

Configurazione di ISE 3.1 con AWS Marketplace

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Topologia della rete](#)

[Configurazioni](#)

[Passaggio opzionale A. Creazione di VPC](#)

[Passaggio B facoltativo. Configurare il dispositivo headend VPN locale](#)

[Passaggio C facoltativo. Creare una coppia di chiavi personalizzata](#)

[Passaggio facoltativo D. Creazione di un gruppo di sicurezza personalizzato](#)

[Passaggio 1. Iscriviti al prodotto AWS ISE Marketplace](#)

[Passaggio 2. Configurare ISE su AWS](#)

[Passaggio 3. Lanciare ISE su AWS](#)

[Passaggio 4. Configurazione dello stack di formazione del cloud per ISE su AWS](#)

[Passaggio 5. Accedere ad ISE su AWS](#)

[Passaggio 6. Configurare la distribuzione tra ISE locale e ISE su AWS](#)

[Passaggio 7. Integrare l'implementazione ISE con Active Directory in sede](#)

[Limitazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Creazione stack CloudFormation non riuscita](#)

[Problemi di connettività](#)

[Appendice](#)

[Configurazione correlata allo switch AAA/Radius](#)

Introduzione

Questo documento descrive come installare Identity Services Engine (ISE) 3.1 tramite Amazon Machine Images (AMI) in Amazon Web Services (AWS). Dalla versione 3.1 ISE può essere distribuito come istanza di Amazon Elastic Compute Cloud (EC2) con l'aiuto di CloudFormation Templates (CFT).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- ISE

- AWS e i suoi concetti come VPC, EC2, CloudFormation

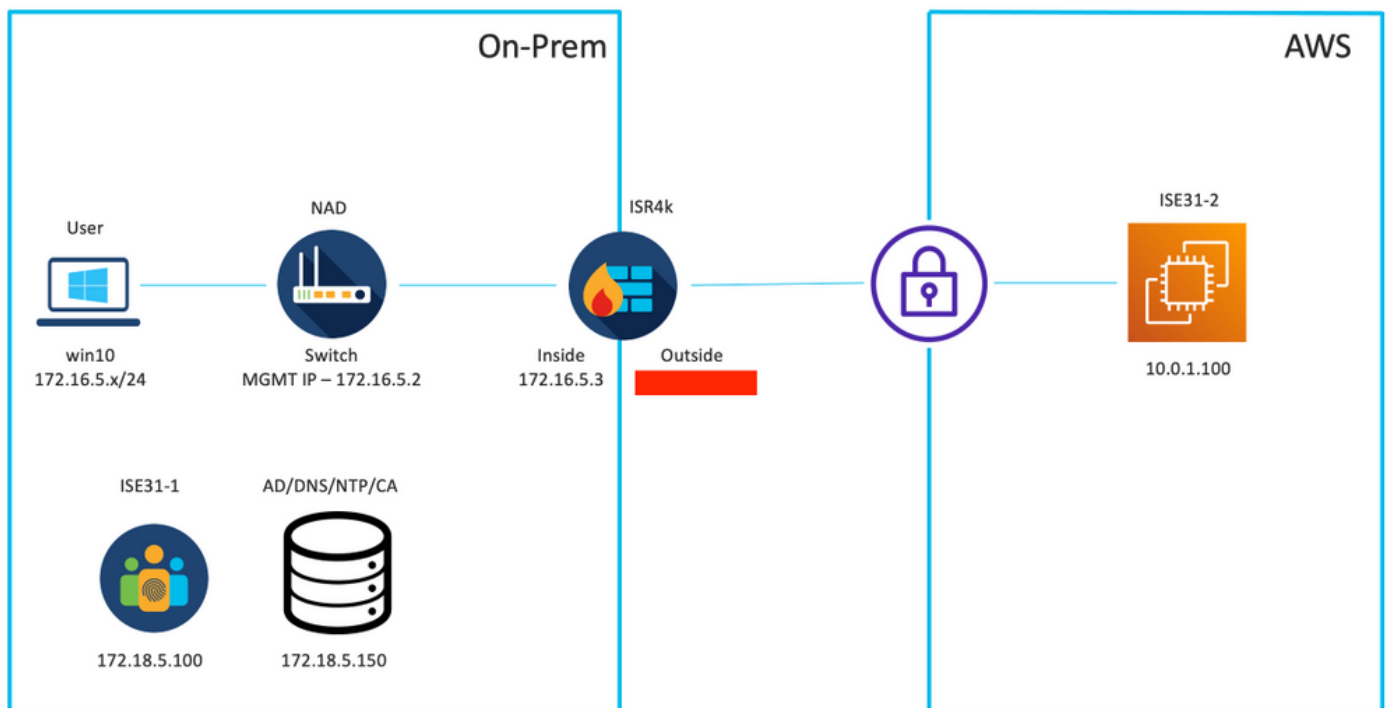
Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco ISE versione 3.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Topologia della rete



Configurazioni

Se non è ancora stato configurato alcun VPC, gruppo di sicurezza, coppia di chiavi e tunnel VPN, è necessario seguire i passaggi facoltativi, in caso contrario, iniziare dal passaggio 1.

Passaggio opzionale A. Creazione di VPC

Passare al servizio **VPC** AWS. Selezionare **Avvia procedura guidata VPC** come illustrato nell'immagine.

The screenshot shows the AWS Management Console interface. At the top, there's a search bar and a navigation menu. On the left, there's a sidebar with 'VIRTUAL PRIVATE CLOUD' expanded. The main content area is titled 'Resources by Region' and shows a list of VPC resources in the Frankfurt region. A 'Launch VPC Wizard' button is highlighted in orange.

Selezionare VPC con solo subnet privata e accesso VPN hardware e fare clic su **Select** (Seleziona), come mostrato nell'immagine.

The screenshot shows the 'Step 1: Select a VPC Configuration' page. On the left, there's a list of VPC configurations. The 'VPC with a Private Subnet Only and Hardware VPN Access' option is selected and highlighted with a red box. In the center, there's a description of the configuration and a 'Select' button, which is also highlighted with a red box. On the right, there's a diagram showing an 'Amazon Virtual Private Cloud Subnet' connected to a 'Corporate Data Center' via a 'VPN' tunnel.

Nota: La selezione di VPC nel Passaggio 1. della procedura guidata VPC dipende dalla topologia poiché ISE non è progettata come server esposto a Internet - viene utilizzata solo la VPN con subnet privata.

Configurare le impostazioni della subnet privata VPC in base al progetto di rete e selezionare **Avanti**.

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**

Configurare la VPN secondo la progettazione della rete e selezionare **Crea 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

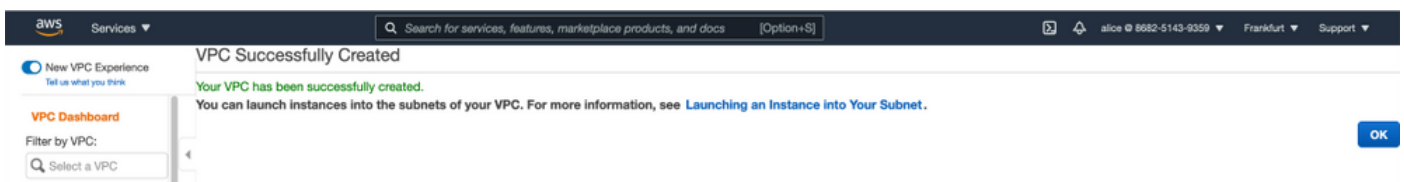
Note: VPN Connection rates apply.

Specify the routing for the VPN Connection (Help me choose)

Routing Type: Dynamic (requires BGP)

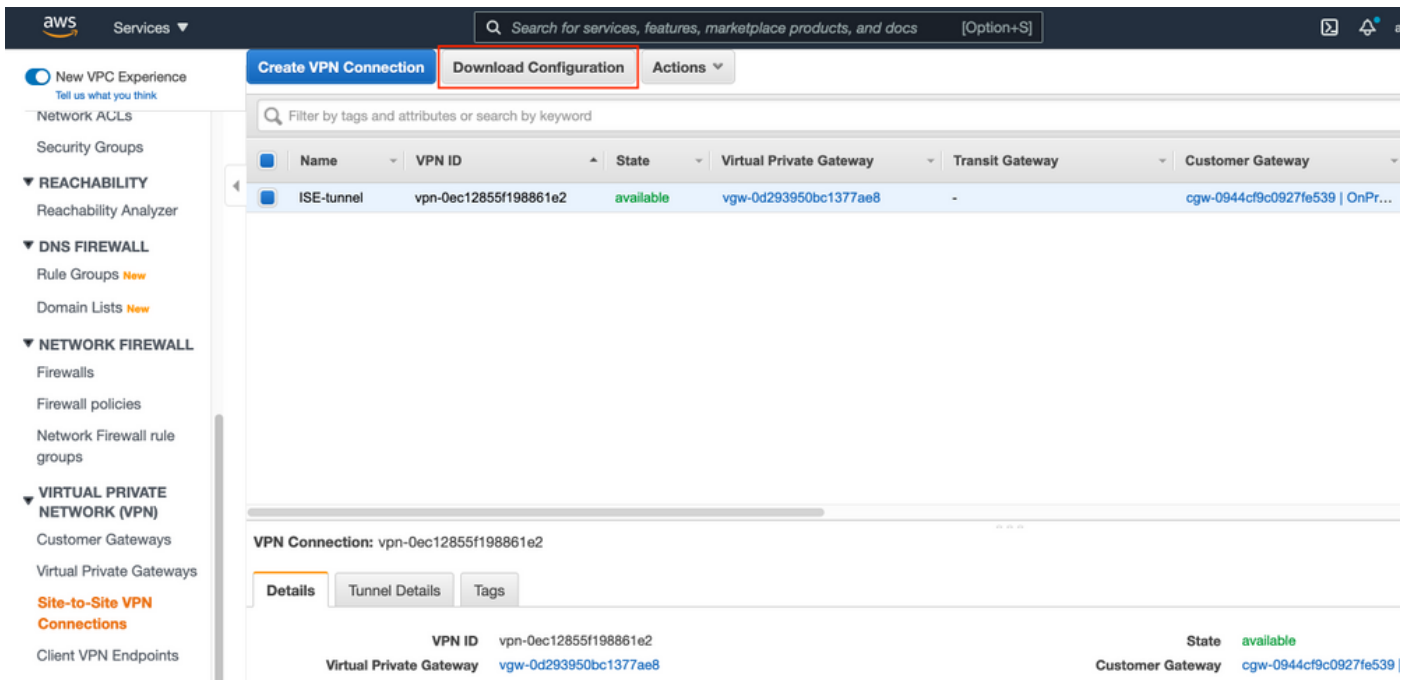
Cancel and Exit Back **Create VPC**

Una volta creato il VPC, viene visualizzato il messaggio "Your VPC has been successfully creation" (Creazione del VPC completata). Fare clic su **OK** come mostrato nell'immagine.

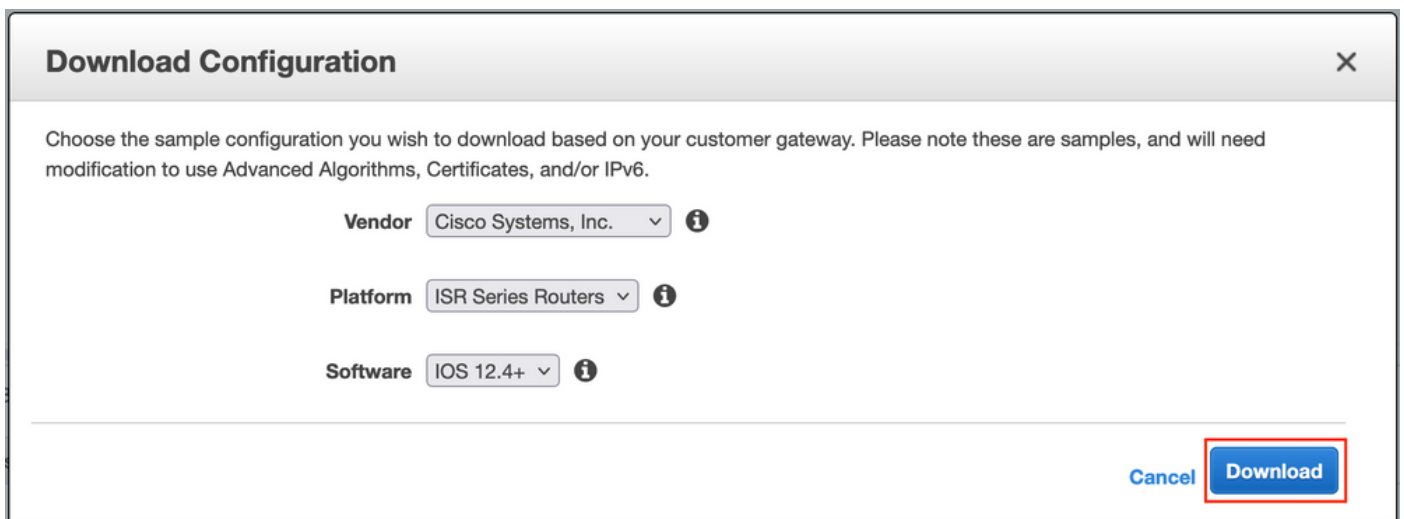


Passaggio B facoltativo. Configurare il dispositivo headend VPN locale

Passare al servizio **VPC AWS**. Scegliere **Connessioni VPN da sito a sito**, selezionare il tunnel VPN appena creato e selezionare **Scarica configurazione**, come mostrato nell'immagine.



Selezionare **Vendor**, **Platform** e **Software**, quindi selezionare **Download** (Download), come mostrato nell'immagine.



Applica la configurazione scaricata sul dispositivo headend VPN locale.

Passaggio C facoltativo. Creare una coppia di chiavi personalizzata

È possibile accedere alle istanze AWS EC2 tramite una coppia di chiavi. Per creare una coppia di chiavi, passare a **EC2 Service**. Selezionare il menu **Key Pairs** in **Network & Security (Rete e sicurezza)**. Selezionare **Crea coppia di chiavi**, assegnarle un **nome**, lasciare gli altri valori predefiniti e selezionare nuovamente **Crea coppia di chiavi**.

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

Passaggio facoltativo D. Creazione di un gruppo di sicurezza personalizzato

L'accesso alle istanze di AWS EC2 è protetto da **Gruppi di sicurezza**. Per configurare il **gruppo di sicurezza**, passare a Servizio **EC2**. Selezionare il menu **Gruppi di sicurezza** in **Rete e sicurezza**. Selezionare **Crea gruppo di sicurezza**, configurare un **nome**, una **descrizione**, nel campo **VPC** selezionare **VPC appena configurato**. Configurare **Inbound Rules** per consentire la comunicazione con ISE. Selezionare **Crea gruppo di protezione** come illustrato nell'immagine.

EC2 > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

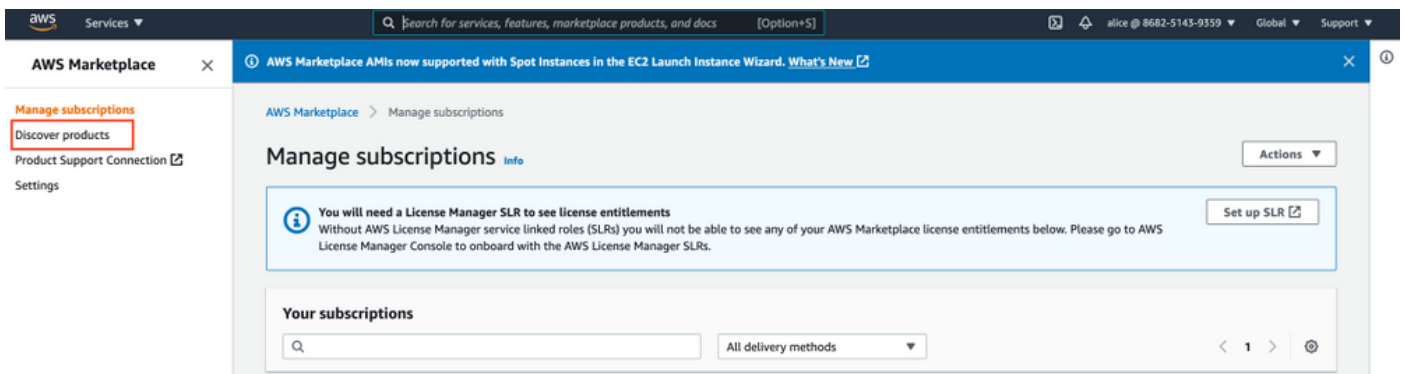
Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
All ICMP - IPv4	ICMP	All	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
HTTPS	TCP	443	Anywhere-IPv4 <input type="text" value="0.0.0.0/0"/>		Delete
All traffic	All	All	Custom <input type="text" value="172.18.5.0/24"/>		Delete

[Add rule](#)

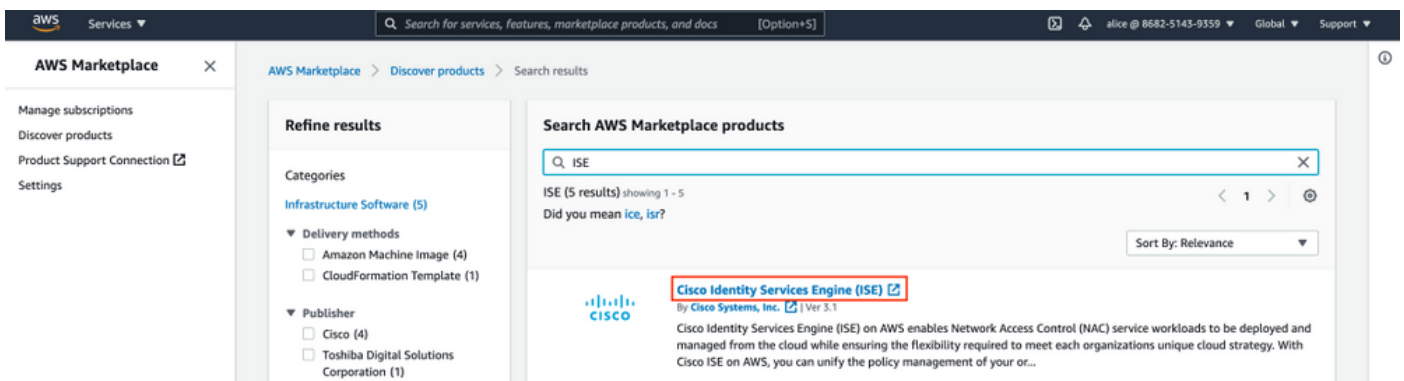
Nota: Il gruppo di sicurezza configurato consente l'accesso SSH, ICMP, HTTPS a ISE e a tutti i protocolli dalla subnet locale.

Passaggio 1. Iscriviti al prodotto AWS ISE Marketplace

Passare a **Sottoscrizioni Marketplace AWS Servizio AWS**. Selezionare **Discover Products**, come mostrato nell'immagine.



Cercare il prodotto **ISE** e selezionare **Cisco Identity Services Engine (ISE)**, come mostrato nell'immagine.



Selezionare il pulsante **Continua** per effettuare la sottoscrizione

aws marketplace

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

Hello, alice ▾

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).

Selezionare il pulsante **Accetta condizioni** come illustrato nell'immagine.

aws marketplace

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

Hello, alice ▾

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)

Una volta effettuato l'abbonamento, lo stato **Effettivo** e la data di scadenza vengono modificati in **In sospeso**, come mostrato nell'immagine.

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

Poco dopo la **data effettiva** viene modificata la data di sottoscrizione e la **data di scadenza** viene modificata in **N/D**. Selezionare **Continue to Configuration (Continua alla configurazione)** come mostrato nell'ima



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

Passaggio 2. Configurare ISE su AWS

Nel menu Delivery Method della schermata **Configure this software** selezionare **Cisco Identity Services Engine (ISE)**. Nella **versione software** selezionare **3.1 (12 ago 2021)**. Selezionare la **Regione** in cui si prevede di implementare ISE. Selezionare **Continua per avviare**.



[< 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	

Passaggio 3. Lanciare ISE su AWS

Dal menu a discesa Azioni della schermata **Avvia il software**, selezionare **Avvia 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](#)

(Facoltativo) Selezionare **Istruzioni d'uso** per familiarizzarsi con esse. Selezionare **Launch**.

Passaggio 4. Configurazione dello stack di formazione del cloud per ISE su AWS

Il pulsante **Launch (Avvia)** consente di reindirizzare l'utente alla schermata di impostazione **dello stack CloudFormation**. Per configurare ISE è necessario utilizzare un modello predefinito. Mantenere le impostazioni predefinite e selezionare **Avanti**.

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready
 Use a sample template
 Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL
 Upload a template file

Amazon S3 URL

Amazon S3 template URL

Cancel

Popolare i dati dello stack CloudFormation con il **nome dello stack**. Configurare i dettagli dell'istanza come **Nome host**, selezionare **Coppia di chiavi dell'istanza** e **Gruppo di sicurezza di gestione**.

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Instance Details

Hostname
Enter the hostname. This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.

Instance Key Pair
To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the username "admin". Create a PEM key pair in AWS now if you have not configured one already. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com

Management Security Group
Choose the Security Group to attach to the Cisco ISE interface. Create a Security Group in AWS now if you have not configured one already.

Continuare la configurazione dei dettagli dell'istanza con **Management Network**, **Management Private IP**, **Time Zone**, **Instance Type**, **EBS Encryption** e **Volume Size**.

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 ↕

Continuare la configurazione di Dettagli istanza con **Dominio DNS**, **Server dei nomi**, **Servizio NTP** e **Servizi**.

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 ▼

Configurare la password dell'utente GUI e selezionare **Next** (Avanti).

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**

Nella schermata successiva non sono necessarie modifiche. Selezionare **Avanti**.

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

Spostarsi sulla schermata **Review Stack**, scorrere verso il basso e selezionare **Create stack**.

Stack creation options

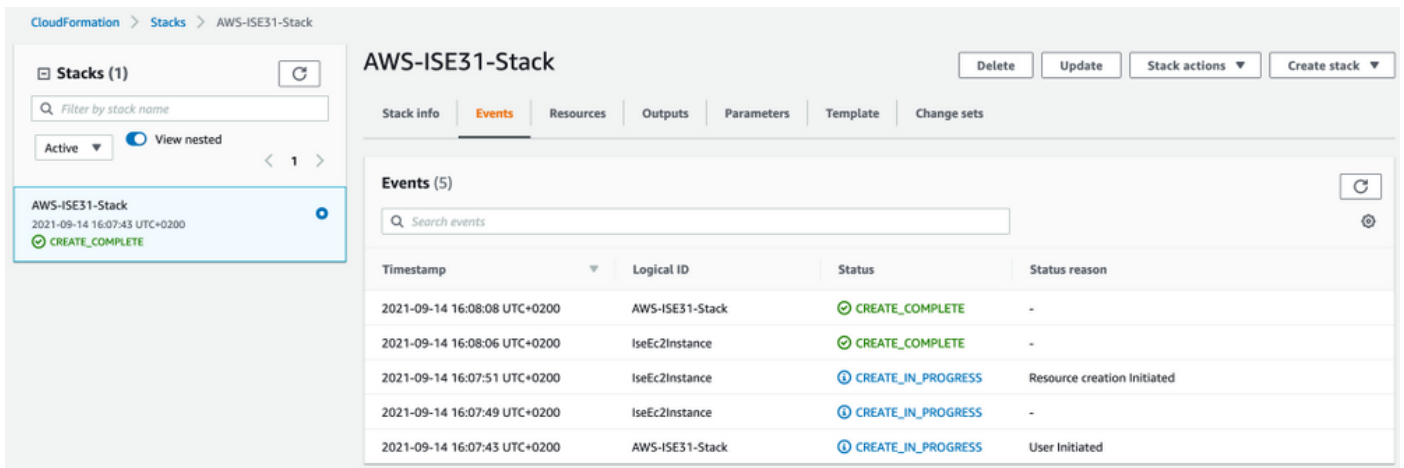
Timeout
-

Termination protection
Disabled

► Quick-create link

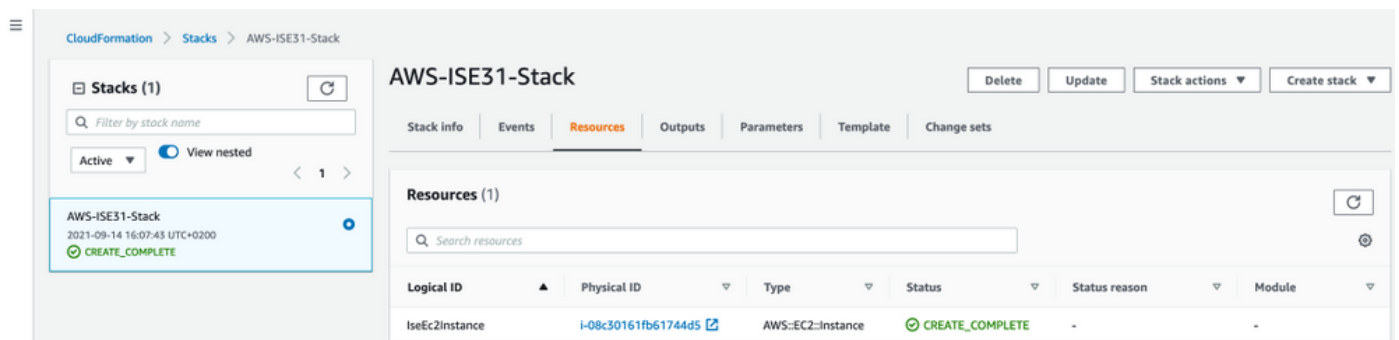
Cancel Previous Create change set **Create stack**

Dopo aver distribuito lo stack, è necessario verificare lo stato di **CREATE_COMPLETE**.

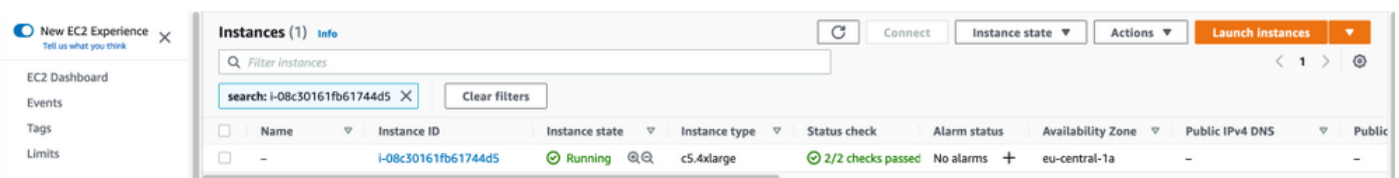


Passaggio 5. Accedere ad ISE su AWS

Per accedere all'istanza ISE, passare alla scheda **Risorse** per visualizzare l'istanza EC2 creata da CloudForms (in alternativa, passare a **Servizi > EC2 > Istanze** per visualizzare le istanze EC2) come mostrato nell'immagine.



Selezionare **Physical ID** per aprire il menu **EC2 Instances**. Verificare che per il controllo dello stato sia stato superato **2/2** controlli.



Selezionare **ID istanza**. È possibile accedere all'ISE tramite **indirizzo IPv4 privato/DNS IPv4 privato** con protocollo SSH o HTTPS.

Nota: Se si accede a ISE tramite **indirizzo IPv4 privato/DNS IPv4 privato** verificare che vi sia connettività di rete verso l'indirizzo privato ISE.

Esempio di accesso ad ISE tramite **indirizzo IPv4 privato** tramite 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:G5NdGZ1rgPYnjlndPcXOLcJg9VICLSxnZA0kn0CfMPs.
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#

Nota: Sono necessari circa 20 minuti prima che ISE sia accessibile tramite SSH. Fino a quel momento, la connettività ad ISE fallisce con "**Autorizzazione negata (chiave pubblica).**" x

Per verificare che i servizi siano in esecuzione, utilizzare il comando **show application status ise**:

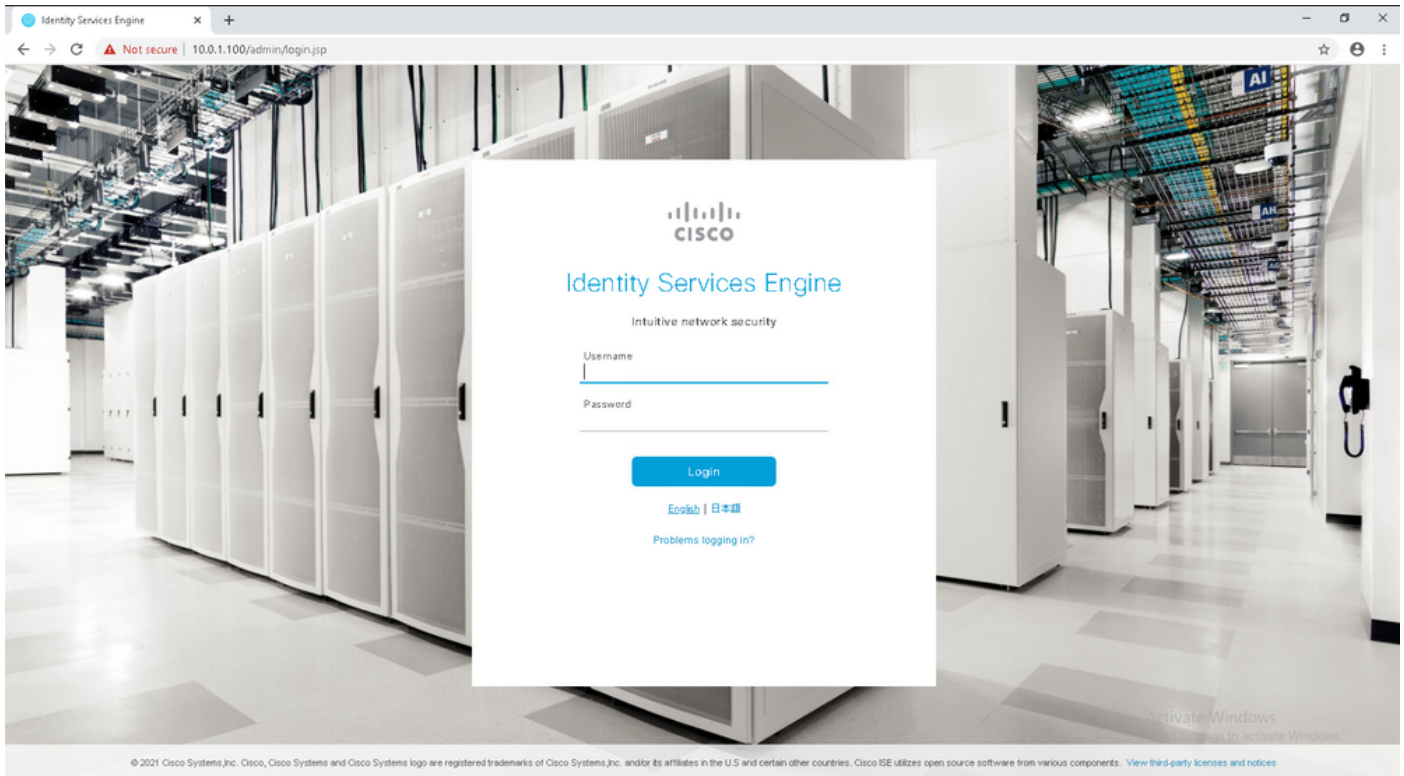
```
ISE31-2/admin# show application status ise
```

```
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#
```

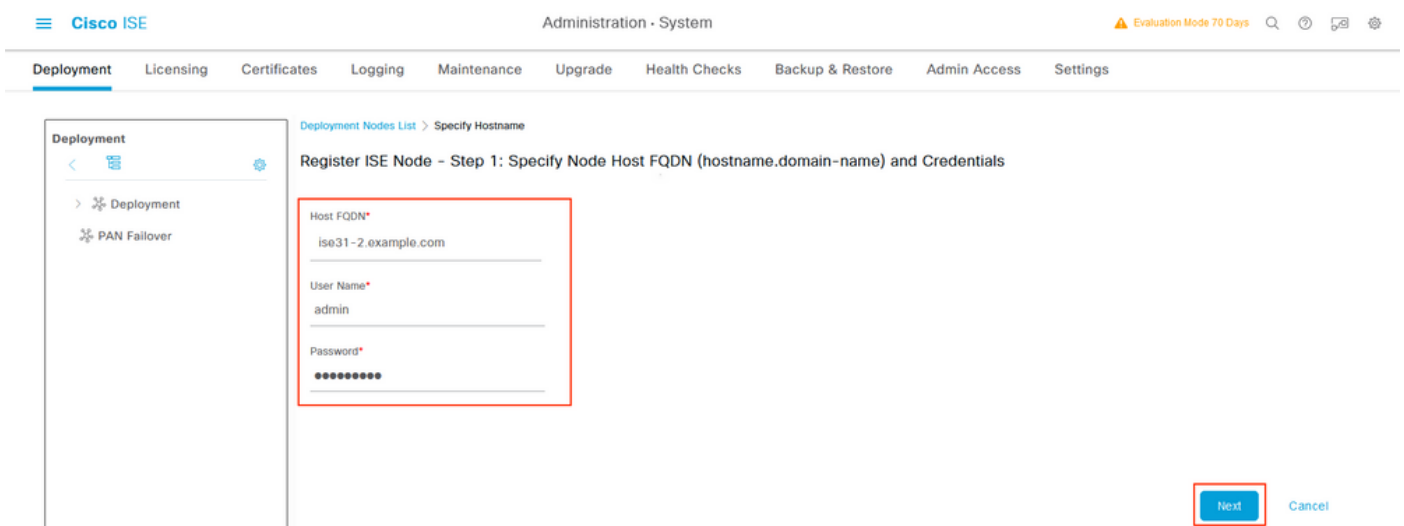
Nota: La disponibilità del protocollo SSH per il passaggio dei servizi ISE a uno stato di esecuzione richiede circa 10-15 minuti.

Una volta che l'**Application Server** è in **esecuzione**, è possibile accedere ad ISE tramite la GUI, come mostrato nell'immagine.



Passaggio 6. Configurare la distribuzione tra ISE locale e ISE su AWS

Accedere a ISE locale e selezionare **Amministrazione > Sistema > Distribuzione**. Selezionare il nodo e selezionare **Rendi principale**. Tornare ad **Amministrazione > Sistema > Distribuzione**, quindi selezionare **Registra**. Configurare l'**FQDN** dell'host di ISE su AWS, **nome utente GUI** e **password**. Fare clic su Next (Avanti).



Poiché in questa topologia vengono utilizzati certificati autofirmati, per eseguire l'importazione incrociata dei certificati amministrativi nell'archivio attendibile selezionare **Importa certificato e procedere**.



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](#)

Selezionare le Persone desiderate e fare clic su **Invia**.

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 Submit

Una volta completata la sincronizzazione, il nodo passa allo stato connesso e viene visualizzata la casella di controllo verde corrispondente.

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 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	✔

Passaggio 7. Integrare l'implementazione ISE con Active Directory in sede

Passare a **Amministrazione > Gestione delle identità > Origini identità esterne**. Selezionare **Active Directory**, quindi **Aggiungi**.

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

Configurare il **nome del punto di giunzione** e il **dominio di Active Directory**, quindi selezionare **Invia**.

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

Per integrare entrambi i nodi con Active Directory Selezionare **Sì**.



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

Immettere **nome utente** e **password AD**, quindi fare clic su **OK**. Una volta integrati correttamente i nodi ISE con Active Directory, lo stato del nodo cambia in Completato.



Join Operation Status

Status Summary: Successful

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

Close

Limitazioni

Per le limitazioni ISE su AWS, consultare la sezione [Known Limitations](#) della guida per l'amministratore di ISE.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare che l'autenticazione venga eseguita sul PSN ISE situato su AWS, selezionare **Operations > Radius > Live Logs**, quindi verificare che nella colonna **Server** sia stata rilevata l'ISE sul PSN AWS.

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Creazione stack CloudFormation non riuscita

La creazione dello stack di formazione del cloud può non riuscire per diversi motivi, uno di questi è quando si seleziona il gruppo di sicurezza dalla VPN, che è diverso dalla rete di gestione di ISE. L'errore è simile a quello nell'immagine.

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: [netC2instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	iseC2Instance	CREATE_FAILED	Security group sg-Qv54161c8423fa63 and subnet subnet-0fb0cda61258143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: b57d9773-f8e9-45c8-8664-8c40895a8464; Proxy: null)
2021-09-17 12:57:17 UTC+0200	iseC2Instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:11 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User initiated

Soluzione:

Assicurarsi di selezionare il gruppo di sicurezza dallo stesso VPC. Passare a **Security Groups** (Gruppi di sicurezza) in **VPC Service** (Servizio VPC), annotare l'**ID del gruppo di sicurezza**, accertarsi che corrisponda al VPC corretto (in cui risiede ISE), verificare l'**ID VPC**.

Problemi di connettività

La connettività ad ISE su AWS può causare diversi problemi e non funzionare.

1. Problema di connettività a causa di **gruppi di sicurezza** non configurati correttamente.

Soluzione: Se i **gruppi di sicurezza** non sono configurati correttamente, ISE non può essere raggiungibile dalla rete locale o anche all'interno delle reti AWS. Verificare che i protocolli e le porte richiesti siano consentiti nel **Gruppo di sicurezza** associato alla rete ISE. Per informazioni sull'apertura delle porte richieste, consultare la [guida di riferimento](#) per le porte ISE.

2. Problemi di connettività causati da routing non configurato correttamente.

Soluzione: A causa della complessità della topologia, è facile perdere alcune route tra la rete locale e AWS. Prima di usare le funzionalità ISE, assicurati di avere una connettività end-to-end.

Appendice

Configurazione correlata allo switch 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