تكوين ISE 3.1 من خلال سوق AWS

المحتويات

المقدمة

يوضح هذا المستند كيفية تثبيت Identity Services Engine (ISE) 3.1 عبر Amazon Machine Image (AMI) في Amazon Web Services (AWS). يمكنك نشره يدويًا من إصدار ISE 3.1 المتاح للسحابة الحوسبة المرنة (EC2) على Amazon بمساعدة قوالب CloudConfiguration (CFT).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- AWS ومفاهيم مثل VPC و EC2 و CloudConfiguration

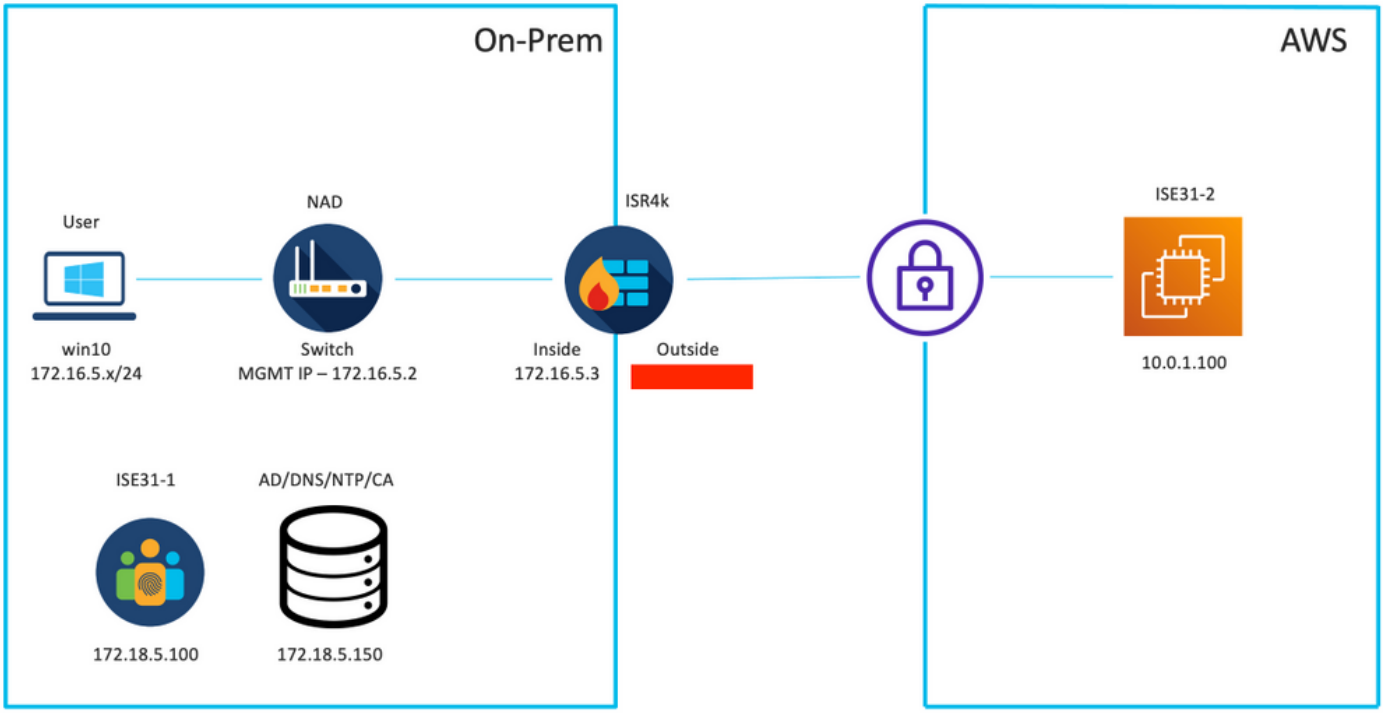
المكونات المستخدمة

أسست المعلومة في هذا وثيقة على cisco ISE صيغة 3.1.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

مخطط الشبكة

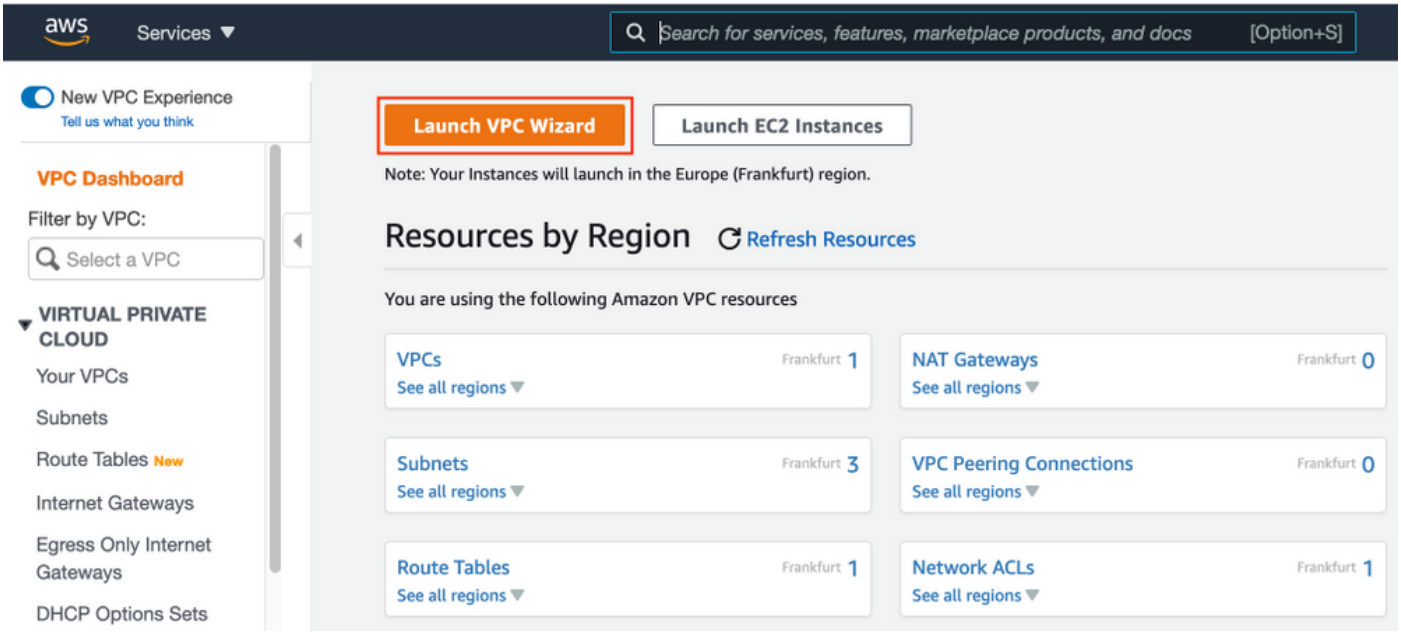


التكوينات

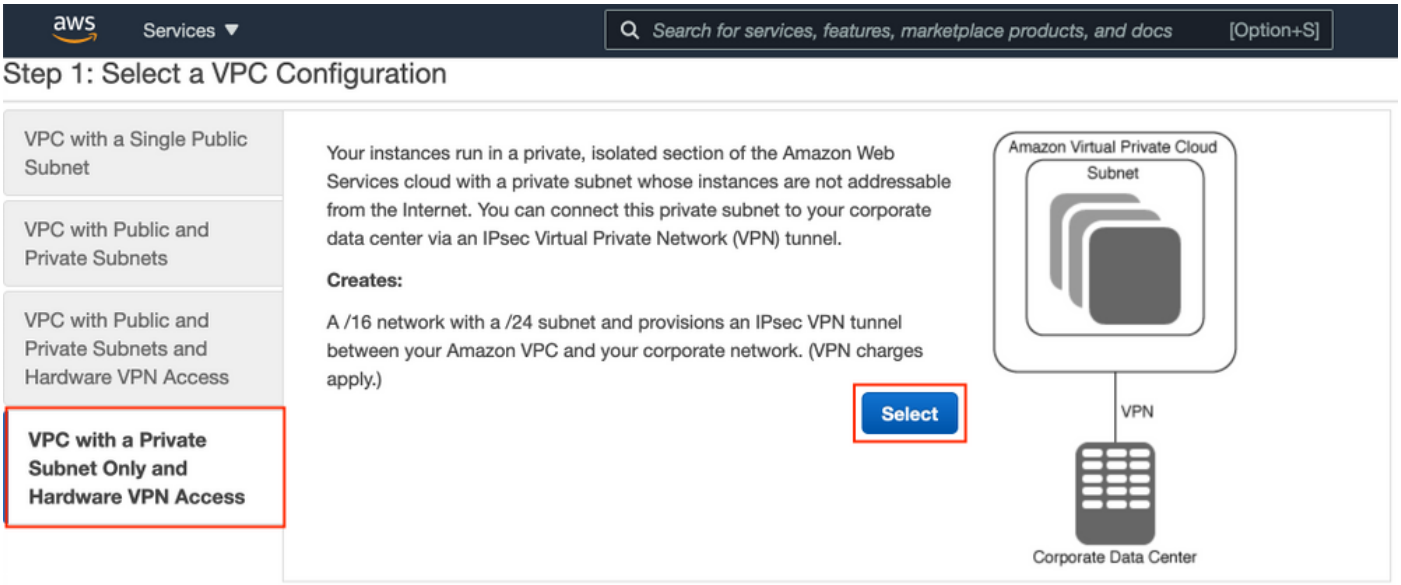
في حالة عدم وجود جهاز كمبيوتر شخصي (VPC) ومجموعات الأمان وأزواج المفاتيح ونفق الشبكة الخاصة الظاهرية (VPN) الذي تم تكوينه بعد، يلزمك اتباع الخطوات الاختيارية، وإلا، فعليك البدء بالخطوة 1.

الخطوة الاختيارية أ. إنشاء VPC

انتقل إلى خدمة AWS **الخاصة بمعرف فئة المورد (VPC)**. حدد **تشغيل معالج VPC** كما هو موضح في الصورة.

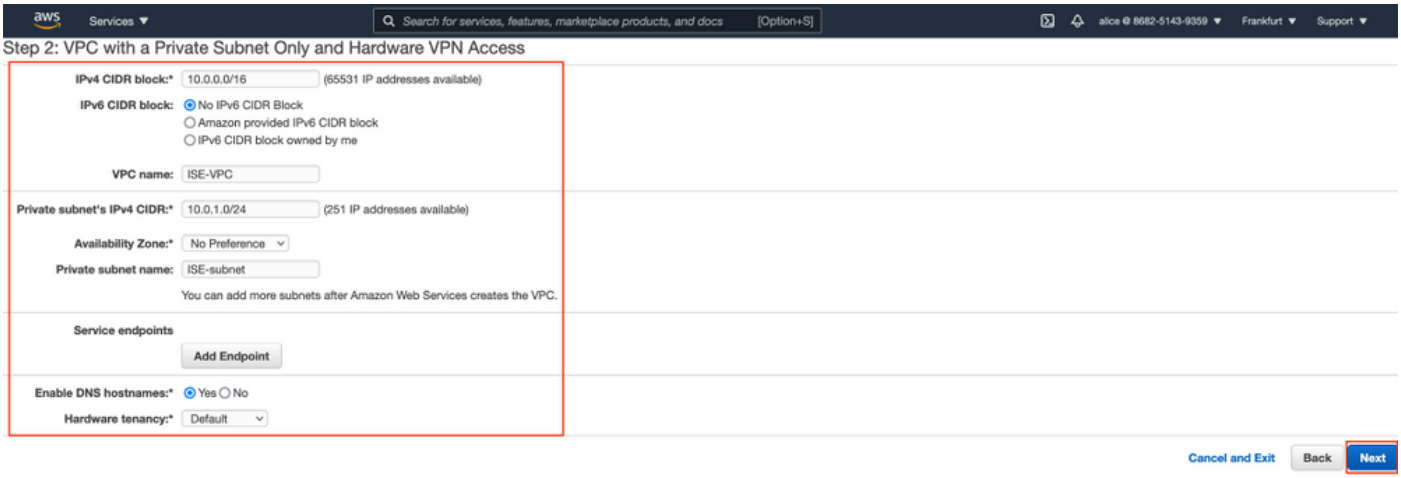


أخترت **VPC مع خاص subnet فقط وجهاز VPN منفذ** وطقطقة **يني تق** كما هو موضح في الصورة.

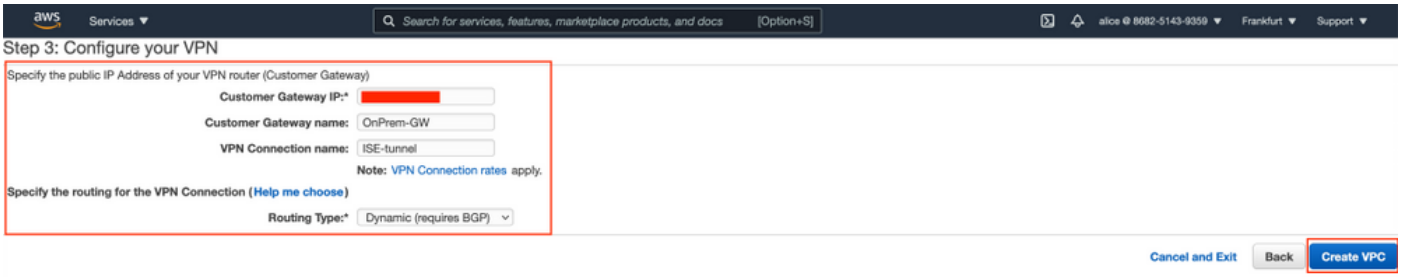


ملاحظة: يعتمد تحديد VPC في الخطوة 1. من معالج VPC على المخطط نظرا لأن ISE لم يتم تصميمه كخادم مكشوف عبر الإنترنت - يتم إستخدام VPN مع شبكة فرعية خاصة فقط.

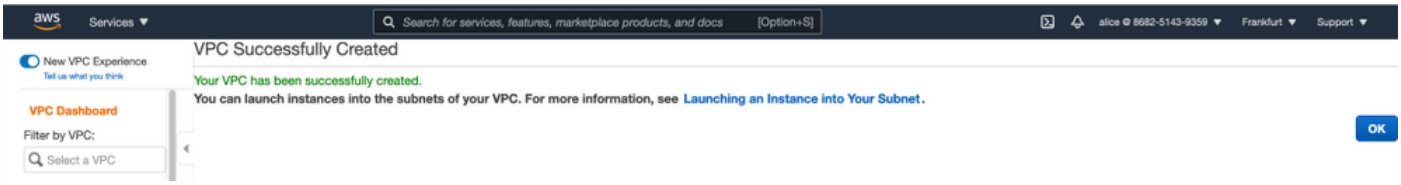
قم بتكوين إعدادات الشبكة الفرعية الخاصة بمعرف فئة المورد (VPC) وفقا لتصميم الشبكة لديك وحدد **التالي**.



قم بتكوين شبكة VPN الخاصة بك وفقا لتصميم الشبكة وحدد **إنشاء VPC**.

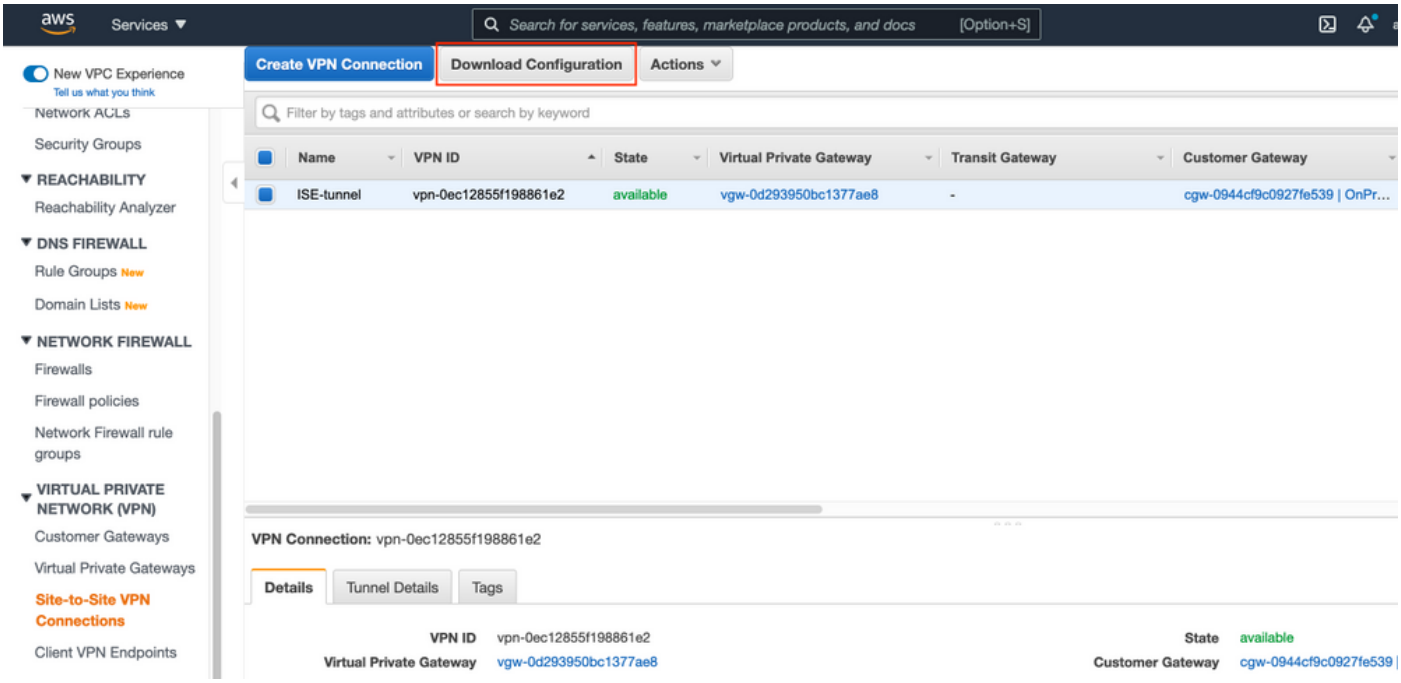


ما إن خلقت الـ VPC يكون، الرسالة **"ك VPC يتلقى يكون بنجاح خلقت"** عرضت. طقطقة **ok** كما هو موضح في الصورة.



الخطوة الاختيارية ب. تكوين جهاز وحدة الاستقبال والبث VPN على PREM

انتقل إلى خدمة AWS **الخاصة بمعرف فئة المورد (VPC)**. أختر **إتصالات VPN من موقع إلى موقع**، وحدد نفق VPN الذي تم إنشاؤه حديثا وحدد **تنزيل التكوين** كما هو موضح في الصورة.

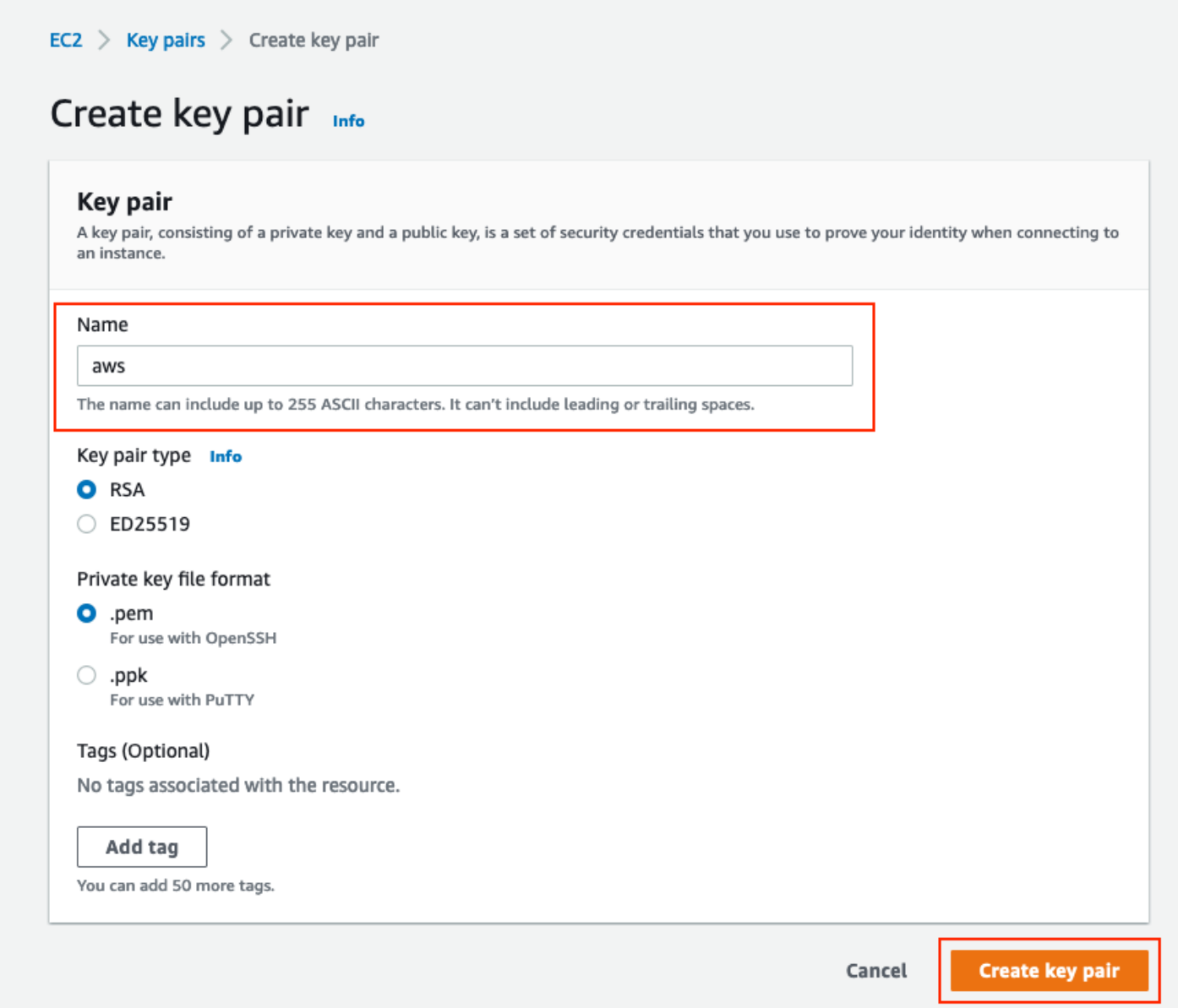


أخترت **باﺋع**، **منصة وبرمجيﺔ**، حدد **تنزيل** كما هو موضح في الصورة.

تطبيق التكوين الذي تم تنزيله على جهاز وحدة الاستقبال والبث الخاصة بشبكة VPN الداخلية.

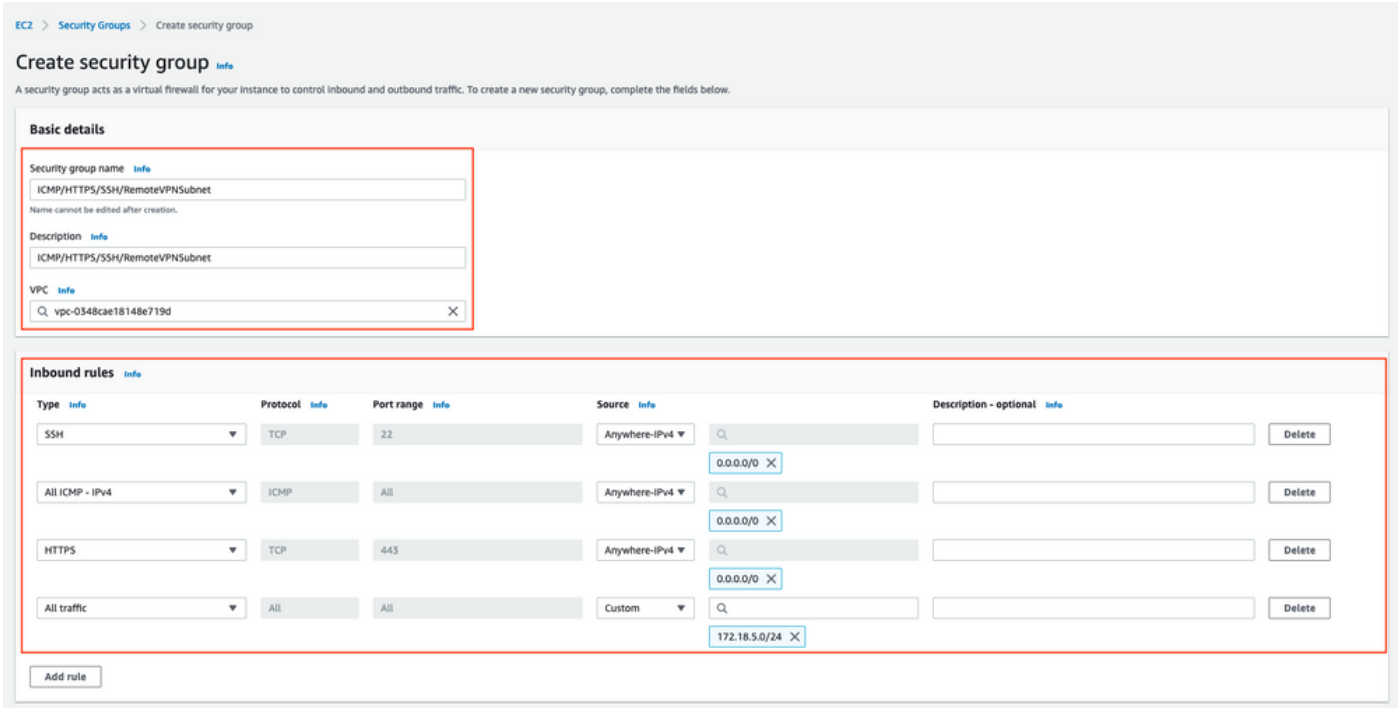
الخطوة C الاختيارية. إنشاء زوج مفاتيح مخصص

يتم الوصول إلى مثيلات AWS EC2 بمساعدة أزواج المفاتيح. لإنشاء زوج مفاتيح، انتقل إلى خدمة **EC2**. حدد قائمة **أزواج المفاتيح** تحت **الشبكة والأمان**. حدد **إنشاء زوج مفاتيح**، وأعطه **اسما**، واترك القيم الأخرى كقيمة افتراضية وحدد **إنشاء زوج مفاتيح** مرة أخرى.



الخطوة D الاختيارية. إنشاء مجموعة أمان مخصصة

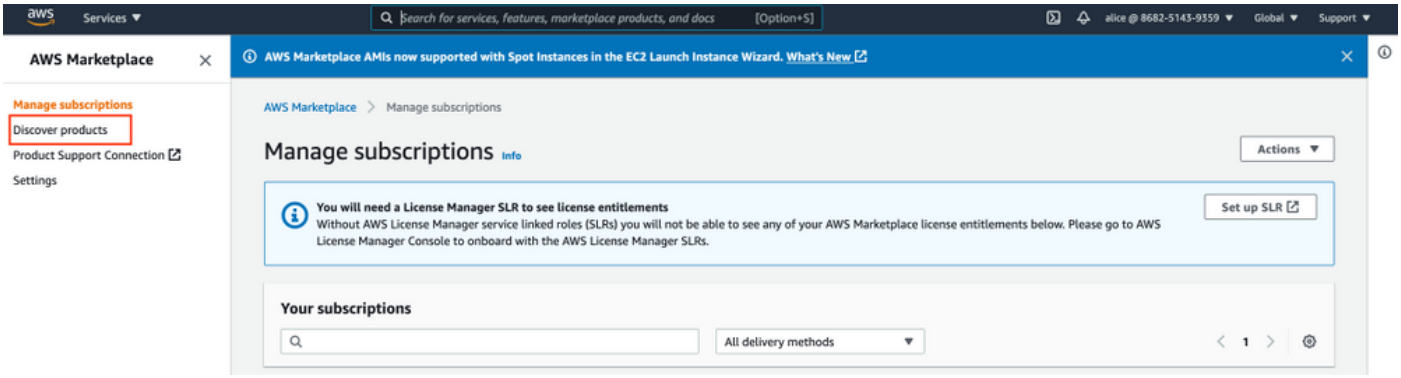
يتم حماية الوصول إلى مثيلات AWS EC2 بواسطة **مجموعات الأمان**، من أجل تكوين **مجموعة الأمان**، انتقل إلى خدمة **EC2**. حدد قائمة **مجموعات التأمين** تحت **الشبكة والأمان.** حدد إنشاء مجموعة أمان، تكوين **اسم**، **وصف،** في حقل **VPC** حدد VPC الذي تم تكوينه حديثا. قم بتكوين **قواعد الوارد** للسماح بالاتصال ب ISE. حدد **إنشاء مجموعة تأمين** كما هو موضح في الصورة.



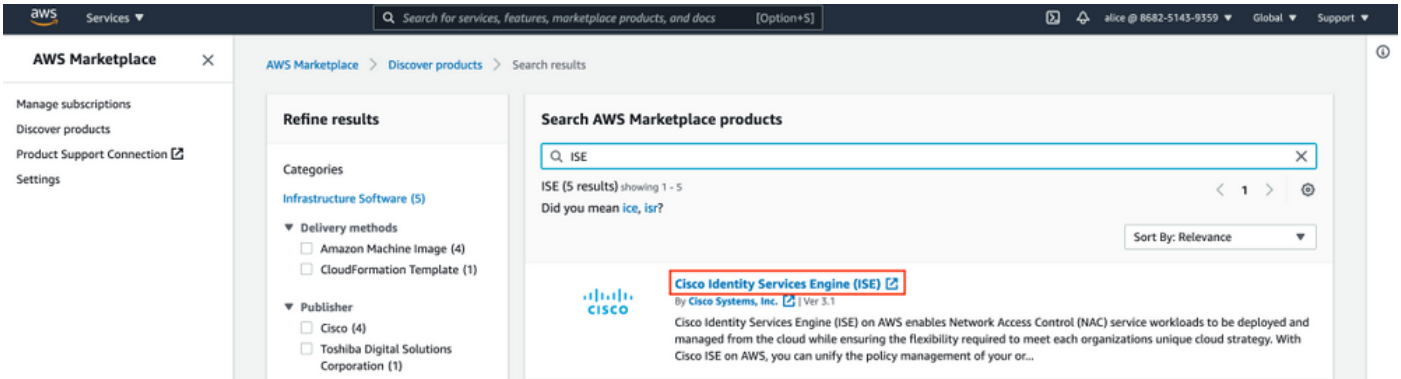
ملاحظة: تسمح مجموعة الأمان التي تم تكوينها بوصول SSH و ICMP و HTTPS إلى ISE والوصول إلى جميع البروتوكولات من الشبكة الفرعية على الخادم.

الخطوة 1. الاشتراك في منتج سوق AWS ISE

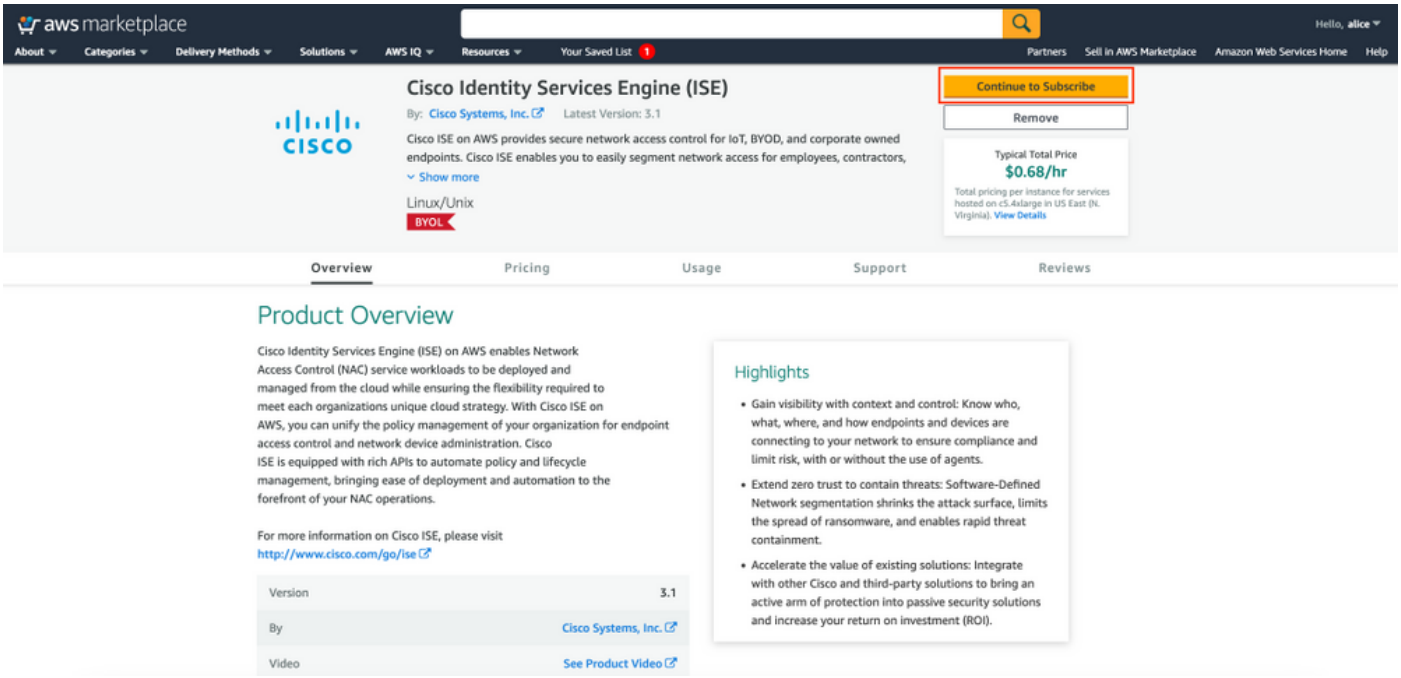
انتقل إلى خدمة AWS **الاشتراكات سوق AWS**. حدد **اكتشاف المنتجات** كما هو موضح في الصورة.



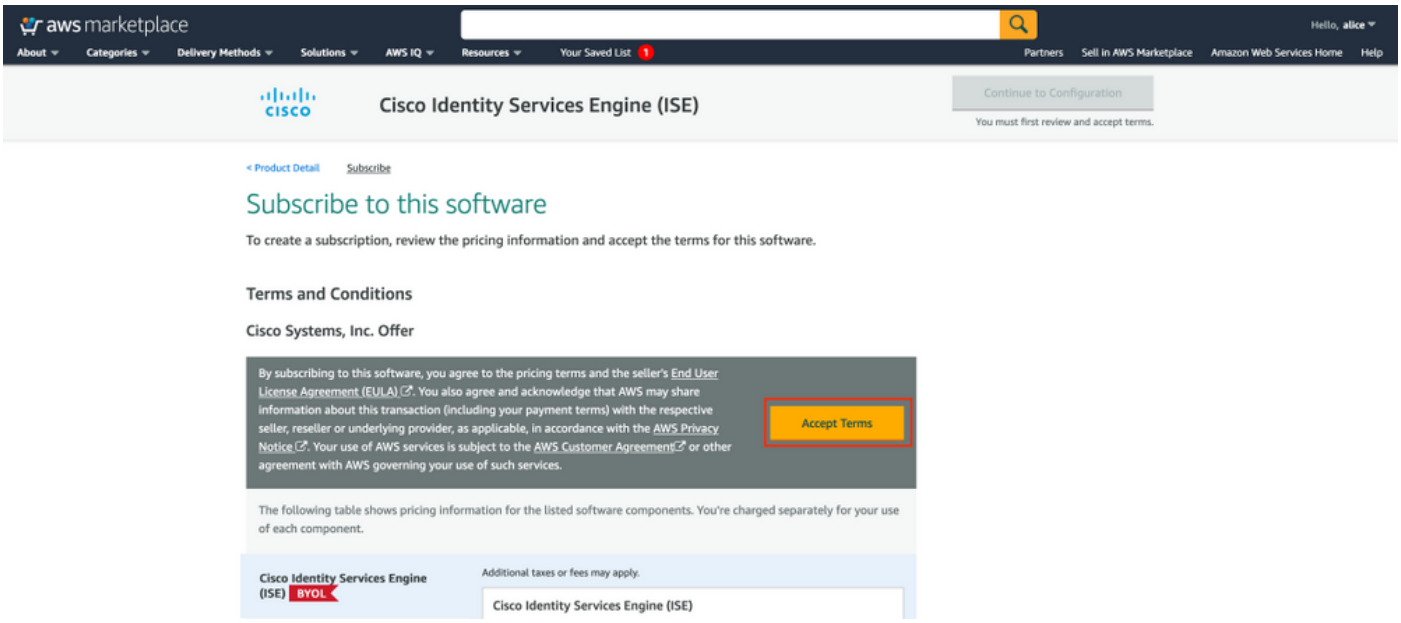
ابحث عن منتج **ISE** وحدد **محرك خدمات الهوية من Cisco (ISE)** كما هو موضح في الصورة.



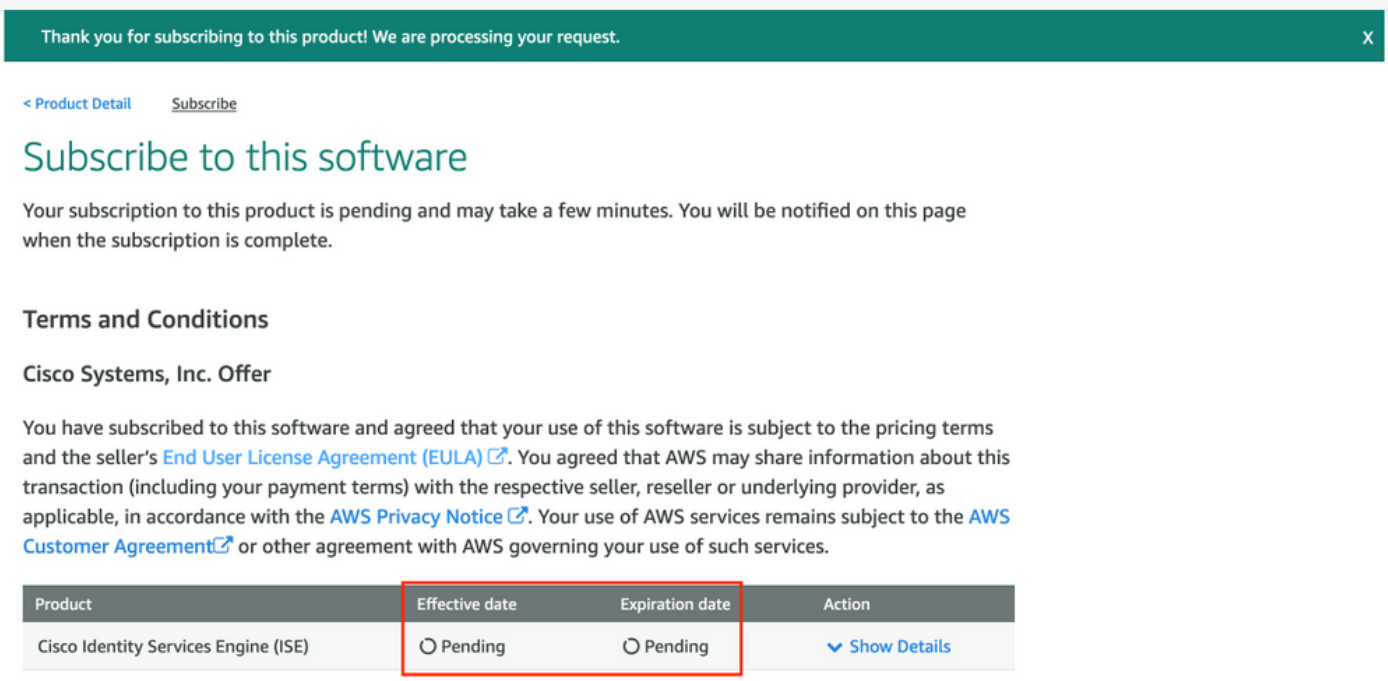
حدد الزر **متابعة الاشتراك**



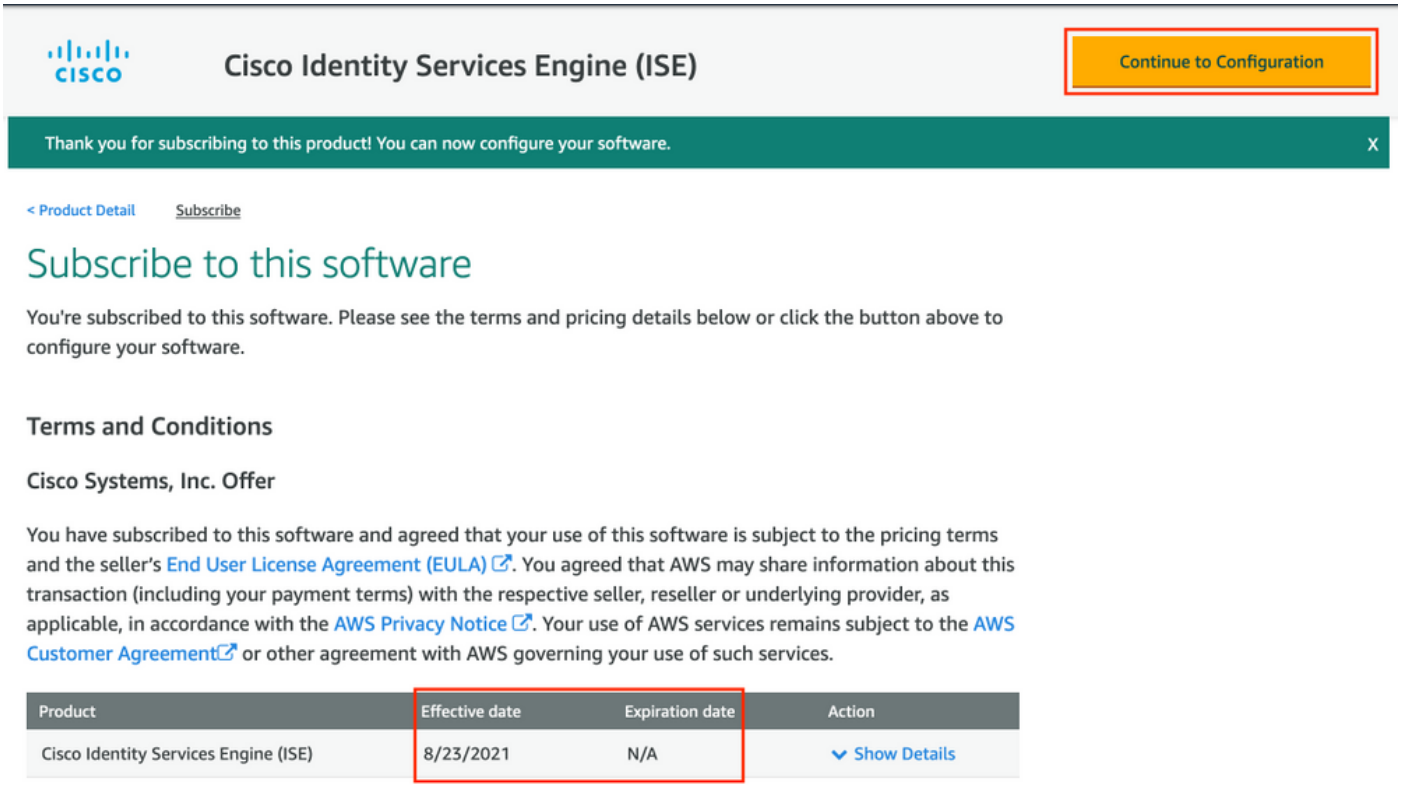
حدد زر **قبول الشروط** كما هو موضح في الصورة.



بمجرد الاشتراك في حالة **تاريخ السريان** و**تاريخ انتهاء الصلاحية** مع تغيير إلى **معلق** كما هو موضح في الصورة.

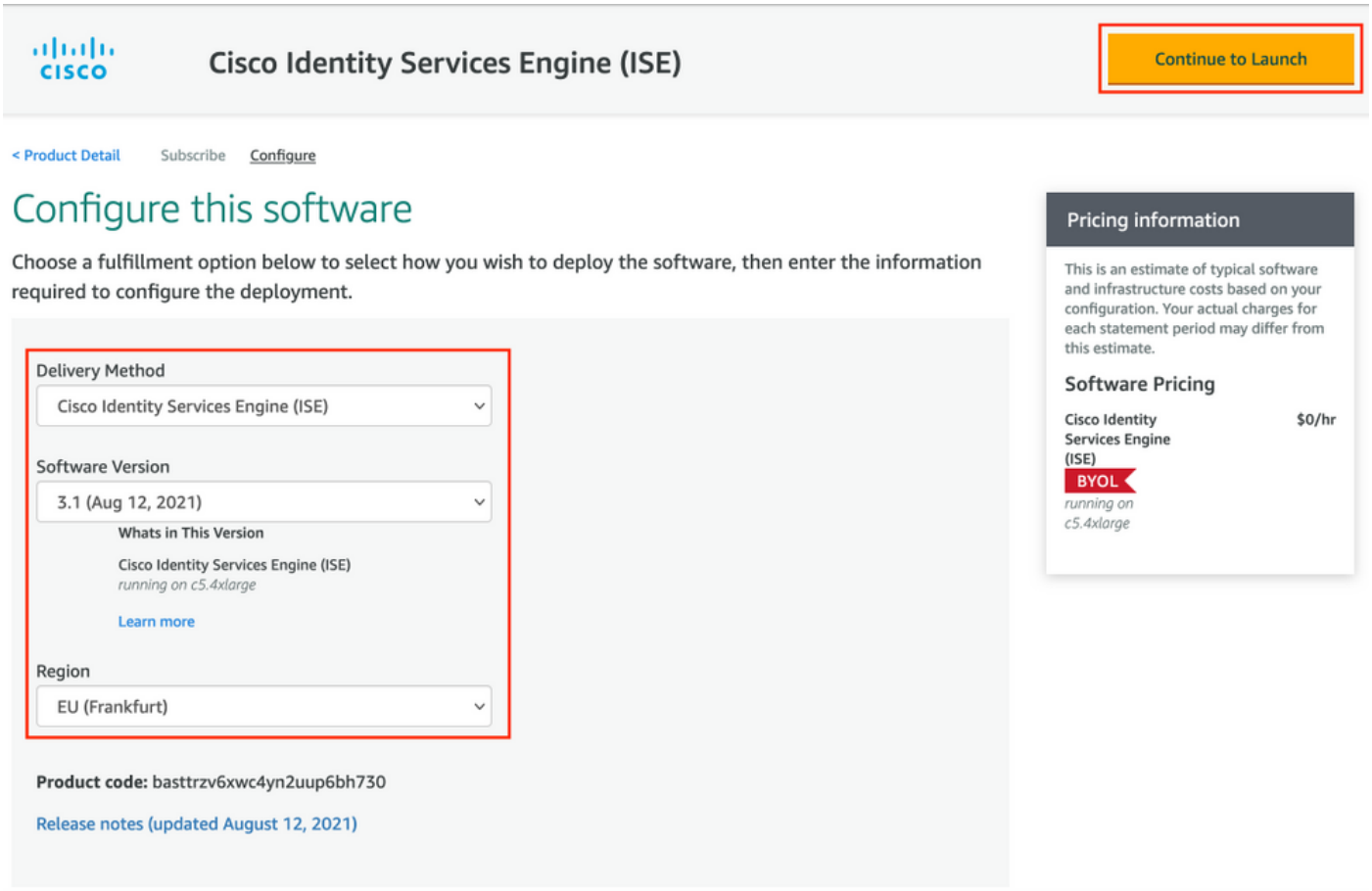


بعد وقت قصير من تغيير **تاريخ السريان** إلى تاريخ الاشتراك **وتغييرات تاريخ انتهاء الصلاحية** إلى N/A. حدد **متابعة التكوين** كما هو موضح في IMA



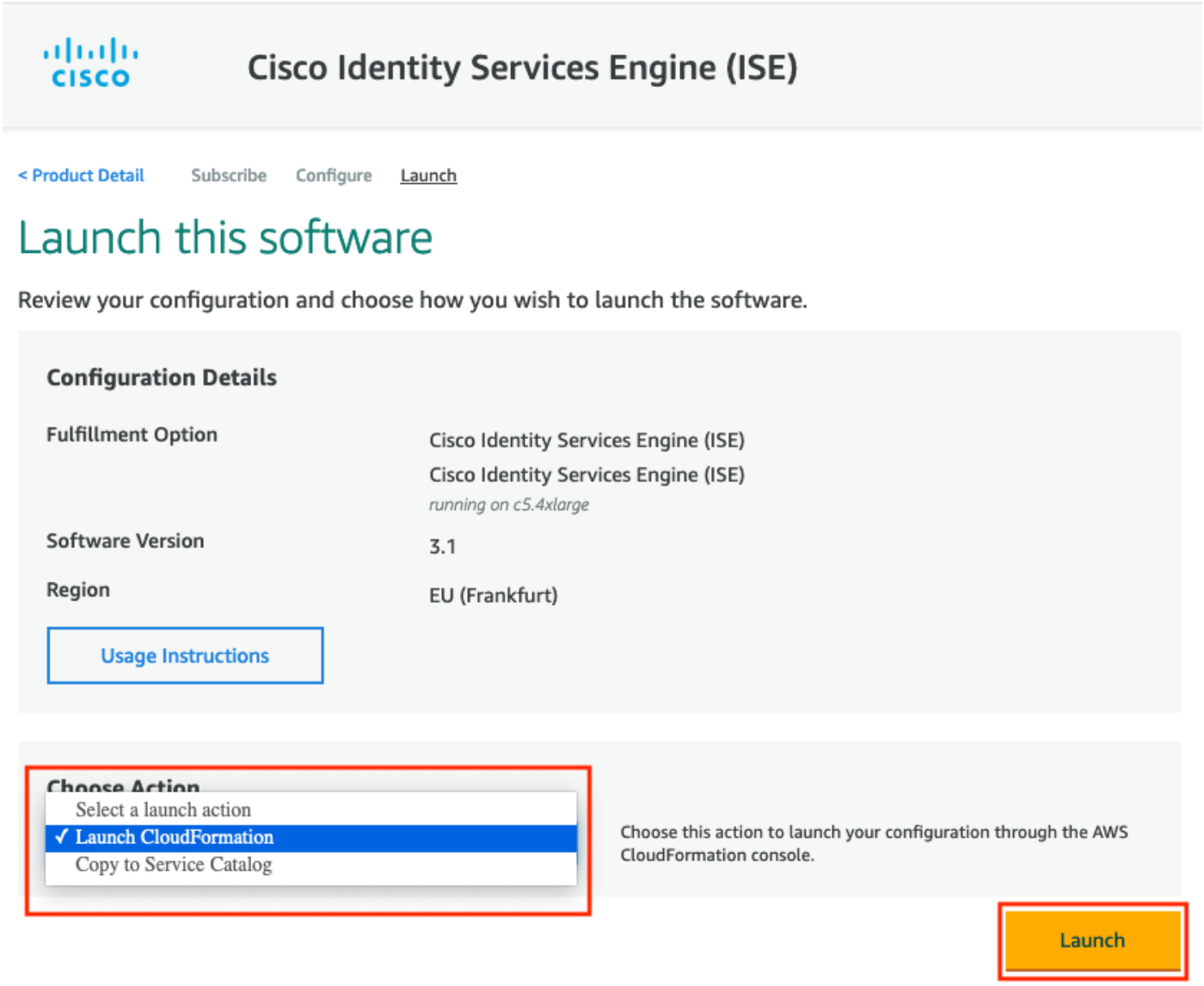
الخطوة 2. تكوين ISE على AWS

في قائمة طريقة التسليم من **شاشة تكوين هذا البرنامج**، حدد **محرك خدمات الهوية من Cisco (ISE)**. في **إصدار البرنامج**، حدد **3.1 (12 أغسطس 2021)**. حدد **المنطقة**، حيث تم تخطيط ISE لنشرها. حدد **متابعة التشغيل**.



الخطوة 3. تشغيل ISE على AWS

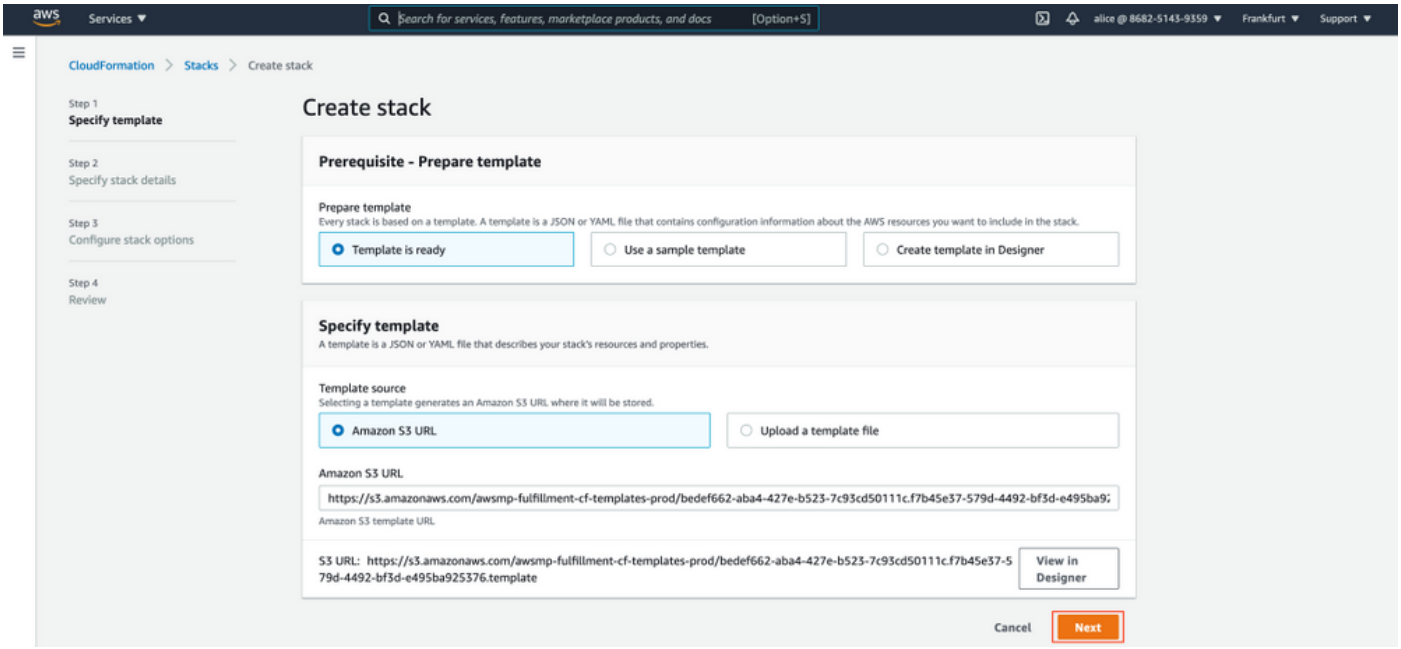
من قائمة الإجراءات المنسدلة من شاشة **تشغيل هذا البرنامج**، حدد **تشغيل CloudConfiguration**.



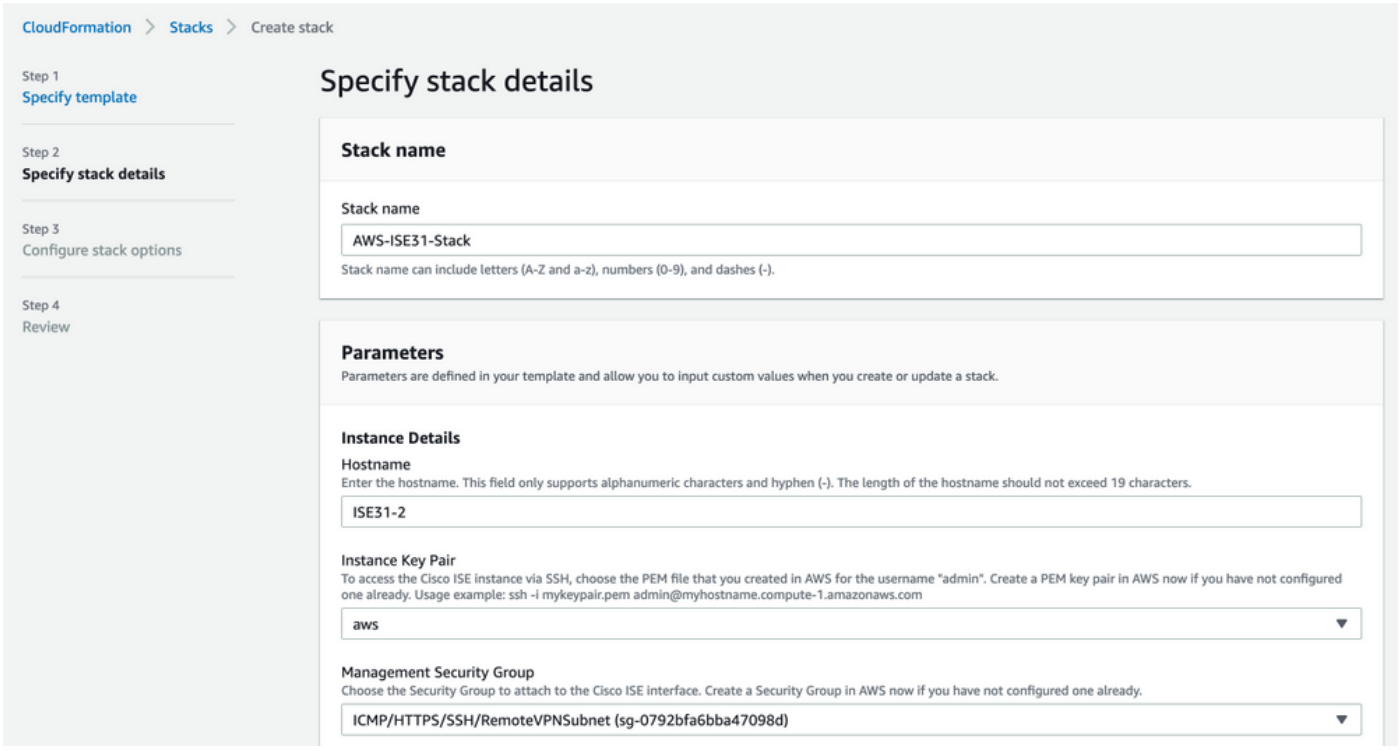
(إختياري) حدد **إرشادات الاستخدام** لتجعل نفسك على دراية بها. حدد **الإطلاق**.

الخطوة 4. تكوين مكدس CloudConfiguration ل ISE على AWS

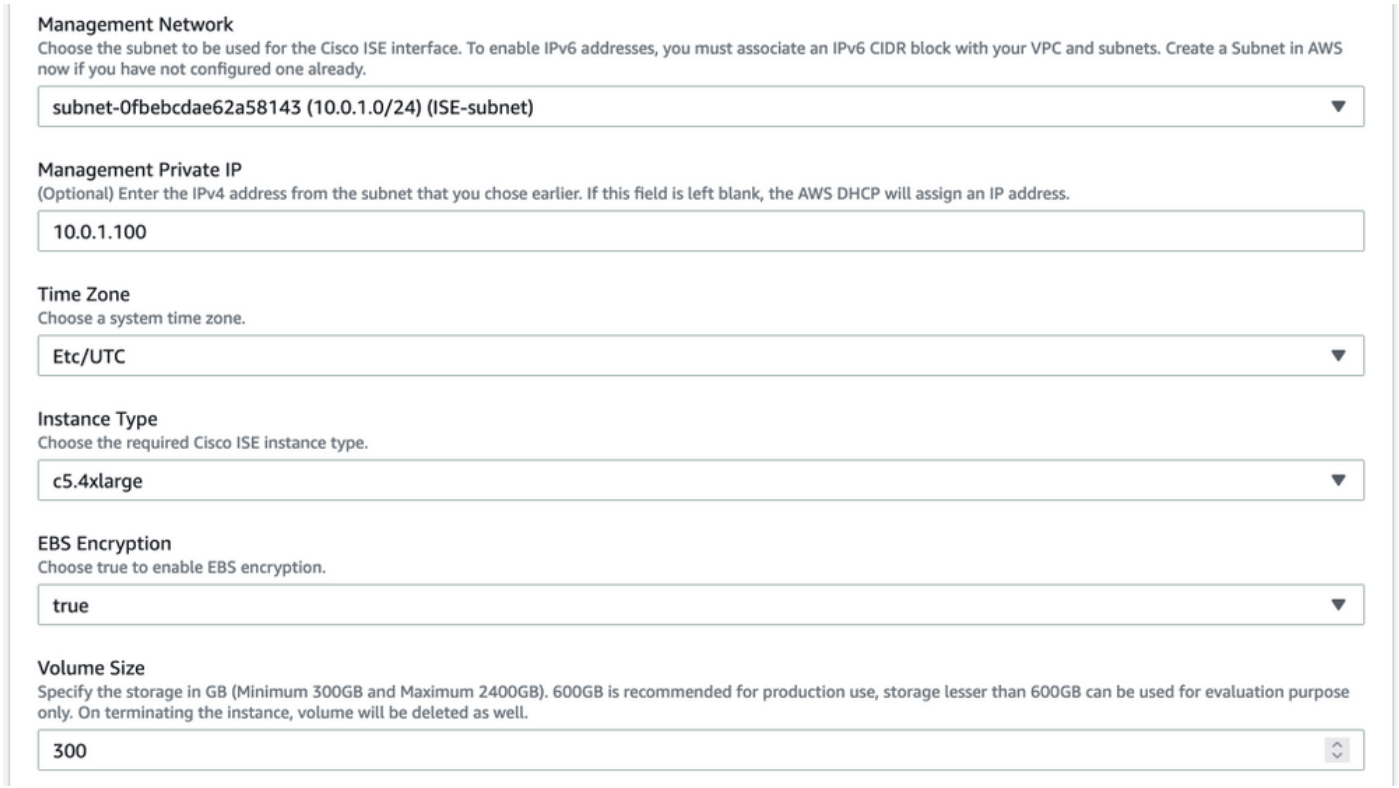
يقوم الزر **بدء التشغيل** بإعادة توجيهك إلى شاشة إعداد **مكدس** CloudConfiguration. هناك قالب تم إنشاؤه مسبقا يجب إستخدامه لإعداد ISE. احتفظ بالإعدادات الافتراضية وحدد **التالي**.



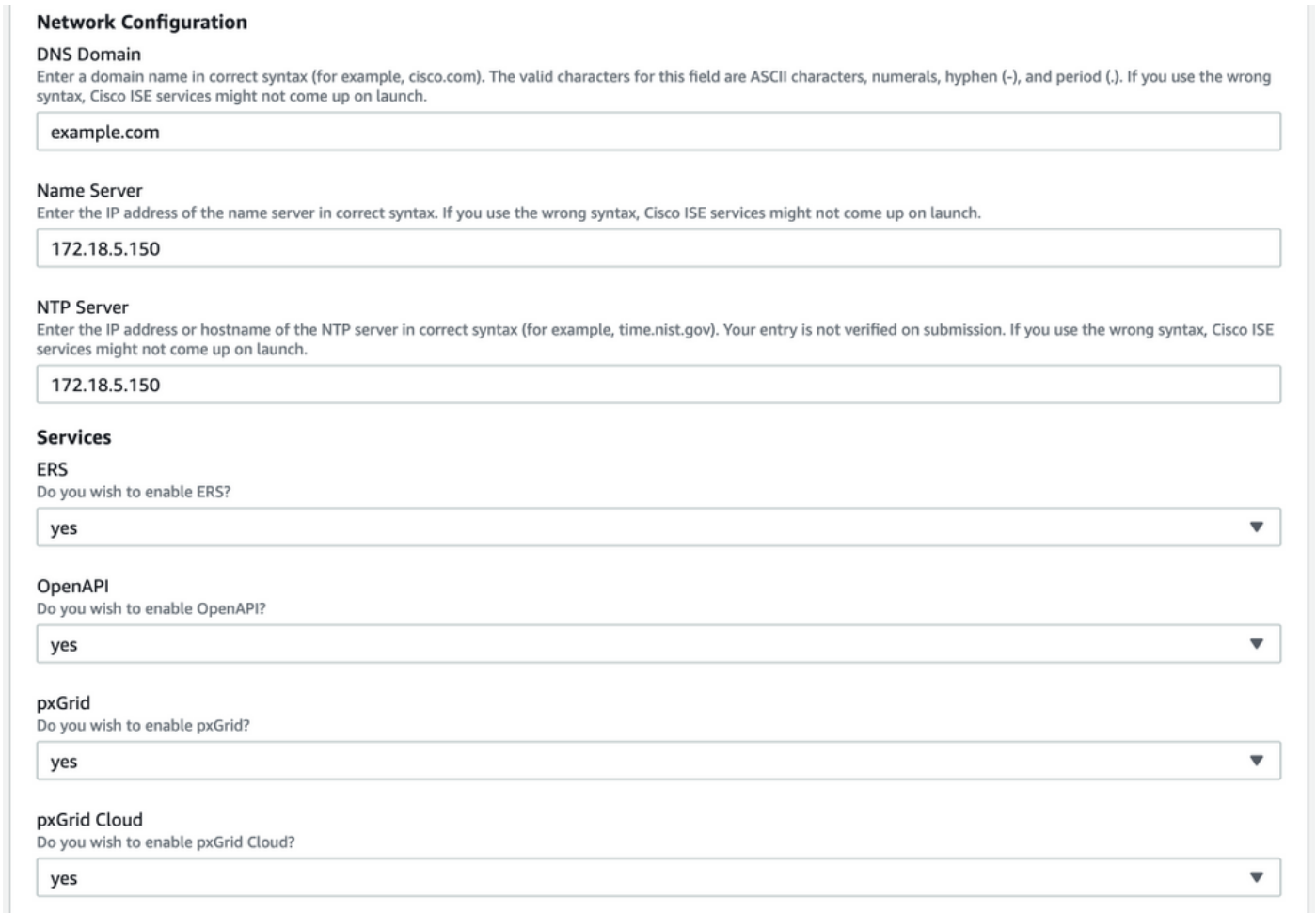
تعبئة بيانات مكدس CloudConfiguration باستخدام **اسم المكدس**. قم بتكوين تفاصيل المثيل مثل **hostname**، وحدد **زوج مفاتيح المثيل** و**مجموعة أمان الإدارة**.



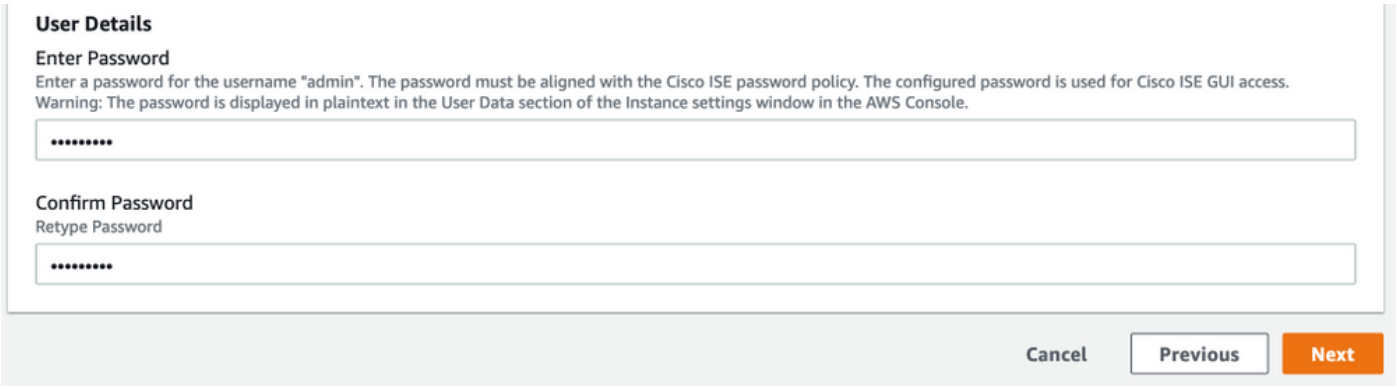
تابع تكوين تفاصيل المثيل باستخدام **شبكة الإدارة** و**IP الخاص بالإدارة** و**المنطقة الزمنية** و**نوع المثيل** و**تشفير EBS** و**حجم الحجم**.



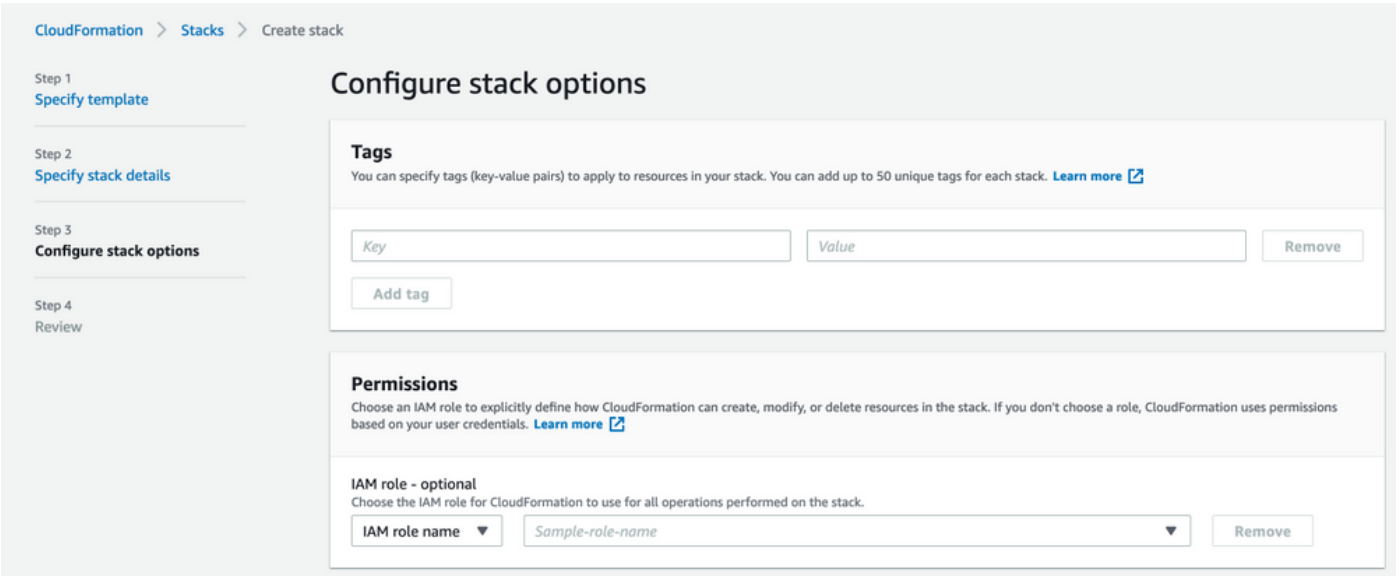
متابعة تكوين تفاصيل المثيل باستخدام **مجال DNS وخادم الاسم ومخدمة NTP والخدمات**.



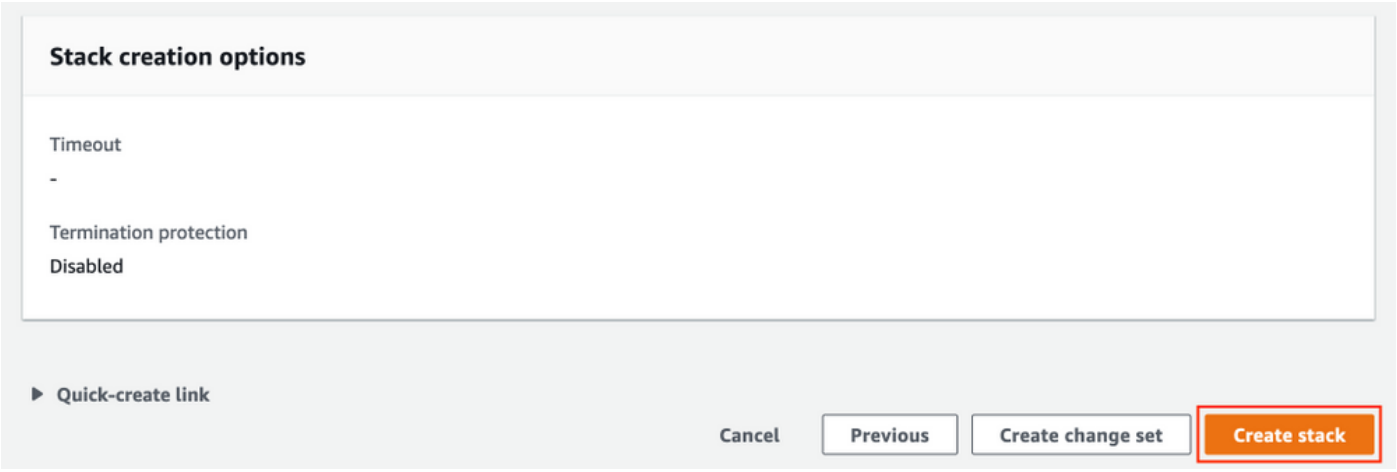
شكلت GUI مستعمل كلمة وحدد **بعد ذلك**.



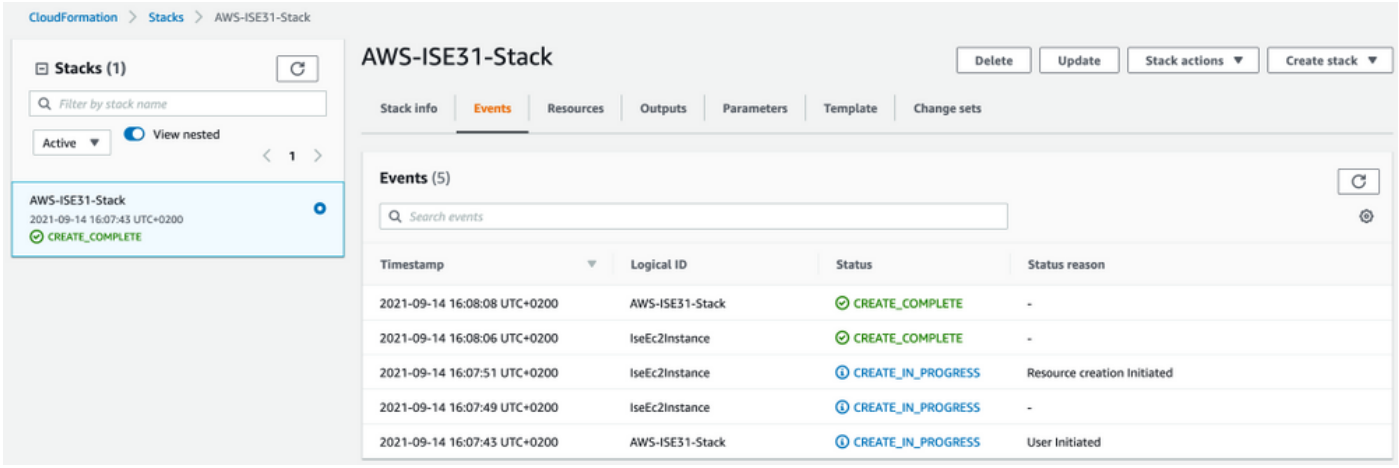
لا توجد تغييرات مطلوبة على الشاشة التالية. حدد **التالي**.



انتقل إلى شاشة **مراجعة المكدس**، وانتقل لأسفل وحدد **إنشاء مكدس**.

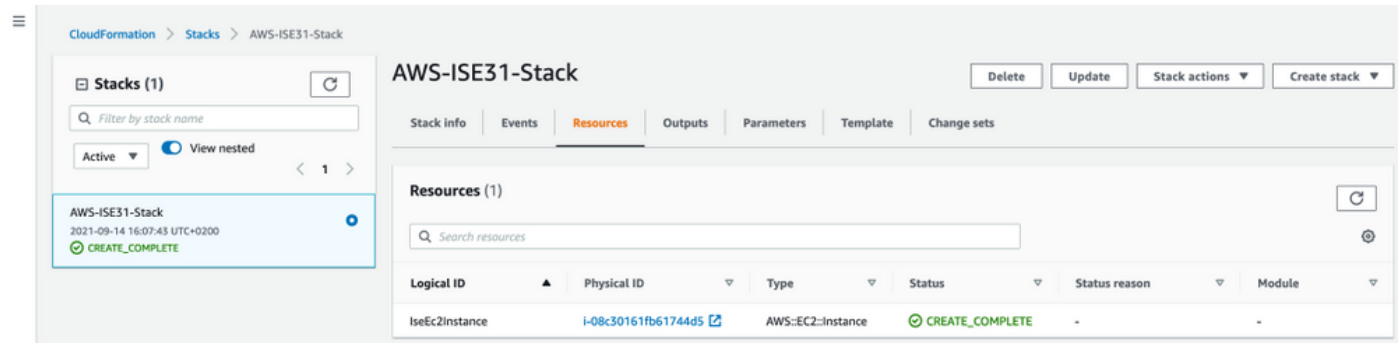


يجب عرض حالة CREATE_COMPLETE بمجرد نشر المكدس.

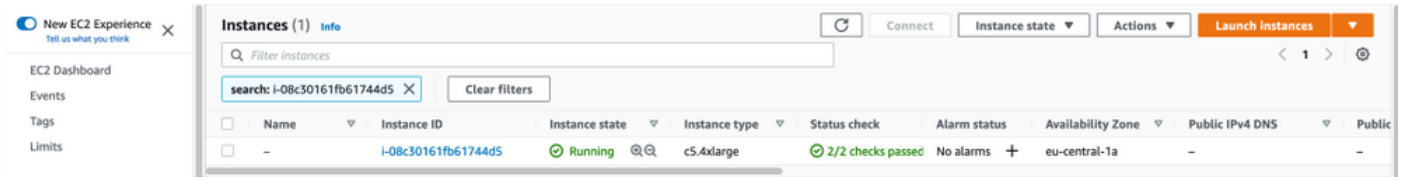


الخطوة 5. الوصول إلى ISE على AWS

للوصول إلى مثيل ISE، انتقل إلى علامة التبويب **الموارد** لعرض مثيل EC2 الذي تم إنشاؤه من CloudForms (بدلاً من ذلك انتقل إلى **الخدمات > EC2 > المثيلات** لعرض مثيلات EC2) كما هو موضح في الصورة.



حدد **معرف فعلي** لفتح قائمة **مثيلات EC2**. تأكد من أن **فحص الحالة** به **2/2 من عمليات التحقق التي تم تمريرها**.



حدد **معرف المثيل**. يمكن الوصول إلى ISE عبر **عنوان IPv4 الخاص/DNS الخاص للإصدار الرابع من بروتوكول الإنترنت (IP)** مع بروتوكول SSH أو HTTPS.

> **ملاحظة**: إذا قمت بالوصول إلى ISE عبر **عنوان IPv4 الخاص/IPv4 DNS الخاص** فتأكد من وجود اتصال شبكة باتجاه عنوان ISE الخاص.

مثال على ISE الذي يتم الوصول إليه عبر **عنوان IPv4 الخاص** عبر SSH:

```
[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#
```

ملاحظة: يستغرق الوصول إلى مزيج حرف الأرقام الثابتة (ISE) عبر بروتوكول SSH حوالي 20 دقيقة. وحتى ذلك الوقت، يفشل الاتصال بـ ISE مع رسالة الخطأ **إذن مرفوض (publicKey)**.

أستخدم **عرض حالة التطبيق** للتحقق من تشغيل الخدمات:

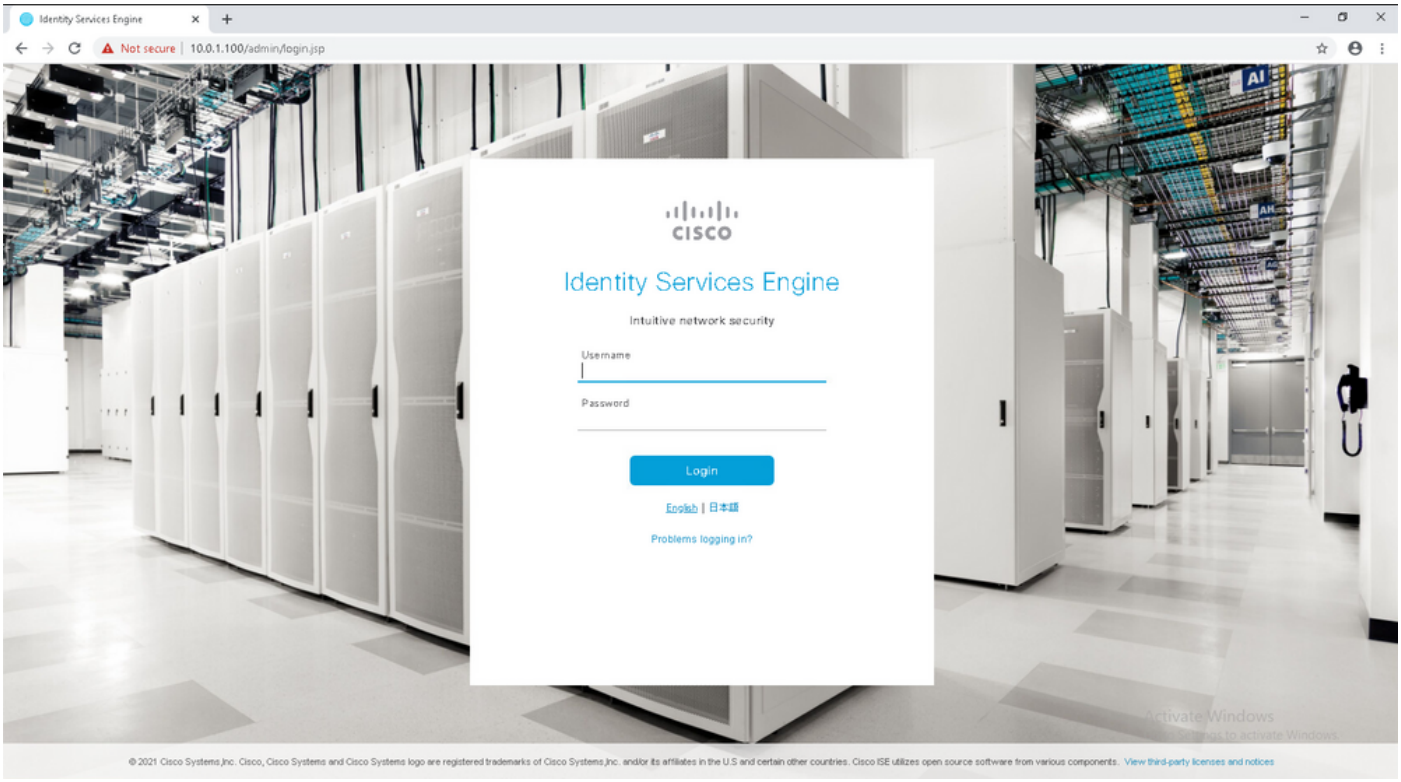
```
ISE31-2/admin# show application status ise

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#
```

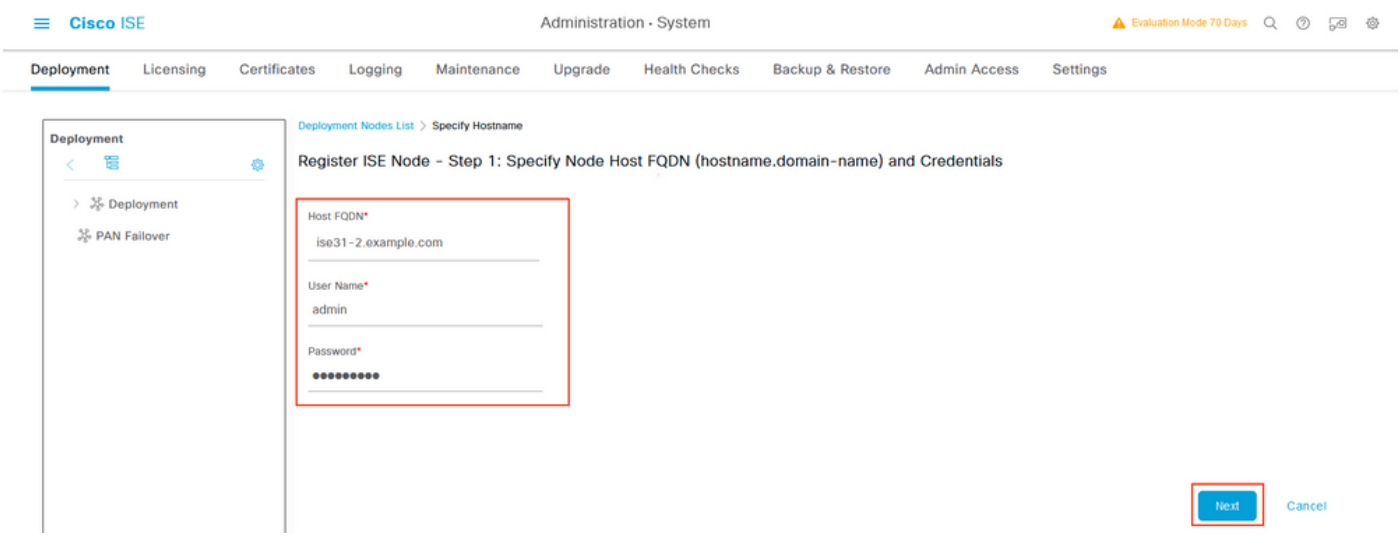
ملاحظة: يستغرق الأمر من 10 إلى 15 دقيقة بعد توفير بروتوكول SSH لخدمات ISE للانتقال إلى حالة التشغيل.

بمجرد أن يكون **التطبيق قيد التشغيل**، يمكنك الوصول إلى ISE عبر واجهة المستخدم الرسومية (GUI) كما هو موضح في الصورة.

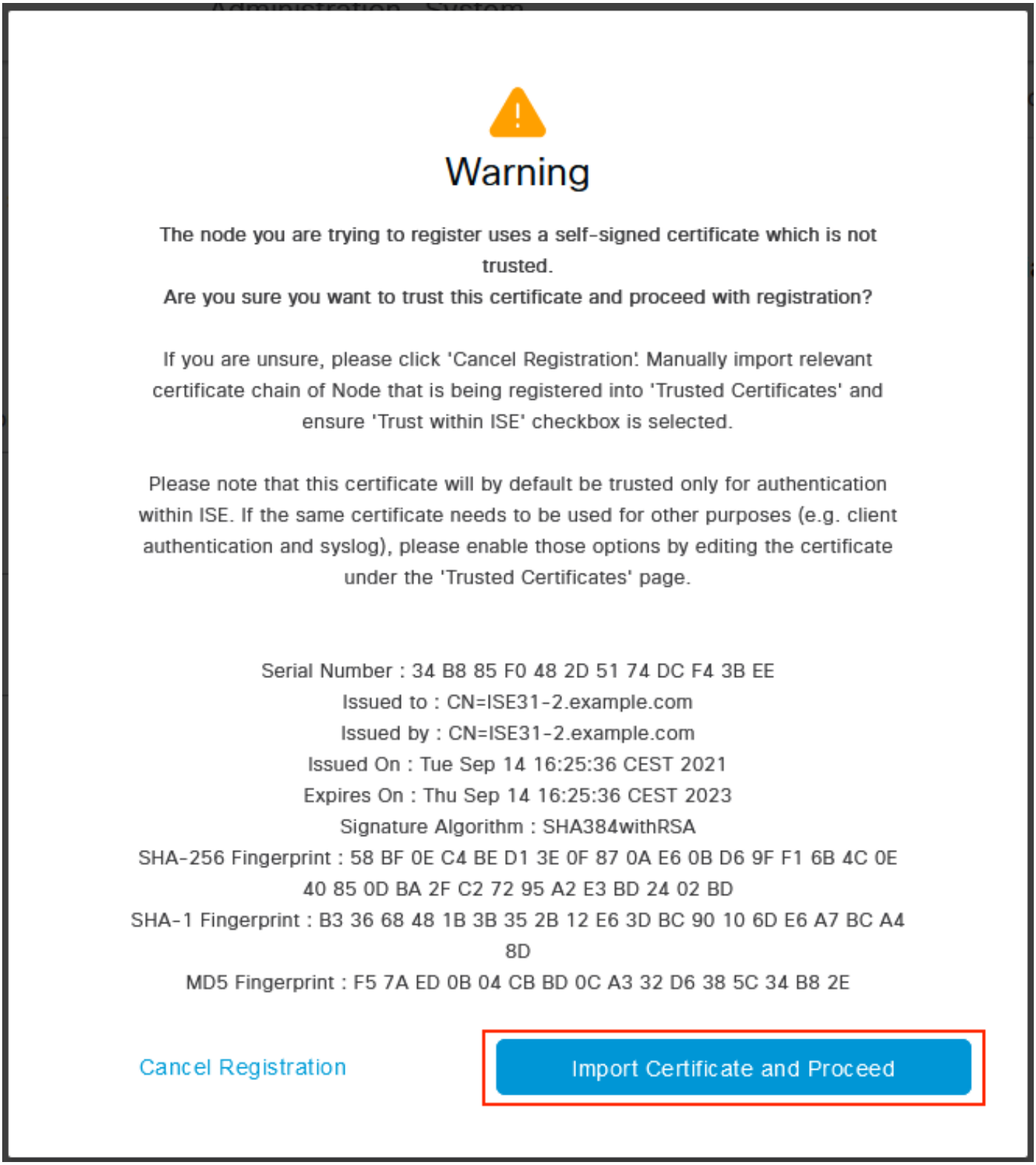


الخطوة 6. تكوين النشر الموزع بين ISE و ISE على AWS

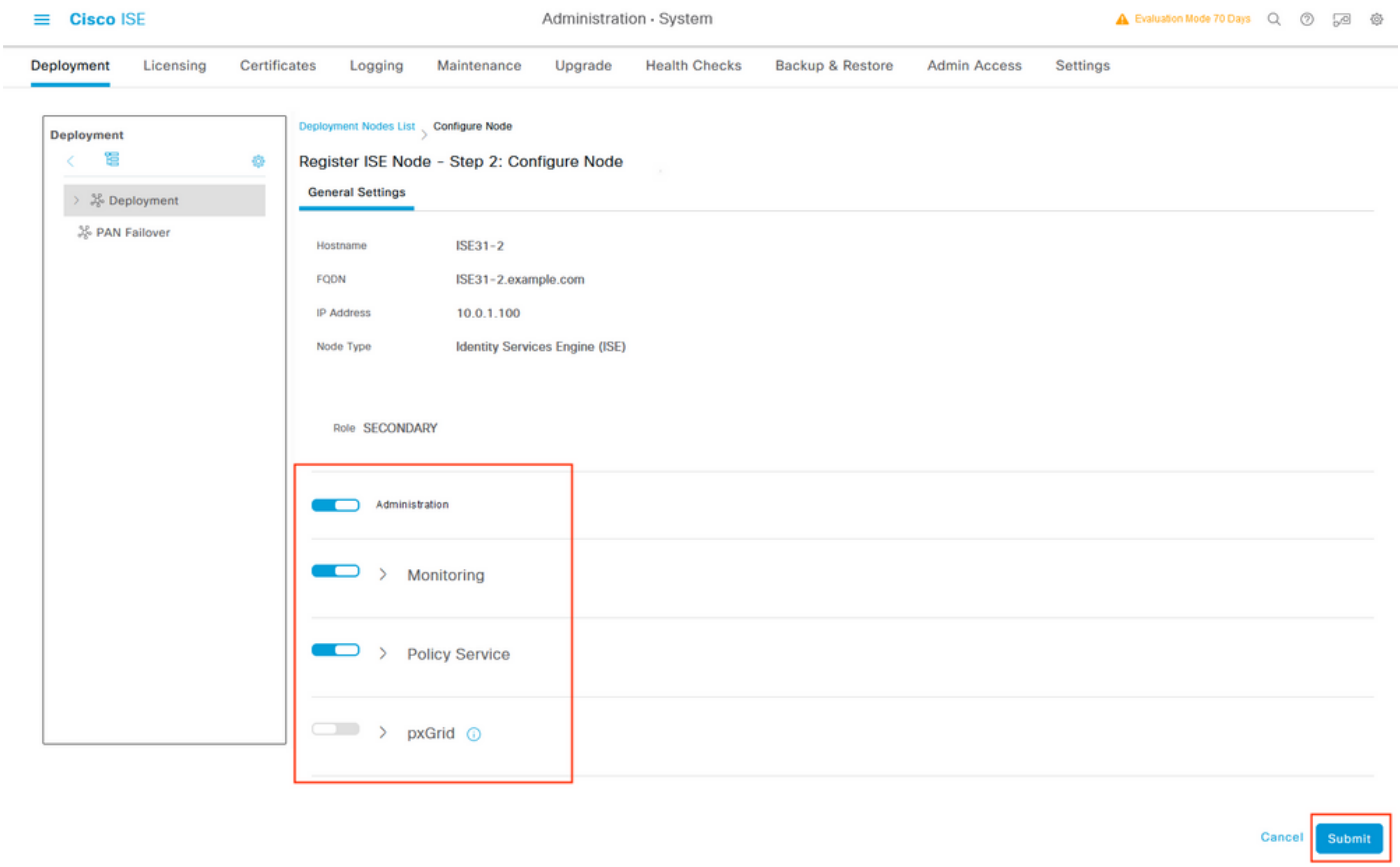
قم بتسجيل الدخول إلى ISE على الإعداد وانتقل إلى **الإدارة > النظام > النشر.** حدد العقدة وحدد **إجراء أساسي. انتقل مرة أخرى إلى الإدارة > النظام > النشر**، حدد **التسجيل**. تكوين **FQDN المضيف** من ISE على AWS، **اسم مستخدم** واجهة المستخدم الرسومية (GUI) **وكلمة المرور.** انقر فوق Next (التالي).



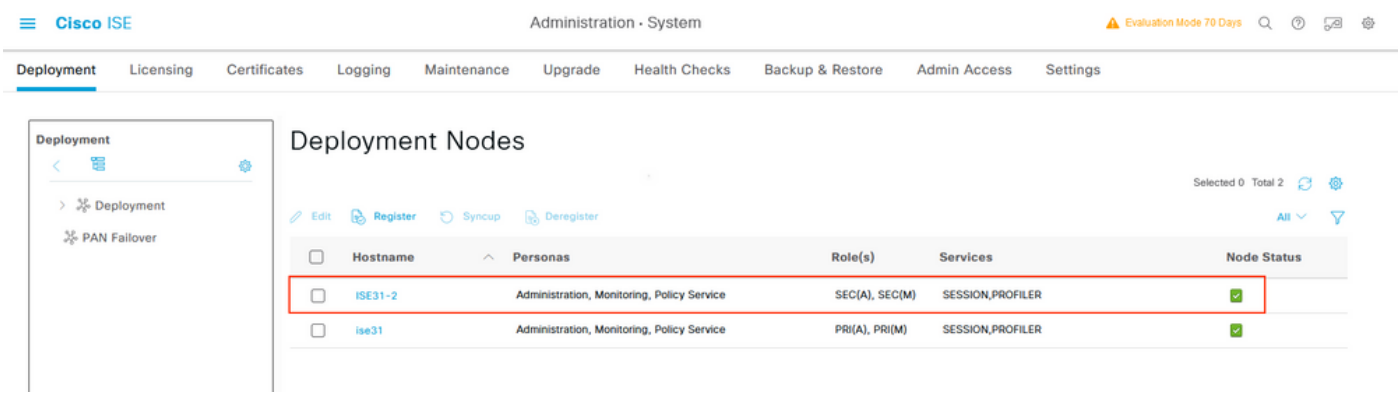
بما أن الشهادات الموقعة ذاتيا يتم إستخدامها في هذا المخطط، فإن إستيراد شهادات المسؤول إلى المخزن الموثوق به يحدد **إستيراد شهادة ويباشر.**



حدد الشخصيات التي تختارها وانقر فوق **إرسال**.

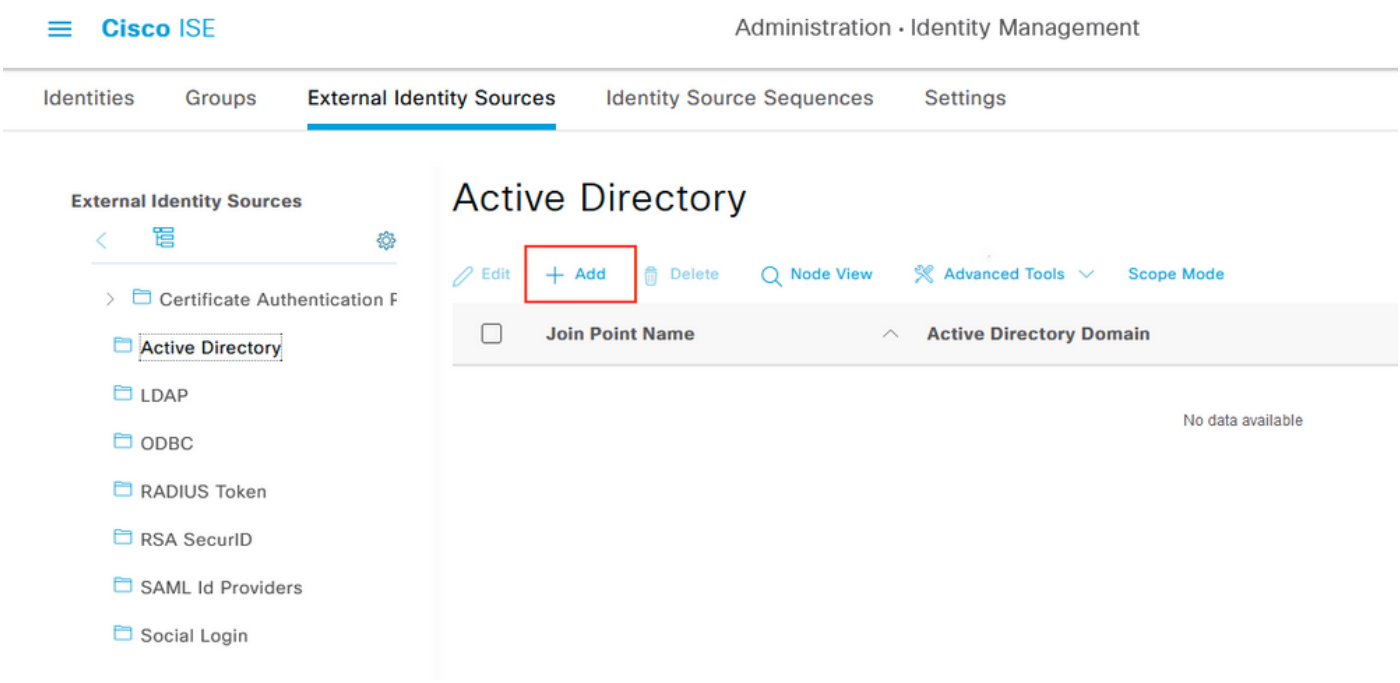


بمجرد اكتمال المزامنة، تنتقل العقدة إلى الحالة المتصلة، يتم عرض خانة الاختيار الخضراء مقابلها.

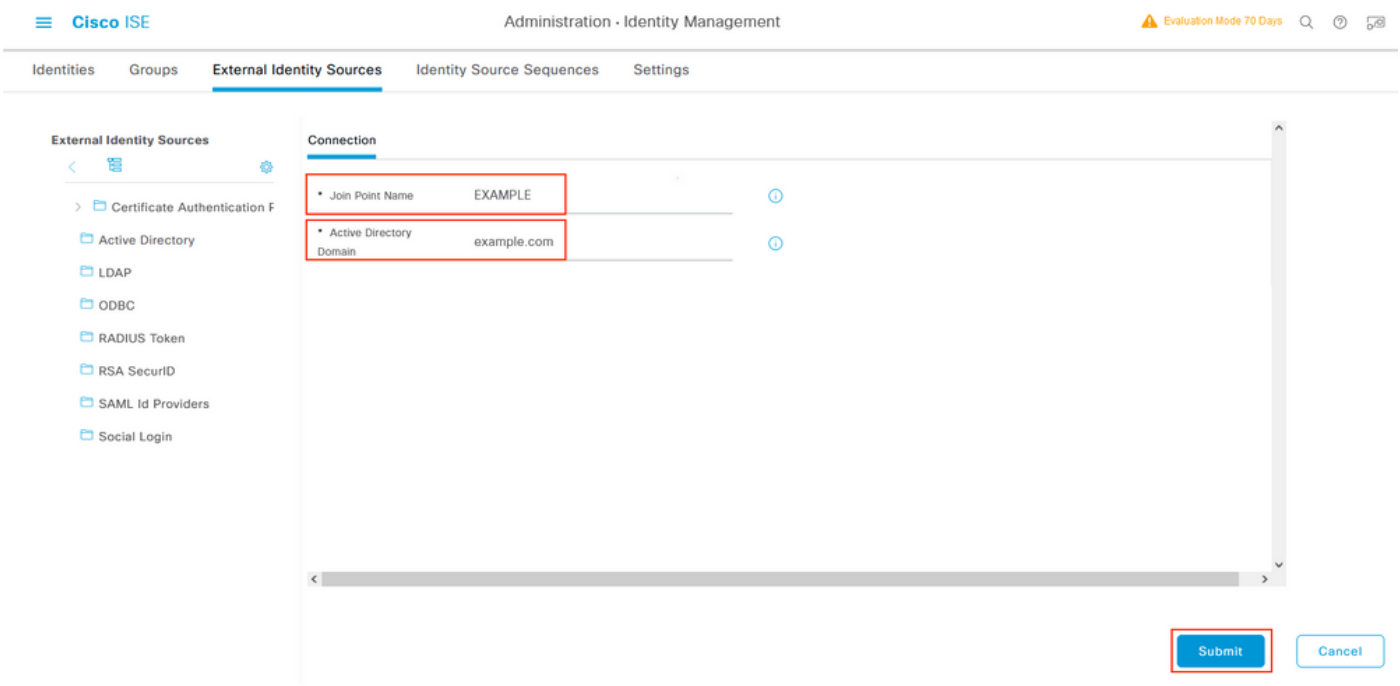


الخطوة 7. دمج نشر ISE مع AD على الجاهزية

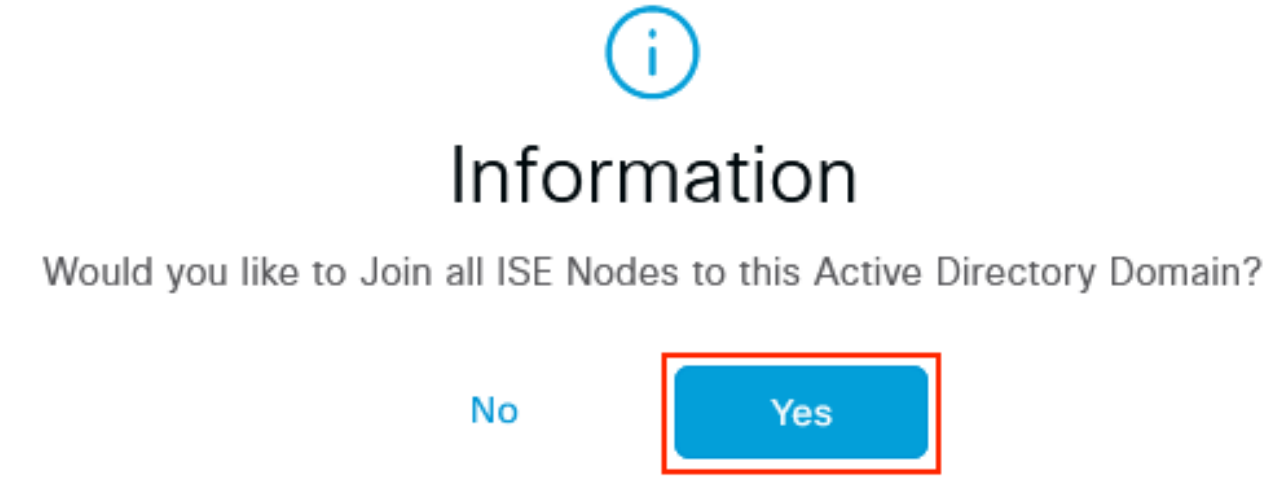
انتقل إلى **إدارة > إدارة الهوية > مصادر الهوية الخارجية**. حدد **Active Directory**، حدد **Add**.



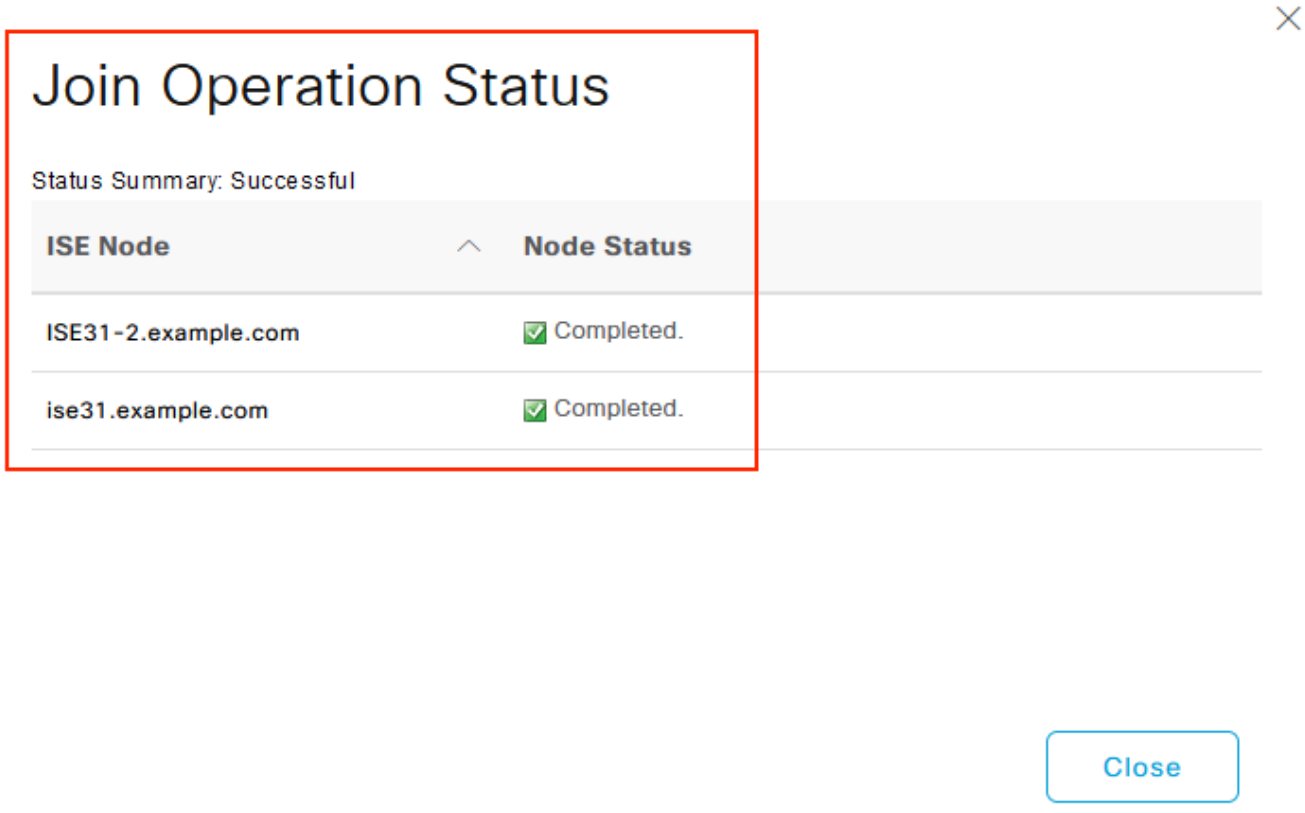
قم بتكوين **اسم النقطة المشتركة ومجال Active Directory**، حدد **إرسال**.



لتكامل كل العقد مع Active Directory، حدد **نعم**.



دخلت **إعلان مستعمل إسم** وكلمة **مرور**، طقطقت **ok**. بمجرد دمج عقد ISE بنجاح مع Active Directory، يتم إكمال تغييرات حالة العقدة.



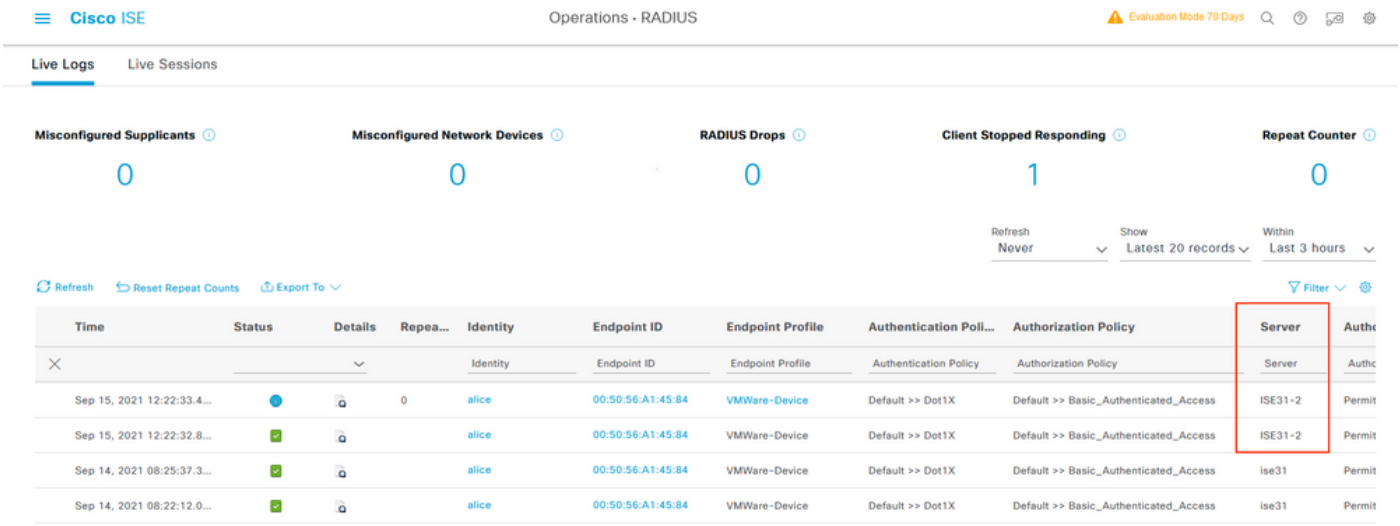
القيود

للحصول على قيود ISE على AWS، يرجى الرجوع إلى قسم [المحددات المعروفة](#) في دليل مسؤول ISE.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من تنفيذ المصادقة على ISE PSN الموجود على AWS، انتقل إلى **العمليات > Radius > السجلات المباشرة**، وتأكد في **عمود الخادم** ISE على AWS PSN.

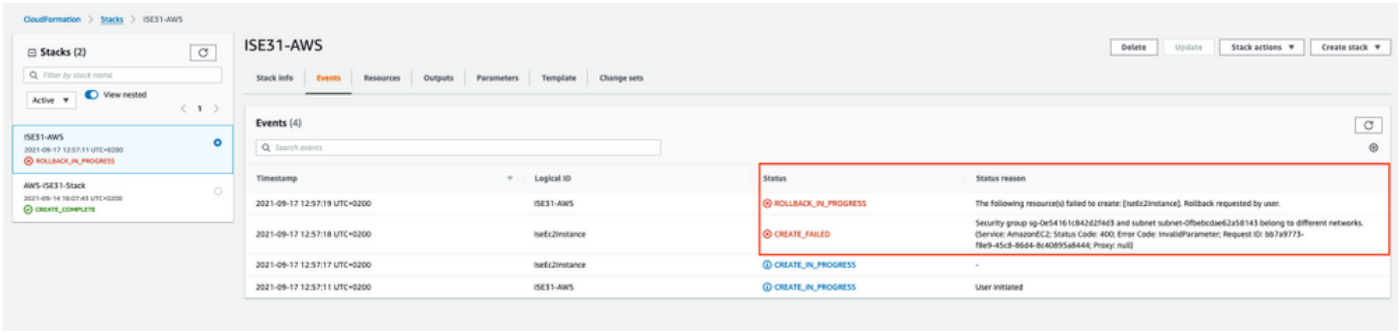


استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فشل إنشاء مكدس CloudConfiguration

يمكن أن يفشل إنشاء مكدس CloudConfiguration بسبب أسباب متعددة، أحدها عندما تحدد مجموعة الأمان هذه من شبكة VPN المختلفة عن شبكة إدارة ISE. يبدو الخطأ كالخطأ الموجود في الصورة.



الحل:

تضمنت أن ينتقي مجموعة الأمان من ال نفس VPC. انتقل إلى **مجموعات الأمان** ضمن **خدمة VPC** ، ولاحظ **معرف مجموعة الأمان**، وتأكد من مطابقته لمعرف مجموعة الأمان (VPC) الأيمن (حيث يقيم ISE)، تحقق من معرف **VPC**.

مشكلات الاتصال

قد تكون هناك مشاكل متعددة قد تتسبب في عدم عمل الاتصال ب ISE على AWS.

1. مشكلة الاتصال بسبب تكوين **مجموعات الأمان** بشكل غير صحيح.

الحل: ال يمكن الوصول إلى ISE من شبكة On-PREM أو حتى داخل شبكات AWS إذا تم تكوين **مجموعات الأمان** بشكل غير صحيح. تأكد من السماح بالبروتوكولات والمنافذ المطلوبة في **مجموعة الأمان** المرتبطة بشبكة ISE. ارجع إلى مرجع منافذ ISE للمنافذ المطلوبة التي سيتم فتحها.

2. مشكلات الاتصال الناجمة عن التوجيه غير المكون بشكل صحيح.

الحل: نظرا لتعقيد المخطط، من السهل فقد بعض المسارات بين شبكة On-Prem و AWS. قبل أن تتمكن من إستخدام ميزات ISE، تأكد من وجود اتصال شامل.

الملحق

التكوين المرتبط بالمحول AAA/RADIUS

```
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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).