Configurer ISE 3.1 via AWS Marketplace

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Configuration
Topologie du réseau
Configurations
Étape A facultative. Créer un VPC
Étape B facultative. Configuration du périphérique de tête de réseau VPN sur site
Étape C. Facultative : création d'une paire de clés personnalisée
Étape D facultative. Créer un groupe de sécurité personnalisé
Étape 1. Abonnez-vous au produit Marketplace ISE AWS
Étape 2. Configurer ISE sur AWS
Étape 3. Lancer ISE sur AWS
Étape 4. Configurer la pile CloudFormation pour ISE sur AWS
Étape 5. Accéder à ISE sur AWS
Étape 6. Configurer le déploiement distribué entre ISE sur site et ISE sur AWS
Étape 7. Intégration du déploiement ISE avec AD sur site
Limites
Vérification
Dépannage
Échec de la création de la pile CloudFormation
Problèmes de connectivité
Annexe
Configuration associée au commutateur AAA/Radius

Introduction

Ce document décrit comment installer Identity Services Engine (ISE) 3.1 via Amazon Machine Images (AMI) dans Amazon Web Services (AWS). À partir de la version 3.1, ISE peut être déployée en tant qu'instance Amazon Elastic Compute Cloud (EC2) avec l'aide de CloudFormation Templates (CFT).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE

- AWS et ses concepts tels que VPC, EC2, CloudFormation

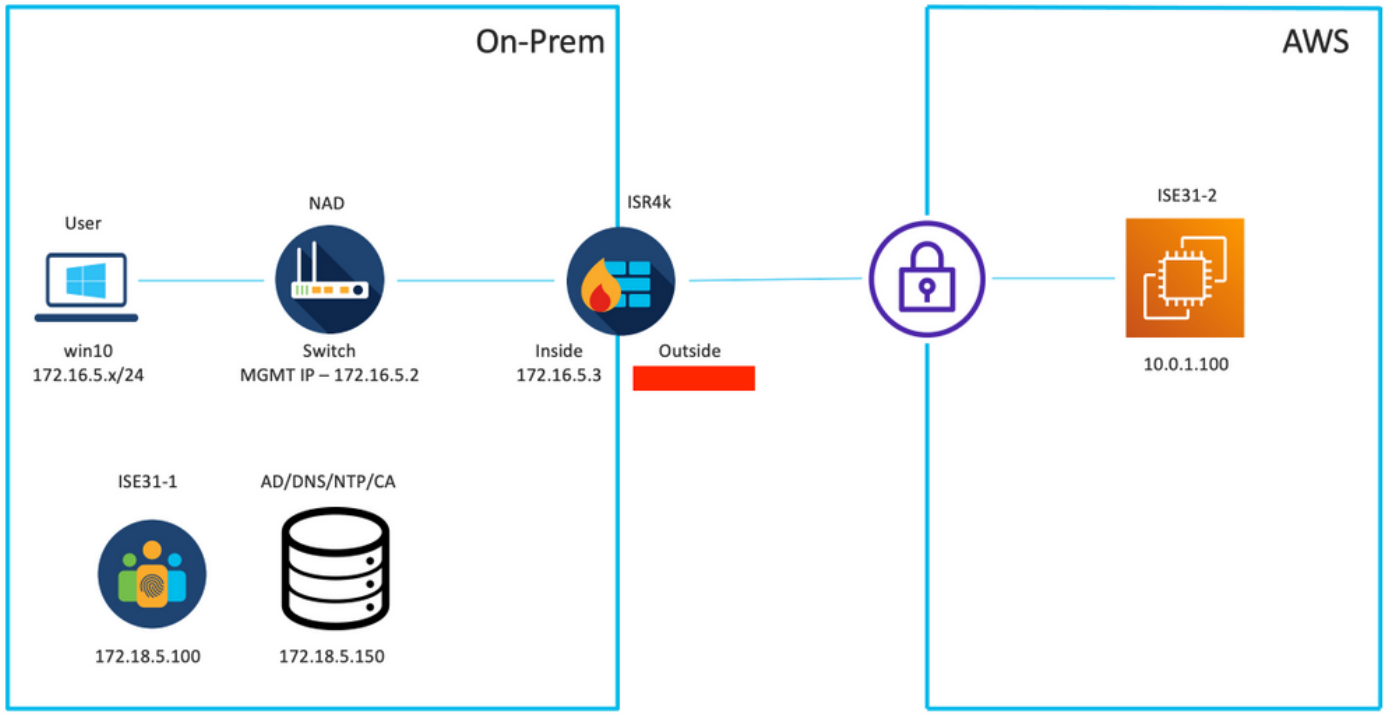
Components Used

Les informations de ce document sont basées sur Cisco ISE version 3.1.

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.

Configuration

Topologie du réseau

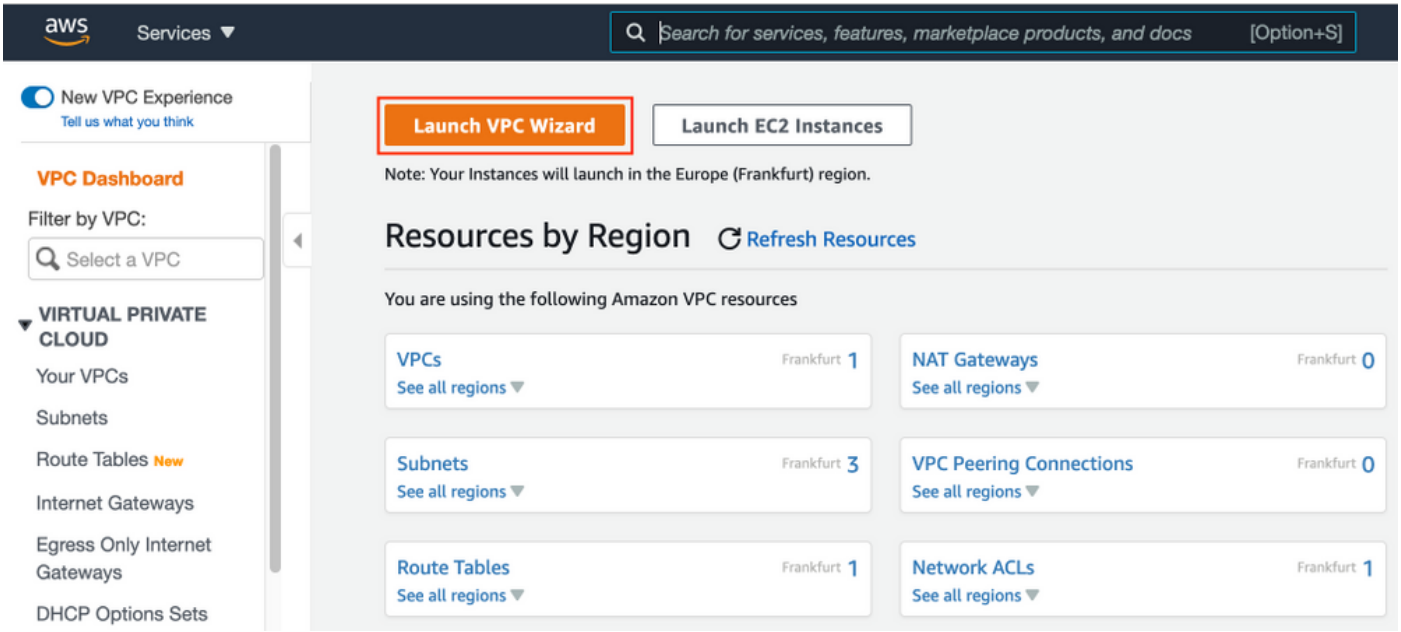


Configurations

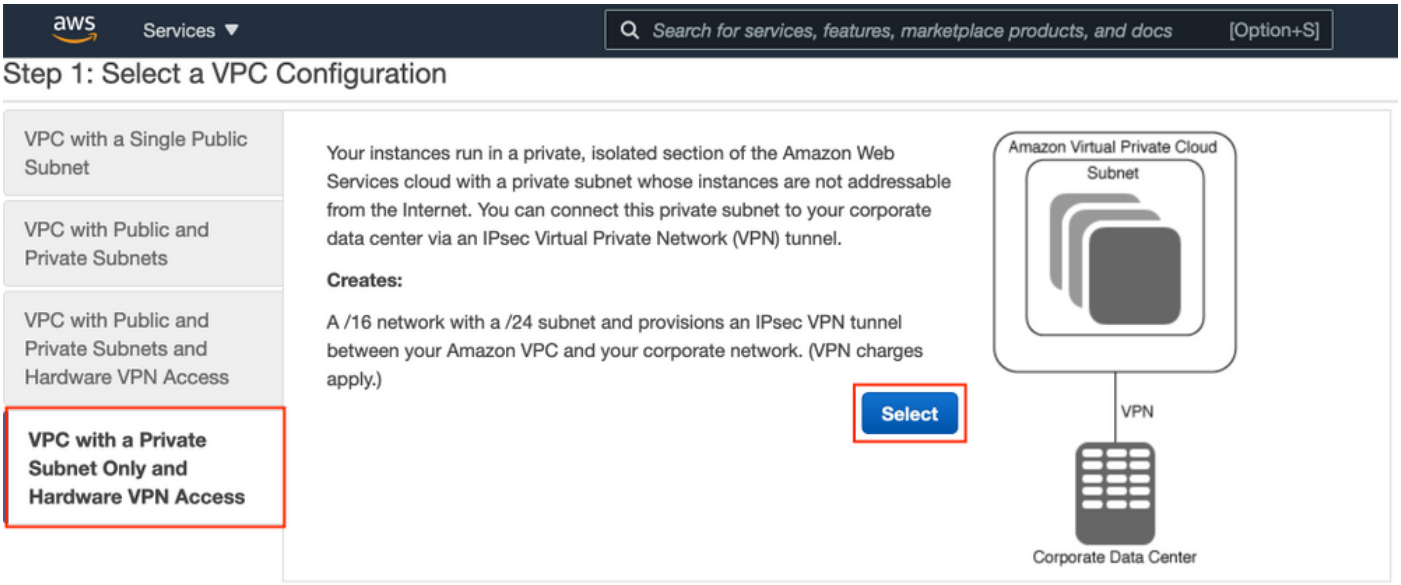
Si aucun VPC, groupe de sécurité, paire de clés et tunnel VPN n'est encore configuré, vous devez suivre les étapes facultatives, sinon, commencer par l'étape 1.

Étape A facultative. Créer un VPC

Accédez à **VPC** AWS Service. Sélectionnez **Lancer l'assistant VPC** comme indiqué dans l'image.

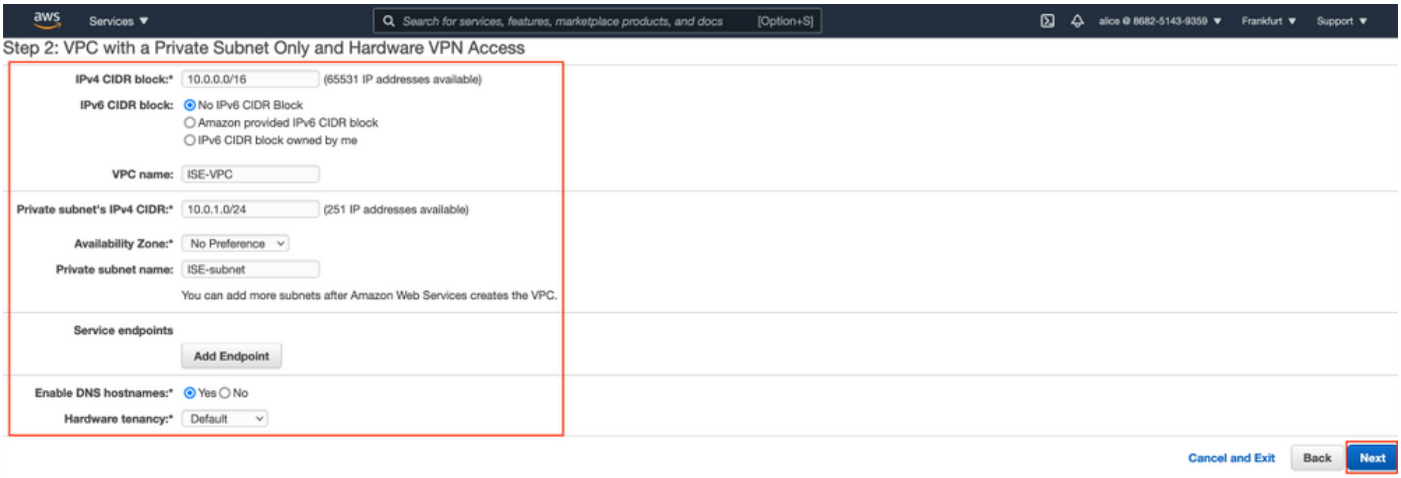


Choisissez **VPC with Private Subnet Only and Hardware VPN Access** et cliquez sur **Select** comme illustré dans l'image.

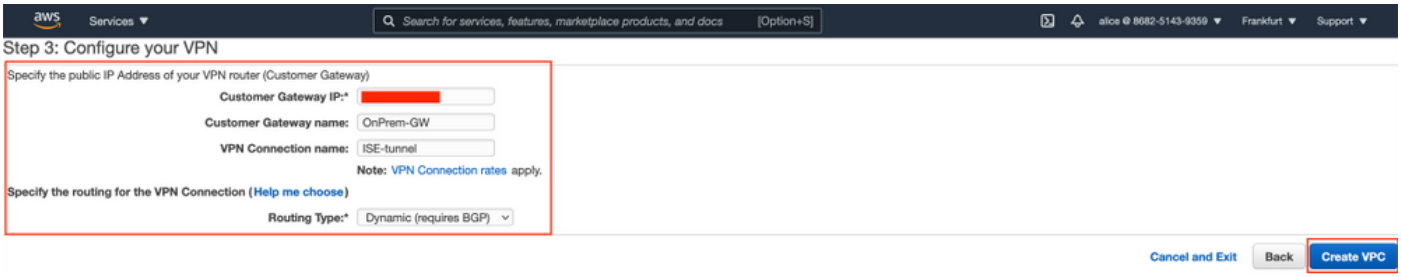


> **Note**: Sélection du VPC à l'étape 1. de l'assistant VPC dépend de la topologie, car ISE n'est pas conçu comme un serveur Internet exposé. Le VPN avec sous-réseau privé uniquement est utilisé.

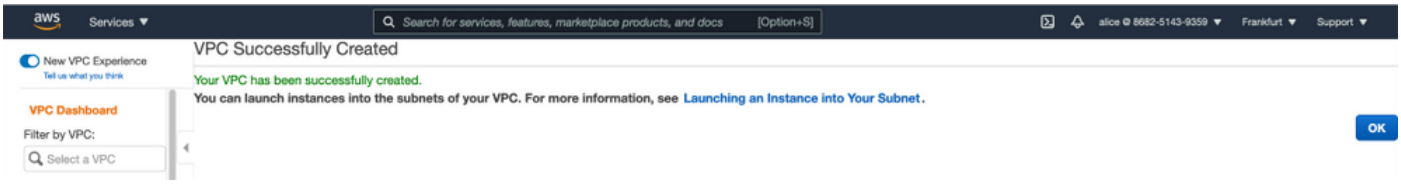
Configurez les paramètres de sous-réseau privé VPC conformément à la conception de votre réseau et sélectionnez **Suivant**.



Configurez votre VPN conformément à la conception de votre réseau et sélectionnez **Créer un VPC**.

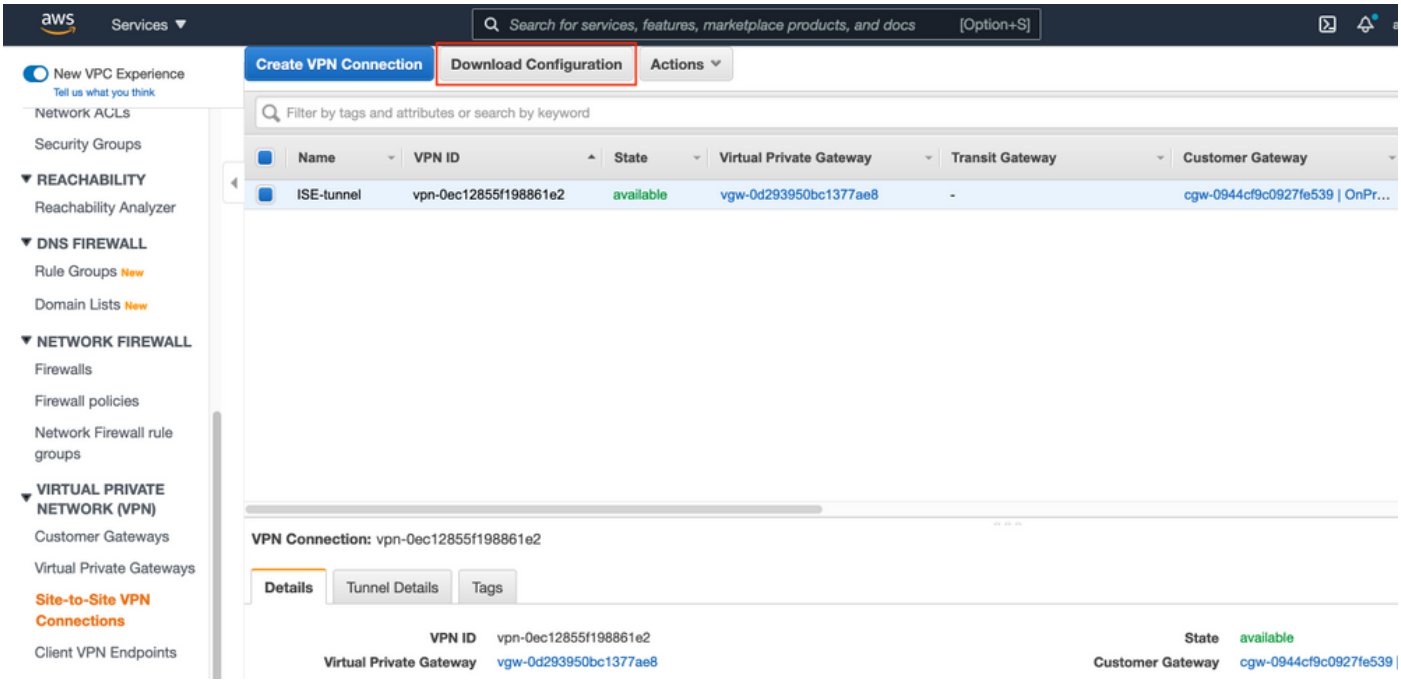


Une fois le VPC créé, le message **« Votre VPC a été créé avec succès »** s'affiche. Cliquez sur **OK** comme indiqué dans l'image.



Étape B facultative. Configuration du périphérique de tête de réseau VPN sur site

Accédez à **VPC** AWS Service. Choisissez **Connexions VPN de site à site**, sélectionnez le tunnel VPN nouvellement créé et sélectionnez **Télécharger la configuration** comme indiqué dans l'image.



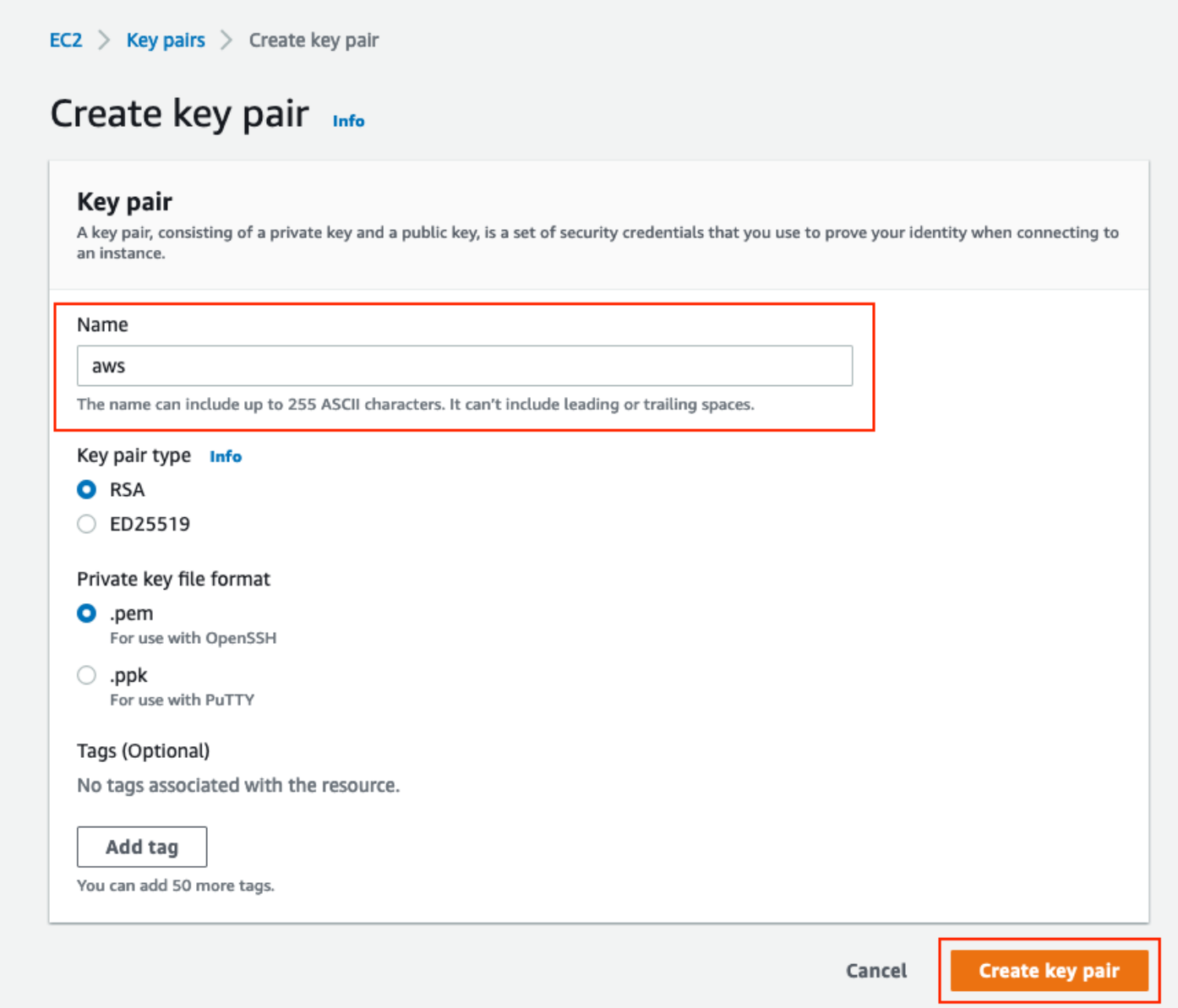
Choisissez **Fournisseur**, **Plateforme** et **Logiciel**, Sélectionnez **Télécharger** comme indiqué dans l'image.



Appliquer la configuration téléchargée sur le périphérique de tête de réseau VPN sur site.

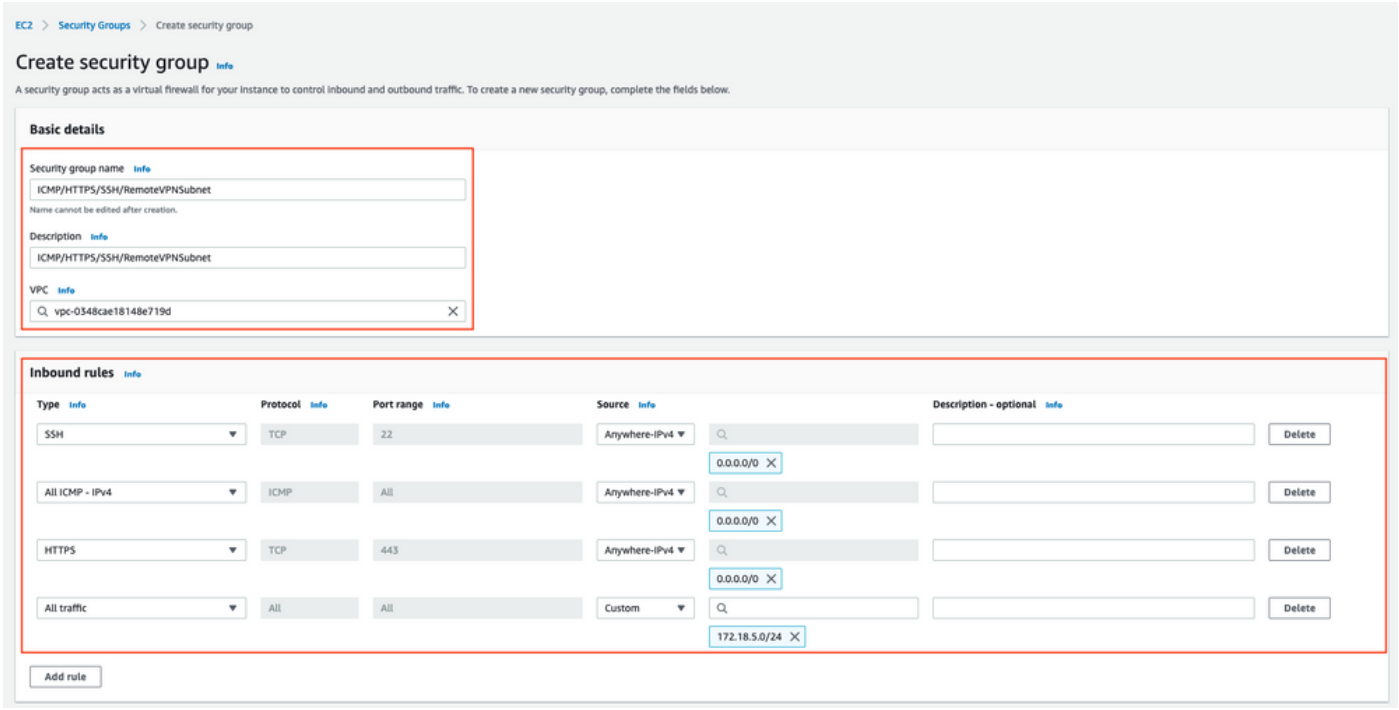
Étape C. Facultative : création d'une paire de clés personnalisée

Les instances AWS EC2 sont accessibles à l'aide de paires de clés. Pour créer une paire de clés, accédez à **EC2** Service. Sélectionnez le menu **Clés** sous **Réseau et sécurité.** Sélectionnez **Créer une paire de clés**, donnez-lui un **nom,** laissez d'autres valeurs par défaut et sélectionnez **Créer une paire de clés** à nouveau.



Étape D facultative. Créer un groupe de sécurité personnalisé

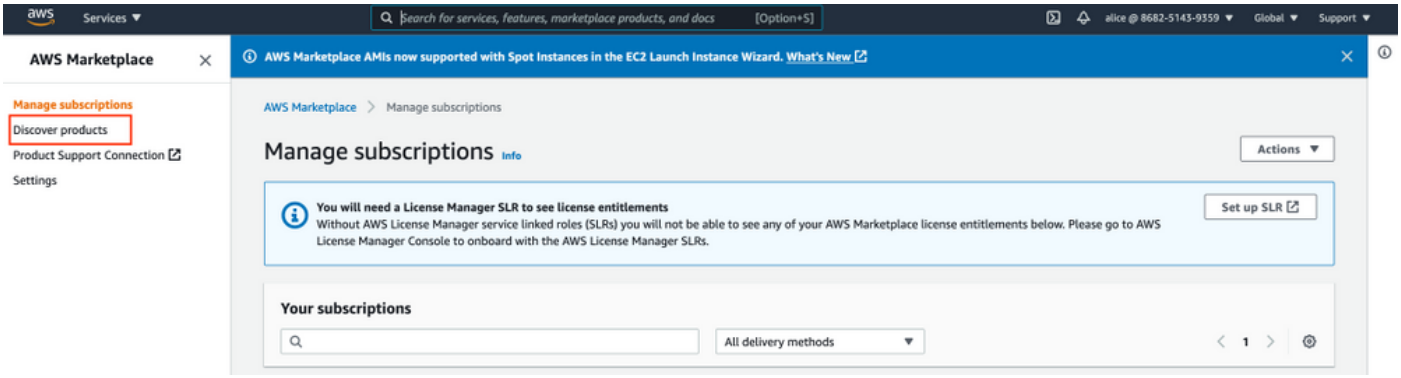
L'accès aux instances AWS EC2 est protégé par **les groupes de sécurité**, afin de configurer **le groupe de sécurité**, accédez au service **EC2**. Sélectionnez le menu **Groupes de sécurité** sous **Réseau et sécurité.** Sélectionnez Créer un groupe de sécurité, configurer un **nom**, **Description,** dans le champ **VPC** sélectionnez **VPC** nouvellement configuré. Configurez **les règles entrantes** pour autoriser la communication vers ISE. Sélectionnez **Créer un groupe de sécurité** comme indiqué dans l'image.



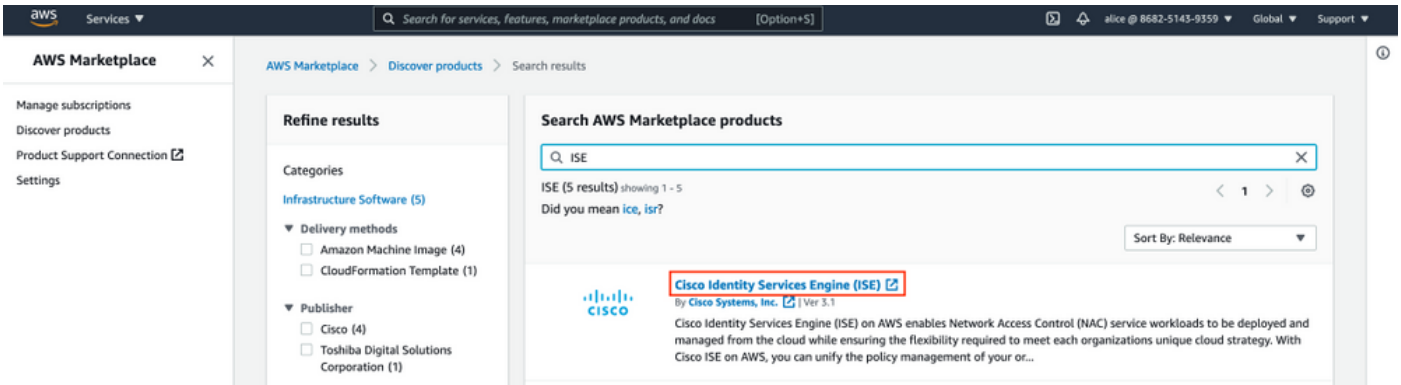
Note: Le groupe de sécurité configuré autorise l'accès SSH, ICMP, HTTPS à ISE et tous les protocoles à partir du sous-réseau On-Prem.

Étape 1. Abonnez-vous au produit Marketplace ISE AWS

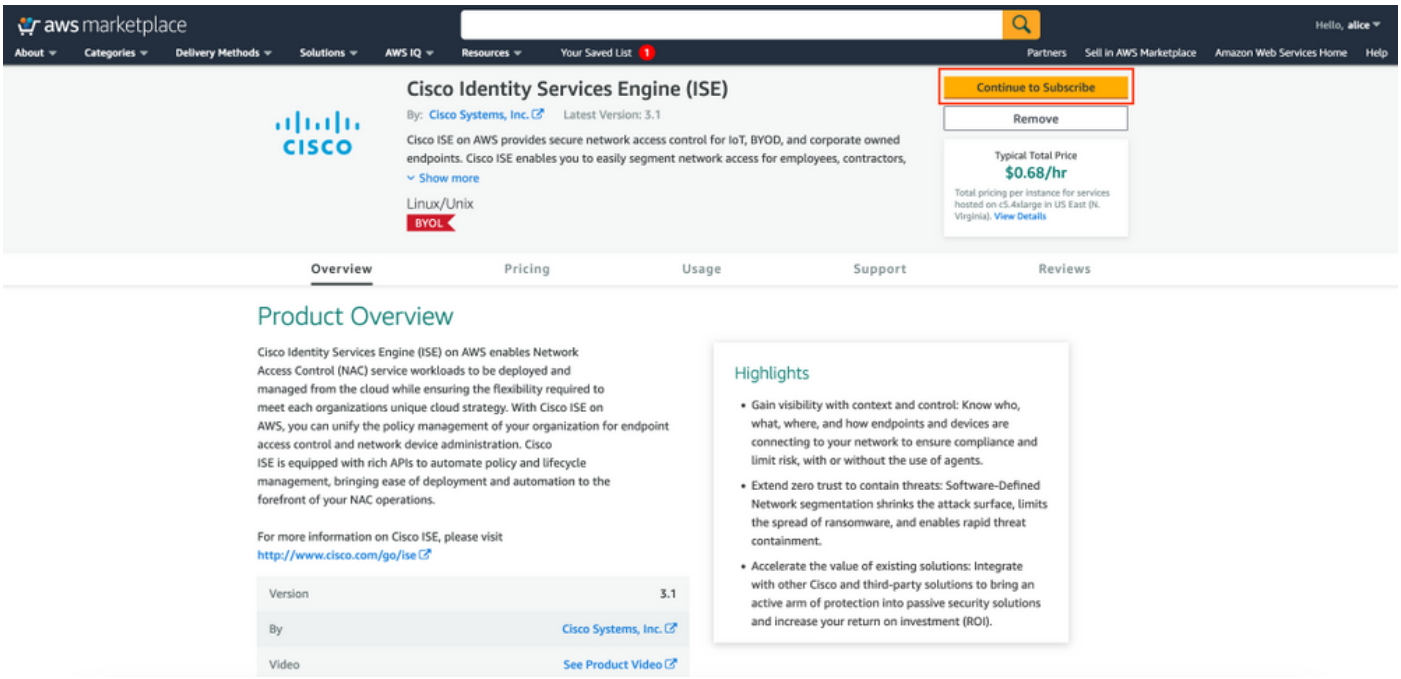
Accédez au service AWS **Abonnements au Marché AWS**. Sélectionnez **Découvrir les produits** comme indiqué dans l'image.



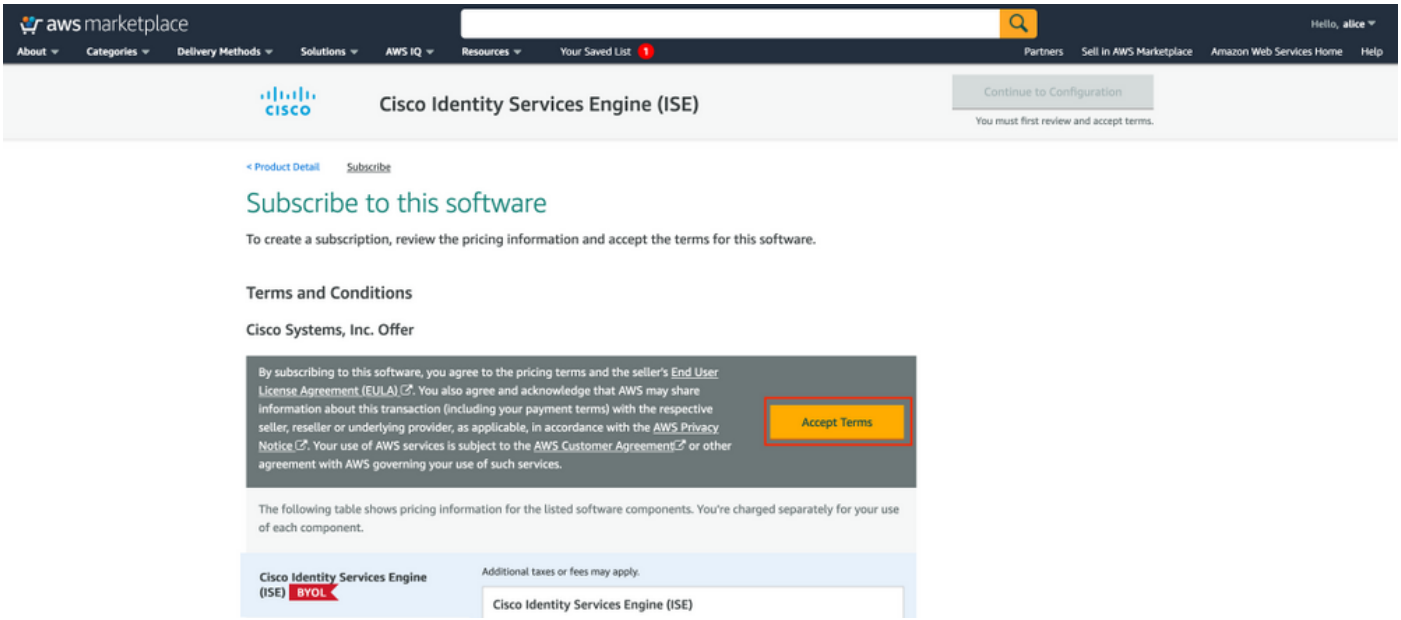
Recherchez le produit **ISE** et sélectionnez **Cisco Identity Services Engine (ISE)** comme indiqué dans l'image.



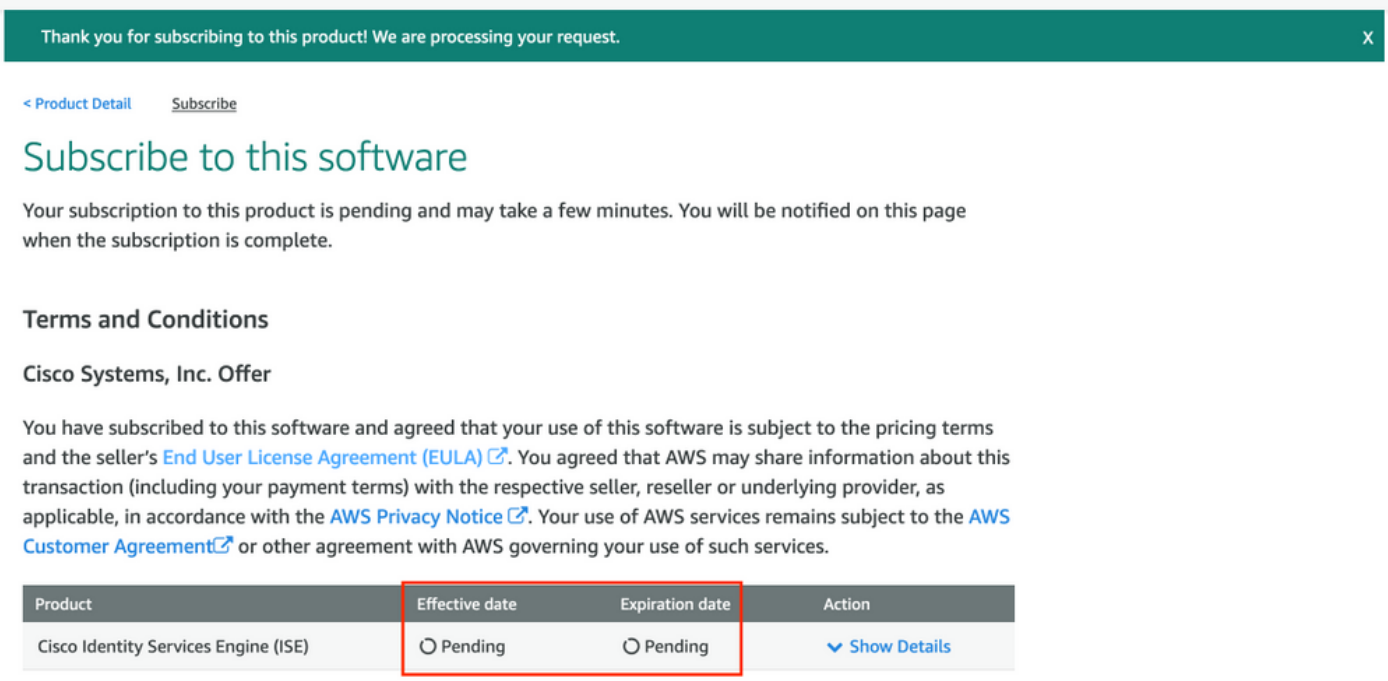
Cliquez sur **le** bouton **Continuer pour vous abonner**



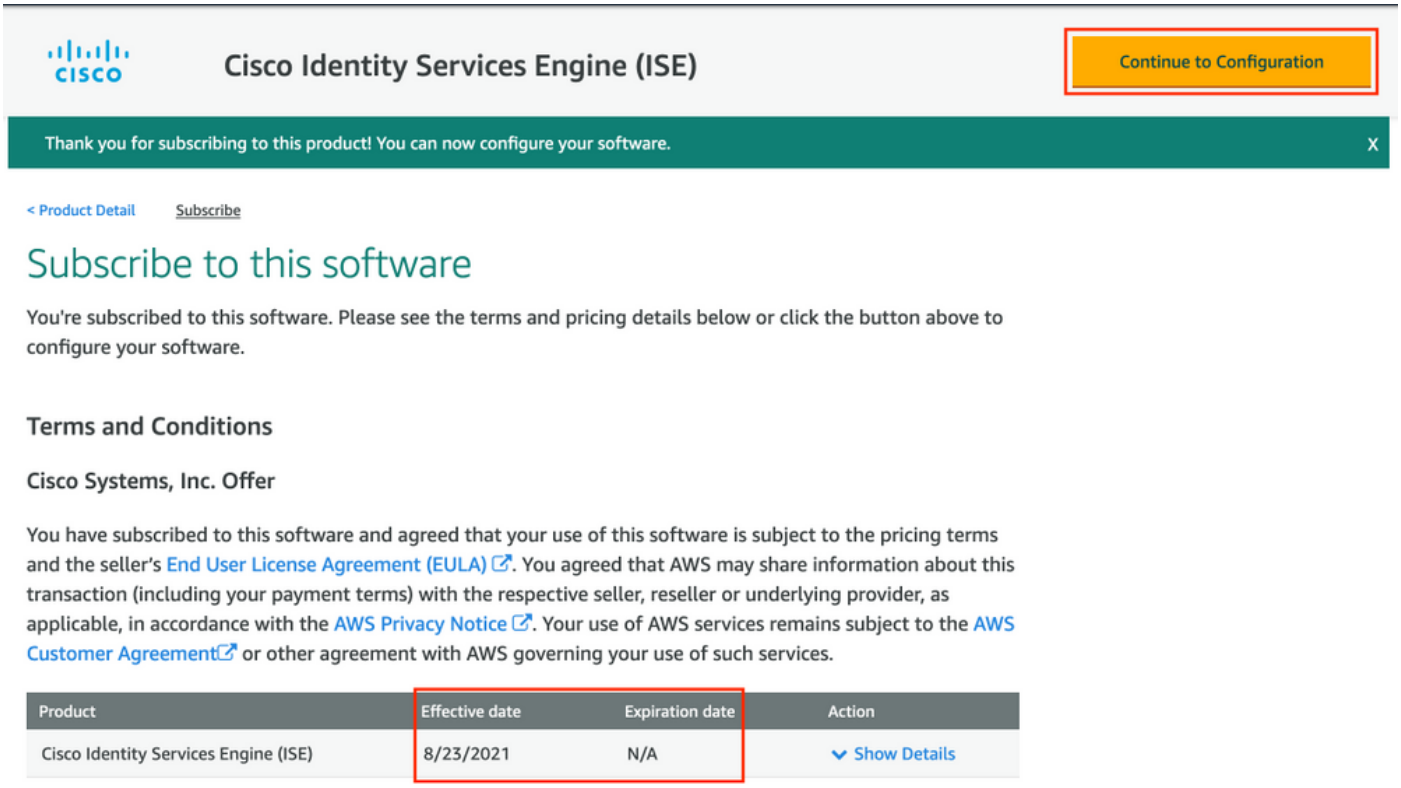
Cliquez sur le bouton **Accepter les termes** comme indiqué dans l'image.



Une fois souscrit l'état de la **date effective** et **d'expiration** avec la modification **En attente** comme indiqué dans l'image.

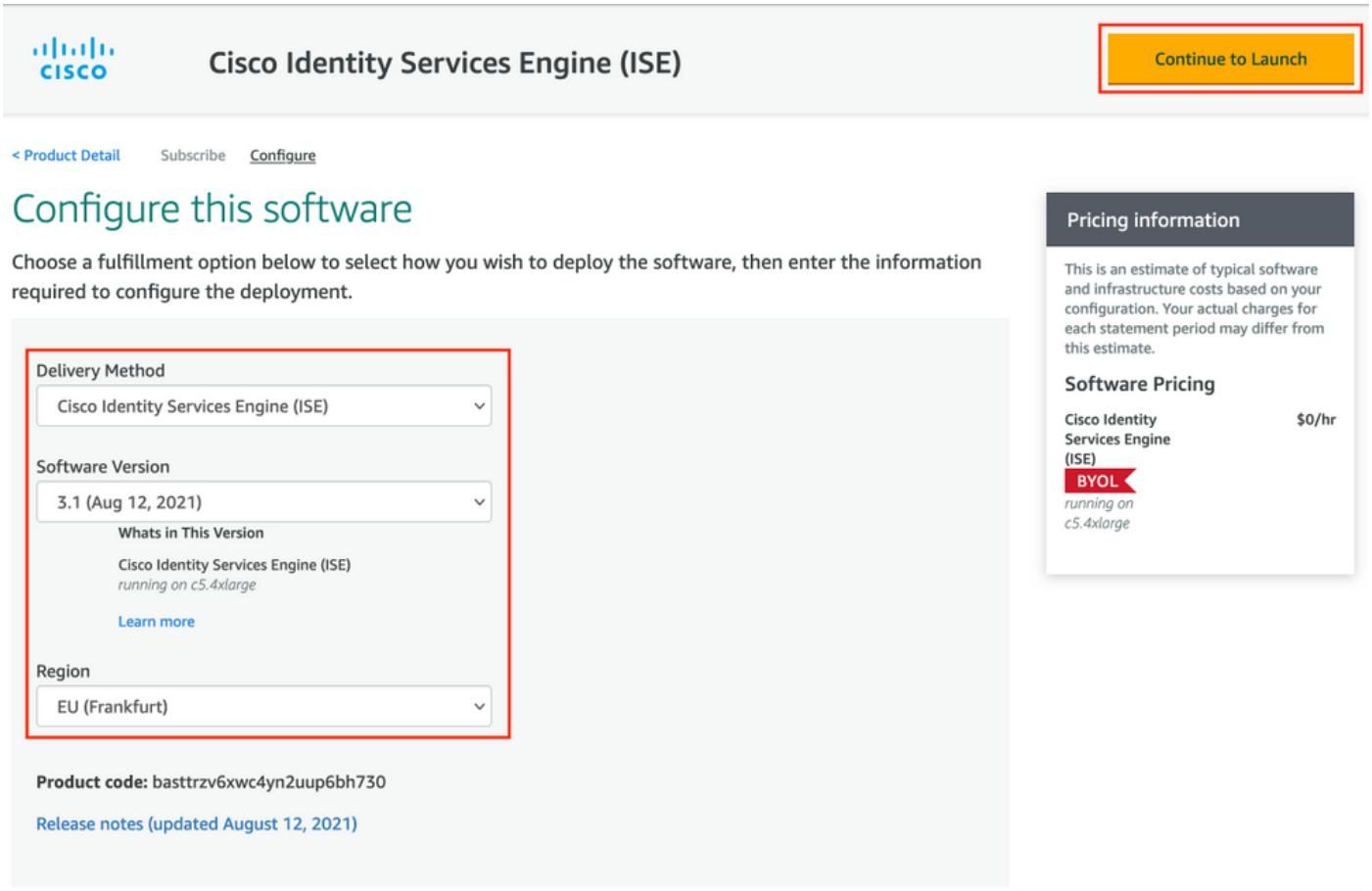


Peu après la **date d'entrée en vigueur** change à la date d'abonnement et la **date d'expiration** change à **S.O.** Sélectionnez **Continuer à la configuration** comme indiqué dans l'image



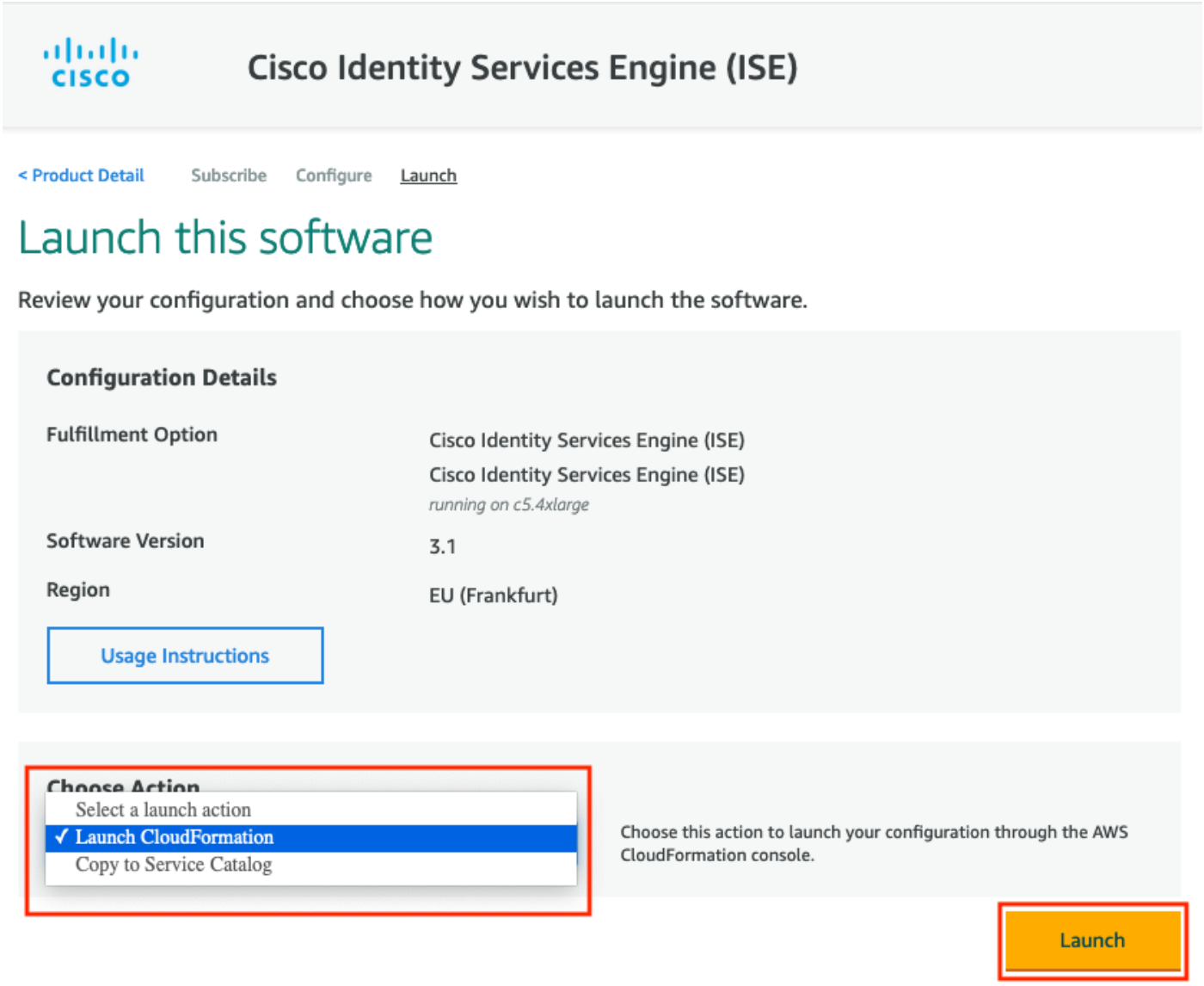
Étape 2. Configurer ISE sur AWS

Dans le menu Delivery Method de l'**écran Configure this software (Configurer ce logiciel)**, sélectionnez **Cisco Identity Services Engine (ISE).** Dans la **version du logiciel** sélectionnez **3.1 (12 août 2021)**. Sélectionnez la **région** où ISE doit être déployé. Sélectionnez **Continuer pour lancer.**



Étape 3. Lancer ISE sur AWS

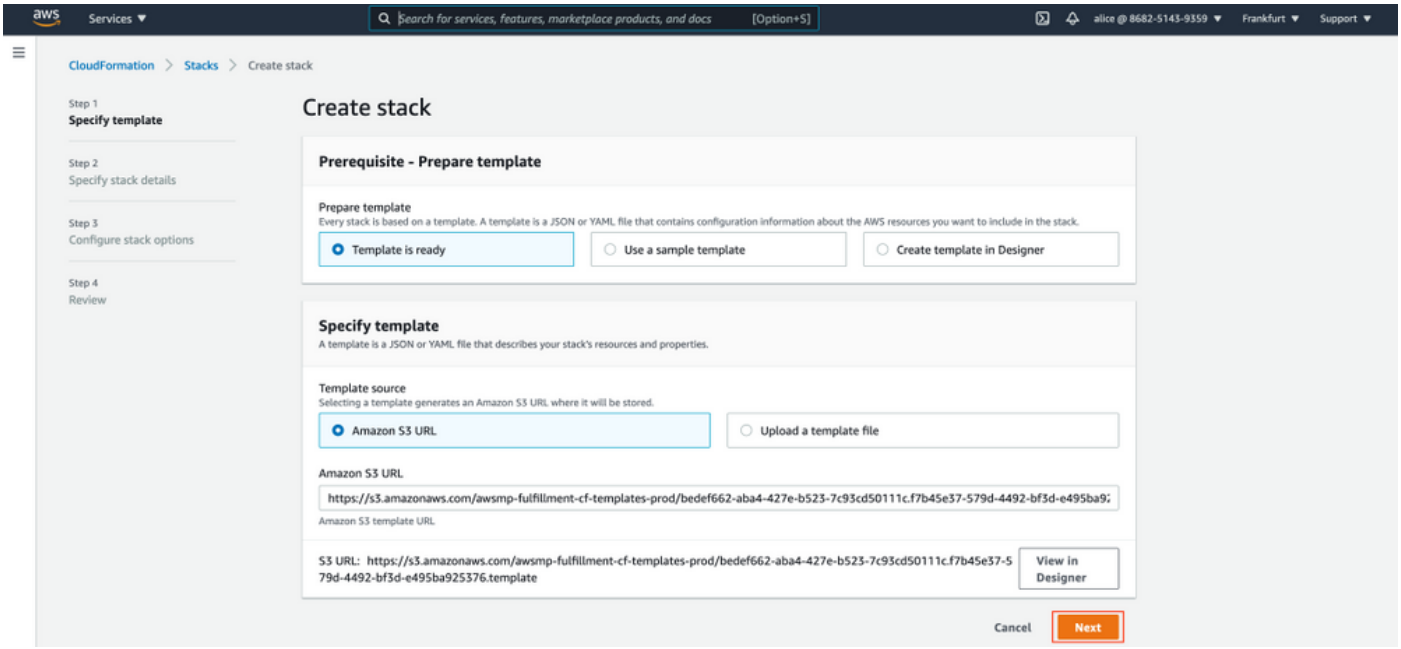
Dans le menu déroulant Actions de l'écran **Lancer ce logiciel**, sélectionnez **Lancer CloudFormation**.



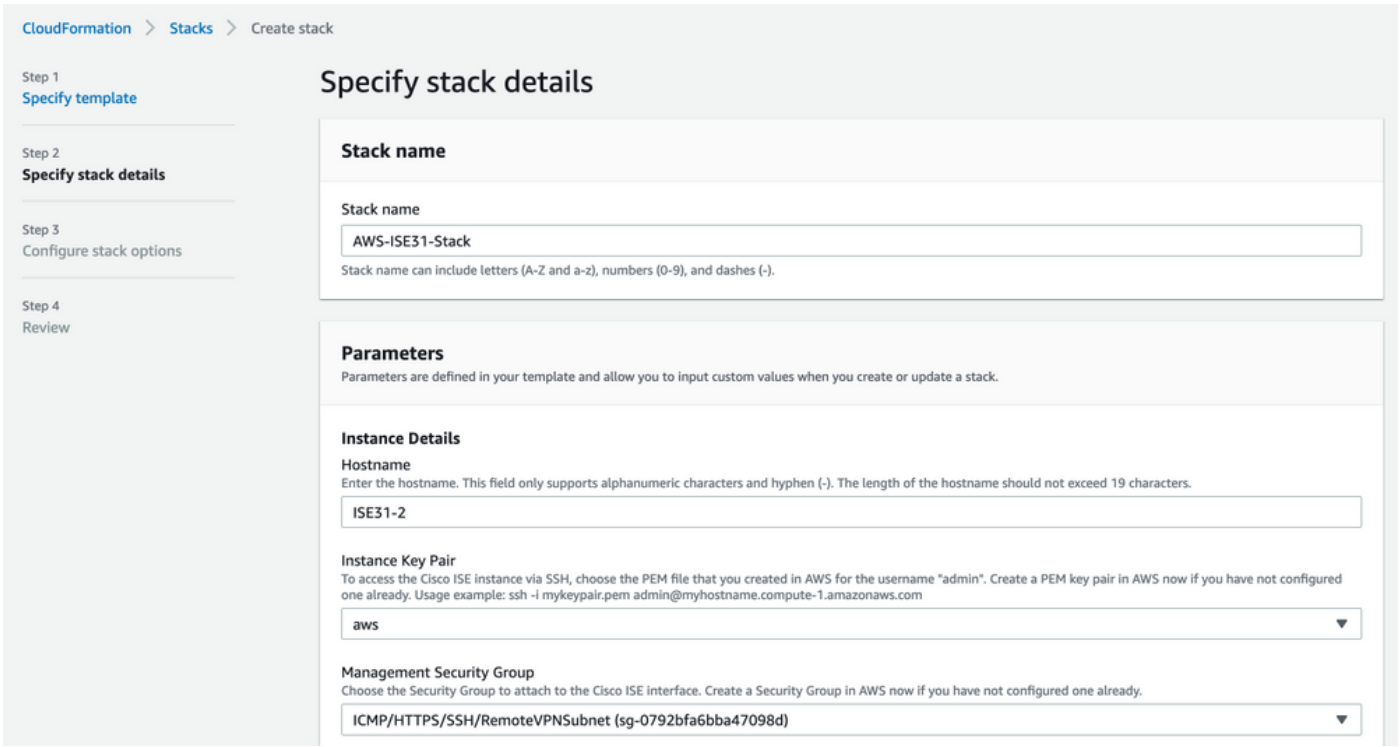
(Facultatif) Sélectionnez **Instructions d'utilisation** pour vous familiariser avec elles. Sélectionnez **Lancer**.

Étape 4. Configurer la pile CloudFormation pour ISE sur AWS

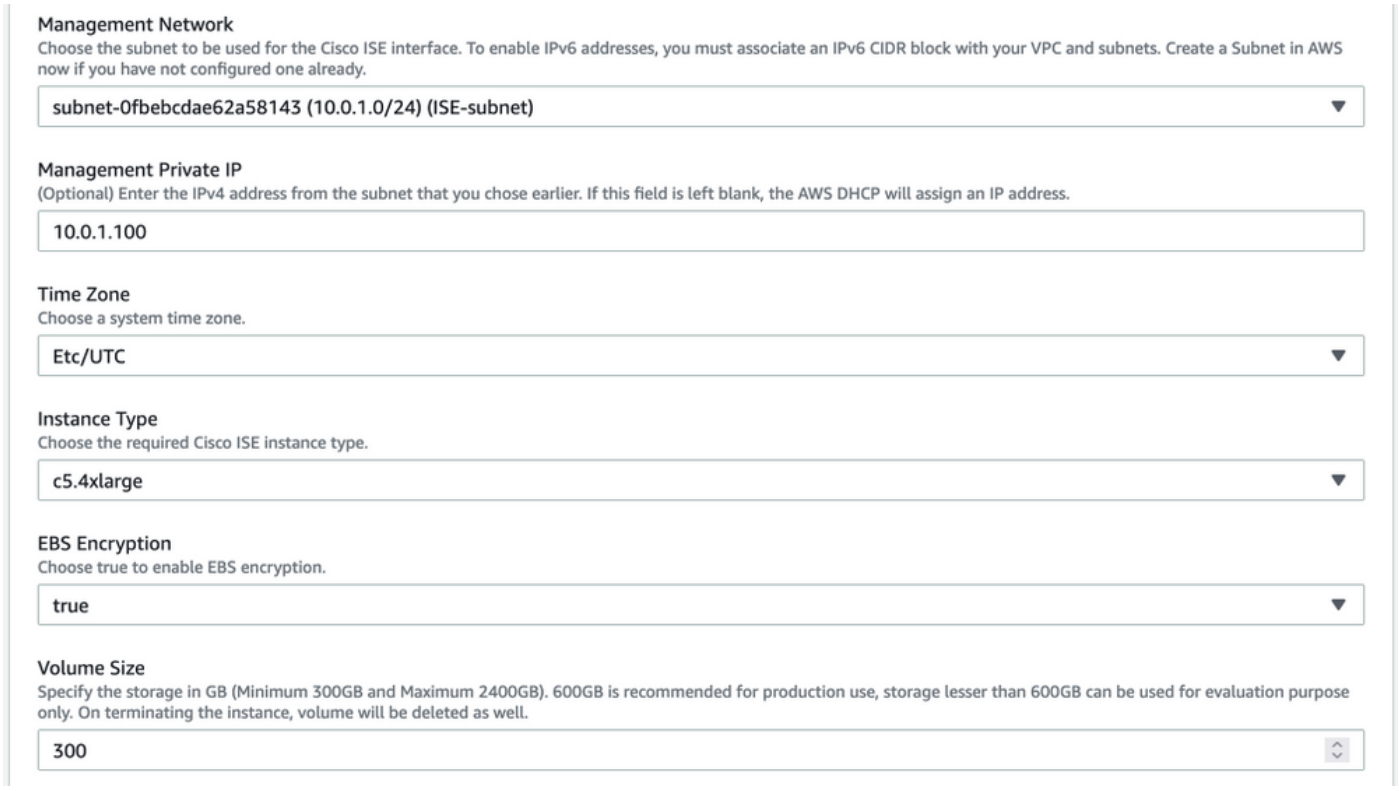
Le bouton de **lancement** vous redirige vers l'écran de configuration de **CloudFormation Stack**. Il existe un modèle préconfiguré qui doit être utilisé pour configurer ISE. Conservez les paramètres par défaut et sélectionnez **Suivant**.



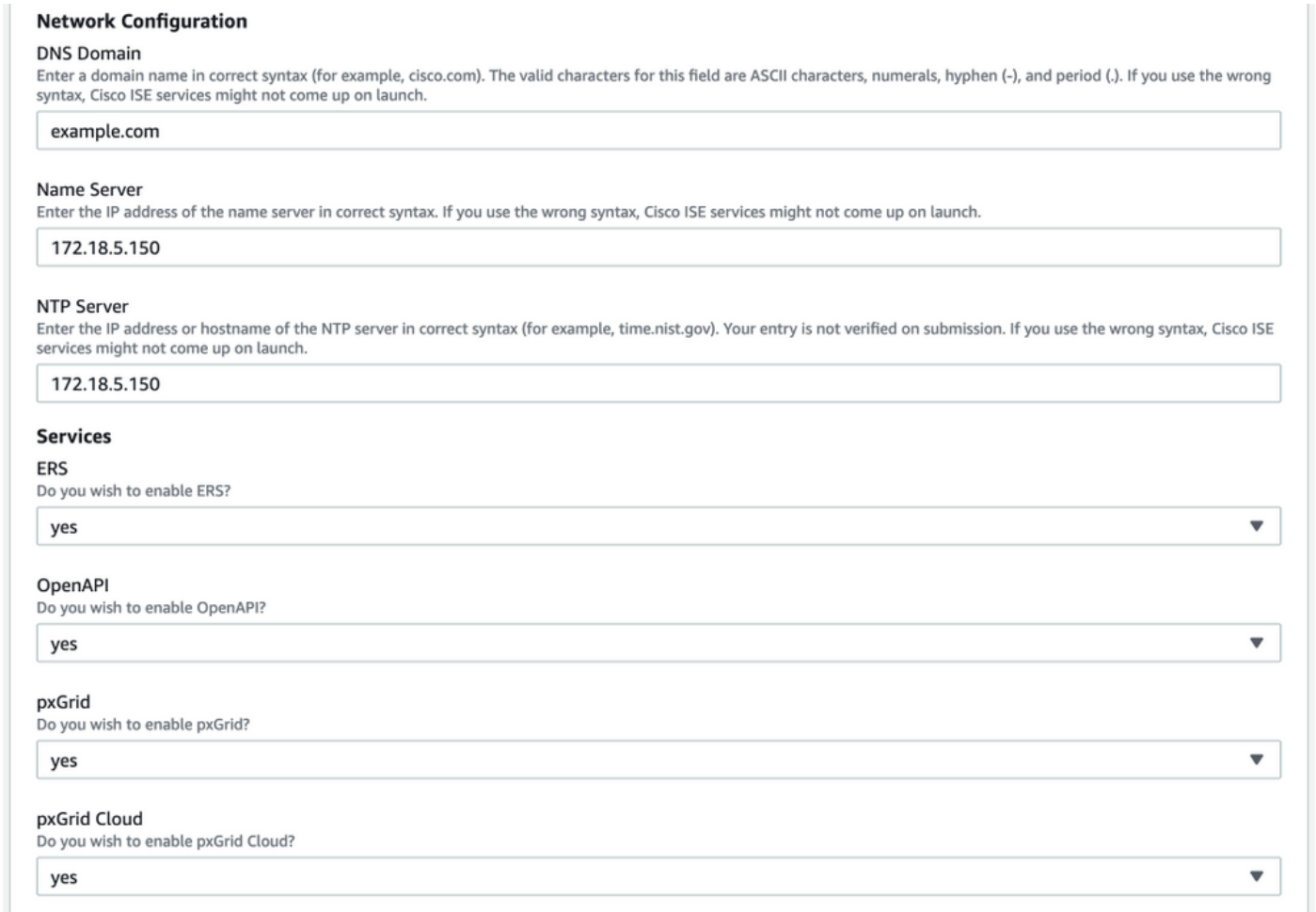
Remplir les données de la pile CloudFormation avec **le nom de la pile**. Configurez les détails de l'instance comme **Nom d'hôte**, sélectionnez **Paire de clés d'**instance et **Groupe de sécurité de gestion.**



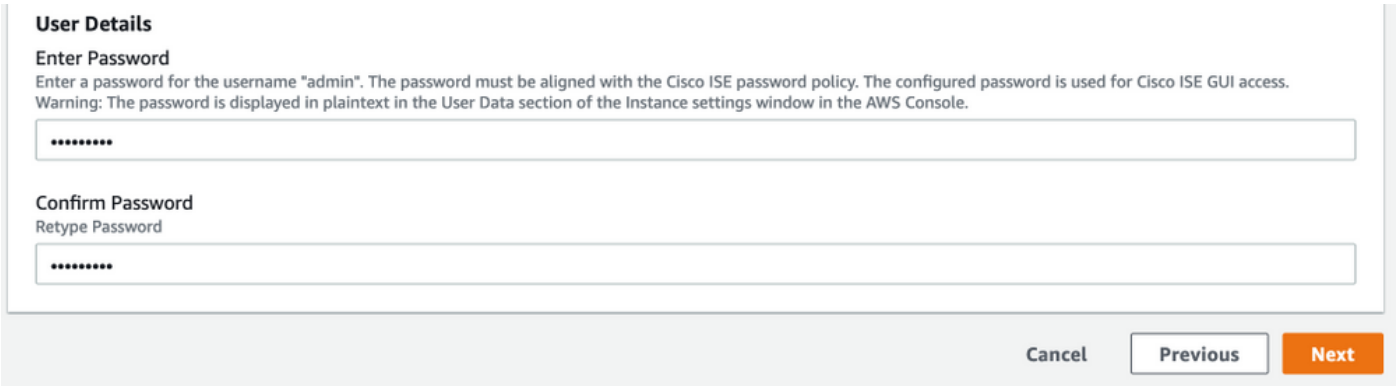
Continuer la configuration des détails de l'instance avec **Management Network, Management Private IP, Time Zone**, **Instance Type, EBS Encryption** et **Volume Size.**



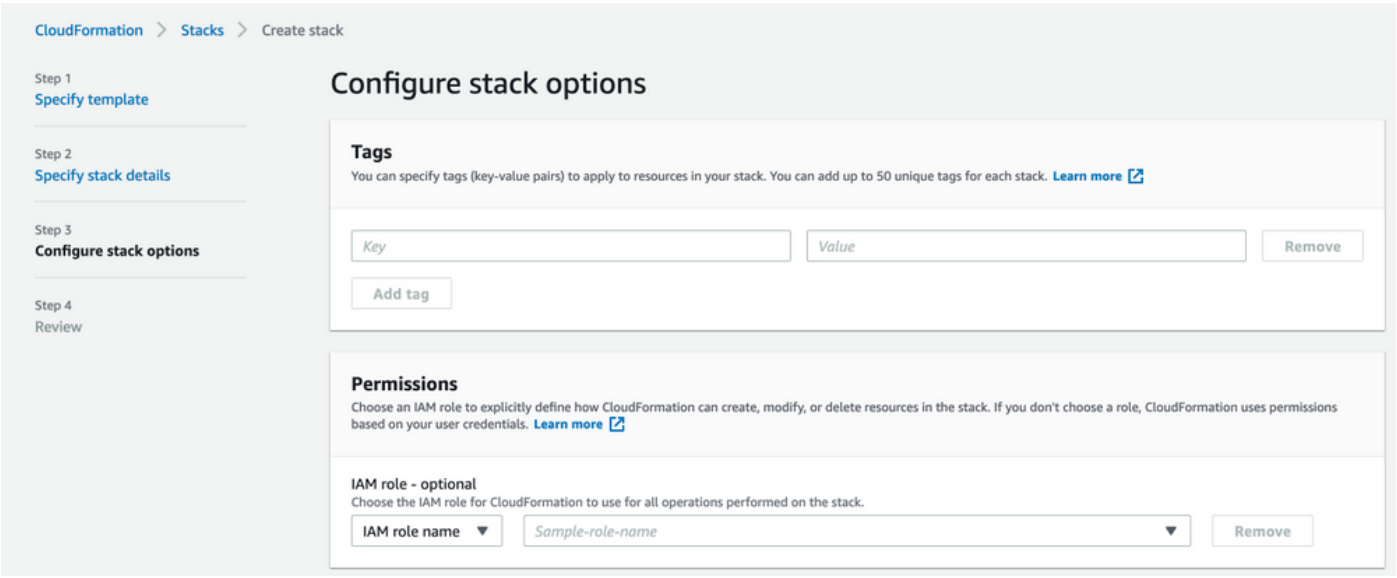
Poursuivez la configuration des détails de l'instance avec **DNS Domain, Name Server, NTP Service** et **Services**.



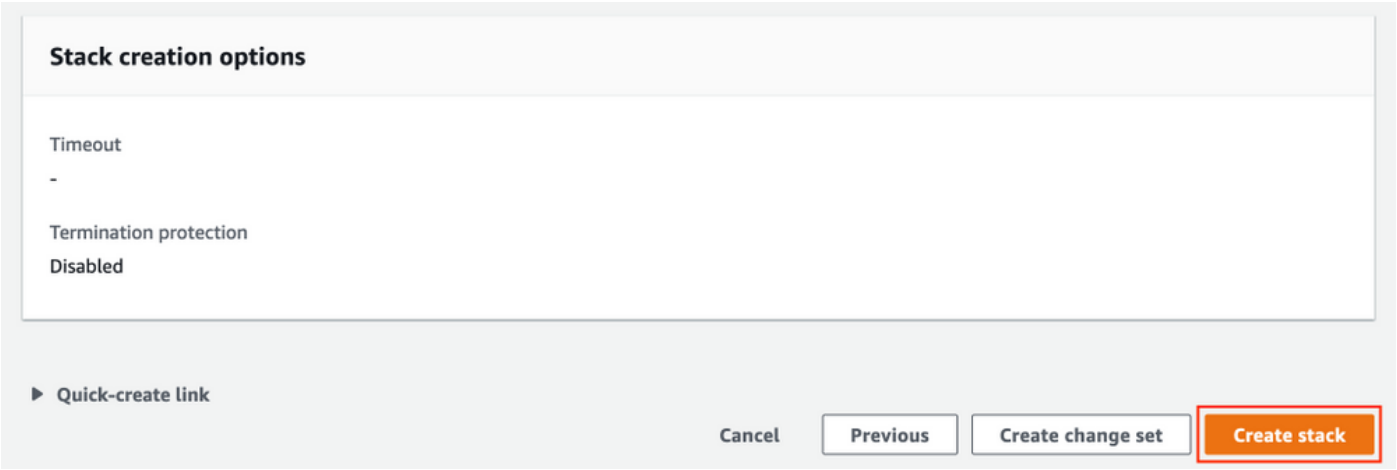
Configurez le mot de passe utilisateur de l'interface utilisateur graphique et sélectionnez **Suivant**.



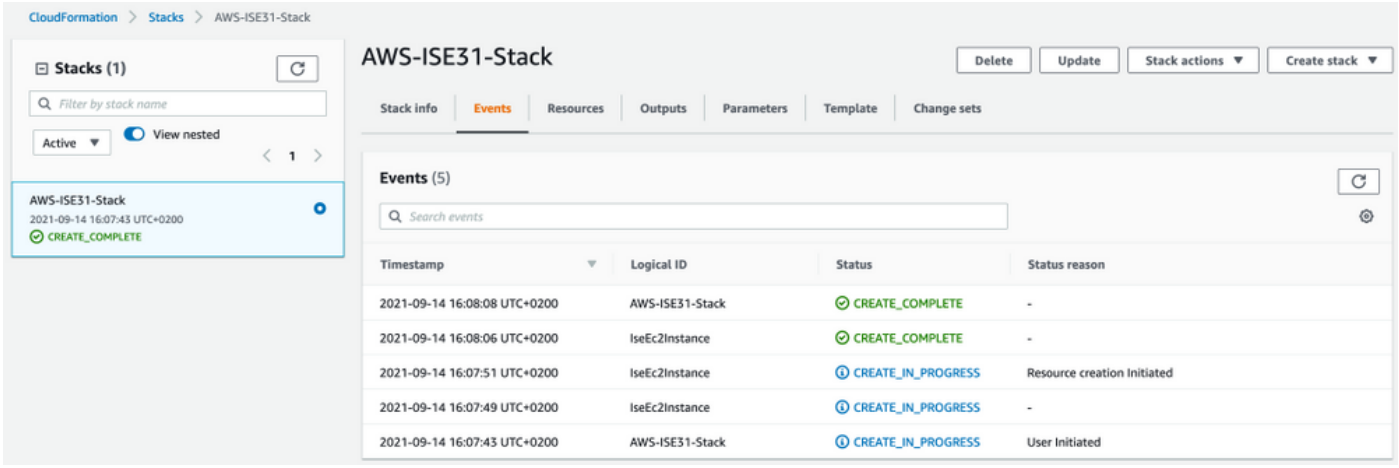
Aucun changement n'est requis sur l'écran suivant. Sélectionnez **Suivant**.



Accédez à l'écran **Vérifier la pile**, faites défiler la page vers le bas et sélectionnez **Créer une pile**.

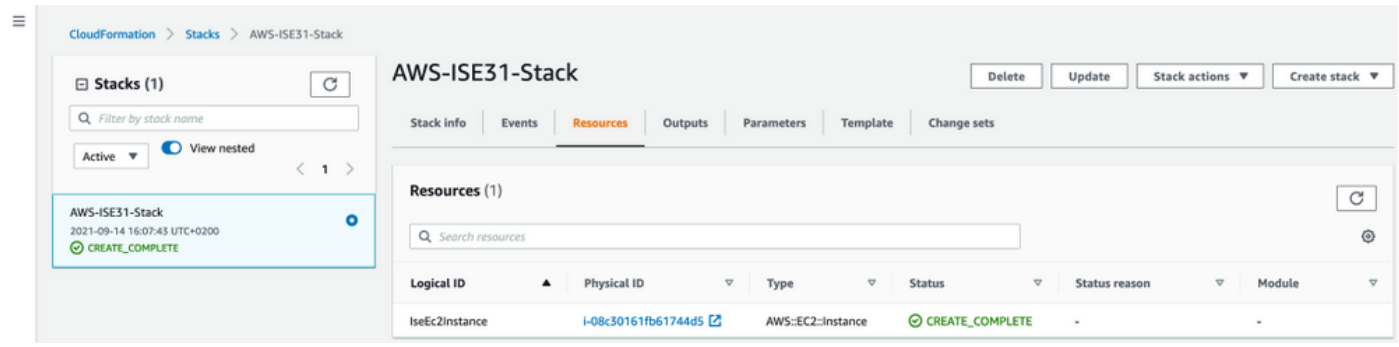


Une fois la pile déployée, l'état **CREATE_COMPLETE** doit être affiché.

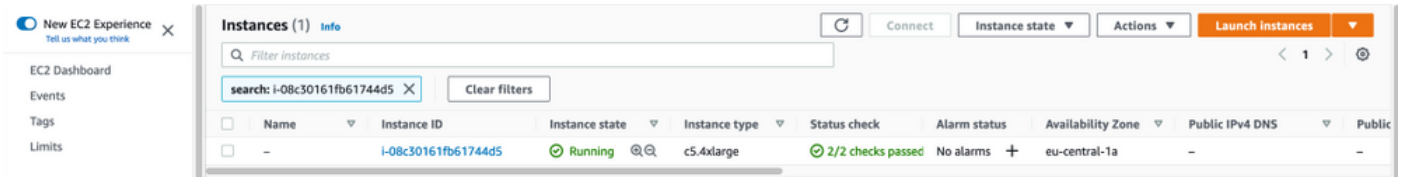


Étape 5. Accéder à ISE sur AWS

Pour accéder à l'instance ISE, accédez à l'onglet **Ressources** pour afficher l'instance EC2 créée à partir de CloudForms (vous pouvez également accéder à **Services > EC2 > Instances** afin d'afficher les instances EC2) comme indiqué dans l'image.



Sélectionnez **ID physique** afin d'ouvrir le menu **Instances EC2**. Assurez-vous que la **vérification d'état** a **réussi les vérifications 2/2**.



Sélectionnez **ID d'instance**. ISE est accessible via **une adresse IPv4 privée/DNS IPv4 privée** avec protocole SSH ou HTTPS.

> **Note**: Si vous accédez à ISE via une **adresse IPv4 privée/DNS IPv4 privée** assurez-vous qu'il existe une connectivité réseau vers une adresse privée ISE.

Exemple d'accès ISE via une **adresse IPv4 privée** via SSH :

```
[centos@ip-172-31-42-104 ~]$ ssh -i aws.pem admin@10.0.1.100
The authenticity of host '10.0.1.100 (10.0.1.100)' can't be established.
ECDSA key fingerprint is SHA256:G5NdGZ1rgPYnjnldPcXOLcJg9VICLSxnZA0kn0CfMPs.
ECDSA key fingerprint is MD5:aa:e1:7f:8f:35:e8:44:13:f3:48:be:d3:4f:5f:05:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.100' (ECDSA) to the list of known hosts.
Last login: Tue Sep 14 14:36:39 2021 from 172.31.42.104
```

```
Failed to log in 0 time(s)
ISE31-2/admin#
```

> **Note**: Il faut environ 20 minutes pour que ISE soit accessible via SSH. Jusqu'à ce moment la connectivité à ISE échoue avec "**Autorisation refusée (clé publique).**" .

Utilisez **show application status ise** afin de vérifier que les services sont en cours d'exécution :

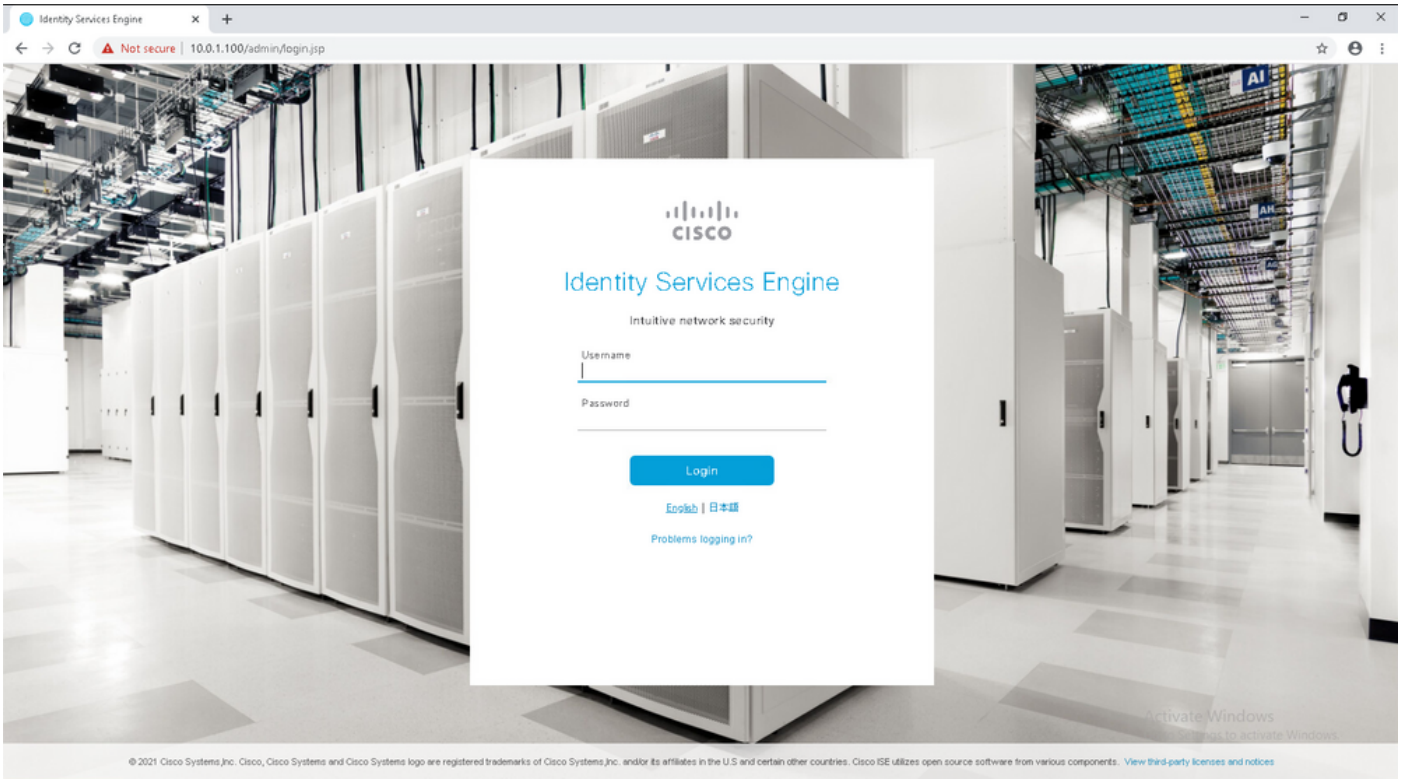
```
ISE31-2/admin# show application status ise

ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 27703
Database Server running 127 PROCESSES
Application Server                      running         47142
Profiler Database running 38593
ISE Indexing Engine running 48309
AD Connector running 56223
M&T Session Database running 37058
M&T Log Processor running 47400
Certificate Authority Service running 55683
EST Service running
SXP Engine Service disabled
TC-NAC Service disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 30760
ISE API Gateway Database Service running 35316
ISE API Gateway Service running 44900
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
Hermes (pxGrid Cloud Agent) Service disabled

ISE31-2/admin#
```

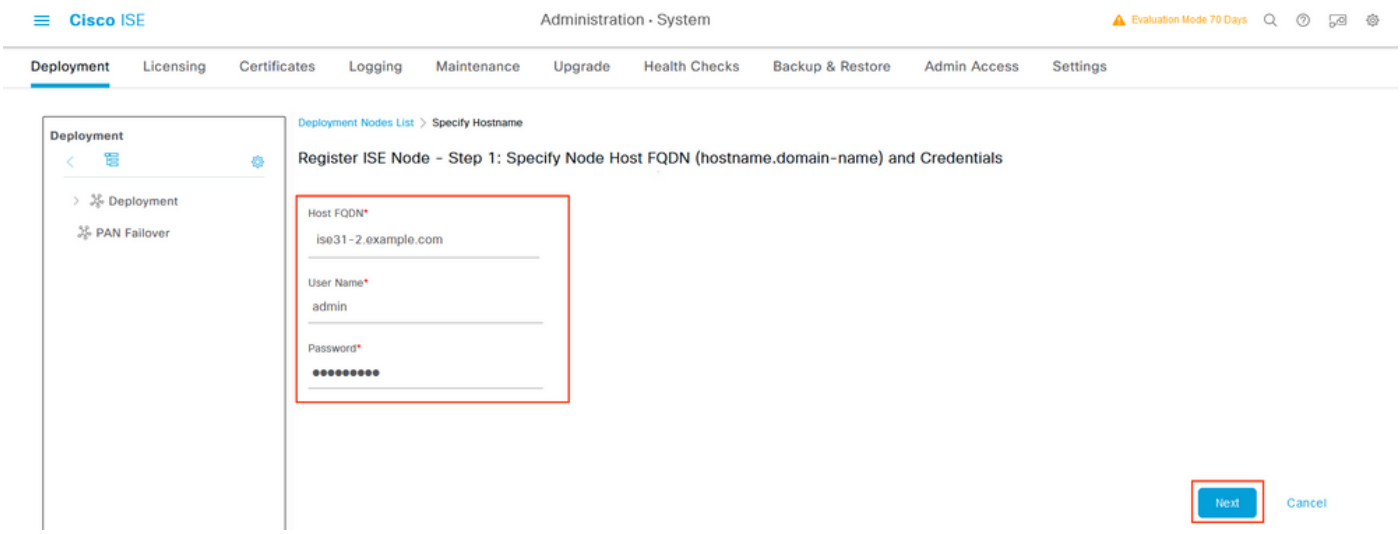
> **Note**: Cela prend environ 10 à 15 minutes depuis que SSH est disponible pour les services ISE pour passer à un état d'exécution.

Une fois que le **serveur d'applications** est en **état d'exécution**, vous pouvez accéder à ISE via l'interface utilisateur graphique, comme illustré dans l'image.

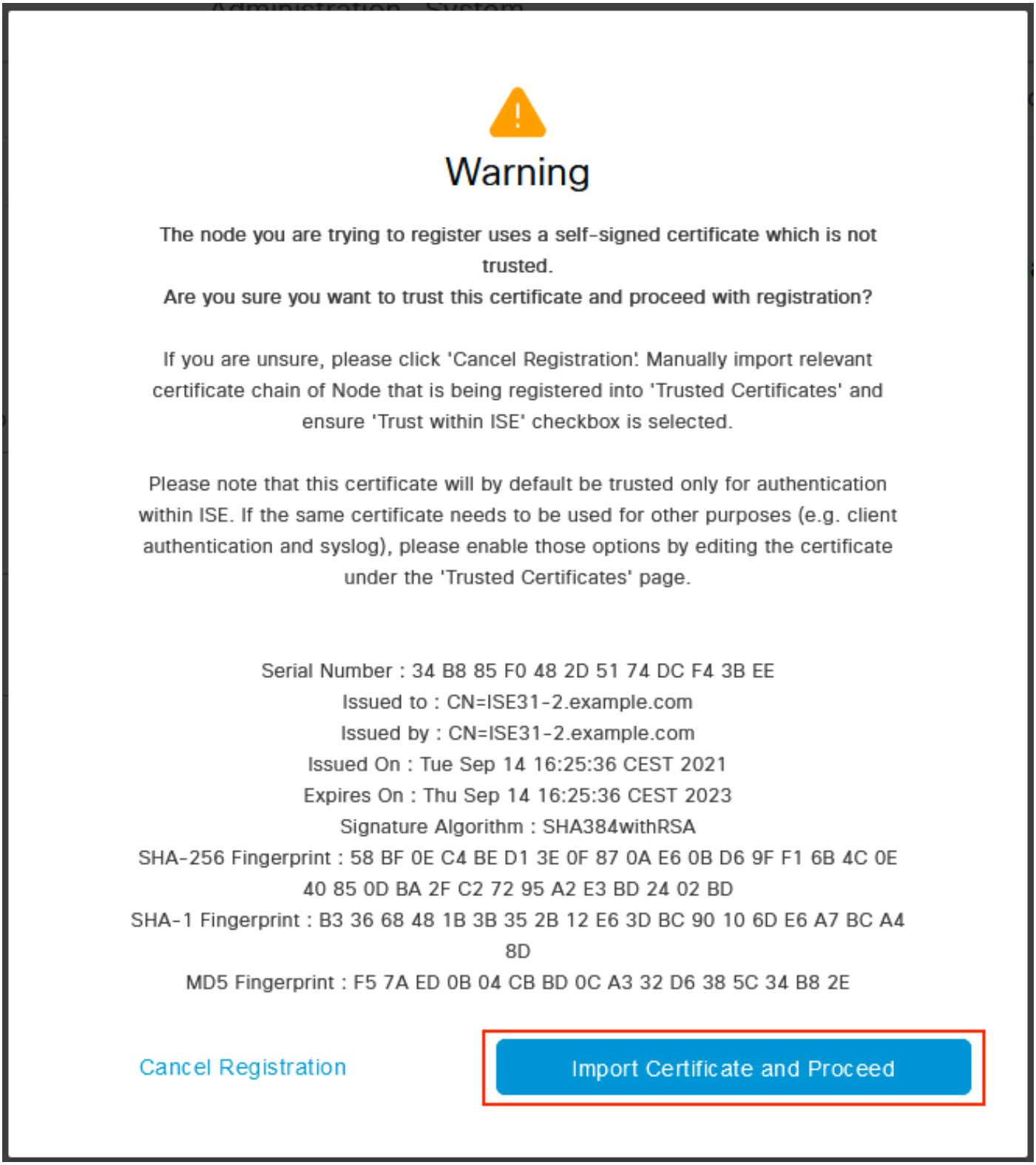


Étape 6. Configurer le déploiement distribué entre ISE sur site et ISE sur AWS

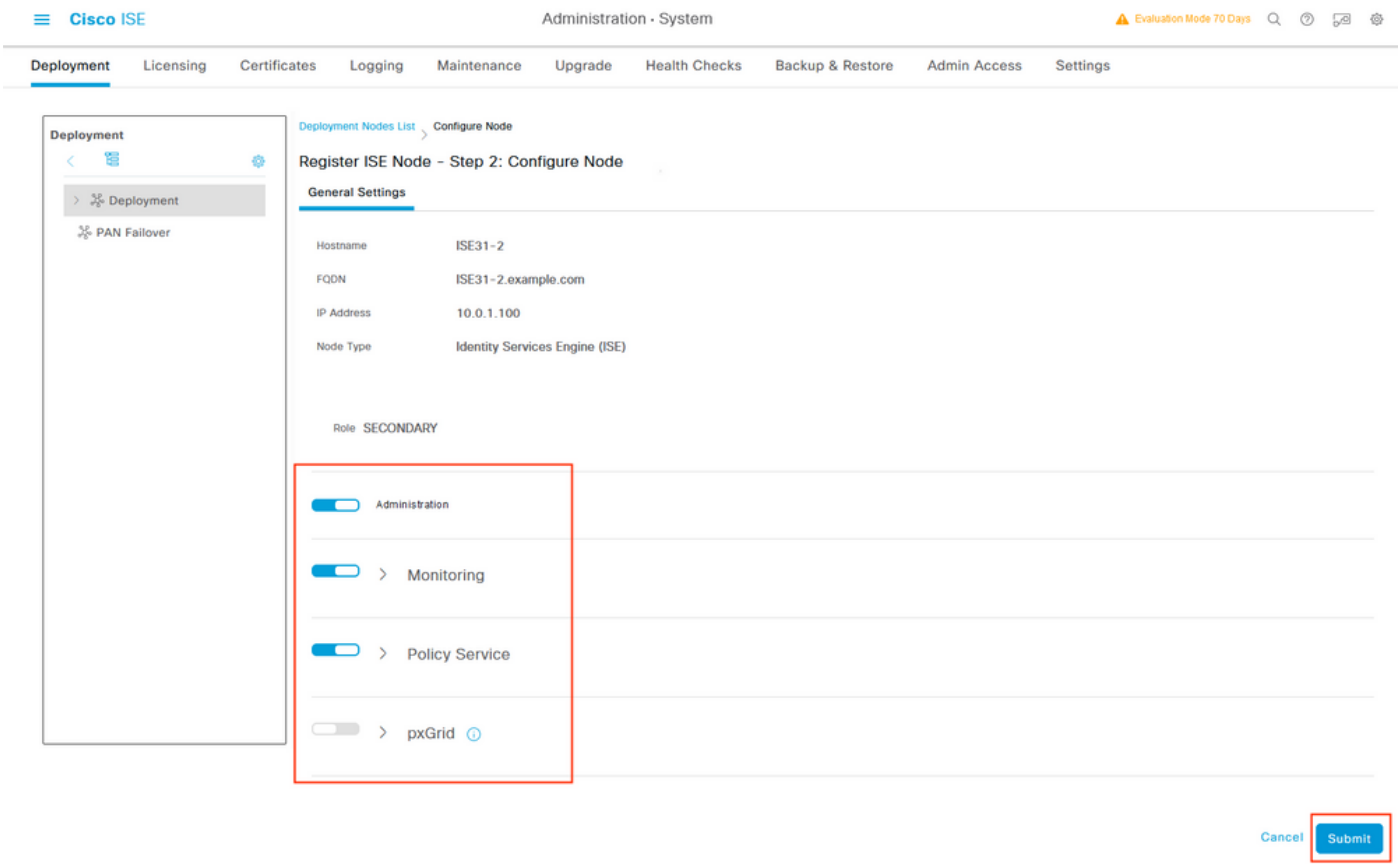
Connectez-vous à l'ISE sur site et accédez à **Administration > System > Deployment.** Sélectionnez le noeud et sélectionnez **Rendre principal.** Revenez à **Administration > System > Deployment**, Select **Register**. Configurez **le nom de domaine complet de l'hôte** ISE sur AWS, le **nom d'utilisateur** et le **mot de passe** de l'interface utilisateur graphique**.** Cliquez sur Next (Suivant).



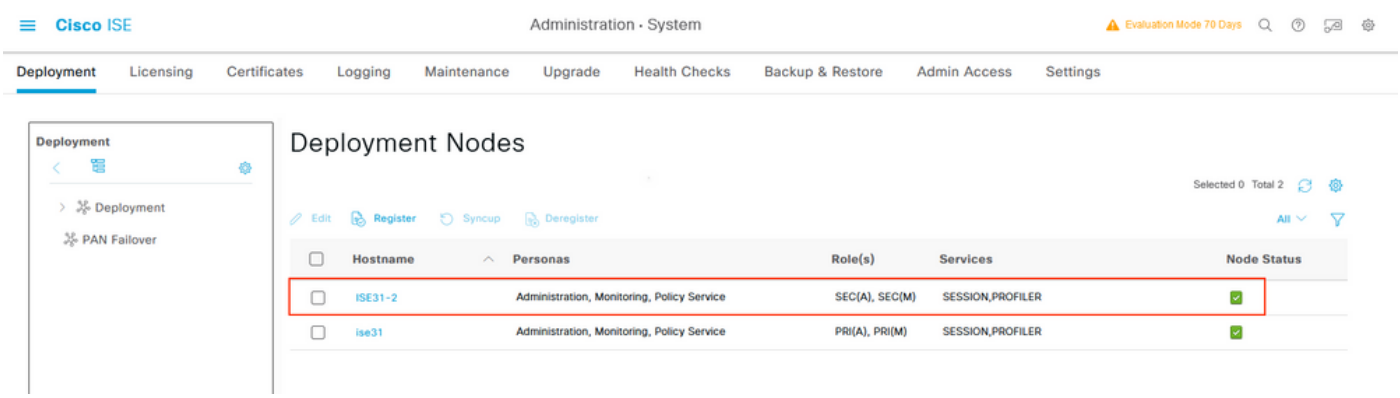
Étant donné que les certificats auto-signés sont utilisés dans cette topologie, pour importer des certificats d'administrateur dans le **certificat d'importation** Select Trusted Store **et continuer.**



Sélectionnez les personnages de votre choix et cliquez sur **Soumettre**.

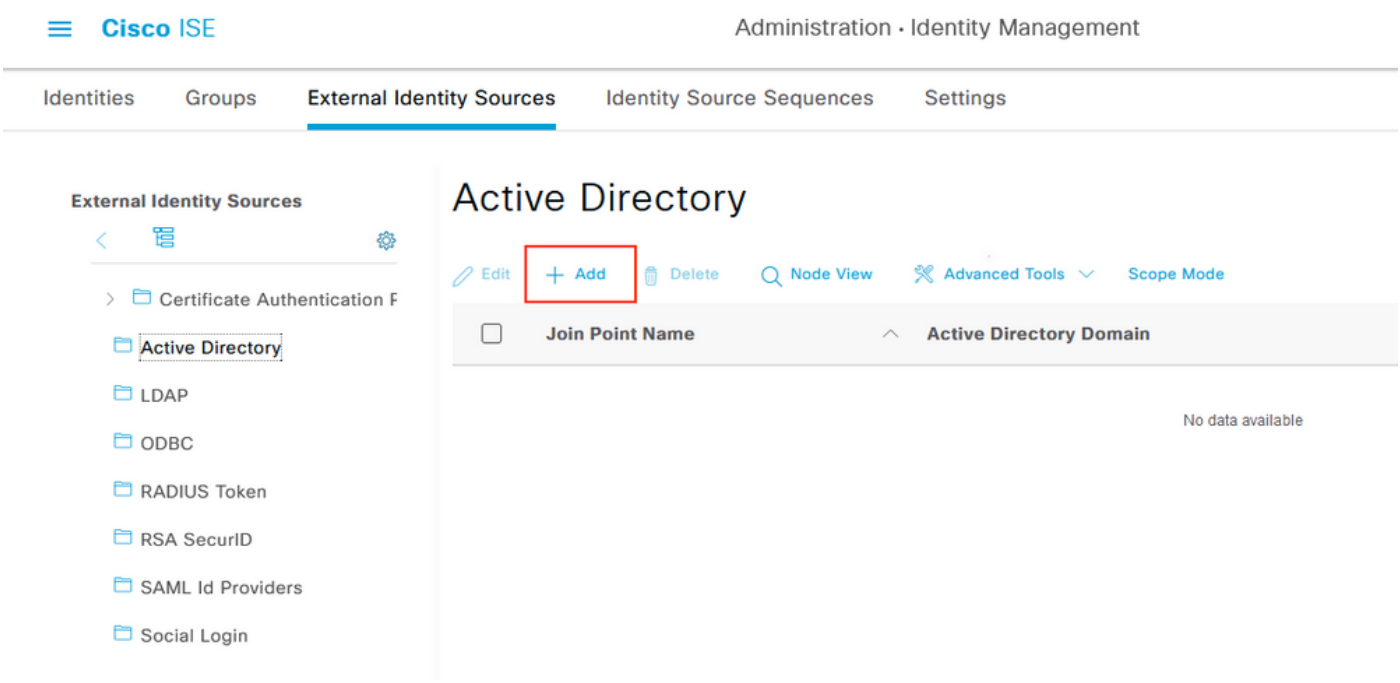


Une fois la synchronisation terminée, le noeud passe à l'état connecté, la case verte s'affiche contre lui.

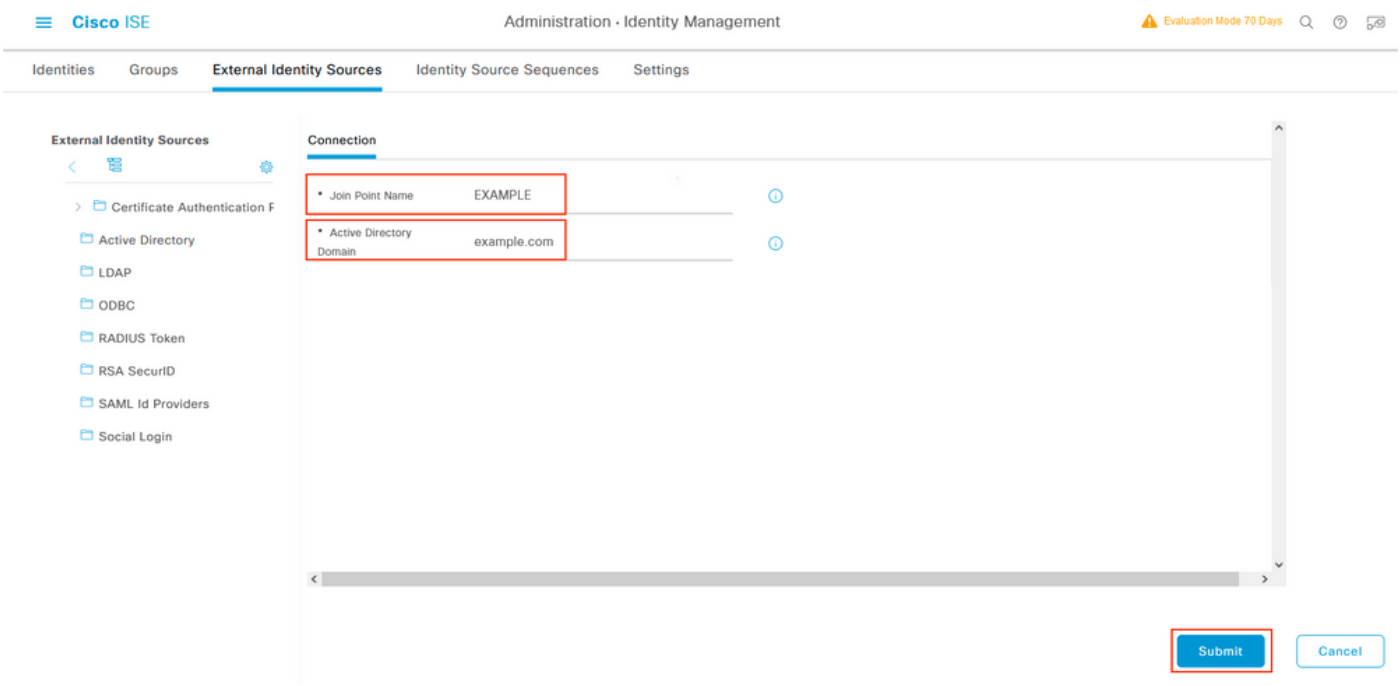


Étape 7. Intégration du déploiement ISE avec AD sur site

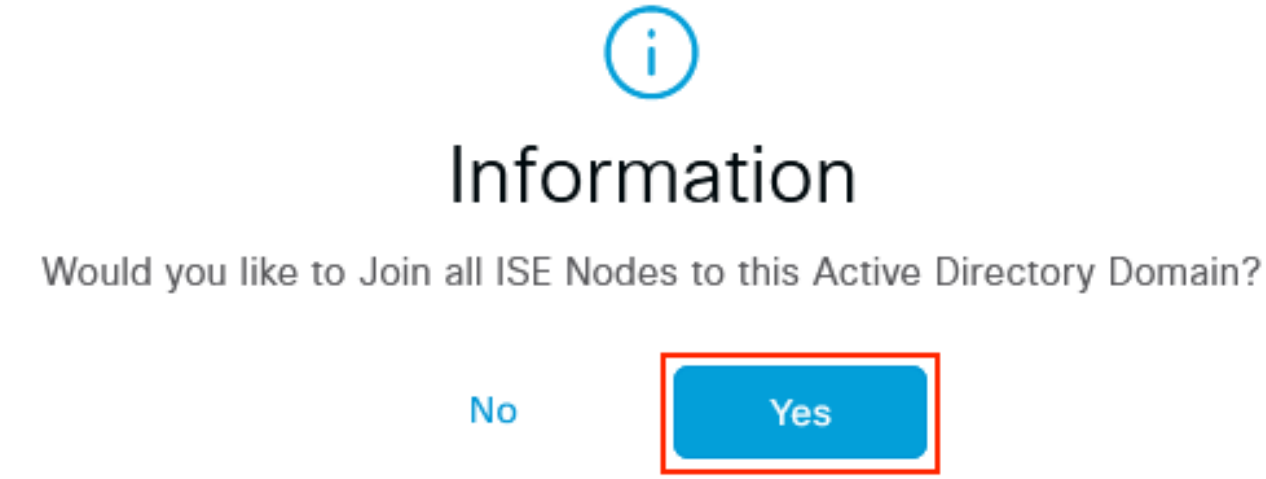
Accédez à **Administration > Identity Management > External Identity Sources**. Sélectionnez **Active Directory**, Sélectionner **Ajouter**.



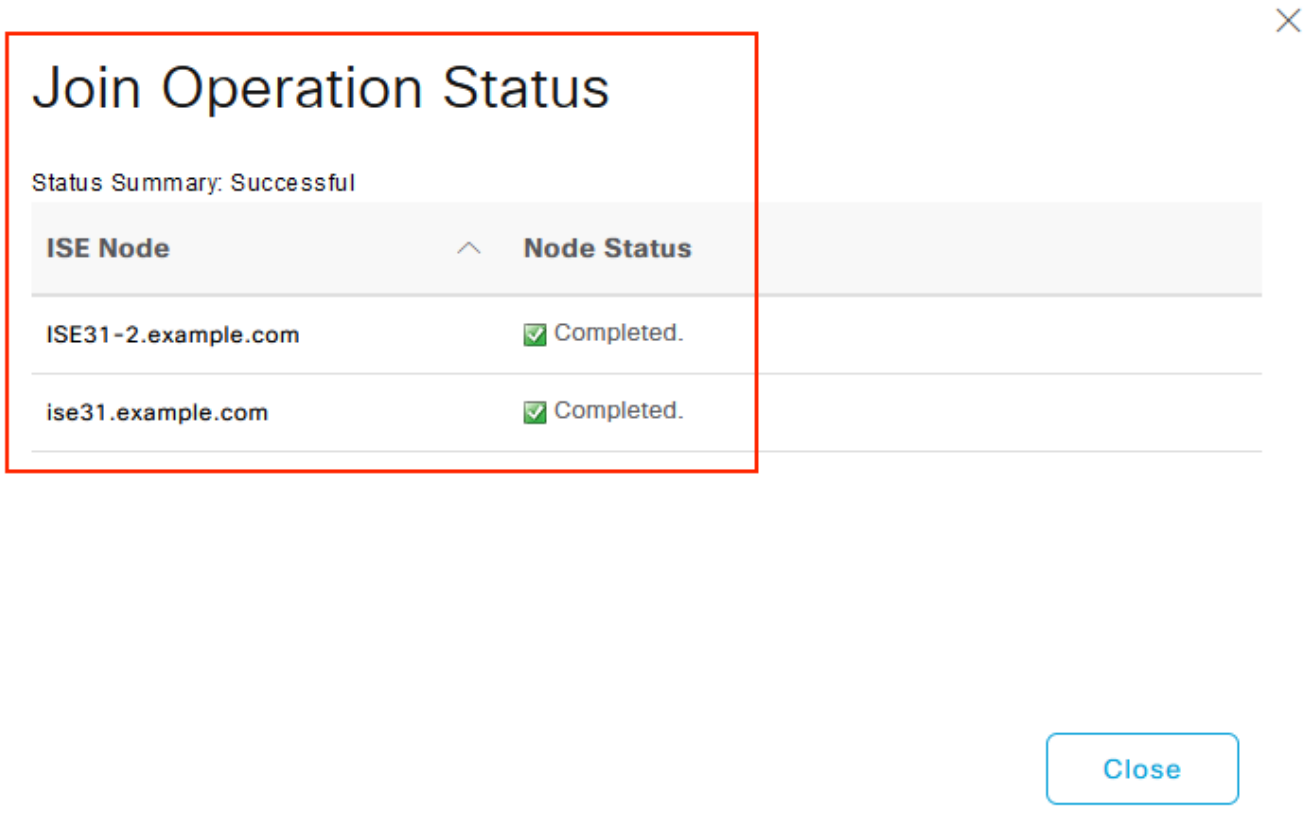
Configurez **Joint Point Name** et **Active Directory Domain**, sélectionnez **Submit**.



Pour intégrer les deux noeuds à Active Directory, sélectionnez **Oui**.



Entrez **Nom d'utilisateur** et **Mot de passe AD**, cliquez sur **OK**. Une fois que les noeuds ISE sont correctement intégrés à Active Directory, l'état du noeud devient Terminé.



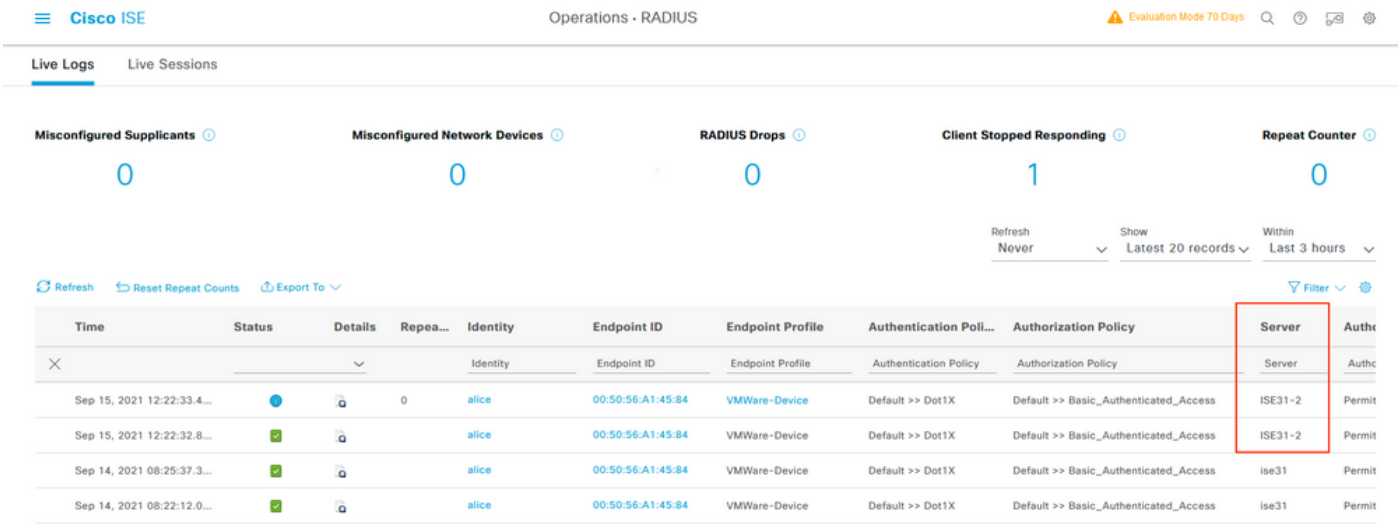
Limites

Pour connaître les limites ISE sur AWS, reportez-vous à la section Limitations connues du Guide d'administration ISE.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier que l'authentification est effectuée sur le PSN ISE situé sur AWS, accédez à **Operations > Radius > Live Logs**, puis confirmez dans la colonne **Server** ISE sur le PSN AWS.

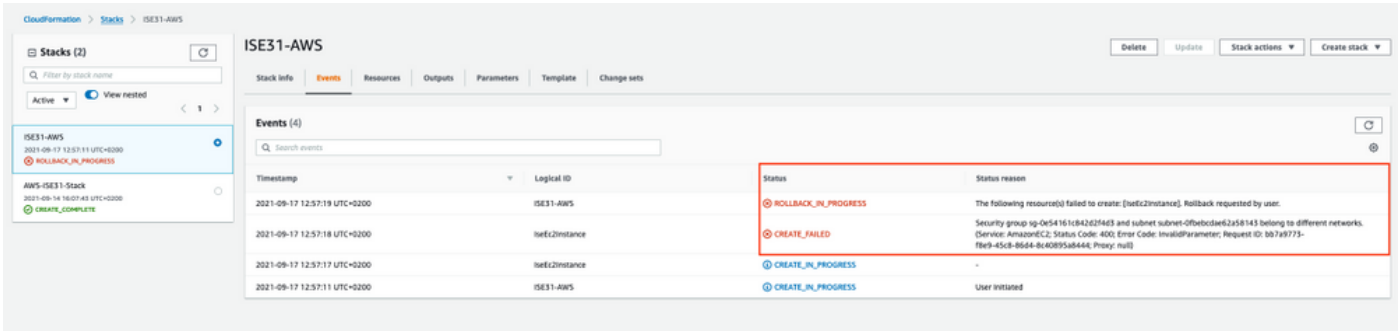


Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Échec de la création de la pile CloudFormation

La création de pile CloudFormation peut échouer pour plusieurs raisons, l'une d'elles étant que vous sélectionnez ce groupe de sécurité dans le VPN qui est différent du réseau de gestion d'ISE. L'erreur ressemble à celle de l'image.



Solution :

Assurez-vous de récupérer le groupe de sécurité à partir du même VPC. Accédez à **Groupes de sécurité** sous **VPC** Service, et notez l'**ID de groupe de sécurité**, assurez-vous qu'il correspond au VPC approprié (où réside ISE), vérifiez l'**ID VPC**.

Problèmes de connectivité

Il peut y avoir plusieurs problèmes qui peuvent empêcher la connectivité à ISE sur AWS de fonctionner.

1. Problème de connectivité en raison de **groupes de sécurité** mal configurés.

Solution : ISE ne peut pas être accessible à partir du réseau sur site ou même au sein des réseaux AWS si **les groupes de sécurité** sont mal configurés. Assurez-vous que les protocoles et les ports requis sont autorisés dans le **groupe de sécurité** associé au réseau ISE. Référez-vous à Référence des ports ISE pour les ports obligatoires à ouvrir.

2. Problèmes de connectivité dus à une configuration incorrecte du routage.

Solution : En raison de la complexité de la topologie, il est facile de rater certaines routes entre le réseau On-Prem et AWS. Avant de pouvoir utiliser les fonctionnalités ISE, assurez-vous que la connectivité de bout en bout est en place.

Annexe

Configuration associée au commutateur AAA/Radius

```
aaa new-model
!
!
aaa group server radius ISE-Group
server name ISE31-2
server name ISE31-1
!
aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group
!
aaa server radius dynamic-author
client 172.18.5.100 server-key cisco
client 10.0.1.100 server-key cisco
!
aaa session-id common
!
dot1x system-auth-control
!
vlan 1805
!
interface GigabitEthernet1/0/2
description VMWIN10
switchport access vlan 1805
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
!
interface Vlan1805
ip address 172.18.5.3 255.255.255.0
!
!
radius server ISE31-1
address ipv4 172.18.5.100 auth-port 1645 acct-port 1646
key cisco
!
radius server ISE31-2
address ipv4 10.0.1.100 auth-port 1645 acct-port 1646
key cisco
```

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.