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.

aws Services ▼		Q Search for services, feature	es, marketplace products, and docs	[Option+S]
New VPC Experience Tell us what you think VPC Dashboard Filter by VPC: Select a VPC	Launch VPC Wizard Note: Your Instances will lau Resources by F	Launch EC2 Instances nch in the Europe (Frankfurt) region. Region C Refresh Resour	rces	
	You are using the followin	g Amazon VPC resources		
Your VPCs	VPCs See all regions T	Frankfurt 1	NAT Gateways See all regions T	Frankfurt 🚺
Subnets				
Route Tables New	Subnets	Frankfurt 3	VPC Peering Connections	Frankfurt 🔵
Internet Gateways	See all regions		See all regions	
Egress Only Internet Gateways	Route Tables	Frankfurt 1	Network ACLs	Frankfurt 1
DHCP Options Sets	See all regions V		See all regions V	

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**.

aws	Services 🔻		Q Search for services, features, m	arketplace products, and docs	[Option+S]	۵	¢	alice @ 8682-5143-9359 🔻	Frankfurt 🔻	Suppor	rt 🔻
Step 2: V	/PC with a Pri	vate Subnet Only and Ha	ardware VPN Access								
	IPv4 CIDR block:*	10.0.0/16 (65531 li	P addresses available)								
	IPv6 CIDR block:	No IPv6 CIDR Block									
		 Amazon provided IPv6 CIDR bloc IPv6 CIDR block owned by me 	ck								
	VPC name:	ISE-VPC									
Private su	ibnet's IPv4 CIDR:*	10.0.1.0/24 (251 IP a	addresses available)								
	Availability Zone:*	No Preference V									
Pri	ivate subnet name:	ISE-subnet									
		You can add more subnets after Am	azon Web Services creates the VPC.								
	Service endpoints										
		Add Endpoint									
Enable	DNS hostnames:*	es ○ No									
н	lardware tenancy:*	Default v									
								Cancel	and Exit	Back	Next

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

aws	Services 🔻	Q Search for services, features, marketplace product	s, and docs [Option+S	Σ 4	À alice @ 8682-5143-9359 ▼	Frankfurt 🔻	Support V
Step 3: 0	Configure your VPN						
Specify the	public IP Address of your VPN router (Customer Gateway)					
	Customer Gateway IP:*						
	Customer Gateway name:	OnPrem-GW					
	VPN Connection name:	SE-tunnel					
	N	ote: VPN Connection rates apply.					
Specify the	routing for the VPN Connection (Help me choose)						
	Routing Type:*	Dynamic (requires BGP)					
					Cancel and Ex	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.

aws Services -	Q. Search for services, features, marketplace products, and docs [Option+S]	∑	Frankfurt V Support V
New VPC Experience	VPC Successfully Created		
Tell us what you think	Your VPC has been successfully created.		
VPC Dashboard	You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.		_
Filter by VPC:			ок
Q Select a VPC			

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 recémcriado e selecione Download Configuration conforme mostrado na imagem.

aws Services ▼				C	Search for	r service	es, features,	marketplace products,	and docs	[Option+S]			D 4	. a
New VPC Experience		Create VP	N Connectio	n Downl	load Config	uration	Actions	. •						
Network AGLs		Q. Filter b	y tags and attr	ributes or sea	arch by keywo	ord								
Security Groups		Nam	e –	VPN ID		^ S	tate -	Virtual Private Gatew	ay -	Transit Gateway	~ C	ustomer Gateway	y	÷
 REACHABILITY Reachability Analyzer 	4	ISE-t	unnel	vpn-0ec1285	5f198861e2	av	vailable	vgw-0d293950bc1377	ae8		ci	yw-0944cf9c0927f	e539 OnP	r
▼ DNS FIREWALL Rule Groups New														
Domain Lists New														
▼ NETWORK FIREWALL														
Firewalls														
Firewall policies														
Network Firewall rule groups														
VIRTUAL PRIVATE NETWORK (VPN)														
Customer Gateways		VPN Conne	ection: vpn-0	ec12855f19	8861e2									
Virtual Private Gateway	5													
Site-to-Site VPN Connections		Details	Tunnel Det	tails lag	IS Octoor		04-0							
Client VPN Endpoints		,	Virtual Private	Gateway	vgw-0d2939	50bc137	77ae8				S Customer Gate	way cgw-0944	cf9c0927fe	539

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

Download Configuration	×
Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6. Vendor Cisco Systems, Inc. Image: Cisco Systems in the second sec	
Cancel	

Aplique 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

Name	
aws	
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.	
Key pair type Info	
• RSA	
C 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.	

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.

EC2 > Security Groups > Create s	security group						
Create security grou	up Info						
A security group acts as a virtual firewa	all for your ins	stance to control inbour	nd and outbound traffic. To create a new securit	y group, complete the fields	below.		
Basic details							
Security group name Info							
ICMP/HTTPS/SSH/RemoteVPNSu	bnet						
Name cannot be edited after creation.							
Description Info							
ICMP/HTTPS/SSH/RemoteVPNSu	bnet						
VPC Infe							
Q. vpc-0348cae18148e719d			×				
Inbound rules Info							
Type Info		Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH	•	TCP	22	Anywhere-IPv4 🔻	۹		Delete
					0.0.0.0/0 ×		
All ICMP - IPv4		ICMP	All	Anywhere-IPv4 🔻	Q		Delete
					0.0.0.0/0 ×		
HTTPS	٣	TCP	443	Anywhere-IPv4 v	Q		Delete
					0.0.0.0/0 ×		
All traffic		All	All	Custom 🔻	Q		Delete
					172.18.5.0/24 ×		
Add rule							

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.

aws Services 🔻		Q bearch for services, features, marketplace products, and docs	[Option+S]			Σ	¢	alice @ 8682-5143-9359 🔻	Global 🔻	Support	Ŧ
AWS Marketplace $\qquad imes$	③ AWS Marketplace A	MIs now supported with Spot Instances in the EC2 Launch Instance	Wizard. <u>What's</u>	New [2]						×	٩
Manage subscriptions Discover products Product Support Connection	AWS Marketplace	Manage subscriptions Ubscriptions Info							Actions	¥	
	You will n Without A License M	need a License Manager SLR to see license entitlements WS License Manager service linked roles (SLRs) you will not be able to anager Console to onboard with the AWS License Manager SLRs.	see any of your	AWS Marketplace lice	nse entitlements t	oelow. P	lease	go to AWS	up SLR 🖸		
	Your subscrip	ptions	l delivery methoc	is 🔻				<	1 >	0	

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

aws Services ▼	Q Search for services, features,	, marketplace products,	, and docs [Option+S]	D 🗘 əl	ice @ 8682-5143-9359 🔻	Global 🔻	Support	•
AWS Marketplace × AWS Marketplace Manage subscriptions Discover products Product Support Connection [2] Settings	Q. Search for services, features, Discover products > Search in Its	over products > Search results Q ISE USE USE				Global V	Support	•
Infrastructure Velivery r Amazz Cloudi Vublisher Cisco i	Software (5) IS bethods n Machine Image (4) ormation Template (1) t)	SE (5 results) showing 1 Did you mean ice, isr?	Cisco Identity Services Engine (ISE) [2] By Cisco Systems, Inc. [2] Ver 3.1 Cisco Identity Services Engine (ISE) on AWS enables Network Access C	ontrol (NAC) s	Sort By: Relevance service workloads to be de	> ployed at	© ▼	
Corpor	a Digital Solutions ation (1)		Cisco ISE on AWS, you can unify the policy management of your or					

Selecione o botão Continuar para assinar

😍 aw	/s marketpl	ace						Q		Hello, alice 🔻	
About 👻	Categories 👻	Delivery Methods 🔻	Solutions 👻	AWS IQ 👻	Resources v	Your Saved List 🏮		Partners	Sell in AWS Marketplace	Amazon Web Services Home Help	P
				Cisco	Identity S	ervices Engine (IS	SE)	Continue to Subscr	ibe		
			ahaha	By: Cisco	Systems, Inc. 🖉	Latest Version: 3.1		Remove			
			CISCO	Cisco ISE endpoint Show r Linux/U BYOL	on AWS provides is. Cisco ISE enable more	secure network access contro es you to easily segment netw	for IoT, BYOD, and corporate owned ork access for employees, contractors,	Typical Total Price \$0.68/hr Total pricing per instance for hosted on c5.4slarge in US Ea Virginia). View Details	services st (N.		
			Overview	,	Pricing	Usa	ge Support	Review	VS		
		Pr Ciso Acco man mee AWS acce ISE I man fore For : http Vu By VV	oldentity Service ess Control (NAC) anged from the cl et each organizati 5, you can unify the sis control and ne is equipped with agement, bringin front of your NAC more information errition	sengine (ISE) of service workloa oud while ensur un unique clour e policy manag twork device ad ich APIs to auto g ease of deplo ; operations. on Cisco ISE, pl m/go/Ise C	n AWS enables Ne ds to be deployed ing the fixebiblity r d strategy. With Ci ement of your org imnistration. Cisco imnistration. Cisco imnistratio	twork and required to sco ISE on anization for endpoint o fecycle ation to the 3.1 Claco Systems, Inc. C See Product Video C	 Highlights Gain visibility with context and co what, where, and how endpoints is connecting to your network to en- limit risk, with or without the use Extend zero trust to contain threa Network segmentation shrinks th the spread of ransomware, and er containment. Accelerate the value of existing so with other Cisco and third-party s active arm of protection into pass and increase your return on invest 	ntrol: Know who, and devices are sure compliance and of agents. tts: Software-Defined e attack surface, limits ables rapid threat ables rapid threat olutions: Dirdig and olutions to bring an ave security solutions iment (ROI).			

Selecione o botão Aceitar termos, conforme mostrado na imagem.

🚰 aws marketplace		Q	Hello, alice 🖛
About - Categories - Delivery Methods - Solutions - AWS IQ - Re	sources 👻 Your Saved List 🤨	Partners Sell in AWS Marketplace	Amazon Web Services Home Help
Cisco Cisco Iden	tity Services Engine (ISE)	Continue to Configuration You must first review and accept terms.	
< Product Detail Subscribe Subscribe to this so To create a subscription, review the pr	ftware ricing information and accept the terms for this software.		
Terms and Conditions			
Cisco Systems, Inc. Offer			
By subscribing to this software, you agree License Agreement (EULA) (2. You also a information about this transaction (inclu seller, reseller or underlying provider, as <u>Notice</u> (2. Your use of AWS services is sub agreement with AWS governing your use	e to the pricing terms and the seller's <u>End User</u> gree and acknowledge that AWS may share ding your payment terms) with the respective applicable, in accordance with the <u>AWS Privacy</u> oject to the <u>AWS Customer Agreement</u> or other of such services.		
The following table shows pricing inform of each component.	ation for the listed software components. You're charged separately for your use		
Cisco Identity Services Engine	Additional taxes or fees may apply.		
(ISE) BYOL	Cisco Identity Services Engine (ISE)		

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

< 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) C. 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 C. 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)	O Pending	O 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 <u>Subscribe</u>	
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) C. You agreed that AWS may share information about thi transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice C. Your use of AWS services remains subject to the AW Customer AgreementC or other agreement with AWS governing your use of such services.	is S

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.

Cisco Identity Services Engine	(ISE) ~
oftware Version	
3.1 (Aug 12, 2021)	~
Whats in This Version	
Cisco Identity Services Eng running on c5.4xlarge	gine (ISE)
Learn more	
Region	
ELL (Frankfurt)	~

This is an estimate of the	
and infrastructure costs configuration. Your actu each statement period n this estimate.	pical software based on your al charges for nay differ from
Software Pricing	
Cisco Identity Services Engine (ISE) BYOL c.5.4/lorge	\$0/hr

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) running on c5.4xlarge
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**.

aw	Services 🔻	Q [Search for services, features, marketplace products, and docs [Option+5] D 🗘 alice @ 6682-5143-9359 ¥ Frankfurt ¥ Support ¥
=	CloudFormation > Stac	s > Create stack
	Step 1 Specify template	Create stack
	Step 2 Specify stack details	Prerequisite - Prepare template
	Step 3 Configure stack options	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
	Step 4 Review	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 53 URL where it will be stored.
		Amazon S3 URL Upload a template tile
		https://s3.amazonaws.com/awsmp-fulfiliment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-bf3d-e495ba9;
		Amazon S3 template UBL
		S3 URL: https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b4Se37-5 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 > Cre	eate stack
Step 1 Specify template	Specify stack details
Step 2 Specify stack details	Stack name
	Stack name
Step 3 Configure stack options	AWS-ISE31-Stack
	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Step 4 Review	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-0fbebcdae62a58143 (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 evalua only. On terminating the instance, volume will be deleted as well.	ation purpose
300	<u>^</u>

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?

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 > Cr	reate stack
Step 1 Specify template	Configure stack options
Step 2 Specify stack details	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 🔀
Step 3 Configure stack options	Key Value Remove
Step 4 Review	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 ▼ 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.

CloudFormation > Stacks > AWS-ISE31-Stack					
E Stacks (1)	AWS-ISE31-Stack		Delet	e Update Stack actions 🔻	Create stack 🔻
Q Filter by stack name	Stack info Events Resources	Outputs Parameters	Template Change sets		
Active View nested	Events (5)				C
AWS-ISE31-Stack 2021-09-14 16:07:43 UTC+0200 () CREATE COMPLETE	Q Search events				0
	Timestamp v	Logical ID	Status	Status reason	
	2021-09-14 16:08:08 UTC+0200	AWS-ISE31-Stack	CREATE_COMPLETE		
	2021-09-14 16:08:06 UTC+0200	IseEc2Instance	O CREATE_COMPLETE		
	2021-09-14 16:07:51 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	Resource creation Initiated	
	2021-09-14 16:07:49 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS		
	2021-09-14 16:07:43 UTC+0200	AWS-ISE31-Stack	CREATE_IN_PROGRESS	User Initiated	

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.

${\small {\sf CloudFormation}} \hspace{0.2cm} \\ {\scriptstyle > } \hspace{0.2cm} {\small {\sf Stacks}} \hspace{0.2cm} \\ {\scriptstyle > } \hspace{0.2cm} {\small {\sf AWS-ISE31-Stack}} \end{array}$	
⊡ Stacks (1)	AWS-ISE31-Stack Delete Update Stack actions v Create stack v
Q. Filter by stock nome	Stack info Events Resources Outputs Parameters Template Change sets
Active View nested	
	Resources (1)
AWS-ISE31-Stack 2021-09-14 16:07:43 UTC+0200 CREATE_COMPLETE	Q. Search resources
	Logical ID 🔺 Physical ID 🗢 Type 🗢 Status 🗢 Status reason 🗢 Module 🗢
	IseEc2Instance i-08c30161fb61744d5 🖸 AWS::EC2::Instance 📀 CREATE_COMPLETE

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

New EC2 Experience X	Instances (1) Info		C Connect Instance st	ate 🔻 Actions 🔻	Launch instances	•
EC2 Dashboard Events	Q. Filter instances search: i-08c30161fb61744d5 X Clear filters				< 1 >	۲
Tags	Name V Instance ID	Instance state ∇ Instance type ∇	Status check Alarm status	Availability Zone 🛛	Public IPv4 DNS v	Public
Linits	- i-08c30161fb61744d5	⊘ Running @ ⊂ c5.4xtarge	⊘ 2/2 checks passed No alarms +	eu-central-1a	-	-

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
```

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 47142 running 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.

ldenbhy Services Engine x +	6	5	×
← → C A Not secure 10.0.1.100/admin/login.jsp	\Rightarrow	Θ	:
A letter 10.100/em/dgrup			
8 2011 Circo States for Circo States for States for states for an extended faderation of Circo States for activity is a state to be notice to be notice to be notice to a state to be notice to a state to be notice to a state to be notice to be notice to a state to be notice to be not to be notice to be not to b			

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.



Selecione as pessoas de sua escolha e clique em Enviar.

_	O		105
_	1.114	200	ISE.
	010	500	101

Administration · System

Peployment Licensing Certifi	cates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Deployment	Deployment Nodes List Configure Node Register ISE Node – Step 2: Configure Node General Settings
Se PAN Failover	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 ()

ncel 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 Q 🕜 🕫 🕸
Deployment Licensing Certifi	cates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings	1
Deployment	Deployment Nodes		Selected 0 Total 2 🔗 🚷
> 2% Deployment	🖉 Edit 🚯 Register 🕤 Syncup 🚯 Deregister		all \sim $~$ ∇
🦃 PAN Fallover	🗌 Hostname 🔿 Personas	Role(s) Services	Node Status
	ISE31-2 Administration, Monitoring, Policy Service	SEC(A), SEC(M) SESSION, PROFILER	
	Administration, Monitoring, Policy Service	PRI(A), PRI(M) SESSION, PROFILER	

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

Navegue até Administration > Identity Management > External Identity Sources. Selecione Ative Diretory, selecione Add.

E Cisco ISE	Administration · Identity Management
dentities Groups External lo	lentity Sources Settings
External Identity Sources	Active Directory
	🖉 Edit 🕂 Add 📋 Delete 🔍 Node View 🕺 Advanced Tools 🗸 Scope Mode
Active Directory	Join Point Name \wedge Active Directory Domain
🗖 LDAP	
C ODBC	No data available
RADIUS Token	
RSA SecurID	
SAML Id Providers	
Social Login	

Configure Joint Point Name e Ative Diretory Domain, selecione Submit.

Identities Groups External Identity Sources Settings External Identity Sources Connection 	≡	Cisco ISE		Administr	ration • Identity Manag	ement	A Evaluation Mode 70 Days	9	9 50
External Identity Sources <td< th=""><th>Identi</th><th>ities Groups External Ide</th><th>ntity Sources Ident</th><th>tity Source Sequer</th><th>ices Settings</th><th></th><th></th><th></th><th></th></td<>	Identi	ities Groups External Ide	ntity Sources Ident	tity Source Sequer	ices Settings				
Certificate Authentication Certificate Authentication Active Directory LDAP ODBC RADIUS Token RSA SecurD SAML Id Providers Social Login	Ext	ternal Identity Sources	Connection				^		
 Sour Pour traine Sour Pour traine Constructory Active Directory Constructory C		¢ 🔋 🔅	Inin Daint Mama	EXAMPLE		0			
LDAP ODBC RADIUS Token RSA SecurID SAML Id Providers Social Login		Certificate Authentication F Active Directory	Active Directory	example.com		0			
 ODBC RADIUS Token RSA SecuriD SAML Id Providers Social Login 		C LDAP	Domain						
 RADIUS Token RSA SecurID SAML Id Providers Social Login 		C ODBC							
RSA SecurID SAML Id Providers Social Legin		C RADIUS Token							
SAML ld Providers Social Login		C RSA SecurID							
Social Login		C SAML Id Providers							
<		🛅 Social Login							
<									
<									
<									
			(v		
							,		
Submit							Submit	Ca	ncel

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

(i) Information

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



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	on 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 <u>Limitações Conhecidas</u> 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			Ope	erations · RADIUS			A Evaluation Mode 70 Day	Q (2)	,a @
Live Logs Live Sessions									
Misconfigured Supplicants ①		Misconfigured N	etwork Devices 🕕	R	ADIUS Drops 🕕	Client Stop	pped Responding 🕕	Repeat C	ounter 🕕
0		(0		0		1	(C
						Re	efresh Show	Within	
Ø Refresh Seset Repeat Co	runts 🗅 Export To \vee					N	Never V Latest 20 records	✓ Last 3 h	ter 🗸 🐵
∯ Refresh Seset Repeat Co Time	uunts ⊥ Export To ∨ Status D	tails Repea	Identity	Endpoint ID	Endpoint Profile	Authentication Poli	Authorization Policy	Last 3 h	ter \checkmark (2) Author
Ø Refresh ≦ Reset Repeat Co Time ×	sunts ⊕ Export To ∨ Status D	tails Repea	Identity Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Never V Latest 20 records Authorization Policy Authorization Policy	Last 3 h	ter V (2) Autho Autho
C Refresh S Reset Repeat Co Time X Sep 15, 2021 12:22:33.4	Status D	tails Repea <u> v</u> 0	Identity Identity alice	Endpoint ID Endpoint ID 00:50:56:A1:45:84	Endpoint Profile Endpoint Profile VMWare-Device	Authentication Policy Default >> Dot1X	Never Latest 20 records Authorization Policy Authorization Policy Default >> Basic_Authenticated_Access	 Last 3 h Filt Server Server ISE31-2 	ter V (2) Author Permit
C Refresh Seset Repeat Co Time × Sep 15, 2021 12:22:33.4 Sep 15, 2021 12:22:32.8	Status D	tails Repea <u> v</u> 0	Identity Identity alice alice	Endpoint ID Endpoint ID 00:50:56:A1:45:84 00:50:56:A1:45:84	Endpoint Profile Endpoint Profile NMWare-Device VMWare-Device	Authentication Policy Authentication Policy Default >> Dot1X Default >> Dot1X	Never Latest 20 records Authorization Policy Authorization Policy Default >> Basic_Authenticated_Access Default >> Basic_Authenticated_Access	Server Server ISE31-2 ISE31-2	ter V (2) Author Author Permit Permit
Refresh Seset Repeat Co Time X Sep 15, 2021 12:22:33.4 Sep 15, 2021 12:22:32.8 Sep 14, 2021 08:25:37.3 Sep 14, 2021 08:25:37.3	Status D C C C C C C C C C C C C	talls Repea <u> v</u> 0	Identity Identity alice alice alice	Endpoint ID Endpoint ID 00:50:56:A1:45:84 00:50:56:A1:45:84	Endpoint Profile Endpoint Profile Endpoint Profile VMWare-Device VMWare-Device VMWare-Device	Authentication Poli Authentication Policy Default >> Dot1X Default >> Dot1X Default >> Dot1X	Never Latest 20 records Authorization Policy Authorization Policy Default >> Basic_Authenticated_Access Default >> Basic_Authenticated_Access Default >> Basic_Authenticated_Access	 Last 3 h Filt Server Server ISE31-2 ISE31-2 ISE31-2 Ise31 	ter V @ Autho Autho Permit 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			Delete Update Stack actions V Create stack V
Q, Filter by stock nome	Stack info Events Resources Outputs Parameters	Template Change sets		
Active w View nested	Events (4)			
ISE31-AWS 2021-09-17 12:57:11 UTC+0200 © ROLLBACK_IN_PROGRESS	Q. Search events			•
AW5-5531-5tack	Timestamp v	Logical ID	Status	Status reason
	2021-09-17 12:57:19 UTC+0200	ISE31-AWS		The following resource(i) failed to create: [teEc2instance]. Rollback requested by user.
	2021-09-17 12:57:18 UTC+0200	IseEc2instance	© CREATE_FAILED	Security group sp-055-161842624643 and rubnet subnet-0fbebcdee5235143 belong to different networks. Service: AnazonGC2; Status Gole: 4000; Emar Gole: InvalidParameter; Request ID: b07x8773- ffer3-455-8642-864095536444, Proor; null)
	2021-09-17 12:57:17 UTC+0200	iseEc2instance	@ CREATE_IN_PROGRESS	
	2021-09-17 12:57:11 UTC+0200	ISE31-AWS	OREATE_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 <u>Referência</u> <u>de Portas ISE</u> 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
1
1
aaa group server radius ISE-Group
server name ISE31-2
server name ISE31-1
1
aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group
1
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
1
vlan 1805
1
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
1
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
```