

# 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

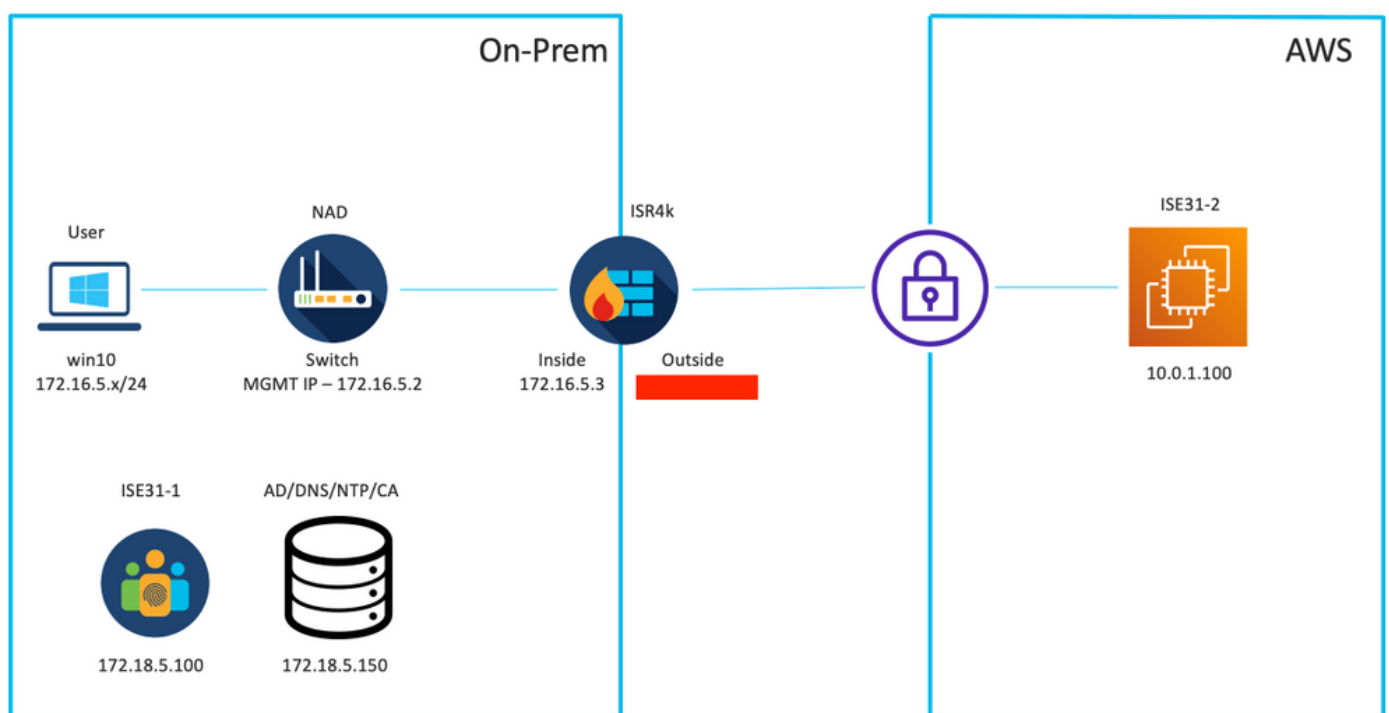
## Components Used

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

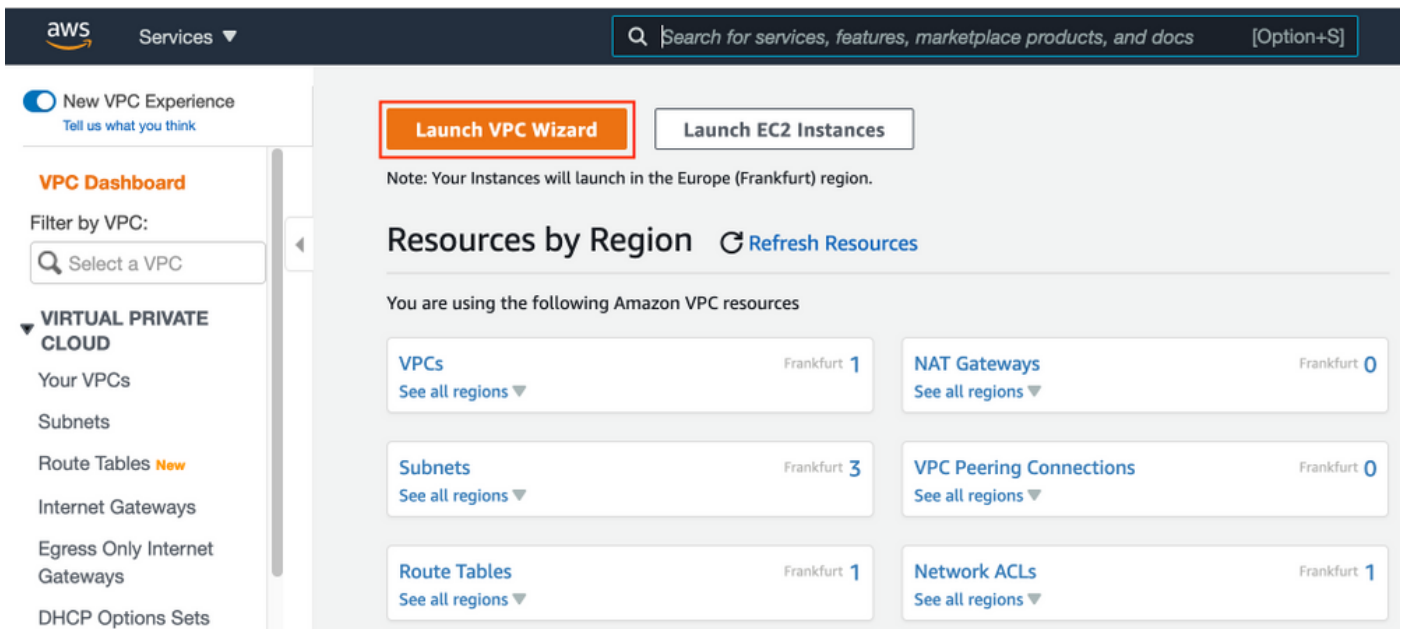


### Configurations

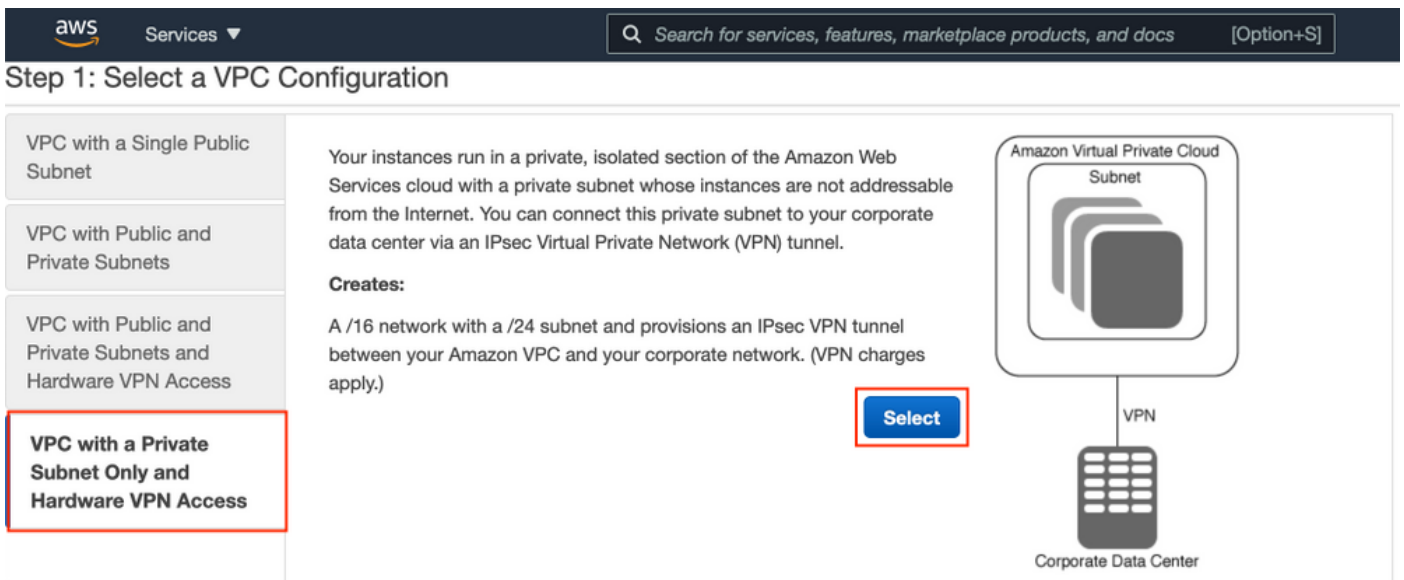
Si aucun VPC, groupe de sécurité, paire de clés et tunnel VPN n'est encore configuré, vous devez suivre les étapes facultatives, sinon, commencer par l'étape 1.

#### 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**.

aws Services Search for services, features, marketplace products, and docs [Option+S] alice @ 8682-5143-9359 Frankfurt Support

### Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block:  No IPv6 CIDR Block  
 Amazon provided IPv6 CIDR block  
 IPv6 CIDR block owned by me

VPC name: ISE-VPC

Private subnet's IPv4 CIDR: 10.0.1.0/24 (251 IP addresses available)

Availability Zone: No Preference

Private subnet name: ISE-subnet  
You can add more subnets after Amazon Web Services creates the VPC.

Service endpoints

Enable DNS hostnames:  Yes  No

Hardware tenancy: Default

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

aws Services Search for services, features, marketplace products, and docs [Option+S] alice @ 8682-5143-9359 Frankfurt Support

### Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP: [redacted]

Customer Gateway name: OnPrem-GW

VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection ([Help me choose](#))

Routing Type: Dynamic (requires BGP)

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

aws Services Search for services, features, marketplace products, and docs [Option+S] alice @ 8682-5143-9359 Frankfurt Support

### VPC Successfully Created

New VPC Experience  
Tell us what you think

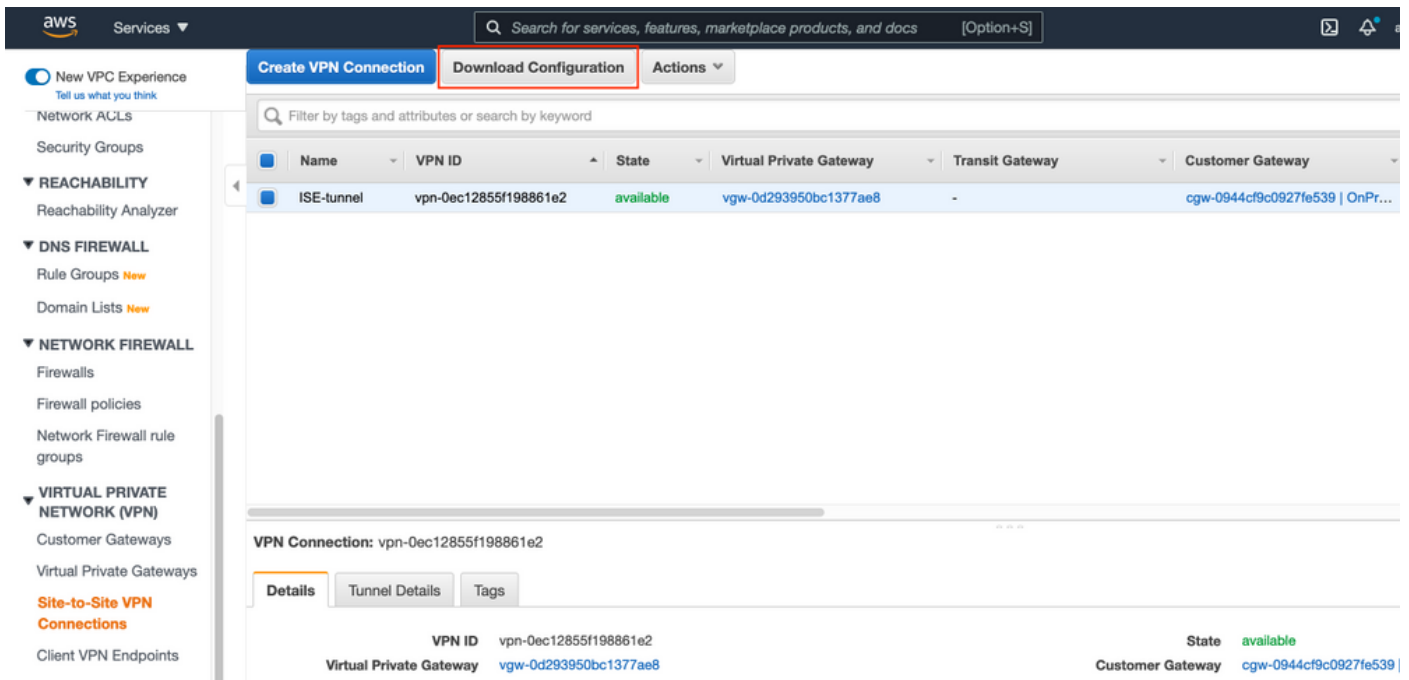
**Your VPC has been successfully created.**

You can launch instances into the subnets of your VPC. For more information, see [Launching an Instance into Your Subnet](#).

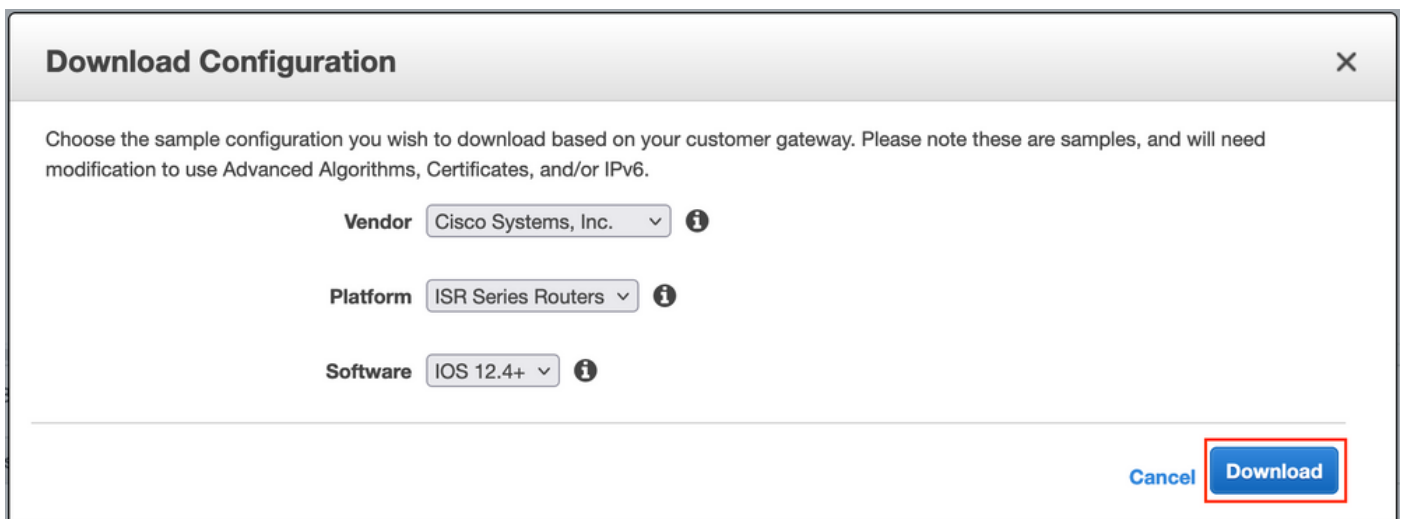
VPC Dashboard  
Filter by VPC:  
Select a VPC

**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**.

## Create key pair [Info](#)

### Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

#### Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

#### Key pair type [Info](#)

- RSA  
 ED25519

#### Private key file format

- .pem  
For use with OpenSSH  
 .ppk  
For use with PuTTY

#### Tags (Optional)

No tags associated with the resource.

You can add 50 more tags.

### 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.

EC2 > Security Groups > Create security group

## Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name [Info](#)  
  
Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

**Inbound rules** [Info](#)

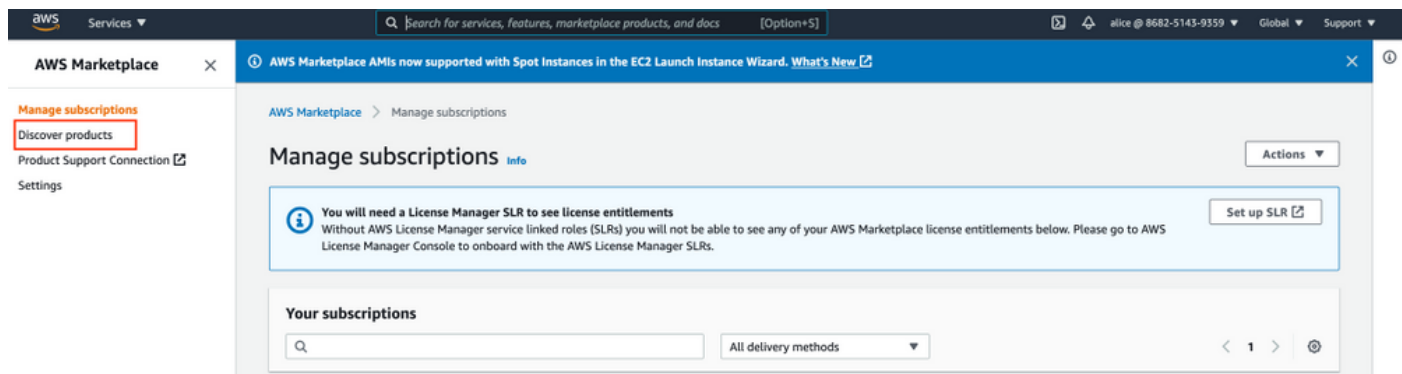
Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
SSH	TCP	22	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
All ICMP - IPv4	ICMP	All	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
HTTPS	TCP	443	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
All traffic	All	All	Custom <input type="text" value="172.18.5.0/24"/>		Delete

[Add rule](#)

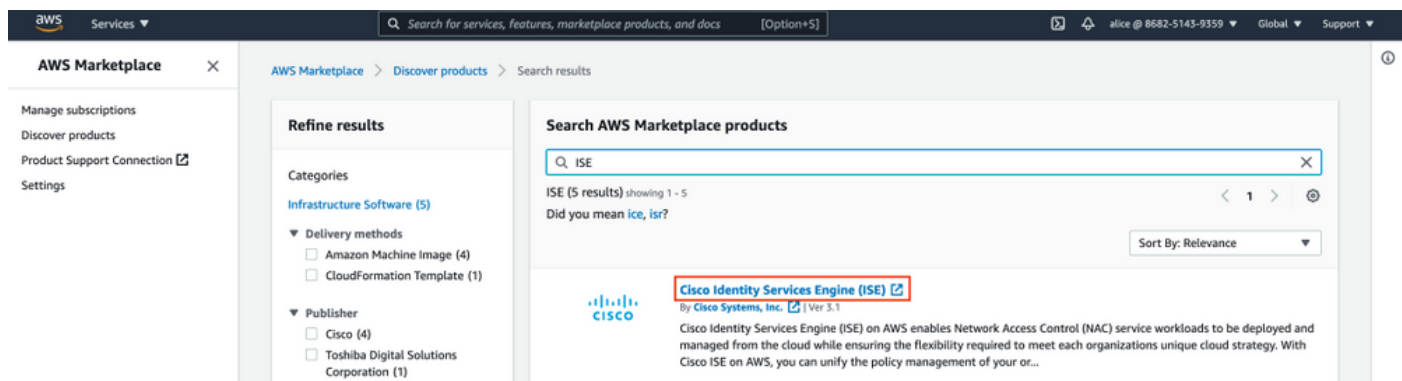
**Note:** Le groupe de sécurité configuré autorise l'accès SSH, ICMP, HTTPS à ISE et tous les protocoles à partir du sous-réseau On-Prem.

## 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**

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List 1

Hello, alice ▾

Partners Sell in AWS Marketplace Amazon Web Services Home Help

### Cisco Identity Services Engine (ISE)

By: [Cisco Systems, Inc.](#) Latest Version: 3.1

Cisco ISE on AWS provides secure network access control for IoT, BYOD, and corporate owned endpoints. Cisco ISE enables you to easily segment network access for employees, contractors, [Show more](#)

Linux/Unix **BYOL**

**Continue to Subscribe**

Remove

Typical Total Price  
**\$0.68/hr**

Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

## Product Overview

Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (NAC) service workloads to be deployed and managed from the cloud while ensuring the flexibility required to meet each organizations unique cloud strategy. With Cisco ISE on AWS, you can unify the policy management of your organization for endpoint access control and network device administration. Cisco ISE is equipped with rich APIs to automate policy and lifecycle management, bringing ease of deployment and automation to the forefront of your NAC operations.

For more information on Cisco ISE, please visit <http://www.cisco.com/go/ise>

Version	3.1
By	<a href="#">Cisco Systems, Inc.</a>
Video	<a href="#">See Product Video</a>

### Highlights

- Gain visibility with context and control: Know who, what, where, and how endpoints and devices are connecting to your network to ensure compliance and limit risk, with or without the use of agents.
- Extend zero trust to contain threats: Software-Defined Network segmentation shrinks the attack surface, limits the spread of ransomware, and enables rapid threat containment.
- Accelerate the value of existing solutions: Integrate with other Cisco and third-party solutions to bring an active arm of protection into passive security solutions and increase your return on investment (ROI).

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

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List 1

Hello, alice ▾

Partners Sell in AWS Marketplace Amazon Web Services Home Help

### Cisco Identity Services Engine (ISE)

**Continue to Configuration**

You must first review and accept terms.

[Product Detail](#) [Subscribe](#)

## Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

### Terms and Conditions

Cisco Systems, Inc. Offer

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

**Accept Terms**

The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Cisco Identity Services Engine (ISE) <b>BYOL</b>	Additional taxes or fees may apply.
	Cisco Identity Services Engine (ISE)

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



Thank you for subscribing to this product! We are processing your request.

X

[< Product Detail](#) [Subscribe](#)

## Subscribe to this software

Your subscription to this product is pending and may take a few minutes. You will be notified on this page when the subscription is complete.

### Terms and Conditions

#### Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	<input type="radio"/> Pending	<input type="radio"/> Pending	<a href="#">Show Details</a>

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



## Cisco Identity Services Engine (ISE)

[Continue to Configuration](#)

Thank you for subscribing to this product! You can now configure your software.

X

[< Product Detail](#) [Subscribe](#)

## Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

#### Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	8/23/2021	N/A	<a href="#">Show Details</a>

## 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**.



[< Product Detail](#)   [Subscribe](#)   [Configure](#)

## Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

**Delivery Method**

Cisco Identity Services Engine (ISE) ▾

**Software Version**

3.1 (Aug 12, 2021) ▾

**Whats in This Version**

Cisco Identity Services Engine (ISE)  
*running on c5.4xlarge*

[Learn more](#)

**Region**

EU (Frankfurt) ▾

Product code: basttrzv6xwc4yn2uup6bh730

[Release notes \(updated August 12, 2021\)](#)

### Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

#### Software Pricing

Cisco Identity Services Engine (ISE)	\$0/hr
<b>BYOL</b>	
<i>running on c5.4xlarge</i>	

## Étape 3. Lancer ISE sur AWS

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



# Cisco Identity Services Engine (ISE)

[< Product Detail](#)   [Subscribe](#)   [Configure](#)   [Launch](#)

## Launch this software

Review your configuration and choose how you wish to launch the software.

### Configuration Details

Fulfillment Option	Cisco Identity Services Engine (ISE) Cisco Identity Services Engine (ISE) <i>running on c5.4xlarge</i>
Software Version	3.1
Region	EU (Frankfurt)

[Usage Instructions](#)

### Choose Action

- Select a launch action
- Launch CloudFormation
- Copy to Service Catalog

Choose this action to launch your configuration through the AWS CloudFormation console.

[Launch](#)

(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**.

CloudFormation > Stacks > Create stack

Step 1  
**Specify template**

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review

## Create stack

**Prerequisite - Prepare template**

**Prepare template**  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready  Use a sample template  Create template in Designer

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

**Template source**  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL  Upload a template file

Amazon S3 URL  
https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba9:

Amazon S3 template URL  
S3 URL: https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba925376.template [View in Designer](#)

Cancel [Next](#)

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**.

CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
**Specify stack details**

Step 3  
Configure stack options

Step 4  
Review

## Specify stack details

**Stack name**

Stack name  
AWS-ISE31-Stack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**  
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Instance Details**

**Hostname**  
Enter the hostname. This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.

ISE31-2

**Instance Key Pair**  
To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the username "admin". Create a PEM key pair in AWS now if you have not configured one already. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com

aws

**Management Security Group**  
Choose the Security Group to attach to the Cisco ISE interface. Create a Security Group in AWS now if you have not configured one already.

ICMP/HTTPS/SSH/RemoteVPNSubnet (sg-0792bfa6bba47098d)

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

### Management Network

Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a Subnet in AWS now if you have not configured one already.

subnet-0fbecdae62a58143 (10.0.1.0/24) (ISE-subnet) ▼

### Management Private IP

(Optional) Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP will assign an IP address.

10.0.1.100

### Time Zone

Choose a system time zone.

Etc/UTC ▼

### Instance Type

Choose the required Cisco ISE instance type.

c5.4xlarge ▼

### EBS Encryption

Choose true to enable EBS encryption.

true ▼

### Volume Size

Specify the storage in GB (Minimum 300GB and Maximum 2400GB). 600GB is recommended for production use, storage lesser than 600GB can be used for evaluation purpose only. On terminating the instance, volume will be deleted as well.

300 ↕

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

### Network Configuration

#### DNS Domain

Enter a domain name in correct syntax (for example, cisco.com). The valid characters for this field are ASCII characters, numerals, hyphen (-), and period (.). If you use the wrong syntax, Cisco ISE services might not come up on launch.

example.com

#### Name Server

Enter the IP address of the name server in correct syntax. If you use the wrong syntax, Cisco ISE services might not come up on launch.

172.18.5.150

#### NTP Server

Enter the IP address or hostname of the NTP server in correct syntax (for example, time.nist.gov). Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

172.18.5.150

### Services

#### ERS

Do you wish to enable ERS?

yes ▼

#### OpenAPI

Do you wish to enable OpenAPI?

yes ▼

#### pxGrid

Do you wish to enable pxGrid?

yes ▼

#### pxGrid Cloud

Do you wish to enable pxGrid Cloud?

yes ▼

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

**User Details**

**Enter Password**  
Enter a password for the username "admin". The password must be aligned with the Cisco ISE password policy. The configured password is used for Cisco ISE GUI access.  
Warning: The password is displayed in plaintext in the User Data section of the Instance settings window in the AWS Console.

**Confirm Password**  
Retype Password

Cancel Previous **Next**

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

CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
Specify stack details

Step 3  
**Configure stack options**

Step 4  
Review

### Configure stack options

**Tags**  
You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more](#)

Key	Value	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

**Permissions**  
Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

**IAM role - optional**  
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name	Remove
<input type="text" value="Sample-role-name"/>	<input type="button" value="Remove"/>

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

### Stack creation options

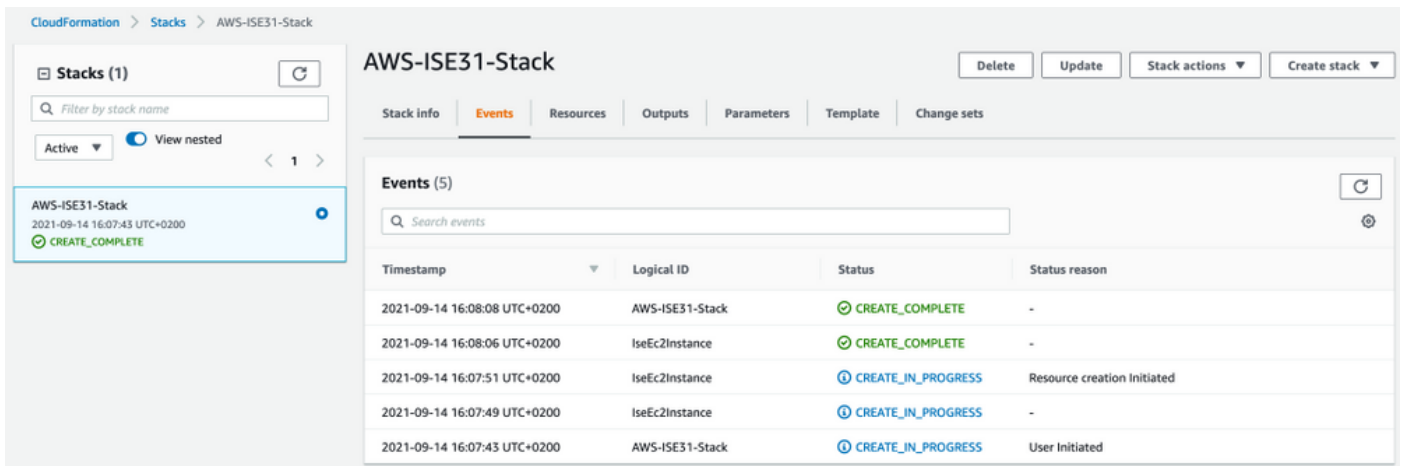
Timeout  
-

Termination protection  
Disabled

► Quick-create link

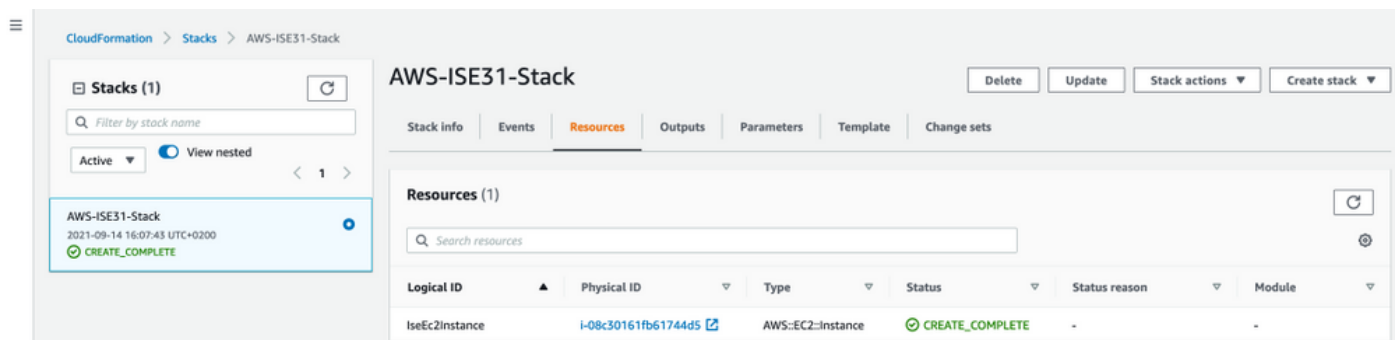
Cancel Previous Create change set **Create stack**

Une fois la pile déployée, l'état **CREATE\_COMPLETE** doit être affiché.

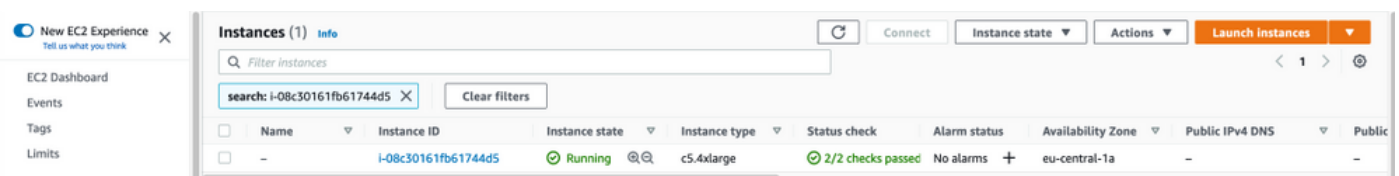


## Étape 5. Accéder à ISE sur AWS

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:G5NdGZ1rgPYnjlndPcXOLcJg9VICLSxnZA0kn0CfMPs.
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
```

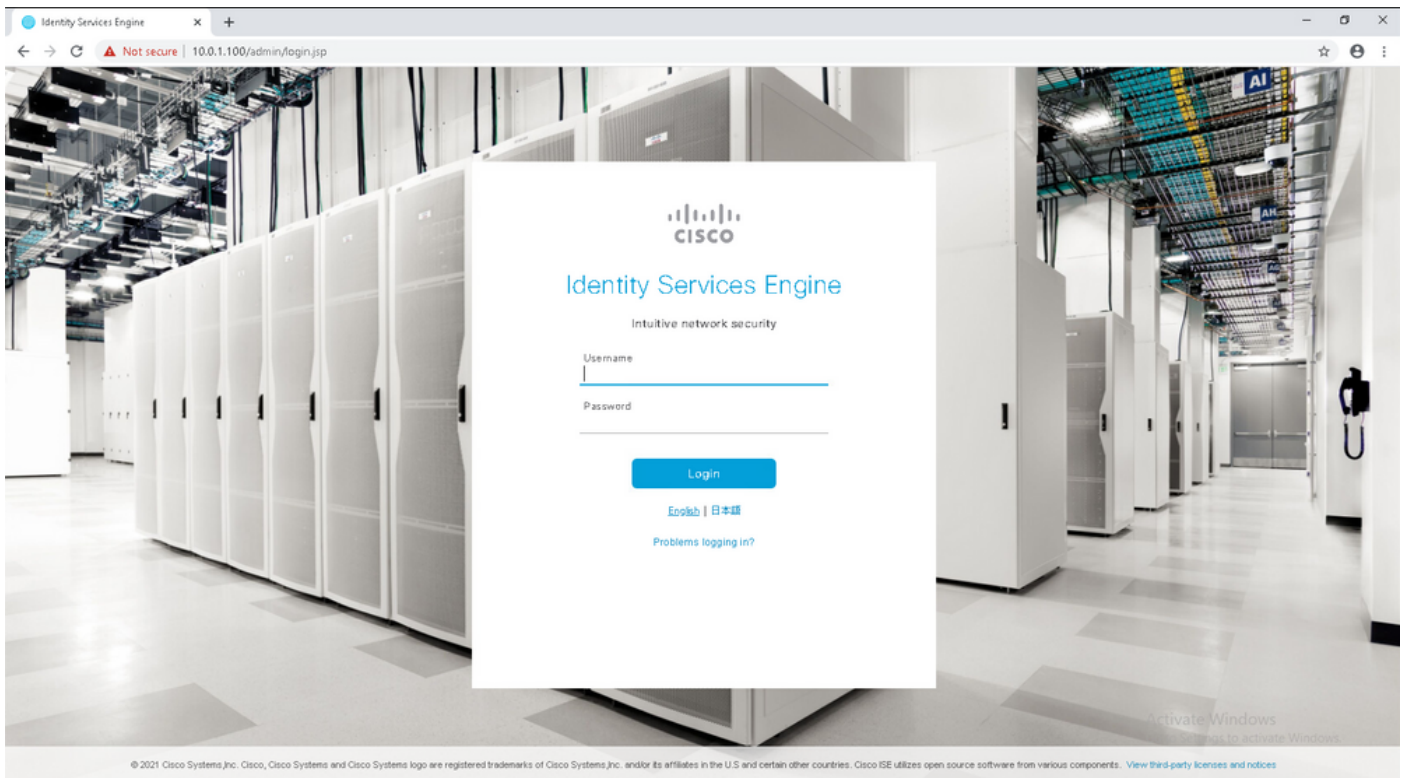
```
ISE PROCESS NAME STATE PROCESS ID
-----
Database Listener running 27703
Database Server running 127 PROCESSES
Application Server running 47142
Profiler Database running 38593
ISE Indexing Engine running 48309
AD Connector running 56223
M&T Session Database running 37058
M&T Log Processor running 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.

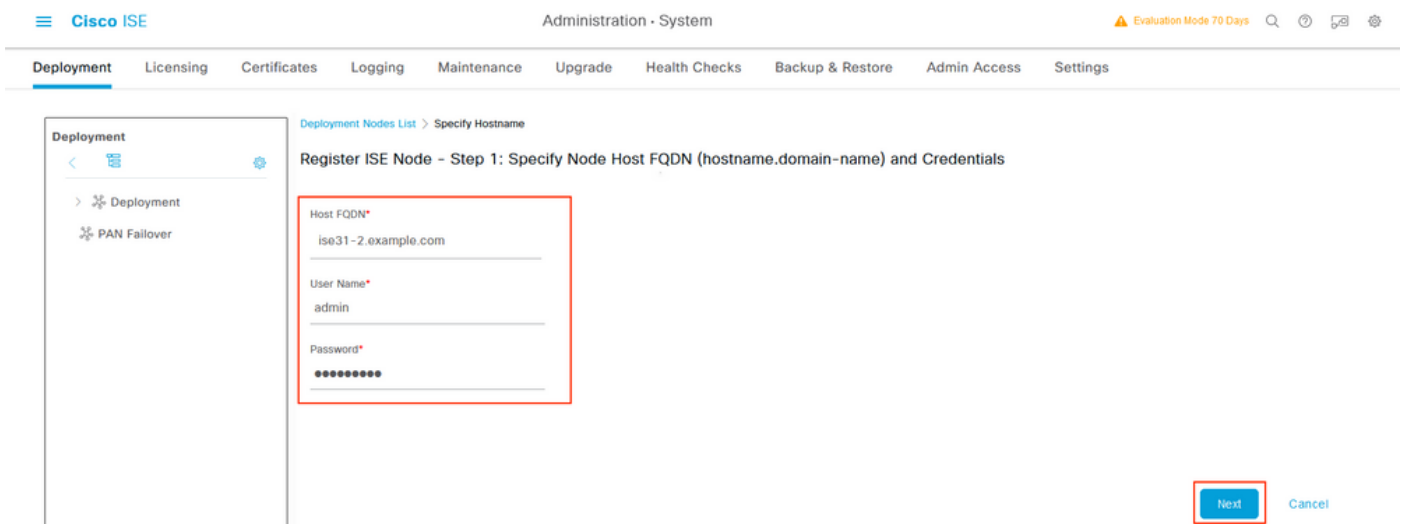
Une fois que le **serveur d'applications** est en **état d'exécution**, vous pouvez accéder à ISE via l'interface utilisateur graphique, comme illustré dans l'image.





## 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**.



## Warning

The node you are trying to register uses a self-signed certificate which is not trusted.

Are you sure you want to trust this certificate and proceed with registration?

If you are unsure, please click 'Cancel Registration'. Manually import relevant certificate chain of Node that is being registered into 'Trusted Certificates' and ensure 'Trust within ISE' checkbox is selected.

Please note that this certificate will by default be trusted only for authentication within ISE. If the same certificate needs to be used for other purposes (e.g. client authentication and syslog), please enable those options by editing the certificate under the 'Trusted Certificates' page.

Serial Number : 34 B8 85 F0 48 2D 51 74 DC F4 3B EE

Issued to : CN=ISE31-2.example.com

Issued by : CN=ISE31-2.example.com

Issued On : Tue Sep 14 16:25:36 CEST 2021

Expires On : Thu Sep 14 16:25:36 CEST 2023

Signature Algorithm : SHA384withRSA

SHA-256 Fingerprint : 58 BF 0E C4 BE D1 3E 0F 87 0A E6 0B D6 9F F1 6B 4C 0E  
40 85 0D BA 2F C2 72 95 A2 E3 BD 24 02 BD

SHA-1 Fingerprint : B3 36 68 48 1B 3B 35 2B 12 E6 3D BC 90 10 6D E6 A7 BC A4  
8D

MD5 Fingerprint : F5 7A ED 0B 04 CB BD 0C A3 32 D6 38 5C 34 B8 2E

[Cancel Registration](#)

[Import Certificate and Proceed](#)

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

Cisco ISE Administration - System Evaluation Mode 70 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Deployment Nodes List > Configure Node

### Register ISE Node - Step 2: Configure Node

**General Settings**

Hostname ISE31-2  
 FQDN ISE31-2.example.com  
 IP Address 10.0.1.100  
 Node Type Identity Services Engine (ISE)

Role SECONDARY

Administration  
 > Monitoring  
 > Policy Service  
 > pxGrid ⓘ

Cancel

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

Cisco ISE Administration - System Evaluation Mode 70 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

### Deployment Nodes

Selected 0 Total 2











Edit Register Syncup Deregister

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>

## Étape 7. Intégration du déploiement ISE avec AD sur site

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

## External Identity Sources

- <  
- >  Certificate Authentication F
-  Active Directory
-  LDAP
-  ODBC
-  RADIUS Token
-  RSA SecurID
-  SAML Id Providers
-  Social Login

## Active Directory











 Edit **+ Add**  Delete  Node View  Advanced Tools  Scope Mode

Join Point Name  Active Directory Domain

No data available

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

## External Identity Sources

- <  
- >  Certificate Authentication F
-  Active Directory
-  LDAP
-  ODBC
-  RADIUS Token
-  RSA SecurID
-  SAML Id Providers
-  Social Login

## Connection

\* Join Point Name EXAMPLE 

\* Active Directory Domain example.com 

**Submit**

Cancel

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



## Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

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.



### Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE31-2.example.com	✓ Completed.
ise31.example.com	✓ Completed.

Close

## 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.

Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 1 Repeat Counter 0

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Authc
Sep 15, 2021 12:22:33.4...	●	🔍	0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	■	🔍		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 14, 2021 08:25:37.3...	■	🔍		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit
Sep 14, 2021 08:22:12.0...	■	🔍		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit

## 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.

CloudFormation > Stacks > ISE31-AWS

Stacks (2)

ISE31-AWS

Stack info Events Resources Outputs Parameters Template Change sets

Events (4)

Timestamp	Logical ID	Status	Status reason
2021-09-17 12:57:19 UTC+0200	ISE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [ise31Instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	ise31Instance	CREATE_FAILED	Security group sg-0454161c94262f463 and subnet subnet-0f6becda62a58143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: 9b799775-fbe9-45c8-8664-6c40995a8444; Proxy: null)
2021-09-17 12:57:17 UTC+0200	ise31Instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:15 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User initiated

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
```