Cloudera Flow Management 2.0.1

Upgrading Cloudera Flow Management

Date published: 2019-06-26
Date modified: 2020-07-17

https://docs.cloudera.com/

Legal Notice

Contents

Before you upgrade

Before you start the upgrade process, there are a few essential things to take care of. This section provides the key steps and requirements you should consider before upgrading to CFM 2.0.1.

CFM migration and upgrade options

When considering the transition to CFM 2.0.1, you have two main options:

Upgrade

It refers to a complete in-place upgrade of CFM on CDP Private Cloud Base.

Migration

This method entails moving existing HDF cluster workloads to a fresh installation of CDP Private Cloud Base. For detailed migration instructions, see the *Migration Guide*.

Upgrade paths

You can upgrade to CFM 2.0.1 from the following previous version:

- CFM 1.1.0

Upgrading your cluster

You must upgrade your cluster to CDP Private Cloud Base 7.1.1.

Important:

You cannot run CFM 2.0.1 on CDH 5.x or 6.x clusters.

Related Information

Migration Guide

Turning off TLS regeneration

Learn how to turn off forced TLS regeneration before you upgrade to CFM 2.0.1.

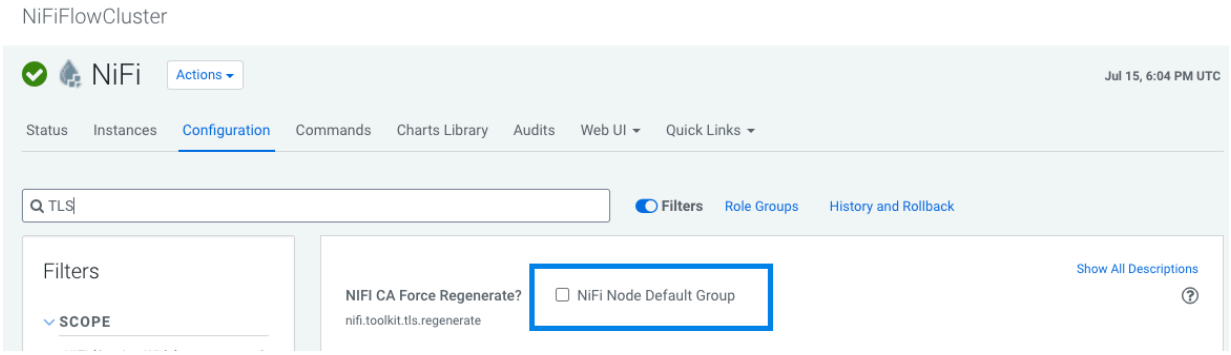
About this task

The NiFi CA is not installed as part of CFM 2.0.1. You must turn off NiFi CA Force Regenerate before proceeding with your upgrade. Once you have completed the upgrade, Cloudera recommends that you use Auto-TLS for your CDP Data Center cluster.

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.



What to do next

Once you have turned off TLS regeneration, back up your keystore and truststore values for NiFi and NiFi Registry, and then proceed with the upgrade to CFM 2.0.1.

Backing up NiFi keystore and truststore settings

If your CFM installation from which you are upgrading is TLS enabled, use the Encrypt Config tools to back up your NiFi 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 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 the backup for NiFi, repeat the same steps for NiFi Registry.

Backing 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 back up 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, proceed with the upgrade to CFM 2.0.1.

Upgrading to CFM 2.0.1

To upgrade from CFM 1.1.0 to CFM 2.0.1, you must stop the CFM services, update the CSD files, restart the SCM Server, and activate the new CFM parcel.

About this task

Cloudera recommends that you upgrade from CFM version 1.1.0 to 2.0.1

If you must upgrade from CFM version 1.0.x, you should first upgrade to CFM 1.1.0. For detailed instructions, see the *Upgrade documentation* for CFM 1.1.0.

Before you begin

Before you begin the CFM upgrade, make sure you have completed the following preparatory steps:

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

Procedure

1. Sequentially stop NiFi, NiFi Registry, and NiFi CA Service.
2. Delete the old CSD files.
3. Download the new CSD files.

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

   Note:

   Ensure that file ownership, access attributes, and SELinux permissions are correctly maintained.
4. Download the new CFM parcel and .sha checksum file appropriate for your operating system.

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

   Note:

   Ensure that file ownership, access attributes, and SELinux permissions are correctly maintained.
5. Restart the cloudera-scm-server service by running the following command:

   ```
   service cloudera-scm-server restart
   ```

6. In Cloudera Manager, navigate to the Parcels page, and distribute and activate the CFM parcel that you want to use.

   After clicking Activate, the Activate CFM 2.0.1.0 on <cluster-name> pop-up displays. Click Activate Only OK .
7. you can clean up by removing the older parcels from the host.
   a) From the Parcel menu, go to the CFM parcel you do not need.
   b) Select Delete Remove From Host .

Important:

Do not start the NiFi and NiFi Registry services at this stage. Ensure that you complete the post-upgrade steps before starting any services.

What to do next

Once the upgrade is complete, perform the following additional tasks:

- Set the keystore and truststore settings using the values from your backup.
- Disable identity mapping for both NiFi and NiFi Registry.
- Start the NiFi and NiFi Registry services.

Note:

Do not start the NiFi CA service! The NiFi CA service is no longer supported as part of CFM 2.0.1.

- Optionally, you can remove the NiFi CA service.

Related Information

Upgrading CFM 1.0.1

Restoring 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 2.0.1.
- 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 the restore action for the NiFi service, repeat the same steps for NiFi Registry.

Restoring 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 2.0.1.
- 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.

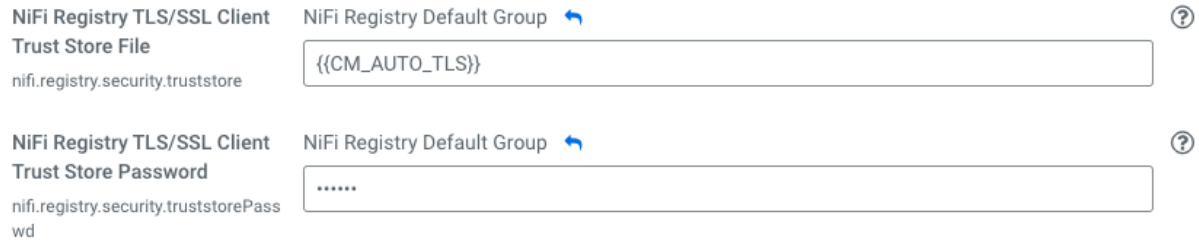
4. Use the search bar to find the Keystore configuration options and update the following three with the values from your backup.

   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, disable identity mapping.

Disabling identity mapping

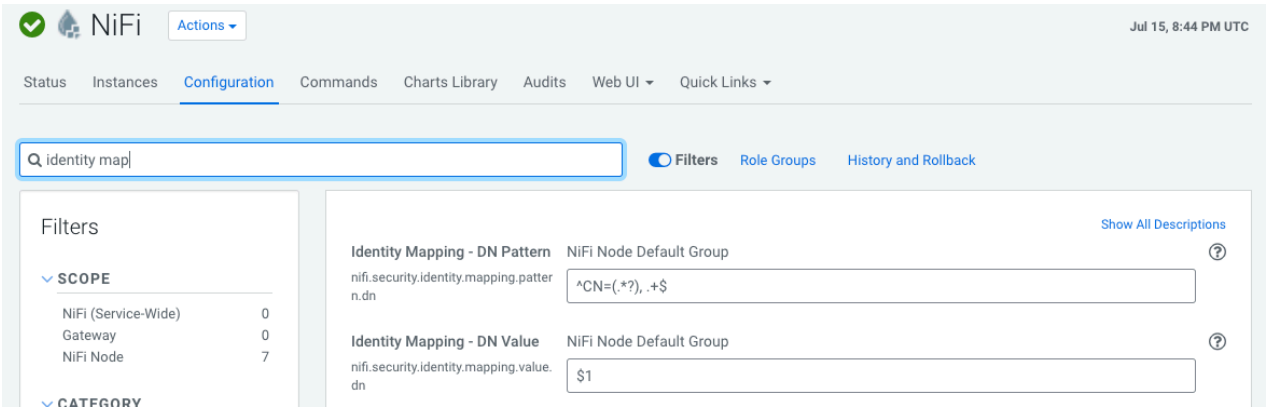
Procedure

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 2.0.1 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.
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"/>
   ```

5. Review the other policies related to the NiFi nodes, to similarly edit any other references to the NiFi nodes.

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 2.0.1 on CDP Private Cloud Base 7.1.1 deployment.

Before you begin

Ranger is running on your CDP Private Cloud Base 7.1.1 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`.

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 2.0.1 on your CDP Private Cloud Base 7.1.1 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.

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 2.0.1 to integrate with Atlas; AND
- The CDP Private Cloud Base 7.1.1 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 integration checkbox.
3. Restart NiFi.
4. Click Create required NiFi objects from the Actions drop-down.

Starting NiFi and NiFi Registry services

Learn how 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.