CHAPTER 7

Upgrading the Cisco Secure Access Control System

This chapter explains how to upgrade an ACS deployment or a standalone ACS server from 5.1/5.2 or from the available latest patch to 5.3.

Note If you are using ACS 5.0, you should first upgrade to ACS 5.1 and then to ACS 5.3. For procedures to upgrade from ACS 5.0 to ACS 5.1, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.1*.

This chapter describes the following scenarios:

- Upgrading an ACS Deployment from 5.2 to 5.3, page 7-2— To upgrade an ACS deployment from 5.2 to 5.3.
- Upgrading an ACS Deployment from 5.1 to 5.3, page 7-11— To upgrade an ACS deployment from 5.1 to 5.3.
- Upgrading ACS Server from 5.2 to 5.3, page 7-11— To upgrade an ACS server from 5.2 to 5.3. You can use any one of the following procedures:
  - Upgrading an ACS Server Using Application Upgrade Bundle, page 7-11— For an incremental upgrade of an ACS server from 5.2 to 5.3.
  - Re-imaging and Upgrading an ACS Server, page 7-12— To back up ACS 5.2 application data and restoring it on ACS 5.3.
- Upgrading an ACS Server from 5.1 to 5.3, page 7-14— To upgrade an ACS server from 5.1 to 5.3.
- Applying ACS Patch, page 7-14— To download and apply upgrade patch.

The upgrade process involves upgrading an ACS server that includes the Monitoring and Report Viewer and the configuration information in the database.

Note ACS 5.3 upgrades the CARS version too as a part of Application upgrade process.

During the upgrade process, ACS upgrades the ACS server to 5.3 and restores the data to the ACS 5.3 server. As part of the restore operation, ACS converts the configuration data to a 5.3-compatible format.

ACS stores the information related to data upgrade in /opt/CSCOacs/logs/acsupgrade.log. To view the content of this log file, download the support bundle.

For information on downloading the support bundle, see the *CLI Reference Guide for the Cisco Secure Access Control System 5.3*. Also, see /var/log/ade/ADE.log, which logs the details of all operations performed in ACS CLI.

If you are migrating ACS from 4.*x* to 5.3, follow the migration procedure as described in the *Migration Guide for the Cisco Secure Access Control System 5.3*.

You must have a repository configured with an FTP, NFS, or SFTP network server (but not a TFTP repository) to perform the ACS upgrade.

To create a repository, use the **`repository`** command. For more details about the commands used in this chapter, see the *CLI Reference Guide for the Cisco Secure Access Control System 5.3*.

Upgrade Paths

You can use the following upgrade paths to upgrade the ACS server from 5.x versions to ACS 5.3:

- **Path 1:** ACS 5.2 to ACS 5.3.

  To upgrade from ACS 5.2 to 5.3, see Upgrading ACS Server from 5.2 to 5.3, page 7-11.

- **Path 2:** ACS 5.1 to ACS 5.3.

  To upgrade from ACS 5.1 to 5.3, see Upgrading an ACS Server from 5.1 to 5.3, page 7-14.

- **Path 3:** ACS 5.0 to ACS 5.1 to ACS 5.3.

  To upgrade from ACS 5.0 to ACS 5.1, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.1*.

Upgrading an ACS Deployment from 5.2 to 5.3

Follow the procedure described in this section to upgrade an ACS 5.2 deployment to 5.3.

The deployment upgrade process consists of the following phases:

- Upgrading the Log Collector Server, page 7-3
- Upgrading the Secondary Servers, page 7-5
- Upgrading the Primary Server, page 7-7

Note ACS does not support interoperability between the ACS 5.2 and 5.3 deployments.

Usually in a deployment scenario of multiple servers, the ACS primary server functions as a master database for the configuration data, and a secondary server stores the monitoring and report data.

Initially, you need to upgrade the log collector server to ACS 5.3 and use this server as a common log collector between the ACS 5.2 and 5.3 deployments until the 5.3 upgrade for all servers is complete.

There are some exceptions to this usual setup, which can be handled as described below:

If ACS 5.2 primary server also functions as a log collector in your 5.2 deployment, you should promote any one of the secondary servers as primary server in the deployment. See Promoting a Secondary Server to Primary, page 7-9

Note Before upgrading any secondary server, you need to deregister it from the primary server.

Upgrading the Log Collector Server

To upgrade a log collector server to ACS 5.3, complete the following steps:

Step 1 Change any other secondary server as a log collector:

a. From the primary ACS server, choose **System Administration** > **Configuration** > **Log Configuration** > **Log Collector**.

The Log Collector page is displayed.

b. From the **Select Log Collector Server** drop down list, choose the new secondary instance as Log Collector and click **Set Log Collector**.

ACS services of the new secondary Log Collector gets restarted.

Step 2 Enter the **`show application status acs`** command in the EXEC to check whether all process are up and running successfully and press **Enter.**

The Console displays:

```
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'adclient'                running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

Now, you can observe that all the process are up and running.

Step 3 Deregister the old log collector server from the deployment and delete it from the ACS 5.2 primary server, so that it is now a standalone server:

a. From the web interface of the ACS 5.2 primary server, select **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. From the Secondary Instances table, check the check box next to the secondary instance that you want to deregister.

c. Click **Deregister**.

The system displays the following message:

```
This operation will deregister the selected ACS Instance from the Primary Instance.

Do you wish to continue?
```

d. Click **OK**.

The secondary instance (old log collector) services gets restarted.

e. From the Secondary Instances table, check the check box next to the deregistered secondary instance that you want to delete.

f. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

g. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

h. Log into the ACS 5.2 secondary server.

i. Select **System Administration > Operations > Distributed System Management**.

j. From the Secondary Instances table, check the check box next to the deregistered secondary instance that you want to delete.

k. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

l. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

Step 4 Back up the log collector data:

From the ACS CLI, enter the following **backup** command in the EXEC mode to perform a backup and place the backup in a remote repository:

backup *backup-file-name* **repository** *repository-name*

Step 5 Upgrade the Old ACS Log Collector:

Use the procedure in Upgrading ACS Server from 5.2 to 5.3, page 7-11.

When the ACS processes of the 5.3 log collector server are up and running, all configuration data, monitoring and report data, and reports are upgraded.

Now, the Old Log Collector is upgraded to 5.3 and functions as the ACS 5.3 standalone primary server as well as a log collector.

Step 6 Define the 5.3 log collector as a remote log target for the 5.2 deployment.

a. Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears.

b. Click **Create**.

The Create page appears.

c. Enter the values for the following fields:

- Name—The name of the remote log target. Maximum length is 32 characters.
- Description—(Optional) A description of the remote log target. Maximum description length is 1024 characters.
- Type—The type of remote log target. Syslog is the only option.
- IP Address—IP address of the remote log target, in the format *x.x.x.x*. Specify the IP address of the 5.3 log collector server.
- Use Advanced Syslog Options—Click to enable the advanced syslog options that include port number, facility code, and maximum length.
- Port—The port number of the remote log target that is used as the communication channel between the ACS and the remote log target (default is 514). Enter **20514** for the port number.

- Facility Code—(Optional) Choose an option from the Facility Code drop-down list box.
- Maximum Length—The maximum length of the remote log target messages. Valid options are from 200 to 1024.

d. Click **Submit**.

The remote log target configuration is saved. The Remote Log Targets page appears with the new remote log target configuration.

Now, the authentication details from the 5.2 deployment are logged in both the 5.2 and 5.3 log collector servers.

Step 7 On the 5.2 primary server, configure the appropriate logging categories for the remote log target:

a. Select **System Administration > Configuration > Log Configuration > Logging Categories > Global**.

The Logging Categories page appears; from here, you can view the logging categories.

b. Click the name of the logging category you want to configure;

Or,

Click the radio button next to the name of the logging category you want to configure and click **Edit**.

c. In the **General** tab, complete the following fields:

- Log Severity—Use the drop-down list box to select the severity level. Valid options are FATAL, ERROR, WARN, INFO, and DEBUG.
- Log to Local Target—Check to enable logging to the local target.
- Local Target is Critical—Check the check box to make this local target the critical target. Usable for accounting and for AAA audit (passed authentication) logging category types only.

d. Click the **Remote Syslog Target** tab and choose the Remote Targets to view the logs.

e. Click **Submit**.

The Logging Categories page appears, with your configured logging category.

Upgrading the Secondary Servers

To upgrade each 5.2 secondary server in your deployment to 5.3:

To ensure that you preserve the local certificates of the secondary server, you should promote each secondary server to primary role and then perform the ACS 5.3 upgrade. See Upgrading the PKI Data and Certificates, page 7-9.

Before upgrading a secondary ACS server, ensure that the server is not inactive and it is not in local mode.

To verify the status, from the web interface of the secondary server, select **System Administration > Operations > Local Operations** and check the status of the secondary ACS server.

Step 1 Verify if the secondary server is a log collector. If so, change the log collector server to any other secondary server; otherwise, proceed to Step 2.

a. From the 5.2 primary server, select **System Administration > Configuration > Log Configuration > Log Collector**.

ACS displays the current log collector server.

b. From the Select Log Collector drop-down list box, choose a different server to configure it as a log collector.

c. Click **Set Log Collector**.

Step 2 Deregister the secondary server from the 5.2 deployment and delete it from the ACS 5.2 primary server, so that it now becomes a standalone server:

a. Select **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. From the Secondary Instances table, check the check box next to the secondary instance that you want to deregister.

c. Click **Deregister**.

The system displays the following message:

```
This operation will deregister the selected ACS Instance from the Primary Instance.

Do you wish to continue?
```

d. Click **OK**.

The ACS machine restarts.

e. Log into the ACS 5.2 primary server.

f. Select **System Administration > Operations > Distributed System Management**.

g. From the Secondary Instances table, check the check box next to the secondary instance that you want to delete.

h. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

i. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

j. Log into the ACS 5.2 secondary server.

k. Select **System Administration > Operations > Distributed System Management**.

l. From the Secondary Instances table, check the check box next to the deregistered secondary instance that you want to delete.

m. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

n. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

Step 3 Back up the secondary server data.

From the ACS CLI, issue the following **backup** command in the EXEC mode to perform a backup and place the backup in a repository:

`backup` *backup-name* **repository** *repository-name*

Step 4 Upgrade the ACS server to 5.3. See Upgrading ACS Server from 5.2 to 5.3, page 7-11.

Step 5 Register the secondary server to the ACS 5.3 primary server.

a. Select **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operation page appears.

b. Complete the following mandatory fields under Registration dialog box:

- Primary Instance—The hostname of the 5.3 primary server that you wish to register the secondary instance with.
- Admin Username—Username of an administrator account.
- Admin Password—The password for the administrator account.
- Hardware Replacement—Check to enable the existing ACS instance to re-register with the primary instance and get a copy of the configuration already present in the primary instance.
- Recovery Keyword—Specify the same hostname that was used in the 5.2 deployment to ensure that you associate this secondary server with the monitoring and report data collected earlier.

  After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword, and marks each record as registered.

c. Click **Register to Primary**.

The system displays the following message:

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

d. Click **OK**.

ACS will restart automatically. Wait for sometime to make sure that all processes are up and running successfully.

Note When you register a secondary to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance are replicated to the secondary instance.

After the registration is complete, ACS performs a full synchronization and sends the ACS 5.3 configuration data to the 5.3 secondary server.

Step 6 Import local and outstanding CSRs.

See Importing Server Certificates and Associating Certificates to Protocols section and Generating Self-Signed Certificates section of the User Guide for the Cisco Secure Access Control System 5.3.

When there is no secondary servers registered with the primary, the primary server itself acts as a log collector. Upgrade the ACS 5.2 primary server to ACS 5.3 once all the secondary servers are upgraded to ACS 5.3.

Upgrading the Primary Server

To upgrade the primary server from a 5.2 to 5.3 deployment:

Step 1 Make sure the primary server is a standalone server:

a. Select **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. Check if there are secondary servers listed in the Secondary Instances table. If there are any secondary servers, upgrade those servers before upgrading the 5.2 primary server. See Upgrading the Secondary Servers, page 7-5.

Step 2 Upgrade the ACS server to 5.3. See Upgrading ACS Server from 5.2 to 5.3, page 7-11.

Step 3 Register the newly upgraded 5.3 server to the existing Primary ACS 5.3 server:

a. Select **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operation page appears.

b. Complete the following mandatory fields under Registration dialog box:

- Primary Instance—The hostname of the primary server that you wish to register the secondary instance with.
- Admin Username—Username of an administrator account.
- Admin Password—The password for the administrator account.
- Hardware Replacement—Check to enable the existing ACS instance with re-register to the primary instance and get a copy of the configuration already present in the primary instance.
- Recovery Keyword—Specify the same hostname as was used in the 5.2 deployment to ensure that you associate this server with the monitoring and report data collected earlier.

  After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword, and marks each record as registered.

c. Click **Register to Primary**.

The system displays the following message:

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

d. Click **OK**.

ACS will restart automatically. Wait for sometime to make sure that all processes are up and running successfully.

Note When you register a secondary to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance are replicated to the secondary instance.

Promote this instance as the ACS 5.3 primary again. See Promoting a Secondary Server to Primary, page 7-9.

Now, the ACS 5.2 deployment is completely upgraded to ACS 5.3 deployment.

Upgrading the PKI Data and Certificates

The ACS 5.2 Public Key Infrastructure (PKI) credentials and the local certificates and outstanding CSRs are restored in ACS 5.3 by reimporting the certificates.

If you upgrade the ACS 5.2 machine to ACS 5.3, all the PKI data will be erased. To preserve the local certificates, you must import all local and outstanding CSRs to the primary node in the deployment.

To preserve the local certificates:

Step 1 On the ACS 5.2 target machine, go to **System Administration** > **Configuration** > **Local Server Certificates** > **Local Certificates**.

Step 2 Check the local certificate.

Step 3 Click **Export**.

Step 4 Export the certificate and the private key.

Step 5 Repeat steps 2 to 4 for all the local certificates.

Step 6 Go to **System Administration** > **Configuration** > **Local Server Certificates** > **Outstanding Signing Requests**.

Step 7 Check the **CSR**.

Step 8 Click **Export**.

Step 9 Repeat steps 7 and 8 for all the CSRs.

Step 10 Save all the exported certificates and CSRs.

Step 11 Upgrade the ACS 5.2 server to 5.3. See Upgrading ACS Server from 5.2 to 5.3, page 7-11.

Step 12 Import all the exported certificates and **CSRs**.

Promoting a Secondary Server to Primary

To promote a secondary server to the primary server:

Step 1 From the web interface of the primary server, select **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

Step 2 In the Secondary Instances table, check the check box next to the secondary server that you want to promote to primary.

Step 3 Click **Promote**.

The system displays the following message:

```
This operation will promote the selected ACS Instance to become the new Primary Instance.
As a consequence, the current Primary Instance will be demoted to a Secondary.

Do you wish to continue?
```

Step 4 Click **OK**.

The system promotes the selected secondary server to primary, moves it to the Primary Instance table, and the existing primary server will be automatically moved to the Secondary Instances table.

When the registration completes, ACS performs a full synchronization and sends the ACS 5.3 configuration data to the newly promoted primary server.

Upgrading the ACS Monitoring and Report Viewer

ACS invokes the upgrade of the Monitoring and Report Viewer as a subtask during upgrade.

The maximum disk space available for ACS Monitoring and Report Viewer is 150 GB.

This section contains:

- Restoring the Monitoring and Report Viewer Data After Upgrade, page 7-101
- Upgrading the Database, page 7-10
- Upgrading the Reports, page 7-10

To check the status of the database upgrade, in the Monitoring and Report Viewer, choose **Monitoring Configuration** > **System Operations** > **Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the status of the Monitoring and Report Viewer data upgrade.

When the database upgrade completes, ACS displays the following message:

```
Upgrade completed successfully.
```

Restoring the Monitoring and Report Viewer Data After Upgrade

When you restore the backup data after upgrading to 5.3, ACS automatically synchronizes the changes with the database and reports, if any changes are found.

The reports data is available only for the period during which you take a backup and not for the period when you restore it. For example, if you back up the data in June and restore it in August, the reports data available will be only for June and not for August. To get the latest reports data you need to run the reports again.

Upgrading the Database

After the 5.3 upgrade, if you restore the backup made prior to the upgrade, ACS displays the database version as **AVPair:DBVersion=5.3** and maintains the schema version as 5.3 in the av_system_settings table. When the database process restarts, ACS checks the ACS version and the database version if they are out-of-date and performs a schema and data upgrade.

Upgrading the Reports

After you upgrade to 5.3, if you restore the backup made before the upgrade, ACS checks whether the reports tag displays "View 5.3" and when the web process starts up, ACS performs the necessary updates.

Note When you click Switch Database, the logs that are generated after performing the Step 7 (upgrading database schema to version 5.1) of the log collector server upgrade will be lost. ACS retains only the logs that are generated before you perform Step 7.

Upgrading an ACS Deployment from 5.1 to 5.3

Follow the same procedure as described Upgrading an ACS Deployment from 5.2 to 5.3, page 7-2.

Upgrading ACS Server from 5.2 to 5.3

These are the following two ways in which you can upgrade an ACS server from 5.2 to 5.3: You can use any one of the methods to upgrade.

- Upgrading an ACS Server Using Application Upgrade Bundle, page 7-11
- Re-imaging and Upgrading an ACS Server, page 7-12

Upgrading an ACS Server Using Application Upgrade Bundle

To upgrade an ACS server from 5.2 to 5.3:

Step 1 Place the ACS 5.3 application upgrade bundle (ACS_5.3.tar.gz) in a remote repository.

To configure the repository, follow the procedure given in the CLI Reference Guide for Cisco Access Control System 5.3.

Step 2 Enter the following application upgrade command in the EXEC mode to upgrade ACS.

application upgrade ACS_5.3.tar.gz *repository-name*

ACS displays the following confirmation message:

```
Do you want to save the current configuration? (yes/no) [yes]?
```

Step 3 Enter **yes**.

When the ACS upgrade is complete, the following message appears:

```
% CARS Install application required post install reboot...

The system is going down for reboot NOW!

Application upgrade successful
```

While ACS upgrades the ACS 5.2 configuration data, it also converts the ACS 5.2 Monitoring and Report Viewer data to the 5.3 format.

Step 4 To monitor the status of the data upgrade, from the Monitoring and Report Viewer, choose **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the status of the Monitoring and Report Viewer data upgrade.

When the database upgrade completes, ACS displays the following message:

```
Upgrade completed successfully.
```

Step 5 Click **OK**.

Step 6 Enter the **`show application version acs`** command to check whether the ACS version is upgraded successfully.

The following message is displayed:

```
Cisco ACS VERSION INFORMATION

-----------------------------

Version : 5.3.0.40

Internal Build ID : B.839.EVAL
```

Step 7 Enter the **`show application status acs`** command in the EXEC to check whether all the process are up and running successfully and press **Enter.**

The Console displays:

```
ACS role: PRIMARY
Process 'database'                   running
Process 'management'                 running
Process 'runtime'                    running
Process 'adclient'                   running
Process 'view-database'              running
Process 'view-jobmanager'            running
Process 'view-alertmanager'          running
Process 'view-collector'             running
Process 'view-logprocessor'          running
```

Now, you can observe that all the process are up and running. It shows that ACS is successfully upgraded to ACS 5.3

Note The recommended method to upgrade the ACS server is **upgrading an ACS Server Using Application Upgrade Bundle** method.

Re-imaging and Upgrading an ACS Server

This section explains how to upgrade ACS 5.2 to 5.3 by backing up the ACS 5.2 data and restoring it on re-imaged ACS 5.3 server. You must have physical access to the ACS box to perform this upgrade procedure.

To perform reimage and upgrade to ACS 5.3:

Step 1 Back up the ACS data from the ACS 5.2 server.

Step 2 Enter the following **`backup`** command in the EXEC mode to perform a backup and place the backup in a repository.

`backup` *backup-name* **`repository`** *repository-name*

Note Ensure that you use a remote repository for the ACS 5.2 data backup. Otherwise, you might lose the backed up data after you install 5.3.

Step 3 Use the ACS 5.3 recovery DVD to install ACS 5.3. See Reimaging the ACS Server, page 5-7

This re-images the ACS server to a fresh ACS 5.3 server without any configuration data.

Step 4 Configure a repository in the fresh ACS 5.3 server to restore the backed up data.

Step 5 Restore the backed up data taken earlier in step 2 to the ACS 5.3 server.

Enter the **restore** command in the EXEC mode to restore the backup:

restore *filename* **repository** *repository-name*

While restoring the data, using the 5.2 backup file, this command restores the ACS 5.2 configuration data. It also converts and upgrades the ACS 5.2 Monitoring and Report Viewer data to the 5.3 format.

Step 6 To monitor the status of the data upgrade, from the Monitoring and Report Viewer, choose **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the upgrade status of the Monitoring and Report Viewer data.

When the database upgrade completes, the following message is displayed.

```
Upgrade completed successfully.
```

Step 7 Click **OK**.

Warning **The ACS restore does not update pki on mgmt/eap. HTTPS uses a self-signed certificate, even though the only cert in the GUI/db was the CA signed one.**

A work-around for this is:
1. Create a self-signed temporary self-signed cert and assign EAP/mgmt to it.
2. Re-assign EAP/mgmt to CA signed cert
3. Delete self-signed cert.

Note Restore the backup file in the same ACS server to avoid IP conflict issues.

Note Before restoring ACS 5.2 database backup in ACS 5.3, you need to install ACS 5.3 patch 4 (or higher).

Upgrading an ACS Server from 5.1 to 5.3

To upgrade your ACS 5.1 server to ACS 5.3, follow the same procedure as described in Upgrading ACS Server from 5.2 to 5.3, page 7-11.

Applying ACS Patch

You can download the ACS 5.3 cumulative patches from the following location:

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

To download and apply the patches:

Step 1 Log into Cisco.com and navigate to **Network Management > Security and Identity Management > Cisco Secure Access Control Server Products > Cisco Secure Access Control System > Cisco Secure Access Control System 5.3**.

Step 2 Download the patch.

Step 3 Install the ACS 5.3 cumulative patch by running the following **acs patch** command in the EXEC mode to install the ACS patch:

acs patch install *patch-name*.**tar.gpg repository** *repository-name*

ACS displays the following confirmation message:

```
Installing an ACS patch requires a restart of ACS services.
Would you like to continue? yes/no
```

Step 4 Enter **yes**.

ACS version is upgraded to the applied patch.

Step 5 Check whether all services are running properly, by using the CLI **show application status acs** command from the EXEC mode.

Note If the backup data is huge in size, then extraction process might take a minimum of 1 hour to many hours.