

Configurar o ISE 3.1 através do AWS Marketplace

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Topologia de rede](#)

[Configurações](#)

[Etapa A opcional. Criar VPC](#)

[Etapa B opcional. Configurar o dispositivo headend de VPN no local](#)

[Etapa C Opcional. Criar Par de Chave Personalizado](#)

[Etapa D opcional. Criar grupo de segurança personalizado](#)

[Etapa 1. Inscrever-se no produto AWS ISE Marketplace](#)

[Etapa 2. Configurar o ISE no AWS](#)

[Etapa 3. Iniciar o ISE no AWS](#)

[Etapa 4. Configurar a pilha de formação de nuvem para ISE no AWS](#)

[Etapa 5. Acesse o ISE no AWS](#)

[Etapa 6. Configurar implantação distribuída entre ISE no local e ISE no AWS](#)

[Passo 7. Integrar a implantação do ISE com o AD no local](#)

[Limitações](#)

[Verificar](#)

[Troubleshoot](#)

[Falha na criação da pilha CloudFormation](#)

[Problemas de conectividade](#)

[Appendix](#)

[Configuração relacionada a AAA/Radius do switch](#)

Introduction

Este documento descreve como instalar o Identity Services Engine (ISE) 3.1 via Amazon Machine Images (AMI) em Amazon Web Services (AWS). A partir da versão 3.1, o ISE pode ser implantado como uma instância da Amazon Elastic Compute Cloud (EC2) com a ajuda do CloudFormation Templates (CFT).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- ISE
- AWS e seus conceitos como VPC, EC2, formação em nuvem

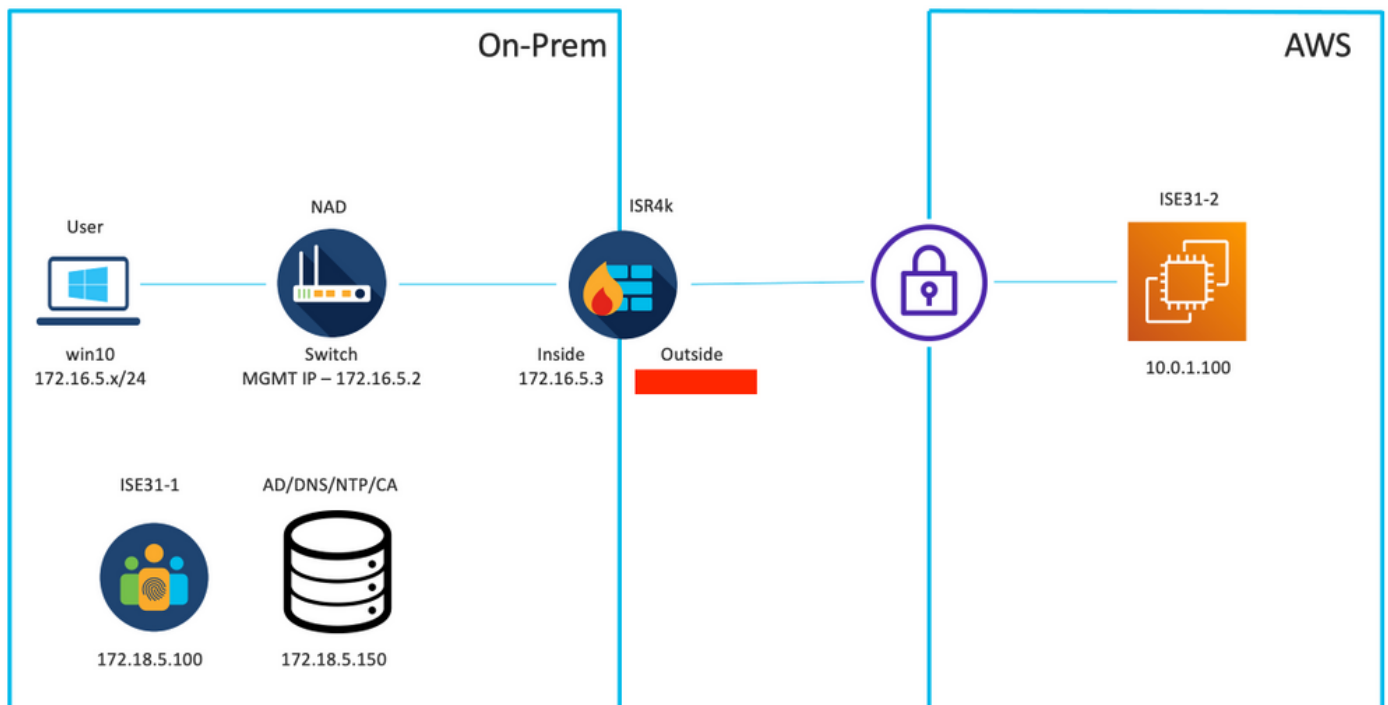
Componentes Utilizados

As informações neste documento são baseadas no Cisco ISE versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Topologia de rede

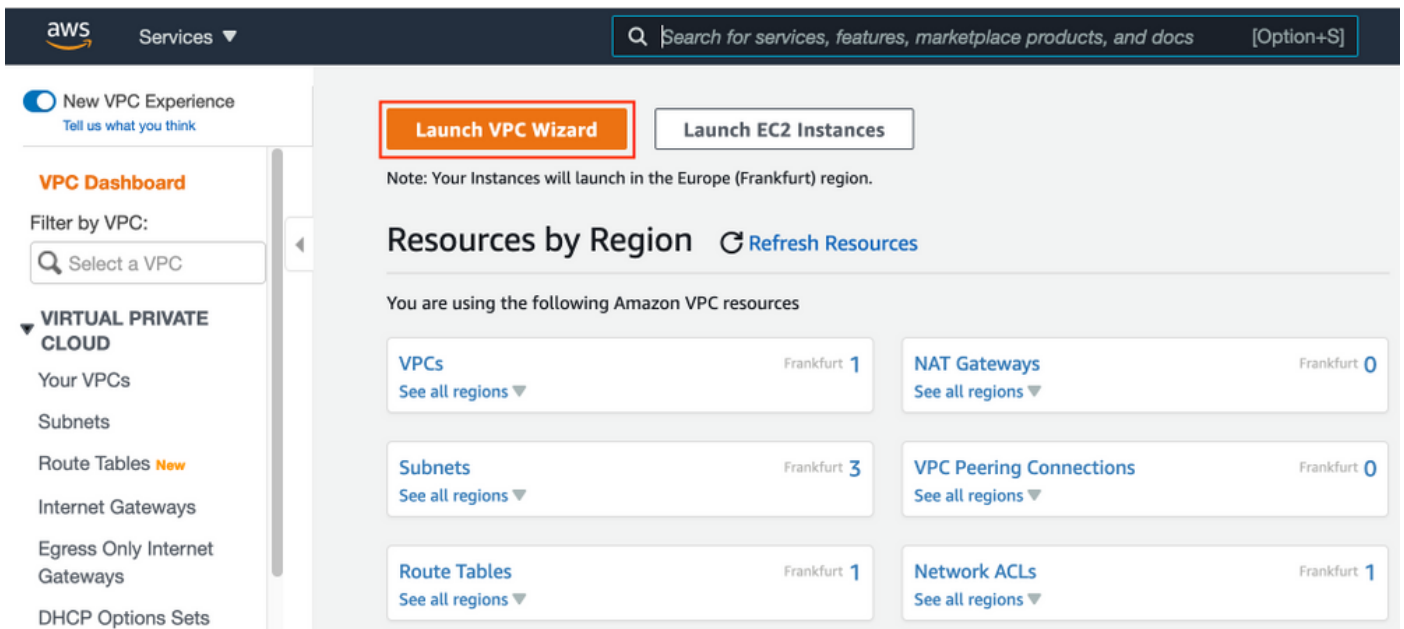


Configurações

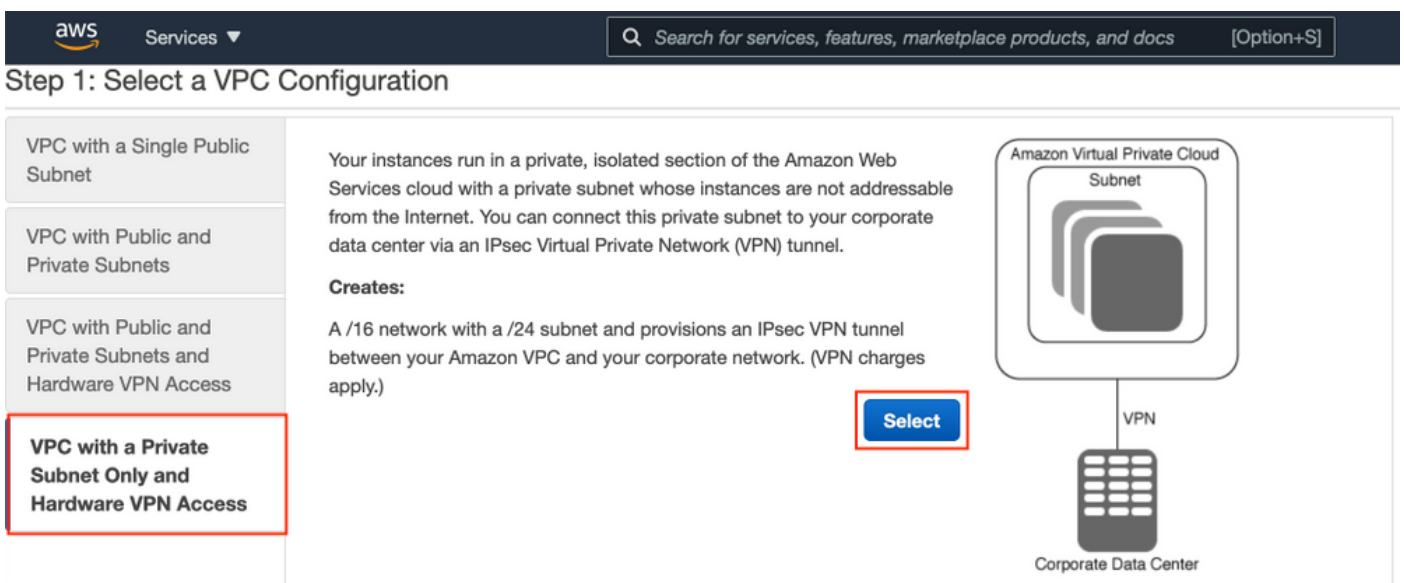
Se ainda não houver VPC, grupos de segurança, pares de chaves e túnel VPN configurados, você precisará seguir as etapas opcionais; caso contrário, comece com a Etapa 1.

Etapa A opcional. Criar VPC

Navegue até **VPC AWS Service**. Selecione **Iniciar Assistente de VPC** conforme mostrado na imagem.



Escolha VPC com Somente sub-rede privada e Acesso VPN de hardware e clique em Selecionar como mostrado na imagem.



Note: A seleção de VPC na Etapa 1. do assistente de VPC depende da topologia, pois o ISE não é projetado como servidor exposto à Internet - o VPN com sub-rede privada somente é usado.

Defina as configurações de sub-rede privada do VPC de acordo com o projeto da rede e selecione **Next**.

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
Add Endpoint

Enable DNS hostnames: Yes No

Hardware tenancy: Default

Cancel and Exit Back **Next**

Configure sua VPN de acordo com seu projeto de rede e selecione **Create VPC**.

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)

Cancel and Exit Back **Create VPC**

Depois que o VPC for criado, a mensagem "O VPC foi criado com êxito" será exibida. Clique em **OK** conforme mostrado na imagem.

VPC Successfully Created

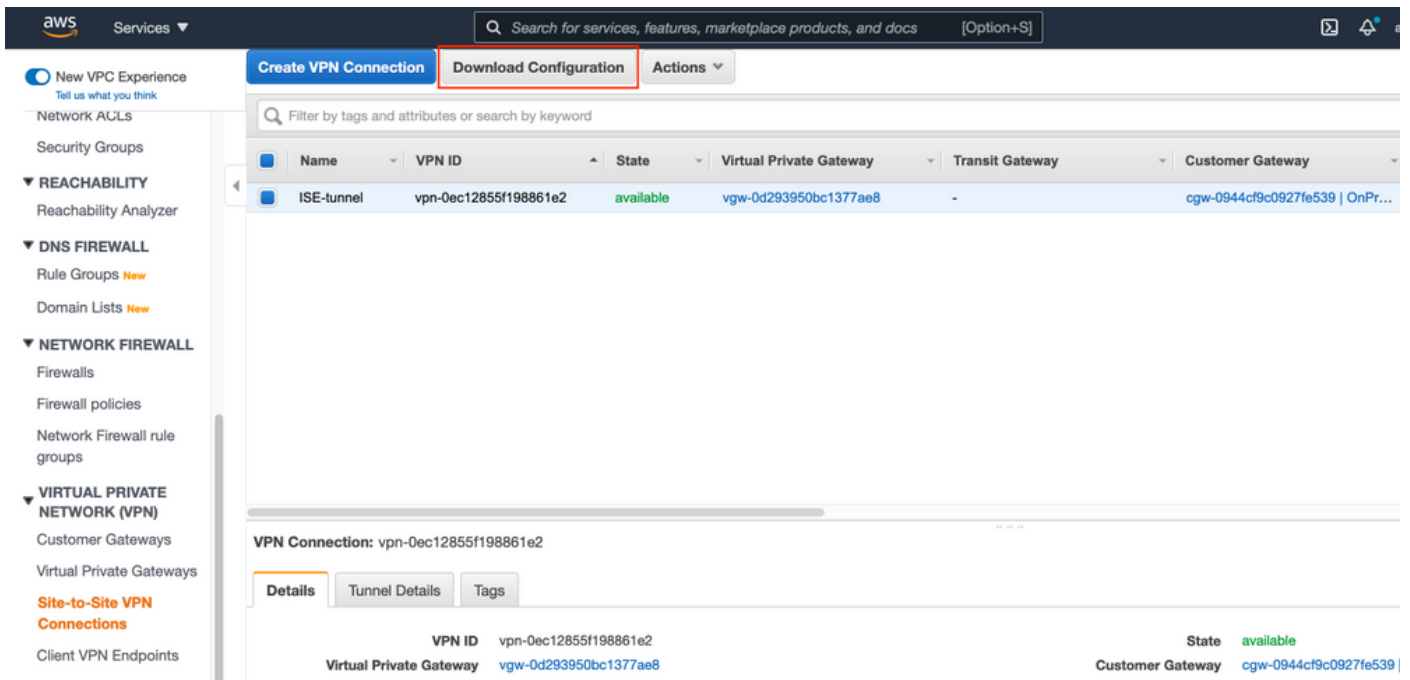
Your VPC has been successfully created.

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

OK

Etapa B opcional. Configurar o dispositivo headend de VPN no local

Navegue até **VPC AWS Service**. Escolha **conexões VPN site a site**, selecione o túnel VPN recém-criado e selecione **Download Configuration** conforme mostrado na imagem.



Escolha **Fornecedor**, **Plataforma** e **Software**, selecione **Download** como mostrado na imagem.



Aplice a configuração baixada no dispositivo headend VPN On-Prem.

Etapa C Opcional. Criar Par de Chave Personalizado

As instâncias AWS EC2 são acessadas com a ajuda de pares de chaves. Para criar um par de chaves, navegue até **EC2 Service**. Selecione o menu **Key Pairs** em **Network & Security (Rede e segurança)**. Selecione **Criar par de chaves**, atribua um **nome**, deixe outros valores como padrão e selecione **Criar par de chaves** novamente.

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.

Add tag

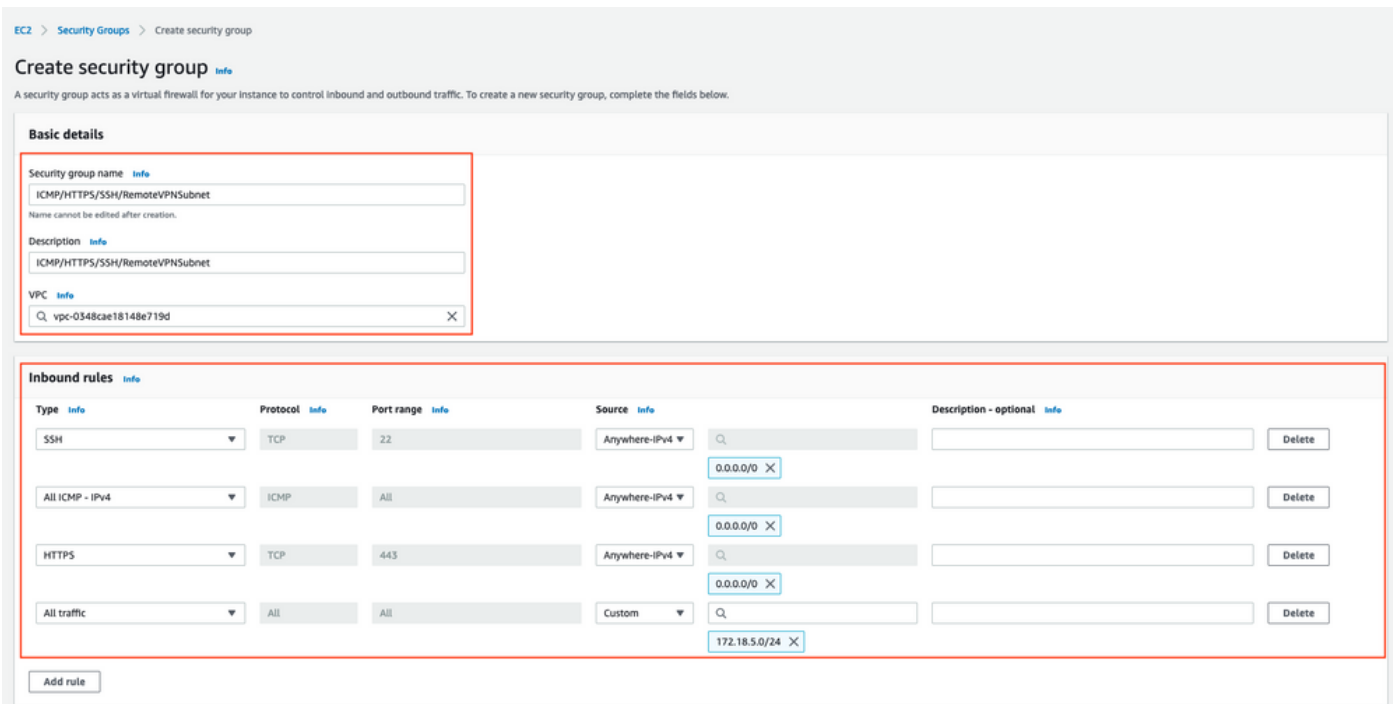
You can add 50 more tags.

Cancel

Create key pair

Etapa D opcional. Criar grupo de segurança personalizado

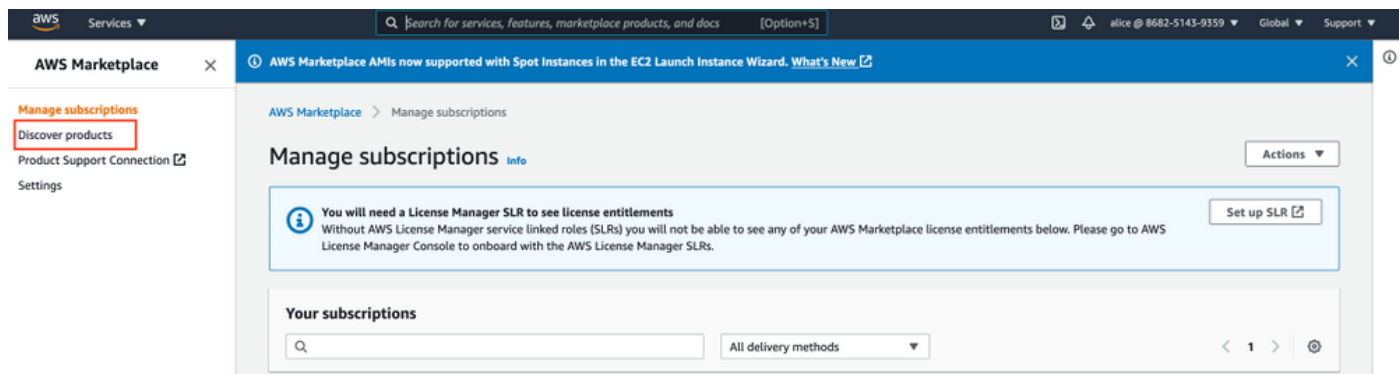
O acesso às instâncias AWS EC2 é protegido por **grupos de segurança**, para configurar o **grupo de segurança**, navegue para **EC2 Service**. Selecione o menu **Grupos de segurança** em **Rede e segurança**. Selecione Criar grupo de segurança, configure um **nome**, **Descrição**, no campo **VPC** selecione **VPC recém-configurado**. Configure **Inbound Rules** para permitir a comunicação com o ISE. Selecione **Criar grupo de segurança** conforme mostrado na imagem.



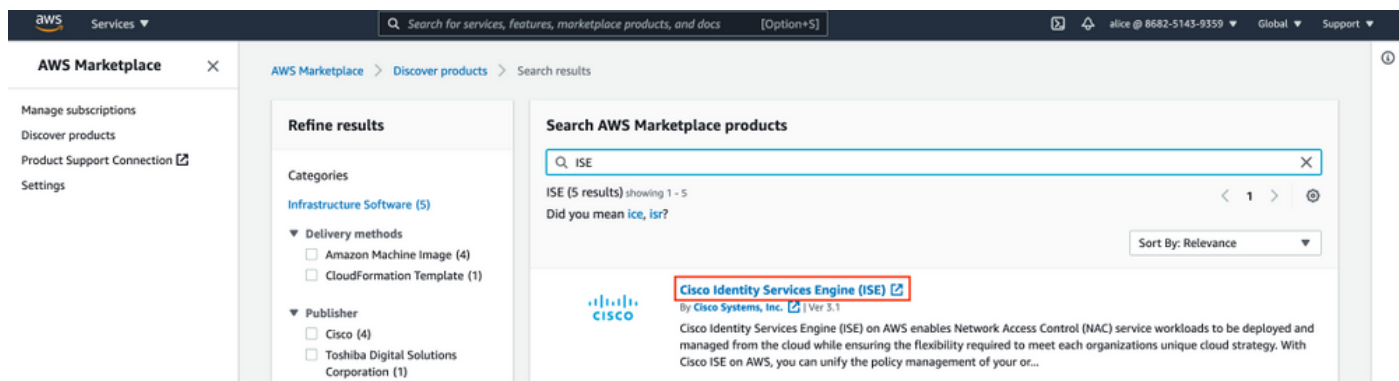
Note: O Grupo de Segurança configurado permite acesso SSH, ICMP, HTTPS ao ISE e a todos os protocolos acesso da sub-rede On-Prem.

Etapa 1. Inscrever-se no produto AWS ISE Marketplace

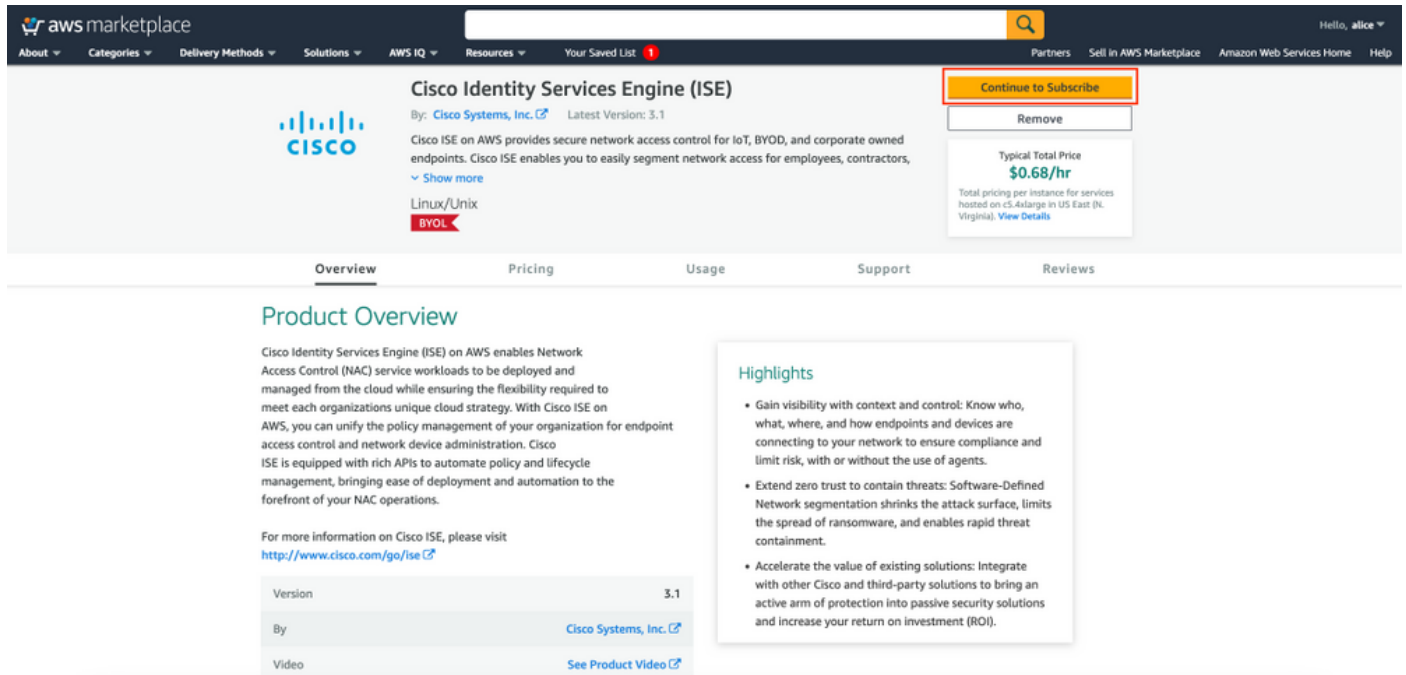
Navegue até **AWS Marketplace Subscriptions AWS Service**. Selecione **Descobrir produtos** conforme mostrado na imagem.



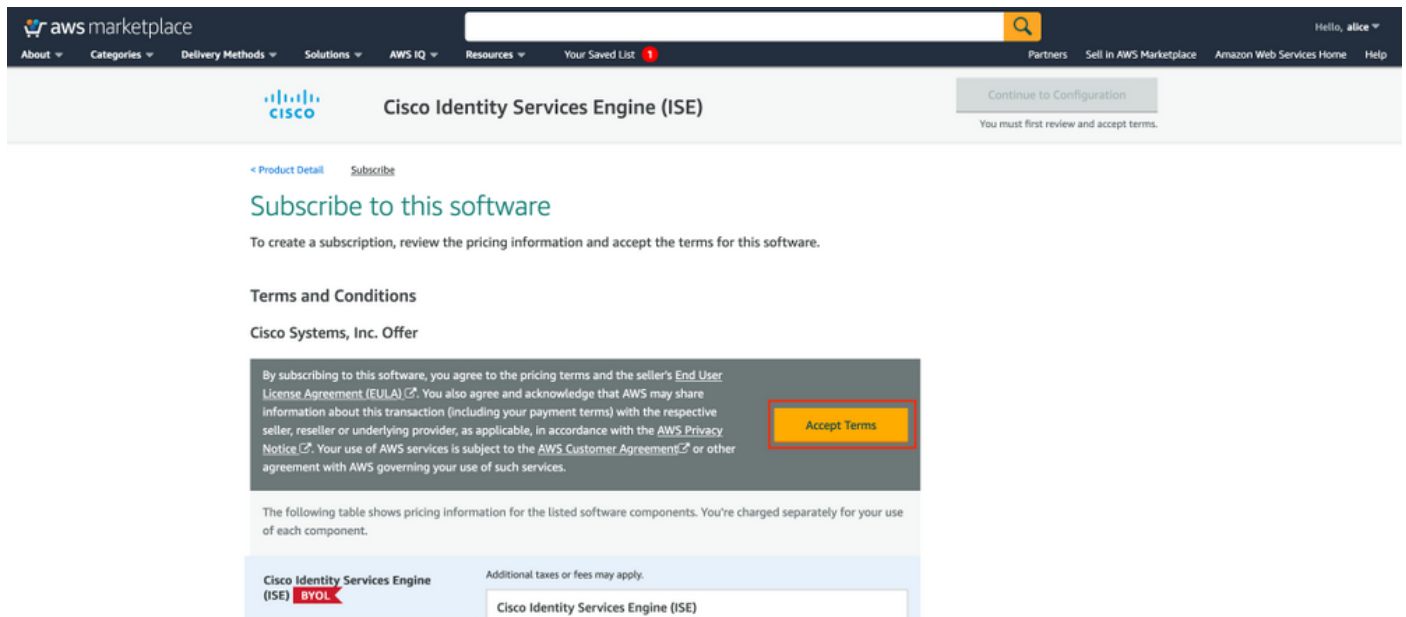
Procure o produto ISE e selecione **Cisco Identity Services Engine (ISE)** como mostrado na imagem.



Selecione o botão **Continuar para assinar**



Selecione o botão **Aceitar termos**, conforme mostrado na imagem.



Depois de inscrever o status de **Efetivo** e **Data de expiração** com alteração para **Pendente** como mostrado na imagem.

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)	○ Pending	○ Pending	▼ Show Details

Pouco depois que a **data de efetivação** for alterada para a data de assinatura e a **data de vencimento** for alterada para **N/A**. Selecione **Continuar para a configuração** conforme mostrado no ima



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	▼ Show Details

Etapa 2. Configurar o ISE no AWS

No menu Método de entrega da **tela Configurar este software**, selecione **Cisco Identity Services Engine (ISE)**. Na **Versão do software**, selecione **3.1 (12 de agosto de 2021)**. Selecione a **região**, onde o ISE está planejado para ser implantado. Selecione **Continuar para iniciar**.



[< 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
BYOL	
running on c5.4xlarge	

Etapa 3. Iniciar o ISE no AWS

No menu suspenso Actions (Ações) da tela **Launch this Software (Iniciar este software)**, selecione **Launch CloudFormation (Iniciar formação em nuvem)**.



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](#)

(Opcional) Selecione **Instruções de uso** para familiarizar-se com elas. Selecione **Iniciar**.

Etapa 4. Configurar a pilha de formação de nuvem para ISE no AWS

O botão **Iniciar** o redireciona para a tela de configuração **CloudFormation Stack**. Há um modelo pré-criado que deve ser usado para configurar o ISE. Mantenha as configurações padrão e selecione **Avançar**.

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-e495ba99

Amazon S3 template URL
S3 URL: https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba9925376.template [View in Designer](#)

Cancel [Next](#)

Preencha os dados da pilha CloudFormation com o **nome da pilha**. Configure os Detalhes da Instância como **Nome de Host**, selecione **Par de Chave da Instância** e **Grupo de Segurança de Gerenciamento**.

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)

Continue a configuração dos detalhes da instância com **Management Network**, **Management Private IP**, **Time Zone**, **Instance Type**, **EBS Encryption** e **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 ↕

Continue a configuração dos detalhes da instância com **DNS Domain**, **Name Server**, **NTP Service** e **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 ▼

Configure a senha do usuário GUI e selecione **Next**.

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**

Nenhuma alteração é necessária na próxima tela. Selecione **Avançar**.

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

Add tag

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 Sample-role-name Remove

Vá até a tela **Revisar pilha**, role para baixo e selecione **Criar pilha**.

Stack creation options

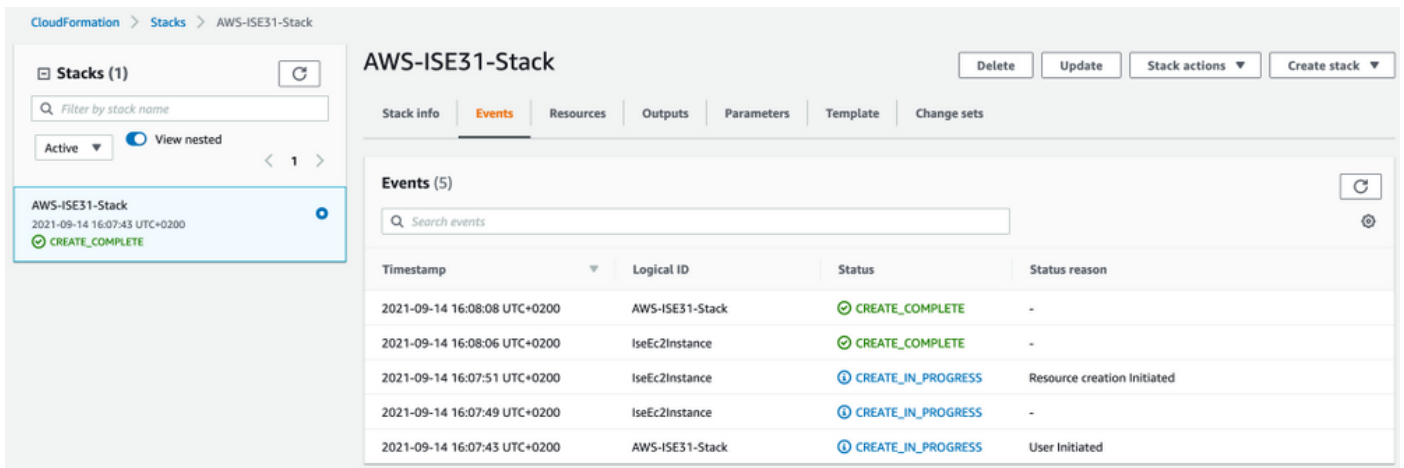
Timeout
-

Termination protection
Disabled

► Quick-create link

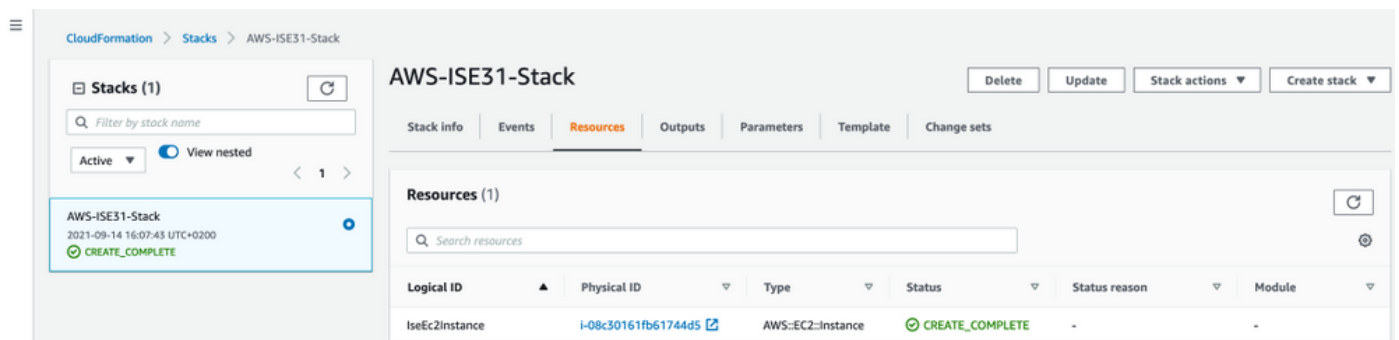
Cancel Previous Create change set **Create stack**

Quando a Pilha for implantada, o status **CREATE_COMPLETE** deverá ser visto.

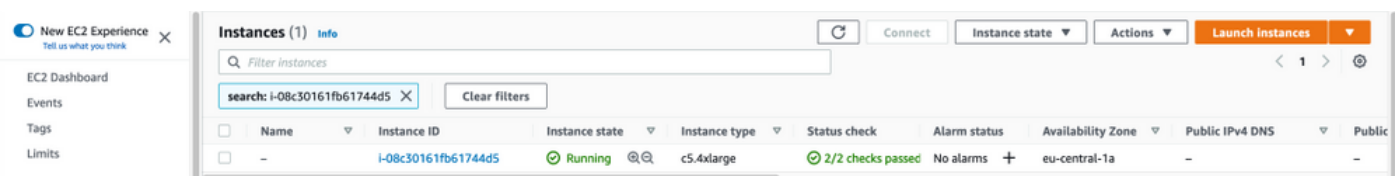


Etapa 5. Acesse o ISE no AWS

Para acessar a instância do ISE, navegue até a guia **Resources** para visualizar a instância EC2 criada a partir do CloudForms (Como alternativa, navegue para **Services > EC2 > Instances** para visualizar as instâncias do EC2) como mostrado na imagem.



Selecione **Physical ID** para abrir o menu **EC2 Instances**. Verifique se a **verificação de status** tem **2/2 verificações de status aprovadas**.



Selecione a **ID da instância**. O ISE pode ser acessado via **endereço IPv4 privado/DNS IPv4 privado** com protocolo SSH ou HTTPS.

Note: Se você acessa o ISE por meio do **endereço IPv4 privado/DNS IPv4 privado** certifique-se de que haja conectividade de rede para o endereço privado ISE.

Exemplo de ISE acessado via **Endereço IPv4 Privado** 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: Leva cerca de 20 minutos para que o ISE seja acessível via SSH. Até que a conectividade com o ISE falhe com "**Permissão negada (chave pública).**" mensagem de erro.

Use **show application status ise** para verificar se os serviços estão em execução:

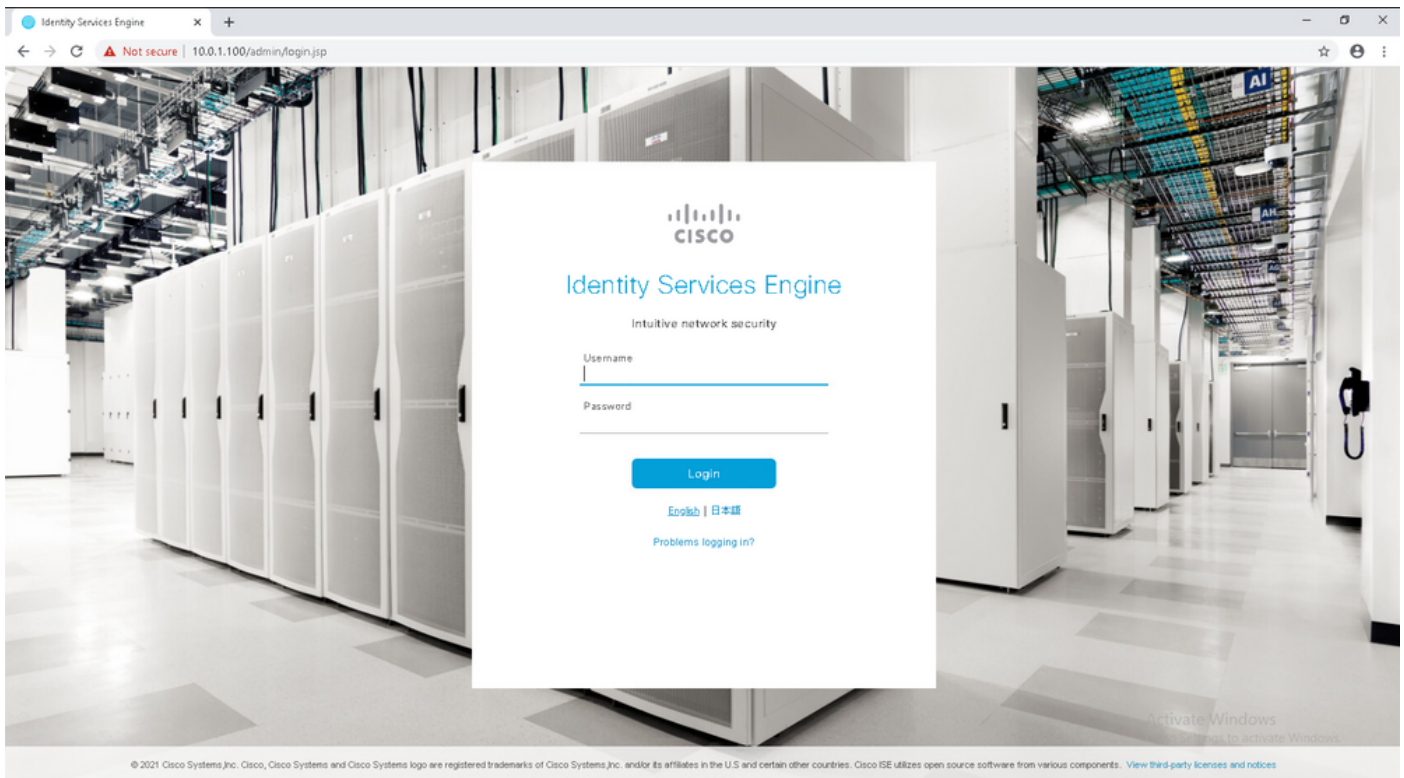
```
ISE31-2/admin# show application status ise
```

```
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#
```

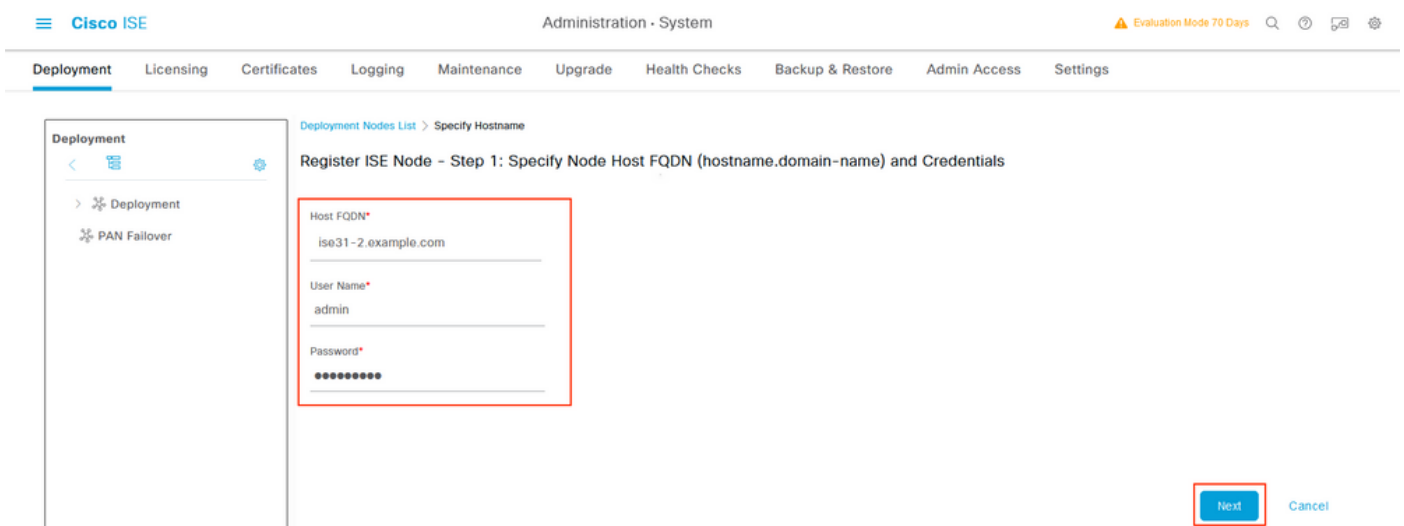
Note: Leva cerca de 10 a 15 minutos desde que o SSH está disponível para que os serviços ISE façam a transição para um estado em execução.

Quando o **Servidor de aplicativos** estiver em **estado em execução**, você poderá acessar o ISE via GUI, como mostrado na imagem.



Etapa 6. Configurar implantação distribuída entre ISE no local e ISE no AWS

Faça login no ISE On-Prem e navegue para **Administration > System > Deployment**. Selecione o nó e selecione **Make Primary**. Navegue até **Administration > System > Deployment**, Select **Register**. Configure o **FQDN** do **Host** do ISE em AWS, nome de usuário GUI e senha. Clique em **Next**.



Como os certificados autoassinados são usados nesta topologia, para importar certificados de administração para o **certificado de importação** Select de armazenamento confiável e **continuar**.



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](#)

Selecione as pessoas de sua escolha e clique em **Enviar**.

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 Submit

Quando a sincronização for concluída, o nó passará para o estado conectado, a caixa de seleção verde será exibida em relação a ele.

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"/>

Passo 7. Integrar a implantação do ISE com o AD no local

Navegue até **Administration > Identity Management > External Identity Sources**. Selecione **Active Directory**, selecione **Add**.

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

Configure **Joint Point Name** e **Ative Diretory Domain**, seleccione **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

Para integrar ambos os nós com o Ative Diretory, seleccione **Sim**.



Information

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

No

Yes

Digite **AD User Name** e **Password**, clique em **OK**. Quando os nós do ISE forem integrados com êxito ao Ative Diretory, o status do nó será alterado para Concluído.



Join Operation Status

Status Summary: Successful

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

Close

Limitações

Para ISE sobre limitações de AWS, consulte a seção [Limitações Conhecidas](#) do Guia de Administração do ISE.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar se a autenticação é executada na PSN do ISE localizada em AWS, navegue para **Operations > Radius > Live Logs** e confirme se a coluna **Server ISE on AWS PSN** é observada.

Cisco ISE 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

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Falha na criação da pilha CloudFormation

A criação da pilha de formação em nuvem pode falhar devido a vários motivos, um deles é quando você seleciona o grupo de segurança da VPN que é diferente da rede de gerenciamento do ISE. O erro se parece com o da imagem.

CloudFormation > Stacks > ISE31-AWS

Stacks (2)

ISE31-AWS 2021-09-17 12:57:11 UTC+0200 ROLLBACK_IN_PROGRESS

AWS-ISE31-Stack 2021-09-14 16:07:43 UTC+0200 CREATE_COMPLETE

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: [iusec2instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	iusec2instance	CREATE_FAILED	Security group sg-0d54161c94262f463 and subnet subnet-0fbbecda62a58143 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	iusec2instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:13 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User initiated

Solução:

Assegure-se de pegar o Grupo de segurança no mesmo VPC. Navegue até **Grupos de segurança** em VPC Service e observe a **ID do grupo de segurança**, verifique se ela corresponde ao VPC correto (onde o ISE reside), verifique a **ID do VPC**.

Problemas de conectividade

Pode haver vários problemas que podem fazer com que a conectividade ao ISE no AWS não funcione.

1. Problema de conectividade devido a **grupos de segurança** configurados incorretamente.

Solução: O ISE não pode ser alcançado na rede local ou mesmo em redes AWS se **os grupos de segurança** estiverem configurados incorretamente. Certifique-se de que os protocolos e portas necessários sejam permitidos no **Grupo de Segurança** associado à rede ISE. Consulte [Referência de Portas ISE](#) para Portas Obrigatórias a serem abertas.

2. Problemas de conectividade devido a roteamento mal configurado.

Solução: Devido à complexidade da topologia, é fácil perder algumas rotas entre a rede On-Prem e a AWS. Antes de usar os recursos do ISE, certifique-se de que a conectividade fim-a-fim esteja estabelecida.

Appendix

Configuração relacionada a AAA/Radius do switch

```
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
```