Setting Up Cisco ISE in a Distributed Environment

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary Administration node to manage the secondary ISE nodes that are deployed onto the network.

Cisco ISE provides distributed deployment of runtime services with centralized configuration and management. Multiple nodes can be deployed together in a distributed fashion to support failover.

This chapter describes the personas, roles, and services that constitute Cisco ISE, and how to configure Cisco ISE nodes.

For information about the Cisco ISE deployment scenarios, refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*.

This chapter contains the following topics:

Cisco ISE Deployment Terminology

The following terms are commonly used when discussing Cisco ISE deployment scenarios:

- Service—A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, monitoring and troubleshooting, and so on.

- Node—A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on VMware. Each instance, appliance or VMware that runs the Cisco ISE software is called a node.
- Persona—The persona or personas of a node determine the services provided by a node. An Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring, and Inline Posture. A Cisco ISE node can assume the Administration, Policy Service, and Monitoring personas. The Inline Posture persona requires a dedicated Cisco ISE node. The menu options that are available through the Admin portal are dependent on the role and personas that an Cisco ISE node assumes.
- Deployment Model—Determines if your deployment is distributed, standalone, or high availability in standalone, which is a basic two-node deployment.

Related Topics

Menu Options Available on Primary and Secondary Nodes, page 3-10

Personas in Distributed Cisco ISE Deployments

A Cisco ISE node can assume any of the following personas:

- Administration Node
- Policy Service Node
- Monitoring Node
- Inline Posture Node

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment, with the exception of the Inline Posture node, can assume the Administration, Policy Service, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration nodes for high availability
- A pair of Monitoring nodes for automatic failover
- One or more Policy Service nodes for session failover
- A pair of Inline Posture nodes for high availability

You need to add Canonical Name (CNAME) record of the ISE hostname to the DNS. Ensure that you create CNAME RR along with the A record for each Cisco ISE node. If CNAME record is not created, it might result in the alarm ‘DNS Resolution failed for CNAME <hostname of the node>’.

Administration Node

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all system-related configurations that are related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the administration persona. The administration persona can take on any one of the following roles: Standalone, Primary, or Secondary.

High Availability in Administration Nodes

In a high-availability configuration, the primary Administration node is in the active state to which all configuration changes are made. The secondary Administration node is in the standby state, and will receive all configuration updates from the primary Administration node. Therefore, it will always have a complete copy of the configuration from the primary Administration node.

If the primary Administration node goes down, you must log in to the user interface of the secondary Administration node and manually promote the secondary Administration node. There is no automatic failover for the Administration persona.

You can use Cisco ISE appliances (ISE 3300 series or SNS 3400 series) or virtual machines or a combination of both to set up a primary-secondary pair of Administration nodes. However, you must ensure that the virtual machine's hardware specification is comparable with the Cisco ISE appliance. See VMware Appliance Specifications for a Production Environment for more details.

When the primary Administration node is down, Sponsor administrators cannot create new guest user accounts. During this time, the guest and sponsor portals will provide read-only access to already created guest and sponsor users, respectively. Also, a sponsor administrator who has never logged in to the sponsor portal before the primary Administration node went offline, will not be able to log in to the sponsor portal until a secondary Administration node is promoted or the primary Administration node becomes available.

At least one node in your distributed setup should assume the Administration persona.

Policy Service Node

A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this persona. Typically, there would be more than one Policy Service node in a distributed deployment. All Policy Service nodes that reside behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any pending sessions.

At least one node in your distributed setup should assume the Policy Service persona.

High Availability in Policy Service Nodes

In distributed deployments, you might have multiple Policy Service nodes located behind a load balancer to distribute the requests evenly. The load balancer distributes the requests to the functional nodes behind it. Also, to detect node failure and to reset sessions in pending state on the failed node, two or more Policy Service nodes can be placed in the same node group. When a node that belongs to a node group fails, another node in the same node group issues a Change of Authorization (CoA) for pending sessions on the failed node.

Note A session is said to be in the pending state if it has been authorized, but posture assessment is not yet complete. It is possible to set up a distributed deployment without node groups, but sessions in pending state on a failed Policy Service node will not be automatically reset.

All the nodes in a node group must be configured on the network access device (NAD) as RADIUS clients to issue a CoA. Typically, these nodes would also be configured as RADIUS servers. See the "Enable RADIUS Change of Authorization (CoA)" section on page F-4 for CoA-related configuration on the switch.

While a single NAD can be configured with many ISE nodes as RADIUS servers and dynamic-author clients, it is not necessary for all the nodes to be in the same node group.

All the nodes within the same node group should be configured on the NAD as RADIUS servers and clients, because any one of them can issue a CoA request for the sessions that are established through that NAD to any node in the node group. The nodes in a node group should be the same as, or a subset of, the RADIUS servers and clients configured on the NAD. All the nodes in a node group share the same multicast address and use it to communicate their health status.

Session Failover in Policy Service Nodes

The heartbeat functionality in Cisco ISE handles session failover in Policy Service nodes. When a Policy Service node that has a few active sessions fails, the endpoints are stuck in an intermediate state. Even if the posture agent detects that the Policy Service node that it has been communicating with has failed, it cannot re-initiate authorization.

If the Policy Service nodes are part of a node group, the nodes within a node group exchange heartbeats to detect node failures. If a node fails, one of its peers from the node group learns about the active sessions on the failed node and issues a CoA to disconnect those sessions.

As a result, the sessions are handled by another Policy Service node that is available using RADIUS load balancing. The session failover does not automatically move the sessions over from a Policy Service node that has gone down to one that is available, but issues a CoA to achieve that.

Machine Access Restriction in Policy Service Nodes

The Policy Service nodes in a distributed deployment do not share their Machine Access Restriction (MAR) cache with each other. For example, if a client machine is authenticated by one of the Policy Service nodes that fails, then another Policy Service node in the deployment handles the user authentication. However, the user authentication then fails because the second Policy Service node does not have the host authentication information in its MAR cache.

Number of Nodes in a Policy Service Node Group

The number of nodes that you can have in a node group depends on your deployment requirements. Node groups ensure that node failures are detected and that a peer issues a CoA for sessions that are authorized, but not yet postured. The size of the node group does not have to be very large.

If the size of the node group increases, the number of messages and heartbeats that are exchanged between nodes increases significantly. As a result, multicast traffic also increases. Having fewer nodes in a node group helps reduce the multicast traffic and at the same time provides sufficient redundancy to detect Policy Service node failures.

You can have a maximum of 10 Policy Service nodes in a node group cluster.

If you want to minimize the number of node groups and thereby reduce the number of multicast addresses that must be managed, then you can group all the RADIUS servers and clients that are configured on the NADs as one node group.

If management of multiple multicast addresses is not a problem, but there is a need for minimizing multicast traffic, then you can have fewer nodes in a node group.

Monitoring Node

A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the administration and Policy Service nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports.

Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring nodes collect log messages. In case the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node.

At least one node in your distributed setup should assume the Monitoring persona. We recommend that you not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the node be dedicated solely to monitoring for optimum performance.

You can access the Monitoring menu from the primary Administration node and the primary Monitoring node in your deployment.

Automatic Failover in Monitoring Nodes

The term automatic failover is used because high availability is not supported on Monitoring nodes in the true sense. For Monitoring nodes, operation audit data is duplicated by the Policy Service node(s), which then sends copies to both the primary and secondary Monitoring nodes.

Note Monitoring is served from the primary (active) Monitoring node. Monitoring data is only served from the secondary (standby) Monitoring node when the active node is down. The secondary monitoring node is read-only.

Automatic Failover Process

When a primary Monitoring node goes down, the secondary Monitoring node takes over all monitoring and troubleshooting information. The secondary node provides read-only capabilities.

To convert the existing secondary node to an active primary node, the administrator must first manually promote the secondary node to a primary role. If the primary node comes back up after the secondary node has been promoted, it assumes the secondary role. If the secondary node was not promoted, the primary Monitoring node will resume its role after it comes back up.

Caution When the primary node comes back up after a failover, a manual backup and restore is required to update the primary node so it can reclaim the data that was lost.

Active-Standby Pair of Monitoring Nodes

You can specify two Monitoring nodes on an ISE network and create an active-standby pair. When you register a secondary Monitoring node, we recommend that you back up the primary Monitoring node and then restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated. Once the active-standby pair is defined, the following rules apply:

- All changes must be made on the primary Monitoring node. The secondary node is read-only.
- Changes made to the primary node are automatically replicated on the secondary node.

- Both the primary and secondary nodes are listed as log collectors to which all other nodes send logs.
- The Cisco ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the primary Monitoring node. If the primary node goes down, the information is served from the secondary node.
- Backing up and purging monitoring data is not part of a standard Cisco ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary Monitoring nodes, and use the same repositories for each.

Monitoring Node Failover Scenarios

The following scenarios apply to the active-standby or single node configurations corresponding to the monitoring nodes:

- In an active-standby configuration of the monitoring nodes, the Administrative PAP always points to the active monitoring node to collect the monitoring data. After the active monitoring node fails, the Administrative PAP points to the standby monitoring node. The failover from the active monitoring node to the standby monitoring node happens within a time period of 1 to 10 seconds.

  However, after the active node fails, the standby node does not become the active node. In case the active node comes back up, the Administrative node starts collecting the monitoring data again from the resumed active node.
- During the time that the active monitoring node is down, if you want to promote the standby monitoring node to active status, you must de-register the existing active monitoring node. When you de-register the existing active monitoring node, the standby node becomes the active monitoring node and the Administrative PAP automatically starts pointing to the newly promoted active node.
- In an active-standby pair, if you choose to de-register the standby monitoring node from the deployment or if the standby monitoring node goes down, the existing active monitoring node still retains the active node status. The Administrative PAP points to the existing active node for data collection.
- If there is only one monitoring node in the ISE deployment, then that node acts as the active monitoring node that provides monitoring data to the Administrative PAP. However, when you register a new monitoring node and make it the active node in the deployment, the existing active monitoring node automatically becomes the standby node. The Administrative PAP begins to point to the newly registered active monitoring node for collecting monitoring data.

Related Topics

- Performing an On-Demand Backup, page 12-4
- Restoration of Monitoring Database, page 12-10

Inline Posture Node

An Inline Posture node is a gatekeeping node that is positioned behind network access devices such as Wireless LAN Controllers (WLC) and VPN concentrators on the network. The Inline Posture node enforces access policies after a user has been authenticated and granted access, and handles change of authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability.

The Inline Posture node must be a dedicated node. It must be dedicated solely for inline posture service, and cannot operate concurrently with other Cisco ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. For example, it cannot act as an

Administration node that offers administration service, or a Policy Service node that offers network access, posture, profile, and guest services, or a Monitoring node that offers monitoring and troubleshooting services for a Cisco ISE network.

The Inline Posture persona is not supported on the Cisco ISE 3495 platform. Ensure that you install The Inline Posture persona on any one of the following supported platforms: Cisco ISE 3315, Cisco ISE 3355, Cisco ISE 3395, or Cisco ISE 3415.

Related Topics

Chapter 4, "Setting Up Inline Posture"

Inline Posture Node Installation

You must download the Inline Posture 1.2 ISO image from Cisco.com and install it on any of the supported platforms. You must then configure certificates through the command-line interface (CLI). You can then register this node from the Admin portal.

Note You cannot access the web-based user interface of the Inline Posture nodes. You can configure them only from the primary Administration node.

After you install and set up the Inline Posture application, you must configure certificates before you can register the Inline Posture nodes. See *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2* for more information.

Cisco ISE Distributed Deployment

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and to improve performance, you can set up your deployment with multiple Cisco ISE nodes in a distributed fashion. In Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across the Policy Service nodes. Depending on your performance needs, you can scale your deployment. Each Cisco ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring. The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node.

This section contains the following topics:

Cisco ISE Deployment Setup

After you install Cisco ISE on all your nodes, as described in *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*, the nodes come up in a standalone state. You must then define one node as your primary Administration node. While defining your primary Administration node, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the primary Administration node. After you complete the task of defining personas on the primary Administration node, you can then register other secondary nodes to the primary Administration node and define personas for the secondary nodes.

All Cisco ISE system and functionality-related configurations should be done only on the primary Administration node. The configuration changes that you perform on the primary Administration node are replicated to all the secondary nodes in your deployment.

There must be at least one Monitoring node in a distributed deployment. At the time of configuring your primary Administration node, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the primary Administration node and disable the Monitoring persona, if required.

Data Replication from Primary to Secondary ISE Nodes

When you register an Cisco ISE node as a secondary node, Cisco ISE immediately creates a database link from the primary to the secondary node and begins the process of replication. Replication is the process of sharing Cisco ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in all Cisco ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. Incremental replication occurs after a full replication and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the primary Administration node are reflected in the secondary nodes. The process of replication ensures that all Cisco ISE nodes in a deployment are in sync. You can view the status of replication in the Node Status column from the deployment pages of the Cisco ISE Admin portal. When you register a Cisco ISE node as a secondary node or perform a manual synchronization with the primary Administration node, the node status shows an orange icon indicating that the requested action is in progress. Once it is complete, the node status turns green indicating that the secondary node is synchronized with the primary Administration node. After the node status turns green, it takes about five minutes for the Cisco ISE application server to restart and run to complete the secondary ISE node configuration.

Cisco ISE Node Deregistration

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary Administration node, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered standalone node.

Note You cannot deregister a primary Administration node.

Related Topics

Chapter 4, “Setting Up Inline Posture”

Automatic Restart of the Cisco ISE Application Server

The application server in an Cisco ISE node restarts which causes a delay when you make any of the following changes:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an Administration node (Secondary to Primary)
- Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
- Modify the services in the Policy Service node (enable or disable the session and profiler services)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment.

- Choose a node type—ISE node or Inline Posture node. For Administration, Policy Service, and Monitoring capabilities, you must choose an ISE node. For Inline Posture service, you must choose the Inline Posture node.
- Choose the same Network Time Protocol (NTP) server for all the nodes—To avoid timezone issues among the nodes, you must provide the same NTP server name during the setup of each node. This setting ensures that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.
- Configure the Cisco ISE Admin password when you install Cisco ISE. The previous Cisco ISE Admin default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup or the current password if it was changed later.
- Configure the Domain Name System (DNS) server—Enter the IP addresses and fully qualified domain names (FQDNs) of all the Cisco ISE nodes that are part of your distributed deployment in the DNS server. Otherwise, node registration will fail.
- Configure the Reverse DNS lookup for all Cisco ISE nodes in your distributed deployment in the DNS server. Otherwise, you may run into deployment related issues when registering Cisco ISE nodes, and restarting Cisco ISE nodes.
- (Optional) Deregister a secondary Cisco ISE node from the primary Administration node to uninstall Cisco ISE from it.
- Back up the primary Monitoring node, and restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated.
- Ensure that the primary Administration node and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE.
- Ensure that the database passwords of the primary and secondary nodes are the same. If these passwords are set differently during node installation, you can modify them using the following commands:

- **application reset-passwd ise internal-database-admin**
- **application reset-passwd ise internal-database-user**

Refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2* for more details on how to use Cisco ISE CLI commands.

Related Topics

- Performing an On-Demand Backup, page 12-4
- Restoration of Monitoring Database, page 12-10

Menu Options Available on Primary and Secondary Nodes

Cisco ISE nodes provide you an Admin portal that you can use to perform your tasks. The menu options available in Cisco ISE nodes that are part of a distributed deployment depend on the personas that are enabled on them. You must perform all administration and monitoring activities through the primary Administration node. For some tasks, you must use the secondary nodes. Therefore, the user interface of the secondary nodes provides limited menu options based on the personas that are enabled on them.

If a node assumes more than one persona, for example, the Policy Service persona, and a Monitoring persona with an Active role, then the menu options listed for Policy Service nodes and Active Monitoring node will be available on that node.

The following table lists the menu options that are available on Cisco ISE nodes that assume different personas.

Table 3-1 Cisco ISE Nodes and Available Menu Options

Cisco ISE Node	Available Menu Options
All nodes	• View and configure system time and NTP server settings. • Install server certificate, manage certificate signing request. **Note** The server certificate operations must be performed directly on each individual node. The private keys are not stored in the local database and are not copied from the relevant node; the private keys are stored in the local file system.
Primary Administration node	All menus and submenus.
Active Monitoring node	• Home and operations menus. • Provides redundant access to monitoring data that can be accessed from both the Primary and the Active Monitoring nodes.

Table 3-1 Cisco ISE Nodes and Available Menu Options (continued)

Cisco ISE Node	Available Menu Options
Policy Service nodes	Option to join, leave, and test Active Directory connection. Each Policy Service node must be separately joined to the Active Directory domain. You must first define the domain information and join the primary Administration node to the Active Directory domain. Then, join the other Policy Service nodes to the Active Directory domain individually.
Secondary Administration node	Option to promote the secondary Administration node to become the primary Administration node. **Note** After you have registered your secondary nodes to your primary Administration node, while logging in to the Admin portal of any of the secondary nodes, you must use the login credentials of the primary Administration node.

Configuring a Cisco ISE Node

After you install a Cisco ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas run on it. This node will be in a standalone state. You must log in to the Admin portal of the Cisco ISE node to configure it. You cannot edit the personas or services of a standalone Cisco ISE node. You can, however, edit the personas and services of the primary and secondary Cisco ISE nodes. You must first configure a primary ISE node and then register secondary ISE nodes to the primary ISE node.

If you are logging in to the node for the first time, you must change the default administrator password and install a valid license.

If you are logging in to the secondary Administration node to promote it as your primary Administration node, see "Promoting Secondary Administration Node To Primary" section on page 3-17.

It is recommended not to change the host name and the domain name on Cisco ISE that have been configured or in production. If it is required, then reimage the appliance, make changes, and configure the details during the initial deployment.

Before You Begin

You should have a basic understanding of how distributed deployments are set up in Cisco ISE. Read the Guidelines for Setting Up a Distributed Deployment, page 3-9.

Step 1 Choose **Administration > System > Deployment**.

Step 2 Check the check box next to the Cisco ISE node that you want to configure, and click **Edit**.

The Node Edit page appears with a list of fields as described in Deployment Settings.

What To Do Next

1. Configuring a Primary Administration Node, page 3-12
2. Registering a Secondary Cisco ISE Node, page 3-12

Related Topics

- Cisco ISE Distributed Deployment, page 3-7
- Guidelines for Setting Up a Distributed Deployment, page 3-9
- Configuring Monitoring Nodes for Automatic Failover, page 3-18
- Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7

Configuring a Primary Administration Node

To set up a distributed deployment, you must first configure a Cisco ISE node as your primary Administration node.

Step 1 Choose **Administration > System > Deployment**.

The Register button will be disabled initially. To enable this button, you must configure a primary Administration node.

Step 2 Check the check box next to the current node, and click **Edit**.

Step 3 Click **Make Primary** to configure your primary Administration node.

Step 4 Enter data on the General Settings tab as described in Deployment Settings.

Step 5 Click **Save** to save the node configuration.

What To Do Next

1. To enable the Profiler service and configure the probes, see Configuring Probes per Cisco ISE Node, page 21-13.
2. To add secondary nodes to your deployment, you must successfully register a secondary node as described in the Registering a Secondary Cisco ISE Node, page 3-12.

Related Topics

Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7

Registering a Secondary Cisco ISE Node

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

If you plan to deploy two Administration nodes for high availability, register the secondary Administration node before you register the other secondary nodes. If you register the nodes in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration node as your primary.

If you plan to deploy multiple Policy Service nodes running Session services with mutual failover among these nodes, place the Policy Service nodes in a node group. You must create the node group before you register the nodes. See Creating a Policy Service Node Group, page 3-16 for more information.

After you register the secondary node, the configuration of the secondary node is added to the database of the primary node and the application server on the secondary node is restarted. After the restart is complete, the secondary node will be running the personas and services that you have enabled on it.

You can view all the configuration changes that you make from the Deployment page of the primary Administration node. However, expect a delay of 5 minutes for your changes to take effect and appear on the Deployment page.

Before You Begin

Ensure that the primary node's Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register.

The certificates that you import into the CTL of the primary Administration node are replicated to the secondary nodes.

Also, after you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

Step 1 Log in to the primary Administration node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Choose **Register > Register an Cisco ISE Node** to register a secondary Cisco ISE node.

Step 4 Enter the DNS-resolvable hostname of the secondary Cisco ISE node.

Note If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com,* must be DNS-resolvable from the primary Administration node. Otherwise, node registration fails. You must have previously defined the IP address and the FQDN of the secondary node in the DNS server.

Step 5 Enter a UI-based administrator credential for the standalone node in the Username and Password fields.

Step 6 Click **Next**.

Cisco ISE contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it.

If you have chosen to register a secondary Cisco ISE node, you can edit the configuration of the secondary node.

If you have chosen to register a secondary Inline Posture node, no additional configuration needs to be performed at this point.

Step 7 Click **Save**.

Result

After a secondary node is registered successfully, you will receive an alarm on your primary Administration node that confirms a successful node registration. If the secondary node fails to register with the primary Administration node, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization,

you must enter the credentials of the primary administrative node to log in to the user interface of the secondary node and perform any of the operations listed in Menu Options Available on Primary and Secondary Nodes.

Note In addition to the existing Primary node in the deployment, when you successfully register a new node, no alarm corresponding to the newly registered node is displayed. The Configuration Changed alarms reflect information corresponding to the newly registered nodes. You can use this information to ascertain the successful registration of the new node.

What To Do Next

- For time-sensitive tasks such as time profiles, guest user access and authorization, logging, and so on, ensure that the system time on your nodes are synchronized. See the "Specifying System Time and NTP Server Settings" section on page 5-3 for information on how to synchronize the system time.
- To configure for high availability, you must complete the tasks described in the following sections:
  - Promoting Secondary Administration Node To Primary, page 3-17
  - Configuring Monitoring Nodes for Automatic Failover, page 3-18
- To add an Inline Posture node to your deployment, follow the instructions as described in the "Setting Up Inline Posture" section on page 4-1.

Related Topics

- Deployment Settings, page A-1
- Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29

Registering an Inline Posture Node

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

Before You Begin

- Ensure that the primary node's Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register.
- After you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

Step 1 Log in to the primary Administration node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Click **Deployment** from the navigation pane on the left.

Step 4 Choose **Register > Register an Inline Posture Node** to register a secondary Inline Posture node.

Related Topics

- Deployment Settings, page A-1
- Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29
- Chapter 4, "Setting Up Inline Posture."

Viewing Nodes in a Deployment

In the Deployment Nodes page, you can view all the Cisco ISE nodes, primary and secondary, that are part of your deployment.

Step 1 Log in to the primary Cisco ISE Admin portal.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Click **Deployment** from the navigation pane on the left.

Step 4 Refer to Deployment Settings for a description of the fields in the Deployment Nodes page.

From this page, you can do the following:

- Edit a node. This option is enabled only when you choose a single node. After you choose a node, click the Edit button to edit the personas and roles of that node.
- Register a secondary node. This option is enabled only after you configure a primary Administration node. Click the Register button to register a Cisco ISE or Inline Posture node.
- Initiate a full database replication from the primary to the selected secondary nodes.
- Deregister one or more secondary nodes.

Synchronizing Primary and Secondary Cisco ISE Nodes

You can make configuration changes to Cisco ISE only through the primary Administration node. The configuration changes get replicated to all the secondary Cisco ISE Nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the secondary Administration nodes with the primary Administration node.

Before You Begin

You must click the Syncup button to force a full replication if the Sync Status is set to Out of Sync or if the Replication Status is Failed or Disabled.

Step 1 Log in to the primary Cisco ISE Admin portal.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Check the check box next to the node that you want to synchronize with the primary Administration node, and click **Syncup** to force a full database replication.

Creating a Policy Service Node Group

You can deploy more than one Policy Service node for load balancing to distribute requests evenly. To detect node failure and to reset sessions in a pending state on the failed node, two or more Policy Service nodes can be placed in the same node group. You must create a node group before you can add a node to it.

You can create, edit, and delete Policy Service node groups from the Deployment pages of the Cisco ISE Admin portal.

Before You Begin:

- Ensure that all the nodes that are going to be part of a node group are Layer 2 adjacent, which means they are on the same subnet, or connected over a routed LAN network that supports IP multicast.
- Enable IP multicast between nodes that are part of the same node group. Typically, all the nodes in a node group will be connected to the same switch and be in the same VLAN. Multicast over Layer 3 connections is also supported, but requires proper IP multicast configuration on all switches that connect members of the same node group. For simplicity and increased availability, we recommend that all nodes in a node group be Layer 2 adjacent.
- Ensure that node group members can communicate over UDP/45588, UDP/45590, and TCP/7802.
- Ensure that node groups do not have the same multicast address.
- Ensure that the multicast address that you assign to a node group is not reserved for use by other network protocols in the deployment. Cisco ISE checks if the multicast address that you enter is a valid and allowed multicast address. It does not allow 224.0.0.0 to be used as a multicast address, but does not check through the reserved list of multicast addresses. For a list of reserved multicast addresses that you should not use, see http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml.

Step 1 Choose **Administration > System > Deployment**.

Step 2 Click the **action** icon, and then click **Create Node Group**.

Step 3 Enter a unique name for your node group.

Step 4 (Optional) Enter a description for your node group.

Step 5 Enter a unique multicast address, which is used to communicate between nodes in a group to monitor the health of the nodes and for session cleanup. The multicast address must be between 224.0.0.1 and 239.255.255.255.

Step 6 Click **Submit** to save the node group.

Result

After you save the node group, it should appear in the navigation pane on the left. If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

What To Do Next

- To add a node to a node group, you must edit the node by choosing the node group from the Member of Node Group drop-down list.
- To remove a node from a node group, you must edit the node by choosing <none> from the Member of Node Group drop-down list.

Related Topics

- Deployment Settings, page A-1
- Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7

Changing Node Personas and Services

You can edit the Cisco ISE node configuration to change the personas and services that run on the node.

Before You Begin

When you enable or disable any of the services that run on a Policy Service node or make any changes to a Policy Service node, you will be restarting the application server processes on which these services run. Expect a delay while these services restart.

Step 1 Log in to the primary Administration node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Check the check box next to the node whose personas or services you want to change, and then click **Edit**.

Step 4 Choose the personas and services that you want.

Step 5 Click **Save**.

Step 6 Verify receipt of an alarm on your primary Administration node to confirm the persona or service change. If the persona or service change is not saved successfully, an alarm is not generated.

Related Topics

- Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7
- Lost Monitoring and Troubleshooting Data After Registering Policy Service Node to Administration Node, page G-13

Promoting Secondary Administration Node To Primary

If the primary Administration node fails, you must manually promote the secondary Administration node to become the new primary node.

If the node that was originally the primary Administration node comes back up, it will become a secondary Administration node. In the Edit Node page of a secondary node, you cannot modify the personas or services because the options are disabled. You have to log in to the Admin portal to make changes.

Before You Begin

Ensure that you have a second Cisco ISE node configured with the Administration persona to promote as your primary Administration node.

Step 1 Log in to the user interface of the secondary Administration node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 In the Edit Node page, click **Promote to Primary**.

Note You can only promote a secondary Administration node to become a primary Administration node. Cisco ISE nodes that assume only the Policy Service or Monitoring persona, or both, cannot be promoted to a primary Administration node.

Step 4 Click **Save**.

Step 5 Restart the secondary Cisco ISE nodes that were registered with the original primary Administration node before you registered the secondary Administration node.

For example, if you registered a secondary Administration node (the new primary) after you registered secondary Cisco ISE Policy Service and Monitoring nodes, then you must restart the secondary Cisco ISE nodes that were registered before the secondary Administration node was registered.

What To Do Next

After you promote your secondary Administration node to become the primary Administration node, you must reconfigure your scheduled Cisco ISE backups in the newly promoted primary Administration node because scheduled backups are not replicated from the primary to secondary Administration node. See Scheduling a Backup, page 12-5 for more information.

Configuring Monitoring Nodes for Automatic Failover

If you have two Monitoring nodes in a deployment, you can configure a primary-secondary pair for automatic failover to avoid downtime in the Cisco ISE Monitoring service. A primary-secondary pair ensures that a secondary Monitoring node automatically provides monitoring should the primary node fail.

Before You Begin

- Before you can configure Monitoring nodes for automatic failover, they must be registered as Cisco ISE nodes. This procedure is described in Guidelines for Setting Up a Distributed Deployment, page 3-9 and Configuring a Cisco ISE Node, page 3-11.
- You must specify monitoring roles and services on both nodes and name them for their primary and secondary roles, as appropriate.
- You must configure repositories for backup and data purging on both the primary and secondary Monitoring nodes, using the same repositories for each. This is important for the backup and purging features to work properly. Purging takes place on both the primary and secondary nodes of a redundant pair. For example, if the primary Monitoring node uses two repositories for backup and purging, you must specify the same repositories for the secondary node.

  You can configure a data repository for a Monitoring node using the **repository** command in the system CLI. For more information, see Back Up and Restore of the Monitoring Database, page 25-29 and the *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*.

Caution For scheduled backup and purge to work properly on the nodes of a Monitoring redundant pair, you must configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.

Before You Begin

From the Cisco ISE dashboard, verify that the Monitoring nodes are ready. The System Summary dashlet shows the Monitoring nodes with a green check mark to the left when their services are ready.

Step 1 Choose **Administration > System > Deployment**.

Step 2 In the Deployment Nodes page, check the check box next to the Monitoring node that you want to specify as active, and click **Edit**.

Step 3 Click the **General Settings** tab and choose **Primary** from the **Role** drop-down list.

When you choose a Monitoring node as primary, the other Monitoring node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.

Step 4 Click **Save**. The active and standby nodes restart.

Removing a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE node. It retains the last configuration that it received from the primary Administration node and assumes the default personas of a standalone node that are Administration, Policy Service, and Monitoring. If you deregister a Monitoring node, this node will no longer be a syslog target.

You can view these changes from the Deployment page of the primary Administration node. However, expect a delay of 5 minutes for the changes to take effect and appear on the Deployment page.

Before You Begin

Before you remove any secondary node from a deployment, perform a backup of Cisco ISE configuration, which you can then restore later on, if needed.

Step 1 Choose **Administration > System > Deployment**.

Step 2 Check the check box next to the secondary node that you want to remove, and then click **Deregister**.

Step 3 Click **OK**.

Step 4 Verify receipt of an alarm on your primary Administration node to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the primary Administration node, the alarm is not generated.

Related Topics

Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7

Changing the Hostname or IP Address of a Standalone Cisco ISE Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE nodes.

Before You Begin

If the Cisco ISE node is part of a distributed deployment, you must remove it from the deployment and ensure that it is a standalone node.

Step 1 Change the hostname or IP address of the Cisco ISE node using the **hostname**, **ip address,** or **ip domain-name** command from the Cisco ISE CLI.

Step 2 Reset the Cisco ISE application configuration using the **application stop ise** command from the Cisco ISE CLI to restart all the services.

Step 3 Register the Cisco ISE node to the primary Administration node if it part of a distributed deployment.

Note If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com* must be DNS-resolvable from the primary Administration node. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE nodes that are part of your distributed deployment in the DNS server.

After you register the Cisco ISE node as a secondary node, the primary Administration node replicates the change in the IP address, hostname, or domain name to the other Cisco ISE nodes in your deployment.

Related Topics

- *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*
- Removing a Node from Deployment, page 3-19
- Registering a Secondary Cisco ISE Node, page 3-12

Replacing the Cisco ISE Appliance Hardware

You should replace the Cisco ISE appliance hardware only if there is an issue with the hardware. For any software issues, you can reimage the appliance and reinstall the Cisco ISE software.

Step 1 Re-image or re-install the Cisco ISE software on the new nodes. Follow the steps 2 - 4, as described in Recovery of Lost Nodes in Standalone and Distributed Deployments, page 12-14.

Step 2 Register the new node as a secondary server with the primary Administration node.

Related Topics

- Removing a Node from Deployment, page 3-19
- Registering a Secondary Cisco ISE Node, page 3-12
- Configuring a Cisco ISE Node, page 3-11