Using Cisco ICFPP ShellAdmin Commands

- Accessing the ShellAdmin Console, page 1
- General Administration, page 1
- Configuring Clusters, page 9
- Working with Databases, page 27
- Accessing Root Privileges, page 30

Accessing the ShellAdmin Console

The ShellAdmin console provides many options for managing and configuring Cisco ICFPP. You can access the ShellAdmin console by using SSH as described in this procedure.

Procedure

Step 1 Using SSH, connect to the ShellAdmin console by using the following information:

- IP address of the Cisco ICFPP virtual appliance.
- The username shelladmin.
- The password that you set when you installed Cisco ICFPP.

The ShellAdmin menu is displayed with the options available for the type of node: Standalone, Primary, or Service.

Step 2 Enter the number of the option you want, and press **Enter**.
If additional information is required for the option that you choose, you are prompted for it.

General Administration

The ShellAdmin console enables you to execute common administration tasks such as changing your password, stopping and starting services, generating log and report data, and performing other system-related tasks.

Viewing Version Information

You can view the Cisco ICFPP product version by choosing the **Show Version** option. The product version number uses the format *version-build-patch* where:

- *version* is the product release, such as 2.3.1.
- *build* is the build number, such as 206.
- *patch* is the patch applied to the build, such as p208.

This information is required for debugging purposes.

Procedure

Step 1 In the ShellAdmin console, choose **Show Version**.
Information similar to the following is displayed:

```
Cisco UCS Director Platform
---------------------------
Product Name     : Intercloud Fabric Provider Platform
Product Version  : 2.3.1-206-p208
Platform Version : 5.3.0.0
Build Number     : 74

Press return to continue ...
```

Step 2 Press **Enter** to return to the menu.

Starting Cisco Services

You can start all Cisco ICFPP services by choosing the **Start Services** option.

Note Services started in the background are not displayed.

Procedure

Step 1 In the ShellAdmin console, choose the **Start Services** option.
The following information is displayed:

```
Press return to continue ...nohup: appending output to `nohup.out'
```

Step 2 Press **Enter** to return to the menu.

Step 3 (Optional) To verify that the services have started, choose the **Display Service Status** option.

Stopping Cisco Services

You can stop all Cisco ICFPP services by choosing the **Stop Services** option.

Procedure

Step 1 In the ShellAdmin console, choose the **Stop Services** option.
Information similar to the following is displayed:

```
Stopping broker [PID=17364]/[Child=17365]
     Stopping controller [PID=17402]/[Child=17404]
     Stopping eventmgr [PID=17471]/[Child=17473]
     Stopping client [PID=17535]/[Child=17537
17615
17678]
     Stopping idaccessmgr [PID=17613]/[Child=]
/opt/infra/stopInfraAll.sh: line 35: kill: (17613) - No such process
     Stopping inframgr [PID=17676]/[Child=]
     Tomcat is running with [PID=17779]. Stoping it and its child process
  Flashpolicyd is running with [PID=17807]. Stopping it
Stopping websock[PID=17812]
Press return to continue ...
```

Step 2 Press **Enter** to return to the menu.

Step 3 (Optional) To confirm that the services have stopped, choose the **Display Service Status** option.

Displaying Service Status

The **Display Services Status** option enables you to view the following services and their status:

- Broker
- Controller
- Eventmgr
- Client
- Idaccessmgr
- Inframgr
- Tomcat
- Websock (VNC interface)
- Database (mysqld)

Procedure

Step 1 In the ShellAdmin console, choose the **Display Service Status** option.
Information similar to the following is displayed with the service name, status, and process ID (PID):

```
Service                  Status        PID
----------            ----------      -----
broker                   RUNNING      27533
controller               RUNNING      27558
eventmgr                 RUNNING      27592
client                   RUNNING      27637
idaccessmgr              RUNNING      27681
inframgr                 RUNNING      27726
TOMCAT                   RUNNING      27783
websock                  RUNNING      27812

4204 ?        00:00:00 mysqld_safe
4625 ?        00:14:45 mysqld
```

Step 2 Confirm that all services are running. If a service is not running, restart the service by choosing **Start Services** in the ShellAdmin console.

Changing Your Password

You can change the password for the Cisco ICFPP shelladmin account by choosing the **Change ShellAdmin Password** option.

Procedure

Step 1 In the ShellAdmin console, choose the **Change ShellAdmin Password** option.
Information similar to the following is displayed:

```
Changing password for user shelladmin.
New UNIX password:
```

Step 2 Enter and confirm the new shelladmin account password.
Information similar to the following is displayed:

```
passwd: all authentication tokens updated successfully. Press return to continue...
```

Step 3 Press **Enter** to return to the menu.

Synchronizing the System Time

You can synchronize the system time to the hardware time and a network time protocol (NTP) server by choosing the **Time Sync** option.

Procedure

Step 1 In the ShellAdmin console, choose the **Time Sync** option.
Information similar to the following is displayed:

```
System time is Tue May  7 14:19:19 UTC 2015
Hardware time is Tue 07 May 2015 02:19:20 PM UTC  -0.107647 seconds
Do you want to sync systemtime [y/n]?
```

Step 2 To synchronize the system time, enter **Y**.

Step 3 To synchronize with NTP, enter **Y** when prompted.

Step 4 If you choose to synchronize with NTP, enter the NTP server IP address when prompted.

Step 5 Press **Enter** to return to the ShellAdmin menu.

Importing a CA Certificate JKS File

You can import a Certificate Authority (CA) signed certificate file by choosing the **Import a CA Certificate (JKS) file** option.

Procedure

Step 1 In the ShellAdmin console, choose the **Import a CA Certificate (JKS) file** option.
Information similar to the following is displayed:

```
Import CA signed certificate from URL.
   E.g. URL --> http://host:port/cert.jks

   URL:
```

Step 2 Enter the URL for the CA signed certificate file and press **Enter**.

Pinging a Host by Hostname or IP Address

You can use the ShellAdmin console to test network connectivity by pinging a host by hostname or IP address.

Procedure

Step 1 In the ShellAdmin console, choose the **Ping Hostname/IP address** option.

Step 2 When asked if you want to use the **ping** or **ping6** command, enter **V4**.

Step 3 When prompted, enter the hostname or IP address of the host you want to ping.
Information similar to the following is displayed:

```
Do you want to run ping/ping6 [v4/v6] ? : v4
 Enter IP Address : 209.165.200.224
```

```
PING 209.165.200.224 (209.165.200.224) 56(84) bytes of data.
64 bytes from 209.165.200.224: icmp_seq=1 ttl=64 time=9.90 ms
64 bytes from 209.165.200.224: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 209.165.200.224: icmp_seq=3 ttl=64 time=0.254 ms
64 bytes from 209.165.200.224: icmp_seq=4 ttl=64 time=0.198 ms
64 bytes from 209.165.200.224: icmp_seq=5 ttl=64 time=0.267 ms

--- 209.165.200.224 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.198/2.187/9.901/3.857 ms
Press return to continue ...
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Configuring a Network Interface

You can configure a network interface for a Cisco ICFPP virtual appliance by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose the **Configure a Network Interface** option.
Information similar to the following is displayed:

```
Do you want to Configure DHCP/STATIC IP  [D/S] ? :
```

Step 2 Choose one of the following configuration selections:

- To configure a DHCP IP address, enter **D**.
- To configure a static IP address, enter **S**.

If you choose to configure a static IP address, information similar to the following is displayed:

```
Configuring STATIC configuration..
Enter the ethernet interface that you want configure E.g. eth0 or eth1:
```

Step 3 When prompted, enter the Ethernet interface to configure, such as eth1.
Information similar to the following is displayed:

```
Configuring STATIC IP for eth1...
   IP Address: 209.165.200.224
   Netmask: 255.255.255.0
   Gateway: 209.187.108.1
   DNS Server1: 198.51.100.1
   DNS Server2: 203.0.113.1
Configuring Network with : INTERACE(eth1), IP(209.165.200.224), Netmask(255.255.255.0),
Gateway(209.187.108.1),
DNS Server1(198.51.100.1), DNS Serverx 2(203.0.113.1)

Do you want to continue  [y/n]? :
```

Step 4 Enter **Y** to complete the configuration.

Viewing Appliance Network Details

You can view the details of a Cisco ICFPP virtual appliance network by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose the **Display Network Details** option.
Information similar to the following is displayed:

```
Network details....
eth0      Link encap:Ethernet  HWaddr 00:50:56:97:1E:2D
          inet addr:192.0.2.23  Bcast:192.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::230:56gg:fe97:1e2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189818223 errors:14832 dropped:17343 overruns:0 frame:0
          TX packets:71520969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105749301003 (98.4 GiB)  TX bytes:27590555706 (25.6 GiB)
          Interrupt:59 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1821636581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1821636581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:327846827946 (305.3 GiB)  TX bytes:327846827946 (305.3 GiB)

Press return to continue ...
```

Step 2 Press **Enter** to return to the ShellAdmin menu.

Viewing Tail Inframgr Logs

The ShellAdmin console enables you to see Infrastructure Manager (inframgr) log data, which is generated by using the UNIX **tail** command. This log data is useful for tracing information when you are debugging problems. Choose the **Tail Inframgr Logs** option to immediately tail the most recent inframgr logs and view the results.

Procedure

Step 1 In the ShellAdmin console, choose the **Tail Inframgr Logs** option.
Information similar to the following is displayed:

```
2015-05-20 23:17:43,500 [pool-23-thread-17]
INFO  getBestAgent(SystemTaskExecutor.java:308)
```

```
- No Agent available for remoting SnapMirrorHistoryStatusSchedulerTask
2015-05-20 23:17:43,502 [pool-23-thread-17]
INFO  updateStatus(SystemTaskStatusProvider.java:181)
- Task: task.SnapMirrorHistoryStatusSchedulerTask changed state to OK
2015-05-20 23:17:43,562 [pool-23-thread-17]
INFO  executeLocally(SystemTaskExecutor.java:133)
- Executing task locally: SnapMirrorHistoryStatusSchedulerTask
2015-05-20 23:17:43,562 [pool-23-thread-17]
INFO  getClusterLeaf(ClusterPersistenceUtil.java:81)
- Leaf name LocalHost
2015-05-20 23:17:43,571 [pool-23-thread-17]
```

Step 2 To exit from the log file display, press **Ctrl-C** and then **Enter**.

Applying a Patch to Cisco ICFPP

You can use the ShellAdmin console to apply Cisco ICFPP patches that include infrastructure changes. For more information or to obtain a patch file, contact your Cisco representative.

Before You Begin

- Download the patch file from Cisco. If you need assistance, contact your Cisco representative.
- Place the patch file on a web server or FTP server that is accessible from Cisco ICFPP.
- Review the patch release notes and README file.
- Take a snapshot of the Cisco ICFPP virtual appliance.
- Back up the Cisco ICFPP virtual appliance database. Although the **Apply Patch** option enables you to back up the database as part of the procedure, we recommend that you create a backup immediately before choosing the **Apply Patch** option.

Procedure

Step 1 In the ShellAdmin console, choose **Stop Services**.

Step 2 After the services have stopped, choose the **Apply Patch** option.
Information similar to the following is displayed:

```
Applying Patch...
Do you want to take database backup before applying patch (y/n)?
```

Step 3 Do one of the following:

- If you did not back up the appliance database before starting this procedure, enter **Y**, and then enter the IP address and credentials for the FTP server where the database is to be backed up.
  Information similar to the following is displayed:

```
y
Backup will upload file to an FTP server.
Provide the necessary access credentials.
   FTP Server IP Address: nnn.nnn.nnn.nnn
   FTP Server Login:
```

- If you backed up the appliance database before starting this procedure, enter **N** and then enter the URL or location of the patch.
  Information similar to the following is displayed:

```
n
Applying Patch:
Patch URL: http://nnn.nnn.nnn.nnn/icfpp-patch.zip

Applying the Patch http://nnn.nnn.nnn.nnn/icfpp-patch.zip [y/n]? y
```

Step 4 When prompted, enter **Y** to confirm that you want to apply the patch.

Step 5 After the patch has been applied, choose the **Start Services** option in the ShellAdmin console.

Configuring Clusters

The topics in this section describe how to configure Cisco ICFPP for multiple-node clusters.

Workflow for Configuring Clusters

The following workflow describes the high-level tasks that are required to configure a multiple-node cluster.

Step	Task	Related Information
1.	Install a minimum of four Cisco ICFPP virtual appliances. The role that is assigned to each appliance during installation depends on whether you are using VMware or OpenStack.	Cisco Intercloud Fabric Provider Platform Installation Guide
2.	Configure two primary nodes.	Configuring a Primary Node, on page 10
3.	Configure two or more service nodes.	Configuring a Service Node, on page 11
4.	Configure additional storage.	Configuring Additional Storage, on page 12
5.	Configure the two primary nodes for HA.	Configuring HA, on page 15
6.	(OpenStack only) Configure VIP access.	Configuring VIP Access for HA in OpenStack, on page 16
7.	Configure a load balancer for the service nodes in the cluster. **Note** The load balancer must be configured to persist sessions based on the PERSISTICFPP cookie that Cisco ICFPP issues.	Your load balancer documentation

Configuring a Primary Node

To configure a Cisco ICFPP virtual appliance that has been installed using the Standalone Mode role for a multiple-node cluster, you must first configure it as a primary node or service node by using the ShellAdmin console. This procedure describes how to configure a standalone node as a primary node. To configure a standalone node as a service node, see Configuring a Service Node, on page 11.

Before You Begin

Install a Cisco ICFPP virtual appliance using the Standalone Mode role.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the standalone node that you want to configure as a primary node.

Step 2 At the ShellAdmin prompt, choose the **Change Node Role** option.

Step 3 When prompted, enter **Y** to change the node role.

Step 4 Enter **A** to configure the node as a primary node.

Step 5 Enter **Y** to confirm that you want to configure the node as a primary node.
Information similar to the following is displayed:

```
user selected 'y'
 Checking DB Status
   2399 ?       00:00:00 mysqld_safe
   2820 ?       00:04:21 mysqld
Configuring as Primary Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as Primary node...
Enabling Remote Database access to ICFPP Service nodes
Checking the MySQL to be ready before enabling remote access to DB...
Waiting a maximum of 900 seconds for MySQL to be up on localhost

Trying a maximum of 900 seconds for enabling remote access to DB
Successfully enabled remote access for database

SUCCESS: Successfully changed node role to Primary Node

Stopping Database and restarting it for changes to take effect
Stopping database...
Database stopped...
Starting services that were previously stopped.
Starting the Database...
Starting the services...
In order for changes to take effect logout and log back in
Do you want to logout [y/n]?
```

Step 6 Enter **Y** when prompted to log out.
You are logged out of the ShellAdmin console. When you log in again, the ShellAdmin menu will include options for configuring HA and viewing HA status.

Configuring a Service Node

To configure a Cisco ICFPP virtual appliance that has been installed using the Standalone Mode role for a multiple-node cluster, you must first configure it as a primary node or as a service node by using the ShellAdmin console. This procedure describes how to configure a standalone node as a service node. To configure a standalone node as a primary node, see Configuring a Primary Node, on page 10.

Before You Begin

- Install a Cisco ICFPP virtual appliance using the Standalone Mode role.
- Obtain the IP address of a primary node in the cluster or the virtual IP address (VIP) of an HA pair in the cluster.
- Back up any data in the virtual appliance database that you want to keep. When the virtual appliance is reconfigured as a service node, the existing data will be deleted.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the standalone node that you want to configure as a service node.

Step 2 At the ShellAdmin prompt, choose the **Change Node Role** option.

Step 3 When prompted, enter **Y** to change the node role.

Step 4 Enter **B** to configure the node as a service node.

Step 5 Enter **Y** to confirm that you want to configure the node as a service node.

Step 6 When asked if you want to continue, do one of the following:

- Enter **N** to stop the configuration so that you can back up the database.
- Enter **Y** to confirm that you want to continue.

If you choose to continue, Cisco ICFPP confirms your choice.

Step 7 When prompted, enter the IP address of the primary node or the VIP of the HA pair that the service node is to use.
Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.60
Disabling Database service at startup

SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for the changes to take effect, log out and log in again
Do you want to log out [y/n]?
```

Step 8 Enter **Y** to log out.
The next time that you log in, the menu will include the options available for a service node.

Configuring Additional Storage

The default disk size of 100 GB for Cisco ICFPP is not sufficient for configuring Cisco ICFPP in a multiple-node cluster. As a result, you must add additional disk space before configuring a multiple-node cluster. You can use either NFS or a Cinder volume as described in the following topics:

- Configuring NFS, on page 12
- Configuring a Cinder Volume, on page 13

Configuring NFS

If you did not configure an NFS server for a Cisco ICFPP virtual appliance when you installed it, you can configure the appliance for NFS by using the ShellAdmin console.

Note We recommend that you configure additional storage for all Cisco ICFPP nodes. If additional storage is not configured, all VM images that are uploaded from Cisco Intercloud Fabric Director are stored on the node's local disk. If the node fails, one or both of the following can occur:

- Any images stored on the node are no longer available.
- If the node is part of a cluster, template creation and VM migration fail.

If NFS is not available, you can configure a Cinder volume as described in Configuring a Cinder Volume, on page 13.

Before You Begin

- Upload all images on the Cisco ICFPP virtual appliance to the cloud. If the images are not uploaded to the cloud, they are deleted when NFS is configured.
- Identify the NFS server IP address and the directory in which the files are to be stored.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console for the Cisco ICFPP virtual appliance that you want to configure for NFS.

Step 2 Choose the **NFS Configuration** option.
Cisco ICFPP displays a menu with options for configuring, removing, and viewing an NFS configuration.

Step 3 At the prompt, enter **A**.
Cisco ICFPP determines whether or not an NFS directory is mounted and displays the results:

```
Checking for mounted NFS directory...
NFS directory is not mounted
Note: Configuring NFS will delete any images that are not uploaded to the cloud! Proceed
[y/n]?
```

Step 4 Enter **Y** to continue.

Cisco ICFPP determines whether or not an NFS IP address or NFS directory has been configured and then prompts you for input.

Step 5 When prompted, enter the NFS server IP address and the NFS directory path.
Information similar to the following is displayed while NFS is configured:

```
Configuring NFS with : NFS Server IP=123.15.1.1, remote directory=/nfs/dir local mounting
point=/mnt/icfpp-images
Creating /mnt/icfpp-images directory.
Starting portmap and nfs services...
Starting portmap:                                          [  OK  ]
mount -t nfs 123.15.1.1:/icfpp-images /mnt/icfpp-images
May wait for mount up to 12-0 seconds..., please be patient...
Successfully mounted 123.15.1.1:/icfpp-images  at /mnt/icfpp-images
Saving NFS Configuration
NFS IP address: 123.15.1.1
NFS Directory Path: /icfpp_images
Saved NFS Configuration
Setting up images directory to use NFS
Image directory setup to NFS done
Press Return to continue
```

Step 6 Press **Enter** to return to the ShellAdmin menu.
To view or remove the NFS configuration, choose the **NFS Configuration** option in the ShellAdmin menu, and then choose the appropriate option from the NFS menu.

Configuring a Cinder Volume

The default disk size of 100 GB for the Cisco ICFPP virtual appliance is not sufficient for configuring Cisco ICFPP in a multiple-node cluster. If you do not have access to an NFS server, you can increase the disk size by creating additional Cinder volumes. Cinder volumes that you create are formatted as physical disks and then combined to form a logical volume that can be mounted on the VM in a specific location.

Before You Begin

- Configure a Cisco ICFPP virtual appliance as a service node by using the ShellAdmin console. For more information, see Configuring a Service Node, on page 11.
- If you have not already done so, configure the root user password for the Cisco ICFPP service node. For more information, see Configuring Root Access, on page 31.
- Collect the following information:
  - Cloud credentials—The username and password for the project in OpenStack.
  - Cloud URL—Obtain the cloud URL as follows:
    1. In the OpenStack dashboard, choose **Project** > ***project*** > **Access & Security**, and click the **API Access** tab.
    2. In the **API Endpoints** table, locate the **Identity** service and note the service endpoint URL.
  - Cisco ICFPP instance ID—Obtain the Cisco ICFPP instance ID as follows:
    1. In the OpenStack dashboard, choose **Project** > ***project*** > **Instances**.
    2. In the list of instances, locate Cisco ICFPP and click the hyperlinked instance name.

The **Instance Detail** page is displayed.

3 In the Overview tab, locate and note the instance ID.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the Cisco ICFPP service node.

Step 2 At the ShellAdmin prompt, choose **Cinder Storage Configuration**.

Step 3 When prompted, enter **Y** and enter the root password.

Step 4 At the Cinder Storage Configuration menu prompt, choose **Deploy Fresh Storage**.
Cisco ICFPP prompts you for information so that it can configure the storage.

Step 5 Enter the following information:

- Cloud username and password
- OpenStack project name
- Cloud URL
- Cisco ICFPP instance ID
- Required storage size in GB
- Required volume size in GB

Note Cinder storage configuration supports a volume with a maximum of 2 TB for each service node.

Information similar to the following is displayed while Cisco ICFPP creates and formats the volume. You do not need to restart the Cisco ICFPP virtual appliance.

```
Cloud user name:- abc1-de2.gen
Enter password:
Project Name:- ABC-DEV1
Cloud URL: [e.g. https://us-texas-3.cloud.abc.com:5000/v2.01]:-
https://us-texas-3.cloud.abc.com:5000/v2.0
ICFPP Instance ID:- 75c8c226-b22c-4041-ab5c-7e7fd544c3b
Expected storage size[GB]:- 10
Expected volume size[GB]:- 10
Deploying fresh storage

*****Creating volumes*****

*****Attaching volumes*****

*****Formatting volumes and creating logical volumes*****

*****Validating final state*****
true
Executed successfully!
```

Step 6 If needed, you can do either of the following from the Cinder Storage Configuration menu:

- To configure additional storage, choose **Add additional storage to existing storage**.
- To delete storage, choose **Cleanup deployed storage**.

Configuring HA

After you deploy Cisco ICFPP virtual appliances, you can configure them for high availability (HA) by using the ShellAdmin console.

When configuring HA:

- Configure the active node and standby node concurrently as described in this procedure.
- The database on the standby node is deleted when the HA pair is configured.

Before You Begin

- Deploy or configure two Cisco ICFPP virtual appliances as primary nodes:
  - To deploy a Cisco ICFPP virtual appliance with the Primary Mode role, see the Cisco Intercloud Fabric Provider Platform Installation Guide.
  - To configure an existing Cisco ICFPP virtual appliance as a primary node, see Configuring a Primary Node, on page 10.
- Identify a virtual IP (VIP) address for the HA pair.
- Determine which node will be the active node and which node will be the standby node.
- On the node that will be the standby node, move any existing data that you want to save to another location.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the node that will be the active node for the HA pair.

Step 2 At the ShellAdmin prompt, choose the **Setup HA** option and press **Enter**.
A warning is displayed stating that the contents of the database on the standby node will be deleted.

Step 3 When prompted, enter **Y** to configure the node for HA.

Step 4 Enter **A** to configure the node as the active node.

Step 5 When prompted, enter **Y** to configure the node as the active node.
Cisco ICFPP detects and displays the IP address of the current node.

Step 6 Enter **Y** to confirm the node IP address.

Step 7 Enter the standby node IP address.

Step 8 Enter the VIP to use for the IP pair.
Information similar to the following is displayed:

```
---------------------------------------------
HA Configuration Information:
---------------------------------------------
This node will be configured as active node
Active Node IP address:   123.45.1.61
Standby Node IP address:  123.45.1.62
Virtual IP address:       123.45.1.60
---------------------------------------------
```

```
Proceed with setting up HA with above configuration [y/n]:
```

Step 9 Enter **Y** to confirm the configuration and proceed or **N** to change the values. If you choose to proceed, Cisco ICFPP displays progress messages while it configures the active node for HA.

Step 10 While Cisco ICFPP is configuring the active node for HA, log in to the ShellAdmin console of the node that will be the standby node for the HA pair.

Step 11 At the ShellAdmin prompt, choose the **Setup HA** option and press **Enter**.

Step 12 Enter **Y** to configure the node for HA.

Step 13 Enter **B** to configure the node as the standby node.

Step 14 When prompted, enter **Y** to configure the node as the standby node.
Cisco ICFPP detects and displays the IP address of the current node.

Step 15 Enter **Y** to confirm the node IP address.

Step 16 Enter the active node IP address.

Step 17 Enter the VIP to use for the HA pair.
Information similar to the following is displayed:

```
--------------------------------------------
HA Configuration Information:
--------------------------------------------
This node will be configured as standby node
Active Node IP address:   123.45.1.61
Standby Node IP address:  123.45.1.62
Virtual IP address:       123.45.1.60
--------------------------------------------
Proceed with setting up HA with above configuration [y/n]:
```

Step 18 Enter **Y** to confirm the configuration.
Cisco ICFPP displays progress messages while it configures the standby node for HA and synchronizes the database information on both nodes.

Step 19 When prompted, press **Enter** to return to the ShellAdmin menu.

What to Do Next

For OpenStack environments, continue with Configuring VIP Access for HA in OpenStack, on page 16.

Configuring VIP Access for HA in OpenStack

After Cisco ICFPP primary nodes are configured for HA, the virtual IP address (VIP) is used in the event of failover. However, OpenStack Neutron does not allow a host to accept packets with an IP address in the packet header that does not match the destination host IP address. As a result, packets sent to the VIP do not reach the node to which the VIP is assigned. To allow the packets to reach HA pair, the VIP must be added as an allowed address for both nodes (active and standby) in the HA pair.

This procedure describes how to configure VIP access on the nodes in the HA pair by using the OpenStack **neutron port-update** command. For more information, see the OpenStack documentation at docs.openstack.org.

Before You Begin

- Confirm that HA has been configured on two Cisco ICFPP primary nodes in an OpenStack environment.
- Confirm that you have access to the OpenStack Neutron command line tool.

Procedure

Step 1 Obtain a list of networks by entering the following command:

```
$ neutron net-list
```

Information similar to the following is displayed:

```
+--------------------------------------+--------------------+-----------------------------------------------------+
| id                                   | name               | subnets
                                     |
+--------------------------------------+--------------------+-----------------------------------------------------+
| 2d84eaa4-8b81-4dc8-9897-dd8ef4719f8b | public-direct-600  |
3e0b77fe-fc66-4913-bc58-7f62d4ab247a 10.203.28.0/23 |
|                                      |                    |
5c2f73a9-4e2f-498c-8244-6aefe5129fdd 10.203.50.0/23 |
|                                      |                    |
ba29165f-c88a-496a-9adc-99ee90407ebe 10.203.24.0/23 |
|                                      |                    |
d5b69780-aefb-42a6-8ba5-aaf405fb36a0 10.203.30.0/24 |
| b5d8d461-74d7-45a4-a1f0-f7ac96586bd5 | Net1               |
c0921b42-2896-4b32-b33e-f54db9e5a3d6 192.168.0.0/24 |
| ca80ff29-4f29-49a5-aa22-549f31b09268 | public-floating-601 |
0cfde3f1-e28b-4b87-8095-e0014b0ee573                |
|                                      |                    |
348a808d-ce64-43bc-a9d9-c20e52d2ac06                |
|                                      |                    |
3784170e-5d7f-48b4-b63d-aab4a0fef769                |
| ff95095f-89f0-4005-b709-70a75212d73c | icfpp-ha-123-network |
1099b814-05d9-4da0-93d1-06167db4891f 192.168.1.0/24 |
+--------------------------------------+--------------------+-----------------------------------------------------+
```

Step 2 Obtain a list of ports on the network on which the active and standby nodes in the HA pair are deployed by entering the following command:

```
$ neutron port-list -- --network_id=net_id
```

where *net_id* is the identifier for the required network. In this example, the network name is icfpp-ha-123-network.

```
$ neutron port-list -- --network_id=ff95095f-89f0-4005-b709-70a75212d73c
```

Information similar to the following is displayed:

```
+--------------------------------------+----+-------------+-------------------------------------------------------------+
| id                                   | name | mac_address       | fixed_ips
                                                                                                  |
+--------------------------------------+----+-------------+-------------------------------------------------------------+
| 4a439cf1-b95e-49ba-a8d6-0b03a8142dd2 |      | fa:16:3e:f6:f8:a9 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.12"} |
| 93d0a69a-7bb8-4719-9ed7-63c10accd78b |      | fa:16:3e:1f:7f:d2 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.11"} |
| 9d626a64-ee7c-410b-ae00-661dd275de79 |      | fa:16:3e:61:81:4b | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.14"} |
| cf56fd7b-2896-4e06-b520-1d2258ad6158 |      | fa:16:3e:ab:27:ca | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.13"} |
| d7457d29-44ba-46ef-b47a-4b94c9199902 |      | fa:16:3e:ad:d0:e9 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.15"} |
+--------------------------------------+----+-------------+-------------------------------------------------------------+
```

Step 3 In the output of the previous step, locate the port ID for the active node.

Step 4 Update the port so that it accepts traffic from the VIP by entering the following command:

```
$ neutron port-update active-port-id --allowed_address_pairs list=true type=dict
```

ip_address=*vip*

where:

- *active-port-id* is the port ID of the active node.
- *vip* is the virtual IP address for the HA pair.

For example, if the IP address of the active node is 192.168.1.11 and the VIP is 192.168.1.10, the command resembles the following:

```
$ neutron port-update 93d0a69a-7bb8-4719-9ed7-63c10accd78b --allowed_address_pairs list=true
 type=dict ip_address=192.168.1.10
```

Step 5 View the port details and confirm that the allowed_address_pairs field lists the VIP by entering the following command:

```
$ neutron port-show active-port-id
```

where *active-port-id* is the identifier for the port configured in the previous step.

Using the current example, the command and results resemble the following:

```
$ neutron port-show 93d0a69a-7bb8-4719-9ed7-63c10accd78b

+----------------------+--------------------------------------------------------------------------------------+
| Field                | Value
                    |
+----------------------+--------------------------------------------------------------------------------------+
| admin_state_up       | True
                    |
| allowed_address_pairs | {"ip_address": "192.168.1.10", "mac_address": "fa:16:3e:1f:7f:d2"}
                  |
| device_id            | b7b8eeb5-70ad-49ac-a3b4-6d8a144293a2
                    |
| device_owner         | compute:alln01-1-csi
                    |
| extra_dhcp_opts      |
                    |
| fixed_ips            | {"subnet_id": "1099b814-05d9-4da0-93d1-06167db4891f","ip_address":
 "192.168.1.11"}  |
| id                   | 93d0a69a-7bb8-4719-9ed7-63c10accd78b
                    |
| mac_address          | fa:16:3e:1f:7f:d2
                    |
| name                 |
                    |
| network_id           | ff95095f-89f0-4005-b709-70a75212d73c
                    |
| security_groups      | f995d22f-edb8-47c0-9aff-6339a15fb5be
                    |
| status               | ACTIVE
                    |
| tenant_id            | b1436740f8db42e39904ee9779f67eb8
                    |
+----------------------+--------------------------------------------------------------------------------------+
```

Step 6 Configure the standby node to accept VIP traffic by entering the following command:

```
$ neutron port-update standby-port-id --allowed_address_pairs list=true type=dict
ip_address=vip
```

where:

- *standby-port-id* is the port ID of the standby node.
- *vip* is the virtual IP address for the HA pair.

Step 7 View the port details for the standby node and confirm that the allowed_address_pairs field lists the VIP:

```
$ neutron port-show standby-port-id
```

Step 8 (Optional) Complete the following steps to configure the VIP so that it is accessible from an external network and so that the VIP uses a floating IP address:

a) Configure a port corresponding to the VIP by entering the following command:

```
$ neutron port-create --fixed-ip ip_address=ip --security-group security-group network-name
```

where:

- *ip* is the fixed IP address for the port.
- *security-group* is the name of the security group to use for this port.
- *network-name* is the name of the network to which the port belongs.

Using the current example, the command and results resemble the following:

```
$ neutron port-create --fixed-ip ip_address=192.168.1.10 --security-group default
icfpp-ha-123-network

Created a new port:
+----------------------+-------------------------------------------------------------------------------------+
| Field                 | Value
                       |
+----------------------+-------------------------------------------------------------------------------------+
| admin_state_up        | True
                       |
| allowed_address_pairs |                |
| device_id             |
                       |
| device_owner          |                                     |
| fixed_ips             | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f","ip_address": "192.168.1.10"}  |
| id                    | ea35e2a9-1b45-4b05-b345-f4758e490052
         |
| mac_address           | fa:16:3e:df:e9:69                                       |
| name                  |                 |
| network_id            | ff95095f-89f0-4005-b709-70a75212d73c            |
| security_groups       | f995d22f-edb8-47c0-9aff-6339a15fb5be
             |
| status                | DOWN                 |
```

```
| tenant_id             | b1436740f8db42e39904ee9779f67eb8
         |
+---------------------+-----------------------------------------------------------------------------------+
```

b) In the OpenStack Horizon GUI, associate a floating IP address with the port to which the fixed IP address is assigned.

Monitoring HA Status

After configuring Cisco ICFPP for HA, you can view the configuration details, check the status of the active and standby nodes, and view detailed replication status.

Procedure

Step 1 Log in to the ShellAdmin console for one of the nodes in the HA pair.

Step 2 At the menu prompt, choose **Display HA Status**.
Information similar to the following is displayed:

```
Configured HA role for this node is:  Active
Current HA role for this node is: Active
HA Configuration properties for this node are:
ACTIVE_IP_ADDRESS=123.16.1.30
STANDBY_IP_ADDRESS=123.16.1.3
VIRTUAL_IP_ADDRESS=123.16.1.25

IP address of this node is: 123.16.1.30
Checking if Virtual IP Address is reachable...OK
Virtual IP Address service status on this node...OK
Checking DB replication from 123.16.1.30 to 123.16.1.3...OK
Checking DB replication from 123.16.1.3 to 123.16.1.30...OK

Do you want to view detailed replication status ? [y/n]
```

Step 3 To view detailed information, enter **Y** and press **Enter**.
Information similar to the following is displayed:

```
                Slave_IO_State : Waiting for master to send event
                   Master_Host : 123.16.1.3
                   Master_User : replicator
                   Master_Port : 3306
                 Connect_Retry : 60
               Master_Log_File : mysql-bin.000002
           Read_Master_Log_Pos : 645644
                Relay_Log_File : mysqld-relay-bin.000004
                 Relay_Log_Pos : 361
         Relay_Master_Log_File : mysql-bin.000002
              Slave_IO_Running : Yes
             Slave_SQL_Running : Yes
               Replicate_Do_DB :
           Replicate_Ignore_DB :
…
```

Step 4 Use your arrow keys to scroll through the information, and enter **Q** to return to the menu.

Moving from a Standalone Setup to a Cluster

Cisco ICFPP enables you to move from a standalone configuration to a cluster. Moving from a standalone configuration to a cluster involves moving the database contents from the existing standalone node to the active HA node in the cluster as described in this procedure.

After moving the database contents, you can configure and test the cluster setup without modifying or affecting the standalone setup. For more information about configuring a multiple-node cluster, see Deployment Workflows.

Before You Begin

- Obtain the FTP server IP address and login credentials for backing up and restoring the database.
- Confirm that the standalone node and both nodes in the HA pair are running the same version of Cisco ICFPP.

Procedure

Step 1 In the ShellAdmin console for the standalone node, back up the existing database as follows:

a) Choose **Stop Services** to stop the Infrastructure Manager services.
b) Choose **Backup Database**.
c) Choose **Start Services**.

Step 2 Deploy or configure two primary nodes by using any of the following methods:

- For VMware environments, deploy two new Cisco ICFPP virtual appliances using the Primary Node role. For more information, see the *Cisco Intercloud Fabric Provider Platform Installation Guide*.
- For OpenStack environments, deploy two new Cisco ICFPP virtual appliances using the Standalone Node role and then configure the appliances as primary nodes. For more information, see the *Cisco Intercloud Fabric Provider Platform Installation Guide*.
- Configure existing Cisco ICFPP virtual appliances using the Standalone Node role as primary nodes. For more information, see Configuring a Primary Node, on page 10.

Step 3 Restore the backed-up database from Step 1 onto one of the primary nodes:

a) In the primary node ShellAdmin console, choose **Stop Services** to stop the Infrastructure Manager services.
b) Choose **Restore Database**.
c) Choose **Start Services**.

Step 4 In the ShellAdmin console, configure the two primary nodes as an HA pair.

Note You must configure the primary node on which the database was restored as the active node in the HA pair. If you configure it as the standby node, the database on that node is deleted.

For more information, see Configuring HA, on page 15.

Step 5 Configure service nodes for the cluster. For more information, see Configuring a Service Node, on page 11.

Restoring a Database onto an Existing HA Pair

Cisco ICFPP enables you to configure an HA pair and then restore a database from an existing standalone node to the HA pair.

Note You must stop and start services in the sequence described in this procedure to successfully restore the database on the HA pair.

Before You Begin

- Confirm that the standalone node and both nodes in the HA pair are running the same version of Cisco ICFPP.
- Back up the required database from a standalone node onto an FTP server.
- Identify the active node in the HA pair on which to restore the backed-up database.

Procedure

Step 1 Stop the VIP service on the current standby node in the HA pair as follows:

a) Log in to the ShellAdmin console for the current standby node.
b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 2 Stop the VIP service on the current active node in the HA pair as follows:

a) Log in to the ShellAdmin console for the current active node.
b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Stopping the VIP service on the active node in an HA pair automatically stops the Infrastructure Manager services if they are running.

Step 3 On the active node in the HA pair, restore the database backup obtained from the standalone node as follows:

a) In the ShellAdmin console for the active node, choose **Restore Database**.
b) When prompted, enter the FTP server IP address and login credentials.
c) Enter the path and filename for the backed up database file on the FTP server.
d) Follow the onscreen prompts to complete the process.

Step 4 Restart the VIP service on the active node as follows:

a) In the ShellAdmin console for the active node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **D** to start the VIP service.

d) Press **Enter** to return to the ShellAdmin menu.

Starting the VIP service on the active node in an HA pair automatically starts the Infrastructure Manager services on that node.

Step 5 Restart the VIP service on the standby node in the HA pair as follows:

a) In the ShellAdmin console for the standby node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **D** to start the VIP service.
d) Press **Enter** to return to the ShellAdmin menu.

Reconfiguring a Virtual IP Address

If you change a virtual IP address (VIP) for an HA pair or on a primary node that supports a service node, you must reconfigure VIP as follows:

- On both nodes in the HA configuration
- On any service nodes that communicate with the HA pair
- On any service node that has been configured to communicate with the primary node

Reconfiguring a VIP involves the following high-level tasks:

1. Stop the VIP service on the standby node in the HA pair.

   If you reconfigure the VIP on the active node in an HA pair without first stopping the VIP service on the standby node, HA will automatically fail over to the standby node.
2. Reconfigure the VIP service on the active node in the HA pair.
3. Reconfigure the VIP service on the standby node in the HA pair.
4. Reconfigure the VIP address on service nodes that used the old VIP to communicate with either the HA pair or the primary node.

The following procedure describes how to perform these tasks.

Procedure

Step 1 Stop the VIP service on the standby node as follows:

a) Log in to the ShellAdmin console for the standby node.
b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 2 Reconfigure VIP service on the active node in the HA pair as follows:

a) Log in to the ShellAdmin console for the active node.

b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) To reconfigure VIP service, enter **A**.
e) When prompted, enter **Y** to reconfigure the VIP.
f) When prompted, enter the new VIP and confirm the entry.

Information similar to the following is displayed:

```
Proceed with setting up VIP as 123.45.1.25 ? [y/n]: y
*****************************************************
Updating Virtual IP Address
*****************************************************
Updating Keepalived configuration for Virtual IP...
Setting up new keepalived configuration for active node...
Setting up IP addresses in keepalived configuration for active node...
Stopping Virtual IP service, Keepalived...
Starting Keepalived...

Successfully reconfigured Virtual IP
```

Step 3 Reconfigure the VIP service on the standby node as follows:

a) In the ShellAdmin console for the standby node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) To reconfigure VIP service, enter **A**.
d) Enter **Y** to confirm the action.
e) When prompted, enter the new VIP and confirm the entry.

Step 4 Reconfigure any service nodes that used the previous VIP as follows:

a) In the ShellAdmin console for the service node, choose **Reconfigure Node**.
b) When asked if you want to change the node role, enter **Y**.
c) At the submenu prompt, enter **A** to reconfigure the service node.
d) When asked if you want to continue, enter **Y**.
e) When prompted for the IP address of the Primary Node, enter the new VIP address.
Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.25
Disabling Database service at startup

SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for changes to take effect logout and login back
Do you want to logout [y/n]?
```

f) Enter **Y** to log out.

Reconfiguring a Service Node

If you change the IP address of a primary node or the VIP of an HA pair that a service node uses for database services, reconfigure the service node to use the updated IP address or VIP through the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console for the service node, choose the **Reconfigure Node** option.

Step 2 When asked if you want to change the node role to configure multi-node setup, enter **Y**.

Step 3 At the submenu prompt, enter **A** to reconfigure the node as a service node.

Step 4 When prompted, enter **Y** to continue.

Step 5 When prompted, enter the IP address of the primary node or the VIP of the HA pair that the service node uses for database access.
Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.30
Disabling Database service at startup

SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for changes to take effect logout and login back
Do you want to logout [y/n]?
```

Step 6 Enter **Y** to log out.
You are logged out of the ShellAdmin console and the GUI, and the changes are applied. Logging in again can take a few minutes while Cisco ICFPP is reconfigured.

Reconfiguring HA

You can reconfigure an HA setup by using the ShellAdmin console.

When reconfiguring HA:

- You must reconfigure both the active and standby nodes for HA.
- Reconfiguring HA restarts all services for the current HA setup, including VIP and the database, which disrupts services for any service nodes using the HA pair.
- The database on the node that you specify as the standby node in this procedure is deleted and replicates the contents of the database on the node that you specify as the active node.

Procedure

Step 1 Log into the ShellAdmin console of the active or standby node in the HA pair.

Step 2 At the ShellAdmin prompt, choose the **Setup HA** option.
Cisco ICFPP displays a message stating that HA is already configured on the node, provides additional information about the HA pair, and asks if you want to reconfigure HA on the node.

Step 3 Enter **Y** to reconfigure HA.

The HA reconfiguration submenu is displayed.

Step 4 Enter **B** to reconfigure the HA setup.
Cisco ICFPP displays informational messages and asks if you want to continue with the reconfiguration.

Step 5 Enter **Y** to continue.
Information similar to the following is displayed:

```
NOTE: The DB contents of the node being configured as the Standby node will be deleted and

the Standby node DB will replicate the contents of the node configured as Active.

Do you want to change this node to configure HA [y/n]?
```

Step 6 Enter **Y** to configure HA on the current node.

Step 7 At the submenu prompt, enter **A** to configure the node as the active node or **B** to configure the node as the standby node.

Step 8 Enter **Y** to continue.
Cisco ICFPP detects and displays the IP address of the current node.

Step 9 Enter **Y** to confirm the node IP address.

Step 10 Enter the IP address for the other node in the HA pair.

Step 11 Enter the VIP to use for the IP pair.
Information similar to the following is displayed:

```
-------------------------------------------------
HA Configuration information:
-------------------------------------------------
This node will be configured as active node
Active Node IP address:  123.45.1.30
Standby Node IP address: 123.45.1.32
Virtual IP address:      123.45.1.25
-------------------------------------------------
Proceed with setting up HA with above configuration [y/n]:
```

Step 12 Enter **Y** to continue.

Step 13 While Cisco ICFPP is configuring the current node for HA, configure the other node in the HA pair by choosing the **Setup HA** option in the ShellAdmin menu and repeating the steps in this procedure.
Cisco ICFPP displays progress messages as it configures the nodes for HA and synchronizes the databases on both nodes.

Step 14 When prompted, press **Enter** to return to the ShellAdmin menu.

Viewing HA Syslog Messages

After configuring Cisco ICFPP for HA, Cisco ICFPP checks HA status every five minutes. Any warning or failure messages that are issued are included in the log file for syslog messages. This log file commonly resides in `/var/log/` with the name `messages`. To view these messages, log in as root and use a text editor as described in this procedure.

Procedure

Step 1 In the ShellAdmin console, choose the **Log in as Root** option.

Step 2 Enter **Y** to confirm the login request, and enter the root account password at the prompt.

Step 3 Enter the following command to view the contents of the log file:

```
vi /directory-path/filename
```

where *directory-path* is location of the log file and *filename* is the name of the log file. For example, you might enter the following:

```
vi /var/log/messages
```

Step 4 To identify messages that pertain to HA, look for entries that contain the string `ICFPP HA` as shown in the following example:

```
Mar 13 03:27:13 localhost logger: ICFPP HA: MySQL replication from 123.45.67.8 to 123.45.67.9
 is in WARN state
Mar 13 03:27:13 localhost logger: ICFPP HA: Please use shelladmin to check HA status details
Mar 13 03:27:13 localhost logger: ICFPP HA: MySQL replication from 122.33.44.5 to 122.33.44.6
 is in WARN state
Mar 13 03:27:13 localhost logger: ICFPP HA: Please use shelladmin to check HA status details
```

Step 5 Address any HA-related messages as needed.

Working with Databases

Cisco ICFPP enables you to start, stop, back up, and restore a database.

Starting the Database

You can start the mysql daemon (mysqld) by choosing the **Start Database** option.

Note This option starts the appliance database only.

Procedure

Step 1 In the ShellAdmin console, choose the **Start Database** option.
Information similar to the following is displayed:

```
Starting database.....
directory (/var/lib/mysql/data/confmgr_production) exists
directory (/var/lib/mysql/data/db_private_admin) exists
the file (/var/lib/mysql/data/ib_logfile1) exists
```

```
the file (/var/lib/mysql/data/ib_logfile0) exists
the file (/var/lib/mysql/data/ibdata1) exists
Database started
Press return to continue ...130917 10:10:54 mysqld_safe Logging to '/var/log/mysqld.log'.
130917 10:10:54 mysqld_safe Starting mysqld daemon with databaes from /var/lib/mysql/data
```

Step 2 Choose the **Start Services** option to start the Cisco services.

Stopping the Database

You can halt the mysql daemon (mysqld) by choosing the **Stop Database** option. This option stops the following Cisco services:

- Broker
- Controller
- Eventmgr
- Client
- Idaccessmgr
- Inframgr
- Tomcat
- Websock

Procedure

Step 1 From the ShellAdmin menu, choose the **Stop Database** option.
The following information is displayed:

```
Do you want to stop the database [y/n]?  y
Stopping database....
Database stopped....
     Stopping broker [PID=21921]/[Child=21923]
     Stopping controller [PID=21959]/[Child=21961]
     Stopping eventmgr [PID=21993]/[Child=21995]
     Stopping client [PID=22052]/[Child=22054
22101
22160]
     Stopping idaccessmgr [PID=22099]/[Child=]
     Stopping inframgr [PID=22158]/[Child=]
     Tomcat is running with [PID=22213]. Stoping it and its child process
  Flashpolicyd is running with [PID=22237]. Stopping it
Stopping websock[PID=22242]
Press return to continue ...
```

Step 2 Follow the onscreen prompts to complete the process.

Step 3 To restart the database, choose the **Start Database** option.

Backing Up the Database

Cisco ICFPP enables you to back up the entire database of a Cisco ICFPP virtual appliance to an FTP server.

Before You Begin

Collect the following information:

- The IP address of the FTP server to use to back up the database.
- The FTP server login credentials.

Procedure

Step 1 Log in to the ShellAdmin console for the node with the database that is to be backed up.

Step 2 Stop Cisco services by choosing **Stop Services**.

Step 3 After the services have stopped, choose **Backup Database**.
Information similar to the following is displayed:

```
Backing database......
Backup will Upload file to an FTP server. Provide the necessary access credentials

   FTP Server IP Address:
```

Step 4 When prompted, enter the FTP server IP address and login credentials.
Cisco ICFPP displays progress messages while the database is being backed up.

Step 5 When the backup operation is complete, restart services by choosing **Start Services**.

What to Do Next

To restore the database, see Restoring the Database, on page 29.

Restoring the Database

Cisco ICFPP enables you to restore a backed up database from an FTP server. After you provide the FTP IP address, login credentials, and file details, Cisco ICFPP restores the database on the current node.

Before You Begin

Gather the following information:

- IP address of the FTP server with the backed-up database.
- FTP server login credentials.
- Absolute path and filename of the backed-up database.

Procedure

Step 1 In the ShellAdmin console, choose the **Stop Services** option.

Step 2 After the services have stopped, choose the **Restore Database** option.
Information similar to the following is displayed:

```
Restore database......
Restore will recover file from an FTP server. Provide the necessary access credentials

   FTP Server IP Address:
```

Step 3 At the prompts, enter the FTP server IP address, login credentials, and the absolute path and filename of the backed-up database file.

Step 4 After the database has been restored, choose the **Start Services** option to restart the Cisco services.

Accessing Root Privileges

Root privileges are required to move directories or files, grant or revoke user privileges, perform general system repairs, and install applications.

Note For security reasons, we recommend that you do not compile software as root.

Enabling Root Access

You can enable root privileges by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose the **Manage Root Access** option.
Information similar to the following is displayed:

```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **E**.
Information similar to the following is displayed:

```
Do you want to Enable Root Access [y/n]? :
```

Step 3 Enter **Y**.
Information similar to the following is displayed:

```
Enabling root access...
        Unlocking password for user root.
        passwd: Success.
        Root access enabled successfully
        Press return to continue
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Configuring Root Access

You can configure root privileges in the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose the **Manage Root Access** option.
Information similar to the following is displayed:
```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **C** to configure root access.
Information similar to the following is displayed:
```
Do you want to Configure/Set Root Privilege/Password [y/n]? :
```

Step 3 Enter **Y** set a new root password.
Information similar to the following is displayed:
```
Changing root password...
         Changing password for user root.
         New UNIX password:
```

Step 4 Enter the new root password and confirm it when prompted.
Information similar to the following is displayed:
```
passswd: all authentication tokens updated successfully.
         Root passwd changed successfully
         Press return to continue...
```

Step 5 Press **Enter** to return to the ShellAdmin menu.

Disabling Root Access

You can disable root privileges by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose the **Manage Root Access** option.
Information similar to the following is displayed:
```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **D**.
Information similar to the following is displayed:
```
Do you want to Disable Root Access [y/n]? :
```

Step 3 Enter **Y**.

Information similar to the following is displayed:

```
disabling root access...
         Locking password for user root.
         Passwd: Success
         Root access disabled sucessfully
         Press return to continue...
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Logging in as Root

You can log in as root from the ShellAdmin console.

Procedure

Step 1 From the ShellAdmin console, choose the **Login As Root** option.
Information similar to the following is displayed:

```
 Do you want to Login As Root [y/n]? :
```

Step 2 Enter **Y**.
Information similar to the following is displayed:

```
Logging in as root
         password:
```

Step 3 Enter the root password.
Information similar to the following is displayed:

```
Logging as root
Password:
[root@localhost shelladmin]#
```

Step 4 To log out, enter **exit**.
Information similar to the following is displayed:

```
[root@localhost shelladmin]# exit
exit
Successful logout
Press return to continue ...
```

Step 5 Press **Enter** to return to the ShellAdmin menu.