, ERS et les informations d'identification de l'administrateur.

Exemple :
hostname=varshaahise2

primarynameserver=x.x.x.x

dnsdomain=varshaah.local

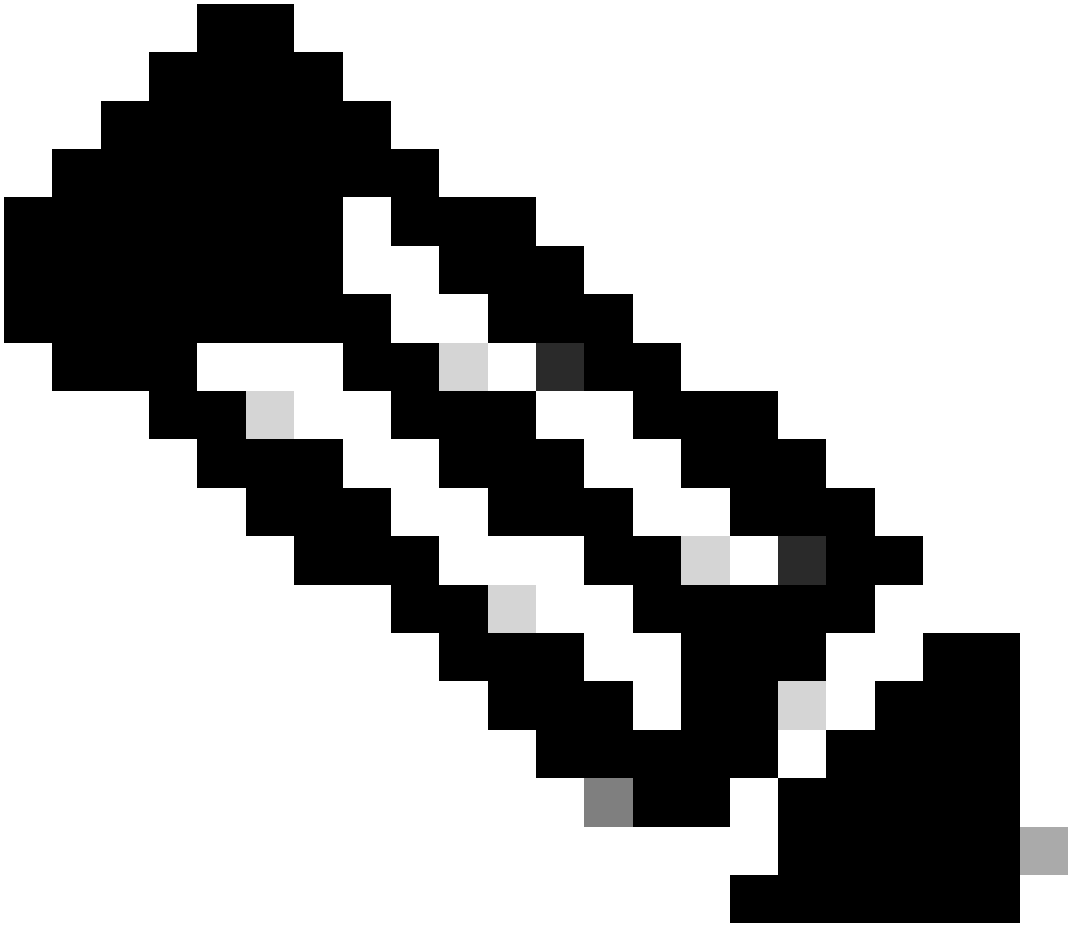
ntpserver=x.x.x.x

timezone=Asie/Calcutta

username=admin

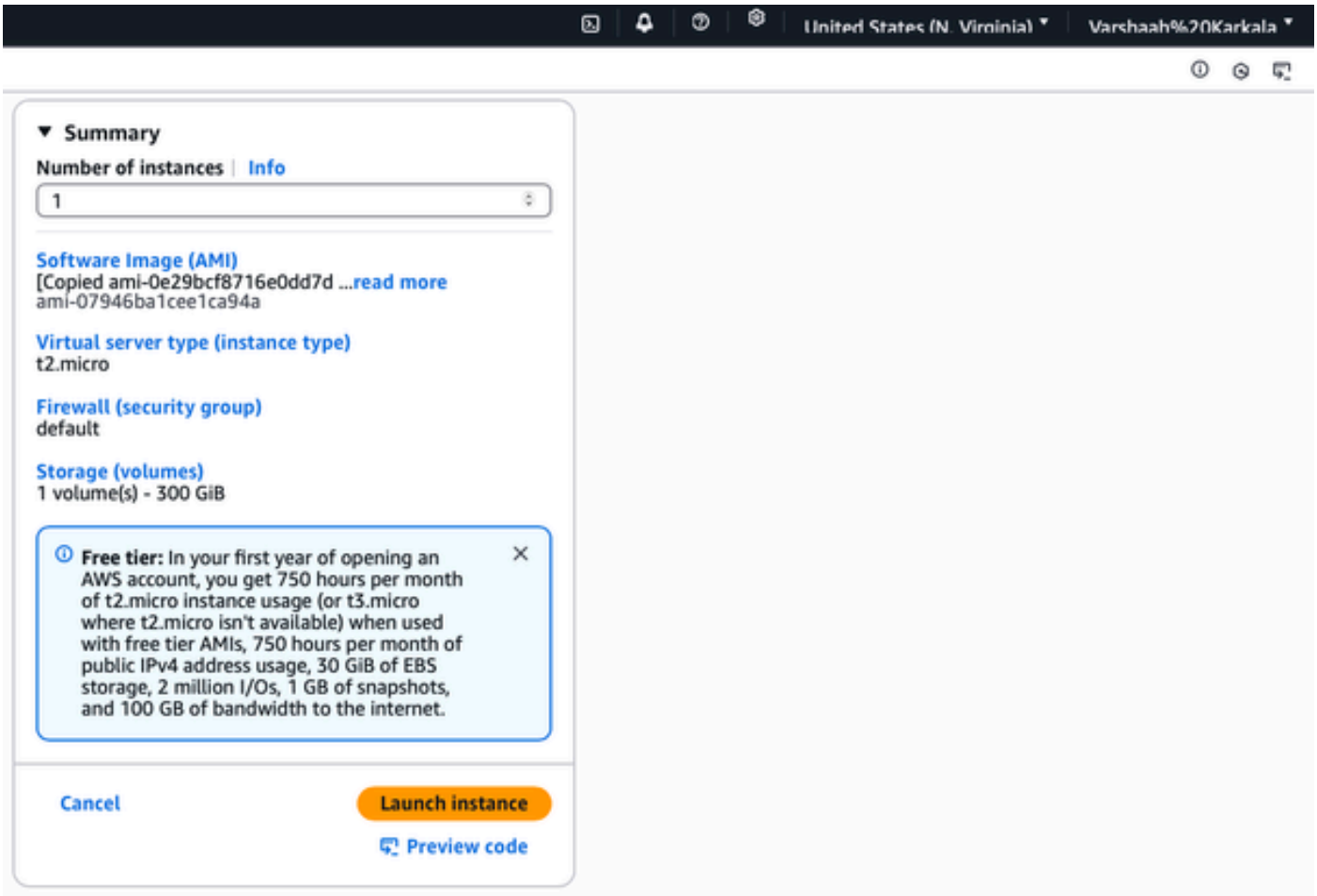
password=Ise@123

ersEnabled=true

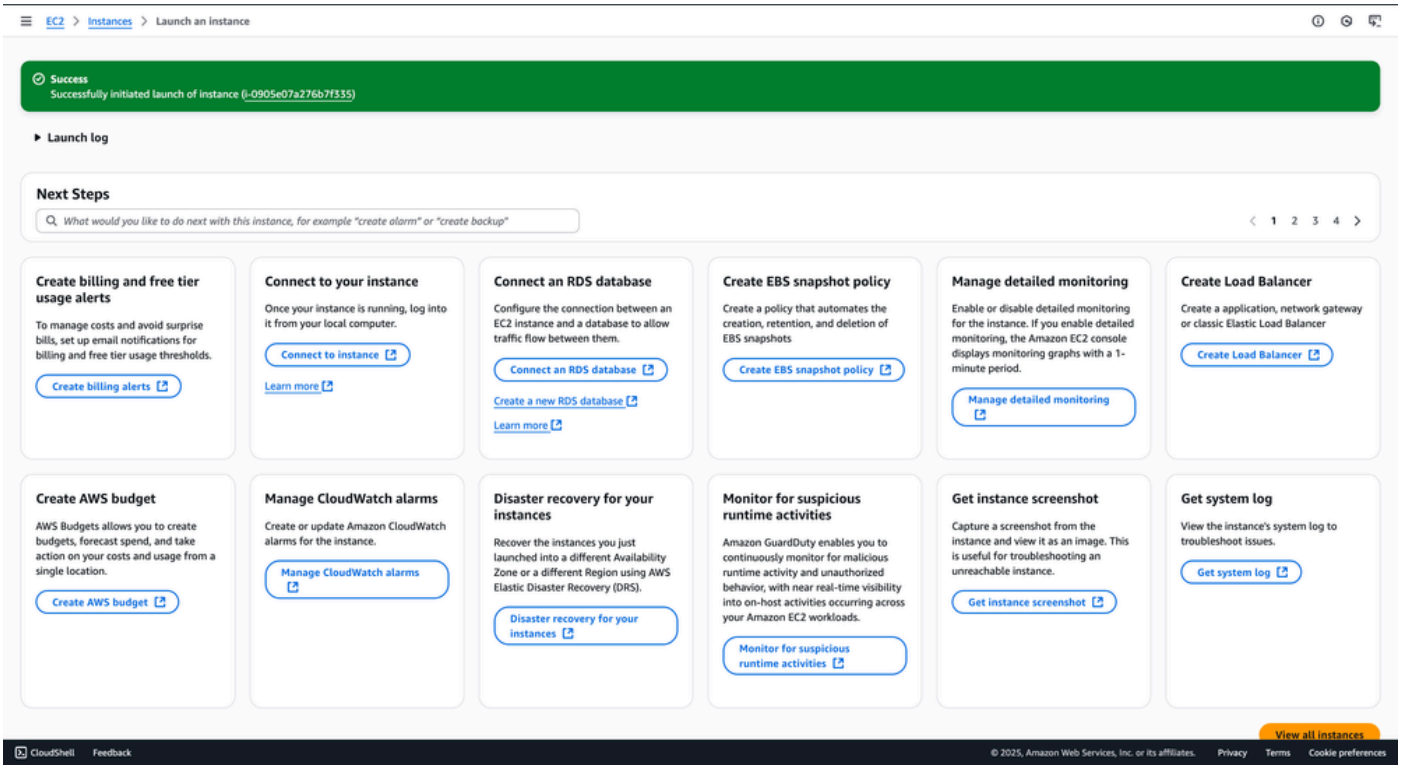


Remarque : Assurez-vous que le mot de passe est conforme à la stratégie de mot de passe Cisco ISE.

Après avoir saisi les données utilisateur et terminé la configuration, cliquez sur Launch Instance.



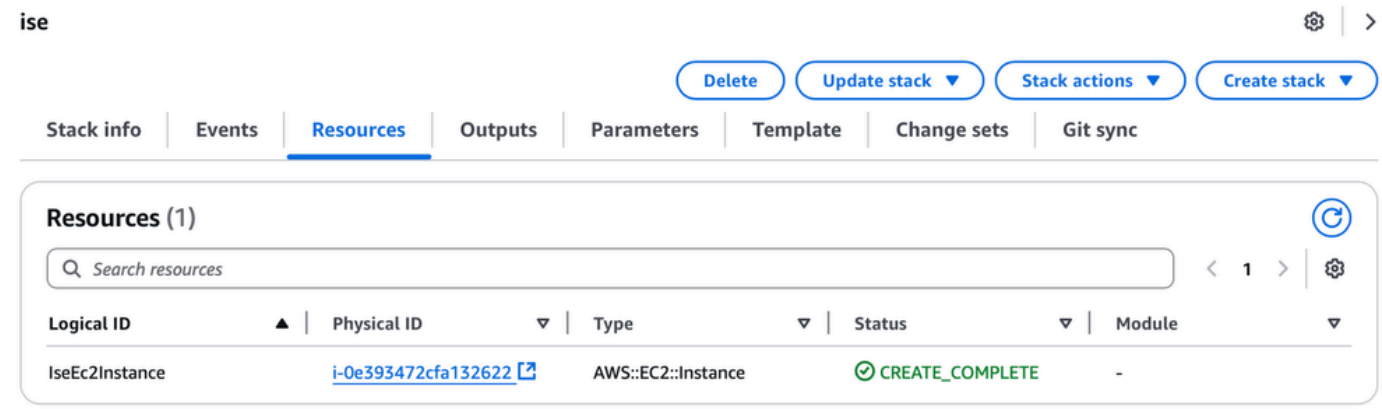
14. Une fois l'instance lancée, un message de confirmation apparaît, indiquant : 'Lancement réussi de l'instance <nom_instance>'. Cela indique que le processus de lancement a démarré avec succès.

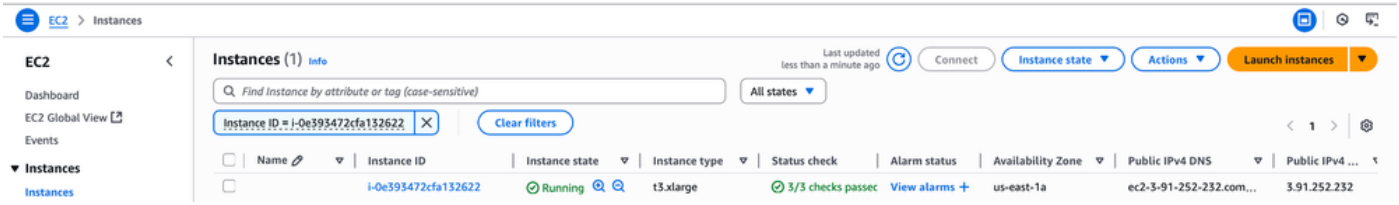


Vérifier

Accès à l'instance ISE créée à l'aide de CFT

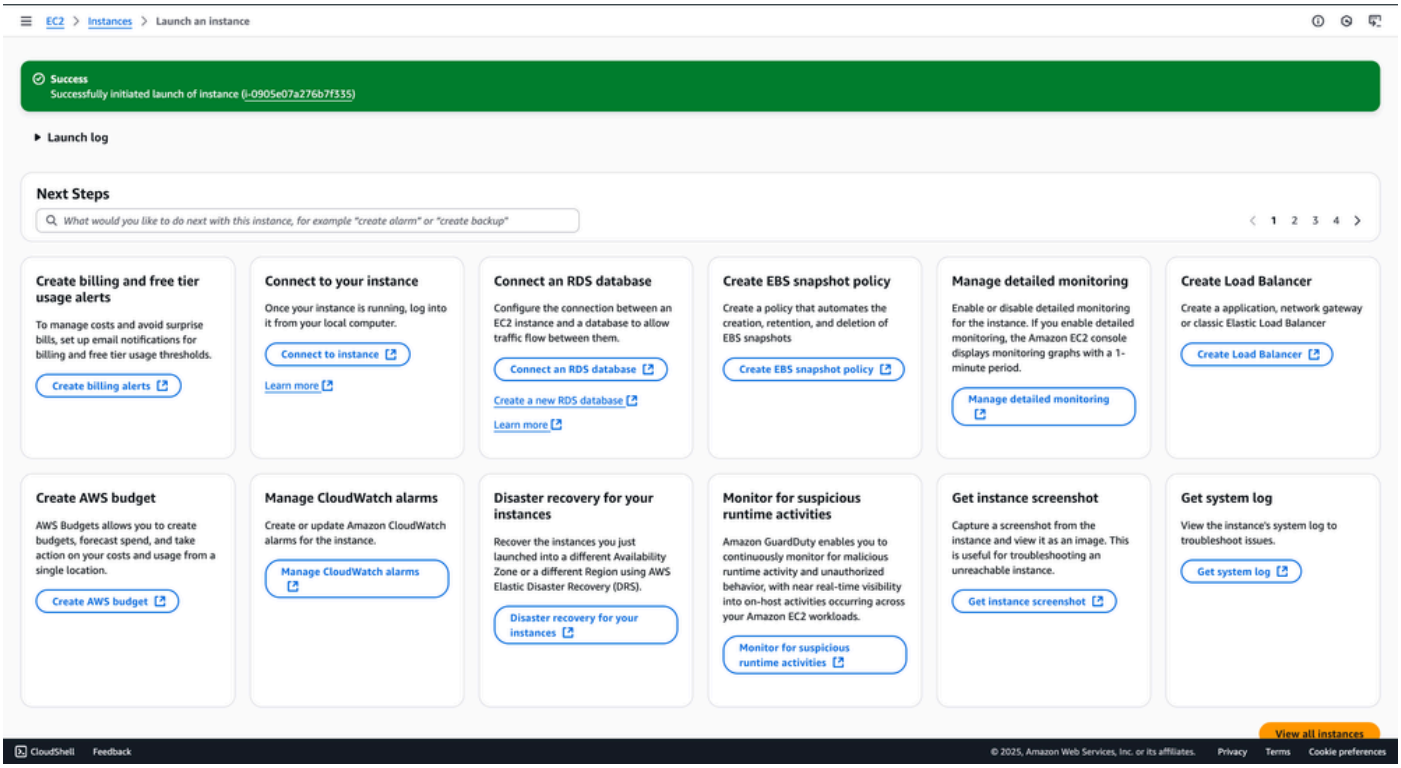
Accédez à l'onglet Resources dans votre pile CloudFormation et cliquez sur l'ID physique. Il vous redirige vers le tableau de bord EC2 où vous pouvez voir l'instance.

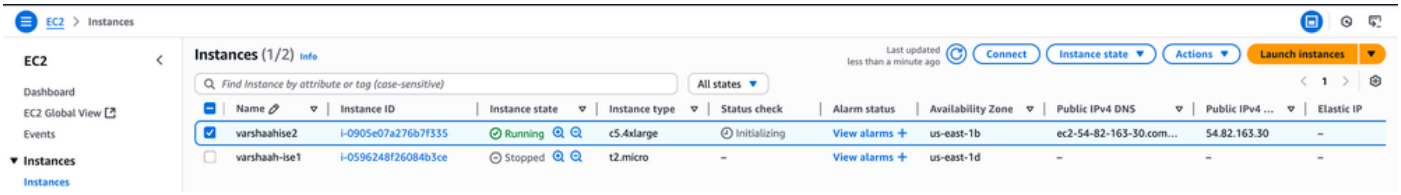




Accès à l'instance ISE créée avec AMI

Cliquez sur Voir toutes les instances pour accéder à la page Instances EC2. Sur cette page, vérifiez que la vérification du statut affiche les 3/3 vérifications réussies, indiquant que l'instance est opérationnelle et en bon état.





Accès à l'interface ISE

Le serveur ISE est maintenant déployé avec succès.

Pour accéder à l'interface utilisateur graphique ISE, vous devez utiliser l'adresse IP de l'instance dans votre navigateur. Comme l’adresse IP par défaut est privée, il est impossible d’y accéder directement à partir d’Internet.

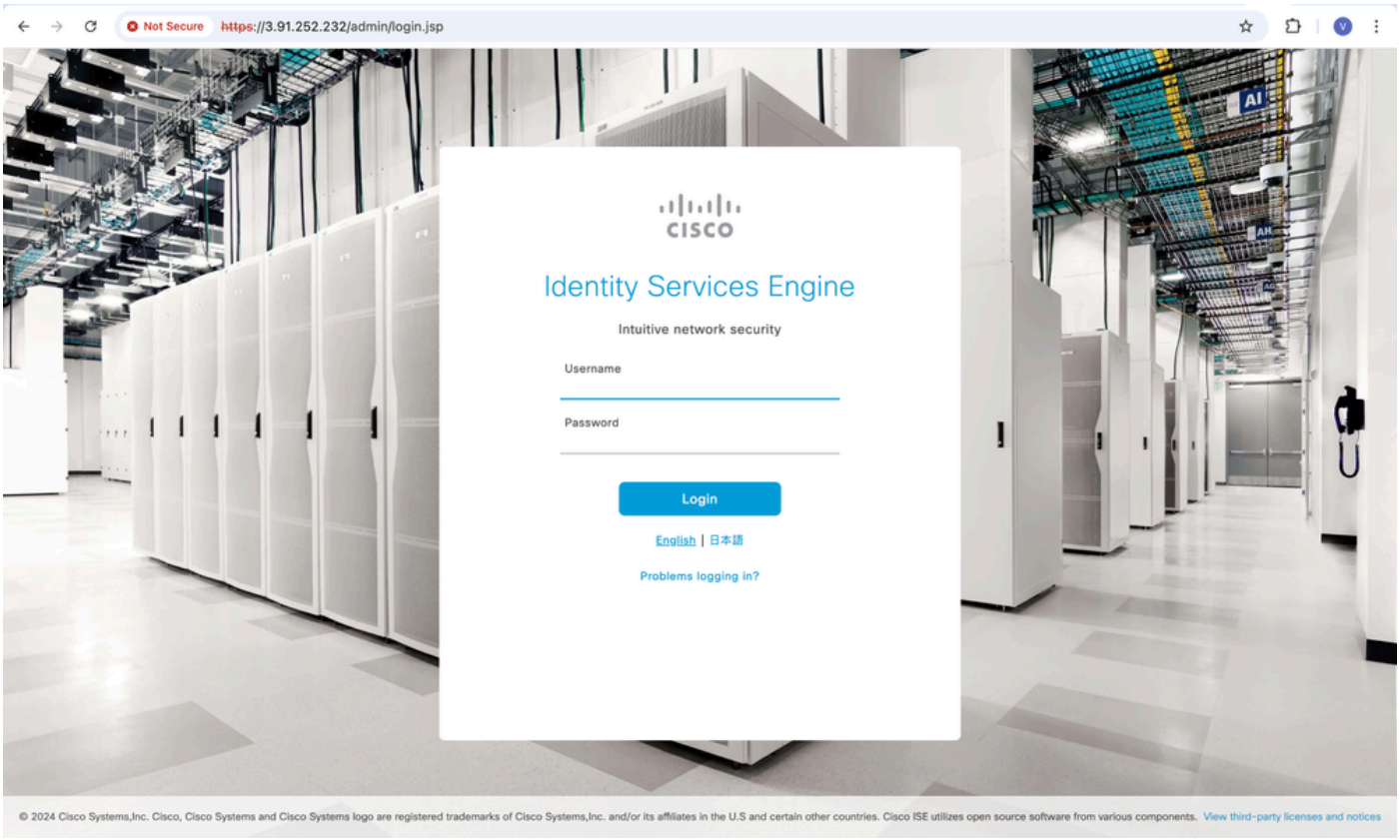
Vérifiez si une adresse IP publique est associée à l'instance :

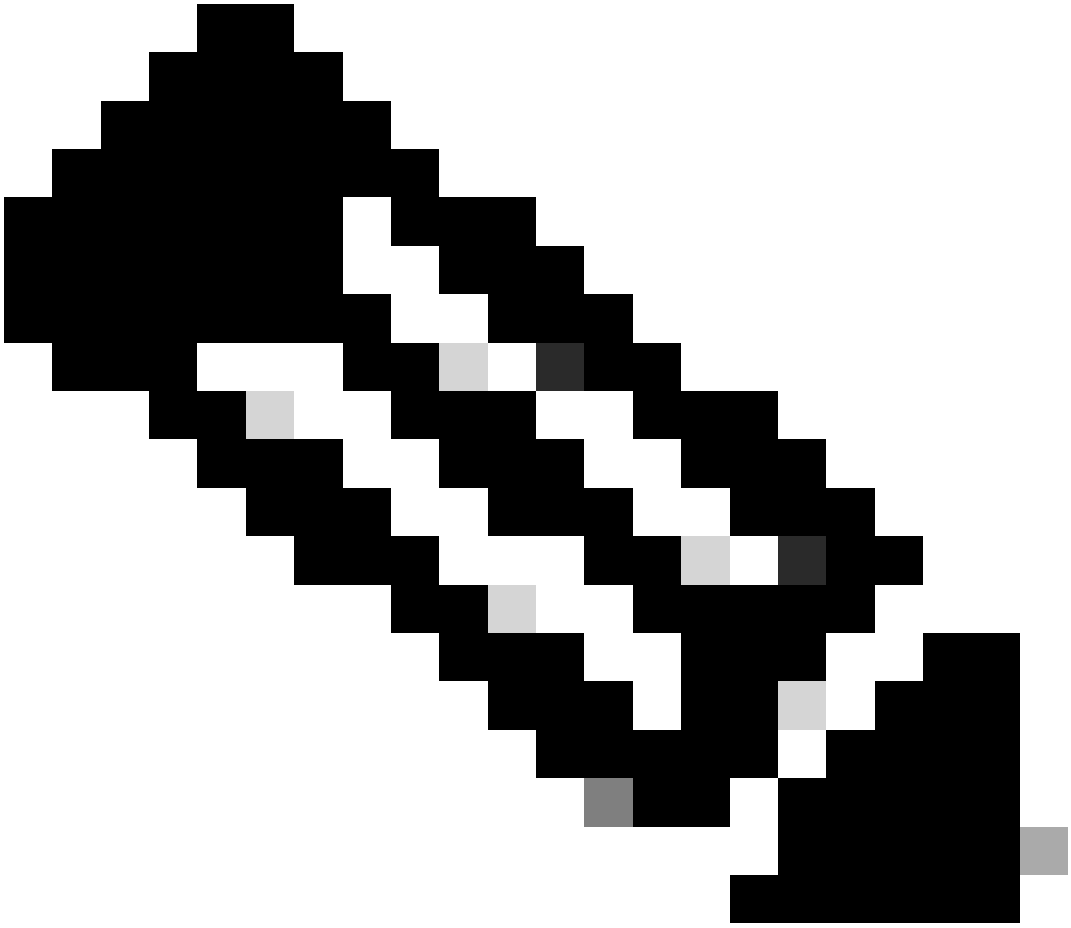
- Accédez à EC2 > Instances et sélectionnez votre instance.
- Recherchez le champ Adresse IPv4 publique.

Ici, vous pouvez voir une adresse IP publique que vous pouvez utiliser pour accéder à l'interface utilisateur graphique ISE.

Ouvrez un navigateur pris en charge (par exemple, Chrome ou Firefox) et saisissez l'adresse IP publique.

La page de connexion à l'interface ISE apparaît.





Remarque : Une fois l'accès SSH disponible, il faut généralement 10 à 15 minutes supplémentaires pour que les services ISE passent entièrement à l'état d'exécution.

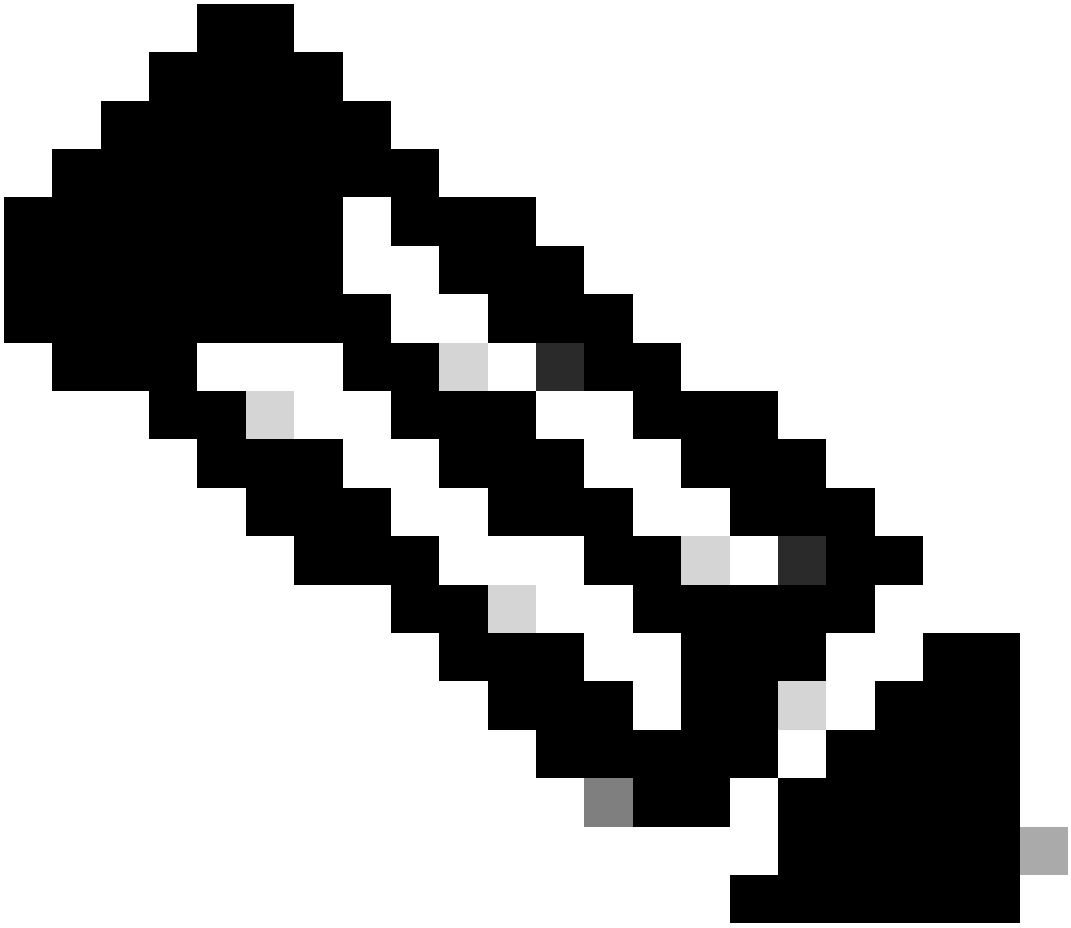
Accès CLI via SSH à partir du terminal

Dans la console EC2, sélectionnez votre instance et cliquez sur Connect.

Sous l'onglet SSH client, procédez comme suit :

- Accédez au dossier contenant le fichier de clé .pem téléchargé.
- Exécutez ces commandes :

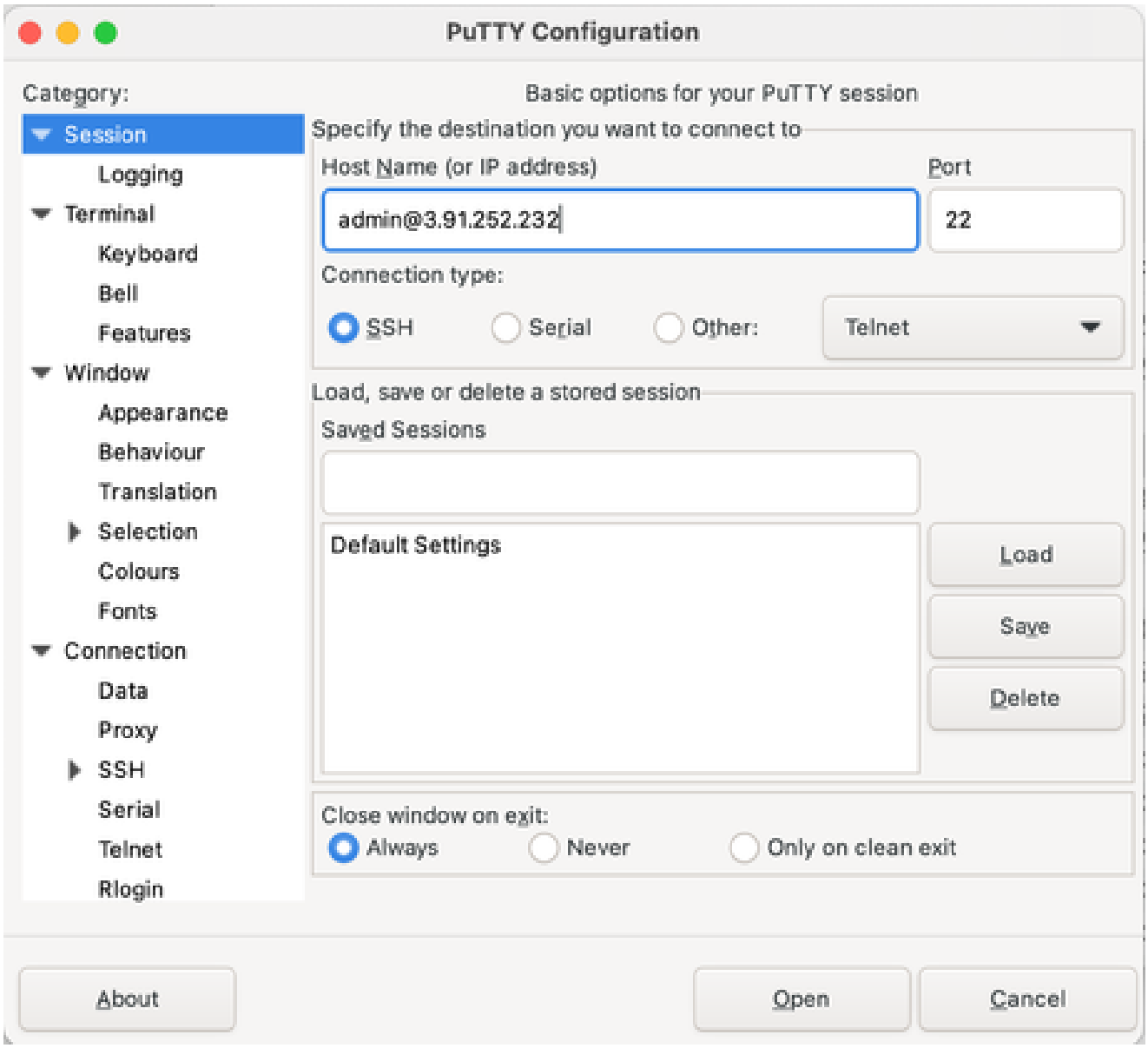
- cd <chemin-vers-fichier-clé>
- chmod 400 <nom-paire-de-clés-que-vous>.pem
- ssh -i "<nom-paire-de-clés-que-vous>.pem" admin@<adresse-ip-publique>



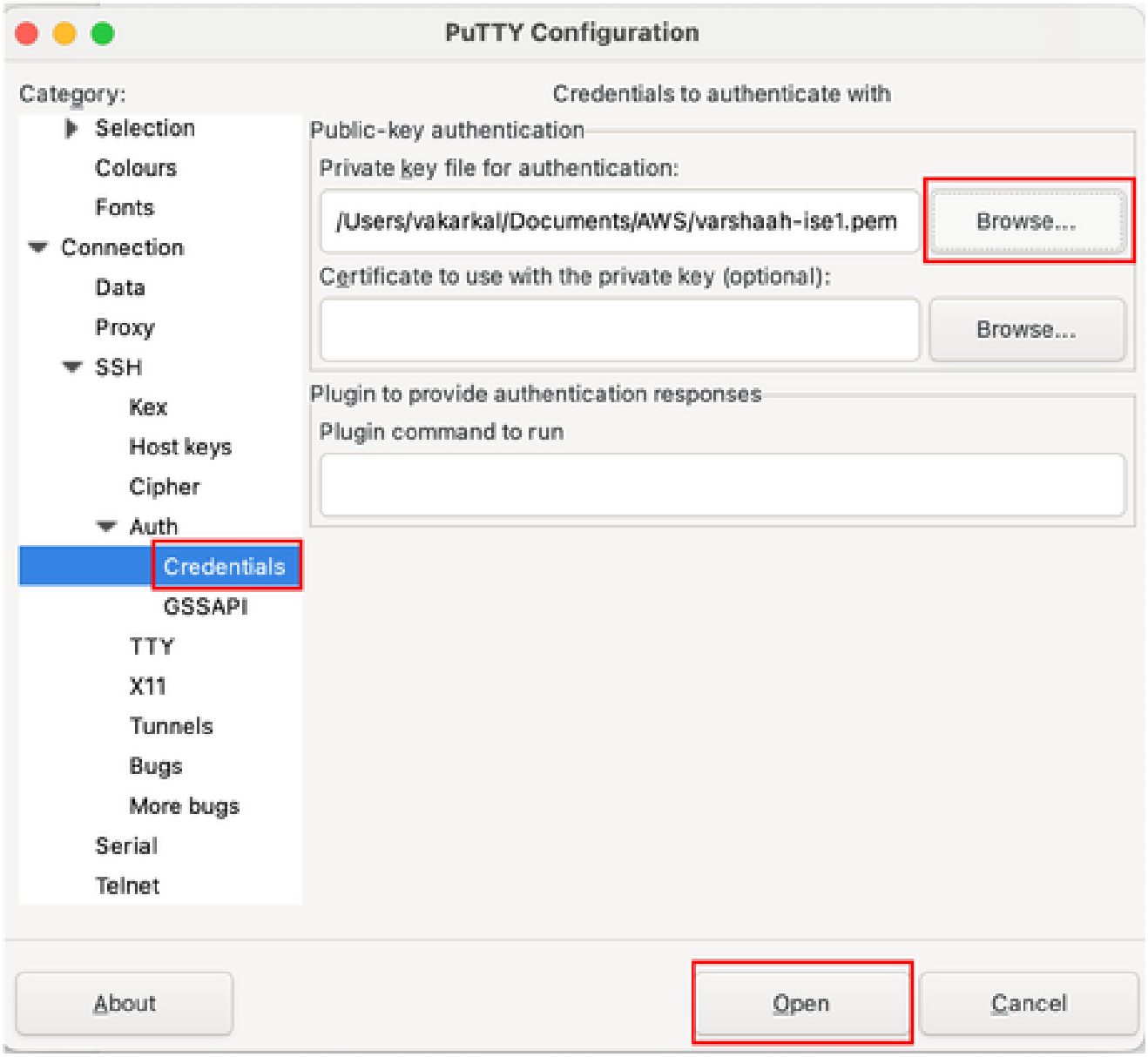
Remarque : Utilisez admin comme utilisateur SSH, puisque Cisco ISE désactive la connexion racine via SSH.

Accès CLI via SSH à l'aide de PuTy

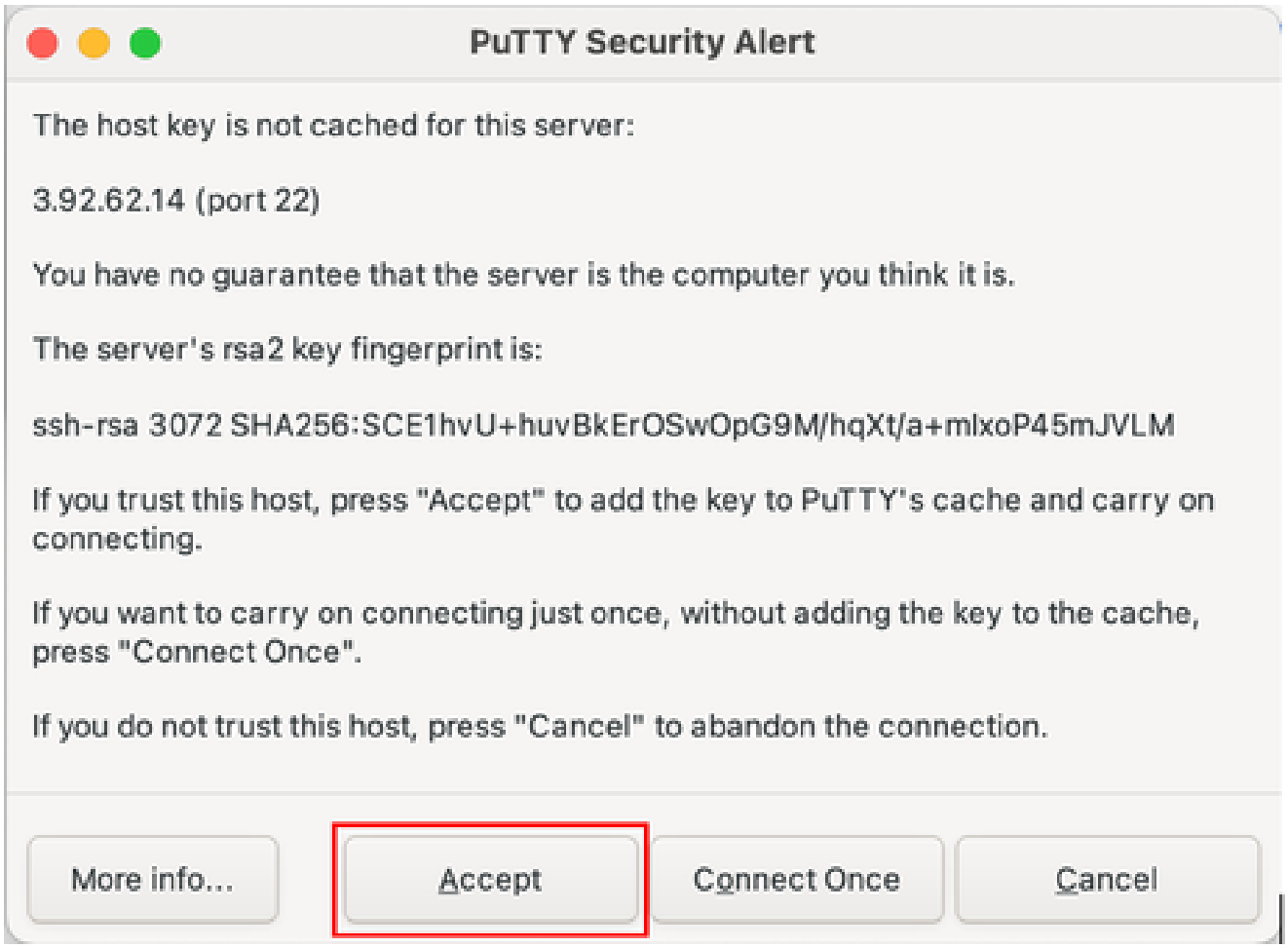
- Ouvrez PuTTY.
- Dans le champ Host Name, saisissez : admin@<adresse-ip-publique>



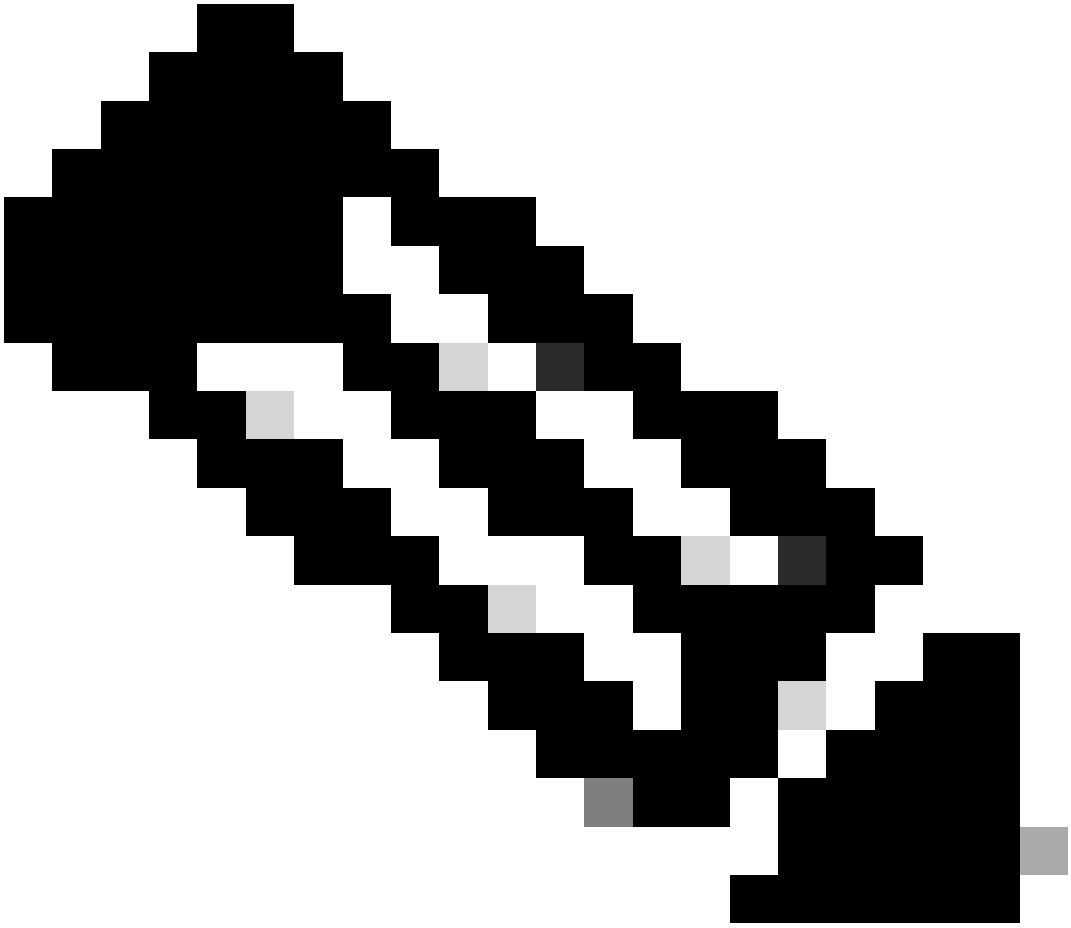
- Dans le volet de gauche, accédez à Connection > SSH > Auth > Credentials.
- Cliquez sur Browse en regard de Private key file for authentication, et sélectionnez votre fichier de clé privée SSH.
- Cliquez sur Open pour lancer la session.



- Lorsque vous y êtes invité, cliquez sur Accept pour confirmer la clé SSH.



- Votre session PuTTY se connecte maintenant à l'interface de ligne de commande ISE.

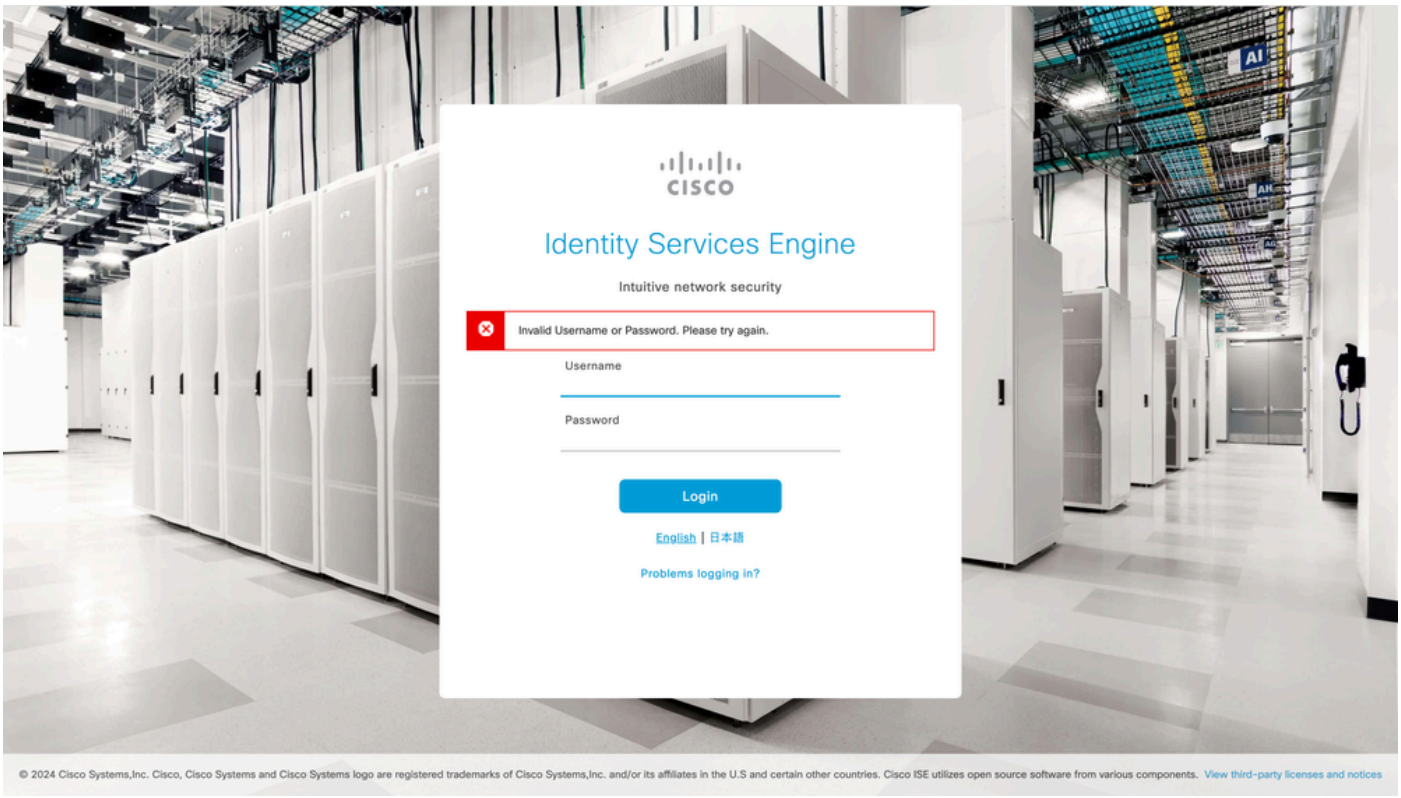


Remarque : L'accès d'ISE via SSH peut prendre jusqu'à 20 minutes. Pendant ce temps, les tentatives de connexion peuvent échouer avec l'erreur suivante : "Autorisation refusée (clé publique)."

Dépannage

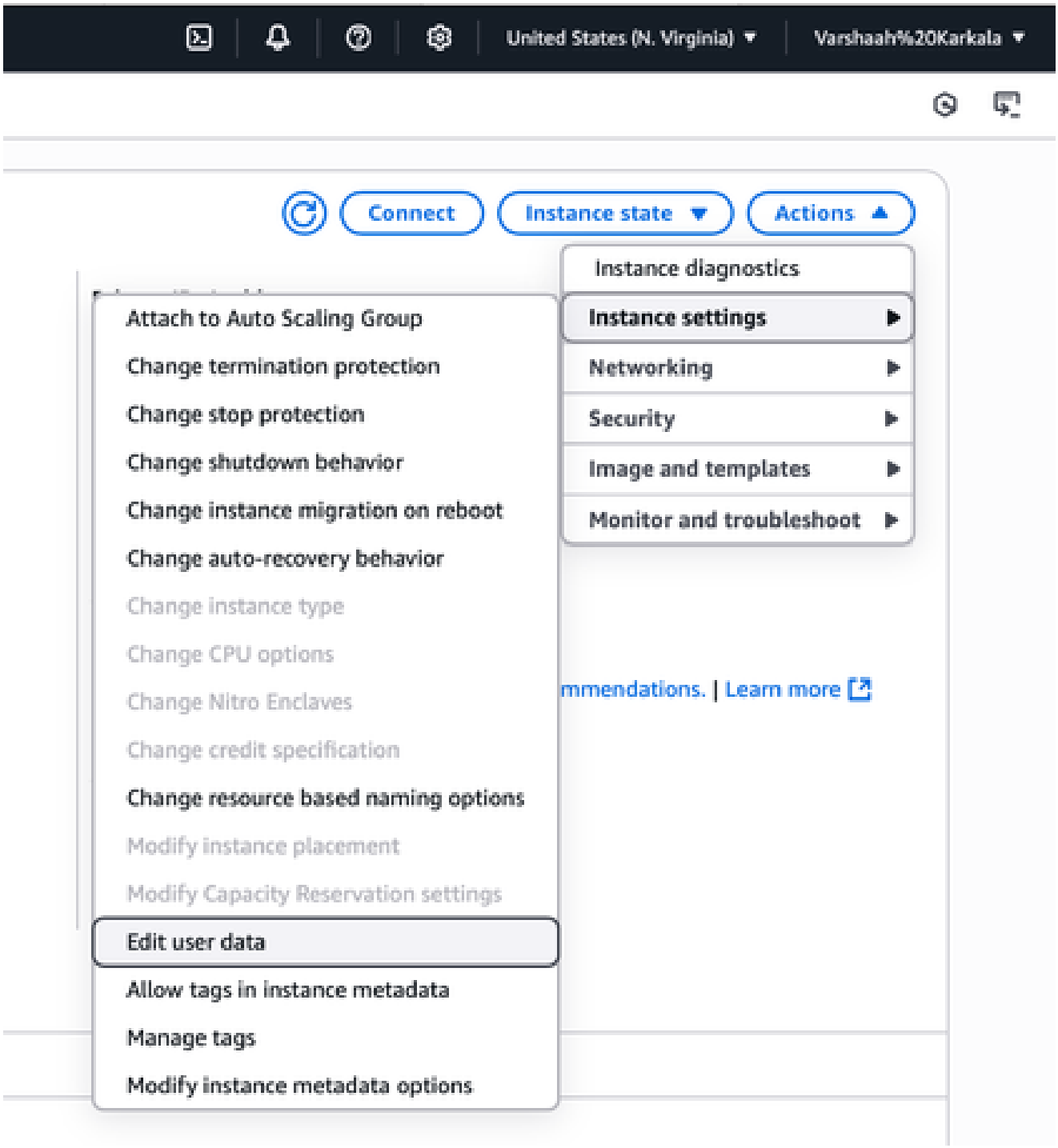
Nom d'utilisateur ou mot de passe non valide

Les problèmes d'authentification sont souvent causés par une entrée utilisateur incorrecte lors de la création de l'instance. Un message d'erreur s'affiche : « Invalid Username or Password. Veuillez réessayer." erreur lors de la tentative de connexion à l'interface utilisateur graphique.

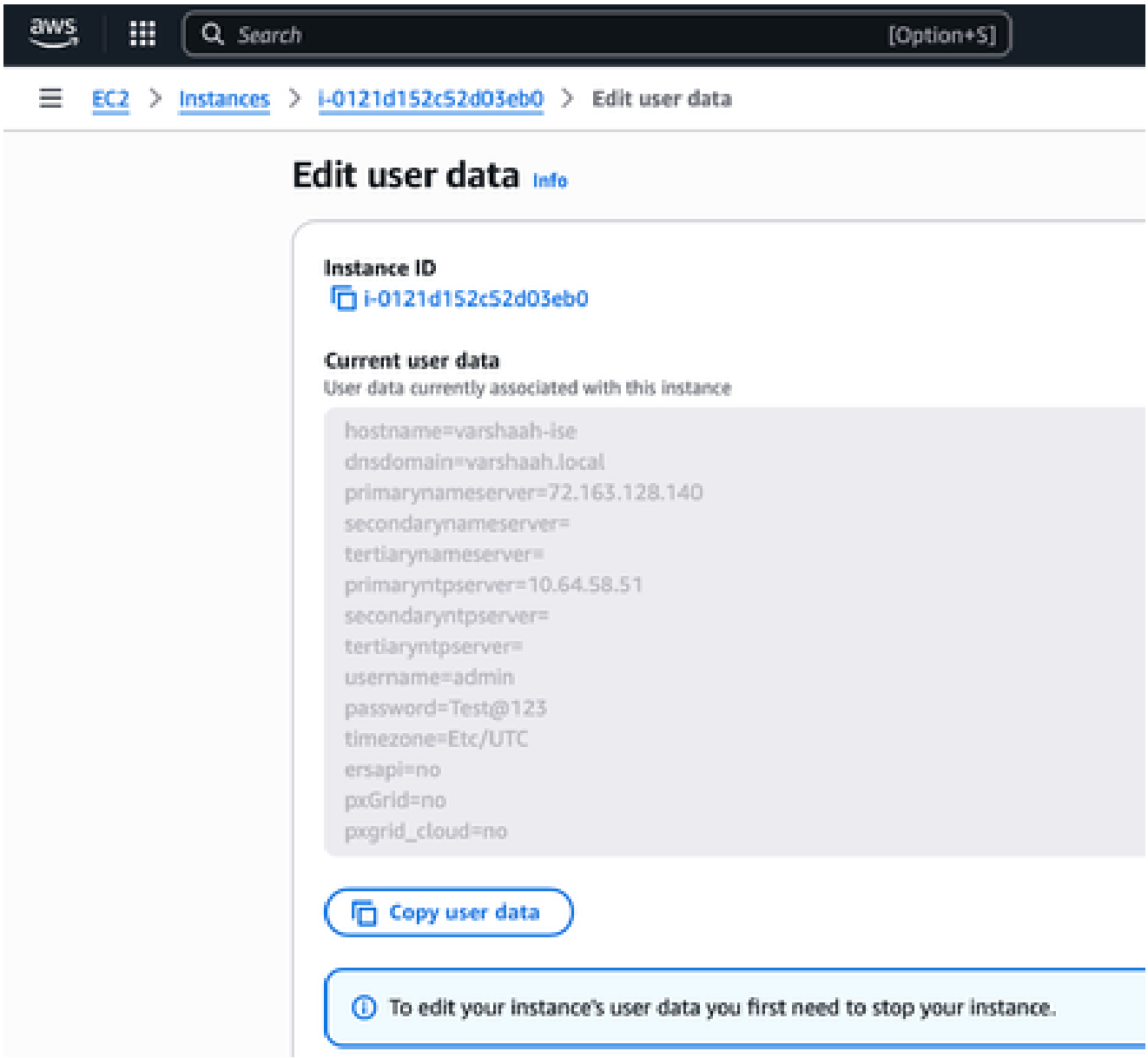


Solution

- Dans la console AWS EC2, accédez à EC2 > Instances > your_instance_id.
- Cliquez sur Actions et choisissez Paramètres d'instance > Modifier les données utilisateur.



- Vous trouverez ici le nom d'utilisateur et le mot de passe spécifiques définis lors du lancement de l'instance. Ces informations d'identification peuvent être utilisées pour se connecter à l'interface utilisateur graphique ISE.



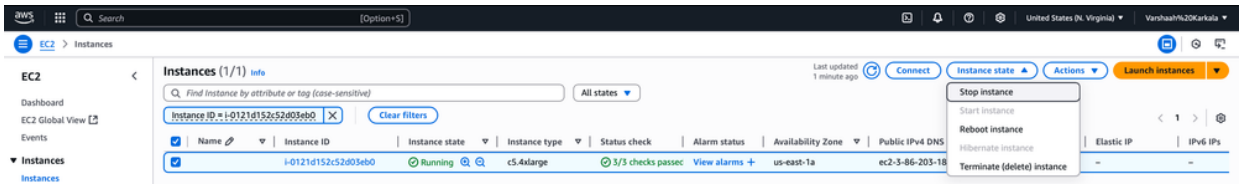
- Vérifiez le nom d'hôte et le mot de passe lors de la configuration :
  - Nom de l'hôte
    - Seuls les caractères alphanumériques et les tirets (-) sont autorisés.
    - Ne doit pas dépasser 19 caractères.
  - Mot de passe
    - Doit respecter la politique de mot de passe Cisco ISE.
    - Reportez-vous au guide officiel de l'administrateur ISE : Stratégie de mot de passe ISE 3.4 - Guide d'administration Cisco

- Si le mot de passe configuré ne répond pas à la stratégie de mot de passe ISE, les tentatives de connexion échouent ; même avec les identifiants corrects.

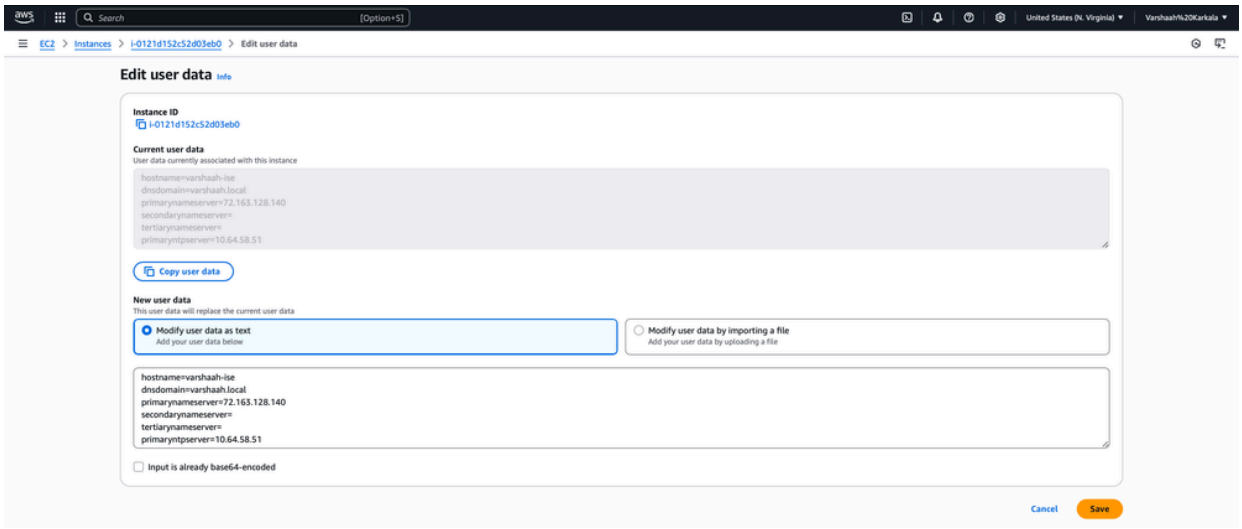
- Si vous pensez que le mot de passe a été mal configuré, procédez comme suit pour le mettre à jour :

    1. Dans la console EC2, accédez à EC2 > Instances > your_instance_id

    2. Cliquez sur État d'instance > Arrêter instance.



    3. Une fois l'instance arrêtée, cliquez sur Actions > Paramètres de l'instance > Modifier les données utilisateur.



    4. Modifiez le script de données utilisateur pour mettre à jour le mot de passe en conséquence.

    5. Cliquez sur Save pour enregistrer vos modifications. Cliquez sur État de l'instance > Démarrer l'instance pour redémarrer l'instance.

Défauts connus

ID de bogue	Description
ID de bogue Cisco 41693	ISE sur AWS ne parvient pas à récupérer les données utilisateur si la version des

	métadonnées est définie sur V2 uniquement. Seul IMDSv1 est pris en charge dans les versions antérieures à ISE 3.4.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.