通過AWS Marketplace配置ISE 3.1

目錄

簡介 必要條件 需求 採用元件 設定 網路拓撲 組態 可選步驟A.建立VPC 可選步驟B.配置內部VPN頭端裝置 <u>可選步驟C.建立自定義金鑰對</u> 可選步驟D.建立自定義安全組 步驟1.訂購AWS ISE Marketplace產品 步驟2.在AWS上配置ISE 步驟3.在AWS上啟動ISE 步驟4.在AWS上為ISE配置CloudFormation堆疊 步驟5.訪問AWS上的ISE 步驟6.在AWS上配置本地ISE和ISE之間的分散式部署 步驟7.將ISE部署與本地AD整合 限制 驗證 疑難排解 CloudFormation堆疊建立失敗 連線問題 附錄 交換器AAA/Radius相關組態

簡介

本文檔介紹如何通過Amazon Web Services(AWS)中的Amazon Machine Images(AMI)安裝Identity Services Engine(ISE)3.1。 從3.1版起,藉助CloudFormation模板(CFT),ISE可以部署為Amazon Elastic Compute Cloud(EC2)例項。

必要條件

需求

思科建議您瞭解以下主題的基本知識:

ISE

• AWS及其概念,如VPC、EC2、CloudFormation

採用元件

本文檔中的資訊基於Cisco ISE版本3.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

網路拓撲



組態

如果尚未配置VPC、安全組、金鑰對和VPN隧道,則需要執行可選步驟,否則從步驟1開始。

可選步驟A.建立VPC

導航至VPC AWS Service。選擇**啟動VPC嚮導**,如下圖所示。

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: 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 Resource	ces	
	You are using the following	g Amazon VPC resources		
Your VPCs	VPCs See all regions 🔻	Frankfurt 1	NAT Gateways See all regions	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		See all regions V	

選擇VPC with Private Subnet Only and Hardware VPN Access,然後按一下Select,如下圖所示。

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 sut from the Internet. You can conne	colated 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		
			Corporate Data Center	

附註:在VPC嚮導的步驟1.中選擇的VPC取決於拓撲,因為ISE不設計為網際網路暴露的伺服器 — 僅使用具有專用子網的VPN。

根據網路設計配置VPC專用子網設定,然後選擇**下一步**。

aws	Services v		Q Search for services, features, m	arketplace products, and docs	[Option+S]	D 4	alice @ 8682-5143-9359 🔻	Frankfurt 🔻	Support 🔻
Step 2: V	PC with a Pri	vate Subnet Only and Har	rdware VPN Access						
	IPv4 CIDR block:*	10.0.0/16 (65531 IP	addresses available)						
	IPv6 CIDR block:	No IPv6 CIDR Block Amazon provided IPv6 CIDR bloci IPv6 CIDR block owned by me	ĸ						
-	VPC name:	ISE-VPC							
Private su	bnet's IPv4 CIDR:*	10.0.1.0/24 (251 IP ad	idresses available)						
	Availability Zone:*	No Preference V							
Pri	vate subnet name:	ISE-subnet							
		You can add more subnets after Ama	zon Web Services creates the VPC.						
	Service endpoints	Add Endpoint							
Enable	DNS hostnames:*	e Yes ○ No							
н	lardware tenancy:*	Default V							
							Cancel	and Exit	Back Naxt

根據您的網路設計配置VPN,然後選擇Create VPC。

aws	Services 🔻	Q Search for services, features, marke	etplace products, and docs	[Option+S]	⊠ ≎	alice @ 8682-5143-9359 🔻	Frankfurt 🔻	Support ¥
Step 3: 0	Configure your VPN							
Specify the p	public IP Address of your VPN router (Customer Gatewa	ñ						
	Customer Gateway IP:*							
	Customer Gateway name:	OnPrem-GW						
	VPN Connection name:	ISE-tunnel						
		lote: 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

建立VPC後,將顯示**消息「已成功建立**VPC」。按一下「**OK**」,如下圖所示。

aws Services	•	Q Search for s	ervices, features, marketplace products, and docs	[Option+S]	Σ	۵	alice @ 8682-5143-9359 V	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									

可選步驟B.配置內部VPN頭端裝置

導航至VPC AWS Service。選擇Site-to-Site VPN connections,選擇新建立的VPN隧道,然後選擇 Download Configuration,如下圖所示。

aws Services T	Q Search for services, features, marketplace products, and docs [Option+S]	D \$**
New VPC Experience	Create VPN Connection Download Configuration Actions *	
Network ACLs	Q Filter by tags and attributes or search by keyword	
Security Groups	Name v VPN ID 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	Detaile Tuppel Detaile Tage	
Site-to-Site VPN Connections		State available
Client VPN Endpoints	VPN UD Vpn-uec12805119880182 Virtual Private Gateway vgw-0d293950bc1377ae8	Customer Gateway cgw-0944cf9c0927fe539

選擇Vendor、Platform和Software,然後選擇Download,如下圖所示。

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 Download	

在內部VPN頭端裝置上應用下載的配置。

可選步驟C.建立自定義金鑰對

藉助金鑰對訪問AWS EC2例項。要建立金鑰對,請導航到EC2 Service。在Network & Security下選 擇Key Pairs選單。 選擇Create Key Pair,為其指定Name,保留其他值為預設值,然後再次選擇 Create Key Pair。

Create key pair Info

Key pair

Name			
aws			
The name can include up to 255 ASCII characters. It can't include leading or trailing space	es.		
Key pair type Info			
S 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.			

可選步驟D.建立自定義安全組

AWS EC2例項訪問受Security Groups保護,要配置Security Group,請導航到EC2 Service。在 Network & Security下選擇Security Groups選單。在VPC欄位中選擇Create Security Group,配置 Name、Description,然後選擇新配置的VPC。配置入站規則以允許與ISE通訊。選擇建立安全組 ,如下圖所示。

C2 > Security Groups > Cre	ate security group	>					
Create security gr	roup Info						
security group acts as a virtual fi	irewall for your in	stance to control inbou	nd and outbound traffic. To create a new securi	ity group, complete the fields	below.		
Basic details							
Security group name Info							
ICMP/HTTPS/SSH/RemoteVP	NSubnet						
Name cannot be edited after creation	n.						
Description Info							
ICMP/HTTPS/SSH/RemoteVP	NSubnet						
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 ¥	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 ×		
Add rule							

附註:配置的安全組允許通過SSH、ICMP、HTTPS訪問ISE,並且允許所有協定從內部子網訪問。

步驟1.訂購AWS ISE Marketplace產品

導航至AWS Marketplace Subscriptions AWS Service。選擇Discover Products,如下圖所示。

aws Services 🔻	Q [search for services, features, marketplace products, and docs [Option+S]	Ŧ								
AWS Marketplace $\qquad imes$	S Marketplace AMIs now supported with Spot Instances in the EC2 Launch Instance Wizard. <u>What's New</u> 🕑									
Manage subscriptions Discover products Product Support Connection 🗹 Settings	AWS Marketplace > Manage subscriptions Manage subscriptions info Actions									
	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.									
	Your subscriptions All delivery methods V									

搜尋ISE產品並選擇思科身分識別服務引擎(ISE),如下圖所示。

aws Services 🔻	Q Search for services, f	atures, marketplace products, and docs [Option+S]	alice @ 8682-5143-9359 🔻 Glob	al 🔻 Supp	port 🔻
AWS Marketplace ×	AWS Marketplace > Discover products >	Search results			٩
Discover products Product Support Connection	Refine results Categories	Search AWS Marketplace products Q. ISE		×	
Settings	Infrastructure Software (5) Delivery methods Amazon Machine Image (4)	ISE (5 results) showing 1 - 5 Did you mean ice, isr?	< 1 > Sort By: Relevance	© •	
	CloudFormation Template (1) Publisher Cisco (4) Toshiba Digital Solutions Corporation (1)	Cisco Identity Services Engine (ISE) C by Cisco Systems, Inc. (2) IVer 3.1 Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (N/ managed from the cloud while ensuring the flexibility required to meet each or Cisco ISE on AWS, you can unify the policy management of your or	AC) service workloads to be deploy ganizations unique cloud strategy.	ed and With	

🛫 aws	s marketpla	ace							Q		Hello,	alice 🔻
About 👻	Categories 🕶	Delivery Methods 👻	Solutions 👻	AWS IQ 🔻	Resources 🔻	Your Saved List 🤨			Partners	Sell in AWS Marketplac	e Amazon Web Services Home	е Неір
			ili.ili. cisco	Cisco ISE endpoint Show I Linux/U BYOL	Identity Se systems, Inc. on AWS provides s s. Cisco ISE enables more Inix	Latest Version: 3.1 ecure network access cont you to easily segment ne	(ISE) trol for IoT, BYOD, and co twork access for employ	orporate owned ees, contractors,	Continue to Subsc Remove Typical Total Price Sto.68/hr Total pricing per instance for hosted on CS-stalarge in US E Virginia). View Details	ribe e * services azt (N.		
			Overview	,	Pricing	U	Isage	Support	Revie	WS		
		Pro Clisto Acce man meet AWS acce iSE ii man foref For r http: We By Vii	oduct O b Identity Service aged from the cl t each organizati so control and ne s equipped with agement, bringi front of your NA4 more information cr/www.clsco.co rision deo	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 Nett ds to be deployed a ing the flexibility re d strategy. With Cis ement of your orga ministration. Cisco mate policy and lift yment and automai ease visit	work ind quired to co ISE on inization for endpoint ecycle tion to the 3.1 Cisco Systems, inc. (? See Product Video (?	Highlights • Gain visibility what, where, connecting to limit risk, with • Extend zero 1 Network seg the spread of containment • Accelerate th with other CI active arm of and increase	y with context and cor and how endpoints a o your network to end h or without the use trust to contain threal mentation shrinks the f ransomware, and en e value of existing so isco and third-party so protection into passi your return on invest	ntrol: Know who, and devices are sure compliance and of agents. ts: Software-Defined a attack surface, limits ables rapid threat ables rapid threat lutions: Integrate olutions to bring an we security solutions ment (ROI).			

選擇Accept Terms按鈕,如下圖所示。

About v Categories v Delivery Method v Solution v Avail v No solution v Varia v Varia Solution v Notice V Available V Varia V<	About v Outprovers Outprovers Ward big Ward big Vers and big Percence v Outprovers Percence v Outprovers Percence v Outprovers Percence v	🐓 aws marketplace						Q _		Hello, a	alice 🖤
Constant Services Engine (ISE) Constant Services Engine (ISE)	Cisco Identity Services Engine (ISE) Contact End Conditions Provide Team Second End Team Contact End Conditions	About - Categories - Delive	ery Methods 👻 Solutions 👻	AWS IQ 👻	Resources 👻	Your Saved List 🌖		Partners	Sell in AWS Marketplace	Amazon Web Services Home	Help
• Product Detail Subscription • Comparison Comparison	Version 2000 Subscription Concerned a subscription, review the pricing information and accept the terms for this software. Correst a subscription, review the pricing information and accept the terms for this software. Correst and Conditions Subscription this software, you agree to the pricing terms and the seller's End User Learner Agreement (EULA) (2 ^A , You also agree and acknowledge that AWS may share Subscription to this software, you agree to the pricing terms and the seller's End User Learner Agreement (EULA) (2 ^A , You also agree and acknowledge that AWS may share Subscription and buch this mascription (Including your payment terms) with the expective Subscription agreement with AWS governing your use of such services. The following table shows pricing Information for the listed software components. You're charged separately for your use of each component. You use of AWS services Engline (SEE)		cisco	Cisco Ide	ntity Ser	vices Engine (ISE)	Cont You mu	tinue to Con ust first review	figuration and accept terms.		
AUXAL INFUTIOR JUST AND AUXALIA			Product Detail Set Subscribing to the following table of each component Cisco Destroition about seller, reseller or un Notice (24, Your use agreement with AW) The following table of each component	ascribe to this so pation, review the ditions ac. Offer as software, you ag this transaction (inc (CULA) C. You also this transaction (inc (CULA) C. You also software, you ag software, you ag softwa	Diftware pricing inform agree and ack fuding your part as applicable, in subject to the <i>A</i> se of such serv rmation for the Additional te Cisco Idi	E mation and accept the terms for this software. 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> ²⁷ or other Listed software components. You're charged separately for your wes or fees may apply. Initity Services Engine (ISE)	r use				

一旦預訂了Effective和Expiration date的狀態,並更改為Pending,如下圖所示。

< 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**為訂閱日期,到期日期**更改**為**N/A後不久。選擇Continue to Configuration**,如ima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

步驟2.在AWS上配置ISE

在**Configure this software**螢幕的Delivery Method選單中,選擇**Cisco Identity Services** Engine(ISE)。在Software Version中選擇3.1(2021年8月12日)。選擇Region,其中計畫部署 ISE。選擇**繼續啟動。**



< 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	
FIL (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

步驟3.在AWS上啟動ISE

從**啟動此軟體**螢幕的「操作」下拉選單中,選擇**啟動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

(可選)選擇使用說明以使自己熟悉這些說明。選擇**啟動**。

步驟4.在AWS上為ISE配置CloudFormation堆叠

啟動按鈕將您重定向到**CloudFormation Stack設**置螢幕。有一個預構建模板必須用於設定ISE。保留 預設設定,然後選擇**下一步**。

aw	s s	Services 🔻	Q Search for services, features, market	tplace products, and docs	[Option+S]		24	alice @ 86	682-5143-9359 🔻	Frankfurt 🔻	Support 🔻
=	Clou	udFormation $>$ Stacks $>$ Create stack									
	Step Spec	cree	ate stack								
	Step Spec	e 2 Pr	erequisite - Prepare template								
	Step Conf	23 Provide a start options	pare template ry stack is based on a template. A template is a JSON o Template is ready	r YAML file that contains confi	uration information about t	the AWS resources you want to include O Create template in Desig	in the stack				
	Step Revi	jew Si	ecify template emplate is a JSON or YAML file that describes your stad	k's resources and properties.							
		Te	mplate source ecting a template generates an Amazon S3 URL where i	it will be stored.							
		An	Amazon S3 URL		 Upload a templa 	te file					
			https://s3.amazonaws.com/awsmp-fulfillment-c	f-templates-prod/bedef66	2-aba4-427e-b523-7c9	3cd50111c.f7b45e37-579d-4492	-bf3d-e4	95ba9;			
		Arr	azon S3 template URL								
		S3 79	URL: https://s3.amazonaws.com/awsmp-fulfil d-4492-bf3d-e495ba925376.template	lment-cf-templates-prod/	oedef662-aba4-427e-b5	623-7c93cd50111c.f7b45e37-5	View in Design	er			
						Cance	et 📘	Next			

使用堆疊名稱填充CloudFormation**堆疊資料**。配置例項詳細資訊,如**主機名**,選擇**例項金鑰對**和管 **理安全組。**

ep 1 pecify template	Specify stack details
ep 2 pecify stack details	Stack name
	Stack name
ep 3 onfigure stack ontions	AWS-ISE31-Stack
ingure start options	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
view	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 usemame "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/HTTP5/SSH/RemoteVPNSubnet (sq-0792bfa6bba47098d)

繼續使用管理網路、管理專用IP、時區、例項類型、EBS加密和卷大小配置例項詳細資訊。

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.

low in 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 Thoose a system time zone.	
Etc/UTC	•
nstance Type Choose the required Cisco ISE instance type.	
c5.4xlarge	•
EBS Encryption Thoose 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

繼續使用DNS域、名稱伺服器、NTP服務和服務配置實例詳細資訊。

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使用者密碼並選擇下一步。

User Details

Enter Password

Enter Password Enter a password for the username "admin". The password must be aligned with the Cisco ISE password policy. The configured pas Warning: The password is displayed in plaintext in the User Data section of the Instance settings window in the AWS Console.	sword is used f	or Cisco ISE GUI acce	SS.
••••••			
Confirm Password Retype Password			
••••••			
	Cancel	Previous	Next

下一螢幕不需要更改。選擇Next。

CloudFormation > Stacks > Step 1 Specify template	Create stack 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

前往Review Stack視窗,向下滾動並選擇Create stack。

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

部署堆疊後,必須看到CREATE_COMPLETE狀態。

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	

步驟5.訪問AWS上的ISE

要訪問ISE例項,請導航到**Resources**頁籤以檢視從CloudForms建立的EC2例項(或者導航到 Services > EC2 > Instances以檢視EC2例項),如下圖所示。

CloudFormation > Stacks > AWS-ISE31-Stack	
🗆 Stacks (1)	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	
(1)	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 -

選擇Physical ID以開啟EC2 Instances選單。確保Status檢查具有2/2個通過檢查的狀態。

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

選擇例項ID。可通過SSH或HTTPS協定通過私有IPv4地址/私有IPv4 DNS訪問ISE。

附註:如果您通過專用IPv4地址/**專用IPv4 DNS**訪問ISE,請確儲存在指向ISE專用地址的網路 連線。

通過專用IPv4地址通過SSH訪問的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# **附註**:通過SSH訪問ISE大約需要20分鐘。直到此時與ISE的連線失敗,出現「**Permission** denied(publickey)(**許可權被拒絕(publickey))」**。 錯誤消息。

使用show application status ise驗證服務是否正在運行:

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#

附註:由於SSH可用於ISE服務,需要大約10-15分鐘才能轉換到運行狀態。

Application Server處於running狀態後,您可以通過GUI訪問ISE,如下圖所示。

● Identity Services Engine × +	- 6	ø	×
← → C 🔺 Not secure 10.0.1.100/admin/fogin.jsp	☆	θ	:
A NORMAL Y CONTROLLED		4	
Settings to activate Wi			
© 2021 Clsco Systems Inc. Clsco, Clsco Systems and Clsco Systems logo are registered trademarks of Clsco Systems Inc. and/or its affiliates in the U.S and certain other countries. Clsco ISE utilizes open source software from various components. View third-party locenses and notices			

步驟6.在AWS上配置本地ISE和ISE之間的分散式部署

登入到本地ISE並導航到**管理>系統>部署。**選擇節點並選擇**Make Primary。導航回管理>系統>部署** ,選擇**註冊**。在AWS上配置ISE的**主機FQDN**、GUI用**戶名**和密**碼。**按「Next」(下一步)。

≡ Cisco ISE	Administration - System	🔺 Evaluation Mode 70 Days Q 🕜 🔎
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Sett	tings
Deployment < 별 > 法 Deployment 炎 PAN Failover	Opployment Nodes List > Specify Hostname Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials Host FQDN* ise31-2.example.com User Name* admin Password* e======	Next Cancel

由於此拓撲中使用自簽名證書,要將管理員證書交叉匯入到受信任的儲存中,請選擇**匯入證書並繼** 續。



Cancel Registration

Import Certificate and Proceed

選擇您選擇的角色,然後按一下**提交**。

Administration - System

🔺 Evaluation Mode 70 Days 📿 💮 🕫

Deployment Licensing Certifica	ates 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
≵ PAN Failover	Hostname ISE31-2 FQDN ISE31-2.example.com IP Address 10.0.1.100 Node Type Identity Services Engine (ISE)
	Administration Administration Monitoring
	Policy Service
	> pxGrid ()

Cancel Submit

同步完成後,節點將轉換到連線狀態,其上方將顯示綠色覈取方塊。

E Cisco ISE		🔺 Evaluation Mode 70 Days Q 💮 🔎		
Deployment Licensing Cert	ficates Logging Main	ntenance Upgrade Health Checks	Backup & Restore Admin Access	Settings
Deployment	Deployment N	Nodes		Selected 0 Total 2 👩 🍈
> 5% Deployment	🖉 Edit 🚯 Register 🕤) Syncup 🕞 Deregister		all \sim $ \nabla$
ogo PAN Fallover	Hostname	∧ Personas	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	

步驟7.將ISE部署與本地AD整合

導航到管理>身份管理>外部身份源。選擇Active Directory,選擇Add。

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

配置**聯合點名稱**和Active Directory域,選擇提交。

E Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 70 Days Q 💮 🕞
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
External Identity Sources	Connection	^
Certificate Authentication F	Join Point Name EXAMPLE	
C Active Directory	Active Directory example.com	
🗂 LDAP		
C ODBC		
C RADIUS Token		
C RSA SecurID		
SAML Id Providers		
🛅 Social Login		
		v
	¢	>
		Submit Cancel

要將兩個節點與Active Directory整合,請選擇**Yes**。

(i) Information

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

No Yes

輸入**AD使用者名稱**和密碼,然後按一下確定。ISE節點成功與Active Directory整合後,節點狀態將 更改為「已完成」。

Close

限制

有關AWS上的ISE限制,請參閱ISE管理指南的<u>已知限制</u>部分。

驗證

要驗證在AWS上的ISE PSN上執行身份驗證,請導航至**Operations > Radius > Live Logs**,然後在 Server列中確認是否觀察到AWS PSN上的ISE。

■ Cisco ISE		Operations • RADIUS						A Evaluation Mode 7	0 Days Q	0	P (\$
Live Logs Live Sessions											
Misconfigured Supplicants ①		Miscor	nfigured Ne	twork Devices 🕕	R	ADIUS Drops 🕕	Client Sto	pped Responding 🕕	Re	opeat Co	ounter 🕕
0			0)		0		1		0)
Ø Refresh	unts ① Export To	∽ Details	Repea	Identity	Endpoint ID	Endooint Profile	Re Muthentication Poli	Never V Latest 20 reco	ords v L	ithin .ast 3 h V Filt	ours ∨ er∨ ⊚ Autho
×		~		Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Se	erver	Autho
Sep 15, 2021 12:22:33.4	•	0	0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE	31-2	Permit
Sep 15, 2021 12:22:32.8		<u>o</u>		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE	31-2	Permit
Sep 14, 2021 08:25:37.3		ò		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise:	31	Permit
Sep 14, 2021 08:22:12.0		6		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise:	31	Permit

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

CloudFormation堆叠建立失敗

CloudFormation堆疊建立可能由於多種原因而失敗,其中一個原因就是您從VPN中選擇與ISE管理 網路不同的安全組。錯誤與影象中的錯誤類似。

CloudFormation > Stacks > ISE31-AWS										
🗆 Stacks (2) 🛛 🔿	ISE31-AWS	E31-AWS Delete Update Stack actions * Create stack *								
Q, Filter by stock nome	Stack info Events Resources Outputs Parameters	Template Change sets								
Active View nested										
	Events (4)			G						
ISE31-AWS 2021-09-17 12:57:11 UTC+0200 © ROLLBACK_IN_PROGRESS	Q. Search events			•						
AW5-I5E31-Stack	Timestamp v L	Logical ID	Status	Status reason						
2021-09-14 16:07:43 UTC+0200 (CREATE_COMPLETE	2021-09-17 12:57:19 UTC+0200 15	SE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [tselfc2instance]. Rollback requested by user.						
	2021-09-17 12:57:18 UTC+0200 8	seEclinstance	© CREATE_FAILED	Security group sq-0x54161c8426234e53 and subnet subnet-offbetbodae62a58143 belong to different networks. (Service AmazonEC); Status Code; 400; mrs Code: Invalid@ranmeter; Request ID: b07x9773- fted=43c5-63e54c4c460553a64c4; Progr. null)						
	2021-09-17 12:57:17 UTC+0200 IN	seEc2instance	@ CREATE_IN_PROGRESS							
	2021-09-17 12:57:11 UTC+0200 IS	SE31-AWS	CREATE_IN_PROGRESS	User Initiated						

解決方案:

確保從同一個VPC獲取安全組。導覽至VPC 服務底下的**安全組**,注意**安全組ID**,確保它對應於正確 的VPC(ISE所在的位置),驗證VPC ID。

連線問題

可能會出現多個問題,導致無法連線到AWS上的ISE。

1.由於安全組配置錯誤而引起的連線問題。

解決方案:如果安全組配置錯誤,則無法從內部網路甚至在AWS網**絡中訪**問ISE。確保在與ISE網路 關聯的**安全組**中允許所需的協定和埠。請參閱<u>ISE埠參考</u>以瞭解需要開啟的埠。 2.由於路由配置錯誤導致的連線問題。

解決方案:由於拓撲的複雜性,很容易遺漏本地網路和AWS之間的某些路由。在使用ISE功能之前 ,請確保端到端連線已就緒。

附錄

交換器AAA/Radius相關組態

```
aaa new-model
1
!
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
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
1
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
```