

AWS قوس لالځ نم 3.1 ISE نيوكت

تايوت حمل

[قمدقمل](#)

[قيساس الابلطت مل](#)

[تابلطت مل](#)

[قمدخت سمل تانوك مل](#)

[نيوكت مل](#)

[قكبش مل ططخم](#)

[تاننيوكت مل](#)

[VPC عاشنا. أقررايتخال. قوطخل](#)

[PREM ىلع VPN ثبل اولابلقت سالا قذو زاهج نيوكت. بقررايتخال. قوطخل](#)

[صصخم حيتافم جوز عاشنا. ققررايتخال. C قوطخل](#)

[قصصخم نامأ قعومجم عاشنا. ققررايتخال. D قوطخل](#)

[AWS ISE قوس جت نم يف كارتشال. 1. قوطخل](#)

[AWS ىلع ISE نيوكت. 2. قوطخل](#)

[AWS ىلع ISE ليغشت. 3. قوطخل](#)

[AWS ىلع ISE ل CloudConfiguration سدكم نيوكت. 4. قوطخل](#)

[AWS ىلع ISE ىل لوصول. 5. قوطخل](#)

[AWS ىلع ISE و ISE نيوب عزومل رشنل نيوكت. 6. قوطخل](#)

[قيزهجال ىلع AD عم ISE رشن جم. 7. قوطخل](#)

[دويقل](#)

[قحصل نم ققحتل](#)

[احجال صاواطخال فاشكتسا](#)

[CloudConfiguration سدكم عاشنا لشف](#)

[لاصتال تالكشم](#)

[قحل مل](#)

[AAA/RADIUS لوملاب طبترم مل نيوكت مل](#)

قمدقمل

Identity Services Engine (ISE) 3.1 ربع Amazon Machine Image (AMI) ف Amazon Web Services (AWS). ليشن نكمي ISE 3.1 رادصال نم. CloudConfiguration (CFT) بلاوق قعاسمب Amazon ىلع (EC2) قنرمل قبسوخل قباحسل اذه حضوي.

قيساس الابلطت مل

تابلطت مل

قيلال عيضاوملاب قيساسأ قفرعم كيدل نوكت ناب Cisco ىصوت:

- (ISE) قوهال فشك تامدخ كرحم
- CloudConfiguration و EC2 و VPC لثم هميهافم و AWS

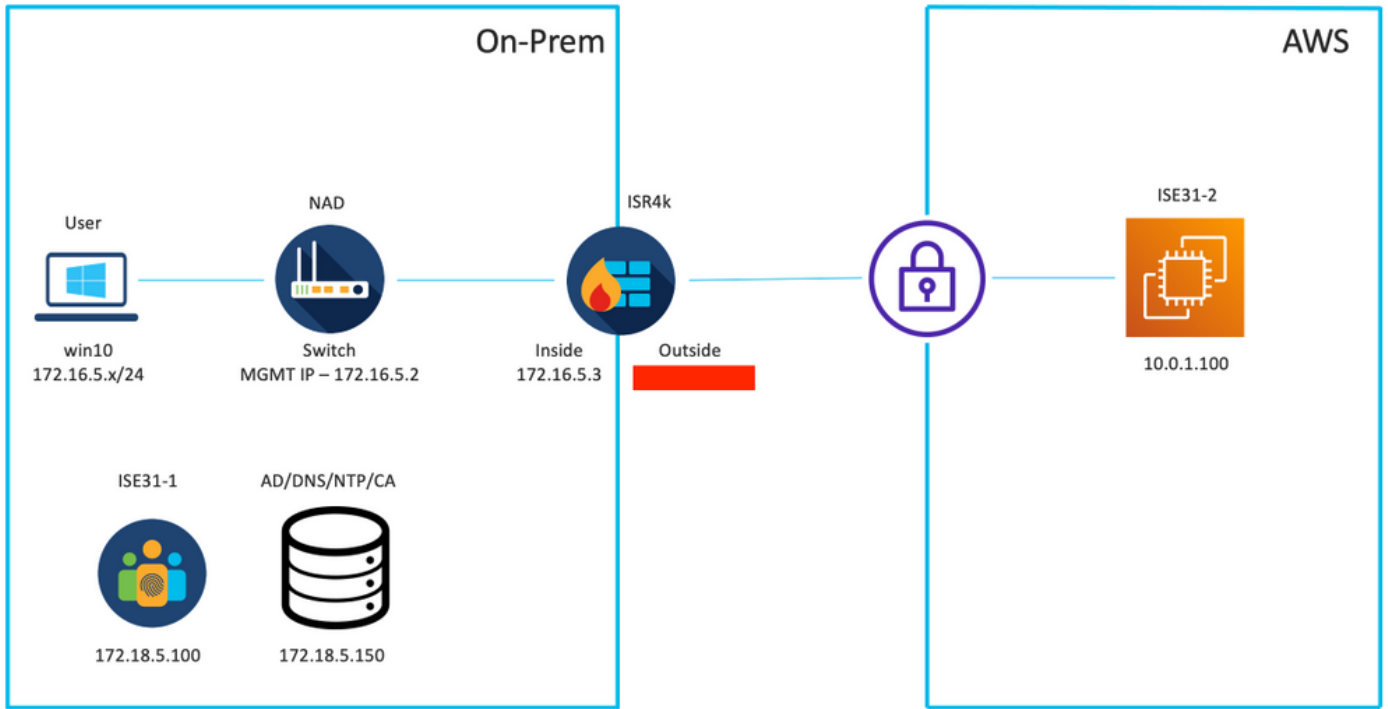
ةمدختسملا تانوكملا

3.1. ةغيص Cisco ISE لىل ةقوئو اذو ف ةمولعملل ةسسأ

ةصاخ ةلمعم ةئيب ف ةدووملا ةزهجال نم دنتسملل اذو ف ةدراولل ةمولعملل ةاشنإ م ت ت ناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملل اذو ف ةمدختسملل ةزهجالل ةيمج ةأب رملل لملحتحملل ريثأتلل كمهف نم دكأتف، ليغشتل ديقتك تكبش

نيوكتلا

ةكبشلل ططخم



تانويوكتلا

قف نوحيتافملا ةاوسأو نامألل ةاعومجمو (VPC) يصخش رتويبمك زاهج دووومدع ةلاح ف ةيرايختخالل ةاوطخالل ةابنل كمزلي، دعب هنيوكت م ت يذلل (VPN) ةيرهاظلل ةصاخلل ةكبشلل 1. ةوطخالل ةدبلل كليل عف، ةاوس

VPC ةاشنإ. ةيرايختخالل ةوطخالل

وه امك VPC ةلامم ليغشت دح. (VPC) دروملا ةئيف فرعمب ةصاخلل AWS ةمدخلل لقتنا ةروصلل ف حضورم.

aws Services

Search for services, features, marketplace products, and docs [Option+S]

New VPC Experience
Tell us what you think

VPC Dashboard

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables **New**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets

Launch VPC Wizard

Launch EC2 Instances

Note: Your Instances will launch in the Europe (Frankfurt) region.

Resources by Region Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions ▼	Frankfurt 1	NAT Gateways See all regions ▼	Frankfurt 0
Subnets See all regions ▼	Frankfurt 3	VPC Peering Connections See all regions ▼	Frankfurt 0
Route Tables See all regions ▼	Frankfurt 1	Network ACLs See all regions ▼	Frankfurt 1

يف حضورم وه امك يق تني ة ق ط ق و ذ ف ن م VPN زا ه و ط ق ف subnet ص ا خ ع م VPC ت ر ت خ أ ة ر و ص ل ل .

aws Services

Search for services, features, marketplace products, and docs [Option+S]

Step 1: Select a VPC Configuration

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

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.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

Select

Amazon Virtual Private Cloud
Subnet

VPN

Corporate Data Center

م ل ISE ن أ ل ا ر ظ ن ط ا ط خ م ل ا ل ع VPC ج ل ا ع م ن م . 1 ة و ط خ ل ا ل ي ف VPC د ي د ح ت د م ت ع ي : ة ط ا ل م ة ي ع ر ف ة ك ب ش ع م VPN م ا د خ ت س ا م ت ي - ت ن ر ت ن ا ل ا ر ب ع ف و ش ك م م د ا خ ك ه م ي م ص ت م ت ي ط ق ف ة ص ا خ .

م ي م ص ت ل ا ق ف و (VPC) د ر و م ل ا ئ ف ف ر ع م ب ة ص ا خ ل ا ة ي ع ر ف ل ا ة ك ب ش ل ا ت ا د ا د ع ا ن ي و ك ت ب م ق ي . ل ل ا ت ل ل د د ح و ك ي د ل ة ك ب ش ل ل

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

VPCءاشن| ددو ةكبشلا ميصتلاق فوكب ةصاخلا VPN ةكبش نيوكتب مق

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

ok ةقطط .تضرع "تقلخ حاجنب نوكي يقلتي VPC ك" ةلاسرلا ،نوكي VPC لا تقلخ نإ ام ةروصلال يف حضوم وه امك

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

PREM ىلع VPN ثبالاولا بقتسالال ددو زاه نيوكتب .ب ةيرايتخالال ةوطخال

ىلإ عقوم نم VPN تالاصت| رتخأ .(VPC) دروملا ةئف فرعمب ةصاخلا AWS ةمدخ ىلإ لقتنا ةروصلال يف حضوم وه امك نيوكتلا ليزنت ددو ائيدح هءاشنإ مت يذلا VPN قفن ددو ،عقوم

aws Services Search for services, features, marketplace products, and docs [Option+S]

Create VPN Connection **Download Configuration** Actions

Filter by tags and attributes or search by keyword

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
ISE-tunnel	vpn-0ec12855f198861e2	available	vgw-0d293950bc1377ae8	-	cgw-0944cf9c0927fe539 OnPr...

VPN Connection: vpn-0ec12855f198861e2

Details Tunnel Details Tags

VPN ID: vpn-0ec12855f198861e2 State: available
Virtual Private Gateway: vgw-0d293950bc1377ae8 Customer Gateway: cgw-0944cf9c0927fe539

ة.روصول ال ي ف حضورم وه امك ل ي زنت ددح ،ةي ج مر ب و ة صن م ، ةئ اب ت رت خ أ

Download Configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Cisco Systems, Inc. ⓘ

Platform: ISR Series Routers ⓘ

Software: IOS 12.4+ ⓘ

Cancel **Download**

VPN ة ك ب ش ب ة ص ا خ ل ا ث ب ل ا و ل ا ب ق ت س ا ل ا ة د ح و ز ا ه ج ي ل ع ه ل ي ز ن ت م ت ي ذ ل ا ن ي و ك ت ل ا ق ي ب ط ت ة ي ل خ ا د ل ا

ص ص خ م ح ي ت ا ف م ج و ز ء ا ش ن ا . ة ي ر ا ي ت خ ا ل ا C ة و ط خ ل ا

ل ق ت ن ا ، ح ي ت ا ف م ج و ز ء ا ش ن ا ل . ح ي ت ا ف م ل ا ج ا و ز ا ة د ع ا س م ب AWS EC2 ت ا ل ي ث م ي ل ا ل و ص و ل ا م ت ي ه ط ع ا و ، ح ي ت ا ف م ج و ز ء ا ش ن ا د د ح . ن ا م ا ل ا و ة ك ب ش ل ا ت ح ت ح ي ت ا ف م ل ا ج ا و ز ا ة م ئ ا ق د د ح . EC2 ة م د خ ي ل ا ي ر خ ا ة ر م ح ي ت ا ف م ج و ز ء ا ش ن ا د د ح و ة ي ض ا ر ت ف ا ة م ي ق ك ي ر خ ا ل ا م ي ق ل ا ك ر ت ا و ، ا م س ا

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.

Add tag

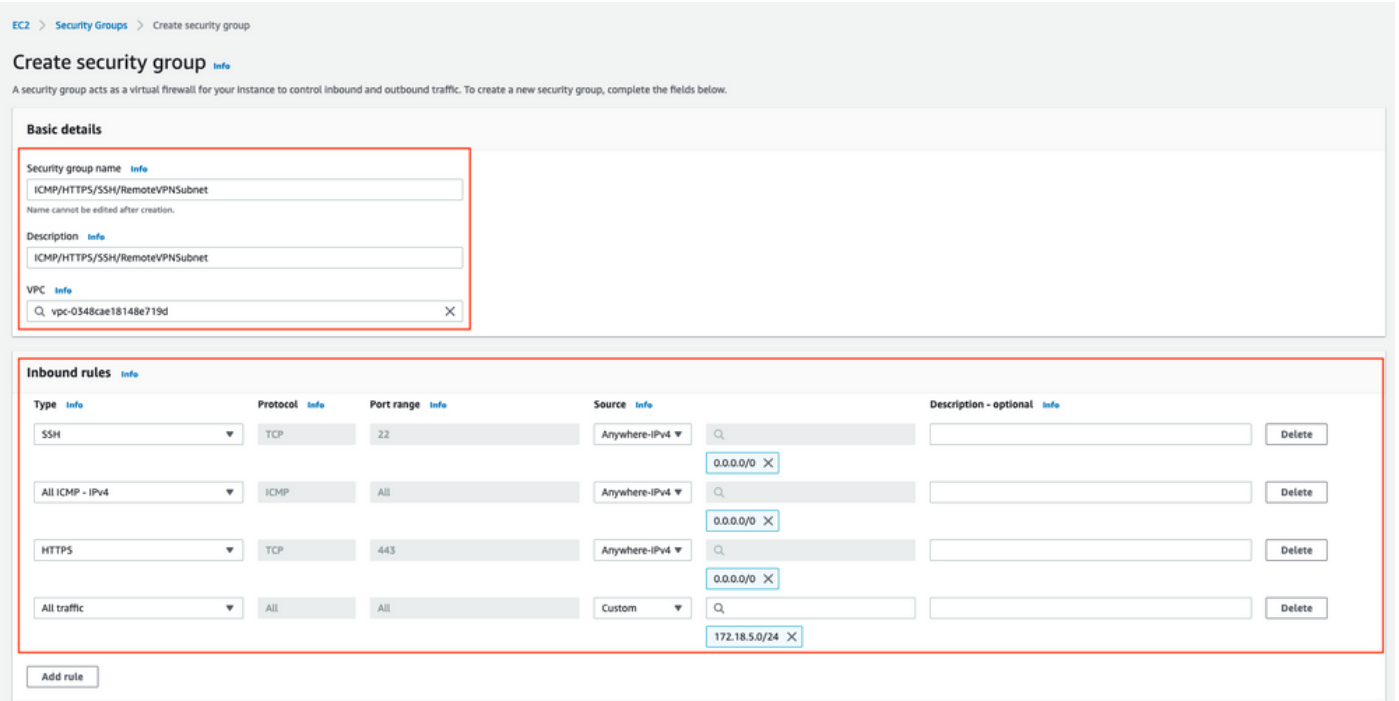
You can add 50 more tags.

Cancel

Create key pair

صصخم نام ةوعومجم عاشن | ةيرايختال D ةوطخال

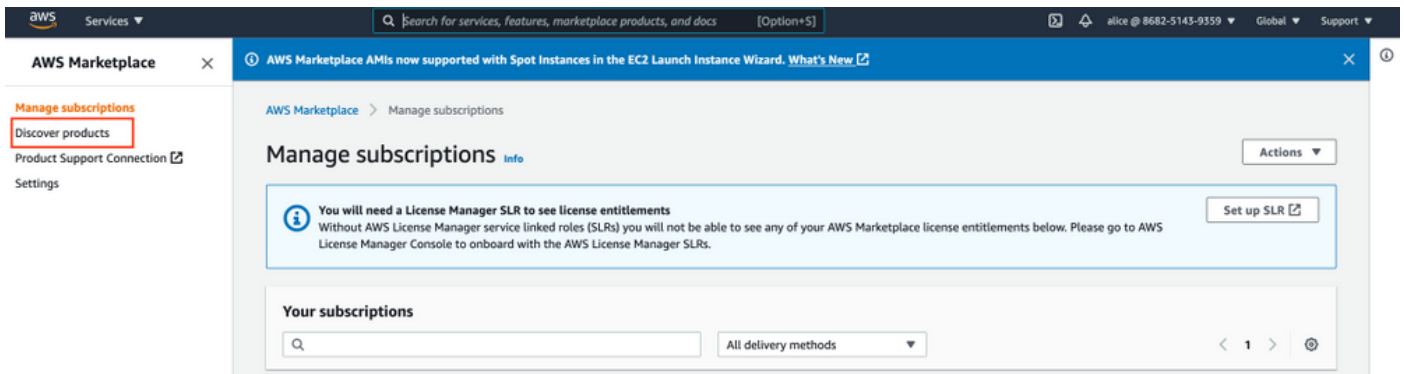
ةوعومجم نيوكت لجأ نم ، نامأل تاوعومجم ةطساوب AWS EC2 تاليثم ىل لوصول ةيامح متي عاشن ددح . نامأل او ةكبشال تحت نيماأل تاوعومجم ةمئاق ددح . EC2 ةمدخ ىل لقتنا ، نامأل نيوكتب مق . اتي دح هنيوكت متي ذل VPC ددح VPC ل قح ي ف ، ف ص و ، م س ا نيوكت ، نام ةوعومجم ةروصل ي ف حضورم وه امك نيماأل ةوعومجم عاشن ددح . ISE ب لاصلتالاب حامس لل ةدراول دعاولل



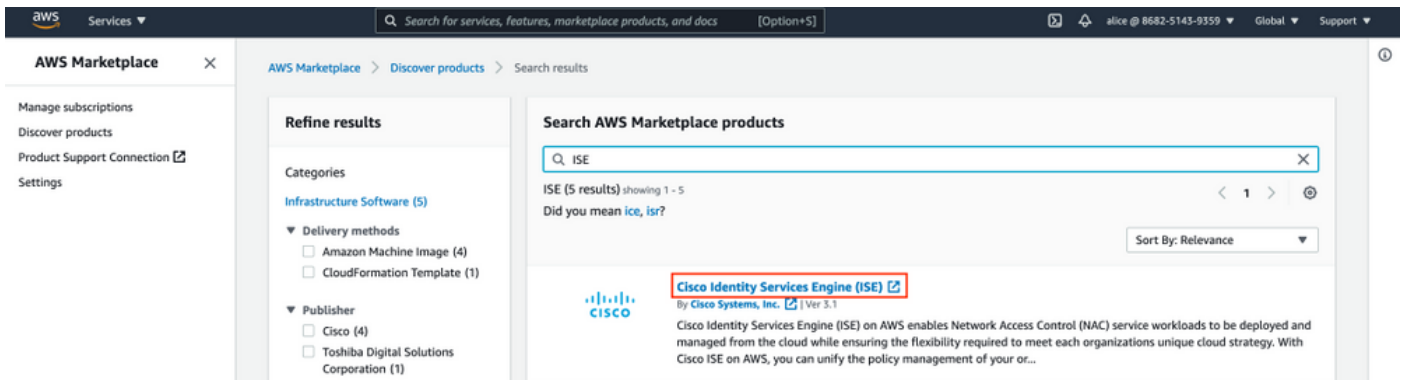
مداخل الـ ISE إلى HTTPS و ICMP و SSH لوصول اهنيوكت مت يتل نام الة و عوم حم ست :ةظ حال م. داخال الة عة يعرف الة ك بشل الة نم الة و كوت و ربل الة عيم ج الة لوصول الة

1. ةوطخال الة AWS ISE قوس جت نم يف كارتشال الة

يف حضور و ه امك اءا جت نم الة فاشتك اءح الة AWS قوس اءا كارتشال الة AWS ةمدخ الة لقتن الة ةروصل الة.



ةروصل الة يف حضور و ه امك الة Cisco (ISE) نم ةي و ه الة اءمدخ كءح و ءءو الة ISE جت نم نع شءب الة.



كارتشال الة ةعباتم رزل الة ءح

aws marketplace Hello, alice

About 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	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).

ةروصللا يف حضوم وه امك طورشللا لوبق رز ددح

aws marketplace Hello, alice

About 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.

Component	Pricing
Cisco Identity Services Engine (ISE) BYOL	Additional taxes or fees may apply.
Cisco Identity Services Engine (ISE)	

امك قلع عم لىل ربيغت عم ةيصالصلا ءاهتنا ونايرسلا خيرات ةلاحي في كارتشالا درجمب ةروصللا يف حضوم وه

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

ماهت نا خيرات تاريخي غتو كارت شال خيرات الى نا رسال خيرات ري غت نم ري صق تقو دعب
IMA يف حضورم وه امك نيوكتلا ةعباتم ددح. N/A الى اي حالصل



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

AWS الى ISE نيوكت 2. ةوطخل

Cisco نم ةي وهال تامدخ كرحم ددح، جم انربل اذه نيوكت ةشاش نم مي لس تال ةقيرط ةمئاق يف
ISE طي طخت مت ثيح، ةقطنم لاددح. (2021 س طس غأ 12) 3.1 ددح، جم انربل رادصل يف (ISE).
لغش تال ةعباتم ددح. اهرشنل



[< 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

AWS ISE لي غشت 3. ةوطخل

لي غشت ددح، جمان ربل اذه لي غشت ةشاش نم ةلدس نمل اءارج اإل ةمئاق نم CloudConfiguration.



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](#)

قالطال ددح. اهب ةيارد ىلع كسفن لعجتل مادختسال تاداشرا ددح (يرايخا).

CloudConfiguration س دكم نيوك ت. 4 ةوطخلا

كانه CloudConfiguration س دكم دادع ةشاش ىل كهيوت ةداعب ليغشتلا ادب رزلا موقبي ددحو ةيضارتفالا تاداعبال ظفتحا. ISE دادعإل همادختسا بجي اقبس م ؤاشنا مت بلاق يلاتلا.

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
https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba9:

Amazon S3 template URL
S3 URL: https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba925376.template [View in Designer](#)

Cancel [Next](#)

لي صافات ني وك تب مق . سد كم ل مسا مادخت ساب CloudConfiguration سد كم تانايب ة ئب عت ة رادال نام ة عوم جم و لي ثمل احي تافم جوز ددحو ، hostname ل ثم لي ثمل

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
AWS-ISE31-Stack

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.
ISE31-2

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
aws

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.
ICMP/HTTPS/SSH/RemoteVPNSubnet (sg-0792bfa6bba47098d)

ة قطن م لا و ة رادال اب صا ل IP و ة رادال ة ك ب ش مادخت ساب لي ثمل ا لي صافات ني وك ت عبات م ج ل م ج و EBS ريف ش ت و لي ثمل ا ع و ن و ة ئب م ز ل ا

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

تامدخال او NTP مةمدخو مسالا مداخلو DNS لاجم مادختساب ليلثمل ليلصافات نيوكت ةعباتم.

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

كلذ دعب ددحو ةم لك لمعتسم GUI تللكش.

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**

ييلاتلا ددح. ةييلاتلا ةشاشلا لىل ع ةبولطم تارييغت دجوت ال

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

سدكم ءاشن | ددحو لفسأل لقتناو ، سدكم لا ةعجارم ةشاش لىل لقتنا

Stack creation options

Timeout
-

Termination protection
Disabled

► Quick-create link

Cancel Previous Create change set **Create stack**

سدكم لا رشن درجم ب CREATE_COMPLETE ةلاح ضرع بجي

The screenshot shows the 'Events' tab for the 'AWS-ISE31-Stack'. The stack is in a 'CREATE_COMPLETE' state. The events table shows the following details:

Timestamp	Logical ID	Status	Status reason
2021-09-14 16:08:08 UTC+0200	AWS-ISE31-Stack	CREATE_COMPLETE	-
2021-09-14 16:08:06 UTC+0200	IseEc2Instance	CREATE_COMPLETE	-
2021-09-14 16:07:51 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	Resource creation initiated
2021-09-14 16:07:49 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	-
2021-09-14 16:07:43 UTC+0200	AWS-ISE31-Stack	CREATE_IN_PROGRESS	User Initiated

5. ةوطخلل AWS ISE لىل لوصول

مت يذلا EC2 لىل م ضرعل دراومل بى وبتلا ةمالع لىل لقتنا ISE، لىل لوصول م تاللى م ضرعل تاللى م > EC2 > تامدخل لىل لقتنا كلذ م ال د ب) CloudForms م هؤاشن EC2 ةوصول لىل ف حضور م وه امك (EC2).

The screenshot shows the 'Resources' tab for the 'AWS-ISE31-Stack'. The stack is in a 'CREATE_COMPLETE' state. The resources table shows the following details:

Logical ID	Physical ID	Type	Status	Status reason	Module
IseEc2Instance	i-08c30161fb61744d5	AWS::EC2::Instance	CREATE_COMPLETE	-	-

تاىلمع م 2/2 هب ةلاخلل صخف نأ م دكأت EC2 تاللى م ةمئاق حتفل لىل فرعم دح اهرىم م يتل قحتللا.

The screenshot shows the 'Instances' page in the AWS Management Console. One instance is shown in a 'Running' state:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
-	i-08c30161fb61744d5	Running	c5.4xlarge	2/2 checks passed	No alarms	eu-central-1a	-	-

عبارللا رادصلل صاخل DNS/صاخل IPv4 ناونع ربع ISE لىل لوصول نكمى. لىل لوصول فرعم دح HTTPS و SSH لوكوتورب م (IP) تنرتنللا لوكوتورب م.

م دكأتف صاخل IPv4 DNS/صاخل IPv4 ناونع ربع ISE لىل لوصول م تمق اذا: ةطخالل صاخل ISE ناونع هاجتاب ةكبش لاصتا دوجو.

SSH ربع صاخل IPv4 ناونع ربع لىل لوصول م يتي يذلا ISE لىل لوصول م:

```
[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#

SSH لوكوتورب ربع (ISE) ةتباتل صارقألا كرحم ةزيم ىلإ لوصولا قرغتسي: **ةظالم**
ضوفرمدنإ أطلخال ةلاس ررم ISE ب لاصلتالا لشفي، تقولا كلذى تحو. ةقيقد 20 يلاوح
(publicKey).

تامدخال ليغشت نم ققحتلل قيبتل ةلاح ضرع مدختسأ

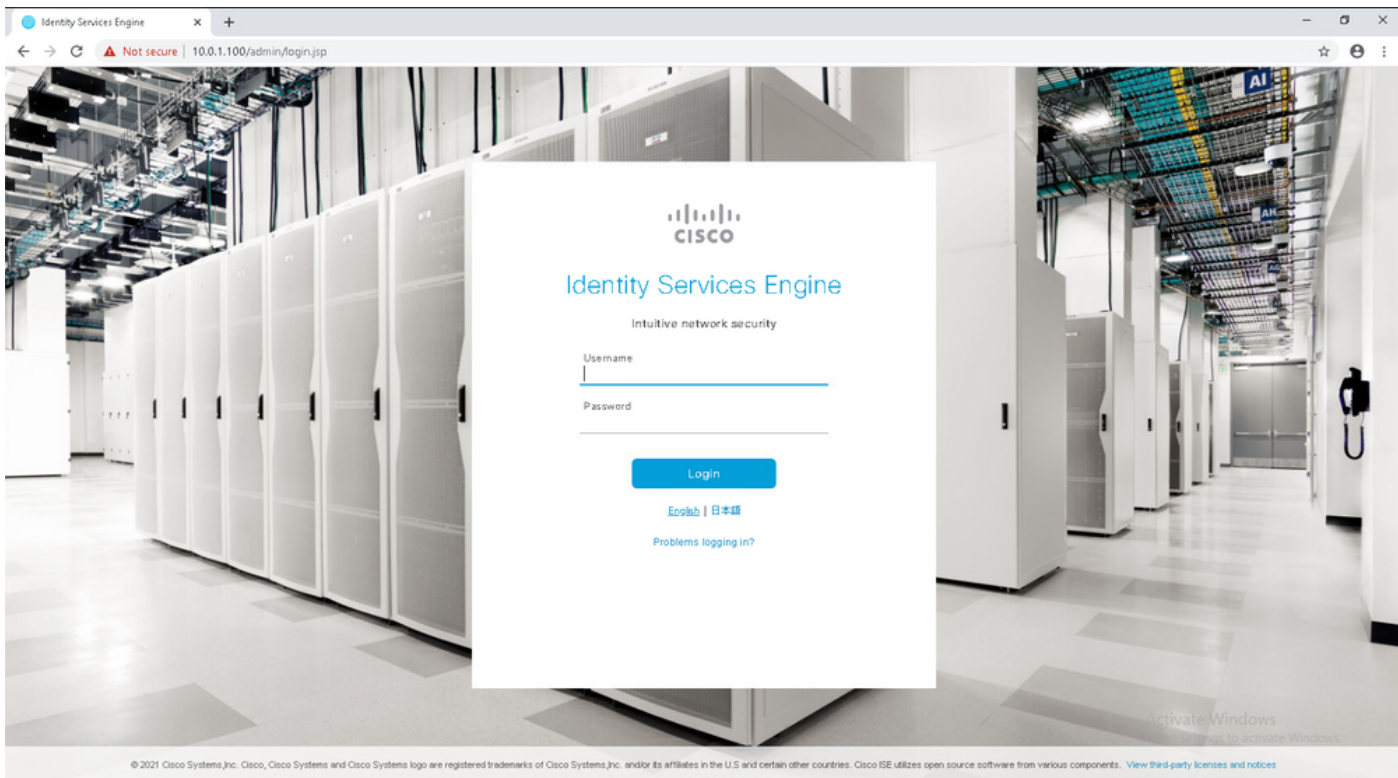
ISE31-2/admin# show application status ise

```
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#

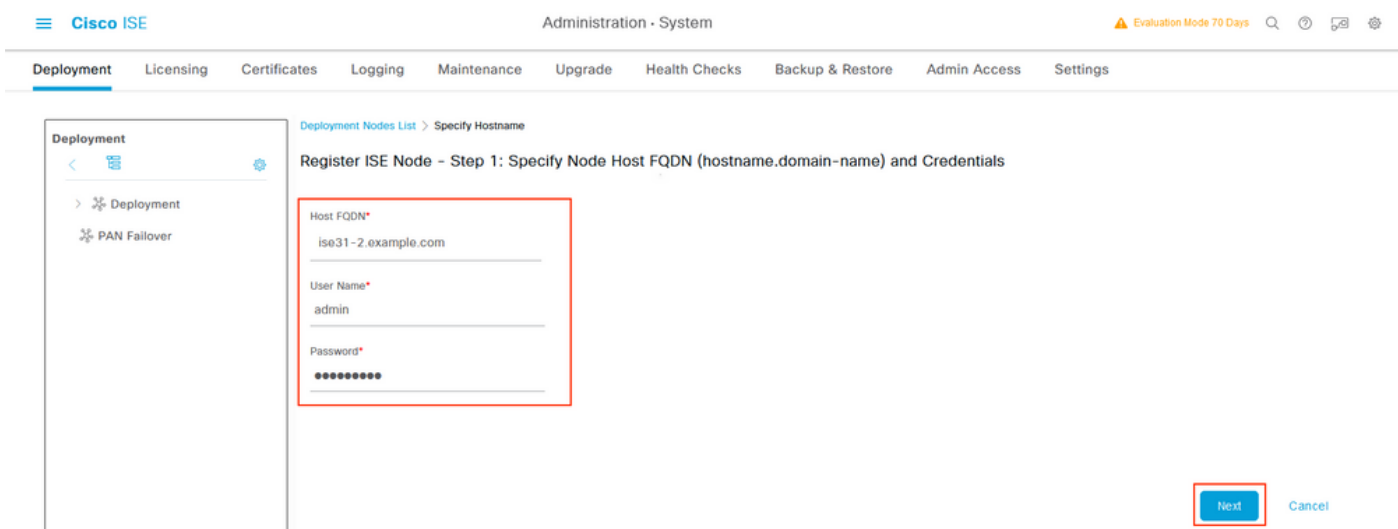
تامدخال SSH لوكوتورب رفوت ذنم ابيرقت ةقيقد 15 ىلإ 10 نم رمالا قرغتسي: **ةظالم**
ليغشتل ةلاح ىلإ لاقنتال ISE

ةهجاو ربع ISE ىلإ لوصولا كنكمي، ليغشتل ةلاح في قيبتل مداخ نوكي نأ درجب
ةروصلال في حضورم وه امك (GUI) ةيموسرل مدختسمل



6. ةوطخلا ISE و ISE نيب عزوملا رشنلا نيوكت

ةدقعل ددح. رشنلا > ماظنلا > ةرادلا ىل لقتناو دادعلا ىل ISE ىل لوخدلا ليجستب مق نيوكت. ليجستلا ددح، رشنلا > ماظنلا > ةرادلا ىل ىرخا ةرم لقتنا. ىساسا ءارج ددحو رورملا ةملاكو (GUI) ةيموسرلا مدختسملا ةهجاو مدختسم مسا، AWS ىل ISE نم فيضملا (ىلاتلا) Next قوف رقنا.



تاداهش داريتسإف، طاطخملا اذه يف اهمادختسإ متي ايتاذ ةعقوملا تاداهشلا نأ امب رشابو ةداهش داريتسإ ددحي هب قوئوملا ننخملا ىل لوؤسملا.



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](#)

لاسرا قوف رقناو اهراتخت يتلا تايشخشا ددح

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

راي تخاللا ةناخ ضرع متي ، ةلصت مل ةلحال الى ةدق ةل لقتنت ، ةنماز مل لامتك درج م ب اهل باقم ةارض ال

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 checked="" type="checkbox"/>
<input type="checkbox"/>	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>

ةزهال الى ةل AD عم ISE رشن جم د 7. ةوطخ ال


Add. دح ، Active Directory دح . ةجراخ ال ةوهال رداصم > ةوهال ةراد > ةراد الى لقتنا

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

لإسراء ددح، Active Directory لإاومو ةكرتشملا ةطقنللا مسان يوكتاب مق.

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

معن ددح، Active Directory عم دقعلا الك لمالكتل.



Information

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

No

Yes

Active Directory عم حاجن ب ISE دقع جم د درجم ب ok. ت ققط ط ، رورم ةم لك و مس | لمعت سم نال ع | تلخد ةدق لال ةلاح تاري ي غت لامك | متي ، Directory.



Join Operation Status

Status Summary: Successful

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

Close

دوي قلا

لي لد ي ف [ةفور عمل ا تادد ح مل ا](#) مسق ي ل ا ع وجر ل ا ي جري ، AWS ي ل ع ISE دوي ق ي ل ع ل و ص ح ل ل ISE ل وؤ س م .

ة ح ص ل ل ا ن م ق ق ح ت ل ا

حجحص لكشب نيوكتلا لمع ديكأتل مسقلا اذ مدختسا

> تاي لمعل اىلا لقتنا ، AWS اىل دوجومل ا ISE PSN اىل عوقداصملا ذيفنت نم ققحتلل
 Radius > اىل عوقداصملا تالاجسلا ، قرشابملا تالاجسلا

The screenshot shows the Cisco ISE Operations - RADIUS dashboard. At the top, there are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (1), and Repeat Counter (0). Below these are controls for Refresh, Reset Repeat Counts, and Export To. The main part of the dashboard is a table with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Profile, Authentication Poli..., Authorization Policy, Server, and Authc. The table contains several rows of log entries for user 'alice' with endpoint ID '00:50:56:A1:45:84' and profile 'VMWare-Device'. The 'Server' column for the first two rows is highlighted with a red box and contains the value 'ISE31-2'.

اهحالص او عاطخال فاشكتسا

اهحالص او نيوكتلا عاطخا فاشكتسال اهم ادختسا كنكمي تامولعم مسقلا اذ رفوي

فاشكتسا CloudConfiguration سدكم عاشن لشف

ددحت امدنع اهدحأ ، ددعتم بابسا ببسب CloudConfiguration سدكم عاشن لشف نأ نكمي
 دوجومل اطلخال اطلخال ودبي . ISE ارادا اكبش نع ةفلتخم ل VPN ةكبش نم هذه نامال اوعومجم
 ةروصل اىل ف

The screenshot shows the AWS CloudFormation console for a stack named 'ISE31-AWS'. The 'Events' tab is selected, showing a list of events. The 'CREATE_FAILED' event is highlighted with a red box. The status reason for this event is: 'Security group sg-0c54161c94262f4e3 and subnet subnet-0fbec0a62a58143 belong to different networks. Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: 8b799775-fbe9-45c8-8664-6c40995a8444; Proxy: null'.

لحل:

ةمدخ نمض نامال تاعومجم اىلا لقتنا . VPC هسفن ل نم نامال اوعومجم اىل قتن نأ تنمض
 نم اىلا (VPC) نامال اوعومجم فرعمل هتقباطم نم دكأتو ، نامال اوعومجم فرعمل احو ، VPC
 فرعمل نم ققحت ، (ISE ميقى شيح)

لاصتالا تالكشم

اىل عوقداصملا ISE ب لاصتالا لمع مدع اىل فاشكتسا دق ددعتم لكاشم كانه نوكت دق

حجحص ريغ لكشب نامال تاعومجم نيوكت ببسب لاصتالا ةلكشم 1.

نېوكت مت اذ AWS تاكېش لخاد ىتح وأ On-PREM ةكېش نم ISE ىل لوصولا نكمي ال :لحل
يف ةبولطملا ذفانملاو تالوكوتورپلاب حامسلا نم دكأت .ححص ريغ لكش ب نامأل اتاعومجم
يتلا ةبولطملا ذفانملا ل ISE [ذفانم عجرم](#) ىل اعجرا . ISE ةكېش ب ةطبترملا نامأل ةعومجم
اهحتف متيس .

2. ححص لكش ب نوكملا ريغ هيچوتلا نع ةمجانلا لاصتالا تالكش م .

AWS و On-Prem ةكېش نيب تاراسملا ضعب دقف لهسلا نم ،ططخملا ديقتل ارطن :لحل
لماش لاصتالا دوجو نم دكأت ، ISE تازيم مادختسا نم نكمتت نأ لب ق .

قحل م لا

AAA/RADIUS لوجم ل اب طبترملا نيوكتلا

```
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
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل