

# 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](#)

[可選步驟C.建立自定義金鑰對](#)

[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

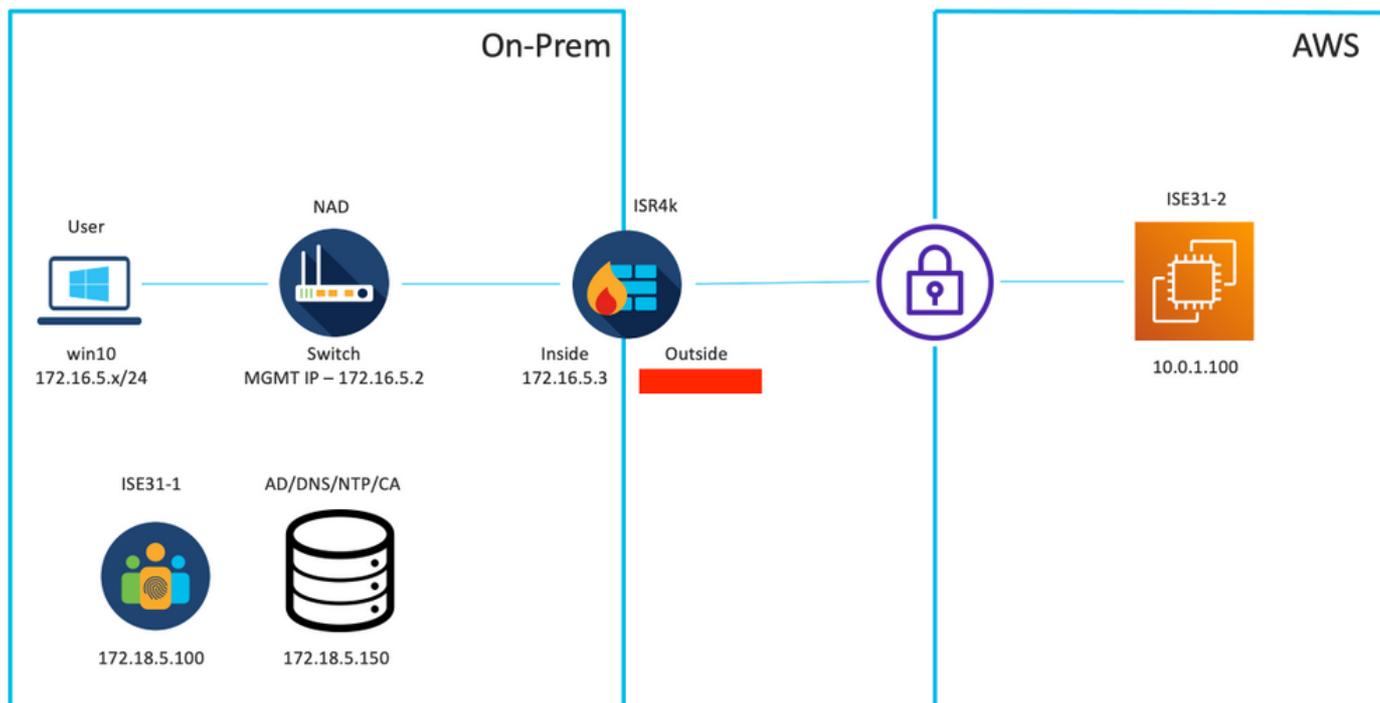
## 採用元件

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。

The screenshot shows the AWS Management Console interface. At the top, there is a search bar and a navigation menu. The main content area is titled 'Launch VPC Wizard' and 'Launch EC2 Instances'. A note indicates that instances will launch in the Europe (Frankfurt) region. Below this, there is a section for 'Resources by Region' with a 'Refresh Resources' button. The resources listed are:

- VPCs: Frankfurt 1
- NAT Gateways: Frankfurt 0
- Subnets: Frankfurt 3
- VPC Peering Connections: Frankfurt 0
- Route Tables: Frankfurt 1
- Network ACLs: Frankfurt 1

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

The screenshot shows the 'Step 1: Select a VPC Configuration' screen. On the left, there are four VPC configuration options:

- VPC with a Single Public Subnet
- VPC with Public and Private Subnets
- VPC with Public and Private Subnets and Hardware VPN Access
- VPC with a Private Subnet Only and Hardware VPN Access** (highlighted with a red box)

The main content area describes the selected option: "Your instances run in a private, isolated section of the Amazon Web Services cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel." It also includes a 'Creates:' section and a 'Select' button (highlighted with a red box). A diagram on the right shows an 'Amazon Virtual Private Cloud Subnet' connected to a 'Corporate Data Center' via a 'VPN' tunnel.

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。

Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block:  No IPv6 CIDR Block  
 Amazon provided IPv6 CIDR block  
 IPv6 CIDR block owned by me

VPC name: ISE-VPC

Private subnet's IPv4 CIDR: 10.0.1.0/24 (251 IP addresses available)

Availability Zone: No Preference

Private subnet name: ISE-subnet  
You can add more subnets after Amazon Web Services creates the VPC.

Service endpoints  
Add Endpoint

Enable DNS hostnames:  Yes  No

Hardware tenancy: Default

Cancel and Exit Back **Next**

根據您的網路設計配置VPN，然後選擇**Create VPC**。

Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP: [Redacted]

Customer Gateway name: OnPrem-GW

VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection ([Help me choose](#))

Routing Type: Dynamic (requires BGP)

Cancel and Exit 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。

VPC Successfully Created

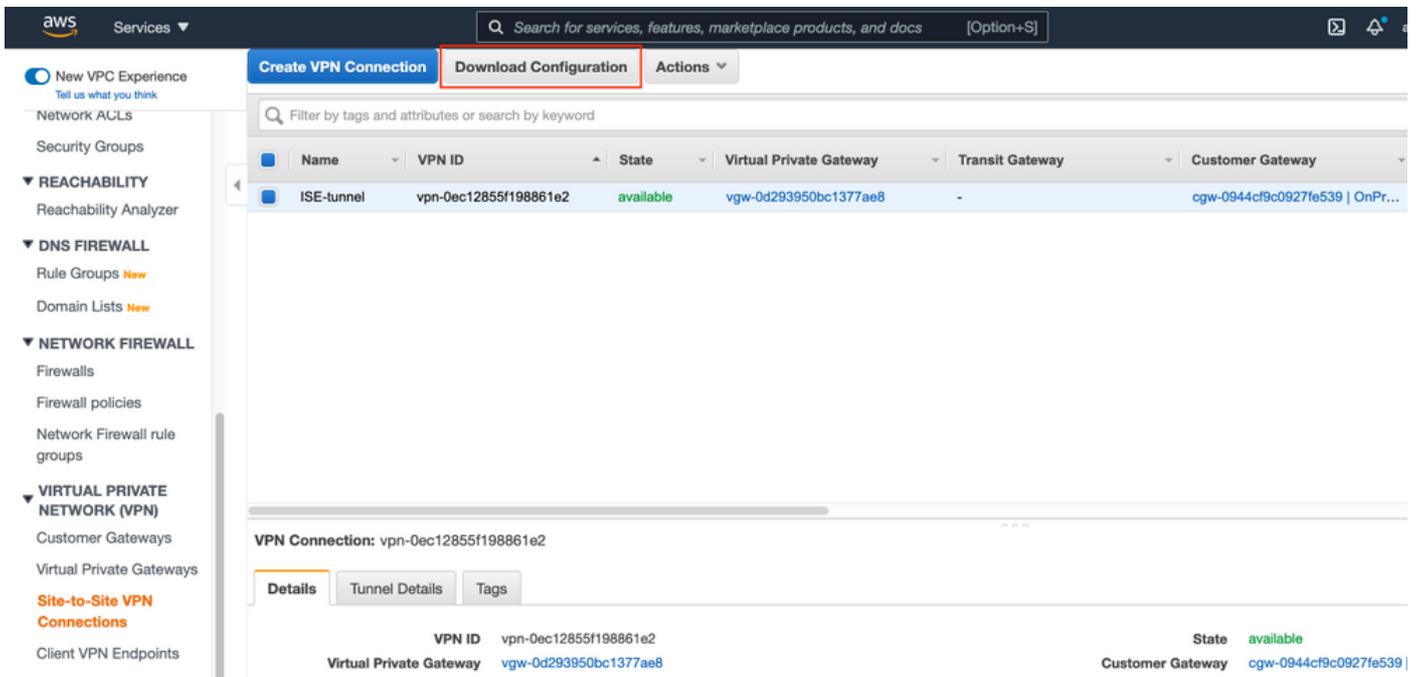
Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see [Launching an Instance into Your Subnet](#).

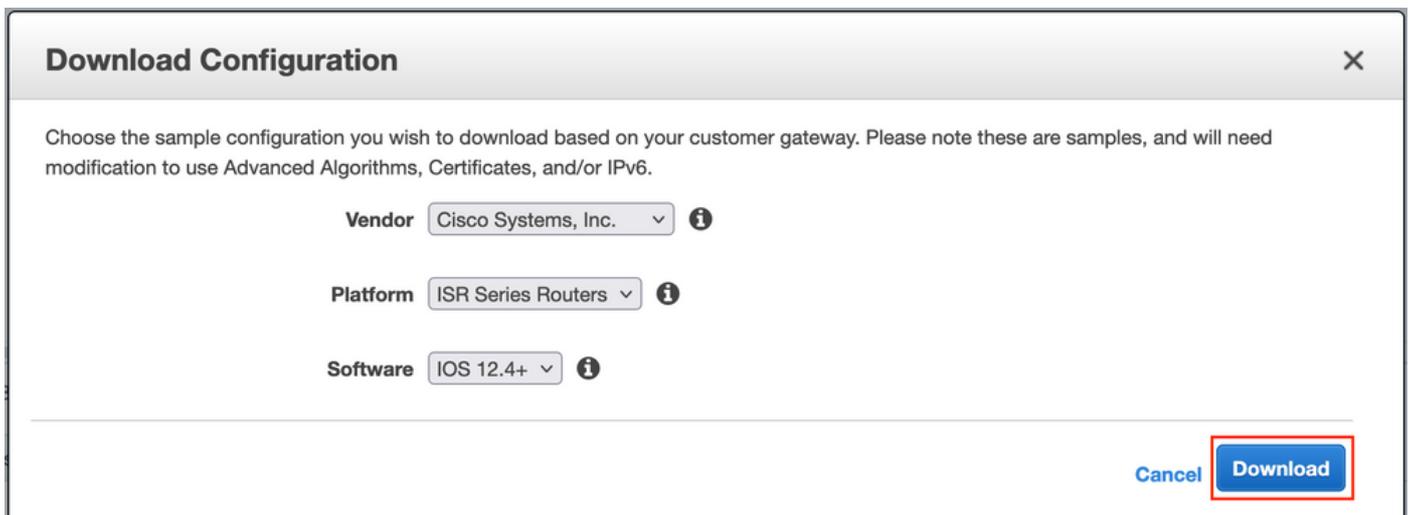
OK

## 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。



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



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

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

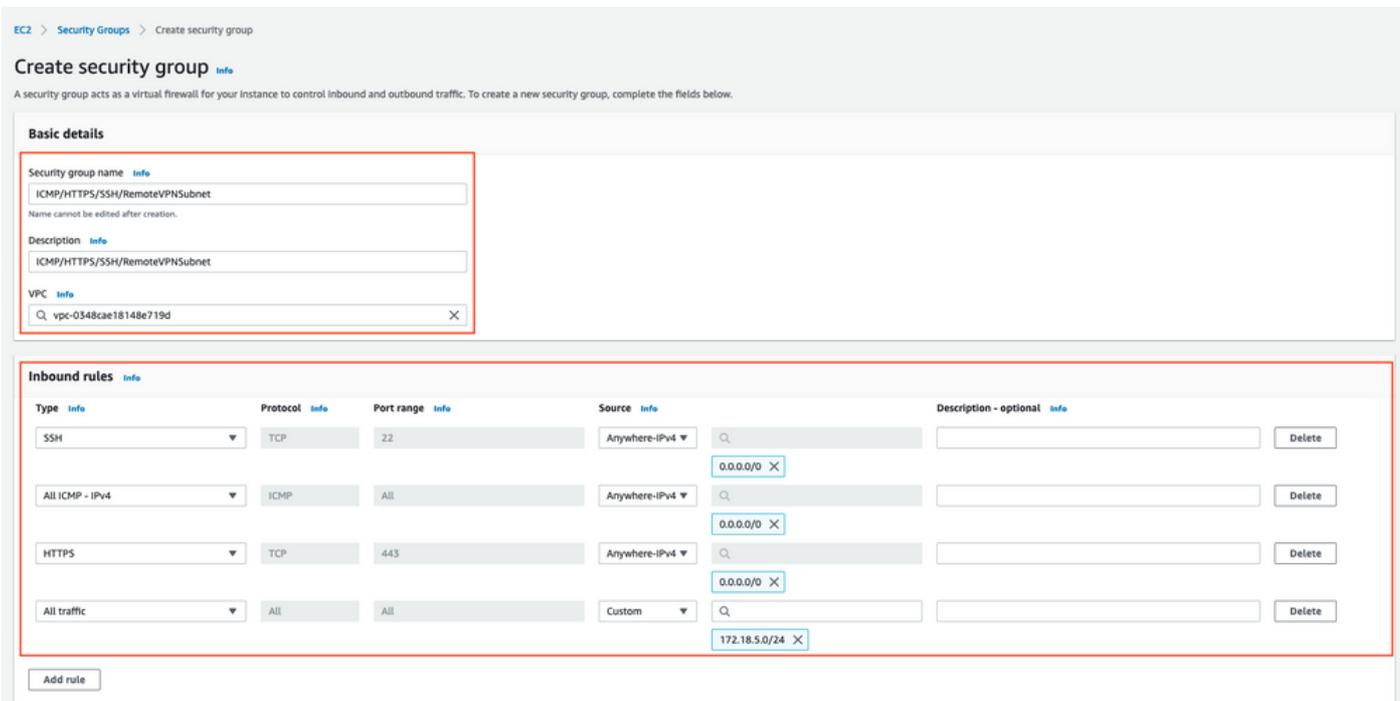
#### Tags (Optional)

No tags associated with the resource.

You can add 50 more tags.

### 可選步驟D.建立自定義安全組

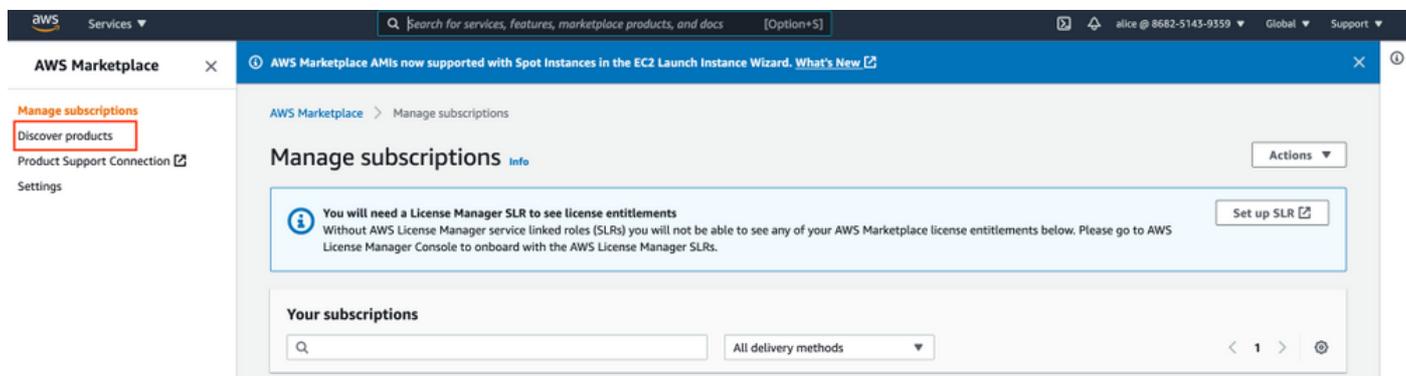
AWS EC2例項訪問受**Security Groups**保護，要配置**Security Group**，請導航到EC2 Service。在**Network & Security**下選擇**Security Groups**選單。在VPC欄位中選擇Create Security Group,配置**Name**、**Description**，然後選擇新配置的VPC。配置入站規則以允許與ISE通訊。選擇**建立安全組**，如下圖所示。



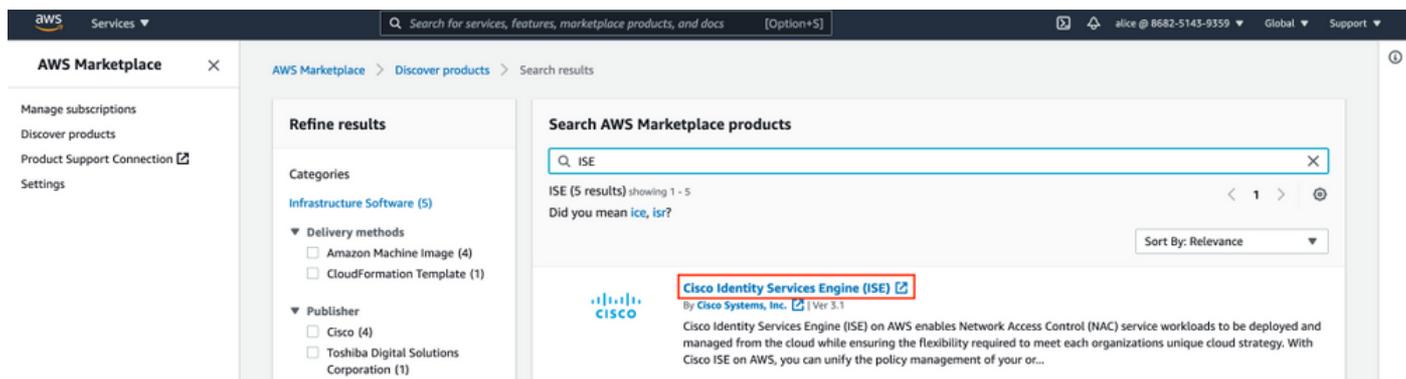
附註：配置的安全組允許通過SSH、ICMP、HTTPS訪問ISE，並且允許所有協定從內部子網訪問。

## 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。



搜尋ISE產品並選擇思科身分識別服務引擎(ISE)，如下圖所示。



選擇繼續訂閱按鈕

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 organization's 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	<a href="#">Cisco Systems, Inc.</a>
Video	<a href="#">See Product Video</a>

### 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).

選擇Accept Terms按鈕，如下圖所示。

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) <b>BYOL</b>	Additional taxes or fees may apply.
	Cisco Identity Services Engine (ISE)

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

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	<a href="#">▼ Show Details</a>

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



## 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	<a href="#">▼ Show Details</a>

## 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**

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
<b>BYOL</b>	
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) <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

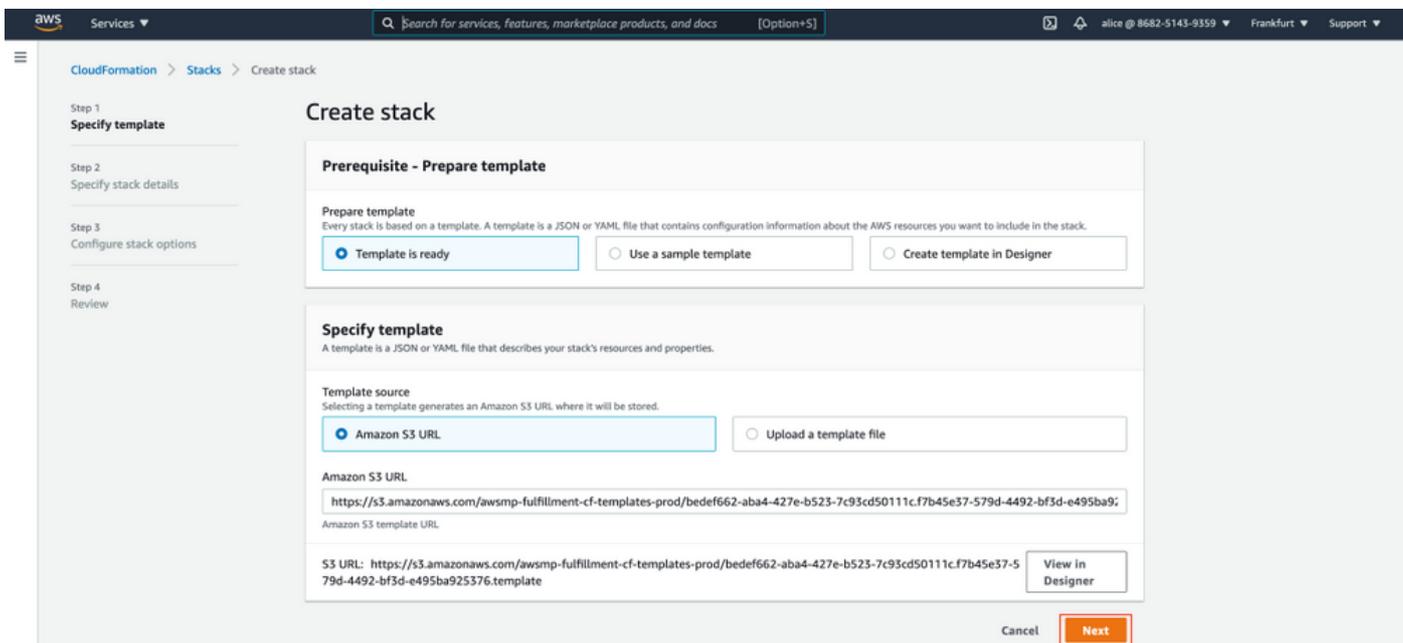
Choose this action to launch your configuration through the AWS CloudFormation console.

[Launch](#)

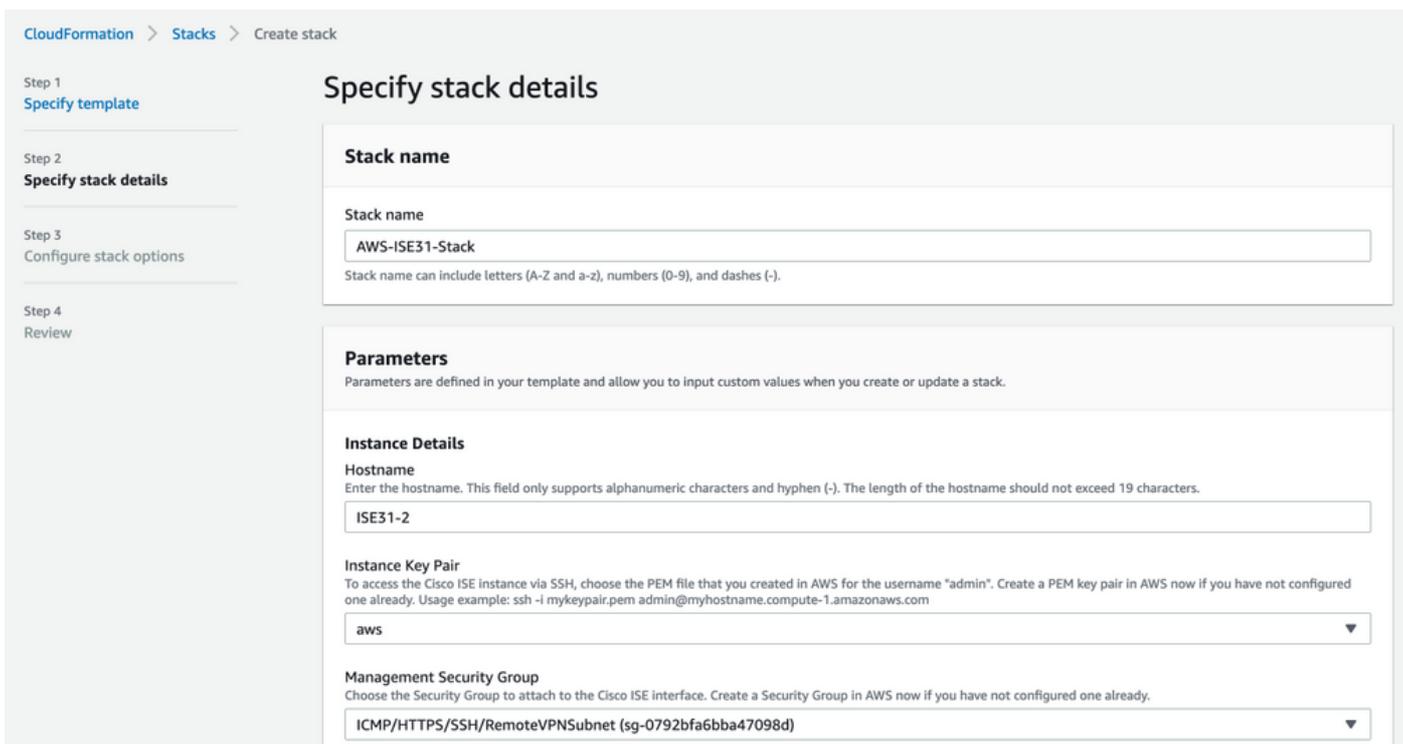
( 可選 ) 選擇**使用說明**以使自己熟悉這些說明。選擇**啟動**。

### 步驟4.在AWS上為ISE配置CloudFormation堆疊

**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**。



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。



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.

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 ↕

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 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**

下一螢幕不需要更改。選擇Next。

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

前往Review Stack視窗，向下滾動並選擇Create stack。

### Stack creation options

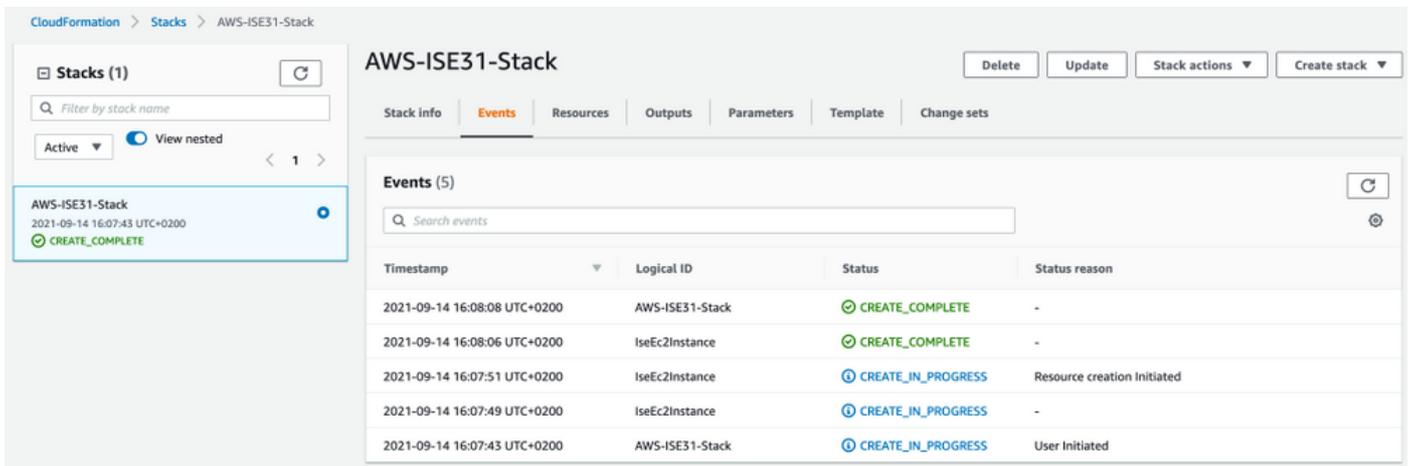
Timeout  
-

Termination protection  
Disabled

► Quick-create link

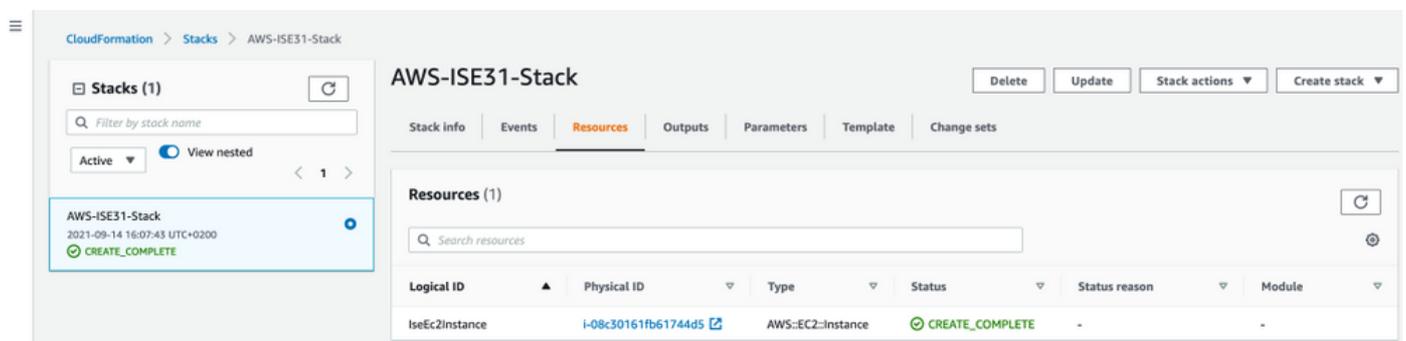
Cancel Previous Create change set **Create stack**

部署堆疊後，必須看到CREATE\_COMPLETE狀態。

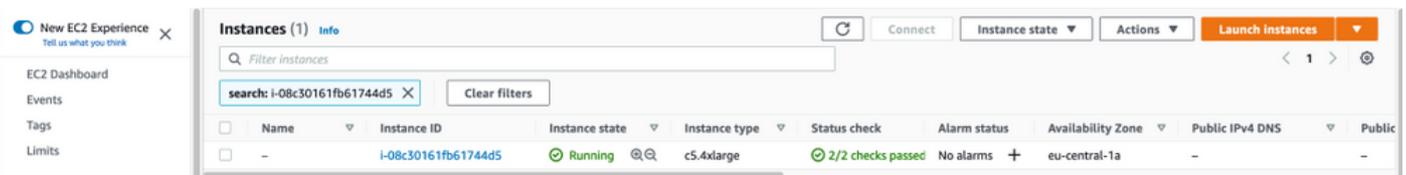


## 步驟5.訪問AWS上的ISE

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。



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。



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:G5NdGZlrgPYnjnldPcXOLcJg9VICLSxnZA0kn0CfMPs.
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：

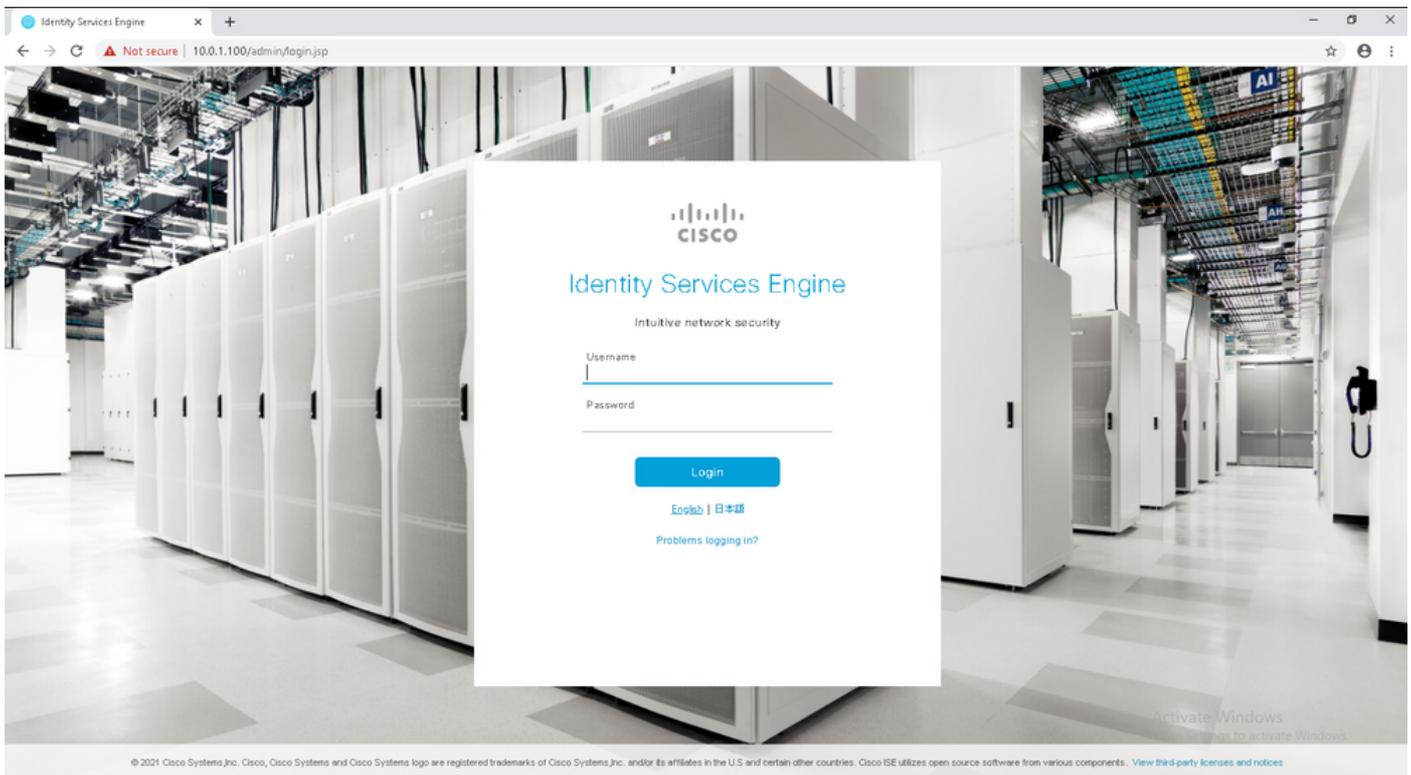
```
ISE31-2/admin# show application status ise

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#
```

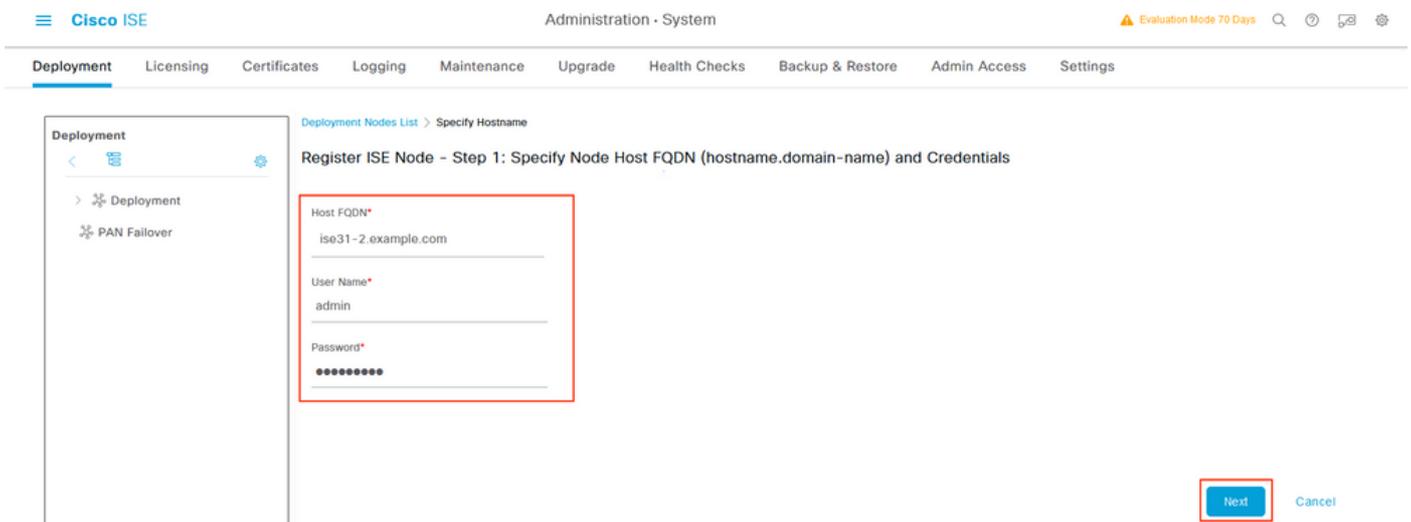
**附註：**由於SSH可用於ISE服務，需要大約10-15分鐘才能轉換到運行狀態。

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



## 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）。



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。



## 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](#)

選擇您選擇的角色，然後按一下提交。

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

同步完成後，節點將轉換到連線狀態，其上方將顯示綠色覈取方塊。

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 All

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>
<input type="checkbox"/> ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>

## 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。

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

配置聯合點名稱和Active Directory域，選擇提交。

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](#)

要將兩個節點與Active Directory整合，請選擇Yes。



# 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」。



## Join Operation Status

Status Summary: Successful

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

Close

## 限制

有關AWS上的ISE限制，請參閱ISE管理指南的[已知限制](#)部分。

## 驗證

使用本節內容，確認您的組態是否正常運作。

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。

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Authc
Sep 15, 2021 12:22:33.4...	●	🔒	0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	●	🔒		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 14, 2021 08:25:37.3...	●	🔒		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit
Sep 14, 2021 08:22:12.0...	●	🔒		alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	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堆疊建立失敗

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。

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: [ise31instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	ise31instance	CREATE_FAILED	Security group sg-0e54161c84262f4e5 and subnet subnet-0f9ebcd3ae6258143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: bb7a9773-fbe9-45c8-86d4-8c40895a8444; Proxy: null)
2021-09-17 12:57:17 UTC+0200	ise31instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:11 UTC+0200	ISE31-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[ISE埠參考](#)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
!
!
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
```