Upgrading Cloudera Manager 5 to the Latest Cloudera Manager (#cmig_topic_9_4)

Minimum Required Role: Full Administrator (cm_sg_user_roles.html#concept_wfh_tvy_qp)

This process applies to upgrading all versions of Cloudera Manager 5.

In most cases it is possible to complete the following upgrade without shutting down most CDH services, although you may need to stop some dependent services. CDH daemons can continue running, unaffected, while Cloudera Manager is upgraded. The upgrade process does not affect your CDH installation. After upgrading Cloudera Manager you may also want to upgrade CDH 4 clusters to CDH 5.

Upgrading Cloudera Manager 5 to the latest version of Cloudera Manager involves the following steps.

1. Review Warnings
2. Before You Begin
3. Stop Selected Services and Roles
4. Back Up the Cloudera Navigator Metadata Server Storage Directory
5. Remove Kafka 1.2 CSD
6. Stop Cloudera Manager Server, Database, and Agent
7. Upgrade the JDK on Cloudera Manager Server and Agent Hosts
8. Upgrade Cloudera Manager Software
9. Start Cloudera Manager Server
10. Upgrade and Start Cloudera Manager Agents
11. Verify the Upgrade Succeeded
12. (Optional) Configure TLS/SSL for Cloudera Management Service
13. Deploy JDK Upgrade
14. Disable Kafka Monitoring
15. Start Selected Services and Roles
16. (Optional) Restart Services and Deploy Updated Client Configurations
17. Test the Installation
18. (Optional) Upgrade CDH

Review Warnings (#concept_c34_2nh_fn)

Warning:

- **Cloudera Management Service TLS/SSL configuration**

  If you have enabled TLS security for the Cloudera Manager Admin Console, as of Cloudera Manager 5.1, Cloudera Management Service roles try to communicate with Cloudera Manager using TLS, and fail to start until TLS/SSL properties have been configured.

- **Navigator**

If you have enabled auditing with Cloudera Navigator, during the upgrade to Cloudera Manager 5, auditing is suspended and is only restarted when you restart the roles of audited services.

- **JDK upgrade**

  If you upgrade the JDK during the installation of the Cloudera Manager Agent, you must *restart all services*. Additionally, if you have enabled TLS/SSL, you must reinstall CA certificates to your truststores. See **Creating Truststores (cm_sg_create_key_trust.html#concept_u35_w2m_l4)**.

Before You Begin (#concept_tsy_5vq_wn)

Ensure that you have performed the following steps:

- **Obtain host credentials** - For Cloudera Manager to upgrade the Agent packages, you must have SSH access and be able to log in using a root account or an account that has password-less sudo permission. See **Cloudera Manager 5 Requirements and Supported Versions (cm_ig_cm_requirements.html#cmig_topic_4)** for more information.
- **Prepare databases** - See **Database Considerations for Cloudera Manager Upgrades (cm_ag_db_for_cm_upgrades.html#cmig_topic_9_2)**.
- Perform pre-upgrade steps required by **Cloudera Navigator (cn_iu_upgrade_navigator.html#xd_583c10bfdbd326ba-7dae4aa6-147c30d0933--7f27__section_qfk_3kc_ks)**.

Stop Selected Services and Roles (#cmig_topic_9_4_2)

If your cluster meets any of the conditions listed in the following table, you must stop the indicated services or roles.

Condition	Procedure
Running a version of Cloudera Manager that has the Cloudera Management Service	Stop the Cloudera Management Service.
Running the embedded PostgreSQL database	Stop all services that are using the embedded database: • Hive service and all services such as Impala and Hue that use the Hive metastore • Oozie • Sentry
Running Cloudera Navigator data management component and the following services are enabled for auditing: • **HDFS** • **HBase** • **Hive** • **Hue**	Stop the following roles: • **HDFS** - NameNode • **HBase** - Master and RegionServers • **Hive** - HiveServer2 • **Hue** - Beeswax Server Stopping these roles renders any service depending on these roles unavailable. For the **HDFS** - NameNode case this implies most of the services in the cluster will be unavailable until the upgrade is finished.

Back Up the Cloudera Navigator Metadata Server Storage Directory (#concept_ixf_35p_ks)

If you are running the Cloudera Navigator data management component, back up the **Navigator Metadata Server storage directory (cn_iu_metadata_server.html#xd_583c10bfdbd326ba--43d5fd93-1410993f8c2--7f71__section_bmv_zzz_vl)** .

Remove Kafka 1.2 CSD (#concept_nyg_jby_pr)

If you have previously installed Kafka 1.2, remove the Kafka CSD:

1. Determine the location of the CSD directory:
   a. Select Administration > Settings.
   b. Click the **Custom Service Descriptors** category.
   c. Retrieve the directory from the **Local Descriptor Repository Path** property.
2. Delete the Kafka CSD from the directory.

Stop Cloudera Manager Server, Database, and Agent (#id_fqz_4mx_zn)

1. Use the Admin Console to stop any running commands. These include commands a user runs and commands Cloudera Manager automatically triggers in response to a state change or a schedule. You can either wait for commands to complete or abort any running commands. For more information on viewing and aborting running commands, see **Viewing Running and Recent Commands (cm_dg_view_running_recent_commands.html#cmug_topic_4_7)** . If you do not stop all commands, the Cloudera Manager Server will *fail to start after upgrade*.
2. On the host running the Cloudera Manager Server, stop the Cloudera Manager Server:

   ```
   $ sudo service cloudera-scm-server stop
   ```

3. If you are using the embedded PostgreSQL database for Cloudera Manager, stop the database:

   ```
   $ sudo service cloudera-scm-server-db stop
   ```

   Important: If you are *not* running the embedded database service and you attempt to stop it, you receive a message indicating that the service cannot be found. If instead you get a message that the shutdown failed, the embedded database is still running, probably because services are connected to the Hive metastore. If the database shutdown fails due to connected services, issue the following command:

   - RHEL-compatible 7 and higher:

     ```
     $ sudo service cloudera-scm-server-db next_stop_fast
     $ sudo service cloudera-scm-server-db stop
     ```

   - All other Linux distributions:

     ```
     sudo service cloudera-scm-server-db fast_stop
     ```

4. If the Cloudera Manager host is also running the Cloudera Manager Agent, stop the Cloudera Manager Agent:

   ```
   $ sudo service cloudera-scm-agent stop
   ```

Upgrade the JDK on Cloudera Manager Server and Agent Hosts (#concept_z1r_qmn_mn)

If you are using JDK 1.6, you *must* upgrade to JDK 1.7 or 1.8. See **Java Development Kit Installation (cdh_ig_jdk_installation.html#topic_29)** .

Upgrade Cloudera Manager Software (#concept_mn4_r1m_2r)

Choose a procedure based on how you installed Cloudera Manager:

- **Upgrade Cloudera Manager Server (Packages)**
- **Install Cloudera Manager Server and Agent Software (Tarballs)**

Upgrade Cloudera Manager Server (Packages) (#concept_qjq_cxz_zn)

1. To upgrade the Cloudera Manager Server packages, you can upgrade from the Cloudera repository at `https://archive.cloudera.com/cm5/`, or you can create your own repository, as described in **Understanding Custom Installation Solutions (cm_ig_custom_installation.html#cmig_topic_21)** . You must create your own repository if you are upgrading a cluster that does not have Internet access.
   a. Find the Cloudera repo file for your distribution by starting at `https://archive.cloudera.com/cm5/` and navigating to the directory that matches your operating system.

      For example, for Red Hat or CentOS 6, you would go to `https://archive.cloudera.com/cm5/redhat/6/x86_64/cm/`. In that directory, find the repo file that contains information including the repository base URL and GPG key. The contents of the `cloudera-manager.repo` are similar to the following:

      ```
      [cloudera-manager]
      # Packages for Cloudera Manager, Version 5, on RHEL or CentOS 6 x86_64
      name=Cloudera Manager
      baseurl=https://archive.cloudera.com/cm5/redhat/6/x86_64/cm/5/
      gpgkey = https://archive.cloudera.com/cm5/redhat/6/x86_64/cm/RPM-GPG-KEY-cloudera
      gpgcheck = 1
      ```

      For Ubuntu or Debian systems, go to the appropriate release directory, for example, `https://archive.cloudera.com/cm4/debian/wheezy/amd64/cm`. The repo file, in this case, `cloudera.list`, is similar to the following:

      ```
      # Packages for Cloudera Manager, Version 5, on Debian 7.0 x86_64
      deb https://archive.cloudera.com/cm5/debian/wheezy/amd64/cm wheezy-cm5 contrib
      deb-src https://archive.cloudera.com/cm5/debian/wheezy/amd64/cm wheezy-cm5 contrib
      ```

   b. Replace the repo file in the configuration location for the package management software for your system.

Operating System	Commands
RHEL	Copy `cloudera-manager.repo` to `/etc/yum.repos.d/`.
SLES	Copy `cloudera-manager.repo` to `/etc/zypp/repos.d/`.
Ubuntu or Debian	Copy `cloudera.list` to `/etc/apt/sources.list.d/`.

   c. Run the following commands:

Operating System	Commands

RHEL	`$ sudo yum clean all`
	`$ sudo yum upgrade cloudera-manager-server cloudera-manager-daemon`
	
	Note:
	▪ `yum clean all` cleans `yum` cache directories, ensuring that you download and i
	▪ If your system is not up to date, any underlying system components must be up components must be upgraded.

SLES	`$ sudo zypper clean --all`
	`$ sudo zypper up -r https://archive.cloudera.com/cm5/sles/11/x86_6`
	
	To download from your own repository:
	
	`$ sudo zypper clean --all`
	`$ sudo zypper rr cm`
	`$ sudo zypper ar -t rpm-md http://myhost.example.com/path_to_cm_re`
	`$ sudo zypper up -r http://myhost.example.com/path_to_cm_repo`

Ubuntu or Debian	The following commands clean cached repository information and update Clouder `$ sudo apt-get clean` `$ sudo apt-get update` `$ sudo apt-get dist-upgrade` `$ sudo apt-get install cloudera-manager-server cloudera-manager-da` During this process, you may be prompted about your configuration file version: `Configuration file `/etc/cloudera-scm-agent/config.ini'` `==> Modified (by you or by a script) since installation.` `==> Package distributor has shipped an updated version.` `What would you like to do about it ? Your options are:` `Y or I : install the package maintainer's version` `N or O : keep your currently-installed version` `D : show the differences between the versions` `Z : start a shell to examine the situation` `The default action is to keep your current version.`  You will receive a similar prompt for `/etc/cloudera-scm-server/db.propertie`

2. If you customized `/etc/cloudera-scm-agent/config.ini`, your customized file is moved to a file with the extension `.rpmsave` or `.dpkg-old`. Merge any customizations into `/etc/cloudera-scm-agent/config.ini` installed by the package manager.

You should now have the following packages, corresponding to the version of Cloudera Manager you installed, on the host that will be the Cloudera Manager Server host.

OS	Packages

RPM-based distributions	`$ rpm -qa 'cloudera-manager-*'`
	`cloudera-manager-repository-5.0-1.noarch`
	`cloudera-manager-server-5.6.1-0.cm561.p0.3.el6.x86_64`
	`cloudera-manager-server-db-2-5.6.1-0.cm561.p0.3.el6.x86_64`
	`cloudera-manager-agent-5.6.1-0.cm561.p0.3.el6.x86_64`
	`cloudera-manager-daemons-5.6.1-0.cm561.p0.3.el6.x86_64`

Ubuntu or Debian	`~# dpkg-query -l 'cloudera-manager-*'`
	`Desired=Unknown/Install/Remove/Purge/Hold`
	`| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/`
	`|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)`
	`||/ Name Version Description`
	`+++-==========-==========-==========`
	`ii cloudera-manager-agent 5.6.1-0.cm561.p0.3~sq The Cloudera Manager`
	`ii cloudera-manager-daemo 5.6.1-0.cm561.p0.3~sq Provides daemons for`
	`ii cloudera-manager-serve 5.6.1-0.cm561.p0.3~sq The Cloudera Manager`

You may also see an entry for the `cloudera-manager-server-db-2` if you are using the embedded database, and additional packages for plug-ins, depending on what was previously installed on the server host. If the `cloudera-manager-server-db-2` package is installed, and you do not plan to use the embedded database, you can remove this package.

Install Cloudera Manager Server and Agent Software (Tarballs) (#concept_m35_t1m_2r)

Tarballs contain both the Cloudera Manager Server and Cloudera Manager Agent in a single file. Download tarballs from the locations listed in **Cloudera Manager Version and Download Information (cm_vd.html#cmvd_topic_1)** . Copy the tarballs and unpack them on all hosts on which you intend to install Cloudera Manager Server and Cloudera Manager Agents, in a directory of your choosing. If necessary, create a new directory to accommodate the files you extract from the tarball. For instance, if `/opt/cloudera-manager` does not exist, create it using a command similar to:

```
$ sudo mkdir /opt/cloudera-manager
```

Extract the contents of the tarball, to this directory. For example, to copy a tar file to your home directory and extract the contents of all tar files to the `/opt/` directory, use a command similar to the following:

```
$ sudo tar xzf cloudera-manager*.tar.gz -C /opt/cloudera-manager
```

The files are extracted to a subdirectory named according to the Cloudera Manager version being extracted. For example, files could be extracted to `/opt/cloudera-manager/cm-5.6.0/`. This full path is needed later and is referred to as *tarball_root* directory.

Configure Cloudera Manager Agents (#concept_m35_t1m_2r__section_ub1_tl3_yr)

- On every Cloudera Manager Agent host, configure the Cloudera Manager Agent to point to the Cloudera Manager Server by setting the following properties in the *tarball_root*`/etc/cloudera-scm-agent/config.ini` configuration file:

Property	Description
`server_host`	Name of the host where Cloudera Manager Server is running.
`server_port`	Port on the host where Cloudera Manager Server is running.

- By default, a tarball installation has a `var` subdirectory where state is stored. In a non-tarball installation, state is stored in `/var`. Cloudera recommends that you reconfigure the tarball installation to use an external directory as the `/var` equivalent (`/var` or any other directory outside the tarball) so that when you upgrade Cloudera Manager, the new tarball installation can access this state. Configure the installation to use an external directory for storing state by editing *tarball_root*`/etc/default/cloudera-scm-agent` and setting the `CMF_VAR` variable to the location of the `/var` equivalent. If you do not reuse the state directory between different tarball installations, duplicate Cloudera Manager Agent entries can occur in the Cloudera Manager database.

Start Cloudera Manager Server (#concept_n3j_w1m_2r)

Choose a procedure based on how you installed Cloudera Manager:

- **Start the Cloudera Manager Server (Packages)**
- **Start the Cloudera Manager Server (Tarball)**

Start the Cloudera Manager Server (Packages) (#concept_f4d_5yd_np)

On the Cloudera Manager Server host (the system on which you installed the `cloudera-manager-server` package) do the following:

1. If you are using the embedded PostgreSQL database for Cloudera Manager, start the database:

   ```
   $ sudo service cloudera-scm-server-db start
   ```

2. Start the Cloudera Manager Server:

   ```
   $ sudo service cloudera-scm-server start
   ```

   You should see the following:

   ```
   Starting cloudera-scm-server:                              [  OK  ]
   ```

Start the Cloudera Manager Server (Tarball) (#concept_xgy_x1m_2r)

The way in which you start the Cloudera Manager Server varies according to what account you want the Server to run under:

- As root:

  ```
  $ sudo tarball_root/etc/init.d/cloudera-scm-server start
  ```

- As another user. If you run as another user, ensure the user you created for Cloudera Manager owns the location to which you extracted the tarball including the newly created database files. If you followed the earlier examples and created the directory `/opt/cloudera-manager` and the user `cloudera-scm`, you could use the following command to change ownership of the directory:

  ```
  $ sudo chown -R cloudera-scm:cloudera-scm /opt/cloudera-manager
  ```

Once you have established ownership of directory locations, you can start Cloudera Manager Server using the user account you chose. For example, you might run the Cloudera Manager Server as `cloudera-service`. In this case, you have the following options:

- Run the following command:

  ```
  $ sudo -u cloudera-service tarball_root/etc/init.d/cloudera-scm-server start
  ```

- Edit the configuration files so the script internally changes the user. Then run the script as root:
  1. Remove the following line from *tarball_root*`/etc/default/cloudera-scm-server`:

     ```
     export CMF_SUDO_CMD=" "
     ```

  2. Change the user and group in *tarball_root*`/etc/init.d/cloudera-scm-server` to the user you want the server to run as. For example, to run as `cloudera-service`, change the user and group as follows:

     ```
     USER=cloudera-service
     GROUP=cloudera-service
     ```

  3. Run the server script as root:

     ```
     $ sudo tarball_root/etc/init.d/cloudera-scm-server start
     ```

- To start the Cloudera Manager Server automatically after a reboot:
  1. Run the following commands on the Cloudera Manager Server host:
     - **RHEL-compatible and SLES**

       ```
       $ cp tarball_root/etc/init.d/cloudera-scm-server /etc/init.d/cloudera-scm-server
       $ chkconfig cloudera-scm-server on
       ```

     - **Debian/Ubuntu**

       ```
       $ cp tarball_root/etc/init.d/cloudera-scm-server /etc/init.d/cloudera-scm-server
       $ update-rc.d cloudera-scm-server defaults
       ```

  2. On the Cloudera Manager Server host, open the `/etc/init.d/cloudera-scm-server` file and change the value of `CMF_DEFAULTS` from `${CMF_DEFAULTS:-/etc/default}` to *tarball_root*`/etc/default`.

Upgrade and Start Cloudera Manager Agents (#concept_kpw_bbm_2r)

Choose a procedure based on how you installed Cloudera Manager:

- **Upgrade and Start Cloudera Manager Agent (Packages)**
- **Restart Cloudera Manager Agents (Tarballs)**

Upgrade and Start Cloudera Manager Agent (Packages) (#cmig_topic_9_4_5)

Important: All hosts in the cluster must have access to the Internet if you plan to use `archive.cloudera.com` as the source for installation files. If you do not have Internet access, create a custom repository.

1. Log in to the Cloudera Manager Admin Console.
2. Upgrade hosts using one of the following methods:
   - **Cloudera Manager installs Agent software**

a. Select **Yes, I would like to upgrade the Cloudera Manager Agent packages now** and click **Continue**.

b. Select the release of the Cloudera Manager Agent to install. Normally, this is the **Matched Release for this Cloudera Manager Server**. However, if you used a custom repository (instead of archive.cloudera.com) for the Cloudera Manager server, select **Custom Repository** and provide the required information. The custom repository allows you to use an alternative location, but that location must contain the matched Agent version.

c. Click **Continue**. The JDK Installation Options page displays.

- Leave **Install Oracle Java SE Development Kit (JDK)** checked to allow Cloudera Manager to install the JDK on each cluster host, or uncheck if you plan to install it yourself.
- If local laws permit you to deploy unlimited strength encryption, and you are running a secure cluster, check the Install Java Unlimited Strength Encryption Policy Files checkbox.

Click **Continue**.

d. Specify credentials and initiate Agent installation:

- Select **root** or enter the username for an account that has password-less sudo permission.
- Select an authentication method:
  - If you choose password authentication, enter and confirm the password.
  - If you choose public-key authentication, provide a passphrase and path to the required key files.
- You can specify an alternate SSH port. The default value is 22.
- You can specify the maximum number of host installations to run at once. The default value is 10.

e. Click Continue. The Cloudera Manager Agent packages and optionally the JDK are installed.

f. Click **Continue**. The Host Inspector runs to inspect your managed hosts for correct versions and configurations. If there are problems, you can make changes and then rerun the inspector. When you are satisfied with the inspection results, click **Continue**.

- **Manually install Agent software**

a. On all cluster hosts except the Cloudera Manager Server host, stop the Agent:

```
$ sudo service cloudera-scm-agent stop
```

b. In the Cloudera Admin Console, select **No, I would like to skip the agent upgrade now** and click **Continue**.

c. Copy the appropriate repo file as described in **Upgrade Cloudera Manager Server (Packages) (cm_ag_upgrade_cm5.html#concept_qjq_cxz_zn)**.

d. Run the following commands:

Operating System	Commands

RHEL	`$ sudo yum clean all`
	`$ sudo yum upgrade cloudera-manager-server cloudera-manager-daer`
	
	Note:
	▪ `yum clean all` cleans `yum` cache directories, ensuring that you download a
	▪ If your system is not up to date, any underlying system components must be components must be upgraded.

Operating System	Commands

SLES	`$ sudo zypper clean --all`
	`$ sudo zypper up -r https://archive.cloudera.com/cm5/sles/11/x8`
	
	To download from your own repository:
	
	`$ sudo zypper clean --all`
	`$ sudo zypper rr cm`
	`$ sudo zypper ar -t rpm-md http://myhost.example.com/path_to_cm_`
	`$ sudo zypper up -r http://myhost.example.com/path_to_cm_repo`

Ubuntu or Debian	Use the following commands to clean cached repository information and updat
	
	`$ sudo apt-get clean`
	`$ sudo apt-get update`
	`$ sudo apt-get dist-upgrade`
	`$ sudo apt-get install cloudera-manager-agent cloudera-manager-d`
	
	During this process, you may be prompted about your configuration file version
	
	`Configuration file '/etc/cloudera-scm-agent/config.ini'`
	`==> Modified (by you or by a script) since installation.`
	`==> Package distributor has shipped an updated version.`
	`What would you like to do about it ? Your options are:`
	`Y or I : install the package maintainer's version`
	`N or O : keep your currently-installed version`
	`D : show the differences between the versions`
	`Z : start a shell to examine the situation`
	`The default action is to keep your current version.`
	
	You will receive a similar prompt for `/etc/cloudera-scm-server/db.proper`

e. If you customized `/etc/cloudera-scm-agent/config.ini`, your customized file is moved to a file with the extension `.rpmsave` or `.dpkg-old`. Merge any customizations into `/etc/cloudera-scm-agent/config.ini` installed by the package manager.

f. On all cluster hosts, start the Agent:

```
$ sudo service cloudera-scm-agent start
```

g. Click **Continue**. The Host Inspector runs to inspect your managed hosts for correct versions and configurations. If there are problems, you can make changes and then rerun the inspector. When you are satisfied with the inspection results, click **Continue**.

3. Click Finish.

4. If you are upgrading from Cloudera Manager 5.0 and are using an external database for Cloudera Navigator, the Database Setup page displays. Configure database settings:

   a. Enter the database host, database type, database name, username, and password for the database that you created when you set up the database.

   b. Click **Test Connection** to confirm that Cloudera Manager can communicate with the database using the information you have supplied. If the test succeeds in all cases, click **Continue**; otherwise check and correct the information you have provided for the database and then try the

test again. (For some servers, if you are using the embedded database, you will see a message saying the database will be created at a later step in the installation process.)

5. The Review Changes page displays. Review the configuration changes to be applied and click **Continue**. The Upgrade wizard displays a dialog box allowing you to choose whether to restart the Cloudera Management Service.
6. Click **Continue**. If you kept the default selection, the Upgrade wizard restarts the Cloudera Management Service.
7. Click **Finish**. The Home > Status tab displays.

All services (except for the services you stopped in **Stop Selected Services and Roles (cm_ag_upgrade_cm5.html#cmig_topic_9_4_2)**) should be running.

Restart Cloudera Manager Agents (Tarballs) (#concept_xr3_2bm_2r)

Stop Cloudera Manager Agents (Tarballs) (#id_src_kbm_2r)

- To stop the Cloudera Manager Agent, run this command on each Agent host:

  ```
  $ sudo tarball_root/etc/init.d/cloudera-scm-agent stop
  ```

- If you are running **single user mode (install_singleuser_reqts.html#xd_583c10bfdbd326ba--69adf108-1492ec0ce48--7ade)** , stop Cloudera Manager Agent using the user account you chose. For example, if you are running the Cloudera Manager Agent as `cloudera-scm`, you have the following options:
  - Run the following command:

    ```
    $ sudo -u cloudera-scm tarball_root/etc/init.d/cloudera-scm-agent stop
    ```

  - Edit the configuration files so the script internally changes the user, and then run the script as root:
    1. Remove the following line from *tarball_root*`/etc/default/cloudera-scm-agent`:

       ```
       export CMF_SUDO_CMD=" "
       ```

    2. Change the user and group in *tarball_root*`/etc/init.d/cloudera-scm-agent` to the user you want the Agent to run as. For example, to run as `cloudera-scm`, change the user and group as follows:

       ```
       USER=cloudera-scm
       GROUP=cloudera-scm
       ```

    3. Run the Agent script as root:

       ```
       $ sudo tarball_root/etc/init.d/cloudera-scm-agent stop
       ```

Start Cloudera Manager Agents (Tarballs) (#id_x3r_kbm_2r)

Start the Cloudera Manager Agent according to the account you want the Agent to run under:

- To start the Cloudera Manager Agent, run this command on each Agent host:

  ```
  $ sudo tarball_root/etc/init.d/cloudera-scm-agent start
  ```

  When the Agent starts, it contacts the Cloudera Manager Server.

- If you are running **single user mode (install_singleuser_reqts.html#xd_583c10bfdbd326ba--69adf108-1492ec0ce48-**

-7ade) , start Cloudera Manager Agent using the user account you chose. For example, to run the Cloudera Manager Agent as `cloudera-scm`, you have the following options:

- Run the following command:

  ```
  $ sudo -u cloudera-scm tarball_root/etc/init.d/cloudera-scm-agent start
  ```

- Edit the configuration files so the script internally changes the user, and then run the script as root:

  1. Remove the following line from *tarball_root*`/etc/default/cloudera-scm-agent`:

     ```
     export CMF_SUDO_CMD=" "
     ```

  2. Change the user and group in *tarball_root*`/etc/init.d/cloudera-scm-agent` to the user you want the Agent to run as. For example, to run as `cloudera-scm`, change the user and group as follows:

     ```
     USER=cloudera-scm
     GROUP=cloudera-scm
     ```

  3. Run the Agent script as root:

     ```
     $ sudo tarball_root/etc/init.d/cloudera-scm-agent start
     ```

- To start the Cloudera Manager Agents automatically after a reboot:
  1. Run the following commands on each Agent host:
     - **RHEL-compatible and SLES**

       ```
       $ cp tarball_root/etc/init.d/cloudera-scm-agent /etc/init.d/cloudera-scm-agent
       $ chkconfig cloudera-scm-agent on
       ```

     - **Debian/Ubuntu**

       ```
       $ cp tarball_root/etc/init.d/cloudera-scm-agent /etc/init.d/cloudera-scm-agent
       $ update-rc.d cloudera-scm-agent defaults
       ```

  2. On each Agent, open the *tarball_root*`/etc/init.d/cloudera-scm-agent` file and change the value of `CMF_DEFAULTS` from `${CMF_DEFAULTS:-/etc/default}` to *tarball_root*`/etc/default`.

Verify the Upgrade Succeeded (#id_x5b_g14_25)

If the commands to update and start the Cloudera Manager Server complete without errors, you can assume the upgrade has completed successfully. To verify, you can check that the server versions have been updated.

1. In the Cloudera Manager Admin Console, click the **Hosts** tab.
2. Click **Host Inspector**. On large clusters, the host inspector may take some time to finish running. You must wait for the process to complete before proceeding to the next step.
3. Click **Show Inspector Results**. All results from the host inspector process are displayed, including the currently installed versions. If this includes listings of current component versions, the installation completed as expected.

(Optional) Configure TLS/SSL for Cloudera Management Service (#id_ywk_md1_yp)

If you have enabled TLS security for the Cloudera Manager Admin Console, as of Cloudera Manager 5.1, Cloudera Management Service roles try to communicate with Cloudera Manager using TLS, and

fail to start until TLS/SSL properties have been configured. Configure Cloudera Management Service roles to communicate with Cloudera Manager over TLS/SSL as follows:

1. Do one of the following:
   - Select Clusters > Cloudera Management Service > Cloudera Management Service.
   - On the Status tab of the Home > Status tab, in Cloudera Management Service table, click the **Cloudera Management Service** link.
2. Click the Configuration tab.
3. Select Scope > Cloudera Management Service (Service-Wide).
4. Select Category > Security.
5. Edit the following TLS/SSL properties according to your cluster configuration.

Property	Description
TLS/SSL Client Truststore File Location	Path to the client truststore file used in HTTPS communication. The contents of this truststore can be modified without restarting the Cloudera Management Service roles. By default, changes to its contents are picked up within ten seconds.
TLS/SSL Client Truststore File Password	Password for the client truststore file.

6. Click Save Changes to commit the changes.
7. Restart the Cloudera Management Service.

For more information, see **HTTPS Communication in Cloudera Manager (cm_sg_roles_interact_ssl.html#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--779b)** .

Deploy JDK Upgrade (#concept_dsp_ppb_dq)

If you upgraded the JDK when installing the Cloudera Manager Agents, do the following:

1. If the Cloudera Manager Server host is also running a Cloudera Manager Agent, restart the Cloudera Manager Server:

   ```
   $ sudo service cloudera-scm-server restart
   ```

   If the Cloudera Manager Server does not start, see **Troubleshooting Installation and Upgrade Problems (cm_ig_troubleshooting.html#cmig_topic_19)** .

2. Restart all services:
   a. From the Home > Status tab click  next to the cluster name and select **Restart**.
   b. In the confirmation dialog box that displays, click **Restart**.

Disable Kafka Monitoring (#concept_m43_4fx_pr)

If you have a Kafka 1.2 service, disable Kafka monitoring:

1. Go to the Kafka service.
2. Click the Configuration tab.

3. Type `enable` in the Search box.
4. Deselect the Enable Kafka monitoring checkbox.
5. Click Save Changes to commit the changes.

Start Selected Services and Roles (#cmig_topic_9_4_8)

Start the services and roles you shut down in **Stop Selected Services and Roles (cm_ag_upgrade_cm5.html#cmig_topic_9_4_2)** that have not be started in other steps:

1. If you do not plan on upgrading CDH, do the following:
   a. If you are running Cloudera Navigator, start the following roles of audited services whose service's Queue Policy configuration (`navigator.batch.queue_policy`) is set to SHUTDOWN:
      - **HDFS** - NameNode
      - **HBase** - Master and RegionServers
      - **Hive** - HiveServer2
      - **Hue** - Beeswax Server
   b. From the Home > Status tab click  next to the name of each service you shut down and select **Start**.
   c. In the confirmation dialog box that displays, click **Start**.
2. From the Home > Status tab click  next to the Cloudera Management Service and select **Start**.
3. In the confirmation dialog box that displays, click **Start**.

(Optional) Restart Services and Deploy Updated Client Configurations (#cmig_topic_9_4_9)

When upgrading Cloudera Manager, even across maintenance releases, sometimes Cloudera Manager reports **stale configurations (cm_mc_stale_configuration.html#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--7e53)** after the upgrade. This can be due to a fix that requires configuring CDH services differently.

You do not need to restart services and redeploy client configurations immediately, but if you do not plan to upgrade CDH, you should plan to apply the configuration change in the near future.

You restart services and update the client configurations as follows:

1. On the Home > Status tab, click  next to the cluster name and select **Restart**.
2. In the confirmation dialog box, click **Restart**.
3. On the Home > Status tab, click  next to the cluster name and select **Deploy Client Configuration**.
4. In the confirmation dialog box, click **Deploy Client Configuration**.

Test the Installation (#id_rtk_tg2_zn)

When you have finished the upgrade to Cloudera Manager, you can test the installation to verify that the monitoring features are working as expected; follow the instructions in **Testing the Installation (cm_ig_testing_the_install.html#xd_583c10bfdbd326ba-204beb9-13ef1573a9e--7fbd)** .

(Optional) Upgrade CDH (#cmig_topic_9_4_10)

Cloudera Manager 5 can manage both CDH 4 and CDH 5, so upgrading existing CDH 4 and 5 installations is not required, but you may want to upgrade to the latest version. For more information on upgrading CDH, see **Upgrading CDH and Managed Services Using Cloudera Manager (cm_mc_upgrading_cdh.html#cmig_topic_10)** .

Categories: Agents (../categories/hub_agents.html) | Cloudera Manager (../categories/hub_cloudera_manager.html) | Deploying (../categories/hub_deploying.html) | Installing (../categories/hub_installing.html) | Java (../categories/hub_java.html) | Kafka (../categories/hub_kafka.html) | Packages (../categories/hub_packages.html) | Planning (../categories/hub_planning.html) | Starting and Stopping (../categories/hub_starting_and_stopping.html) | Tarballs (../categories/hub_tarballs.html) | Troubleshooting (../categories/hub_troubleshooting.html) | Upgrading (../categories/hub_upgrading.html) | All Categories (../categories/hub.html)

Page generated April 11, 2017.