Cloudera Flow Management 2.1.1

Upgrading Cloudera Flow Management

Date published: 2019-06-26
Date modified: 2021-04-28

CLOUDERA

https://docs.cloudera.com/

Legal Notice

Contents

Before you upgrade

Before beginning your CFM upgrade, it is crucial that you review the migration and upgrade options, upgrade paths, and your CDP Private Cloud Base cluster requirements to ensure that you understand the pre-requisites.

CFM migration and upgrade options

You have two options for moving to CFM 2.1.1.

- Upgrade refers to a full in-place upgrade of CFM to CDP Private Cloud Base.
- Data migration refers to moving existing HDF cluster workloads to a new installation of CDP Private Cloud Base. For migration information see the *Migration Guide.*

Note:

Review the *Upgrade Paths* document for detailed information on the upgrade and migration options appropriate for your use case.

Upgrade paths

You can upgrade to CFM 2.1.1 from the following previous version:

- CFM 2.0.4
- CFM 1.1.0

Note:

You can upgrade CFM 1.1.0 running on CDH 5.x to CFM 2.1.1 on CDP 7.1.6.

Supported CDP Private Cloud Base cluster versions

CFM 2.1.1 runs on the following CDP Private Cloud Base cluster versions:

- 7.1.6
- 7.1.7
- 7.1.7 SP1
- 7.1.7 SP2

Important:

You cannot run CFM 2.1.1 on CDH 5.x or 6.x clusters. To upgrade your underlying cluster, see the CDP upgrade documentation appropriate for your use case.

- *Getting Started with CDP Upgrade and Migration*
- *In-Place Upgrade of CDH to CDP Private Cloud Base*
- *In-Place Upgrade of CDP Private Cloud Base*

Related Information

Upgrade Paths
Migration Guide
Getting Started with CDP Upgrade and Migration
In-Place Upgrade from CDH to CDP Private Cloud Base
In-Place Upgrade of CDP Private Cloud Base

Upgrading to CFM 2.1.1 from CFM 2.0.x

To upgrade to CFM 2.1.1 from earlier version of CFM on CDP Private Cloud Base, you must stop the CFM services, update the CSD files, restart the SCM Server, activate the new CFM parcel, and then restart your CFM services.

Before you begin

- You have upgrade Cloudera Manager and CDP Private Cloud Base if needed.

  Important:

  CFM 2.1.1 requires CDP Private Cloud Base 7.1.6.
- You have reviewed *Upgrade Paths* to be sure you are performing the right upgrade for your use case.
- You have reviewed the following information in *Before you upgrade* are sure that you have met the pre-requites.
  - CFM migration and upgrade options
  - Upgrade paths
  - Supported CDP Private Cloud Base cluster versions

Procedure

1. Stop the NiFi and NiFi Registry services, in this order.
2. Delete the old CSD files.
3. Download the new CSD files.

   The default CSD location is /opt/cloudera/csd, but you can configure that location from Cloudera Manager Administration | Settings | Local Descriptor Repository Path.

   Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.
4. Download the new CFM parcel and .sha checksums file appropriate for your operating system.

   The default parcel location is /opt/cloudera/parcel-repo/.

   Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.
5. Restart the cloudera-scm-server service:

   ```
   service cloudera-scm-server restart
   ```
6. In Cloudera Manager, from the **Parcels** page, distribute and activate the CFM 2.1.1 parcel.

   After clicking Activate, the Activate CFM <version> on <cluster-name> pop-up displays. Click Activate Only, and then OK.
7. Restart NiFi and NiFi Registry and deploy the client configurations.
8. Optionally, to clean up, remove the previous parcels from the host.
   a) From the Parcel menu, go to the older CFM parcel.
   b) Select Remove From Host.
   c) Select Delete.

Related Information

Upgrade Paths
Before you upgrade

Upgrading to CFM 2.1.1 from CFM 1.1.0

You must perform the following steps to upgrade to CFM 2.1.1 from CFM 1.1.0.

Note:

You can upgrade from CFM 1.1.0 running on CDH 5.x. Upgrades from CFM 1.1.0 running on CDH 6.x are not currently possible.

Turn off TLS regeneration

The NiFi CA is not installed as part of CFM 2.0.x. You must turn off NiFi CFM upgrade edits CA Force Regenerate before proceeding with your upgrade.

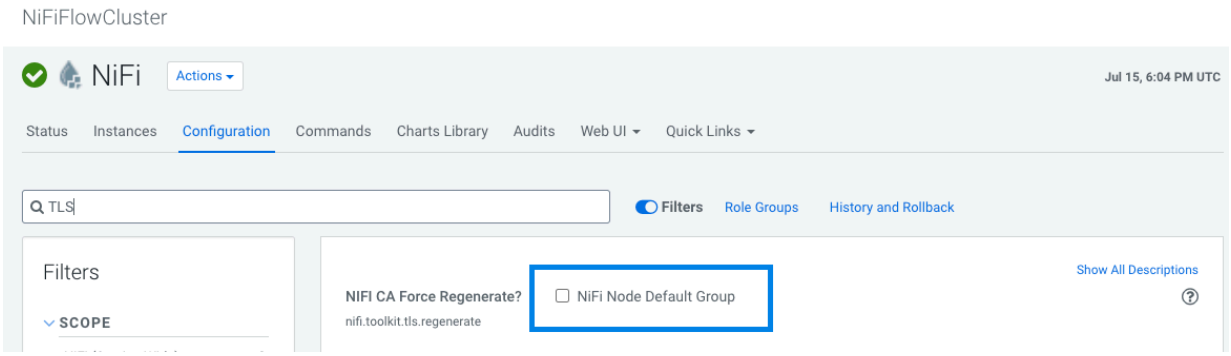
Before you begin

You have reviewed the following *Before you upgrade* information and are sure that you are performing the right upgrade for your use case.

- CFM migration and upgrade options
- Upgrade paths
- Supported CDP Private Cloud Base cluster versions

Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi in the list of services to display the NiFi service page.
3. Select the Configuration tab.
4. Deselect the TLS regeneration check-box.



5. Repeat these steps for NiFi Registry.

What to do next

Once you have turned off TLS regeneration, backup your keystore and truststore values for NiFi and NiFi Registry, and then proceed with the upgrade to CFM 2.0.x.

Once you have completed the upgrade, Cloudera recommends that you use Auto-TLS for your CDP Private Cloud Base cluster.

Back up NiFi keystore and truststore settings

If your CFM installation from which you are upgrading is TLS enabled, use the Encrypt Config tools to backup your NiFi keystore and truststore settings. You will set these values in Cloudera Manager once you complete the upgrade.

Before you begin

- You have turned of TLS regeneration.
- If JAVA_HOME is not set, you should set it before proceeding. The default path is /usr/java/default.

Procedure

1. Locate the `encrypt-config.sh` script from the NiFi Toolkit.

   The default location is /opt/cloudera/parcels. You can find your location by running:

   ```
   find /opt/cloudera/parcels -name 'encrypt-config.sh'
   ```

   Note:

   If you have installed more than one CFM parcel, you may have more than one script. In this case, ensure that you have the script from CFM 1.1.0.

2. Find the latest NiFi process directory:

   ```
   find /var/run/cloudera-scm-agent/process/ -name nifi.properties | grep
   "NIFI_NODE"
   ```

3. Run `encrypt-config.sh`:

   ```
   <path_to_encrypt-config.sh>
   -c
   -b <path_to_nifi_proc_dir>/bootstrap.conf
   -n <path_to_nifi_proc_dir>/nifi.properties
   ```

   For example:

   ```
   /opt/cloudera/parcels/CFM-1.1.0.0/encrypt-config.sh
   -c
   -b /run/cloudera-scm-agent/182-NIFI_NODE.../bootstrap.conf
   -n /run/cloudera-scm-agent/182-NIFI_NODE.../nifi.properties
   ```

4. Back up the `encrypt-config.sh` output.

Results

The `encrypt-config.sh` output will be similar to:

```
keystore=/var/lib/nifi/cert/keystore.jks
keystorePasswd=/TLVwnnFESyIwn2YrBGiVWrANNhiSk
keyPasswd=/TLVwnnFESyIwn2YrBGiVWrANNhiSk
truststore=/var/lib/nifi/cert/truststore.jks
truststorePasswd=4wIWsNhpkVa5MR8P353s3ruMDGj1UL
```

What to do next

Once you have completed this step for NiFi, do the same for NiFi Registry.

Back up NiFi Registry keystore and truststore settings

If your CFM installation from which you are upgrading is TLS enabled, use the Encrypt Config tools to backup your NiFi Registry keystore and truststore settings. You will set these values in Cloudera Manager once you complete the upgrade.

Before you begin

If JAVA_HOME is not set, you should set it before proceeding. The default path is /usr/java/default.

Procedure

1. Locate the `encrypt-config.sh` script from the NiFi Toolkit.
   The default location is /opt/cloudera/parcels. You can find your location by running:

   ```
   find /opt/cloudera/parcels -name 'encrypt-config.sh'
   ```

   Note:
   If you have installed more than one CFM parcel, you may have more than one script. In this case, ensure that you have the script from CFM 1.1.0.
2. Find the latest NiFi Registry process directory:

   ```
   find /var/run/cloudera-scm-agent/process/ -name nifi-registry.properties
    | grep "NIFI_NODE"
   ```
3. Run `encrypt-config.sh`:

   ```
   ${ENCRYPT_CONFIG_PATH}
   --nifiRegistry
   --decrypt
   -r ${NIFIREG_PROC_DIR}/nifi-registry.properties
   -b ${NIFIREG_PROC_DIR}/bootstrap.conf
   ```
4. Back up the `encrypt-config.sh` output.

Results

The `encrypt-config.sh` output will be similar to:

```
nifi.registry.security.keystore=/var/lib/nifiregistry/cert/keystore.jks
nifi.registry.security.keystorePasswd=5BNrrLRmcrsGi+qq1BNpEpoIzyOALo
nifi.registry.security.truststore=/var/lib/nifiregistry/cert/truststore.jks
nifi.registry.security.truststorePasswd=qKdbQ9Q0a0uX/XApHhLjR4d2zxRHQ3
```

Note:
nifi.registry.security.keystorePasswd is the same as keyPassword.

What to do next

Once you have completed this step for NiFi Registry, you may proceed with the upgrade to CFM 2.0.x.

Upgrading to CFM 2.0.x

To upgrade from CFM 1.1.0 to CFM 2.1.1, you must stop the CFM services, update the CSD files, restart the SCM Server, and activate the new CFM parcel.

About this task

If you must upgrade from CFM version 1.0.x, you should first upgrade to CFM 1.1.0. See the *Upgrade documentation* for CFM 1.1.0 for more information.

Before you begin

Before you begin the CFM upgrade, ensure that you have completed the steps to:

- Turn off TLS regeneration.
- Back up your keystore and truststore settings for NiFi and NiFi Registry.

Procedure

1. Stop NiFi, NiFi Registry, and NiFi CA Service in this order.
2. Delete the old CSD files.
3. Download the new CSD files.

   The default CSD location is /opt/cloudera/csd, but you can configure that location from Cloudera Manager Administration | Settings | Local Descriptor Repository Path.

   Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.
4. Download the new CFM parcel and .sha checksum file appropriate for your operating system.

   The default parcel location is /opt/cloudera/parcel-repo/.

   Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.
5. Restart the cloudera-scm-server service:

   ```
   service cloudera-scm-server restart
   ```
6. In Cloudera Manager, from the **Parcels** page, distribute and activate the CFM parcel to which you want to upgrade.

   After clicking Activate, the Activate CFM <version-number> on <cluster-name> pop-up displays. Click Activate Only, and then OK.
7. Optionally, to clean up, remove the older parcels from the host.
   a) From the Parcel menu, go to the older CFM parcel.
   b) Select Remove From Host.
   c) Select Delete.

   Important:

   Do not start the NiFi and NiFi Registry services yet. Complete the post-upgrade steps before you start any services.

What to do next

Once you have completed the upgrade, perform the following additional tasks:

- Set the keystore and truststore settings with the values from your backup.
- Turn off identity mapping for both NiFi and NiFi Registry.
- Start the NiFi and NiFi Registry.

  Note:

  Do not start the NiFi CA service, as this is no longer supported as part of CFM 2.1.1.
- Optionally, you can remove the NiFi CA service.

Related Information

Upgrading CFM 1.0.1

Restore NiFi keystore and truststore settings

Learn how to restore your NiFi keystore and truststore settings from the backup you made prior to upgrade.

Before you begin

- You have completed your upgrade to CFM 2.0.x.

- You have the NiFi keystore and truststore settings that you backed up before beginning your upgrade.

Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi in the list of services to display the NiFi service page.
3. Select the Configuration tab.
4. Use the search bar to find the Keystore configuration options and update the following three with the values from your backup.

   Note:

   The `nifi.security.keystorePasswd` value should be the same as the `keyPassword` value.

5. Use the search bar to find the Truststore configuration options and update the following two with the values from your backup.

What to do next

Once you have completed this step for the NiFi service, do the same for NiFi Registry.

Restore your NiFi Registry keystore and truststore settings

Learn how to restore your NiFi Registry keystore and truststore settings from the backup you made prior to upgrade.

Before you begin

- You have completed your upgrade to CFM 2.0.x.
- You have the NiFi Registry keystore and truststore settings that you backed up before beginning your upgrade.

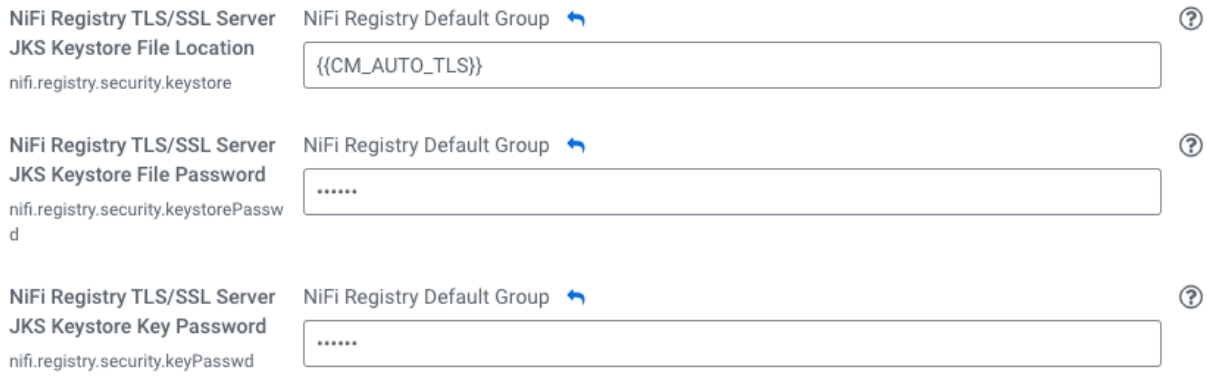
Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi Registry in the list of services to display the NiFi Registry service page.

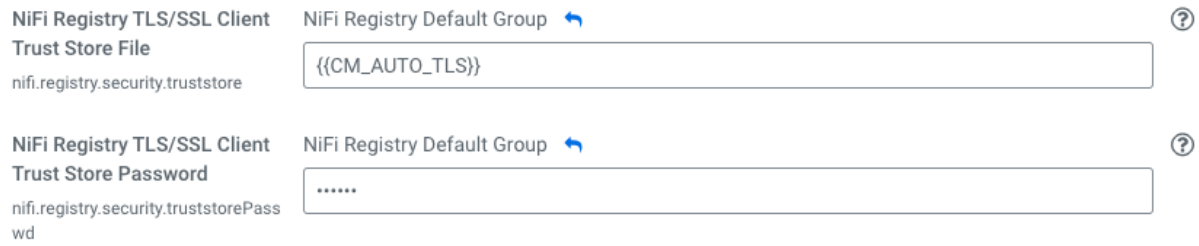
3. Select the Configuration tab.
4. Use the search bar to find the Keystore configuration options and update the following three with the values from your backup.

   Note:

   The `nifi.registry.security.keystorePasswd` value should be the same as the `keyPassword` value.



5. Use the search bar to find the Truststore configuration options and update the following two with the values from your backup.



What to do next

Once you have restored NiFi and NiFi Registry keystore and truststore settings, turn off identity mapping.

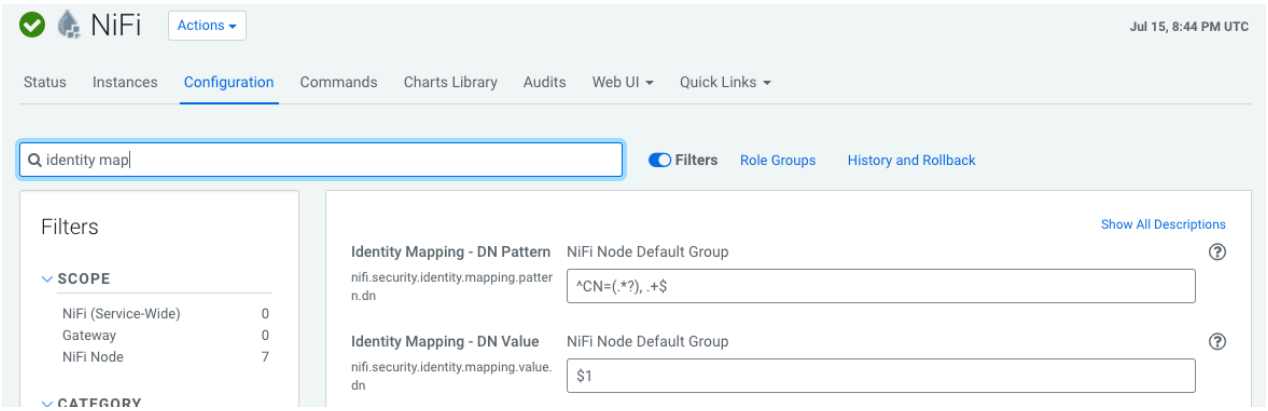
Turn off identity mapping

Describes the steps to turn off identity mapping.

Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi in the list of services to display the NiFi service page.
3. Select the Configuration tab.
4. Use the search bar to find the Identity Mapping configuration options and remove the values for the following parameters:
   - Identity Mapping - DN Pattern (`nifi.security.identity.mapping.pattern.dn`)
   - Identity Mapping - DN Value (`nifi.security.identity.mapping.value.dn`)
5. Repeat these steps for NiFi Registry. The NiFi Registry Identity Mapping configuration options are:
   - Identity Mapping - DN Pattern (`nifi.registry.security.identity.mapping.pattern.dn`)
   - Identity Mapping - DN Value (`nifi.registry.security.identity.mapping.value.dn`)

Example



What to do next

Once you have turned off identity mapping, review the additional post-upgrade steps for any additional requirements that pertain to your CFM 2.0.x deployment scenario.

Additional post-upgrade steps for some upgrade scenarios

Depending on the type of CFM 1.1.0 installation you are upgrading, there are some additional post-upgrade steps you must take. You should review the following information for anything pertaining to your upgrade scenario.

Enable Auto-TLS for CFM

Provides steps to enable Auto-TLS for CFM.

About this task

You should perform these steps if you are upgrading from a CFM 1.1.0 installation where:

- TLS is enabled for CFM 1.1.0; AND
- Auto-TLS is enabled on the CDH cluster.

Procedure

1. Launch the API Explorer from the Cloudera Manager Support menu at the bottom of the left navigation pane.

2. Run the `configureAutoTlsServices` API call.

3. Edit the users.xml, to remove the users associated with the NiFi nodes.

   Repeat these steps for NiFi Registry.
4. Edit the authorizations.xml file.

   In the `/proxy` policy, remove the users corresponding to the NiFi nodes and replace them with:

   ```
   <group identifier="nifi"/>
   ```

   Repeat these steps for NiFi Registry/
5. Review the other policies related to the NiFi nodes, to similarly edit any other references to the NiFi nodes.

Related Tasks

Create a Ranger user for the Initial Admin Identity

Manually integrate with Atlas

Integrate with Atlas when Auto-TLS is enabled

Create a Ranger user for the Initial Admin Identity

In some upgrade scenarios, you must manually create a Ranger user for the Initial Admin Identity and add it to the `nifi` group.

About this task

You should perform these steps if you are upgrading from a CFM 1.1.0 installation where:

- CFM has Kerberos and TLS enabled; AND
- The CDP Private Cloud Base cluster does not have Auto-TLS enabled; AND
- You want Ranger as part of your CFM 2.0.x on CDP Private Cloud Base 7.1.x deployment.

Before you begin

Ranger is running on your CDP Private Cloud Base 7.1.x cluster.

Procedure

1. Create a Ranger user with the same user name as your NiFi Initial Admin Identity.
2. Assign this user to the Ranger group `nifi`.
3. Create a Ranger user with the same username as your NiFi Registry Initial Admin Identity.
4. Assign this user to the Ranger group `nifiregistry`.

Related Tasks

Enable Auto-TLS for CFM
Manually integrate with Atlas
Integrate with Atlas when Auto-TLS is enabled

Manually integrate with Atlas

Provides steps to manually integrate with Atlas by creating the `ReportLineageToAtlas` reporting task.

About this task

If you are upgrading from a CFM 1.1.0 installation where:

- CFM does not have TLS enabled; AND
- The CDP Private Cloud Base cluster does not have Auto-TLS enabled; AND
- You do not want to enable Auto-TLS; AND
- You want Atlas as part of CFM 2.0.x on your CDP Private Cloud Base 7.1.x deployment.

Procedure

1. Start NiFi.
   a) From Cloudera Manager, click the Clusters tab in the left-hand navigation.
   b) Click NiFi in the list of services to display the NiFi service page.
   c) Click the Actions drop-down, and then click Start.
2. From the Global Menu located in NiFi's upper right corner, select Controller Services and click the Reporting Tasks tab.
3. Click the Add (+) icon to launch the Add Reporting Task dialog.
4. Select `ReportLineageToAtlas` and click Add.
5. Click the Edit icon to launch the Configure Reporting Task dialog. The following properties are required:
   - Atlas URLs – a comma-separated list of Atlas Server URLs. Once you have started reporting, you cannot modify an existing Reporting Task to add a new Atlas Server. When you need to add a new Atlas Server, you must create a new reporting task.
   - Atlas Authentication Method – Specifies how to authenticate the Reporting Task to the Atlas Server. Basic authentication is the default.
   - NiFi URL for Atlas – Specifies the NiFi cluster URL
   - Lineage Strategy – Specifies the level of granularity for your NiFi dataflow reporting to Atlas. Once you have started reporting, you should not switch between simple and complete lineage reporting strategies.
   - Provenance Record Start Position – Specifies where in the Provenance Events stream the Reporting Task should start.
   - Provenance Record Batch Size – Specifies how many records you want to send in a single batch
   - Create Atlas Configuration File – If enabled, the atlas-application-properties file and the Atlas Configuration Directory are automatically created when the Reporting Task starts.
   - Kafka Security Protocol – Specifies the protocol used to communicate with Kafka brokers to send Atlas hook notification messages. This value should match Kafka's `security.protocol` property value.

Related Tasks

Enable Auto-TLS for CFM

Create a Ranger user for the Initial Admin Identity
Integrate with Atlas when Auto-TLS is enabled

Integrate with Atlas when Auto-TLS is enabled

Provides manual steps to integrate with Atlas when Auto-TLS is enabled on your CDP Data Center cluster.

About this task

You must perform these steps if:

- You want CFM 2.0.x to integrate with Atlas; AND
- The CDP Private Cloud Base 7.1.x cluster has Auto-TLS enabled

Procedure

1. Start NiFi.
   a) From Cloudera Manager, click the Clusters tab in the left-hand navigation.
   b) Click NiFi in the list of services to display the NiFi service page.
   c) Click the Actions drop-down, and then click Start.
2. Select the Atlas Dependency d checkbox.
3. Restart NiFi.
4. Click Create required NiFi objects from the Actions drop-down.

Related Tasks

Enable Auto-TLS for CFM
Create a Ranger user for the Initial Admin Identity
Manually integrate with Atlas

Start your NiFi and NiFi Registry services

Provides steps to start your NiFi and NiFi Registry services.

About this task

The final upgrade step is to start your NiFi and NiFi Registry services if you have not already done so.

Before you begin

You have completed all applicable post-upgrade steps. If you have not completed these steps, your services may fail to start.

Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation.
2. Click NiFi in the list of services to display the NiFi service page.
3. Click the Actions drop-down, and then click Start.
4. Repeat these steps for NiFi Registry.