通过AWS Marketplace配置ISE 3.1

目录

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：
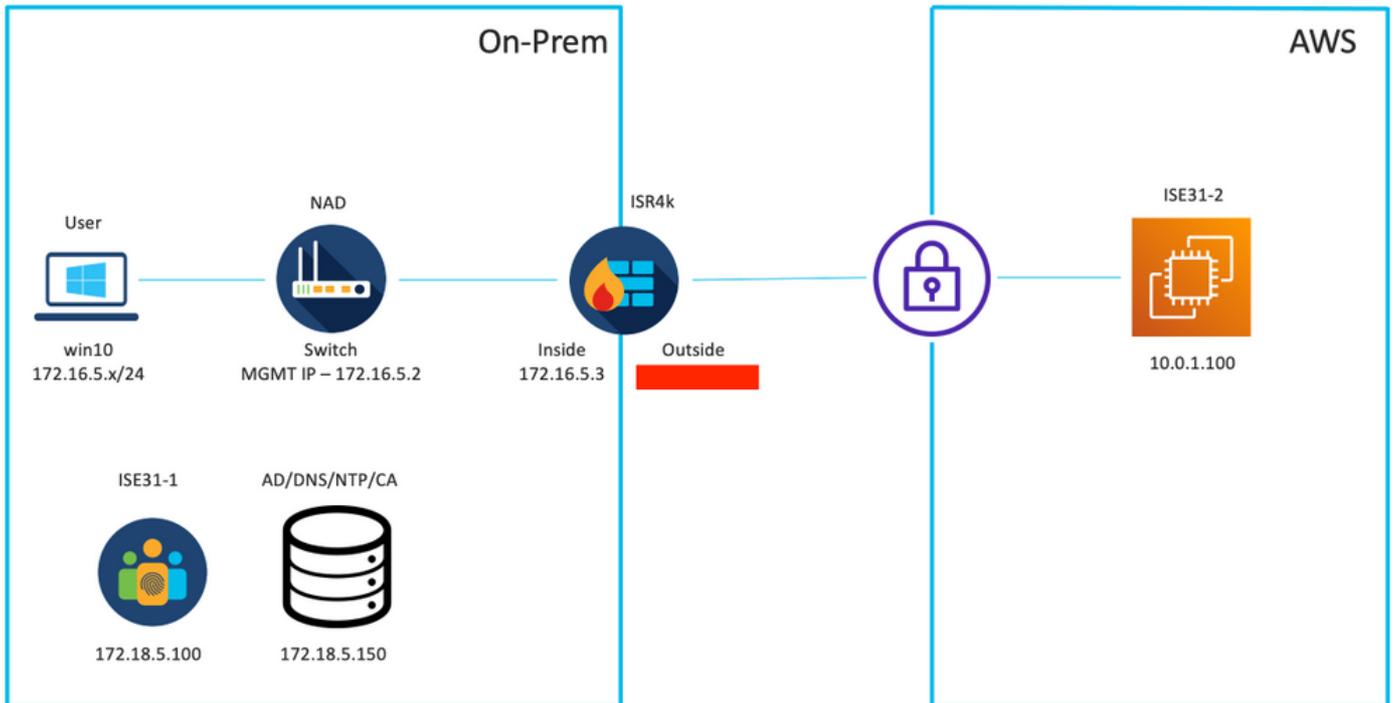
- ISE
- AWS及其概念，如VPC、EC2、CloudFormation

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。
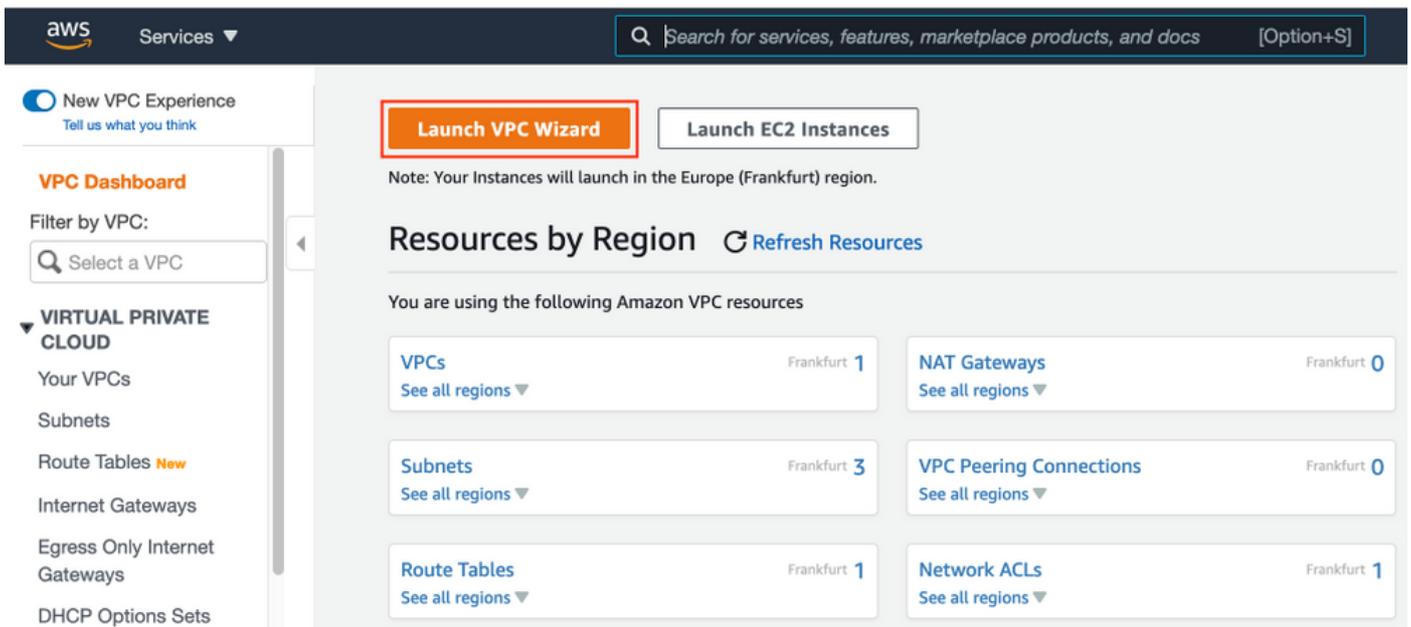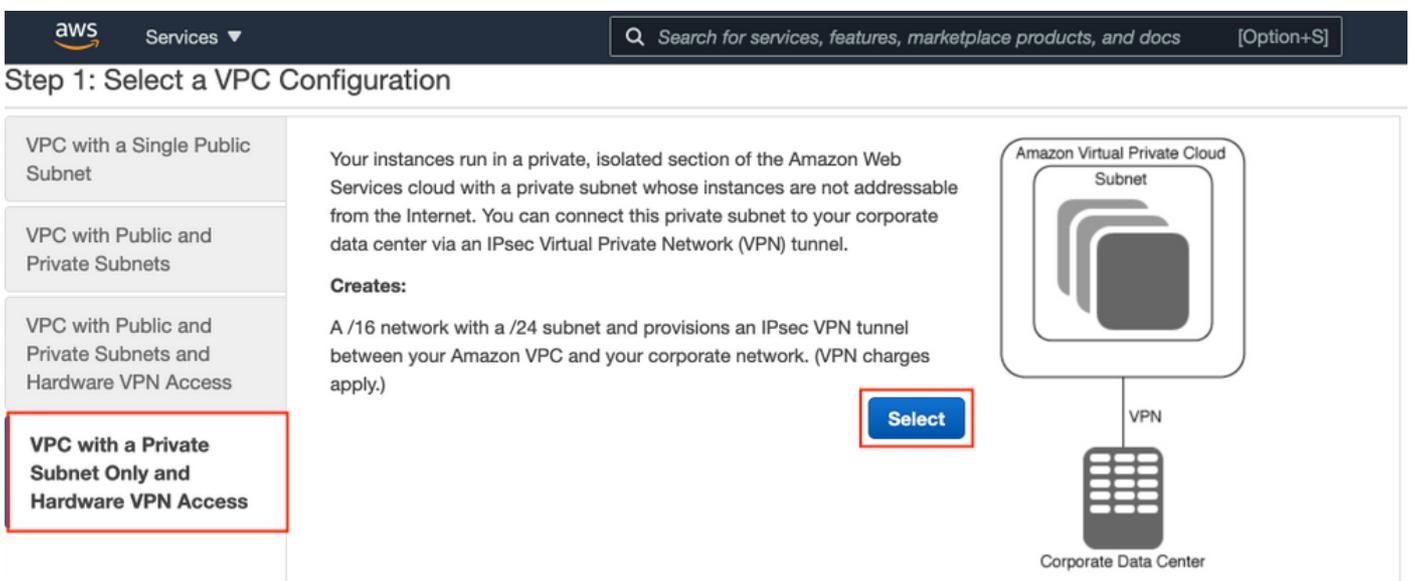
配置

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。
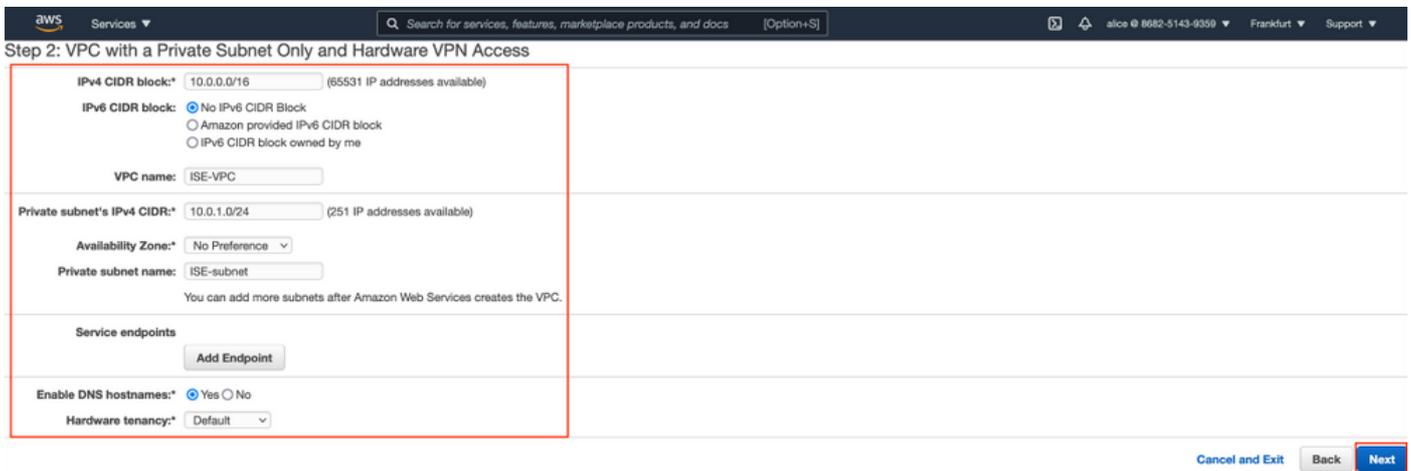
可选步骤A.创建VPC

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。
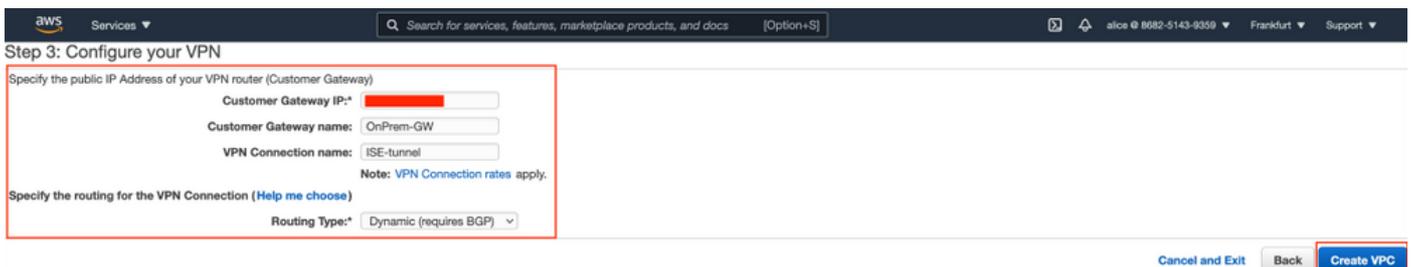

注意：VPC向导步骤1.中VPC的选择取决于拓扑，因为ISE不设计为Internet外露服务器 — 仅使用带私有子网的VPN。

根据您的网络设计配置VPC专用子网设置并选择下一步。
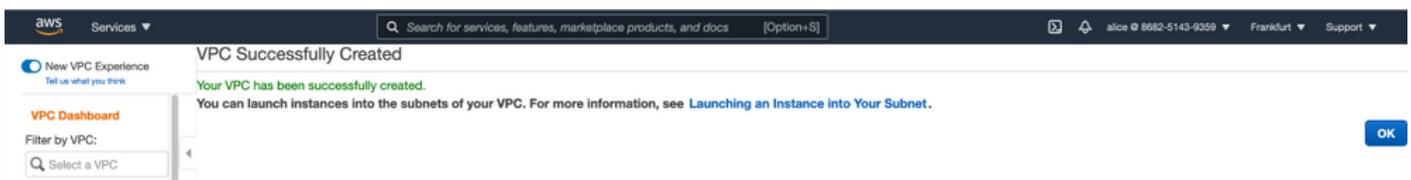
根据网络设计配置VPN，然后选择"创建VPC"。

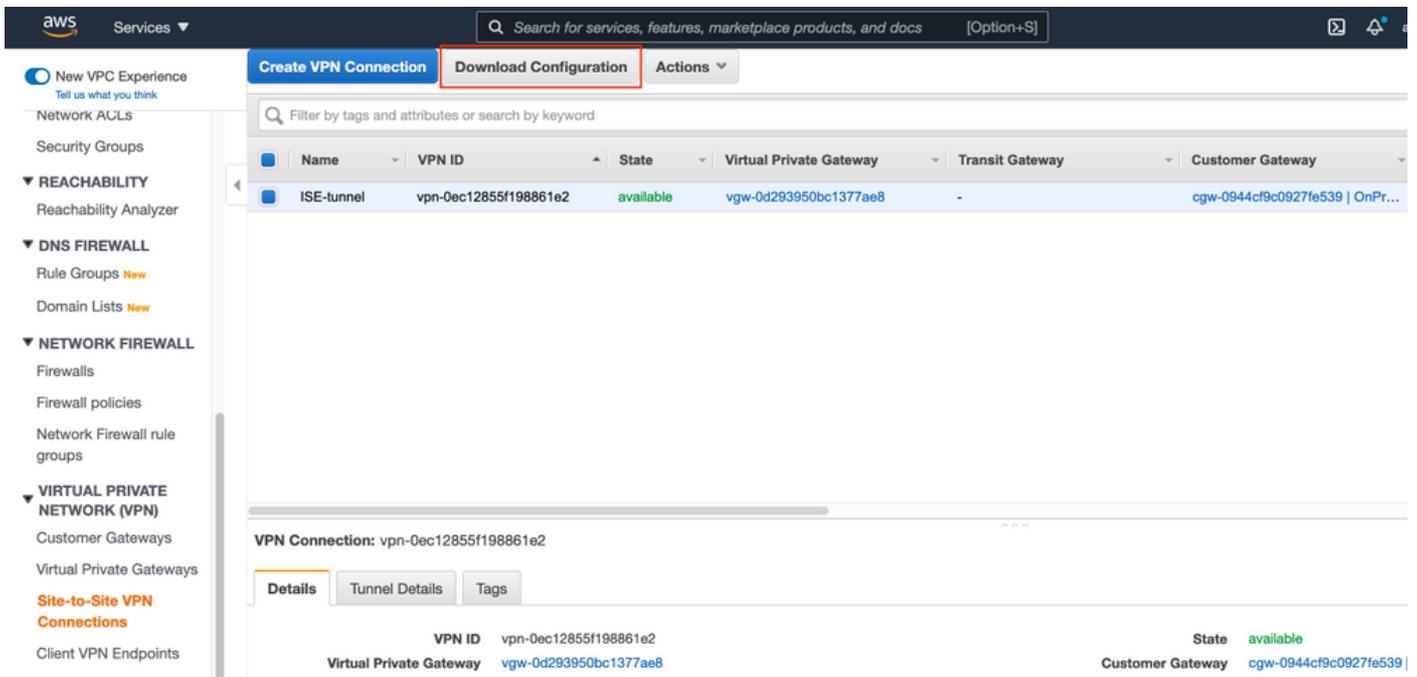创建VPC后，将显示"**Your VPC has been successfully created**"(您的VPC已成功创建)消息。单击**OK(确**定)，如图所示。

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。

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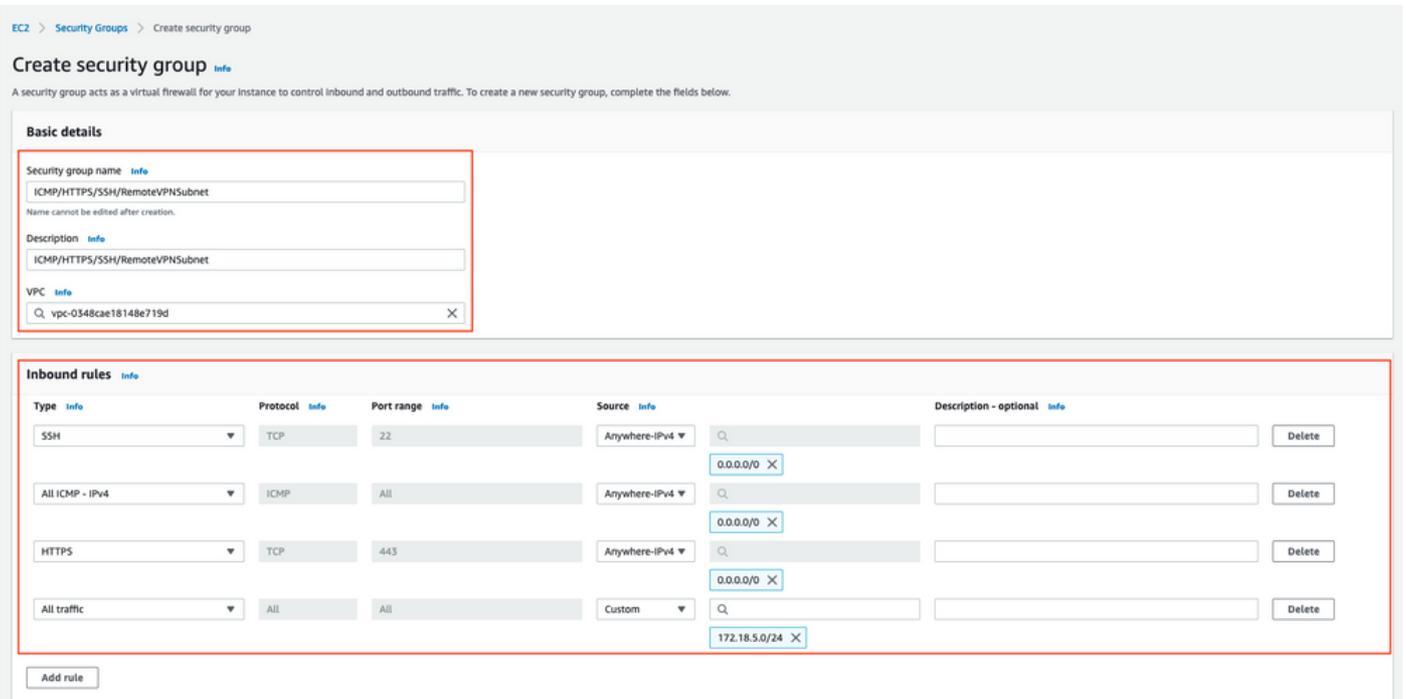
注意：配置的安全组允许SSH、ICMP、HTTPS访问ISE，以及从内部子网访问所有协议。

步骤1.订用AWS ISE市场产品

导航至AWS Marketplace Subscriptions AWS Service。选择Discover Products，如图所示。
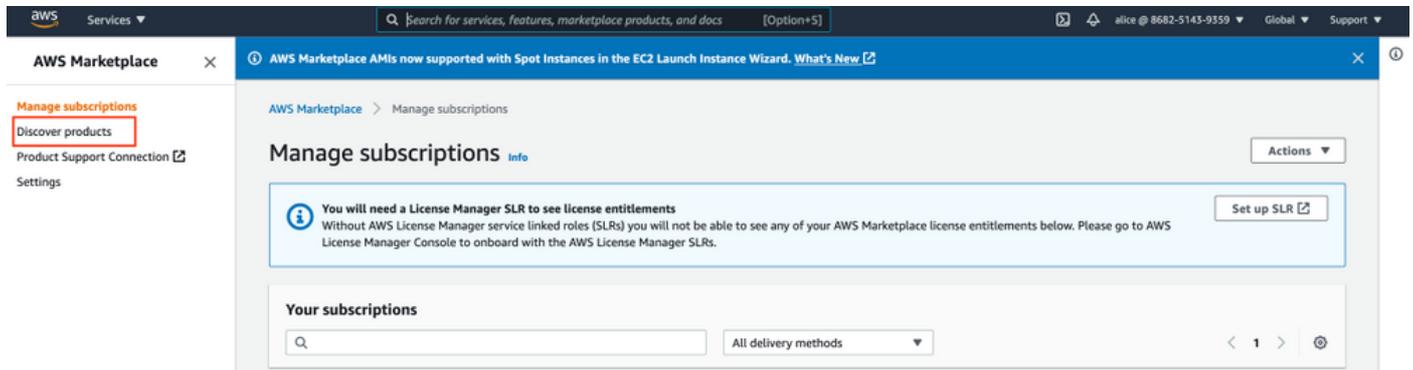
搜索ISE产品并选择**思科身份服务引擎**(ISE)，如图所示。

选择"**继续订阅**"按钮

选择**接受**术语按钮，如图所示。

订用有效和到期**日期**后，**更改**为**待定**，如图所示。

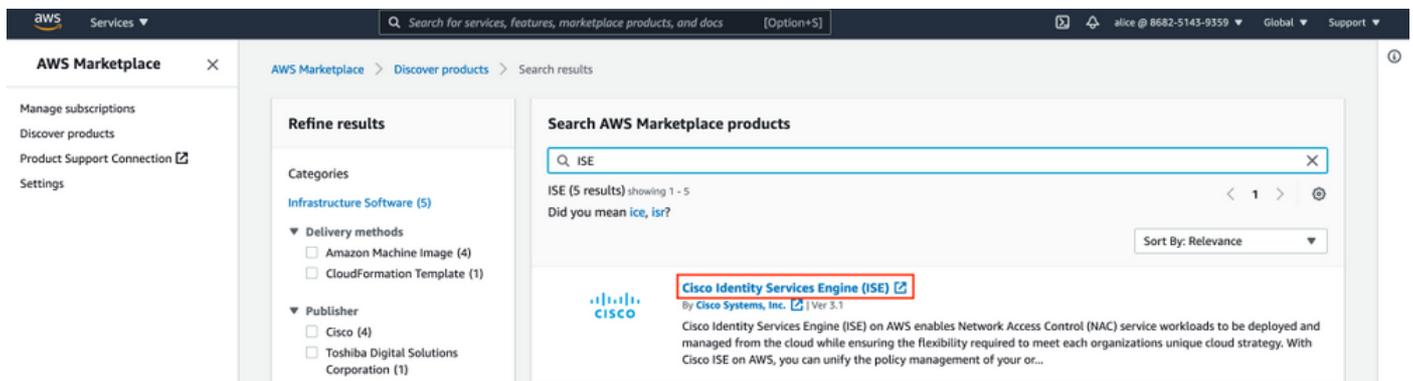Thank you for subscribing to this product! We are processing your request.   X

< 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

altaltı CISCO   **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。**

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"。

（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**"。
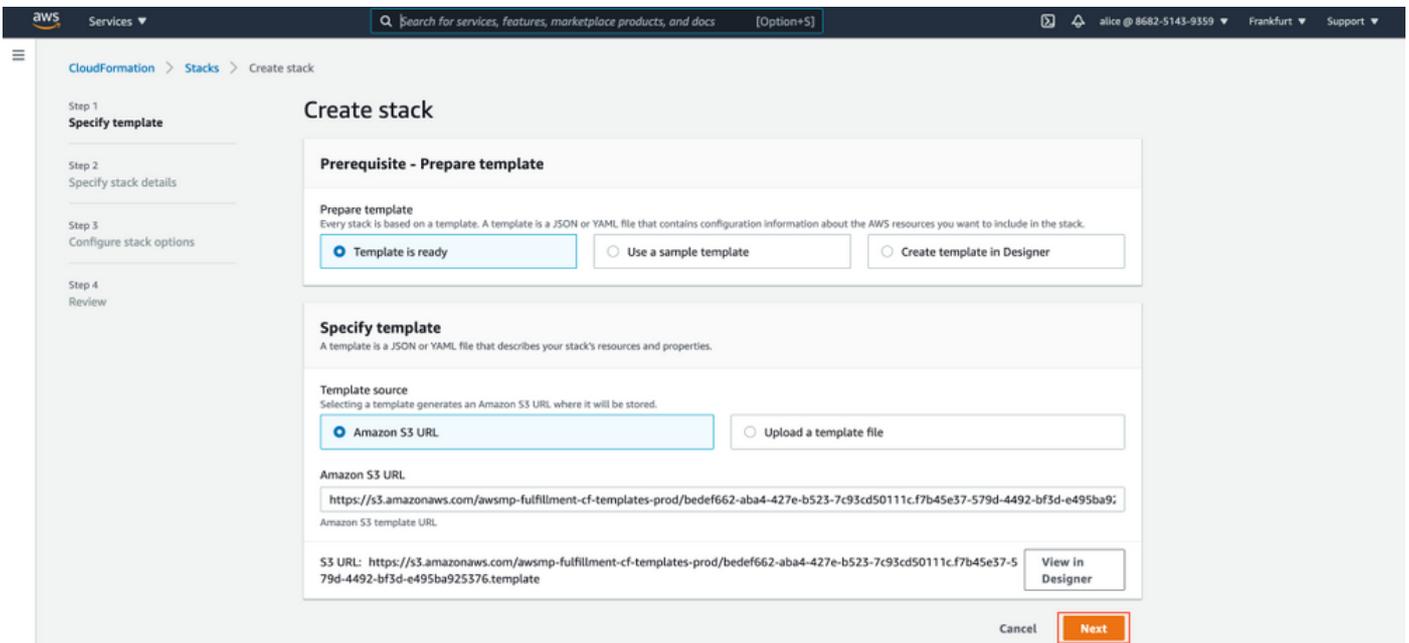
使用堆栈名称填充CloudFormation**堆栈数据**。配置实例详细信息(**如主机名**)，选择实**例密钥对**和管**理安全组**。
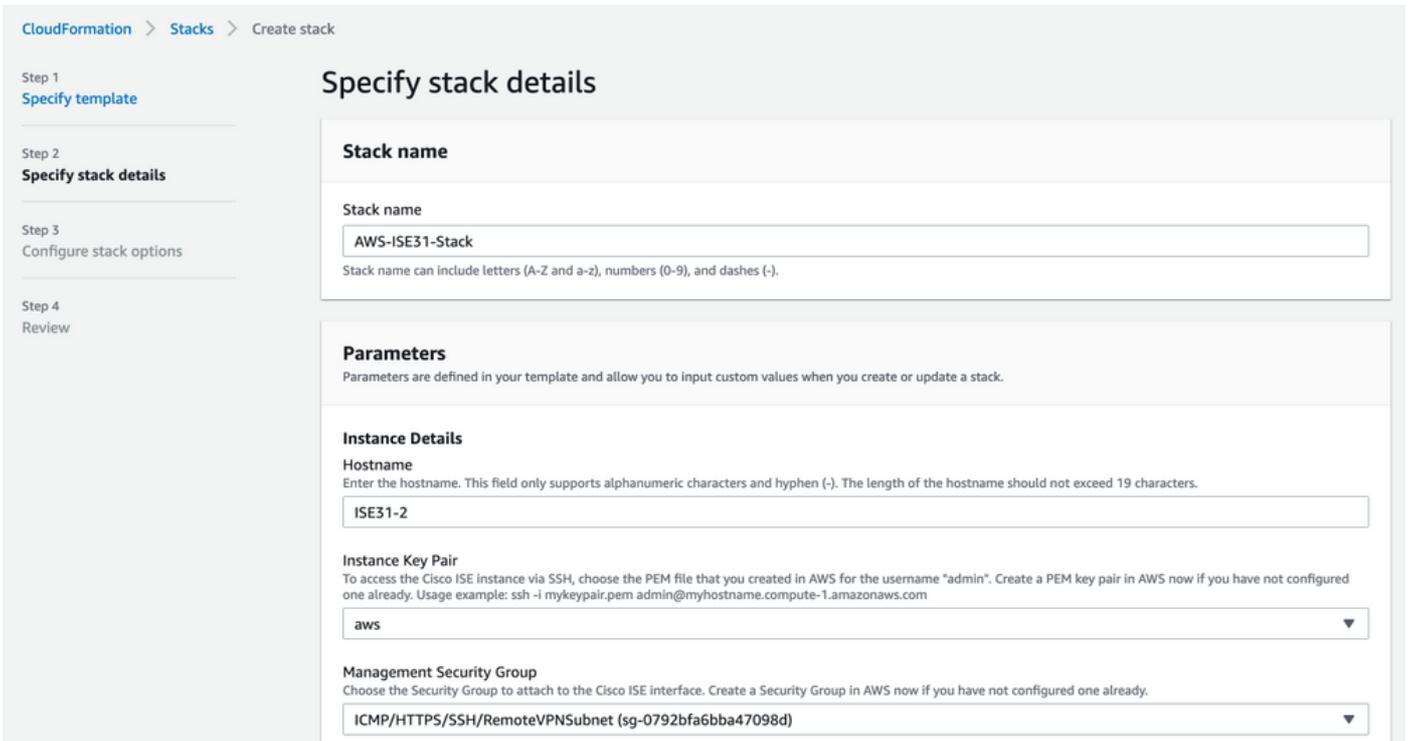
使用Management Network、Management Private IP、Time Zone、Instance Type、**EBS Encryption**和**Volume Size继续配置Instance** Details。

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-0fbebcdae62a58143 (10.0.1.0/24) (ISE-subnet)   ▼

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

10.0.1.100

Time Zone
Choose a system time zone.

Etc/UTC   ▼

Instance Type
Choose the required Cisco ISE instance type.

c5.4xlarge   ▼

EBS Encryption
Choose true to enable EBS encryption.

true   ▼

Volume Size
Specify the storage in GB (Minimum 300GB and Maximum 2400GB). 600GB is recommended for production use, storage lesser than 600GB can be used for 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"。

下一屏幕无需更改。选择 Next（下一步）。

转到"查看**堆栈**"屏幕，向下滚动并选择"创**建堆栈**"。

部署堆栈后，必**须看到**CREATE_COMPLETE状态。
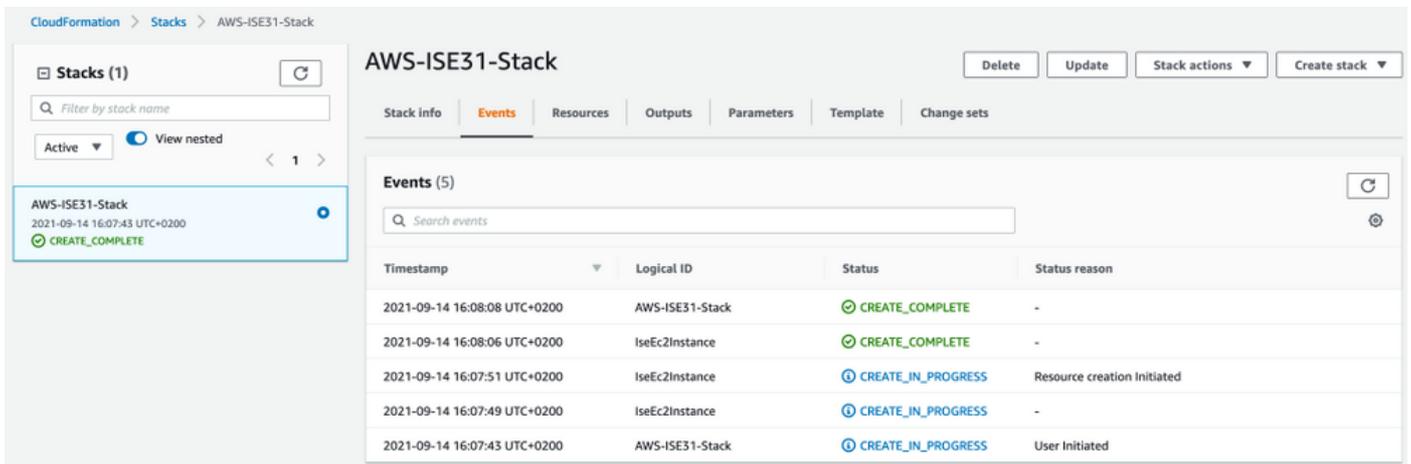
步骤5.访问AWS上的ISE

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。
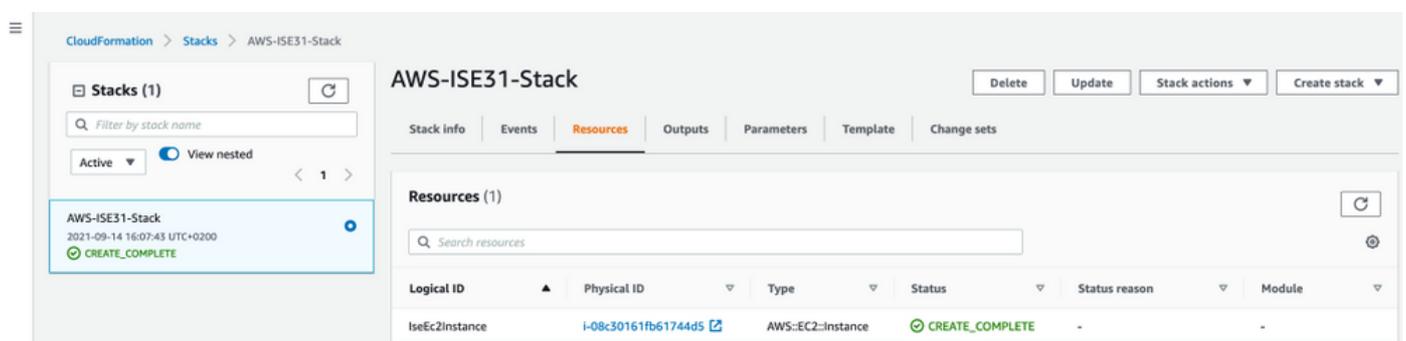
选择**物理ID**以打开"**EC2实例**"菜单。确保状**态检查**已**通过2/2的**检查。
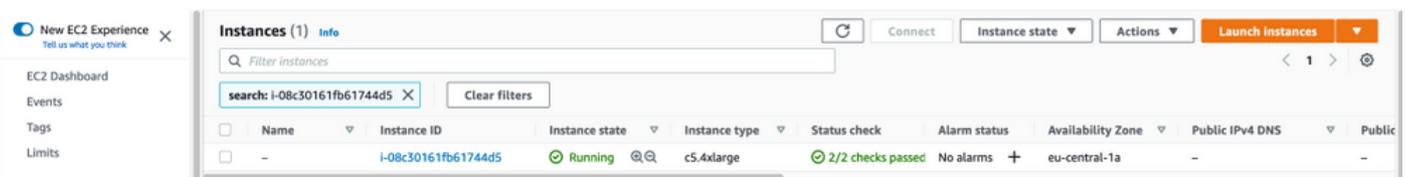
选择**实例ID**。ISE可以通过SSH**或HTTPS协议**通过**私有IPv4地**址/私有IPv4 DNS。

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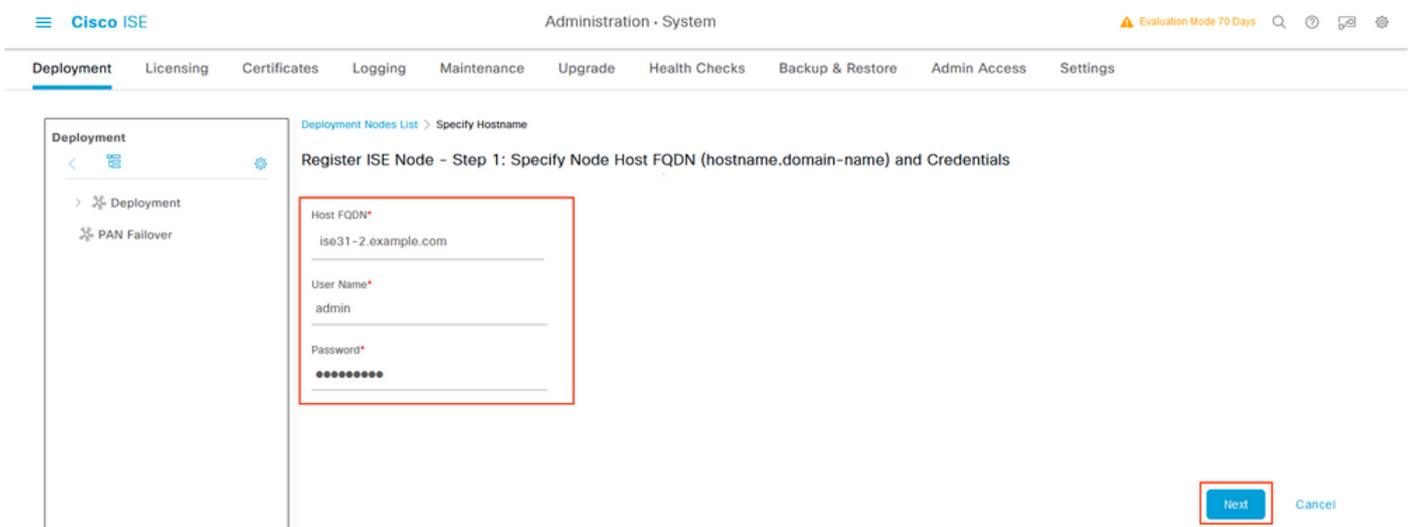
注意：由于ISE服务可使用SSH转换到运行状态，因此需要大约10-15分钟。

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。
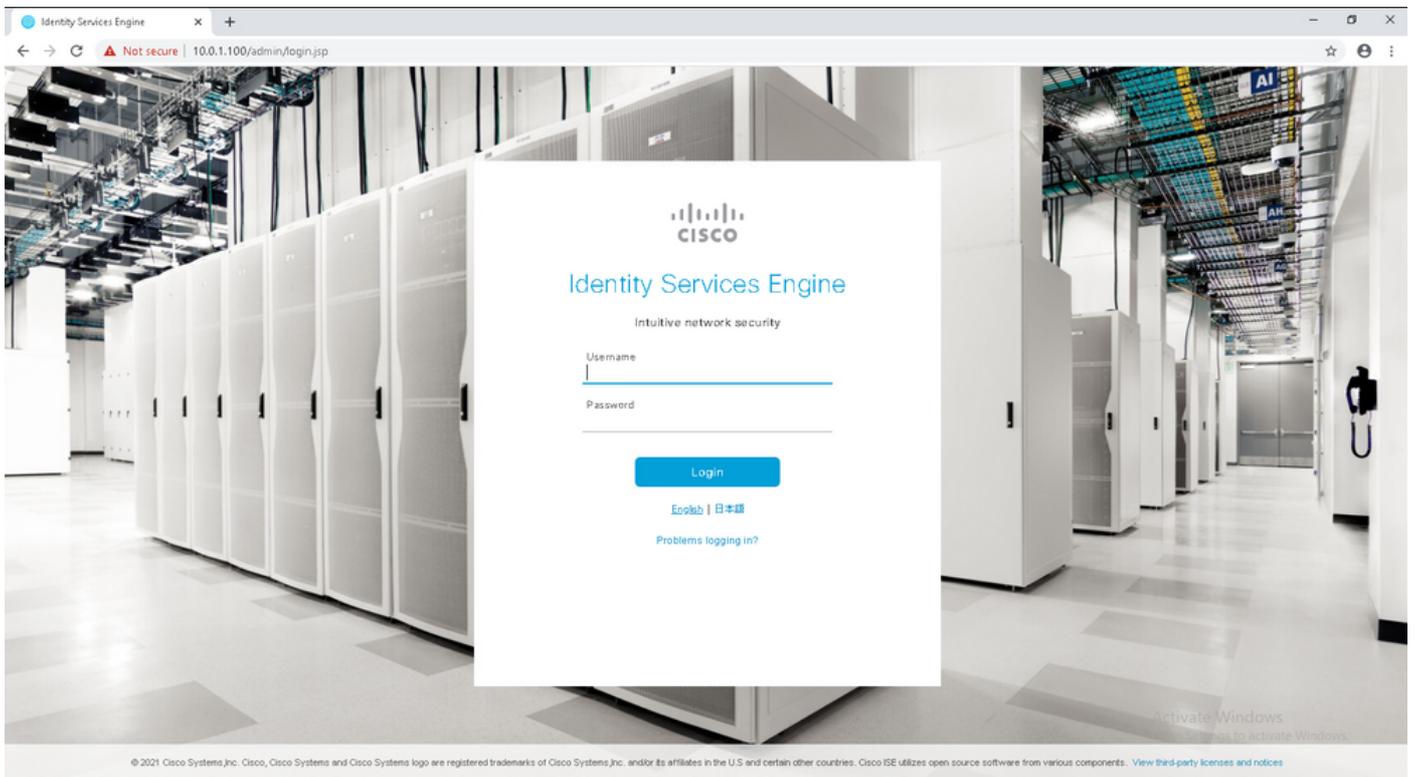
步骤6.在AWS上配置内部ISE和ISE之间的分布式部署

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"。

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。

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**。

配置**联合点名**称**和Active Directory域**，选择**提交**。

要将两个节点与Active Directory集成，请选择**是**。

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。

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。

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。

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
!
!
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
```