通过AWS Marketplace配置ISE 3.1

目录

简介 先决条件 要求 使用的组件 配置 网络拓扑 配置 可选步骤A.创建VPC 可选步骤B.配置内部VPN头端设备 可选步骤C.创建自定义密钥对 可选步骤D.创建自定义安全组 步骤1.订用AWS ISE市场产品 步骤2.在AWS上配置ISE 步骤3.在AWS上启动ISE 步骤4.在AWS上为ISE配置CloudFormation堆栈 步骤5.访问AWS上的ISE 步骤6.在AWS上配置内部ISE和ISE之间的分布式部署 步骤7.将ISE部署与内部AD集成 限制 验证 故障排除 CloudFormation堆栈创建失败 连接问题 Appendix 交换机AAA/RADIUS相关配置

简介

本文档介绍如何通过Amazon Machine Images(AMI)在Amazon Web Services(AWS)中安装Identity Services Engine(ISE)3.1。 在3.1版中,ISE可以在CloudFormation Templates(CFT)的帮助下部署 为Amazon弹性计算云(EC2)实例。

先决条件

要求

Cisco 建议您具有以下主题的基础知识:

ISE

• AWS及其概念,如VPC、EC2、CloudFormation

使用的组件

本文档中的信息基于Cisco ISE版本3.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

网络拓扑



配置

如果尚未配置VPC、安全组、密钥对和VPN隧道,则需要执行可选步骤,否则,从步骤1开始。

可选步骤A.创建VPC

导航至VPC AWS服务。选择启动VPC向导,如图所示。

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:	Launch VPC Wizard Note: Your Instances will laur Resources by R	Launch EC2 Instances ch in the Europe (Frankfurt) region. Region C Refresh Resour	ces	
VIRTUAL PRIVATE CLOUD Your VPCs	You are using the following VPCs See all regions ▼	Amazon VPC resources	NAT Gateways See all regions	Frankfurt ()
Subnets Route Tables New Internet Gateways	Subnets See all regions ▼	Frankfurt 3	VPC Peering Connections See all regions	Frankfurt 0
Egress Only Internet Gateways DHCP Options Sets	Route Tables See all regions ▼	Frankfurt 1	Network ACLs See all regions	Frankfurt 1

选择VPC with Private Subnet Only and Hardware VPN Access,然后单击Select,如图所示。

aws Services ▼		Q Search for services, features, marketp	lace products, and docs	[Option+S]
Step 1: Select a VPC 0	Configuration			
VPC with a Single Public Subnet	Your instances run in a private, is Services cloud with a private sub from the Internet. You can conne	polated section of the Amazon Web onet whose instances are not addressable ct this private subnet to your corporate	Amazon Virtual Private Clou Subnet	d
Private Subnets	data center via an IPsec Virtual F Creates:	rivate Network (VPN) tunnel.		
VPC with Public and Private Subnets and Hardware VPN Access	A /16 network with a /24 subnet between your Amazon VPC and apply.)	and provisions an IPsec VPN tunnel your corporate network. (VPN charges		
VPC with a Private Subnet Only and Hardware VPN Access		Select	VPN	
			Corporate Data Center	

注意:VPC向导步骤1.中VPC的选择取决于拓扑,因为ISE不设计为Internet外露服务器 — 仅 使用带私有子网的VPN。

根据您的网络设计配置VPC专用子网设置并选择**下一步**。

aws	Services v		Q Search for services, features, m	arketplace products, and docs	[Option+S]	ک ا	🗘 alice @ 8682-5143-9359	▼ Frankfurt ▼	Support 🔻
Step 2: V	/PC with a Pri	vate Subnet Only and H	ardware VPN Access						
	IPv4 CIDR block:*	10.0.0/16 (65531	IP addresses available)						
	IPv6 CIDR block:	No IPv6 CIDR Block Amazon provided IPv6 CIDR block IPv6 CIDR block owned by me	sck						
	VPC name:	ISE-VPC							
Private su	ibnet's IPv4 CIDR:*	10.0.1.0/24 (251 IP	addresses available)						
	Availability Zone:*	No Preference V							
Pri	ivate subnet name:	ISE-subnet							
		You can add more subnets after An	nazon Web Services creates the VPC.						
	Service endpoints	Add Endpoint							
Enable	DNS hostnames:*	Yes ○ No							
н	fardware tenancy:*	Default ~							
							Can	el and Exit	Back Next

根据网络设计配置VPN,然后选择"创建VPC"。

aws	Services V	Q Search for services, features, marketplace products, and d	locs [Option+S]	D	⇔ alice @ 8682-5143-9359 ▼	Frankfurt 🔻	Support ¥
Step 3: C	Configure your VPN						
Specify the p	public IP Address of your VPN router (Customer Gateway)					
	Customer Gateway IP:*						
	Customer Gateway name:	OnPrem-GW					
	VPN Connection name:	SE-tunnel					
	M	ote: VPN Connection rates apply.					
Specify the	routing for the VPN Connection (Help me choose)						
	Routing Type:*	Dynamic (requires BGP)					
					Cancel and Exi	Back	Create VPC

创建VPC后,将显示"Your VPC has been successfully created"(您的VPC已成功创建)消息。单击 OK(确定),如图所示。

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

可选步骤B.配置内部VPN头端设备

导航至VPC AWS服务。选择Site-to-Site VPN connections,选择新创建的VPN隧道,然后选择 Download Configuration,如图所示。

aws Services T	Q Search for services, features, marketplace products, and docs [Option+S]	۲ <u>۲</u>
New VPC Experience	Create VPN Connection Download Configuration Actions *	
Network ACLs	Q Filter by tags and attributes or search by keyword	
Security Groups	Name VPN ID A State Virtual Private Gateway Transit Gateway	✓ Customer Gateway ✓
 REACHABILITY Reachability Analyzer 	ISE-tunnel vpn-0ec12855f198861e2 available vgw-0d293950bc1377ae8 -	cgw-0944cf9c0927fe539 OnPr
▼ DNS FIREWALL Rule Groups New		
Domain Lists New		
 NETWORK FIREWALL Firewalls 		
Firewall policies		
Network Firewall rule groups		
VIRTUAL PRIVATE NETWORK (VPN)		
Customer Gateways	VPN Connection: vpn-0ec12855f198861e2	
Virtual Private Gateways	Details Transl Details Trans	
Site-to-Site VPN Connections	Details Tunner Details Tags	
Client VPN Endpoints	VPN ID vpn-0ec12855f198861e2 Virtual Private Gateway vgw-0d293950bc1377ae8	State available Customer Gateway cgw-0944cf9c0927fe539

选择供应商、平台和软件,选择下载,如图所示。

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.	
Platform ISR Series Routers V	
Software IOS 12.4+ V	
Cancel	d

在内部VPN头端设备上应用下载的配置。

可选步骤C.创建自定义密钥对

AWS EC2实例通过密钥对进行访问。要创建密钥对,请导航到EC2服务。在"网络和安全"下选择"密 钥对"菜单。选择创建密钥对,为其指定名称,保留其他值为默认值,然后再次选择创建密钥对。

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		-	
SA 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.			

可选步骤D.创建自定义安全组

AWS EC2实例访问受安全组**保护**,要配置安全组,**请导航**至EC2**服务**。在"网**络和安全**"下选**择"安全** 组"菜单。在VPC字段中,选择创建安全组,配置名称,说明,选择新配置的VPC。配置入站规则以 允许与ISE通信。选择创建安全组,如图所示。

C2 > Security Groups > Create security group						
reate security group Info						
security group acts as a virtual firewall for your ins	tance to control inboun	d and outbound traffic. To create a new security gr	oup, complete the fields	below.		
Basic details						
for the second second second						
ICMP/HTTPS/SSH/Pamotal/DNSuboat						
Name cannot be edited after creation.						
Description to fe						
ICMP/UTTPS/SSU/Demotel/DNSubpet						
A STATE OF A STATE AND A STATE A STATE A						
VPC Info						
Q, vpc-0348cae18148e719d		×				
Inbound rules info						
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH 💌	TCP	22	Anywhere-IPv4 V	Q		Delete
				0.0.0.0/0 ×		
All ICMP - IPv4 🔻	ICMP	All	Anywhere-IPv4 🔻	Q		Delete
				0.0.0.0/0 ×		
HTTPS •	TCP	443	Anywhere-IPv4 ▼	Q		Delete
				0.0.0.0/0 ×		
All traffic 🛛 🔻	All	All	Custom 🔻	Q,		Delete
				172.18.5.0/24 ×		

注意:配置的安全组允许SSH、ICMP、HTTPS访问ISE,以及从内部子网访问所有协议。

步骤1.订用AWS ISE市场产品

导航至AWS Marketplace Subscriptions AWS Service。选择Discover Products,如图所示。

aws Services ▼	Q bearch for services, features, marketplace products, and docs [Option+S]	🗸 Global 🔻	Support 🔻
AWS Marketplace $\qquad imes$	③ AWS Marketplace AMIs now supported with Spot Instances in the EC2 Launch Instance Wizard. What's New [2]		× ©
Manage subscriptions Discover products Product Support Connection	AWS Marketplace > Manage subscriptions Manage subscriptions Info	Actions	•
Jerong J	You will need a License Manager SLR to see license entitlements Without AWS License Manager service linked roles (SLRs) you will not be able to see any of your AWS Marketplace license entitlements below. Please go to AWS License Manager Console to onboard with the AWS License Manager SLRs.	et up SLR 🖸]
	Your subscriptions Q All delivery methods	1 > @	>

搜索ISE产品并选择思科身份服务引擎(ISE),如图所示。

aws Services V	Q Search for services, fe	tures, marketplace products, and docs [Option+S]	⇔ alice @ 8682-5143-9359 ▼ 0	Slobal 🔻	Support 🔻	
AWS Marketplace \times	AWS Marketplace > Discover products > 5	earch results				٩
Manage subscriptions Discover products Product Support Connection 🗗 Settings	Refine results Categories Infrastructure Software (5) ▼ Delivery methods	Search AWS Marketplace products Q. ISE ISE (5 results) showing 1 - 5 Did you mean ice, isr?	< 1 Sort By: Relevance	× > ©)	
	Publisher Cisco (4) Toshiba Digital Solutions Corporation (1)	CISCO Identity Services Engine (ISE) CISCO Cisco Systems, Inc. [2] Iver 3.1 Cisco Identity Services Engine (ISE) on AWS enables Network Access Contra managed from the cloud while ensuring the flexibility required to meet ex Cisco ISE on AWS, you can unify the policy management of your or	rol (NAC) service workloads to be dep ach organizations unique cloud strate	loyed and gy. With		

选择"**继续订阅"**按钮

👷 aw	s marketpl	ace						Q		Hello, a	elice 🕶
About 👻	Categories 👻	Delivery Methods 👻	Solutions 👻	AWS IQ 👻	Resources - Your	Saved List 🚺		Partners	Sell in AWS Marketplac	e Amazon Web Services Home	Help
			ılı.ılı. cısco	Cisco ISE endpoint Show I Linux/U BYOL	Didentity Servi o Systems, Inc. C Late on AWS provides secure ts. Cisco ISE enables you more Unix	ces Engine (I st Version: 3.1 network access contro to easily segment netw	SE) of for IoT, BYOD, and corporate owned work access for employees, contractors,	Continue to Subs Remove Typical Total Pri \$0.68/hr Total pricing per Instance Nated on c5.4slarge in US Virginia, View Details	ribe R r services East ().		
			Overview	,	Pricing	Usa	age Support	Revi	2WS		
		Pro Clisto Acce man meet AWS acce ISE II man foref For r http: We By Vii	oldentity Service so Control (NAC) aged from the cl e ach organizati so control and ne e quipped with agement, bringi front of your NAC more information c//www.clsco.co rsion	verview s Engine (ISE) or service workloa oud while ensur ons unique clouw the policy manage twork device ad trich APIs to auto g ease of deplog c operations.	n AWS enables Network ds to be deployed and ing the flexibility require d strategy. With Cisco IS ement of your organizati iministration. Cisco mate policy and lifecycle yment and automation to lease visit Cisco See	d to on for endpoint the 3.1 o Systems, Inc. C Product Video C	Highlights • Gain visibility with context and what, where, and how endpoir connecting to your network to limit risk, with or without the 4 • Extend zero trust to contain th Network segmentation shrinks the spread of ransomware, and containment. • Accelerate the value of existing with other Cisco and third-par active arm of protection into p and increase your return on im	I control: Know who, ts and devices are ensure compliance and se of agents. reats: Software-Defined the attack surface, limits I enables rapid threat solutions: Integrate ty solutions to bring an assive security solutions restment (ROI).			

选择**接受**术语按钮,如图所示。

🐓 aws marketplace						Q		Hello, a	alice 🕶
About - Categories - Delivery Me	thods 🛩 Solutions 🛩	AWS IQ 👻 I	Resources 👻	Your Saved List 🚺		Partners	Sell in AWS Marketplace	Amazon Web Services Home	Help
	altalta cisco	Cisco Ider	ntity Ser	vices Engine (ISE)		Continue to Confi	guration		
			-	2		You must first review a	and accept terms.		
	< Product Detail Subse	tribe							
	Subscribe t	to this so	oftware	õ					
	To create a subscript	ion, review the p	pricing inform	nation and accept the terms for this	software.				
	Terms and Cond	itions							
	terns and cond								
	Cisco Systems, Inc.	. Offer							
	By subscribing to this License Agreement (E information about th seller, reseller or unde <u>Notice</u> 2 ⁸ . Your use of agreement with AWS	software, you age <u>[ULA]</u> [2]. You also is transaction (incl erlying provider, a: I AWS services is si governing your us	ree to the prici agree and ackr luding your pay is applicable, in subject to the <u>A</u> se of such servi	ng terms and the seller's <u>End User</u> nowledge that AWS may share yment terms) with the respective accordance with the <u>AWS Privacy</u> <u>WS Customer Agreement</u> ² or other ces.	Accept Terms				
	The following table s of each component.	hows pricing infor	rmation for the	listed software components. You're charg	ed separately for your use				
	Cisco Identity Servic	tes Engine	Additional ta	xes or fees may apply.					
	(ISE) BYOL		Cisco Ide	intity Services Engine (ISE)					
			_						

订用有效和到期**日期**后,**更改**为**待定**,如图所示。

< 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)	O Pending	O Pending	✓ Show Details

生效日期**更改**为订用日期后不久,到**期日**期更**改为N/A。**选择**Continue to Configuration(继续**配置),如映像所示



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

步骤2.在AWS上配置ISE

在配置此软件屏幕的**交付方法菜**单中**选择思科身份服务引擎(ISE)。**在"软**件版**本"中选择 3.1(2021年8月12日)。选择Region,其中ISE计划部署。选择继续启动。



< 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.

Deliver	y Method	
Cisco	Identity Services Engine (ISE)	~
Softwa	re Version	
3.1 (Aug 12, 2021)	~
	Whats in This Version	
	Cisco Identity Services Engine (ISE) running on c5.4xlarge	
	Learn more	
Region		
	Frankfurt)	~

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 \$0/hr Services Engine (ISE) BYOL

running on c5.4xlarge

步骤3.在AWS上启动ISE

从"启动此软件"屏幕的"操作"下**拉菜单中**,选择"启动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) 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

(可选)选择"**使用说明**"以便您熟悉这些说明。选择"**启动**"。

步骤4.在AWS上为ISE配置CloudFormation堆栈

"启动"按钮将您重定向**到CloudFormation堆**栈设置屏幕。有一个预建模板必须用于设置ISE。保留默 认设置并选择"下**一步"**。

aw	/S	Services V	Q Search for services, features, marketplace products, and docs	[Option+S]	24	alice @ 86	82-5143-9359 🔻	Frankfurt 🔻	Support 🔻
=	c	loudFormation > Stacks > Create stack							
	St SI	pecify template	eate stack						
	St St	tep 2 Po	rerequisite - Prepare template						
	St	Pr By Pr Ev onfigure stack options	epare template ery stack is based on a template. A template is a JSON or YAML file that contains configs Template is ready Use a sample template	uration information about the AWS resources you want to include in late Create template in Design	n the stac	k.			
	St	tep 4 eview Si	pecify template template is a JSON or YAMI. file that describes your stack's resources and properties.						
		Te	mplate source secting a template generates an Amazon 53 URL where it will be stored.						
			Amazon S3 URL	 Upload a template file 					
		Ar	mazon S3 URL						
			https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef66	2-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-	bf3d-e4	95ba9;			
		An	nazon S3 template URL						
		53 79	URL: https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/b 3d-4492-bf3d-e495ba925376.template	edef662-aba4-427e-b523-7c93cd50111c.f7b45e37-5	View in Design	n Ier			
				Cancel		Next			

使用堆栈名称填充CloudFormation**堆栈数据**。配置实例详细信息(**如主机名**),选择实**例密钥对**和管 **理安全组。**

stack name Stack name Stack name AWS-ISE31-Stack Stack name can include letters (A-Z and a-2), numbers (0-9), and dashes (-). tep 4 eview Parameters Parameters Parameters Parameters Parameters 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 Details Masegment Security Group To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the usemame "admin". Create a PEM key pair in AWS now if you have not come in eadedy. Usage example: sh - i mykeypair.pair admin@myhostname.compute-1.amazonaws.com aws Masegment Security Group Choose the Security Group Choose the Security Group in the Information on a larget or the starter to the Cisco ISE instance to a starte to the Information on a larget or the starter to the Cisco ISE instance to a starter to the Information on a larget for the us	tep 1 pecify template	Specify stack details
Stack name AWS-ISE31-Stack Stack name can include letters (A-Z and a-2), numbers (0-9), and dashes (-). Parameters 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 "admint". Create a PEM key pair in AWS now if you have not con one already. Usage example: ssh - impkeypair.pem admin@myhostname.compute-1.amazonaws.com ws Choose the Security Group Choose the Security Group Choose the Security Group in AWS new if you have not configured one already:	ep 2 pecify stack details	Stack name
p3 AWS-ISE31-Stack Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-). ep 4 tview Parameters 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 con one already. Usage example: sh-i mykeypair.pem admin@myhostname.compute-1.amazonaws.com aws Management Security Group Choose the bestruits for up to stack to the file to the file to ISE interface. Create a Security for up to an atravity.		Stack name
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-). Parameters 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 "admint". Create a PEM key pair in AWS now if you have not conone already. Usage example: ssh - i mykeypair.pem admin@myhostname.compute-1.amazonaws.com aws	ep 3 Infigure stack options	AWS-ISE31-Stack
Parameters	angure start options	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
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 content and the second structure of the second st		Parameters Parameters are defined in your template and allow you to input custom values when you create or update a stack. Instance Details
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 conore already. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-T.amazonaws.com aws Management Security Group Choose the Security Group Choose the Security Group		Hostname Hostname. This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.
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 con one already. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com aws Management Security Group Choose the 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.		ISE31-2
aws Management Security Group Choose the Security Group		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
Management Security Group Choose the Security Group to attach to the Circo ISE interface. Create a Security Group in AWS new if you have not configured one already		aws
choose the security droup to attach to the cisco isc interface. Create a security droup in Arts now in you nave not comingured one already.		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.

使用Management Network、Management Private IP、Time Zone、Instance Type**、EBS** Encryption和Volume Size继续配置Instance Details。

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	
Fime Zone Choose a system time zone.	
Etc/UTC	•
Instance Type Choose the required Cisco ISE instance type.	
c5.4xlarge	•
E BS 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.

 $\hat{}$

▼

▼

▼

▼

300

继续使用DNS域、名称服务器、NTP服务和服务配置实例详细信息。

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

配置GUI用户密码并选择"下一步"。

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 Warning: The password is displayed in plaintext in the User Data section of the Instance settings window in the AWS Console.	SE GUI access	5.
Confirm Password Retype Password		
•••••		
Cancel	evious	Next

下一屏幕无需更改。选择 Next(下一步)。

CloudFormation > Stacks > 0 Step 1	Configure stack ontions
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 V Sample-role-name V Remove

转到"查看**堆栈"**屏幕,向下滚动并选择"创**建堆栈"**。

Stack creation options	
Timeout -	
Termination protection Disabled	
Quick-create link	
	Cancel Previous Create change set Create stack

部署堆栈后,必须看到CREATE_COMPLETE状态。

CloudFormation > Stacks > AWS-ISE31-Stack					
🗉 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 heated	Events (5)				C
AWS-ISE31-Stack 2021-09-14 16:07:43 UTC+0200 CREATE_COMPLETE	Q. Search events				۲
	Timestamp 🔻	Logical ID	Status	Status reason	
	2021-09-14 16:08:08 UTC+0200	AWS-ISE31-Stack	O CREATE_COMPLETE		
	2021-09-14 16:08:06 UTC+0200	IseEc2Instance	⊘ 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	

步骤5.访问AWS上的ISE

要访问ISE实例,请导航至**Resources** 选项卡以查看从CloudForms创建的EC2实例(或者导航至 Services > EC2 > Instances 以查看EC2实例),如图所示。

CloudFormation > Stacks > AWS-ISE31-Stack	
⊡ Stacks (1) C	AWS-ISE31-Stack Delete Update Stack actions V Create stack V
Q Filter by stack name	Stack info Events Resources Outputs Parameters Template Change sets
Active View nested	
	Resources (1)
AWS-ISE31-Stack 2021-09-14 16:07:45 UTC+0200 © CREATE_COMPLETE	Q. Search resources
	Logical ID 🔺 Physical ID 🗢 Type 🗢 Status 🗢 Status reason 🗢 Module 🗢
	IseEc2Instance i-08c30161fb61744d5 🖸 AWS::EC2::Instance 📀 CREATE_COMPLETE

选择物理ID以打开"EC2实例"菜单。确保状态检查已通过2/2的检查。

New EC2 Experience ×	Instances (1) Info		C Connect Instance st	ate 🔻 Actions 🔻 Launch i	instances 🔻
EC2 Dashboard	Q Filter instances	7			< 1 > ©
Events Tags	Name V Instance ID	Instance state V Instance type V	Status check Alarm status	Availability Zone 🗵 Public IPv4 D	NS 🔻 Public
Limits	- i-08c30161fb61744d5	⊘ Running ඬ©, c5.4xlarge	⊙ 2/2 checks passed No alarms +	eu-central-1a –	-

选择实例ID。ISE可以通过SSH或HTTPS协议通过私有IPv4地址/私有IPv4 DNS。

注意:如果通过专用IPv4**地址/专用IPv4 DNS访问ISE**,请确**保有到ISE专用地址**的网络连接 。

通过SSH通过私有IPv4地址访问的ISE示例:

```
[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#
```

注意:通过SSH访问ISE大约需要20分钟。在此之前,与ISE的连接失败,并**显示"Permission** denied(publickey)"。 错误消息。

使用show application status ise 以验证服务是否正在运行:

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#

注意:由于ISE服务可使用SSH转换到运行状态,因此需要大约10-15分钟。

一旦应**用服**务器处于运行状态,您就可以通过GUI访问ISE,如图所示。

Menthy Services Engine x +	-	ø	×
← → C ▲ Not secure 10.0.1.100/admin/login.jsp	\$	θ	:
A stever 101.100/univerging	*	đ	-
Activate Windows these to activate			

步骤6.在AWS上配置内部ISE和ISE之间的分布式部署

登录到On-Prem ISE并导航至Administration > System > Deployment。选择节点并选择"**Make Primary"。**导航回管**理>系统>部署,**选择注册。在AWS**上配**置ISE的主机FQDN、GUI**用户名**和密**码** 。单击 Next。

E Cisco ISE	4	Administration - System			A Evaluation Mode 70 Days	QC	50	Ô
Deployment Licensing Ce	artificates Logging Maintenance	Upgrade Health Checks	Backup & Restore	Admin Access Setting:	S			
Deployment Image: Second system Image: Se	Deployment Nodes List > Specify Hostname Register ISE Node - Step 1: Specify Host FQDN* ise31-2.example.com User Name* admin Password* eeeeeeee	ify Node Host FQDN (hostnar	ne.domain-name) and C	Credentials		7		

由于此拓扑中使用自签名证书,因此要交叉导入管理证书到受信任存储选择导入证书并继续。



Cancel Registration

Import Certificate and Proceed

选择您选择的角色,然后单击"提**交"**。

Administration · System

Deployment Licensing Certific	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
्रिः 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 Administration Monitoring
	Policy Service
	> pxGrid ()

Cancel Submit

同步完成后,节点会转换到连接状态,此时会显示绿色复选框。

E Cisco ISE	Administration · System	, Evaluation Mode 70 Days Q 🕜 🗔 🕸	
Deployment Licensing Cert	ificates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings	
Deployment	Deployment Nodes		Selected 0 Total 2 👩 🍈
> 3% Deployment	🖉 Edit 🚯 Register 🐑 Syncup 🚯 Deregister		all \sim $ \nabla$
age PAN Fallover	Hostname	Role(s) Services	Node Status
	ISE31-2 Administration, Monitoring, Policy Service	SEC(A), SEC(M) SESSION, PROFILER	
	ise31 Administration, Monitoring, Policy Service	PRI(A), PRI(M) SESSION, PROFILER	

步骤7.将ISE部署与内部AD集成

导航至管理>身份管理>外部身份源。选择Active Directory,选择添加。

■ Cisco ISE	Administration · Identity Management				
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings				
External Identity Sources	Active Directory				
	🖉 Edit 🕂 Add 📋 Delete 📿 Node View 😤 Advanced Tools 🗸 Scope Mode				
> Certificate Authentication F					
Active Directory	Join Point Name Active Directory Domain				
LDAP					
DDBC	ivo data available				
RADIUS Token					
🗎 RSA SecurID					
SAML Id Providers					
🗎 Social Login					

配置联合点名称和Active Directory域,选择提交。

■ Cisco ISE	Administratio	n · Identity Management	🛕 Evaluation Mode 70 Days Q 🕜 🔂
Identities Groups External Iden	tity Sources Identity Source Sequences	Settings	
External Identity Sources	Connection		î
Certificate Authentication F	Join Point Name EXAMPLE	O	
C Active Directory	Active Directory example.com	0	
C LDAP			
CODBC			
C RSA SecuriD			
SAML Id Providers			
Social Login			
	<		>
			Submit Cancel

要将两个节点与Active Directory集成,请选择**是**。

(i) Information

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

No Yes

输入AD User Name(AD用户名)和Password(密码),单击OK(确定)。ISE节点成功与Active Directory集成后,节点状态将更改为Completed。

			\times
Join Operation	St		
Status Summary: Successful			
ISE Node	^	Node Status	
ISE31-2.example.com		Completed.	
ise31.example.com		Completed.	

C	ose	

限制

有关AWS上的ISE限制,请参阅《ISE管<u>理指南</u>》的"已知限制"部分。

验证

要验证在AWS上的ISE PSN上执行身份验证,请导航至**操作> Radius >实时日志**,并在AWS PSN上**的服**务器列ISE中进行确认。

≡ Cisco ISE	Op	erations · RADIUS	A Evaluation Mode 70 Da	ns Q Ø 59 @
Live Logs Live Sessions				
Misconfigured Supplicants 🕕	Misconfigured Network Devices 🕕	RADIUS Drops	Client Stopped Responding 🕠	Repeat Counter 🕕
0	0	0	1	0
🖉 Refresh 🛛 🕒 Reset Repeat Counts 📣 Expo	int To \sim		Refresh Show Never V Latest 20 records	Within Last 3 hours ↓ VFilter ↓ ③
Time Status	Details Repea Identity	Endpoint ID Endpoint Profile	Authentication Poli Authorization Policy	Occurrent Australia
×	∽ Identity	Endpoint ID Endpoint Profile	Authentication Policy Authorization Policy	Server Autoc
				Server Autho
Sep 15, 2021 12:22:33.4	. 0 alice	00:50:56:A1:45:84 VMWare-Device	Default >> Dot1X Default >> Basic_Authenticated_Access	Server Author Server Author ISE31-2 Permit
Sep 15, 2021 12:22:33.4 O	0 alice	00:50:56:A1:45:84 VMWare-Device 00:50:56:A1:45:84 VMWare-Device	Default >> Dot1X Default >> Basic_Authenticated_Access Default >> Dot1X Default >> Basic_Authenticated_Access	Server Author ISE31-2 Permit ISE31-2 Permit
Sep 15, 2021 12:22:33.4 •	0 alice 0 alice 0 alice	00:50:56:A1:45:84 VMWare-Device 00:50:56:A1:45:84 VMWare-Device 00:50:56:A1:45:84 VMWare-Device	Patientication Pointy Patientication Pointy Default >> Dot1X Default >> Basic_Authenticated_Access Default >> Dot1X Default >> Basic_Authenticated_Access Default >> Dot1X Default >> Basic_Authenticated_Access Default >> Dot1X Default >> Basic_Authenticated_Access	Server Author ISE31-2 Permit ISE31-2 Permit Ise31 Permit

故障排除

本部分提供了可用于对配置进行故障排除的信息。

CloudFormation堆栈创建失败

CloudFormation堆栈创建可能因多种原因而失败,其中一种原因是从VPN选择安全组(与ISE的管 理网络不同)。错误类似于映像中的错误。

CloudFormation > Stacks > ISE31-AWS								
🗆 Stacks (2)	ISE31-AWS			Delete Update Stack actions ¥ Create stack ¥				
Q. Filter by stock nome	Stack info Events Resources Outputs Parameters	Template Change sets						
Active ¥ View nested < 1 >	Active v Vew rested							
ISE31-WWS 2021-09-17 12:57:11 UTC+0200 © HOLLBACK_IN_PROGRESS	Q. Search events			•				
AWS-ISE31-Stack	Timestamp v	Logical ID	Status	Status reason				
2021-05-14 16/07.43 UTC+0200	2021-09-17 12:57:19 UTC+0200	ISE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [tielEc2instance]. Rollback requested by user.				
	2021-09-17 12:57:18 UTC+0200	IseEc2instance	⊗ CREATE_FAILED	Security group sp.0454161(882201463 and submet-offbabcide63255143 belong to different networks. IService: Anazon622; Status Code: 400; Errar Code: InvalidParameter; Request ID: b07x9773- f864-3458-8648-86409536444; Prozr, null				
	2021-09-17 12:57:17 UTC+0200	IseEc2instance	CREATE_IN_PROSRESS					
	2021-09-17 12:57:11 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User initiated				

解决方案:

确保从同一VPC中提取安全组。导航至VPC服务下的安全组,并注意安全组ID,确保它与正确的 VPC(ISE所在的位置)对应,然后验证VPC ID。

连接问题

可能存在多个问题,导致AWS上ISE的连接无法正常工作。

1.由于安全组配置错误,导**致连接问题。**

解决方案:如果安全组配置错误,ISE无法从内部网络访问,甚至在AWS网**络中也**无法访问。确保 在与ISE网络关联的安全组中**允许所**需的协议和端口。有关要打<u>开的必需</u>端口,请参阅ISE端口参考 2.由于路由配置错误而导致的连接问题。

解决方案:由于拓扑的复杂性,很容易错过On-Prem网络和AWS之间的某些路由。在您使用ISE功 能之前,请确保端到端连接到位。

Appendix

交换机AAA/RADIUS相关配置

```
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
1
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
1
radius server ISE31-2
address ipv4 10.0.1.100 auth-port 1645 acct-port 1646
key cisco
```