Cisco ISE on Amazon Web Services

- Cisco ISE on Amazon Web Services, on page 1
- Prerequisites to Create a Cisco ISE AWS Instance, on page 3
- Known Limitations of Using Cisco ISE on AWS, on page 3
- Launch a Cisco ISE CloudFormation Template Through AWS Marketplace, on page 5
- Launch Cisco ISE with CloudFormation Template, on page 8
- Launch a Cisco ISE AMI, on page 11
- Postinstallation Notes and Tasks, on page 14
- Compatibility Information for Cisco ISE on AWS, on page 15
- Retrieve deprecated Amazon Machine Images in AWS, on page 15
- Password Recovery and Reset on AWS, on page 16

Cisco ISE on Amazon Web Services

Extend the Cisco ISE policies in your home network to new remote deployments securely through Amazon Web Services (AWS).

You can configure and launch Cisco ISE in AWS through AWS CloudFormation Templates (CFTs) or Amazon Machine Images (AMIs). We recommend that you use CFTs through one of the ways in the following list. To launch Cisco ISE on AWS, perform one of the following procedures:

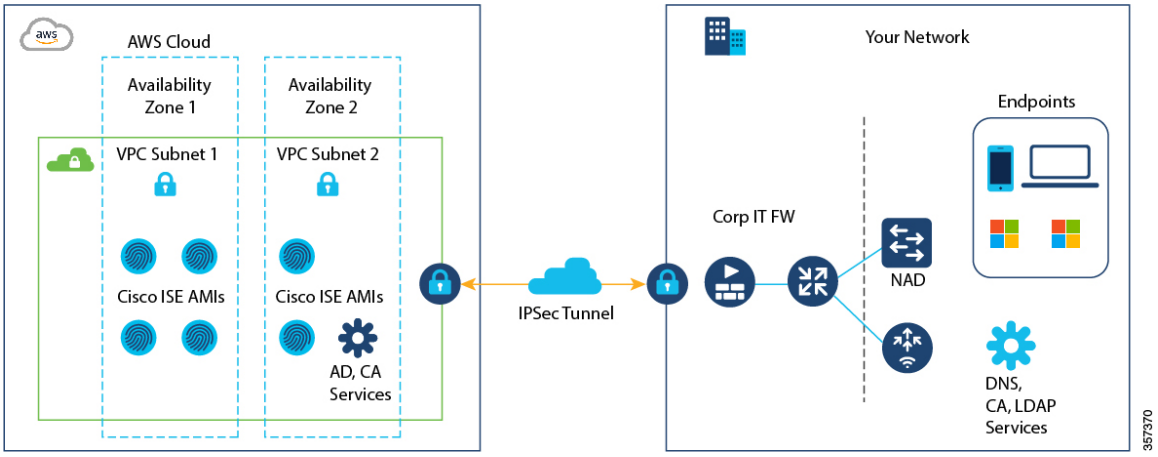
- Launch a Cisco ISE CloudFormation Template Through AWS Marketplace, on page 5
- Launch Cisco ISE with CloudFormation Template, on page 8
- Launch a Cisco ISE AMI

CFTs are AWS solutions that allow you to easily create and manage cloud deployments. Extend your network into the cloud by creating a virtual private cloud in AWS and configure a virtual private gateway to enable communication with your organization's network over an IPsec tunnel.

The following illustration is only an example. You can place common services such as Certificate Authority (CA), Active Directory (AD), Domain Name System (DNS) servers, and Lightweight Directory Access Protocol (LDAP) on premises or in AWS, based on the requirements of your organization.

Cisco ISE on Amazon Web Services

Figure 1: An Example of a Deployment Connected to AWS Cloud



For information about using CFTs in AWS, see the AWS CloudFormation User Guide.

The following table contains details of the Cisco ISE instances that are currently available. You must purchase a Cisco ISE VM license to use any of the following instances. See Amazon EC2 On-Demand Pricing for information on EC2 instance pricing for your specific requirements.

Table 1: Cisco ISE Instances

Cisco ISE Instance Type	CPU Cores	RAM (in GB)
t3.xlarge This instance supports the Cisco ISE evaluation use case and is supported in Cisco ISE Release 3.1 Patch 1 and later. 100 concurrent active endpoints are supported.	4	16
m5.2xlarge	8	32
c5.4xlarge	16	32
m5.4xlarge	16	64
c5.9xlarge	36	72
m5.8xlarge	32	128
m5.16xlarge	64	256

Compute-optimized instances such as c5.4xlarge and c5.9xlarge are intended for compute-intensive tasks or applications and are best suited for Policy Service Node (PSN) use.

General purpose instances such as m5.4xlarge, m5.8xlarge, and m5.16xlarge are intended for data processing tasks and database operations and are best suited for use as Policy Administration Node (PAN) or Monitoring and Troubleshooting (MnT) nodes, or both.

If you use a general purpose instance as a PSN, the performance numbers are lower than the performance of a compute-optimized instance as a PSN.

The m5.2xlarge instance must be used as an extra small PSN only.

For information on the scale and performance data for AWS instance types, see the *Performance and Scalability Guide for Cisco Identity Services Engine*.

You can leverage the AWS S3 storage service to easily store backup and restore files, monitoring and troubleshooting reports, and more.

In addition to the procedures explained above, you can also use the following Cisco developed solutions to install and automatically create multinode Cisco ISE deployments on AWS:

- Cisco ISE AWS Partner Solution for small deployments.
- Cisco Developed Terraform Script for deployments of any size.

Prerequisites to Create a Cisco ISE AWS Instance

- You must be familiar with AWS solutions such as Amazon Elastic Compute Cloud (EC2) instances and Amazon Elastic Block Store (EBS) volumes, and concepts such as Regions, Availability Zones, Security Groups, Virtual Private Cloud (VPC), and so on. See the AWS documentation for information on these solutions.

  You must also be familiar with managing AWS service quotas.

- You must configure VPC in AWS.

  See VPC with public and private subnets and AWS Site-to-Site VPN access.

- To create encrypted EBS volumes, your AWS Identity and Access Management (IAM) policy must allow access to Key Management Service (KMS) resources. See Policies and permissions in IAM.

- Create security groups, subnets, and key pairs in AWS before you configure a Cisco ISE instance.

  When you create a security group for Cisco ISE, you must create rules for all the ports and protocols for the Cisco ISE services you want to use. See Chapter "Cisco ISE Ports Reference" in the *Cisco ISE Installation Guide* for your release.

- To configure an IPv6 address for the network interface, the subnet must have an IPv6 Classless Inter-Domain Routing (CIDR) pool that is enabled in AWS.

- The IP address that you enter in the **Management Network** field in the Cisco ISE CloudFormation template must not be an IP address that exists as a network interface object in AWS.

- You can configure a static IP as a private IP in your deployment. However, the static IP must be configured with a DNS-resolvable hostname.

Known Limitations of Using Cisco ISE on AWS

The following are the known limitations with using Cisco ISE in AWS:

- You cannot take an Amazon EBS snapshot of a Cisco ISE instance and then create another EBS volume with the snapshot.

- The Amazon VPC supports only Layer 3 features. Cisco ISE nodes on AWS instances do not support Cisco ISE functions that depend on Layer 1 and Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocols that use the Cisco ISE CLI is currently not supported.

- NIC bonding is not supported.
- Dual NIC is supported with only two NICs—Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC in your Cisco ISE instance, you must first create a network interface object in AWS, power off your Cisco ISE instance, and then attach this network interface object to Cisco ISE. After you install and launch Cisco ISE on AWS, use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.
- Cisco ISE upgrade workflow is not available in Cisco ISE on AWS. Only fresh installs are supported. However, you can carry out backup and restore of configuration data. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- SSH access to Cisco ISE CLI using password-based authentication is not supported in AWS. You can only access the Cisco ISE CLI through a key pair, and this key pair must be stored securely.

  If you use a private key (or PEM) file and you lose the file, you will not be able to access the Cisco ISE CLI.

  Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported, for example, Cisco DNA Center Release 2.1.2 and earlier.
- You might receive an `Insufficient Virtual Machine Resources` alarm when Cisco ISE is in idle state. You can ignore this alarm because the CPU frequency is maintained lower than the required baseline frequency (2 GHz) for effective power conservation.
- In the software version Cisco ISE 3.1, when you run the **show inventory** command through a Cisco ISE instance that is launched through AWS, the output for the command does not display the instance type of the Cisco ISE on AWS in the output. This issue does not occur with software versions Cisco ISE 3.1 Patch 1 and later releases.
- You cannot configure an IPv6 server as an NTP server when launching Cisco ISE through AWS.
- An initial administrator user account name, iseadmin, is generated by default. This user account name is used for both SSH and GUI access to Cisco ISE after the installation process is complete.
- You cannot resize an EC2 instance.
- You cannot convert the Cisco ISE Disk EBS Volume as an AMI and then relaunch another EC2 instance with this AMI.
- You cannot change the IP address or the default gateway of an instance after it has been created successfully.
- You can integrate the external identity sources that are located on the premises. However, because of latency, when on-premises identity sources are used, Cisco ISE performance is not at par with Cisco ISE performance when AWS-hosted identity sources or the Cisco ISE internal user database is used.
- The following deployment types are supported, but you must ensure that internode latencies are below 300 milliseconds:
  - Hybrid deployments with some Cisco ISE nodes on premises and some nodes in AWS.
  - Inter-region deployments through VPC peering connections.
- Amazon EC2 user data scripts are not supported.

- In the Cisco ISE CFT that you configure, you define Volume Size in GB. However, AWS creates EBS storage volumes in Gibibyte (GiB). Therefore, when you enter 600 as the Volume Size in the Cisco ISE CFT, AWS creates 600 GiB (or 644.25 GB) of EBS volume.
- When you run the restore operation during a configuration data backup through the Cisco ISE CLI or GUI, do not include the ADE-OS parameter.
- IMDSv2 metadata is supported in Cisco ISE release 3.1 patch 8, Cisco ISE release 3.2 patch 4, Cisco ISE release 3.3 patch 1, Cisco ISE release 3.4, and later releases. In all earlier versions, IMDSv1 metadata is supported.

Note

- The communication from on-prem devices to the VPC must be secure.
- In Cisco ISE Release 3.1 Patch 3, Cisco ISE sends traffic to AWS Cloud through IP address 169.254.169.254 to obtain the instance details. This is to check if it is a cloud instance and can be ignored in on-prem deployments.

Launch a Cisco ISE CloudFormation Template Through AWS Marketplace

This method may launch standalone Cisco ISE instances only. To create a Cisco ISE deployment, see the Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

Note

- You cannot add multiple DNS or NTP servers through the CFT. After you create a Cisco ISE instance, you can add more DNS or NTP servers through the Cisco ISE CLI. However, from Cisco ISE Release 3.4, you can add secondary and tertiary DNS or NTP servers through the CFT.
- You cannot configure IPv6 DNS or NTP servers through the CFT. You can use the Cisco ISE CLI to configure IPv6 servers.

The Cisco ISE CFT creates an instance of the General Purpose SSD (gp2) volume type.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

Before you begin

In AWS, create the security groups and management networks that you want to include in your Cisco ISE CFT configuration.

Procedure

Step 1 Log in to the Amazon Management Console at https://console.aws.amazon.com/, and search for **AWS Marketplace Subscriptions**.

Step 2 In the **Manage Subscriptions** window that is displayed, click **Discover Products** in the left pane.

Step 3 Enter **Cisco Identity Services Engine (ISE)** in the search bar.

Step 4 Click the product name.

Step 5 In the new window that is displayed, click **Continue to Subscribe**.

Step 6 Click **Continue to Configuration**.

Step 7 In the **Configure this software** area, click **Learn More** and then click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

You can also click **View Template** in the **Learn More** dialog box to view the CFT in the AWS CloudFormation Designer.

Step 8 Choose the required values from the **Software Version** and **AWS Region** drop-down lists.

Step 9 Click **Continue to Launch**.

Step 10 Choose **Launch CloudFormation** from the **Choose Action** drop-down list.

Step 11 Click **Launch**.

Step 12 In the **Create Stack** window, click the **Template Is Ready** and **Amazon S3 URL** radio buttons.

Step 13 Click **Next**.

Step 14 In the new window, enter a value in the **Stack Name** field.

Step 15 Enter the required details in the following fields in the **Parameters** area:

- **Hostname**: This field only supports alphanumeric characters and hyphens (-). The length of the hostname can't exceed 19 characters.
- **Instance Key Pair**: To access the Cisco ISE instance through SSH, choose the PEM file that you created in AWS for the username iseadmin (username admin, for Cisco ISE Release 3.1). Create a PEM key pair in AWS now if you have not configured one already. An example of an SSH command in this scenario is **ssh -i mykeypair.pem iseadmin@myhostname.compute-1.amazonaws.com**.
- **Management Security Group**: Choose the security group from the drop-down list. You must create the security group in AWS before configuring this CFT.

  Note
  You can add only one security group in this step. You can add additional security groups in Cisco ISE after installation. The network traffic rules that you want to be available in Cisco ISE at launch must be configured in the security group that you add here.

- **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.
- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

After the Cisco ISE instance is created, copy the private IP address from the **Instance Summary** window. Then, map the IP and hostname in your DNS server before you create a Cisco ISE deployment.

- **Timezone**: Choose a system time zone from the drop-down list.
- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is **False**. The default value for this field is **False**. In Cisco ISE Release 3.3 and later releases, the default value of the **EBS Encryption** field is **True**.
- (Optional) **KMS Key**: Enter the **KMS Key** or Amazon Resource Name or alias for data encryption.

  Note
  This is an optional field applicable for Cisco ISE Release 3.3 and later releases. If the **KMS Key** is provided, it will be used for data encryption. If the **KMS Key** is not provided, the default key will be used for data encryption.

- **Volume Size**: Specify the volume size, in GB. The accepted range is 300 GB to 2400 GB. We recommend 600 GB for production use. Configure a volume size lesser than 600 GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note
  AWS creates EBS storage volumes in Gibibyte (GiB). When you enter 600 in the **Volume Size** field, AWS creates 600 GiB (or 644.25 GB) of EBS volume.

- **DNS Domain**: Accepted values for this field are ASCII characters, numerals, hyphen (-), and period (.).
- **Name Server**: Enter the IP address of the name server in the correct syntax.

  Note
  You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation. From Cisco ISE Release 3.4, you can add secondary and tertiary DNS servers as well in this step. If the **Secondary DNS Server** field is left blank, you cannot use the **Tertiary DNS Server** option.

- **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.

  Note
  If the IP address or the hostname that you enter here is incorrect, Cisco ISE cannot synchronize with the NTP server. Use an SSH terminal to log in to Cisco ISE and then use the Cisco ISE CLI to configure the correct NTP server.

  You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation. From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary NTP Server** field is left blank, you cannot use the **Tertiary NTP Server** option.

- **ERS**: To enable External RESTful Services (ERS) services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **OpenAPI**: To enable OpenAPI services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **pxGrid**: To enable pxGrid services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **pxGrid Cloud**: The default value for this field is **no**.

- **Enter Password**: Enter the administrative password that must be used for GUI. The password must be compliant with the Cisco ISE password policy. The password is displayed in plain text in the **User Data** area of the instance settings window in the AWS console. See the "User Password Policy" section in the Chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- **Confirm Password**: Re-enter the administrative password.

Step 16 Click **Next** to initiate the instance-creation process.

Launch Cisco ISE with CloudFormation Template

This method may launch standalone Cisco ISE instances only. To create a Cisco ISE deployment, see the chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

Note
- You cannot add multiple DNS or NTP servers through the CFT. After you create a Cisco ISE instance, you can add additional DNS or NTP servers through the Cisco ISE CLI. However, from Cisco ISE Release 3.4, you can add secondary and tertiary DNS or NTP servers through the CFT.
- You cannot configure IPv6 DNS or NTP servers through the CFT. You can only use the Cisco ISE CLI to configure IPv6 servers.

The Cisco ISE CFT creates an instance of the General Purpose SSD (gp2) volume type.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically; there's no need to send OpenAPI-related options while launching an instance.

Before you begin

In AWS, create the security groups and management networks that you want to include in your Cisco ISE CFT configuration.

Procedure

Step 1 Log in to the Amazon Management Console at https://console.aws.amazon.com/ and search for **AWS Marketplace Subscriptions**.

Step 2 In the **Manage Subscriptions** window, click **Discover Products** in the left pane.

Step 3 Enter **Cisco Identity Services Engine (ISE)** in the search bar.

Step 4 Click the product name.

Step 5 In the new window that is displayed, click **Continue to Subscribe**.

Step 6 Click **Continue to Configuration**.

Step 7 In the **Configure this software** area, click **Learn More** and then click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

You can also click **View Template** in the **Learn More** dialog box to view the CFT in the AWS CloudFormation Designer.

Step 8 Using the AWS search bar, search for **CloudFormation**.

Step 9 From the **Create Stack** drop-down list, choose **With new resources (standard)**.

Step 10 In the **Create Stack** window, choose **Template Is Ready** and **Upload a Template File**.

Step 11 Click **Choose File** and upload the CFT file that you downloaded in Step 7.

Step 12 Click **Next**.

Step 13 In the new window, enter a value in the **Stack Name** field.

Step 14 Enter the required details in the following fields in the **Parameters** area:

- **Hostname**: This field only supports alphanumeric characters and hyphens (-). The length of the hostname can't exceed 19 characters.
- **Instance Key Pair**: To access the Cisco ISE instance through 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. An example of an SSH command in this scenario is **ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com**.
- **Management Security Group**: Choose the security group from the drop-down list. You must create the security group in AWS before configuring this CFT.

  Note
  You can add only one security group in this step. You can add additional security groups in Cisco ISE after installation. The network traffic rules that you want available in Cisco ISE at instance launch must be configured in the security group that you add here.

- **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.
- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

  After the Cisco ISE instance is created, copy the private IP address from the **Instance Summary** window. Then, map the IP address and hostname in your DNS server before you create a Cisco ISE deployment.
- **Timezone**: Choose a system time zone from the drop-down list.
- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is **False**. In Cisco ISE Release 3.3 and later, the default value of the **EBS Encryption** field is **True**.
- (Optional) **KMS Key**: Enter the **KMS Key** or Amazon Resource Name or alias for data encryption.

  Note
  This is an optional field applicable for Cisco ISE Release 3.3 and later. If the **KMS Key** is provided, it will be used for data encryption. If the **KMS Key** is not provided, the default key will be used for data encryption.

- **Volume Size**: Specify the volume size in GB. The accepted range is 300 GB to 2400 GB. We recommend 600 GB for production use. Configure a volume size less than 600 GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note
  AWS creates EBS storage volumes in Gibibyte (GiB). When you enter 600 in the **Volume Size** field, AWS creates 600 GiB (or 644.25 GB) of EBS volume.

- **DNS Domain**: Accepted values for this field are ASCII characters, numerals, hyphens (-), and periods (.).
- **Name Server**: Enter the IP address of the name server in correct syntax.

  Note
  You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation.

  From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary DNS Server** field is left blank, you cannot use the **Tertiary DNS Server** option.

- **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.

  Note
  If the IP address or the hostname that you enter here is incorrect, Cisco ISE cannot synchronize with the NTP server. Use an SSH terminal to log in to Cisco ISE and use the Cisco ISE CLI to configure the correct NTP server.

  You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation.

  From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary NTP Server** field is left blank, you cannot use the **Tertiary NTP Server** option.

- **ERS**: To enable ERS services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **OpenAPI**: To enable OpenAPI services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **pxGrid**: To enable pxGrid services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.
- **pxGrid Cloud**: The default value for this field is **no**.

  Note
  The pxGrid Cloud feature is not available because there are dependencies on complementary product releases. Do not enable pxGrid Cloud services.

- **Enter Password**: Enter the administrative password that must be used for GUI. The password must be compliant with the Cisco ISE password policy. The password is displayed in plain text in the **User Data** area of the instance settings window in the AWS console. See the "User Password Policy" section in the chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- **Confirm Password**: Re-enter the administrative password.

Step 15 Click **Next** to initiate the instance-creation process.

Launch a Cisco ISE AMI

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

Procedure

Step 1 Log in to your Amazon EC2 console at https://console.aws.amazon.com/ec2/.

Step 2 In the left pane, click **Instances**.

Step 3 In the **Instances** window, click **Launch Instances**.

Step 4 In the **Step 1: Choose AMI** window, in the left menu, click **AWS Marketplace**.

Step 5 In the search field, enter **Cisco Identity Services Engine**.

Step 6 In the **Cisco Identity Services Engine (ISE)** option, click **Select**.

A **Cisco Identity Services Engine (ISE)** dialog box is displayed with various details of the AMI.

Step 7 Review the information and click **Continue** to proceed.

Step 8 In the **Step 2: Choose an Instance Type** window, click the radio button next to the instance type that you want to use.

Step 9 Click **Next: Configure Instance Details**.

Step 10 In the **Step 3: Configure Instance Details** window, enter the required details in the following fields:

- **Number of Instances**: Enter **1** in this field.
- **Network**: From the drop-down list, choose the VPC in which you want to launch the Cisco ISE instance.
- **Subnet**: From the drop-down list, choose the subnet in which you want to launch the Cisco ISE instance.
- **Network Interfaces**: The drop-down list displays **New Network Interface** by default, which means that an IP address is auto-assigned to Cisco ISE by the connected DHCP server. You can choose to enter an IP address in this field to assign a fixed IP address to Cisco ISE. You can also choose an existing network interface from the same subnet, from the **Network Interfaces** drop-down list. You can only configure one interface during the setup process. After Cisco ISE is installed, you can add more interfaces through Cisco ISE.

Step 11 In the **Advanced Details** area, in the **User Data** area, click the **As Text** radio button and enter the key-value pairs in the following format:

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

tertiarynameserver=<*IPv4 address of tertiary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

timezone=<*timezone*>

username=<*admin*>

Note
From Cisco ISE release 3.2, the username is fixed as iseadmin; therefore, the tag username=<admin> is not supported.

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important
From Cisco ISE Release 3.4,

a. The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start.

b. OpenAPI is enabled by default. Hence, the **openapi=<yes/no>** field is not required.

c. If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start.

d. If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start.

You must use the correct syntax for each of the fields that you configure through the user data entry. The information you enter in the **User Data** field is not validated when it is entered. If you use the wrong syntax, Cisco ISE services might not come up when you launch the AMI. The following are the guidelines for the configurations that you submit through the **User Data** field:

- hostname: Enter a hostname that contains only alphanumeric characters and hyphen (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).
- primarynameserver: Enter the IP address of the primary name server. Only IPv4 addresses are supported. From Cisco ISE Release 3.4, you can configure secondarynameserver and tertiarynameserver during installation by using the **secondarynameserver** and **tertiarynameserver** fields.
- dnsdomain: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- ntpserver: Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov. From Cisco ISE Release 3.4, you can configure secondary and tertiary NTP servers during installation by using the **secondaryntpserver** and **tertiaryntpserver** fields.
- timezone: Enter a timezone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized.

- password: Configure a password for GUI-based login to Cisco ISE. The password that you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least one numeral, one uppercase letter, and one lowercase letter. The password cannot contain or be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. See the "User Password Policy" section in the Chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- ersapi: Enter **yes** to enable ERS, or **no** to disallow ERS.
- openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.
- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- pxgrid_cloud: Enter **yes** to enable pxGrid Cloud or **no** to disallow pxGrid Cloud. To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled at launch.

Step 12 Click **Next: Add Storage**.

Step 13 In the **Step 4: Add Storage** window:

a) Enter a value in the **Size (GiB)** column.

The valid range for this field is 279.4 to 2235.2 GiB. In a production environment, you must configure storage equal to or greater than 558.8 GiB. Storage lesser than 558.8 GiB only supports an evaluation environment. Note that Cisco ISE is created with storage defined in GB. The GiB value that you enter here is automatically converted into GB values during the Cisco ISE image-creation process. In GB, the valid storage range is 300 to 2400 GB, with 600 GB as the minimum value for a Cisco ISE in a production environment.

b) From the **Volume Type** drop-down list, choose **General Purpose SSO (gp2)**.

c) To enable EBS encryption, from the **Encryption** drop-down list, choose an encryption key.

Note
Do not click the **Add New Volume** button that is displayed on this window.

Step 14 Click **Next: Add Tags**.

Step 15 (Optional) In the **Step 5: Add Tags** window, click **Add Tag** and enter the required information in the **Key** and **Value** fields. The check boxes in the **Instances**, **Volumes**, and **Network Interfaces** columns are checked by default. If you have chosen a specific network interface in the **Step 3: Configure Instance Details** window, you must uncheck the **Network Interfaces** check box for each tag that you add in this window.

Step 16 Click **Next: Configure Security Group**.

Step 17 In the **Step 6: Configure Security Group** window, in **Assign a security group area**, you can choose to create a new security group or choose an existing security group by clicking the corresponding radio button.

a) If you choose **Create a new security group**, enter the required details in the **Type**, **Protocol**, **Port Range**, **Source**, and **Description** fields.

b) If you choose **Select an existing security group**, check the check boxes next to the security groups you want to add.

Step 18 Click **Review and Launch**.

Step 19 In the **Step 7: Review Instance Launch** window, review all the configurations that you have created in this workflow. You can edit the values of these sections by clicking the corresponding **Edit** link.

Step 20 Click **Launch**.

Step 21 In the **Select an existing key pair or create a new key pair** dialog box choose one of the following options from the drop-down list:

- **Choose an existing key pair**
- **Create a new key pair**

Note
To use SSH to log in to Cisco ISE, use a key pair where the username is **iseadmin**. The key pair must be kept intact. If the key pair is lost or corrupted, you cannot recover your Cisco ISE because you cannot map a new key pair to the existing instance.

Step 22 Check the check box for the acknowledgment statement and click **Launch Instances**.

The **Launch Status** window displays the progress of the instance creation.

Postinstallation Notes and Tasks

To check the status of the instance launch, in the left pane of the AWS console, click **Instances**. The **Status Check** column for the instance displays **Initializing** while the instance is being configured. When the instance is ready and available, the column displays **x checks done**.

You can access the Cisco ISE GUI or CLI about 30 minutes after the Cisco ISE EC2 instance is built. You can access the CLI and GUI of Cisco ISE with the IP address that AWS provides for your instance, and log in to the Cisco ISE administration portal or console.

When the Cisco ISE instance is ready and available for use, carry out the following steps:

1. When you create a key pair in AWS, you are prompted to download the key pair into your local system. Download the key pair because it contains specific permissions that you must update to successfully log in to your Cisco ISE instance from an SSH terminal.

   If you use Linux or MacOS, run the following command from your CLI:

   sudo chmod 0400 mykeypair.pem

   If you use Windows:

   a. Right-click the key file in your local system.

   b. Choose **Properties** > **Security** > **Advanced**.

   c. In the **Permissions** tab, assign full control to the appropriate user by clicking the corresponding option, and click **Disable Inheritance**.

   d. In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.

   e. In the **Permissions** tab, in the **Permissions entries** area, choose system and administrator users by clicking the corresponding entries, and then click **Remove.**

   f. Click **Apply**, and then click **OK**.

2. Access the Cisco ISE CLI by running the following command in your CLI application:

   ssh -i mykeypair.pem iseadmin@<*Cisco ISE Private IP Address*>

3. At the login prompt, enter **iseadmin** as the username.

4. At the system prompt, enter **show application version ise** and press **Enter**.
5. To check the status of the Cisco ISE processes, enter **show application status ise** and press **Enter**.

   If the output displays that an application server is in Running state, Cisco ISE is ready for use.
6. You can then log in to the Cisco ISE GUI.
7. Carry out the postinstallation tasks listed in the topic "List of Post-Installation Tasks" in the Chapter "Installation Verification and Post-Installation Tasks" in the *Cisco ISE Installation Guide* for your release.

Compatibility Information for Cisco ISE on AWS

This section details compatibility information that is unique to Cisco ISE on AWS. For general compatibility details for Cisco ISE, see Cisco Identity Services Engine Network Component Compatibility, Release 3.1.

Cisco DNA Center Integration Support

You can connect your Cisco ISE to Cisco DNA Center Release 2.2.1 and later releases.

Load Balancer Integration Support

You can integrate the AWS-native Network Load Balancer (NLB) with Cisco ISE for load balancing the RADIUS traffic. However, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in NLB.
- Unequal load balancing might occur because NLB only supports source IP affinity and not the calling station ID-based sticky sessions.
- Traffic can be sent to a Cisco ISE PSN even if the RADIUS service is not active on the node because NLB does not support RADIUS-based health checks.

You can integrate the AWS-native Network Load Balancer (NLB) with Cisco ISE for load balancing TACACS traffic. However, traffic might be sent to a Cisco ISE PSN even if the TACACS service is not active on the node because NLB does not support health checks based on TACACS+ services.

NIC Jumbo Frame Support

Cisco ISE supports jumbo frames. The Maximum Transmission Unit (MTU) for Cisco ISE is 9,001 bytes, while the MTU of Network Access Devices is typically 1,500 bytes. Cisco ISE supports and receives both standard and jumbo frames without issue. You can reconfigure the Cisco ISE MTU as required, through the Cisco ISE CLI in configuration mode.

Retrieve deprecated Amazon Machine Images in AWS

Amazon Machine Images (AMIs) are given an automatic two-year deprecation date from the day they are published in AWS. AWS hides all AMI IDs after their deprecation date, meaning that images cannot be found in the AMI Catalog or EC2 Console but are still available when referenced explicitly by their AMI ID. You can retrieve deprecated AMIs from AWS marketplace or by using the AWS CLI.

For information on how to fetch deprecated AMIs using the AWS CLI, see Describe deprecated AMIs.

Follow these steps to retrieve deprecated AMIs from AWS marketplace.

Procedure

Step 1 Login to AWS marketplace.

Step 2 Search for **ISE** using the search bar.

Step 3 Select **Cisco Identity Services Engine (ISE)** from the search results.

Step 4 Click **Continue to Subscribe**.

Step 5 Click **Continue to Configuration**.

Step 6 From the **Fulfillment option** drop-down list, select **Amazon Machine Image**.

Step 7 From the **Software version** drop-down list, select the required software version.

Step 8 From the **Region** drop-down list, select the required region.

Step 9 Click **Continue to Launch**.

Step 10 From the **Choose Action** drop-down list, select **Launch through EC2**.

Step 11 Click **Launch**.

A new tab opens showing the required region and the EC2 console which can be used to launch the instance.

Step 12 From the **AMI from catalog** tab in the **Application and OS Images (Amazon Machine Image)** section, copy the deprecated AMI IDs for the chosen region.

Password Recovery and Reset on AWS

The following tasks guide you through the tasks that help your reset your Cisco ISE virtual machine password. Choose the tasks that you need and carry out the steps detailed.

Change Cisco ISE GUI Password via Serial Console

Procedure

Step 1 Log in to your AWS account and go to the EC2 dashboard.

Step 2 Click **Instances** from the left-side menu.

Step 3 Click the instance ID for which you need to change the password. If you know the password, skip to Step 5 of this task.

Step 4 To log in to the serial console, you must use the original password that was set at the installation of the instance. To view the configured password, carry out the following steps:

a) Click **Actions**.

b) Choose **Instance Settings**.

c) Click **Edit user data**.

The current user data is displayed, including the password.

Step 5 Click **Connect**.

The EC2 serial console tab is displayed.

Step 6 Click **Connect**.

Step 7 A new browser tab is displayed. If the screen is black, press Enter to view the login prompt.

Step 8 Log in to the serial console. If the password that was displayed in Step 4 does not work, see the Password Recovery section.

Step 9 Use the **application reset-passwd ise iseadmin** command to set a new web UI password for the iseadmin account.

Create New Public Key Pair

Through this task, you add additional key pairs to a repository. The existing key pair that was created at the time of Cisco ISE instance configuration is not replaced by the new public key that you create.

Procedure

Step 1 Create a new public key in AWS. For instructions on how to create public key pairs, see Create key pairs.

Step 2 Log in to the AWS serial console as detailed in the preceding task.

Step 3 To create a new repository to save the public key to, see Creating a private repository.

If you already have a repository that is accessible through the CLI, skip to the next step.

Step 4 To import the new public key, use the command **crypto key import <public key filename> repository <repository name>**

Step 5 When the import is complete, you can log in to Cisco ISE via SSH using the new public key.

Password Recovery

There is no mechanism for password recovery for Cisco ISE on AWS. You may need to create new Cisco ISE instances and perform backup and restore of configuration data.

Editing the user data for an EC2 instance in AWS does not change the CLI password that is used to log in to the serial console, as the setup script is not run. The Cisco ISE virtual instance is not affected.