

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

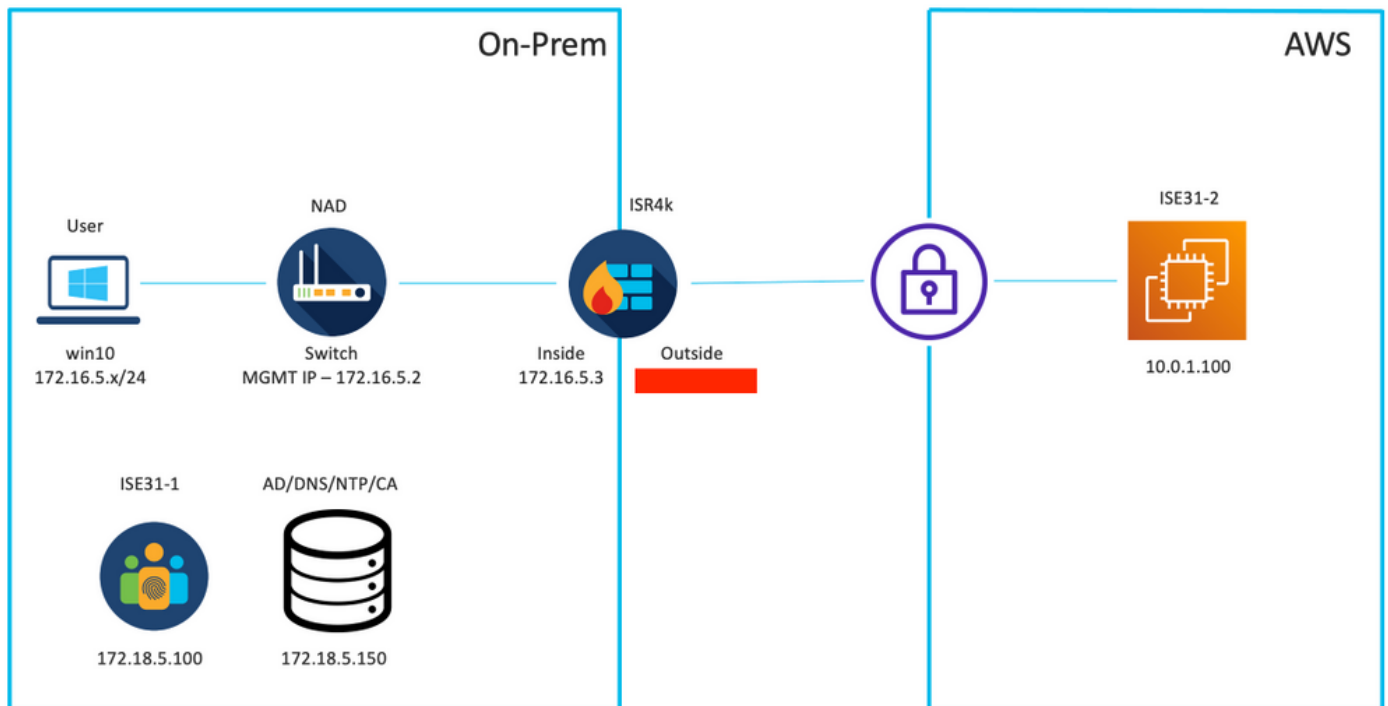
使用的组件

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

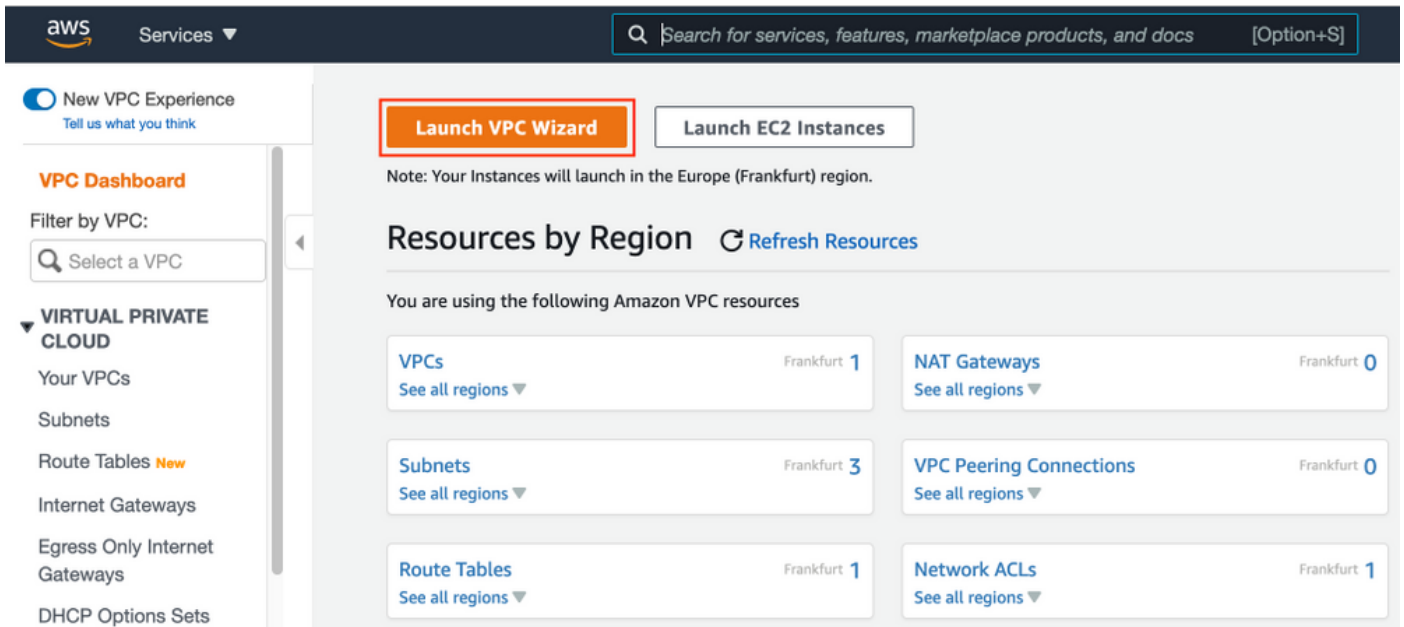


配置

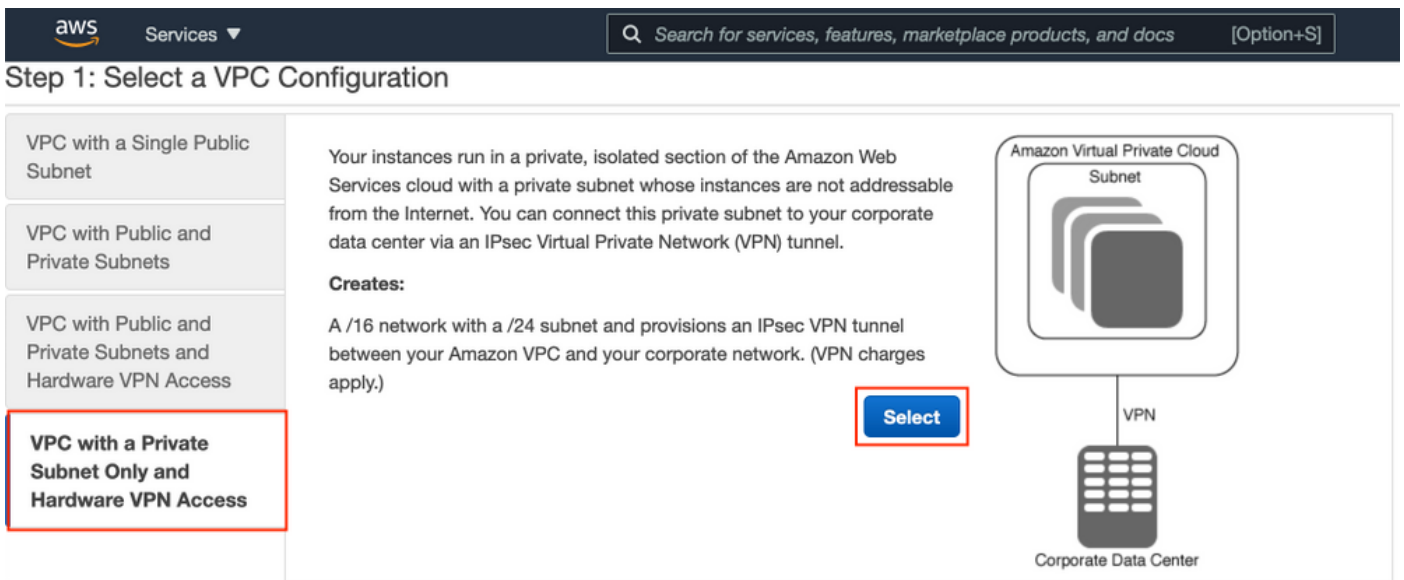
如果尚未配置VPC、安全组、密钥对和VPN隧道，则需要执行可选步骤，否则，从步骤1开始。

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。

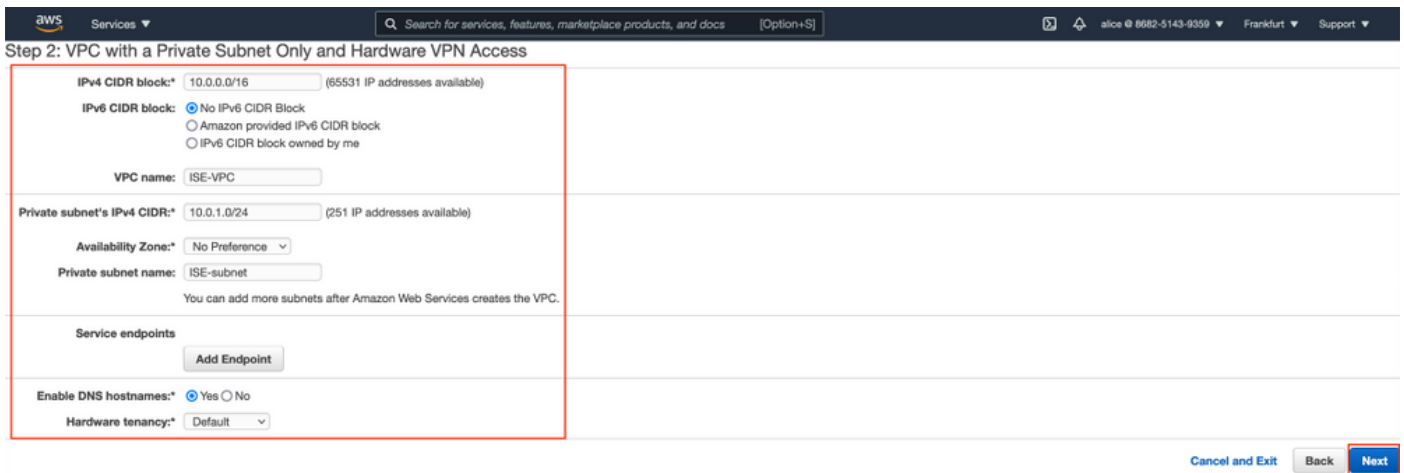


选择VPC with Private Subnet Only and Hardware VPN Access，然后单击Select，如图所示。

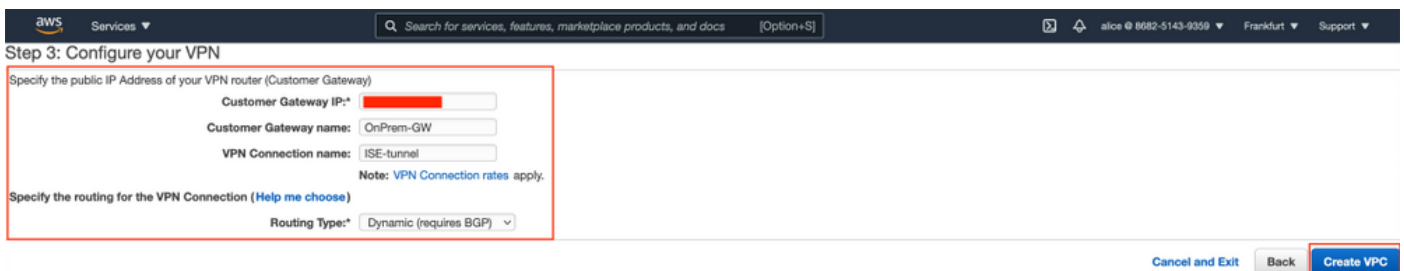


注意： VPC向导步骤1.中VPC的选择取决于拓扑，因为ISE不设计为Internet外露服务器 — 仅使用带私有子网的VPN。

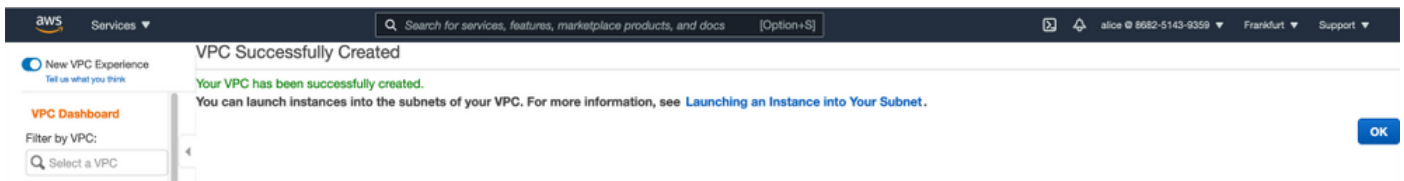
根据您的网络设计配置VPC专用子网设置并选择下一步。



根据网络设计配置VPN，然后选择“创建VPC”。

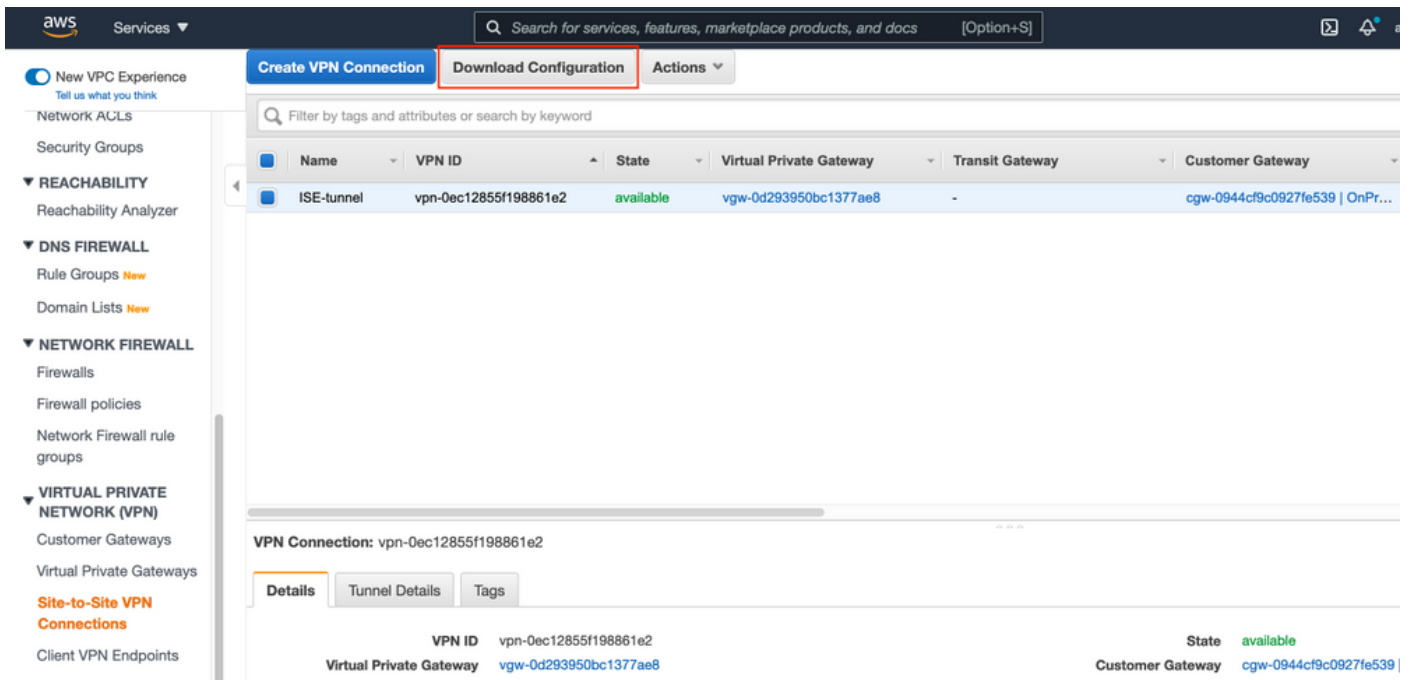


创建VPC后，将显示“Your VPC has been successfully created”(您的VPC已成功创建)消息。单击OK(确定)，如图所示。

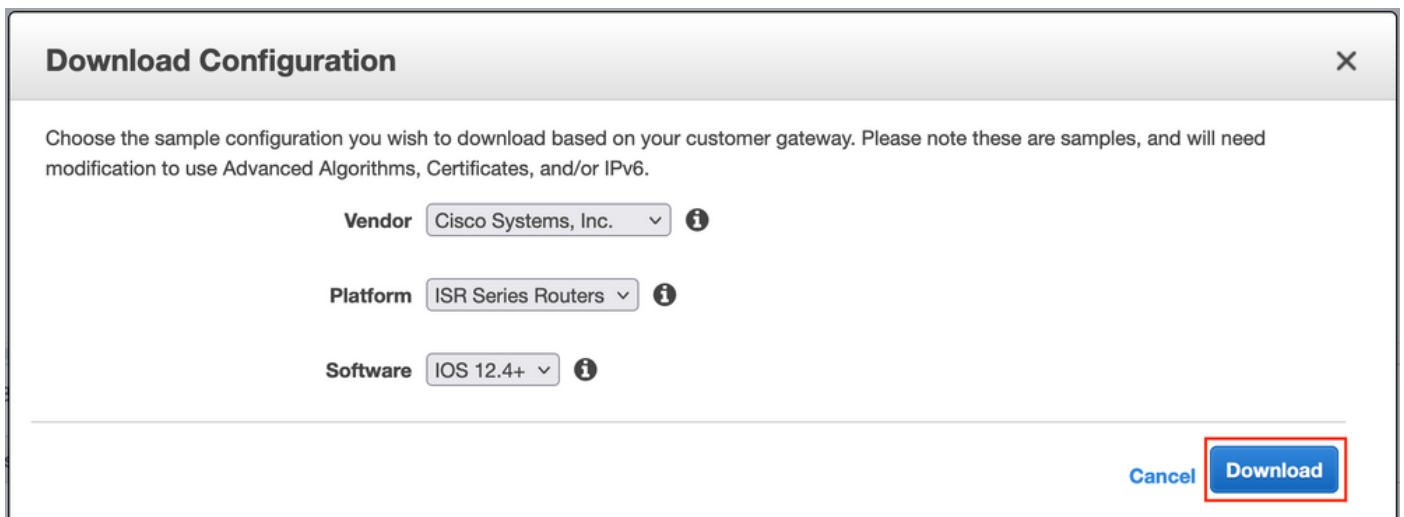


可选步骤B.配置内部VPN头端设备

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。



选择供应商、平台和软件，选择下载，如图所示。



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

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

Name

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

Key pair type [Info](#)

- RSA
 ED25519

Private key file format

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

Tags (Optional)

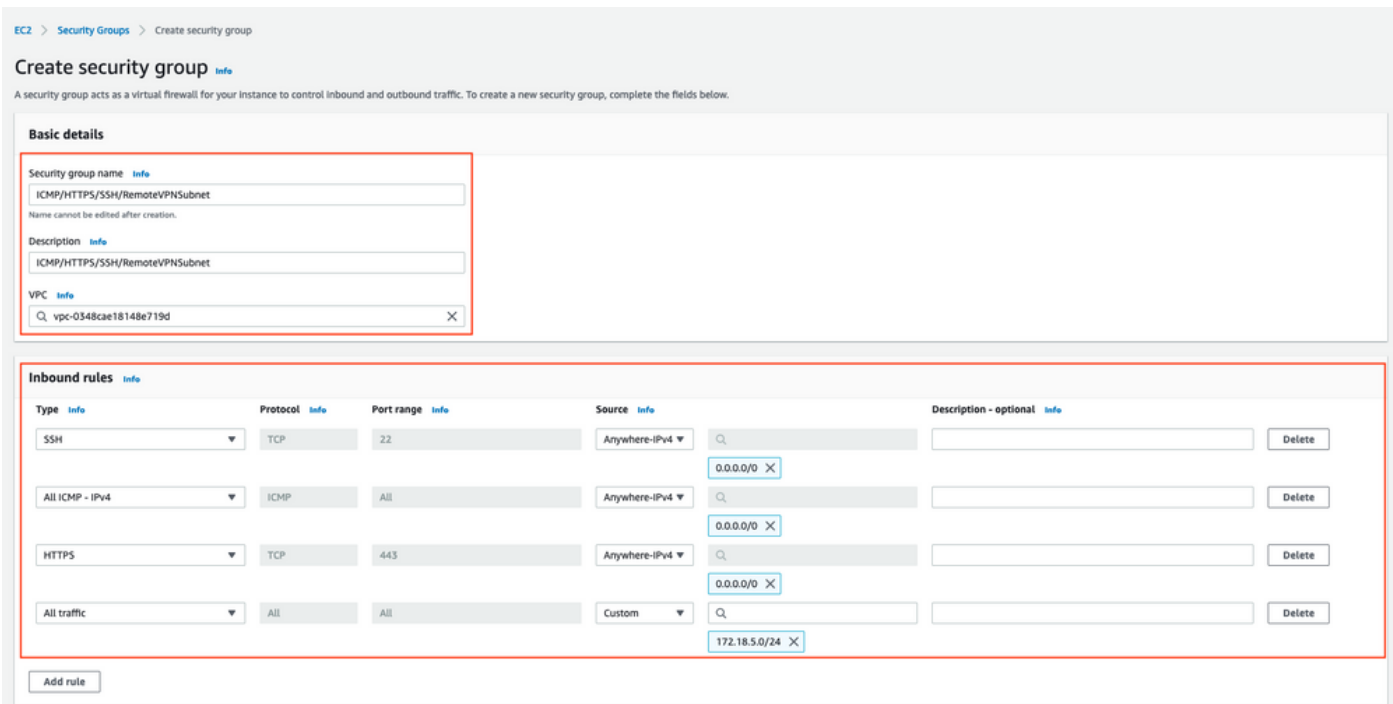
No tags associated with the resource.

You can add 50 more tags.

Cancel

可选步骤D.创建自定义安全组

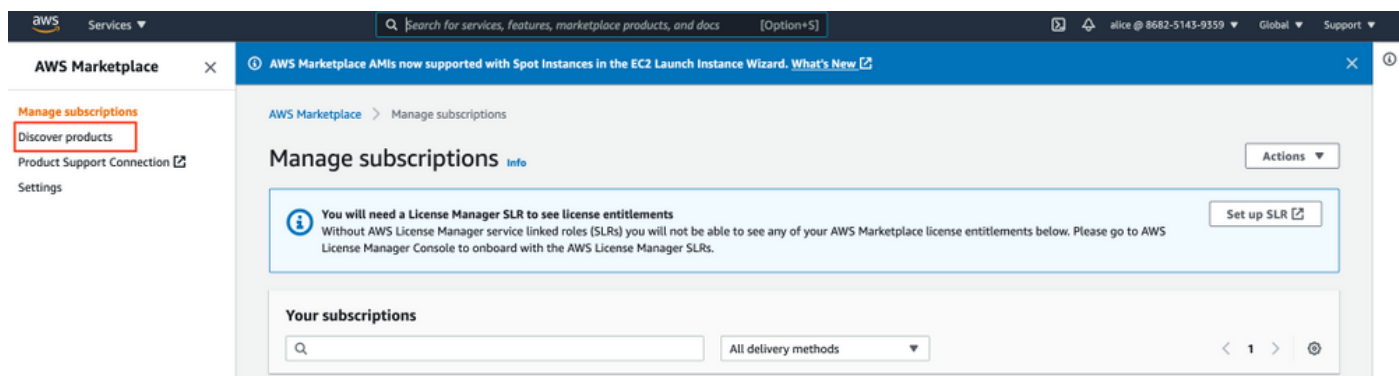
AWS EC2实例访问受安全组保护，要配置安全组，请导航至EC2服务。在“网络和安全”下选择“安全组”菜单。在VPC字段中，选择创建安全组，配置名称，说明，选择新配置的VPC。配置入站规则以允许与ISE通信。选择创建安全组，如图所示。



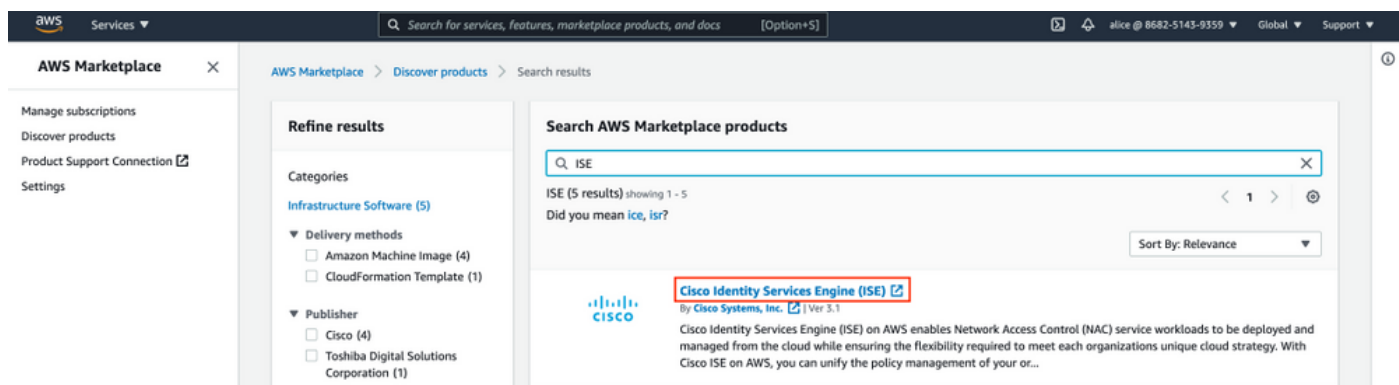
注意：配置的安全组允许SSH、ICMP、HTTPS访问ISE，以及从内部子网访问所有协议。

步骤1. 订购AWS ISE市场产品

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



搜索ISE产品并选择思科身份服务引擎(ISE)，如图所示。



选择“继续订阅”按钮

aws marketplace

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

Partners Sell in AWS Marketplace Amazon Web Services Home Help

Cisco Identity Services Engine (ISE)

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

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

Linux/Unix
BYOL

Continue to Subscribe

Remove

Typical Total Price
\$0.68/hr
Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

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

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

Version	3.1
By	Cisco Systems, Inc.
Video	See Product Video

Highlights

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

选择**接受术语**按钮，如图所示。

aws marketplace

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

Partners Sell in AWS Marketplace Amazon Web Services Home Help

Cisco Identity Services Engine (ISE)

[Continue to Configuration](#)
You must first review and accept terms.

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

Subscribe to this software

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

Terms and Conditions

Cisco Systems, Inc. Offer

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

Accept Terms

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

Cisco Identity Services Engine (ISE) BYOL	Additional taxes or fees may apply.
	Cisco Identity Services Engine (ISE)

订用有效和到期日期后，更改为**待定**，如图所示。

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

X

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

Subscribe to this software

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

Terms and Conditions

Cisco Systems, Inc. Offer

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

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	○ Pending	○ Pending	▼ Show Details

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



Cisco Identity Services Engine (ISE)

[Continue to Configuration](#)

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

X

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

Subscribe to this software

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

Terms and Conditions

Cisco Systems, Inc. Offer

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

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	8/23/2021	N/A	▼ Show Details

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.

Delivery Method

Cisco Identity Services Engine (ISE) ▼

Software Version

3.1 (Aug 12, 2021) ▼

Whats in This Version

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

[Learn more](#)

Region

EU (Frankfurt) ▼

Product code: basttrzv6xwc4yn2uup6bh730

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

Pricing information

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

Software Pricing

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

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) <i>running on c5.4xlarge</i>
Software Version	3.1
Region	EU (Frankfurt)

[Usage Instructions](#)

Choose Action

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

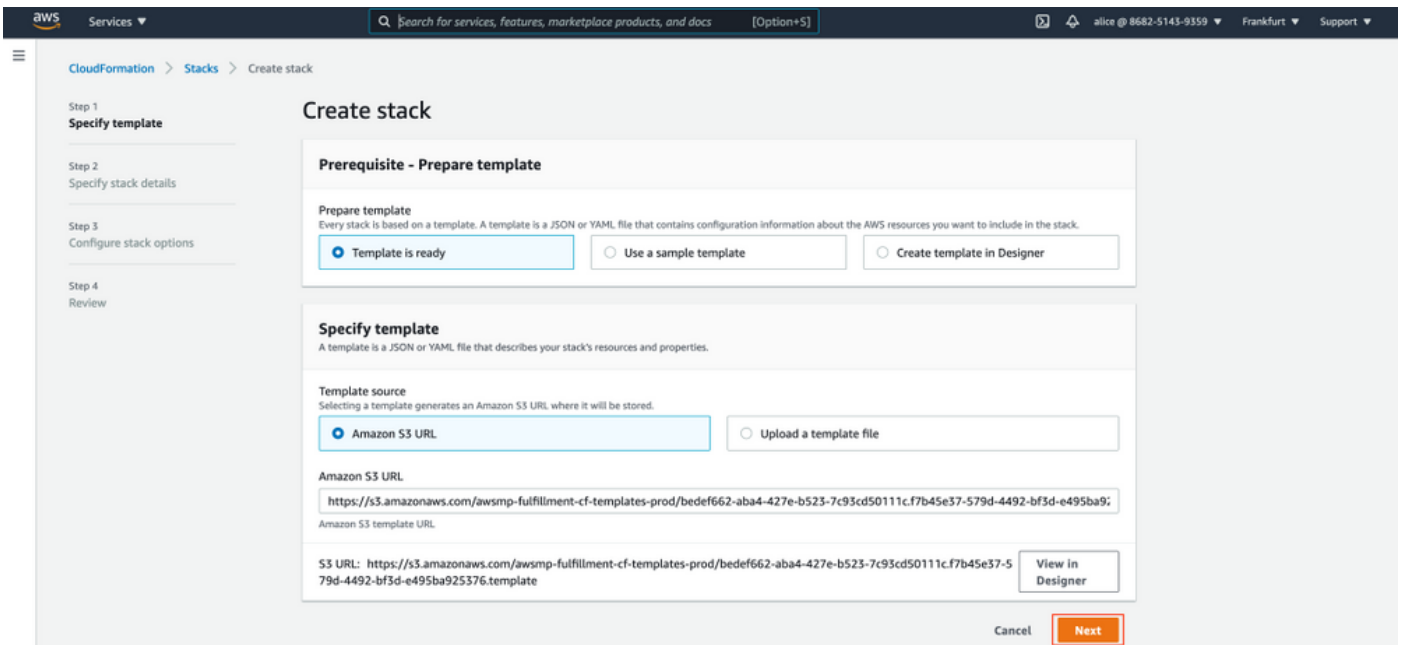
Choose this action to launch your configuration through the AWS CloudFormation console.

[Launch](#)

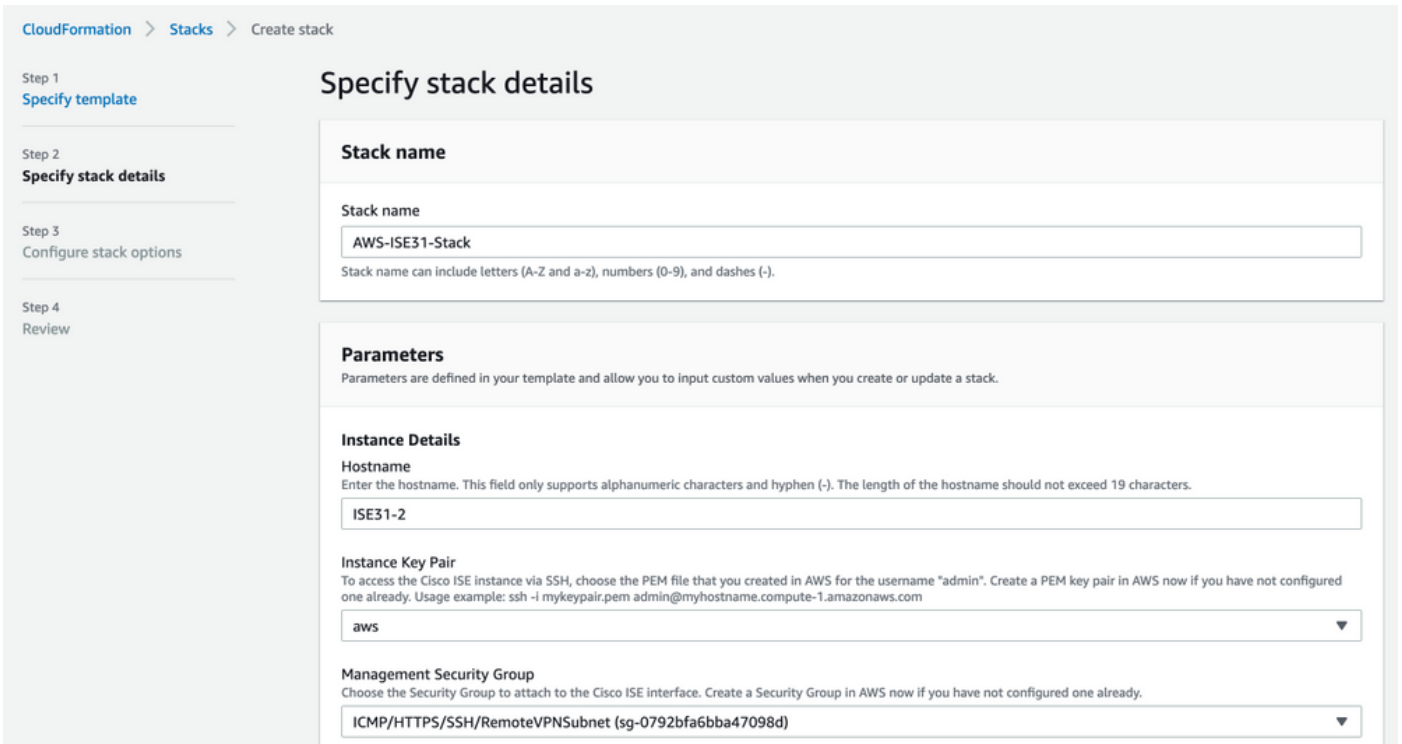
(可选) 选择“**使用说明**”以便您熟悉这些说明。选择“**启动**”。

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**”。



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。



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

Management Private IP

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

10.0.1.100

Time Zone

Choose a system time zone.

Etc/UTC ▼

Instance Type

Choose the required Cisco ISE instance type.

c5.4xlarge ▼

EBS Encryption

Choose true to enable EBS encryption.

true ▼

Volume Size

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

300 ↕

继续使用DNS域、名称服务器、NTP服务和配置实例详细信息。

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 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**

下一屏幕无需更改。选择 Next (下一步)。

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Configure stack options

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

Key Value Remove

Add tag

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

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

IAM role name Sample-role-name Remove

转到“查看堆栈”屏幕，向下滚动并选择“创建堆栈”。

Stack creation options

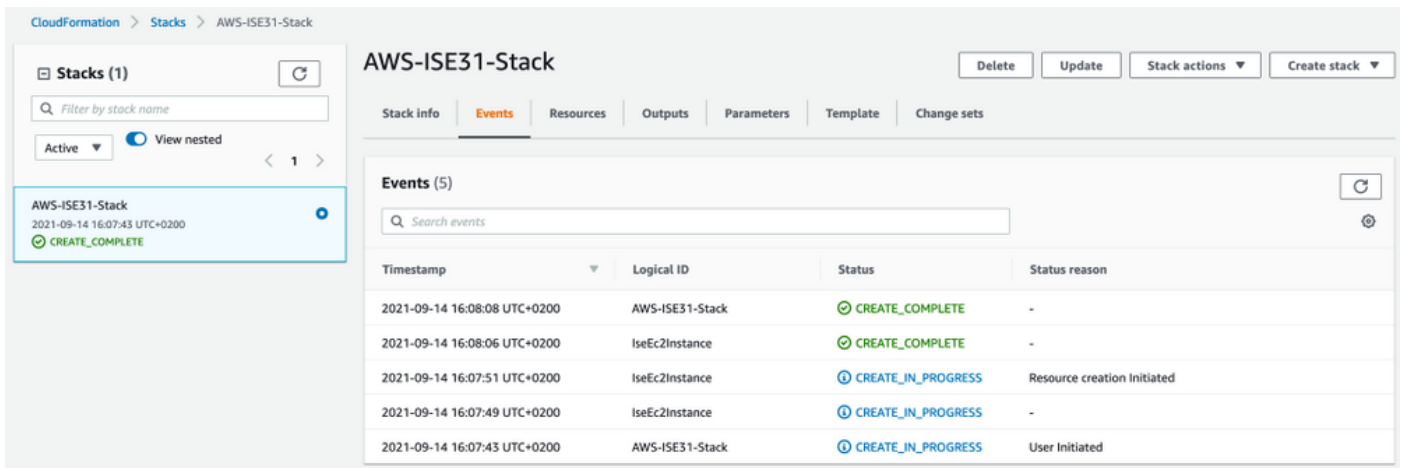
Timeout
-

Termination protection
Disabled

► Quick-create link

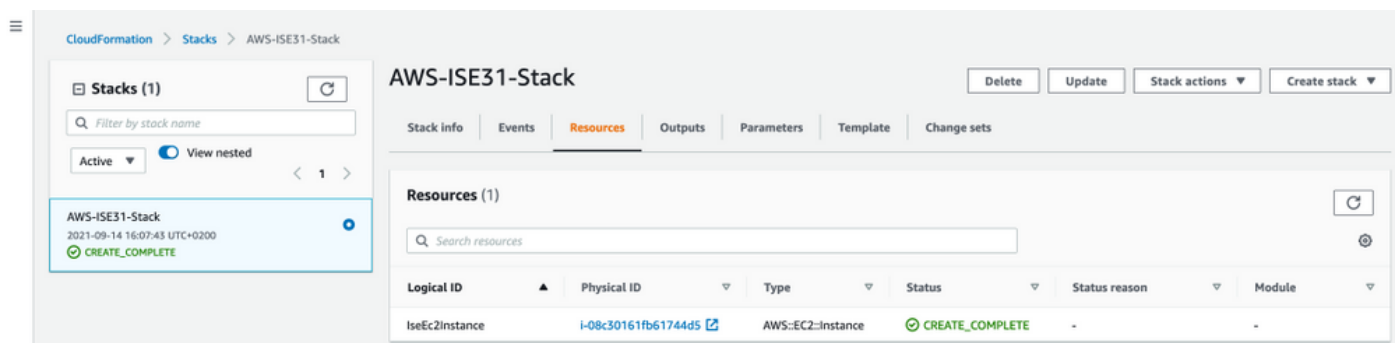
Cancel Previous Create change set **Create stack**

部署堆栈后，必须看到CREATE_COMPLETE状态。

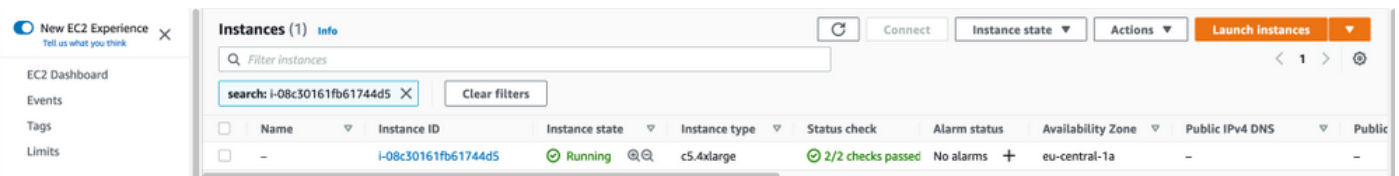


步骤5.访问AWS上的ISE

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。



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。



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：

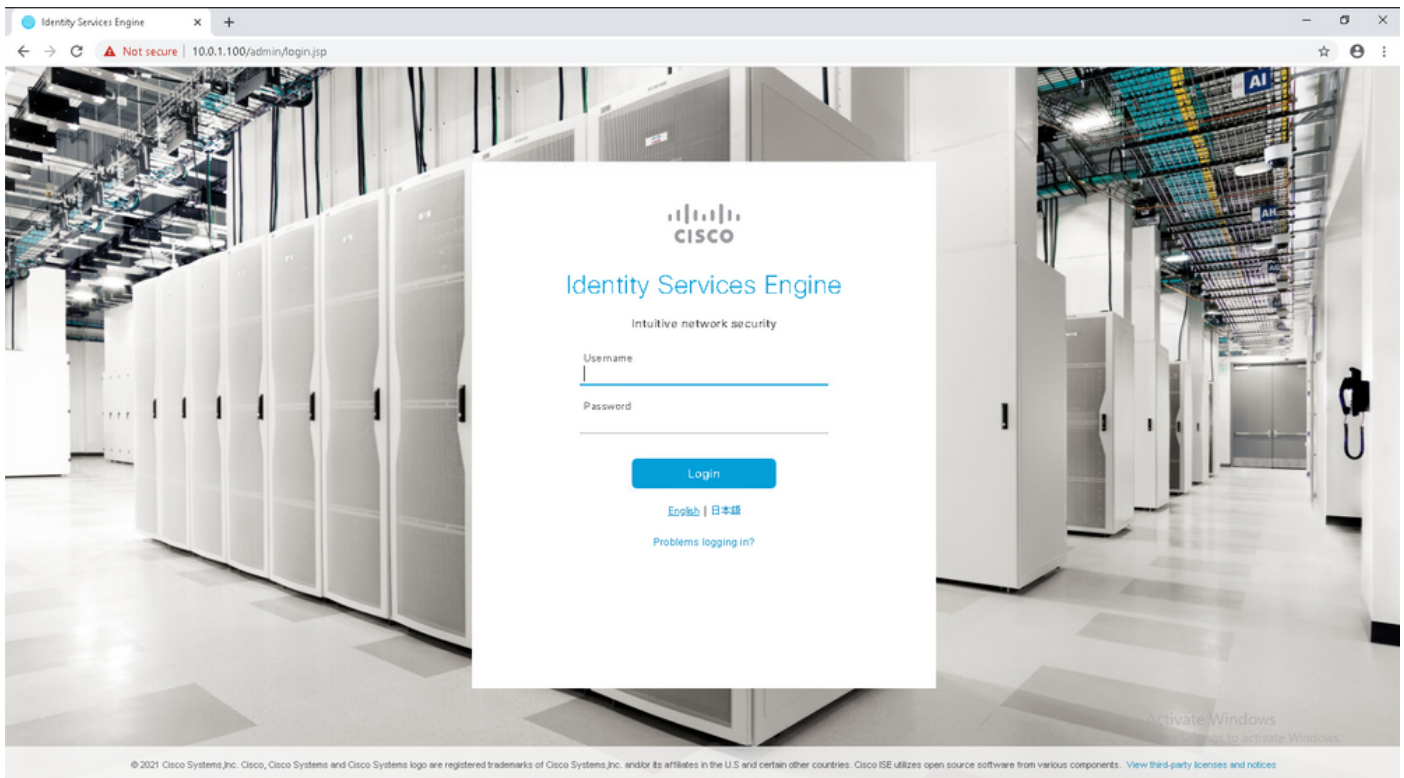
```
ISE31-2/admin# show application status ise

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#
```

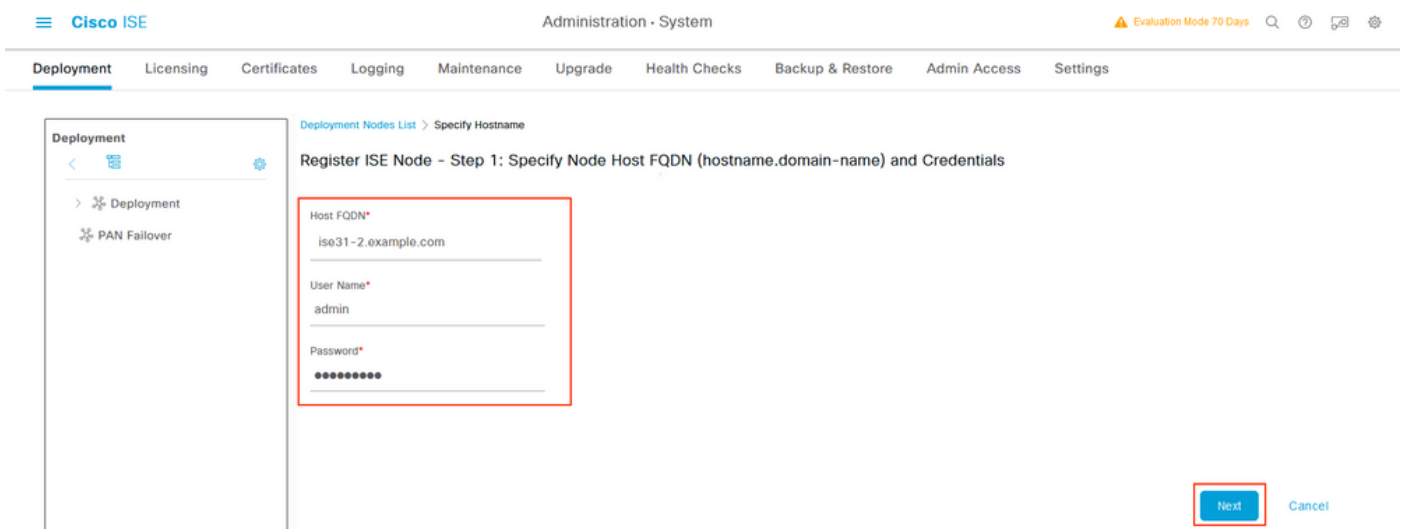
注意：由于ISE服务可使用SSH转换到运行状态，因此需要大约10-15分钟。

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。



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。



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。



Warning

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

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

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

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

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

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

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

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

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

Signature Algorithm : SHA384withRSA

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

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

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

[Cancel Registration](#)

[Import Certificate and Proceed](#)

选择您选择的角色，然后单击“提交”。

Cisco ISE Administration - System Evaluation Mode 70 Days

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

Deployment Nodes List > Configure Node

Register ISE Node - Step 2: Configure Node

General Settings

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

Role SECONDARY

Administration
 > Monitoring
 > Policy Service
 > pxGrid

Cancel

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。

Cisco ISE Administration - System Evaluation Mode 70 Days

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

Deployment Nodes

Selected 0 Total 2

Edit Register Syncup Deregister











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

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

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

Active Directory











 Edit **+ Add**  Delete  Node View  Advanced Tools  Scope Mode **Join Point Name** ^ **Active Directory Domain**

No data available

配置联合点名称和Active Directory域，选择提交。

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

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

Connection

* Join Point Name	EXAMPLE	
* Active Directory Domain	example.com	

Submit Cancel

要将两个节点与Active Directory集成，请选择是。



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。



Join Operation Status

Status Summary: Successful

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

Close

限制

有关AWS上的ISE限制，请参阅《ISE管理指南》的“已知限制”部分。

验证

使用本部分可确认配置能否正常运行。

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。

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are several summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (1), and Repeat Counter (0). Below these cards is a table of RADIUS records. The table has columns for Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Profile, Authentication Poli..., Authorization Policy, Server, and Authc. The 'Server' column is highlighted with a red box, showing values like 'ISE31-2' and 'ise31'. The 'Authc' column shows '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。

The screenshot shows the AWS CloudFormation console for a stack named 'ISE31-AWS'. The 'Events' tab is selected, showing a list of events. One event is highlighted with a red box, indicating a failure. The event details are as follows:

Timestamp	Logical ID	Status	Status reason
2021-09-17 12:57:19 UTC+0200	ISE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [beta2Instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	Isse2Instance	CREATE_FAILED	Security group sg-0e54161c84262f4e5 and subnet subnet-0f9ebc3ae6258143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: bb7a9773-fbe9-45c8-8664-8c40895a8444; Proxy: null)
2021-09-17 12:57:17 UTC+0200	Isse2Instance	CREATE_IN_PROGRESS	-
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。有关要打开的必需端口，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
!
!
aaa group server radius ISE-Group
server name ISE31-2
server name ISE31-1
!
aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group
!
aaa server radius dynamic-author
client 172.18.5.100 server-key cisco
client 10.0.1.100 server-key cisco
!
aaa session-id common
!
dot1x system-auth-control
!
vlan 1805
!
interface GigabitEthernet1/0/2
description VMWIN10
switchport access vlan 1805
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
!
interface Vlan1805
ip address 172.18.5.3 255.255.255.0
!
!
radius server ISE31-1
address ipv4 172.18.5.100 auth-port 1645 acct-port 1646
key cisco
!
radius server ISE31-2
address ipv4 10.0.1.100 auth-port 1645 acct-port 1646
key cisco
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。