通過AWS Marketplace配置ISE 3.1

目錄

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

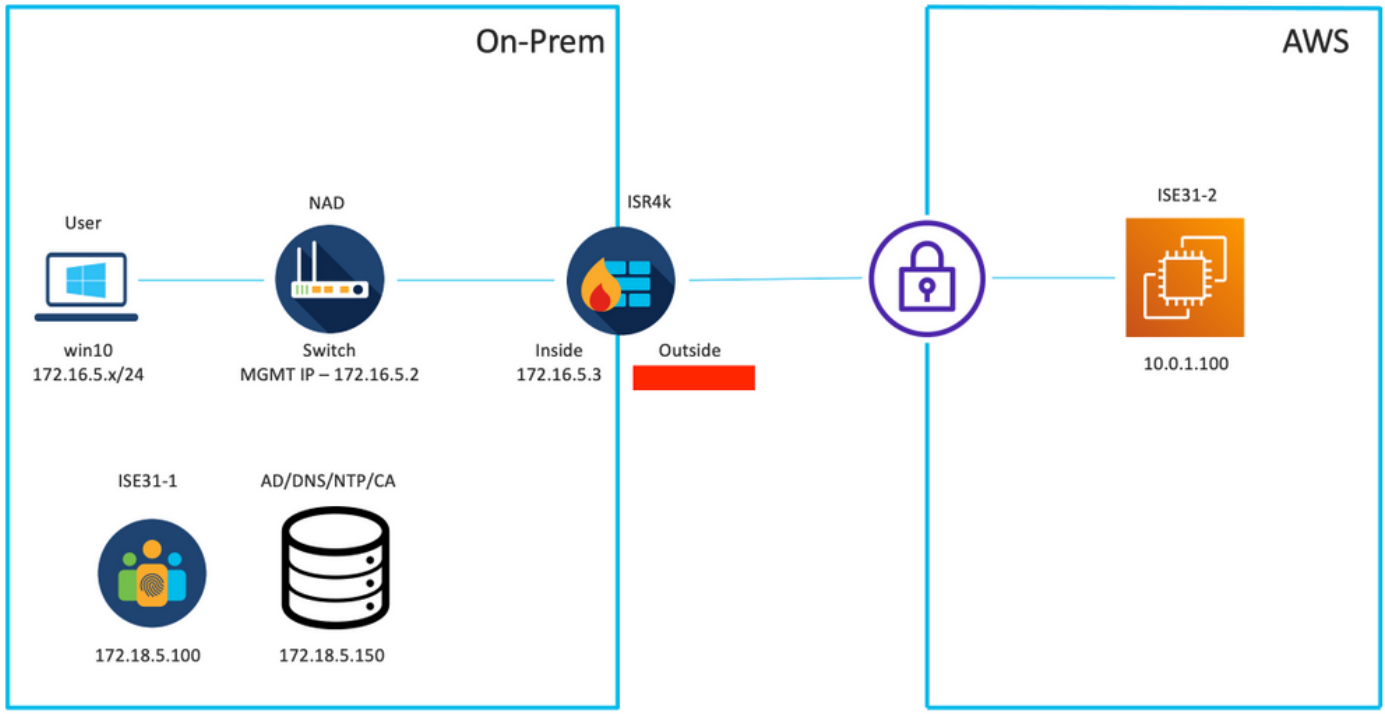
採用元件

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

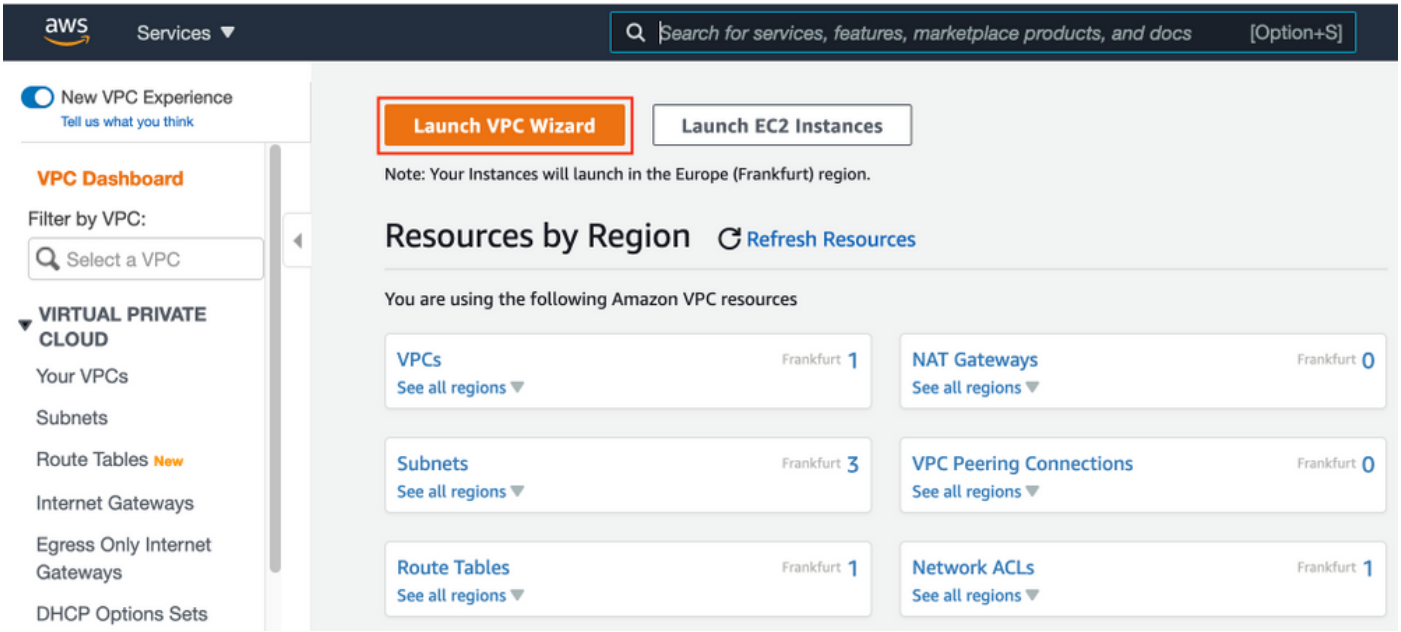


組態

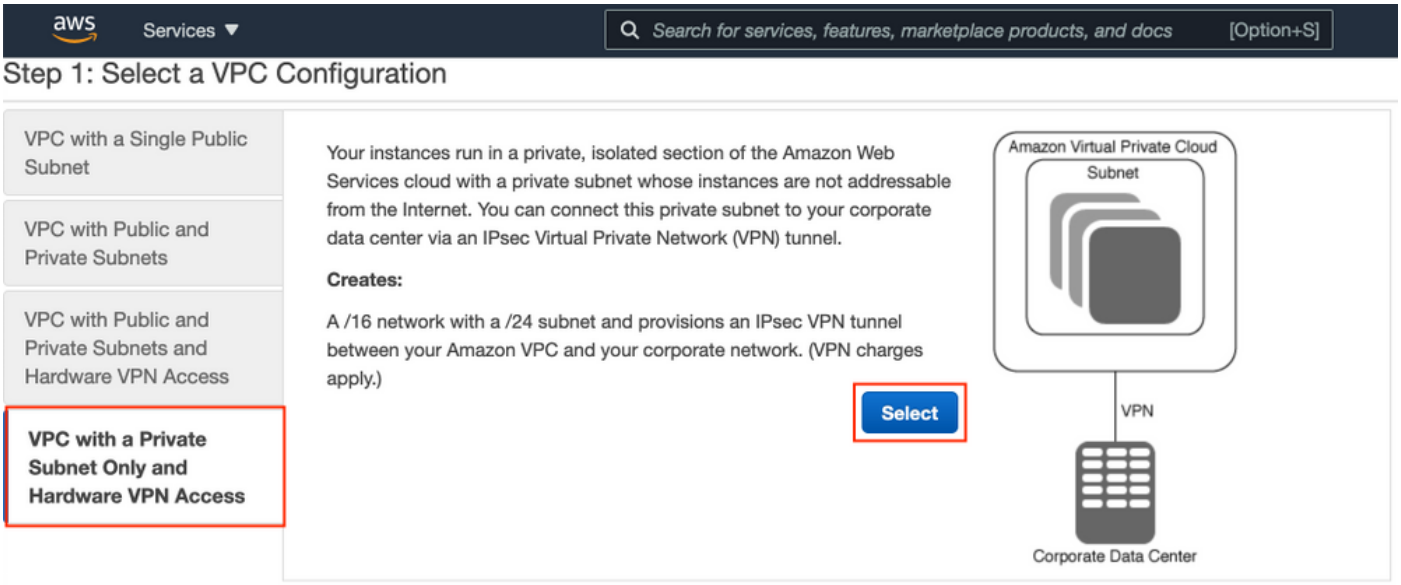
如果尚未配置VPC、安全組、金鑰對和VPN隧道，則需要執行可選步驟，否則從步驟1開始。

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。

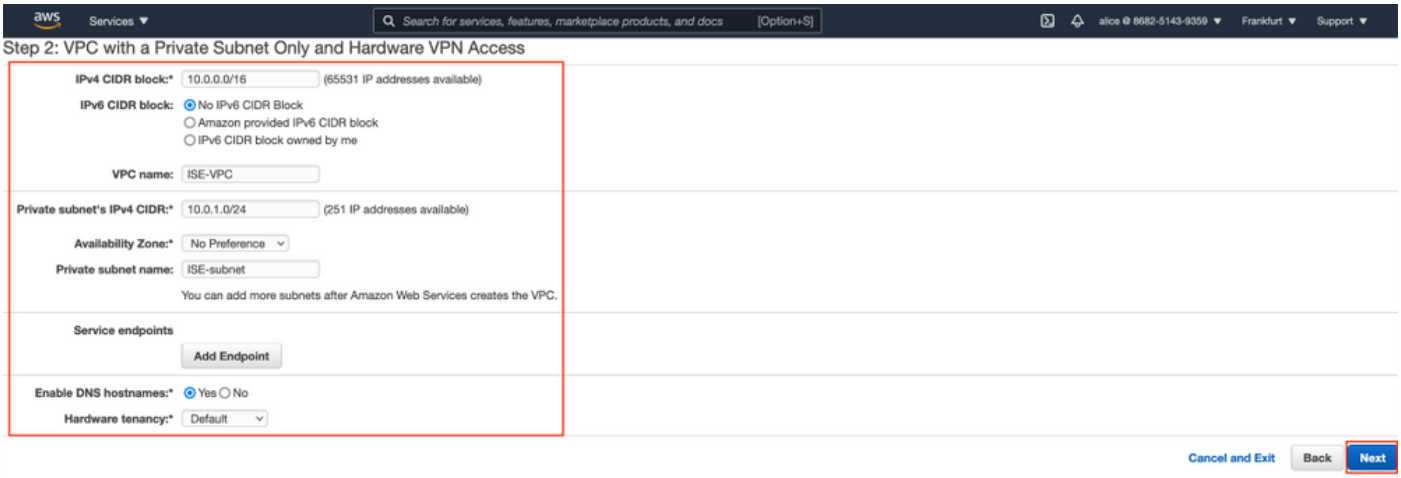


選擇**VPC with Private Subnet Only and Hardware VPN Access**，然後按一下**Select**，如下圖所示。

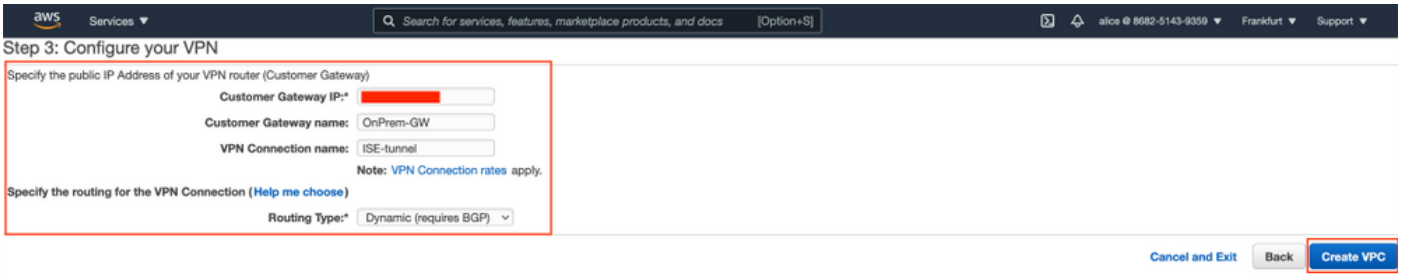


附註：在VPC嚮導的步驟1.中選擇的VPC取決於拓撲，因為ISE不設計為網際網路暴露的伺服器 — 僅使用具有專用子網的VPN。

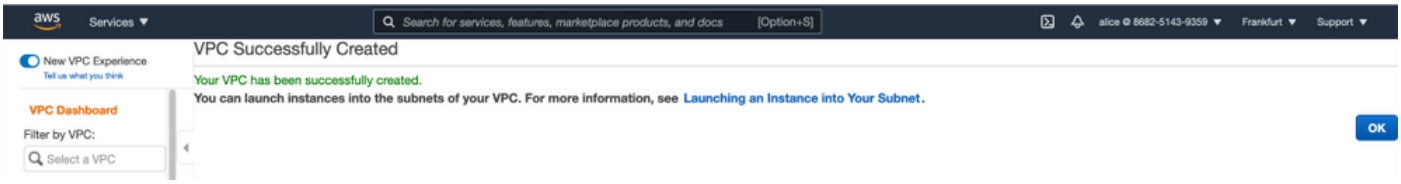
根據網路設計配置VPC專用子網設定，然後選擇**下一步**。



根據您的網路設計配置VPN，然後選擇**Create VPC**。

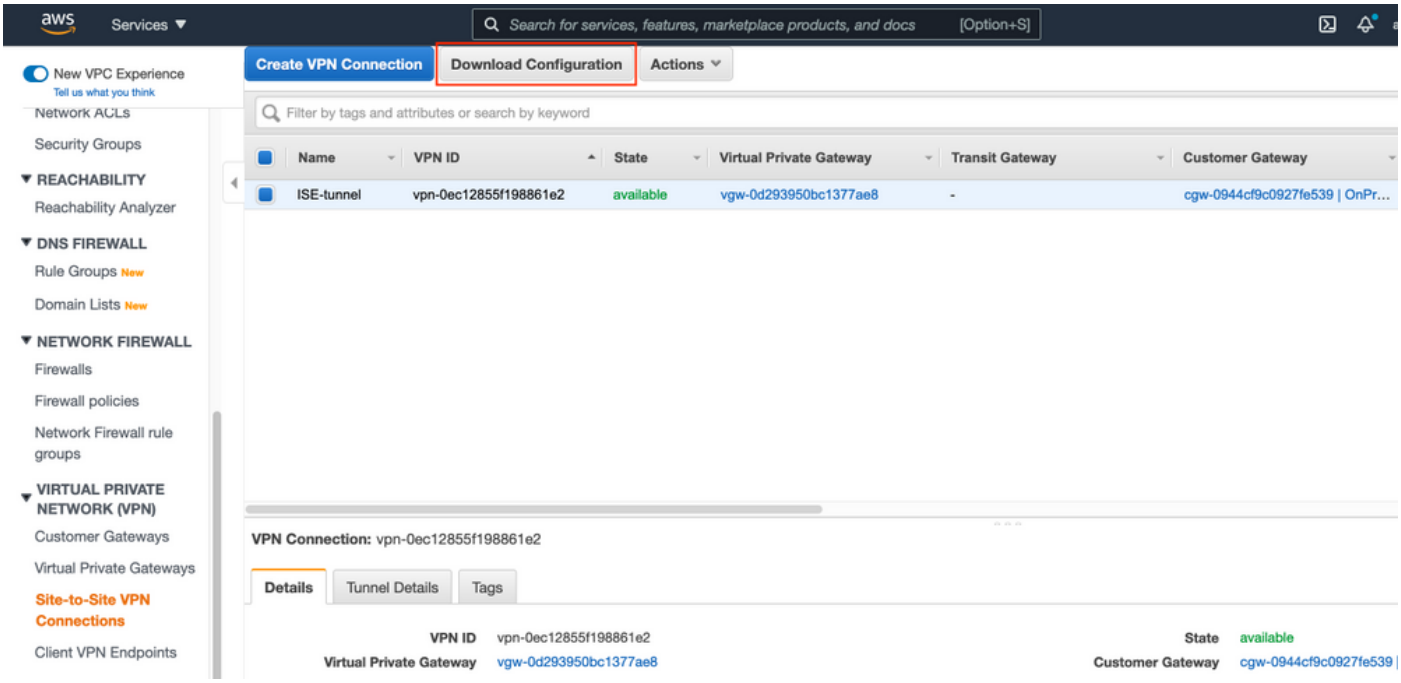


建立VPC後，將顯示**消息「已成功建立**VPC」。按一下「**OK**」，如下圖所示。



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。

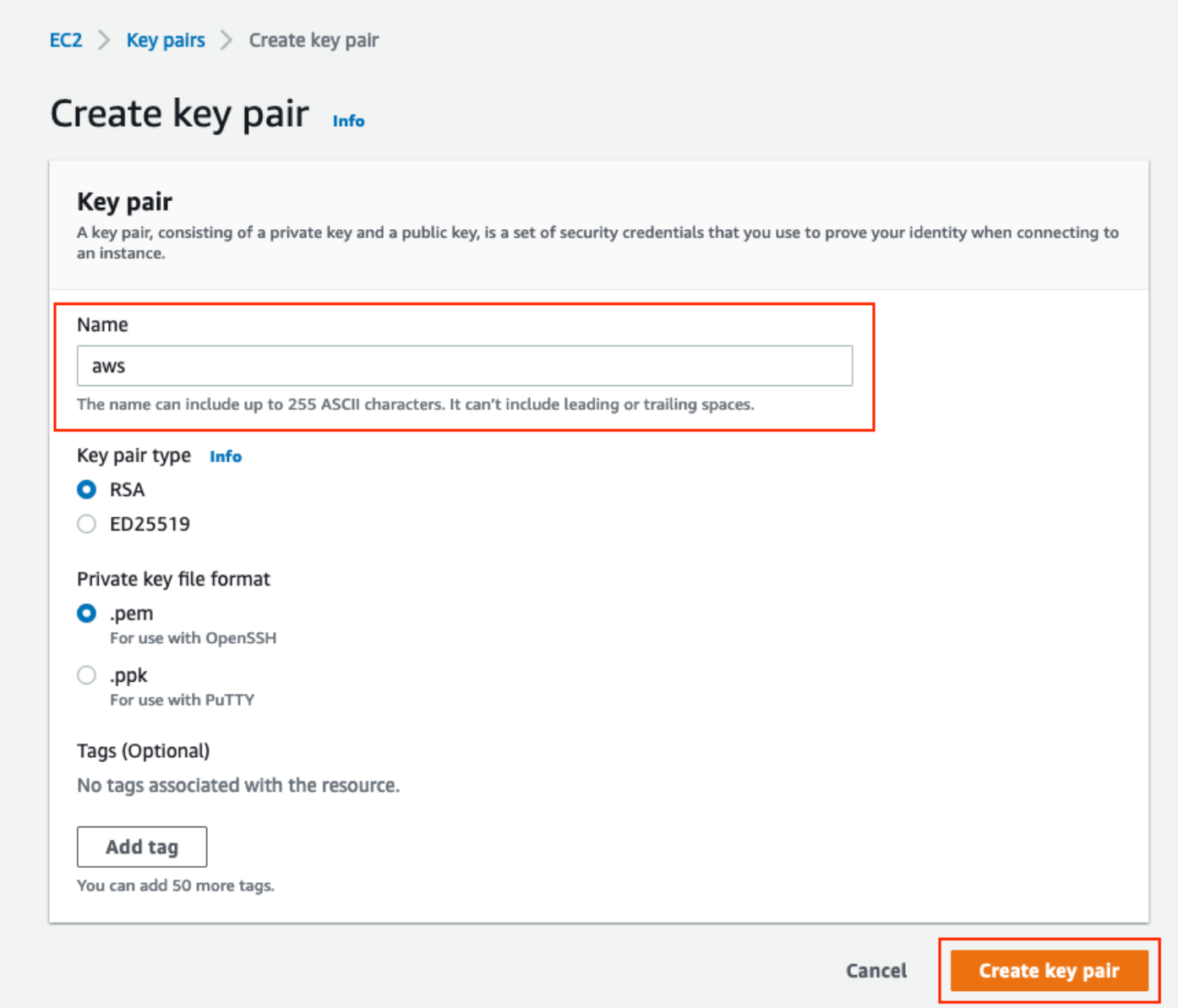


選擇**Vendor**、**Platform**和**Software**，然後選擇**Download**，如下圖所示。

在內部VPN頭端裝置上應用下載的配置。

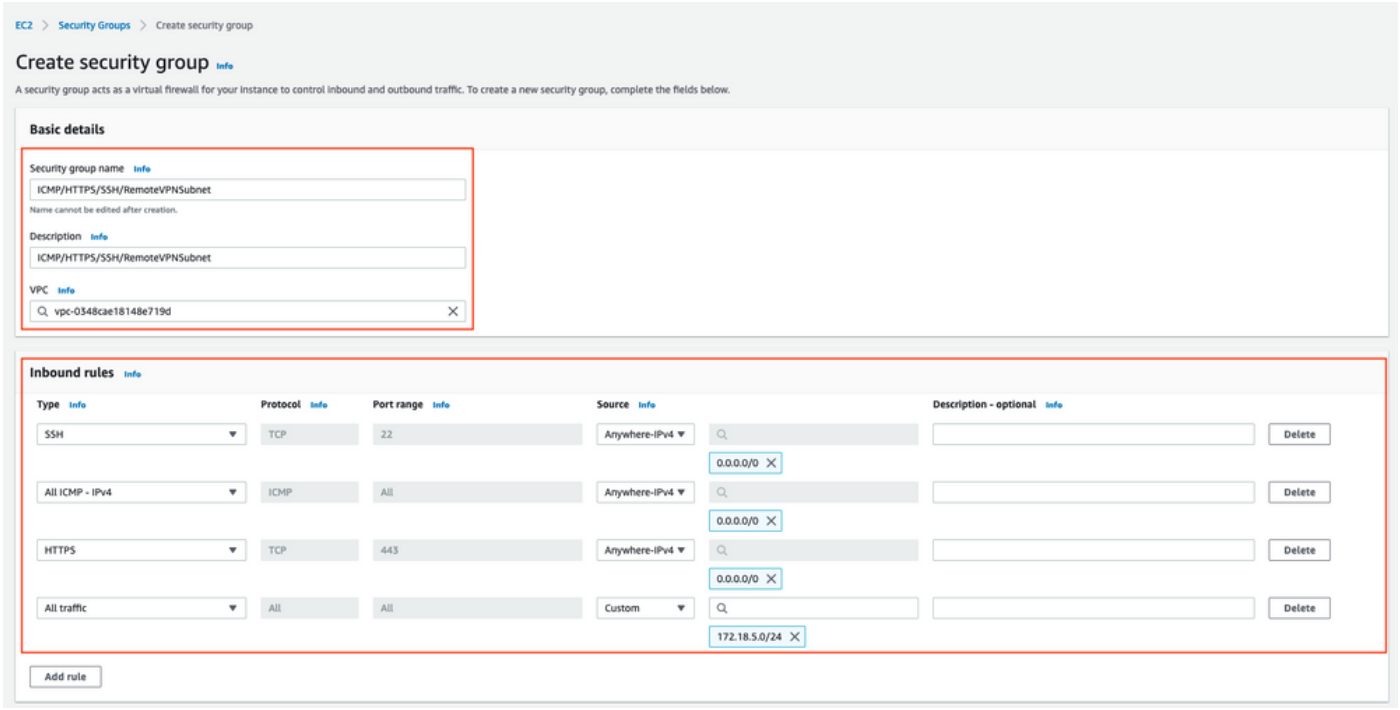
可選步驟C.建立自定義金鑰對

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**。



可選步驟D.建立自定義安全組

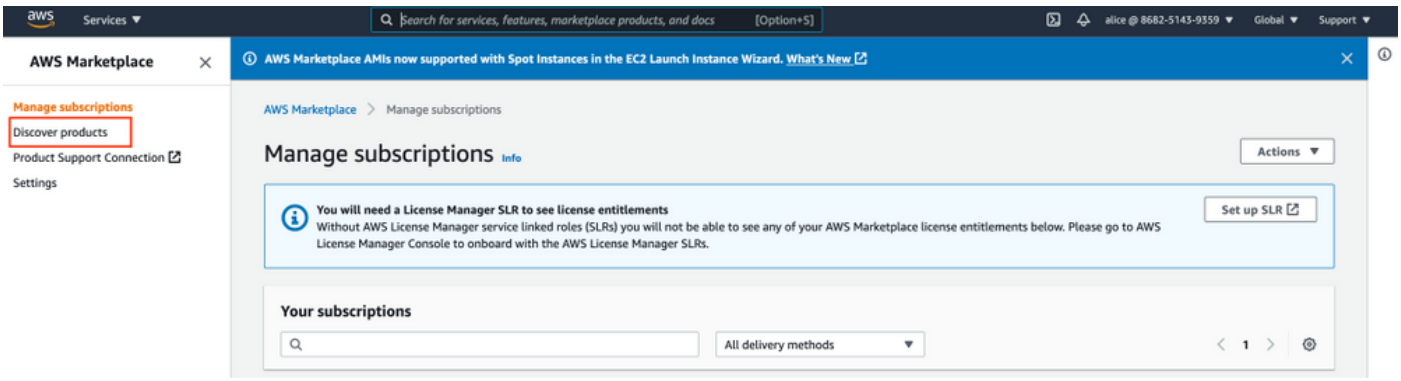
AWS EC2例項訪問受**Security Groups**保護，要配置**Security Group**，請導航到**EC2** Service。在**Network & Security**下選擇**Security Groups**選單。在VPC欄位中選擇Create Security Group,配置**Name、Description**，然後選擇新配置的VPC。配置**入站規則**以允許與ISE通訊。選擇**建立安全組**，如下圖所示。



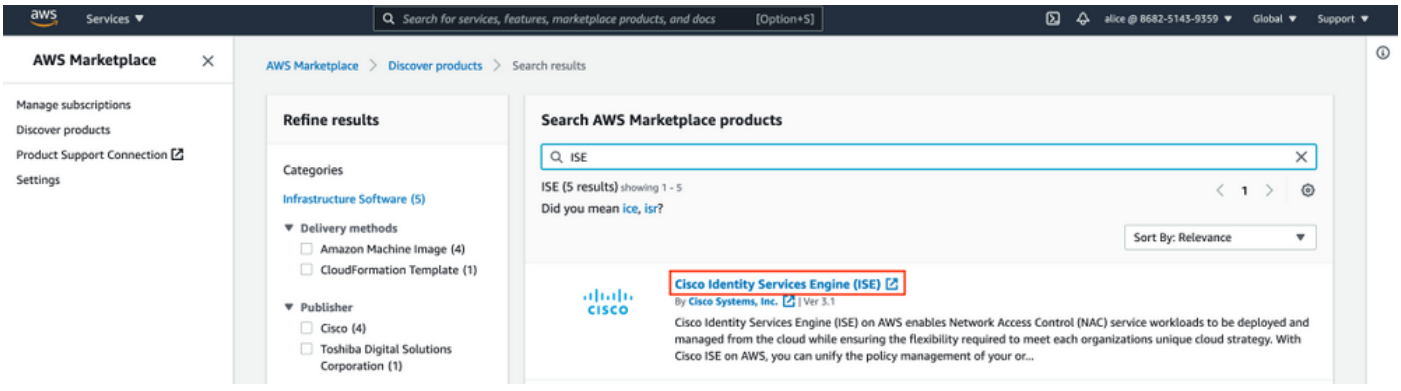
附註：配置的安全組允許通過SSH、ICMP、HTTPS訪問ISE，並且允許所有協定從內部子網訪問。

步驟1.訂購AWS ISE Marketplace產品

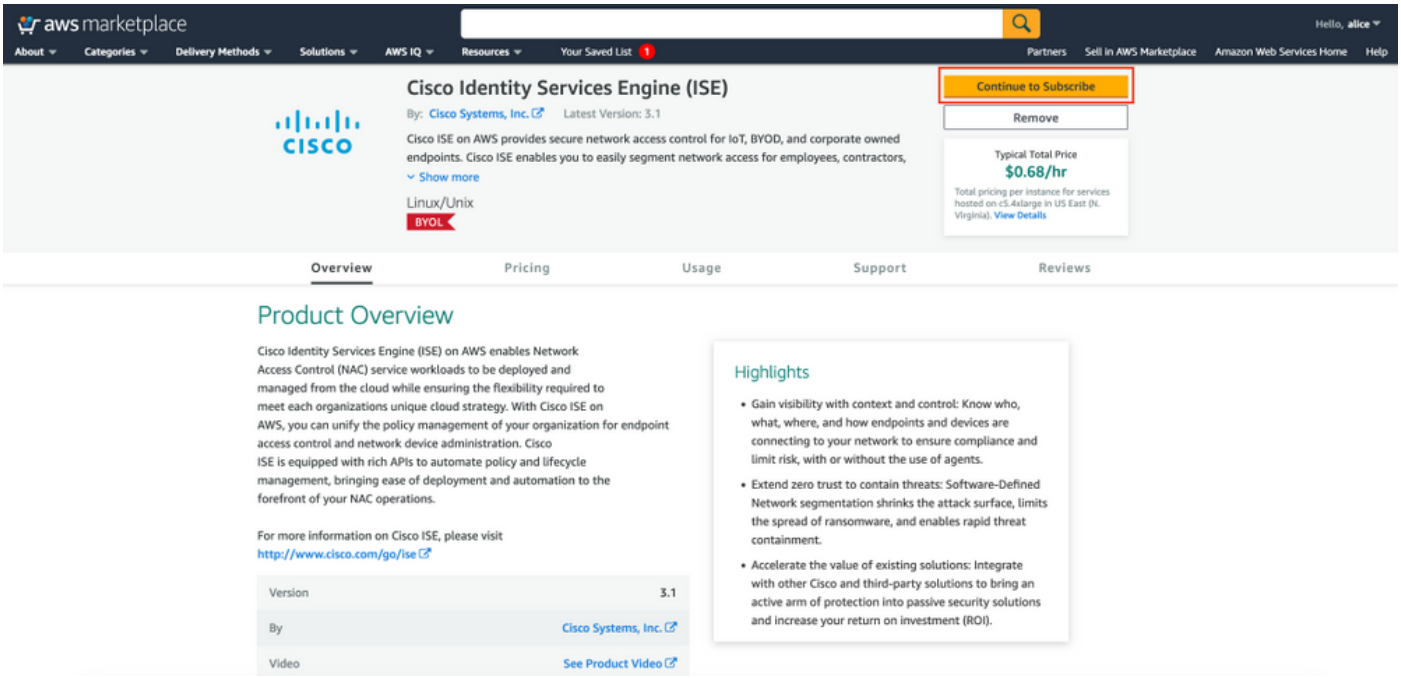
導航至**AWS Marketplace Subscriptions** AWS Service。選擇**Discover Products**，如下圖所示。



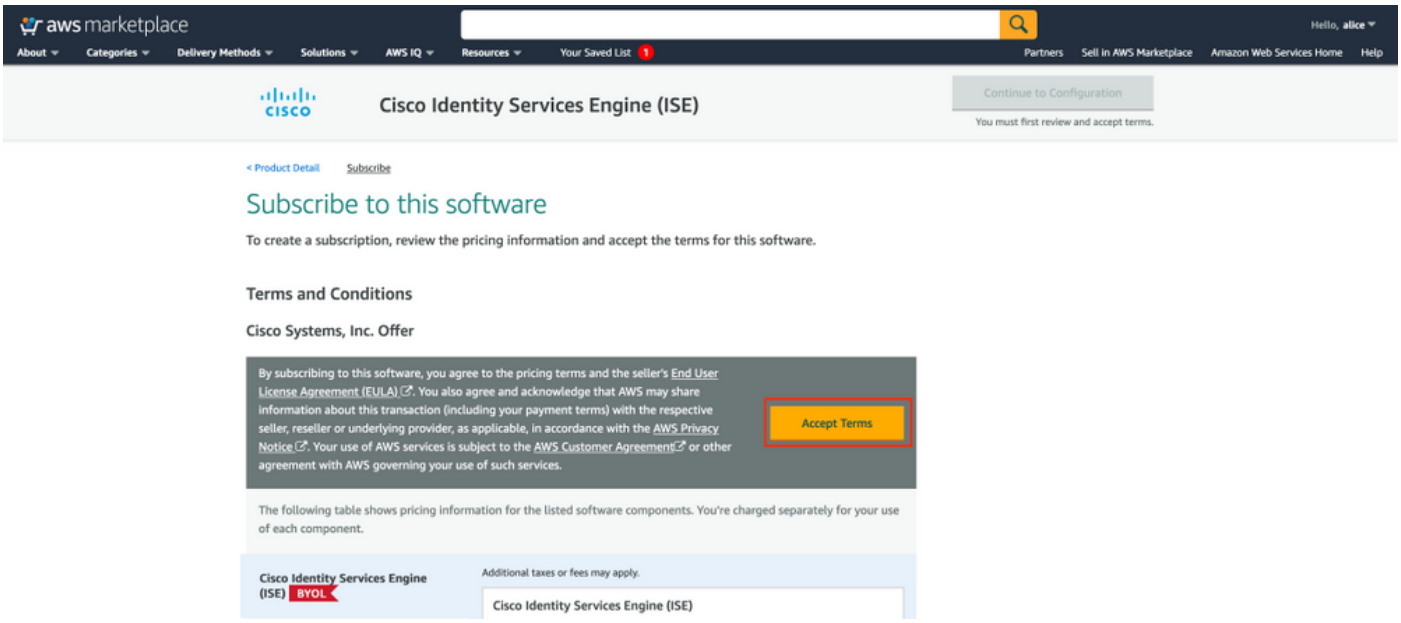
搜尋**ISE**產品並選擇**思科身分識別服務引擎(ISE)**，如下圖所示。



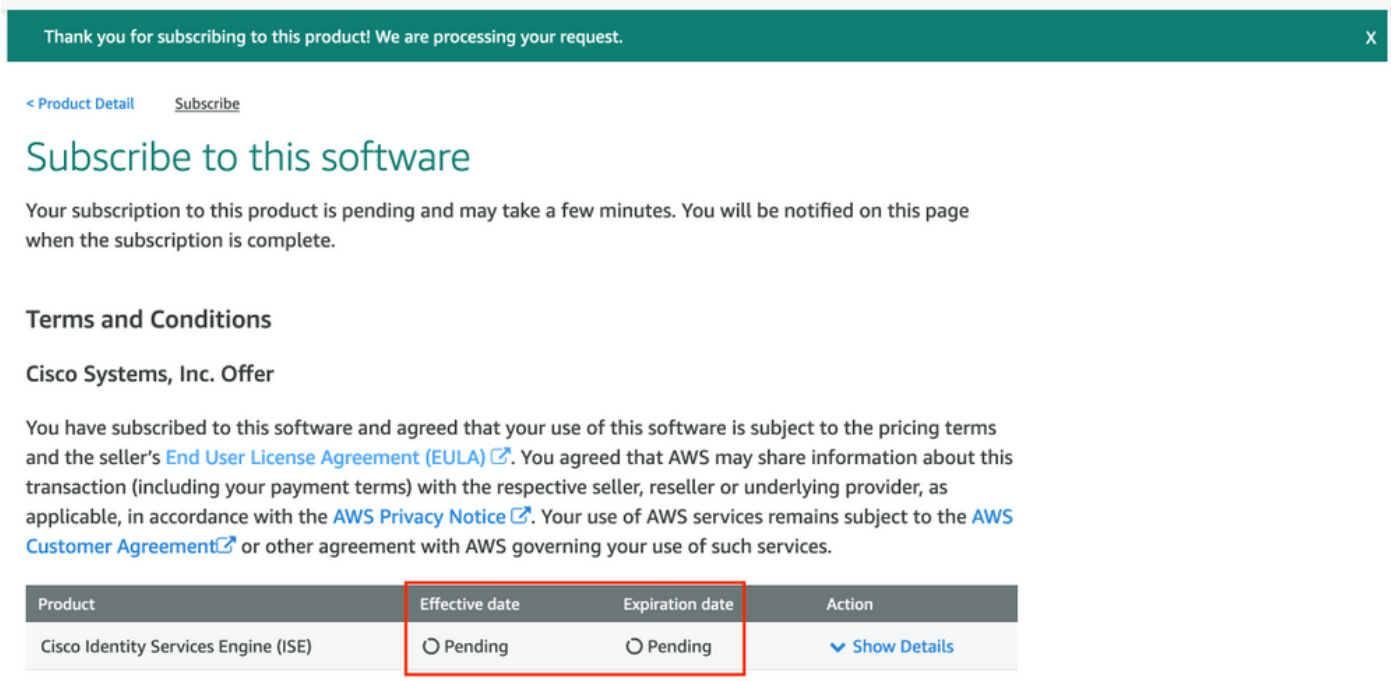
選擇**繼續訂閱**按鈕



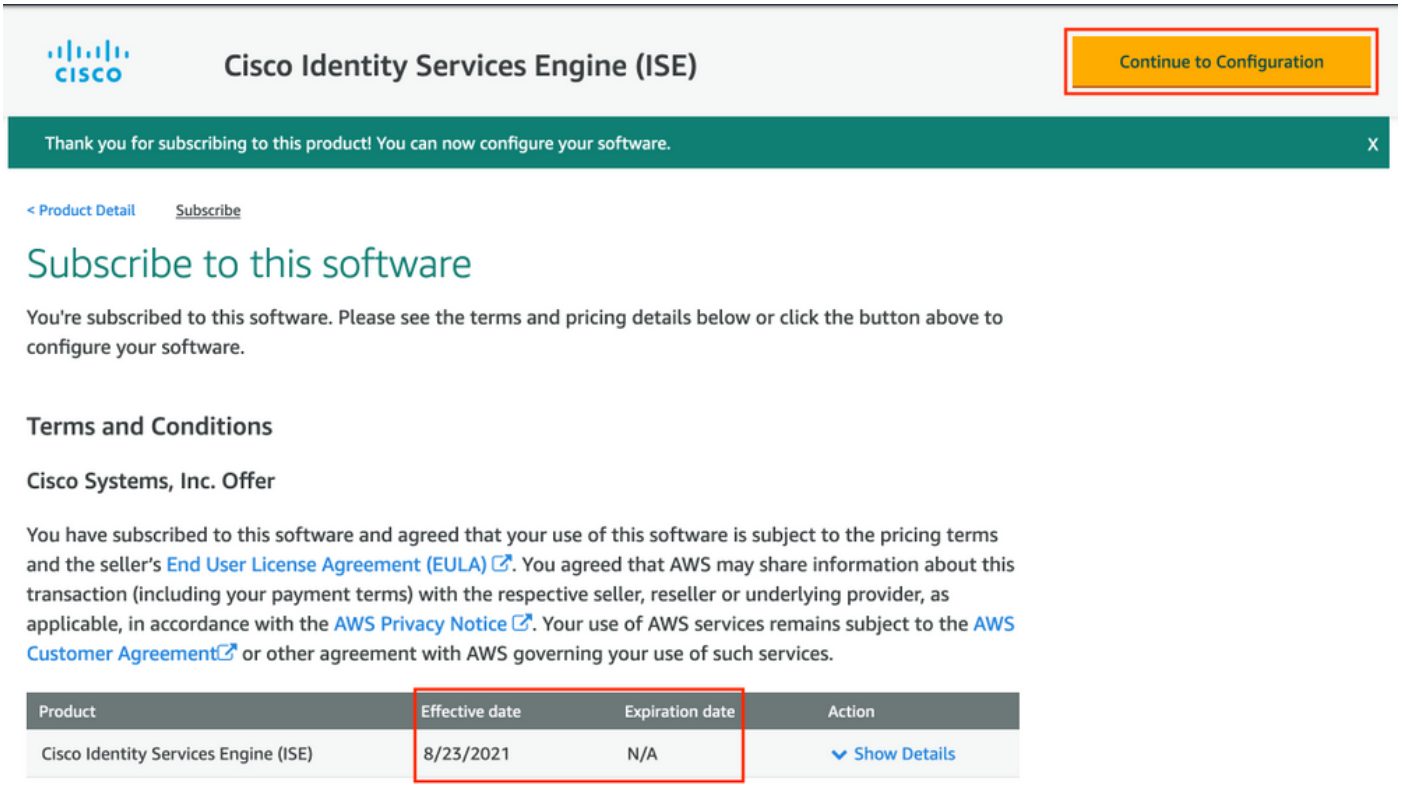
選擇**Accept Terms**按鈕，如下圖所示。



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

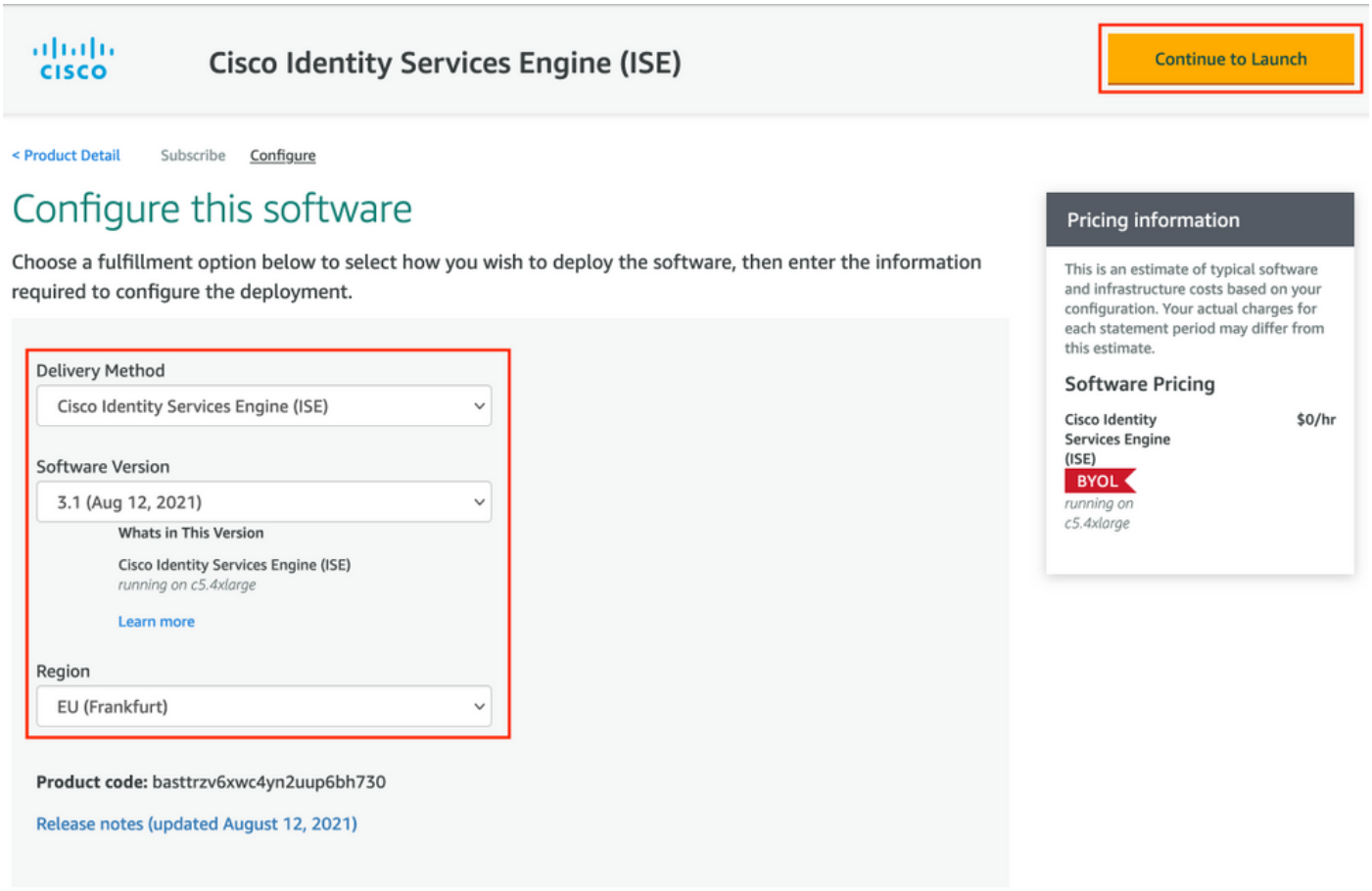


生效日期**更改**為訂閱日期，到期日期**更改為N/A後不久。選擇Continue to Configuration**，如ima所示



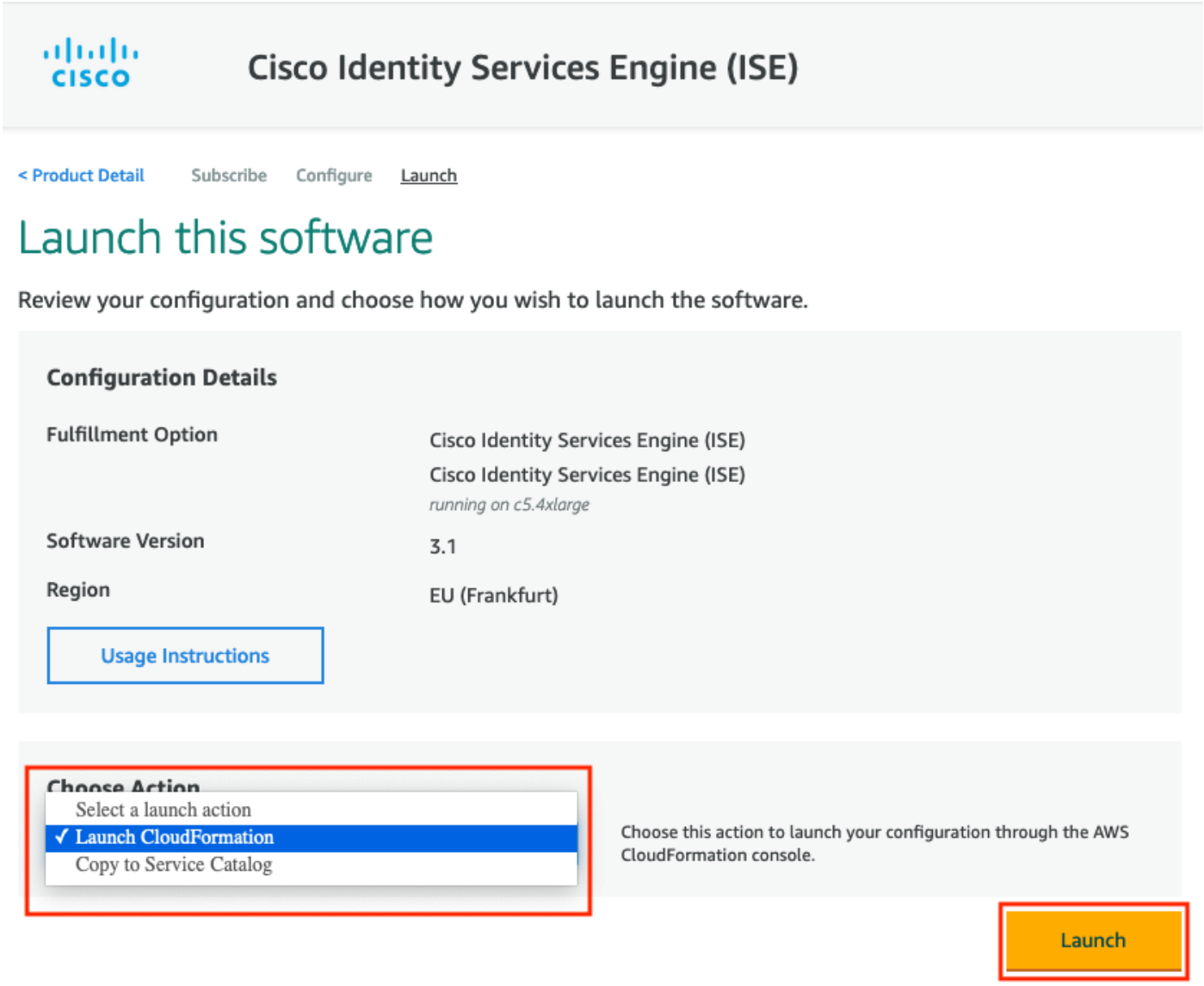
步驟2.在AWS上配置ISE

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。**



步驟3.在AWS上啟動ISE

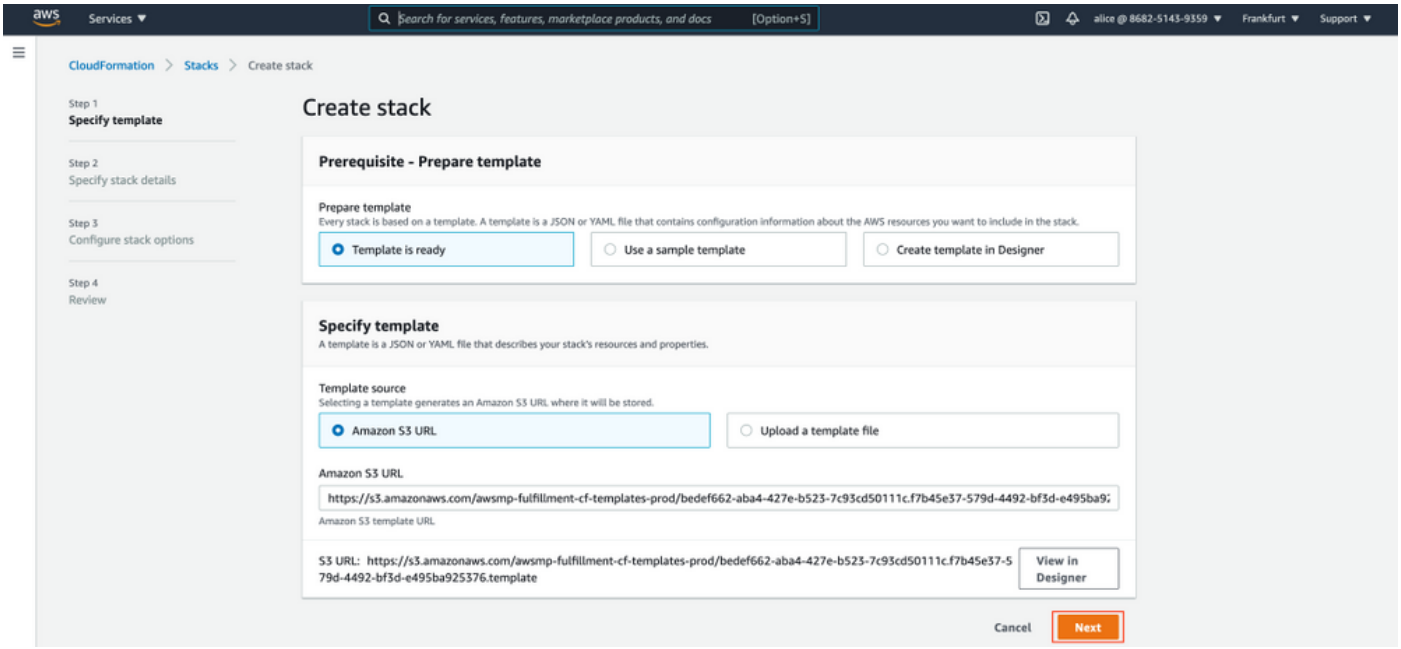
從**啟動此軟體**螢幕的「操作」下拉選單中，選擇**啟動**CloudFormation。



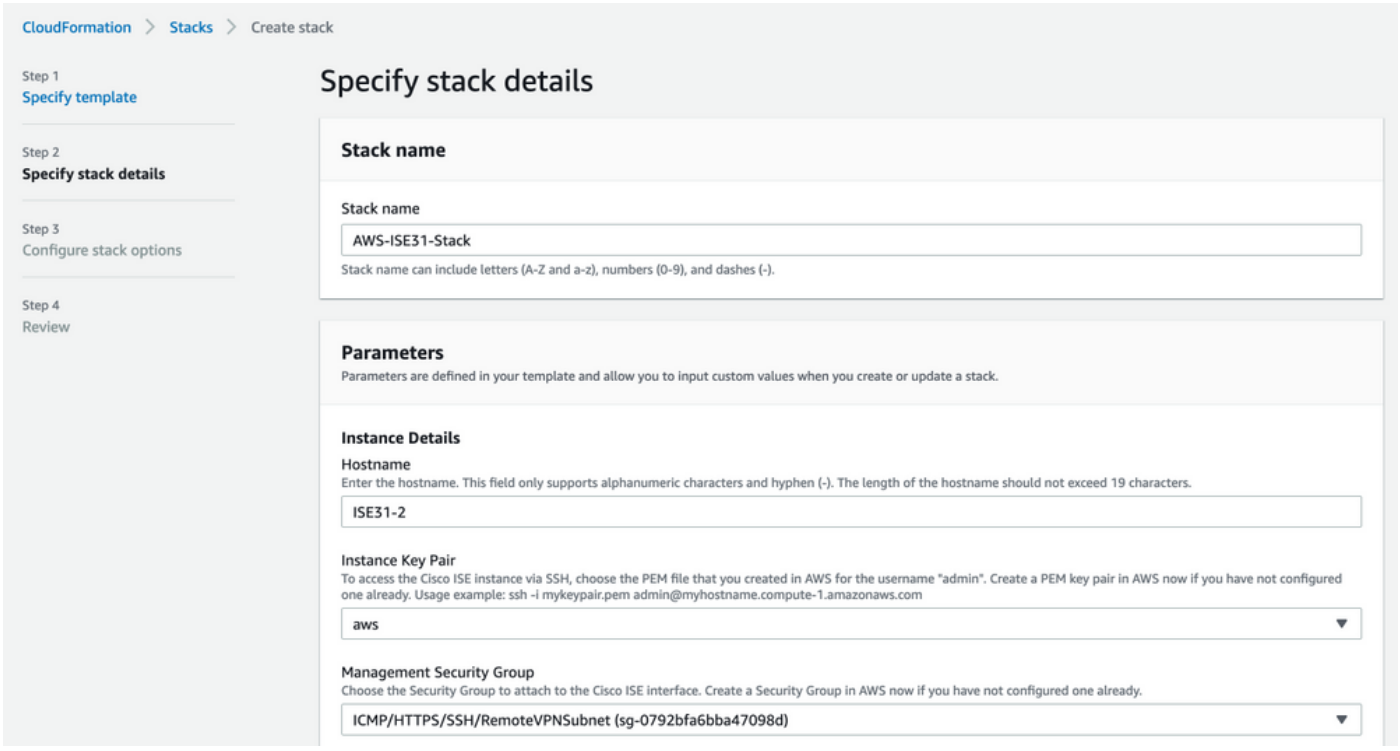
（可選）選擇**使用說明**以使自己熟悉這些說明。選擇**啟動**。

步驟4.在AWS上為ISE配置CloudFormation堆疊

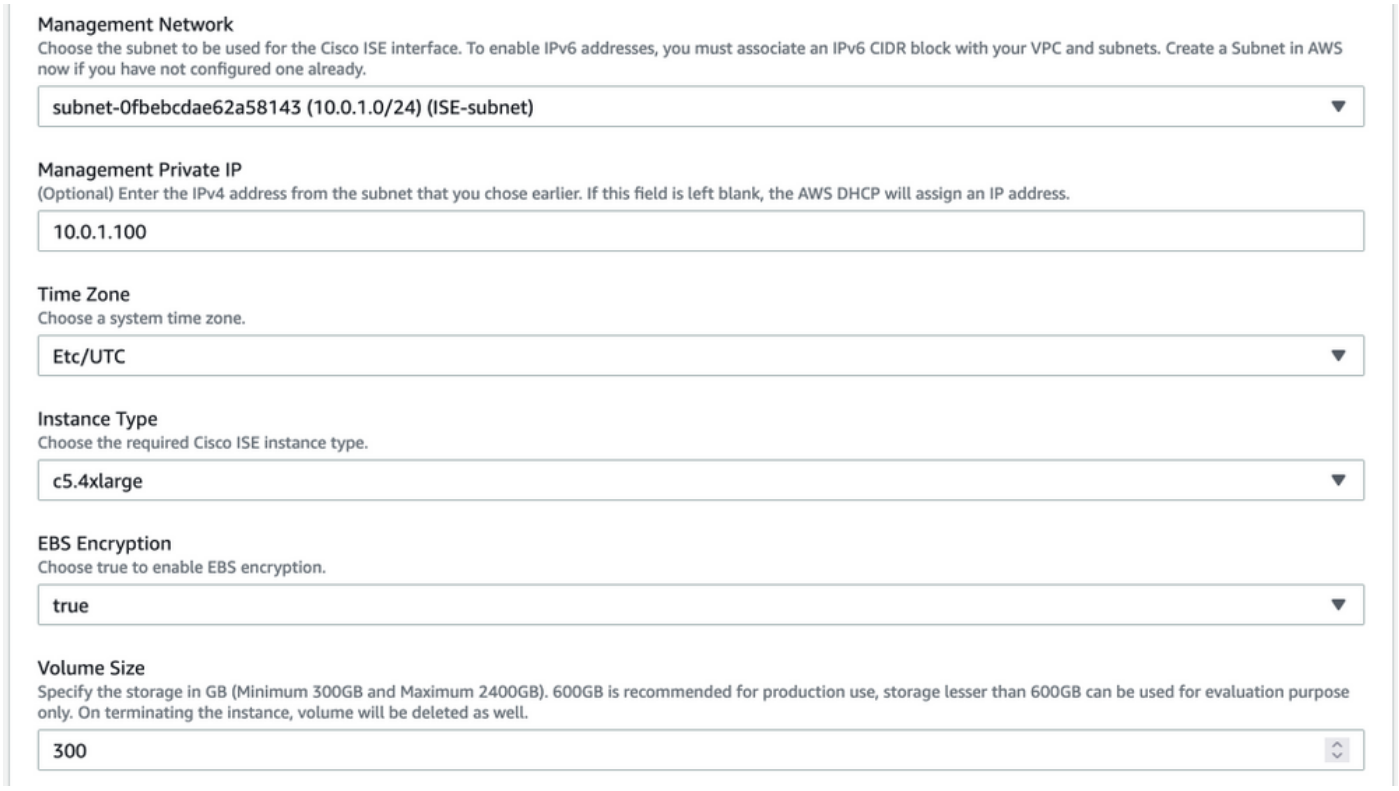
啟動按鈕將您重定向到CloudFormation Stack設置螢幕。有一個預構建模板必須用於設定ISE。保留預設設定，然後選擇**下一步**。



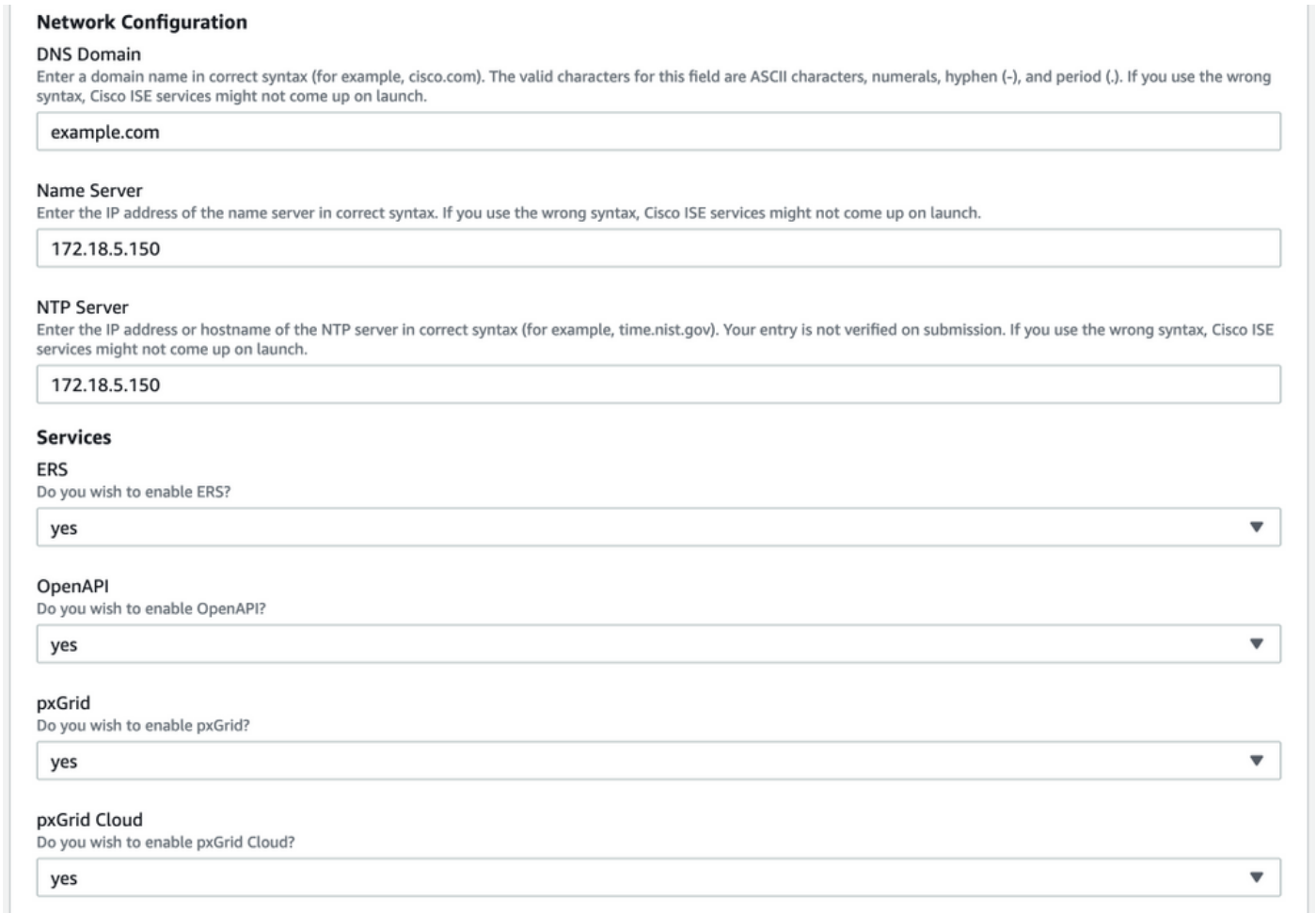
使用堆疊名稱填充CloudFormation**堆疊資料**。配置例項詳細資訊，如**主機名**，選擇**例項金鑰對**和**管理安全組**。



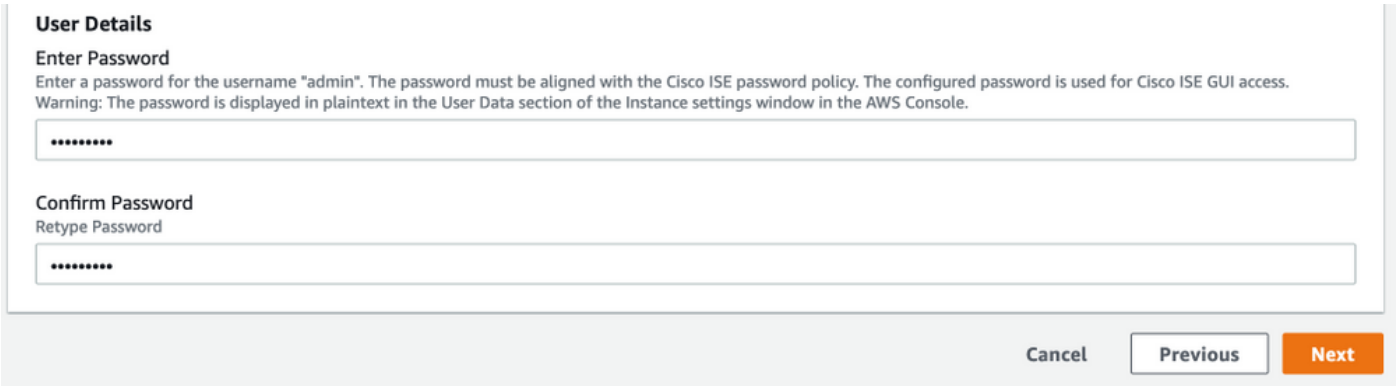
繼續使用管理網路、**管理專用IP**、**時區**、**例項類**型、**EBS加密和卷大小配**置例項**詳細資訊**。



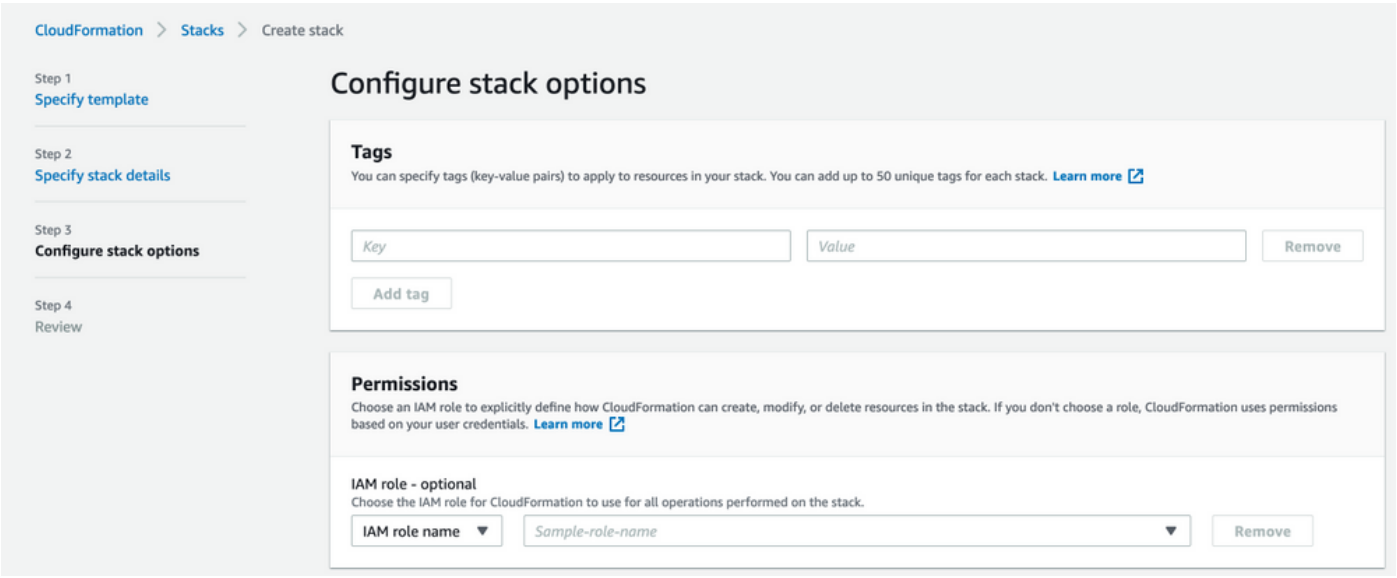
繼續使用DNS域、名稱伺服器、NTP服務和服務配置實例詳細資訊。



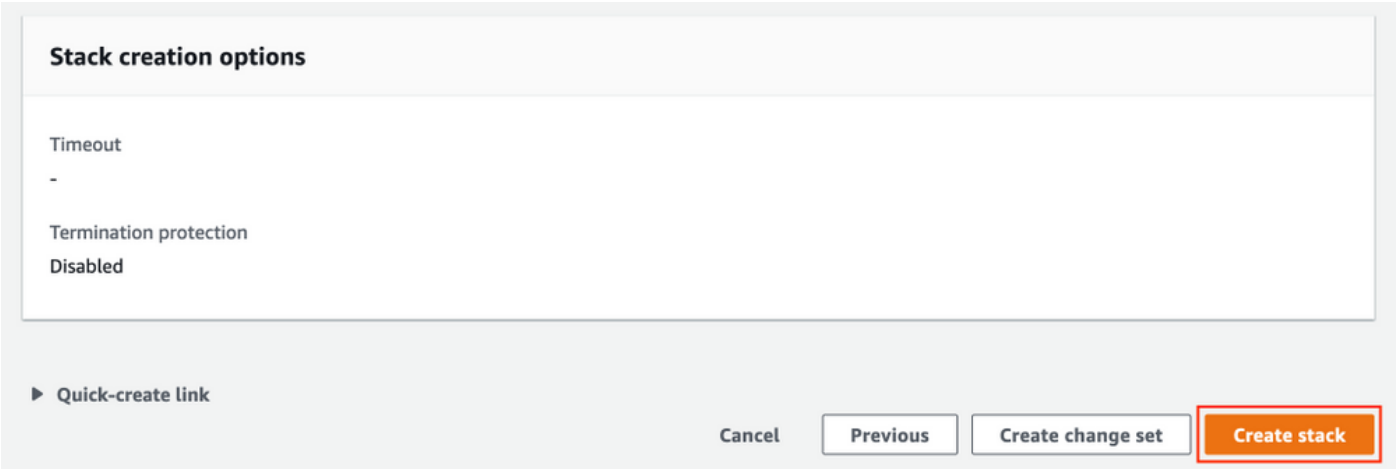
配置GUI使用者密碼並選擇下一步。



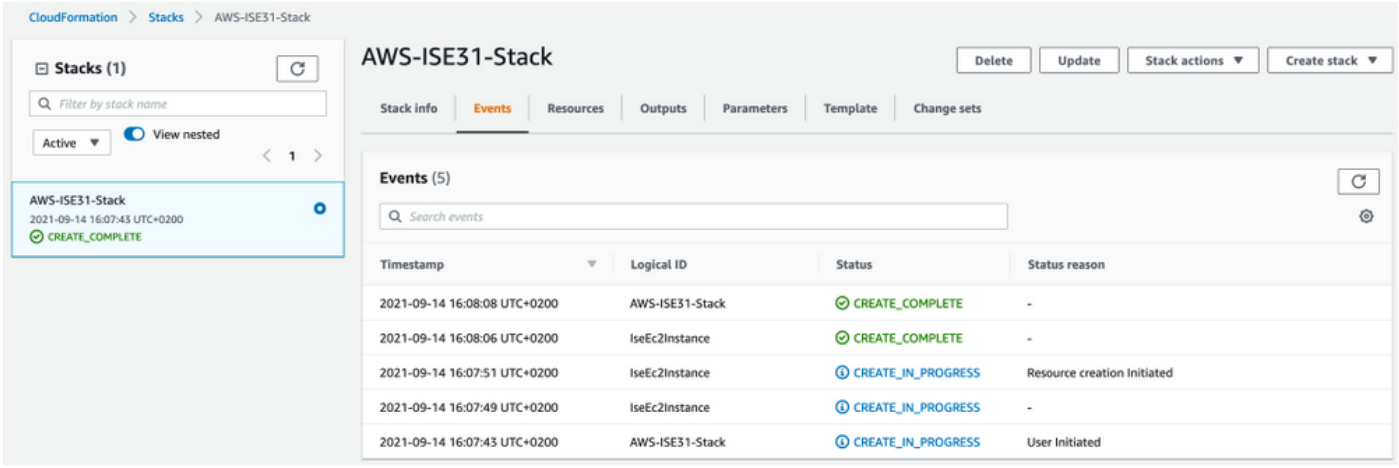
下一螢幕不需要更改。選擇**Next**。



前往**Review Stack**視窗，向下滾動並選擇**Create stack**。

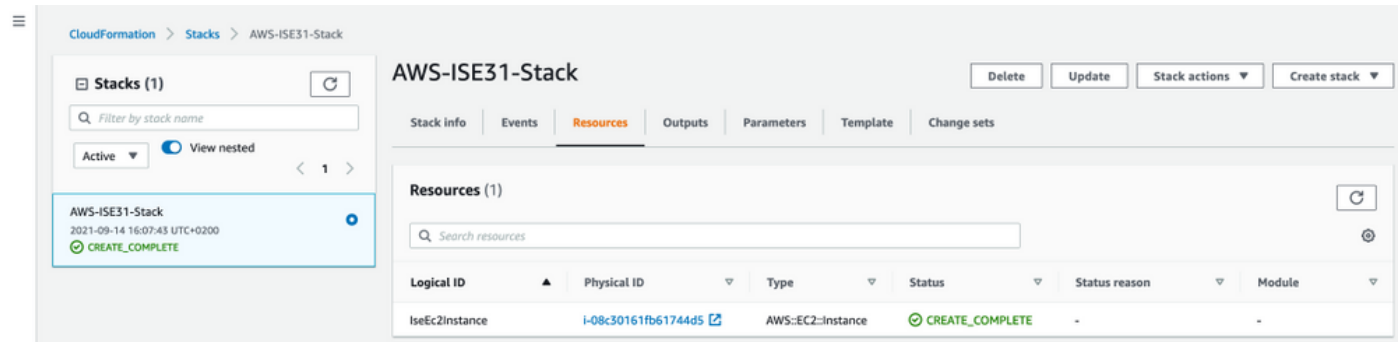


部署堆疊後，必須看到**CREATE_COMPLETE**狀態。

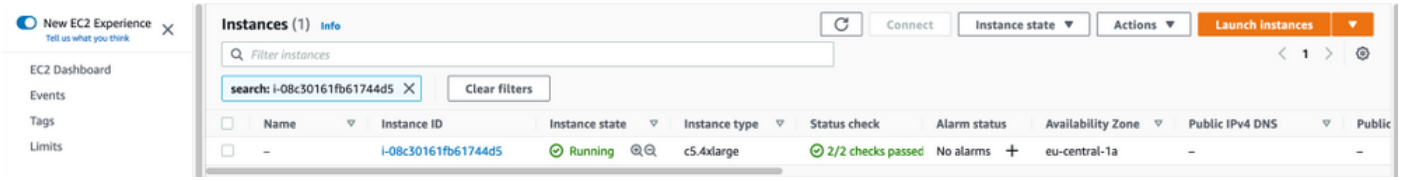


步驟5.訪問AWS上的ISE

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: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：

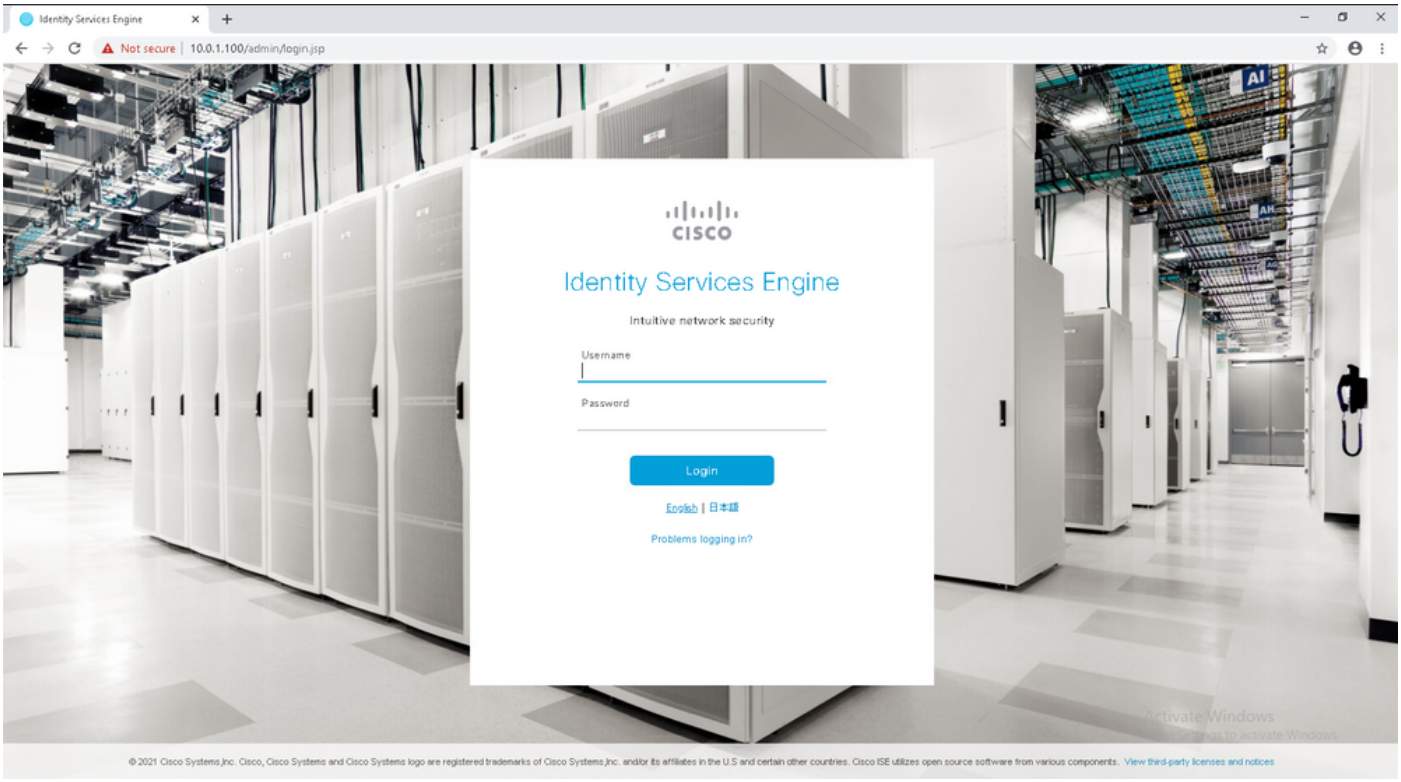
```
ISE31-2/admin# show application status ise

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#
```

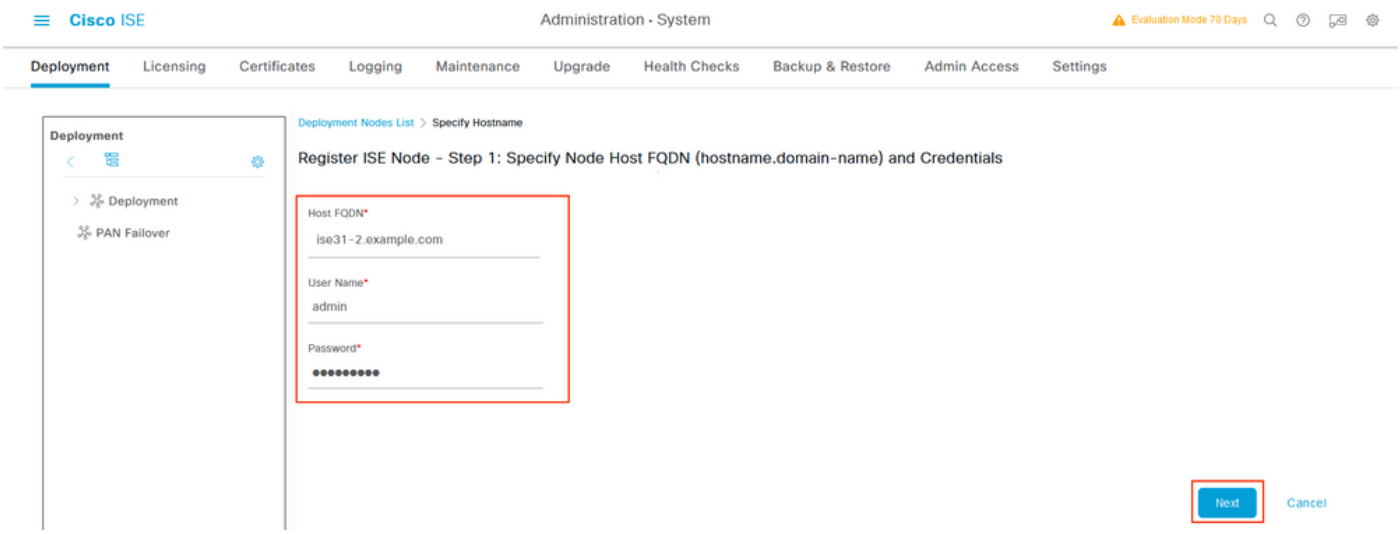
附註：由於SSH可用於ISE服務，需要大約10-15分鐘才能轉換到運行狀態。

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

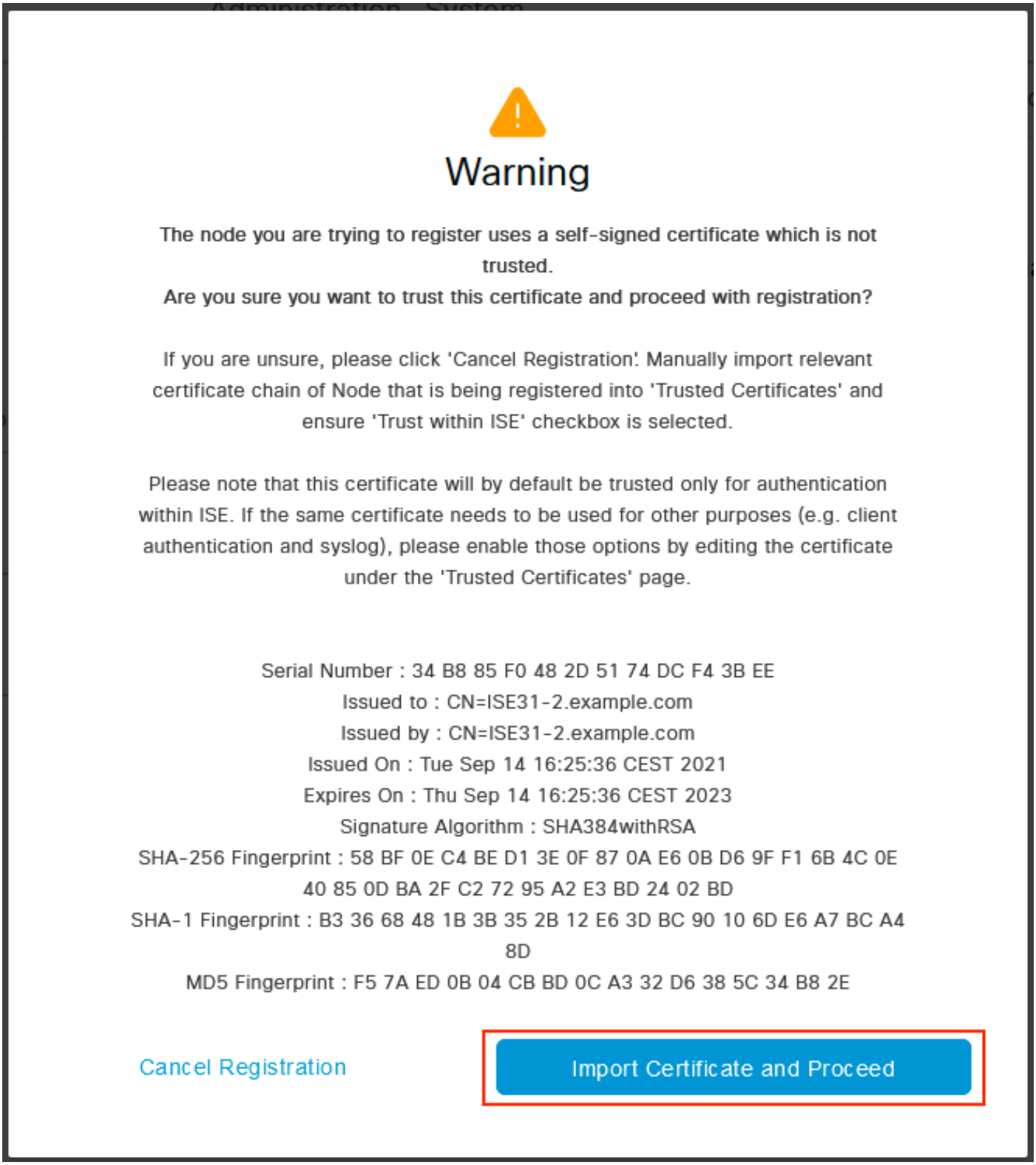


步驟6.在AWS上配置本地ISE和ISE之間的分散式部署

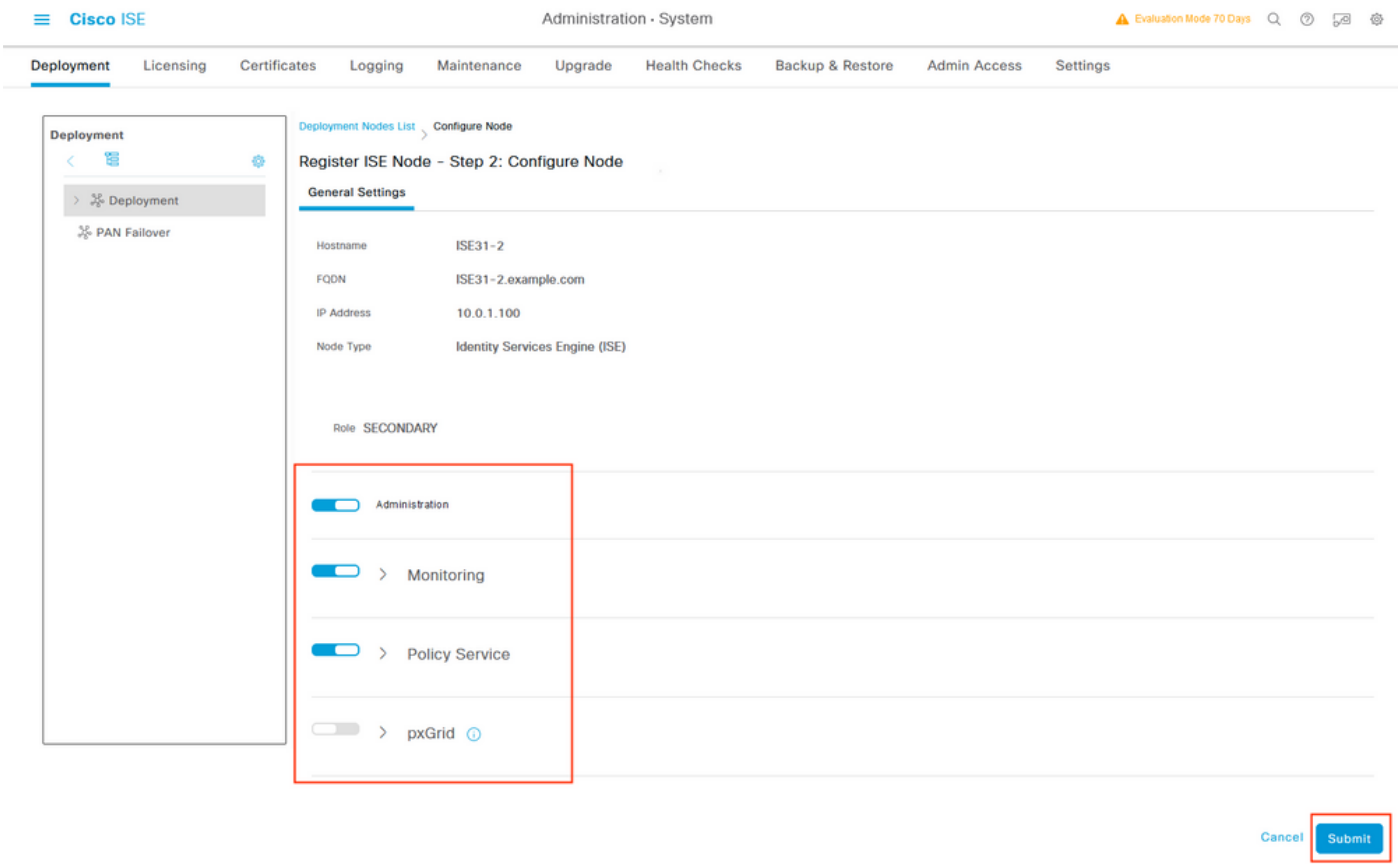
登入到本地ISE並導航到**管理>系統>部署。**選擇節點並選擇**Make Primary。導航回管理>系統>部署**，選擇**註冊**。在AWS上配置ISE的**主機FQDN**、GUI用**戶名**和密**碼。**按「Next」（下一步）。



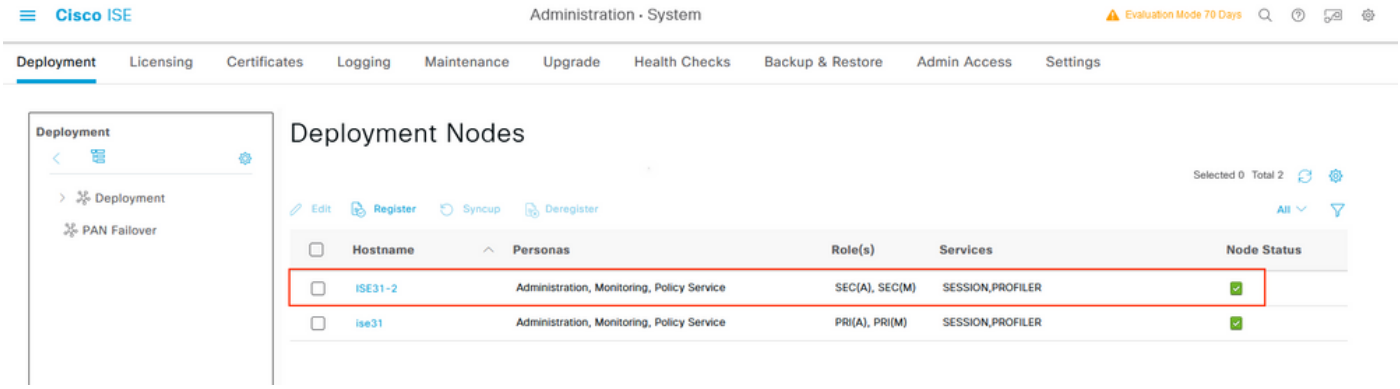
由於此拓撲中使用自簽名證書，要將管理員證書交叉匯入到受信任的儲存中，請選擇**匯入證書並繼續。**



選擇您選擇的角色，然後按一下**提交**。

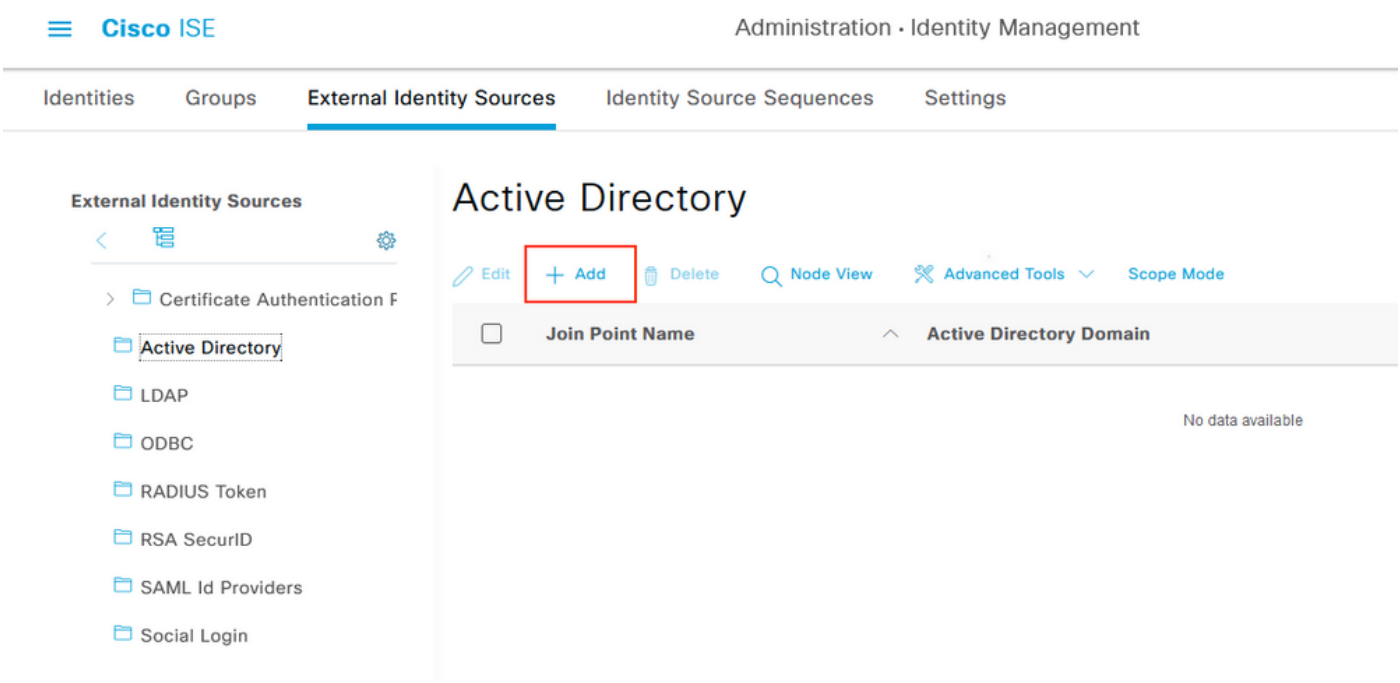


同步完成後，節點將轉換到連線狀態，其上方將顯示綠色覈取方塊。

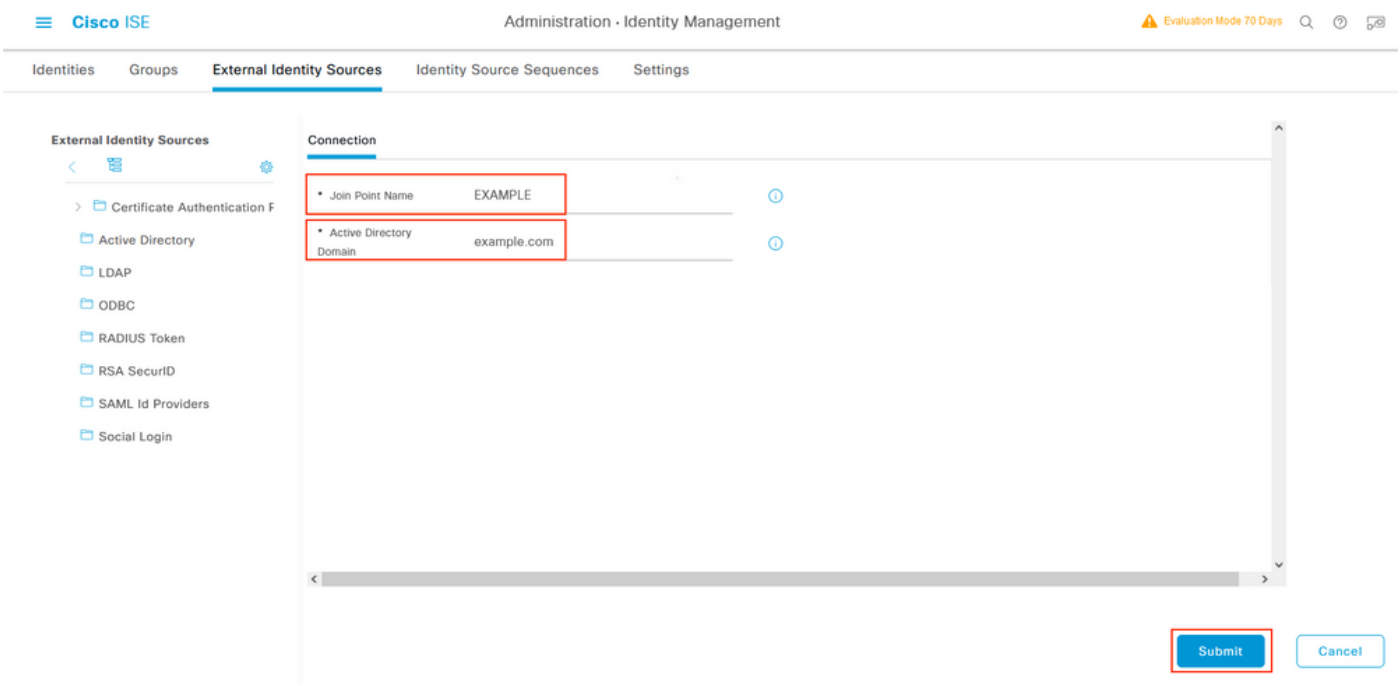


步驟7.將ISE部署與本地AD整合

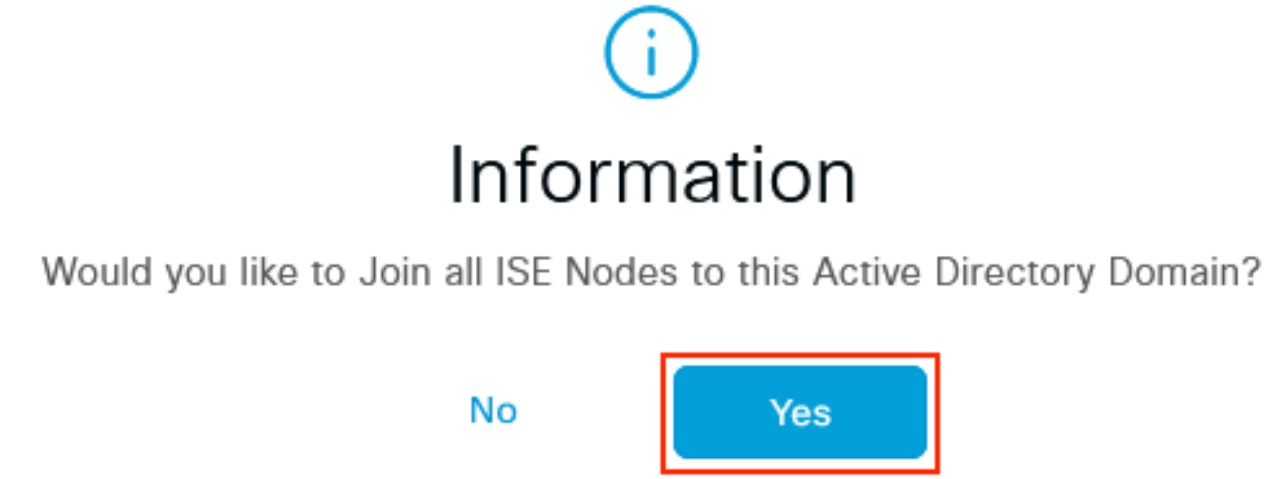
導航到**管理>身份管理>外部身份源**。選擇Active Directory，選擇Add。



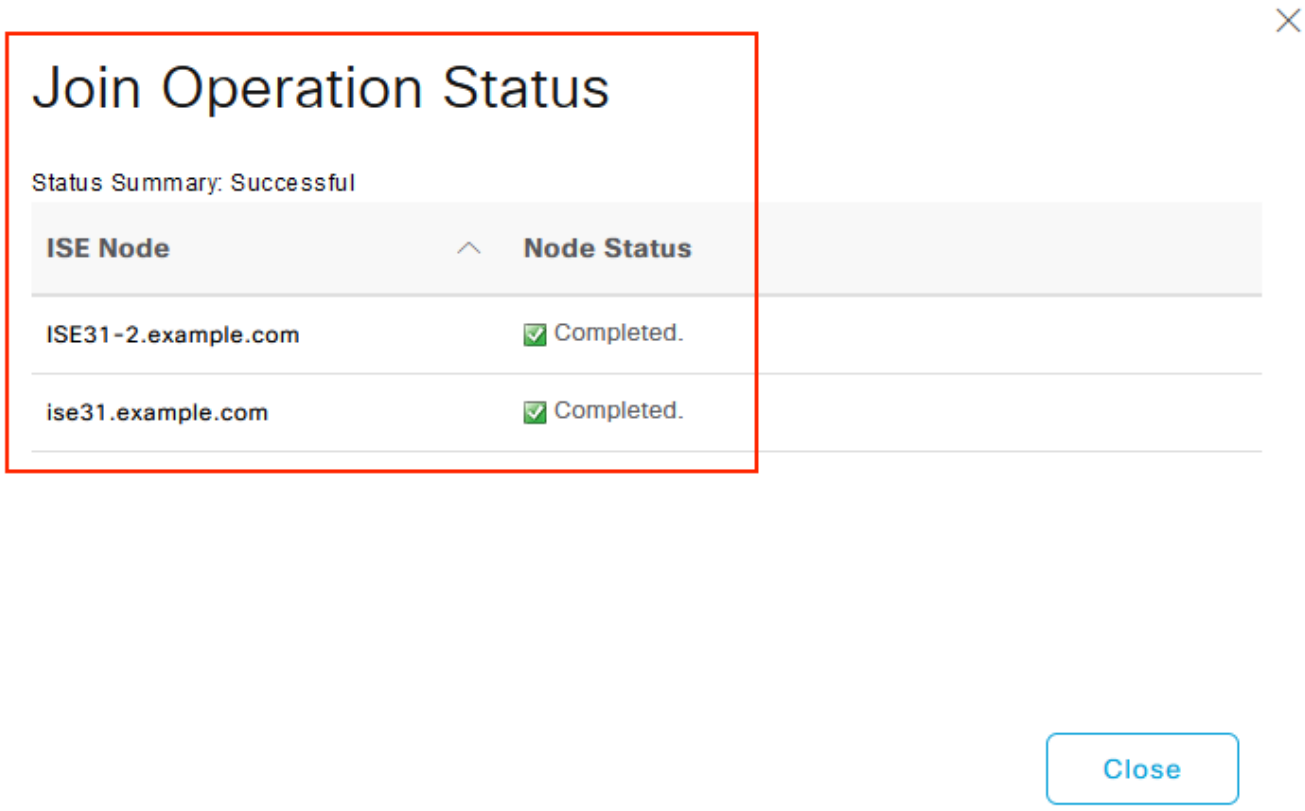
配置**聯合點名稱**和**Active Directory域**，選擇**提交**。



要將兩個節點與Active Directory整合，請選擇**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」。



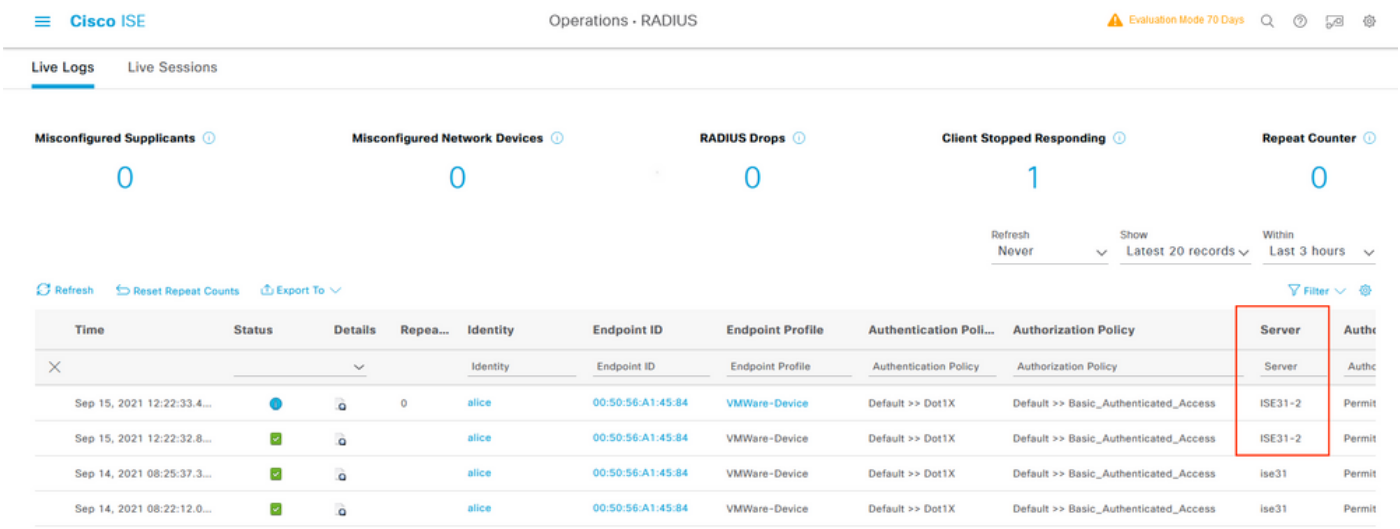
限制

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。

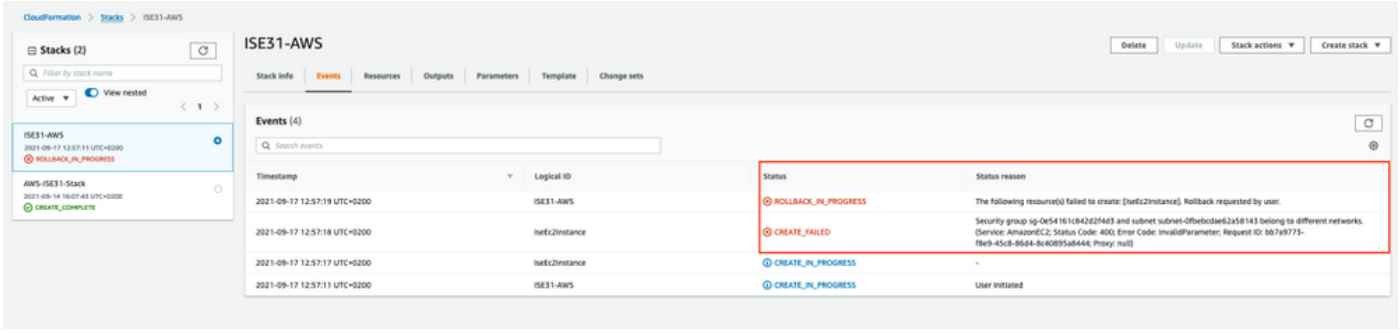


疑難排解

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。



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
```