Cloudera Manager
Backup and Disaster Recovery
Important Notice

(c) 2010-2015 Cloudera, Inc. All rights reserved.

Cloudera, the Cloudera logo, Cloudera Impala, and any other product or service names or slogans contained in this document are trademarks of Cloudera and its suppliers or licensors, and may not be copied, imitated or used, in whole or in part, without the prior written permission of Cloudera or the applicable trademark holder.

Hadoop and the Hadoop elephant logo are trademarks of the Apache Software Foundation. All other trademarks, registered trademarks, product names and company names or logos mentioned in this document are the property of their respective owners. Reference to any products, services, processes or other information, by trade name, trademark, manufacturer, supplier or otherwise does not constitute or imply endorsement, sponsorship or recommendation thereof by us.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Cloudera.

Cloudera may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Cloudera, the furnishing of this document does not give you any license to these patents, trademarks copyrights, or other intellectual property. For information about patents covering Cloudera products, see http://tiny.cloudera.com/patents.

The information in this document is subject to change without notice. Cloudera shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.

Cloudera, Inc.
1001 Page Mill Road Bldg 2
Palo Alto, CA 94304
info@cloudera.com
US: 1-888-789-1488
Intl: 1-650-362-0488
www.cloudera.com

Release Information

Version: 5.1.x
Date: September 8, 2015
Table of Contents

**About this Guide**.........................................................................................................5

**Backup and Disaster Recovery Overview**................................................................7

**Data Replication**.........................................................................................................9
  Designating a Replication Source ......................................................................................10
  *Configuring a Peer Relationship* ......................................................................................10
  *Modifying Peers* ...............................................................................................................11
  HDFS Replication ..............................................................................................................11
    *Configuring Replication of HDFS Data* ........................................................................11
    *Viewing Replication Job Status* ..................................................................................12
  Hive Replication ..............................................................................................................13
    *Configuring Replication of Hive Data* ........................................................................13
    *Viewing Replication Job Status* ..................................................................................15
  Impala Metadata Replication ...........................................................................................15
  Enabling Replication Between Clusters in Different Kerberos Realms .........................16

**Snapshots**..................................................................................................................17
  Snapshot Policies ............................................................................................................17
  Browsing and Managing Snapshots ................................................................................19
    *Managing HBase Snapshots* .......................................................................................19
    *Managing HDFS Directory Snapshots* ......................................................................20
About this Guide

This guide describes the Cloudera Manager backup and disaster recovery (BDR) features, which provide an integrated, easy-to-use solution for enabling data protection in the Hadoop platform.

- **Important:** This feature is available only with a Cloudera Enterprise license.
  
  For other licenses, the following applies:
  - Cloudera Express - The feature is not available.
  - Cloudera Enterprise Data Hub Edition Trial - The feature is available until you end the trial or the trial license expires.

To obtain a license for Cloudera Enterprise, please fill in this [form](#) or call 866-843-7207. After you install a Cloudera Enterprise license, the feature will be available.
Backup and Disaster Recovery Overview

Cloudera Manager provides an integrated, easy-to-use management solution for enabling data protection in the Hadoop platform. Cloudera Manager provides rich functionality aimed towards replicating data stored in HDFS and accessed through Hive across data centers for disaster recovery scenarios. When critical data is stored on HDFS, Cloudera Manager provides the necessary capabilities to ensure that the data is available at all times, even in the face of the complete shutdown of a data center.

Cloudera Manager also provides the ability to schedule, save and (if needed) restore snapshots of HDFS directories and HBase tables.

Cloudera Manager provides key capabilities that are fully integrated into the Cloudera Manager Admin Console:

- **Select** - Choose the key datasets that are critical for your business operations.
- **Schedule** - Create an appropriate schedule for data replication and/or snapshots – trigger replication and snapshots as frequently as is appropriate for your business needs.
- **Monitor** - Track progress of your snapshots and replication jobs through a central console and easily identify issues or files that failed to be transferred.
- **Alert** - Issue alerts when a snapshot or replication job fails or is aborted so that the problem can be diagnosed expeditiously.

Replication capabilities work seamlessly across Hive and HDFS – replication can be setup on files or directories in the case of HDFS and on tables in the case of Hive—without any manual translation of Hive datasets into HDFS datasets or vice-versa. Hive metastore information is also replicated which means that the applications that depend upon the table definitions stored in Hive will work correctly on the replica side as well as the source side as table definitions are updated.

Built on top of a hardened version of `distcp`—the replication uses the scalability and availability of MapReduce and YARN to parallelize the copying of files using a specialized MapReduce job or YARN application that diffs and transfers only changed files from each Mapper to the replica side efficiently and quickly.

Also available is the ability to do a “Dry Run” to verify configuration and understand the cost of the overall operation before actually copying the entire dataset.

**Port Requirements**

You must ensure that the following ports are open and accessible across clusters to allow communication between the source and destination Cloudera Manager servers and the HDFS, Hive, MapReduce, and YARN hosts:

- **Cloudera Manager Admin Console port**: Default is 7180.
- **HDFS NameNode port**: Default is 8020.
- **HDFS DataNode port**: Default is 50010.
- **WebHDFS port**: Default is 50070.

See [Configuring Ports for Cloudera Manager](#) for more information, including how to verify the current values for these ports.
Data Replication

Cloudera Manager provides rich functionality for replicating data (stored in HDFS or accessed through Hive) across data centers. When critical data is stored on HDFS, Cloudera Manager provides the necessary capabilities to ensure that the data is available at all times, even in the face of the complete shutdown of a data center.

For recommendations on using data replication and Sentry authorization, see Configuring Sentry to Enable BDR Replication.

In Cloudera Manager 5, replication is supported between CDH 5 or CDH 4 clusters. In Cloudera Manager 5, support for HDFS and Hive replication is as follows.

**Important:** To use HDFS replication, both the target and source HDFS services must use Kerberos authentication, or both the target and source HDFS services must not use Kerberos authentication.

**Supported Replication Scenarios**

- **HDFS and Hive**
  - Cloudera Manager 4 with CDH 4 to Cloudera Manager 5 with CDH 4
  - Cloudera Manager 5 with CDH 4 to Cloudera Manager 4.7.3 or later with CDH 4
  - Cloudera Manager 5 with CDH 4 to Cloudera Manager 5 with CDH 4
  - Cloudera Manager 5 with CDH 5 to Cloudera Manager 5 with CDH 5
  - Cloudera Manager 4 or 5 with CDH 4.4 or later to Cloudera Manager 5 with CDH 5
  - Cloudera Manager 5 with CDH 5 to Cloudera Manager 5 with CDH 4.4 or later.

- **SSL**
  - Between CDH 5.0 with SSL and CDH 5.0 with SSL.
  - Between CDH 5.0 with SSL and CDH 5.0 without SSL.
  - From a CDH 5.1 source cluster with SSL and YARN.

**Unsupported Replication Scenarios**

- **HDFS and Hive**
  - Cloudera Manager 5 with CDH 5 as the source, and Cloudera Manager 4 with CDH 4 as the target.
  - Between Cloudera Enterprise and any Cloudera Manager free edition: Cloudera Express, Cloudera Standard, Cloudera Manager Free Edition.
  - Between CDH 5 and CDH 4 (in either direction) where the replicated data includes a directory that contains a large number of files or subdirectories (several hundreds of thousands of entries), causing out-of-memory errors. This is because of limitations in the WebHDFS API. The workaround is to increase the heap size as follows:
    1. On the target Cloudera Manager instance, go to the HDFS service page.
    2. Click the Configuration tab.
    3. Expand the Service-Wide category.
    4. Click Advanced > HDFS Replication Advanced Configuration Snippet.
    5. Increase the heap size by adding a key-value pair, for instance, HADOOP_CLIENT_OPTS=-Xmx1g. In this example, 1g sets the heap size to 1 GB. This value should be adjusted depending on the number of files and directories being replicated.
  - Replication involving HDFS data from CDH 5 HA to CDH 4 clusters or CDH 4 HA to CDH5 clusters will fail if a NameNode failover happens during replication. This is because of limitations in the CDH WebHDFS API.
Data Replication

- **HDFS**
  - Between a source cluster that has encryption enabled and a target cluster running CDH 4.0. This is because the CDH 4 client is used for replication in this case, and it does not support encryption.
  - From CDH 5 to CDH 4 where there are URL-encoding characters such as % in file and directory names. This is because of a bug in the CDH 4 WebHDFS API.
  - HDFS replication does not work from CDH 5 to CDH 4 with different realms when using older JDK versions. This is because of a JDK SPNEGO issue. For more information, see [JDK-6670362](#). Use JDK 7 or upgrade to JDK6u34 or later on the CDH 4 cluster to work around this issue.

- **Hive**
  - *With* data replication, between a *source* cluster that has encryption enabled and a *target* cluster running CDH 4. This is because the CDH 4 client used for replication does not support encryption.
  - *Without* data replication, between a *source* cluster running CDH 4 and a *target* cluster that has encryption enabled.
  - Between CDH 4.2 or later and CDH 4, if the Hive schema contains views.
  - With the same cluster as both source and destination
  - Replication from CDH 4 to CDH 5 HA can fail if a NameNode failover happens during replication.
  - Hive replication from CDH 5 to CDH 4 with different realms with older JDK versions, if data replication is enabled (since this involves HDFS replication). This is because of a JDK SPNEGO issue. For more information, see [JDK-6670362](#). Use JDK 7 or upgrade to JDK6u34 or later on the CDH 4 cluster to work around this issue.
  - Hive replication from CDH 4 to CDH 5 with different realms with older JDK versions (even without data replication enabled). This is because of a JDK SPNEGO issue. For more information, see [JDK-6670362](#). Use JDK 7 or upgrade to JDK6u34 or later on the CDH 4 cluster to work around this issue.

- **SSL**
  - From a CDH 4.x source cluster with SSL.
  - From CDH 5.0 source cluster with SSL and YARN (because of a YARN bug).
  - Between CDH 5.0 with SSL and CDH 4.x.

- **Kerberos**
  - From a source cluster configured to use Kerberos authentication to a target cluster that is not configured to use Kerberos authentication.
  - From a source cluster not configured to use Kerberos authentication to a target cluster that is configured to use Kerberos authentication.

Designating a Replication Source

**Required Role:** Administrator

The Cloudera Manager Server that you are logged in to will be treated as the destination of replications setup via that Cloudera Manager. From the Admin Console of this destination Cloudera Manager, you can designate a peer Cloudera Manager Server which will be treated as a source of HDFS and Hive data for replication.

Configuring a Peer Relationship

1. Navigate to the Peers page by selecting Administration > Peers. The Peers page displays. If there are no existing peers, you will see only an Add Peer button in addition to a short message. If you have existing peers, they are listed in the Peers list.
2. Click the Add Peer button.
3. In the Add Peer pop-up, provide a name, the URL (including the port) of the Cloudera Manager Server that will act as the source for the data to be replicated, and the login credentials for that server. Cloudera recommends that SSL be used and a warning is shown if the URL scheme is http instead of https.

4. Click the Add Peer button in the pop-up to create the peer relationship. The peer is added to the Peers list.

5. To test the connectivity between your Cloudera Manager Server and the peer, select Actions > Test Connectivity.

Modifying Peers

1. Navigate to the Peers page by selecting Administration > Peers. The Peers page displays. If there are no existing peers, you will see only an Add Peer button in addition to a short message. If you have existing peers, they are listed in the Peers list.

2. Choose an action and follow the procedure:
   - **Edit**
     1. From the Actions menu for the peer, select Edit.
     2. Make your changes.
     3. Click Update Peer to save your changes.
   - **Delete** - From the Actions menu for the peer, select Delete.

HDFS Replication

**Required Role:** Administrator

HDFS replication enables you to copy (replicate) your HDFS data from one HDFS service to another, keeping the data set on the target service synchronized with the data set on the source service, based on a user-specified replication schedule. The target service needs to be managed by the Cloudera Manager Server where the replication is being set up, and the source service could either be managed by that same server or by a peer Cloudera Manager Server.

**Important:** To use HDFS replication, both the target and source HDFS services must use Kerberos authentication, or both the target and source HDFS services must not use Kerberos authentication.

Configuring Replication of HDFS Data

1. Verify that your cluster conforms to the supported replication scenarios.
2. If the source cluster is managed by a different Cloudera Manager server from the target cluster, configure a peer relationship.
3. Do one of the following:
   - From the Backup tab, select Replications.
   - From the Clusters tab, go to the HDFS service and select the Replication tab.

   The Schedules tab of the Replications page displays.
4. Click the Schedule HDFS Replication link.
5. Select the source HDFS service from the HDFS services managed by the peer Cloudera Manager Server or the HDFS services managed by the Cloudera Manager Server whose Admin Console you are logged into.
6. Enter the path to the directory (or file) you want to replicate (the source).
7. Select the target HDFS service from the HDFS services managed by the Cloudera Manager Server whose Admin Console you are logged into.
8. Enter the path where the target files should be placed.
9. Select a schedule. You can have it run immediately, run once at a scheduled time in the future, or at regularly scheduled intervals. If you select Once or Recurring you are presented with fields that let you set the date and time and (if appropriate) the interval between runs.
Data Replication

10. If you want to modify the parameters of the job, click **More Options**. Here you will be able to change the following parameters:

- **MapReduce Service** - The MapReduce or YARN service to use.
- **Scheduler Pool** - The scheduler pool to use.
- **Run as** - The user that should run the job. By default this is hdfs. If you want to run the job as a different user, you can enter that here. If you are using Kerberos, you must provide a user name here, and it must be one with an ID greater than 1000. Verify that the user running the job has a home directory, /user/<username>, owned by username:supergroup in HDFS.
- **Log path** - An alternative path for the logs.
- **Maximum map slots** and **Maximum bandwidth** - Limits for the number of map slots and for bandwidth per mapper. The defaults are unlimited.
- **Abort on error** - Whether to abort the job on an error (default is not to do so). This means that files copied up to that point will remain on the destination, but no additional files will be copied.
- **Skip Checksum Checks** - Whether to skip checksum checks (the default is to perform them). If checked, checksum validation will not be performed.
- **Remove deleted files** - Whether to remove deleted files from the target directory if they have been removed on the source. When this option is enabled, files deleted from the target directory are sent to trash if HDFS trash is enabled, or are deleted permanently if trash is not enabled. Further, with this option enabled, if files unrelated to the source exist in the target location, then those files will also be deleted.
- **Preserve** - Whether to preserve the block size, replication count, and permissions as they exist on the source file system, or to use the settings as configured on the target file system. The default is to preserve these settings as on the source.

   **Note:** To preserve permissions, you must be running as a superuser. You can use the “Run as” option to ensure that is the case.

- **Alerts** - Whether to generate alerts for various state changes in the replication workflow. You can alert on failure, on start, on success, or when the replication workflow is aborted.

11. Click **Save Schedule**.

To specify additional replication tasks, select **Create > HDFS Replication**.

A replication task appears in the All Replications list, with relevant information about the source and target locations, the timestamp of the last job, and the next scheduled job (if there is a recurring schedule). A scheduled job will show a calendar icon to the left of the task specification. If the task is scheduled to run once, the calendar icon will disappear after the job has run.

Only one job corresponding to a replication schedule can occur at a time; if another job associated with that same replication schedule starts before the previous one has finished the second one is canceled.

From the **Actions** menu for a replication task, you can:
- Test the replication task without actually transferring data (“Dry Run”)
- Edit the task configuration
- Run the task (immediately)
- Delete the task
- Disable or enable the task (if the task is on a recurring schedule). When a task is disabled, instead of the calendar icon you will see a Stopped icon, and the job entry will appear in gray.

**Viewing Replication Job Status**

- While a job is in progress, the calendar icon turns into spinner, and each stage of the replication task is indicated in the message after the replication specification.
- If the job is successful, the number of files copied is indicated. If there have been no changes to a file at the source since the previous job, then that file will not be copied. As a result, after the initial job, only a subset of the files may actually be copied, and this will be indicated in the success message.
• If the job fails, a  icon displays.
• To view more information about a completed job, click the task row in the Replications list. This displays sub-entries for each past job.
• To view detailed information about a past job, click the entry for that job. This opens another sub-entry that shows:
  – A result message
  – The start and end time of the job.
  – A link to the command details for that replication job.
  – Details about the data that was replicated.
• When viewing a sub-entry, you can dismiss the sub-entry by clicking anywhere in its parent entry, or by clicking the return arrow icon at the top left of the sub-entry area.

Hive Replication

**Required Role**: Administrator

Hive replication enables you to copy (replicate) your Hive metastore and data from one cluster to another and keep the Hive metastore and data set on the target cluster synchronized with the source based on a user specified replication schedule. The target cluster needs to be managed by the Cloudera Manager Server where the replication is being set up and the source cluster could either be managed by that same server or by a peer Cloudera Manager Server.

**Note**: If the `hadoop.proxyuser.hive.groups` configuration has been changed to restrict access to the Hive Metastore Server to certain users or groups only, then the `hdfs` group or a group containing the `hdfs` user must also be included in the list of groups specified in order for Hive replication to work. This can be specified either on the Hive service as an override, or in the core-site HDFS configuration. This note applies to configuration settings on both the source and target clusters.

Configuring Replication of Hive Data

1. Verify that your cluster conforms to the supported replication scenarios.
2. If the source cluster is managed by a different Cloudera Manager server from the target cluster, configure a peer relationship.
3. Do one of the following:
   - From the Backup tab, select Replications.
   - From the Clusters tab, go to the Hive service and select the Replication tab.
   The Schedules tab of the Replications page displays.
4. Click the Schedule Hive Replication link.
5. Select the Hive service from one managed by the local Cloudera Manager Server or from one of the Hive services managed by the peer Cloudera Manager Server to be the source of the replicated data.
6. Leave Replicate All checked to replicate all the Hive metastore databases from the source. To replicate only selected databases, uncheck this option and enter the database name(s) and tables you want to replicate.

   - You can specify multiple data bases and tables using the plus symbol to add more rows to the specification.
   - You can specify multiple databases on a single line by separating their names with the "|" character. For example: `mydbname1 | mydbname2 | mydbname3`.
   - Regular expressions can be used in either database or table fields. For example:

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\w.+</code></td>
<td>Any database/table name</td>
</tr>
</tbody>
</table>


### Regular Expression

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>(?!myname\b).+</td>
<td>Any database/table except the one named “myname”</td>
</tr>
<tr>
<td>db1</td>
<td>db2</td>
</tr>
<tr>
<td>[\w_]+</td>
<td>Get all tables of the db1 and db2 databases</td>
</tr>
<tr>
<td>db1[\w_]+</td>
<td>Alternate way to get all tables of the db1 and db2 databases</td>
</tr>
<tr>
<td>Click the “+” button and then enter db2[\w_]+</td>
<td></td>
</tr>
</tbody>
</table>

#### 7. Select the target destination.
If there is only one Hive service managed by Cloudera Manager available as a target, then this will be specified as the target. If there are more than one Hive services managed by this Cloudera Manager, select from among them.

#### 8. Select a schedule.
You can have it run immediately, run once at a scheduled time in the future, or at regularly scheduled intervals. If you select **Once** or **Recurring** you are presented with fields that let you set the date and time (if appropriate) and the interval between runs.

#### 9. Uncheck the **Replicate HDFS Files** checkbox to skip replicating the associated data files.

#### 10. Use the **More Options** section to specify an export location, modify the parameters of the MapReduce job that will perform the replication, and other options. Here you will be able to select a MapReduce service (if there is more than one in your cluster) and change the following parameters:

- **By default**, Hive metadata is exported to a default HDFS location (`/user/${user.name}/.cm/hive`) and then imported from this HDFS file to the target Hive metastore. The default HDFS location for this export file can be overridden by specifying a path in the **Export Path** field.
- The **Force Overwrite** option, if checked, forces overwriting data in the target metastore if there are incompatible changes detected. For example, if the target metastore was modified and a new partition was added to a table, this option would force deletion of that partition, overwriting the table with the version found on the source.

  **Important:** If the **Force Overwrite** option is not set and the Hive replication process detects incompatible changes on the source cluster, Hive replication will fail. This situation may arise especially with recurring replications, where the metadata associated with an existing database or table on the source cluster changes over time.

- **By default**, Hive’s HDFS data files (say, `/user/hive/warehouse/db1/t1`) are replicated to a location relative to “/” (in this example, to `/user/hive/warehouse/db1/t1`). To override the default, enter a path in the **Destination** field. For example, if you enter a path such as `/ReplicatedData`, then the data files would be replicated to `/ReplicatedData/user/hive/warehouse/db1/t1`.
- Select the MapReduce service to use for this replication (if there is more than one in your cluster). The user is set in the **Run As** option.
- To specify the user that should run the MapReduce job, use the **Run As** option. By default MapReduce jobs run as `hdfs`. If you want to run the MapReduce job as a different user, you can enter that here. If you are using Kerberos, you **must** provide a user name here, and it must be one with an ID greater than 1000.
- An alternative path for the logs.
- Limits for the number of map slots and for bandwidth per mapper. The defaults are unlimited.
- Whether to abort the job on an error (default is not to abort the job). Check the checkbox to enable this. This means that files copied up to that point will remain on the destination, but no additional files will be copied.
- Whether to skip checksum checks (default is to perform them).
- Whether to remove deleted files from the target directory if they have been removed on the source.
• Whether to preserve the block size, replication count, and permissions as they exist on the source file system, or to use the settings as configured on the target file system. The default is to preserve these settings as on the source.

  Note: If you leave the setting to preserve permissions, then you must be running as a superuser. You can use the "Run as" option to ensure that is the case.

• Whether to generate alerts for various state changes in the replication workflow. You can alert on failure, on start, on success, or when the replication workflow is aborted.

11. Click Save Schedule.

To specify additional replication tasks, select Create > Hive Replication.

A replication task appears in the All Replications list, with relevant information about the source and target locations, the timestamp of the last job, and the next scheduled job (if there is a recurring schedule). A scheduled job will show a calendar icon to the left of the task specification. If the task is scheduled to run once, the calendar icon will disappear after the job has run.

Only one job corresponding to a replication schedule can occur at a time; if another job associated with that same replication schedule starts before the previous one has finished the second one is canceled.

From the Actions menu for a replication task, you can:
• Test the replication task without actually transferring data ("Dry Run")
• Edit the task configuration
• Run the task (immediately)
• Delete the task
• Disable or enable the task (if the task is on a recurring schedule). When a task is disabled, instead of the calendar icon you will see a Stopped icon, and the job entry will appear in gray.

Viewing Replication Job Status

• While a job is in progress, the calendar icon turns into spinner, and each stage of the replication task is indicated in the message after the replication specification.
• If the job is successful, the number of files and tables replicated is indicated. If there have been no changes to a file at the source since the previous job, then that file will not be copied. As a result, after the initial job, only a subset of the files may actually be copied, and this will be indicated in the success message.
• If the job fails, a ✗ icon displays.
• To view more information about a completed job, click the task row in the Replications list. This displays sub-entries for each past job.
• To view detailed information about a past job, click the entry for that job. This opens another sub-entry that shows:
  – A result message
  – The start and end time of the job.
  – A link to the command details for that replication job.
  – Details about the data that was replicated.
• When viewing a sub-entry, you can dismiss the sub-entry by clicking anywhere in its parent entry, or by clicking the return arrow icon at the top left of the sub-entry area.

Impala Metadata Replication

Impala metadata replication is performed as an automatic part of Hive replication. Impala replication is only supported between two CDH 5 clusters. The Impala and Hive services must be running on both clusters. As long as these conditions are met, the replication of Impala metadata happens automatically as part of Hive replication.
This ensures that Impala UDFs (user-defined functions) will be available on the target cluster, just as on the source cluster. As part of replicating the UDFs, the binaries in which they're defined are also replicated.

## Enabling Replication Between Clusters in Different Kerberos Realms

**Required Role:** Administrator

If you want to enable replication between clusters that reside in different Kerberos Realms, there are some additional setup steps you need to perform to ensure that the source and target clusters can communicate.

- **Note:** If either the source or target cluster is running Cloudera Manager 4.6 or later, then both clusters (source and target) must be running 4.6 or later. Cross-realm authentication does not work if one cluster is running Cloudera Manager 4.5.x and one is running Cloudera Manager 4.6 or later.

### For HDFS replication:

1. On the hosts in the **target** cluster, ensure that the `krb5.conf` file on each host has the following information:
   - The kdc information for the **source** cluster's Kerberos realm.
   - Domain/host to realm mapping for the **source** cluster NameNode hosts.
2. On the **target** cluster, through Cloudera Manager, add the realm of the **source** cluster to the Trusted Kerberos Realms configuration property.
   a. Go the the HDFS service page and click the **Configuration** tab.
   b. In the search field type "Trusted Kerberos" to find the Trusted Kerberos Realms property.
   c. Enter the source cluster realm and save your changes.
3. It is recommended that you restart all the affected services. However, you MUST restart the JobTracker to enable it to pick up the new Trusted Kerberos Realm settings. Failure to restart the JobTracker prior to the first replication attempt may cause the JobTracker to fail.

### For Hive replication:

1. Perform the steps described above on the **target** cluster, including restarting the JobTracker.
2. On the hosts in the **source** cluster, ensure that the `krb5.conf` file on each host has the following information:
   - The kdc information for the **target** cluster's Kerberos realm.
   - Domain/host to realm mapping for the **target** cluster NameNode hosts.
3. On the **source** cluster, through Cloudera Manager, add the realm of the **target** cluster to the Trusted Kerberos Realms configuration property.
   a. Go the the HDFS service page and click the **Configuration** tab.
   b. In the search field type "Trusted Kerberos" to find the Trusted Kerberos Realms property.
   c. Enter the target cluster realm and save your changes.
4. It is not necessary to restart any services on the source cluster.
Snapshots

Cloudera Manager supports both HBase and HDFS snapshots:

- HBase snapshots allow you to create point-in-time backups of tables without making data copies, and with minimal impact on RegionServers. HBase snapshots are supported for clusters running CDH 4.2 or later.
- HDFS snapshots allow you to create point-in-time backups of directories or the entire filesystem without actually cloning the data. These snapshots appear on the filesystem as read-only directories that can be accessed just like any other ordinary directories. HDFS snapshots are supported for clusters running CDH 5 or later. CDH 4 does not support snapshots for HDFS.

For further information about how snapshots work, see the section on snapshots in the CDH 5 Installation Guide.

Cloudera Manager enables the creation of snapshot policies that define the directories or tables to be snapshotted, the intervals at which snapshots should be taken, and the number of snapshots that should be kept for each snapshot interval and lets you create, delete, and restore snapshots manually with Cloudera Manager.

Snapshot Policies

**Required Role:** Administrator

Cloudera Manager enables the creation of snapshot policies that define the directories or tables to be snapshotted, the intervals at which snapshots should be taken, and the number of snapshots that should be kept for each snapshot interval. For example, you can create a policy that takes both daily and weekly snapshots, and specify that 7 daily snapshots and 5 weekly snapshots should be maintained.

Managing Snapshot Policies

- **Note:** An HDFS directory must be enabled for snapshots in order to allow snapshot policies to be created for that directory. To designate a HDFS directory as snapshottable, follow the procedure in Enabling HDFS Snapshots.

To create a snapshot policy:

1. Click the **Backup** tab in the top navigation bar and select **Snapshots**.
   
   Existing snapshot policies are shown in a list organized by service. Currently running policies (if any) are shown in the **Running Policies** area.

2. To create a new policy, click **Create**. If no policies currently exist, click the **Create snapshot policy** link. This displays the Create Snapshot Policy pop-up.

3. Select the service for which you want to create a policy from the pull-down list.

4. Provide a name for the policy and optionally a description.

5. Specify the directories or tables that should be included in the snapshot.

   - For an HDFS service, select the paths of the directories that you want to include in the snapshot. The pull-down list will allow you to select only directories that have been enabled for snapshotting. If no directories have been enabled for snapshotting, a warning is displayed.
   
   Click **+** to add another path, **−** to remove a path.

   - For an HBase service, list the tables you want included in your snapshot. You can use a Java regular expression to specify a set of tables. An example is `finance.*` which will match all tables with names starting with `finance`.


6. Specify the snapshot schedule. You can schedule snapshots hourly, daily, weekly, monthly, or yearly, or any combination of those. Depending on the frequency you’ve selected, you can specify the time of day to take the snapshot, the day of the week, day of the month, or month of the year, and the number of snapshots to keep at each interval. Each time unit in the schedule information is shared with the time units of larger granularity. That is, the minute value is shared by all the selected schedules, hour by all the schedules for which hour is applicable, and so on. For example, if you specify that hourly snapshots are taken at the half hour, and daily snapshots taken at the hour 20, the daily snapshot will occur at 20:30.

- To select an interval, check its box. The description will then display the current schedule and the number of snapshots to retain.
- To edit the schedule (time of day, day of week and so on as relevant), and the number of snapshots to keep, click the edit icon (✓) that appears at the end of the description once you check its box. This opens an area with fields you can edit. When you have made your changes, click the Close button at the bottom of this area. Your changes will be reflected in the schedule description.

7. Click More Options to specify whether alerts should be generated for various state changes in the snapshot workflow. You can alert on failure, on start, on success, or when the snapshot workflow is aborted.

To edit or delete a snapshot policy:
1. Click the Backup tab in the top navigation bar and select Snapshots.
2. Click the Actions menu shown next to a policy and select Edit or Delete.

Orphaned Snapshots

When a snapshot policy includes a limit on the number of snapshots to keep, Cloudera Manager checks the total number of stored snapshots each time a new snapshot is added, and automatically deletes the oldest existing snapshot if necessary. When a snapshot policy is edited or deleted, files, directories, or tables that were previously included but have now been removed from the policy may leave “orphaned” snapshots behind that will no longer be deleted automatically because they are no longer associated with a current snapshot policy. Cloudera Manager will never select these snapshots for automatic deletion because selection for deletion only occurs when the policy causes a new snapshot containing those files, directories, or tables to be made.

Unwanted snapshots can be deleted manually through the Cloudera Manager interface or by creating a command-line script that uses the HDFS or HBase snapshot commands. Orphaned snapshots may be hard to locate for manual deletion. Snapshot policies are automatically given a prefix cm-auto followed by a globally unique identifier (guid). For a specific policy, all its snapshots can be located by searching for those whose names start with the prefix cm-auto-guid that is unique to that policy. The prefix is prepended to the names of all snapshots created by that policy.

To avoid orphaned snapshots, delete them before editing or deleting the associated snapshot policy, or make note of the identifying name for the snapshots you want to delete. This prefix is displayed in the summary of the policy in the policy list and appears in the delete dialog. Making note of the snapshot names, including the associated policy prefix, is necessary because the prefix associated with a policy cannot be determined once the policy has been deleted, and snapshot names do not contain recognizable references to snapshot policies.

Viewing Snapshot History

- To view the history of scheduled snapshot jobs, click a policy. This displays a list of the snapshot jobs, and their status.
- Click a snapshot job to view an expanded status for that job. (Click ◀️ to return to the previous view.)
- From the expanded status, click the **details** link to view the details for the command. From here you can view error logs and or click **Download Result Data** to a JSON file named `summary.json` that captures information about the snapshot. For example:

```
{
  "createdSnapshotCount" : 1,
  "createdSnapshots" : [ {
    "creationTime" : null,
    "path" : "/user/oozie",
    "snapshotName" : "cm-auto-f9299438-a6eb-4f6c-90ac-5e86e5b2e283_HOURLY_2013-11-05_05-25-04",
    "snapshotPath" : "/user/oozie/.snapshot/cm-auto-f9299438-a6eb-4f6c-90ac-5e86e5b2e283_HOURLY_2013-11-05_05-25-04"
  } ],
  "creationErrorCount" : 0,
  "creationErrors" : [ ],
  "deletedSnapshotCount" : 0,
  "deletedSnapshots" : [ ],
  "deletionErrorCount" : 0,
  "deletionErrors" : [ ],
  "processedPathCount" : 1,
  "processedPaths" : [ "/user/oozie" ],
  "unprocessedPathCount" : 0,
  "unprocessedPaths" : [ ]
}
```

See **Browsing and Managing Snapshots** on page 19 for information about the managing snapshots.

### Browsing and Managing Snapshots

**Required Role: Administrator**

For both HBase (CDH 4.2 or later or CDH 5) and HDFS (CDH 5 only) services, a Browse tab is available where you can view the HBase tables or HDFS directories associated with a service on your cluster. From here you can view the currently saved snapshots for your tables or files, and delete or restore them as appropriate.

#### Managing HBase Snapshots

From the HBase Browse tab you can:

- View the HBase tables that you can snapshot.
- Initiate immediate (unscheduled) snapshots of a table.
- View the list of saved snapshots currently being maintained. These may include one-off immediate snapshots, as well as scheduled policy-based snapshots.
- Delete a saved snapshot.
- Restore from a saved snapshot.
- Restore a table from a saved snapshot to a new table (Restore As).

### Browsing HBase Tables

To browse the HBase tables to view snapshot activity:

1. From the Clusters tab, select your HBase service.
2. Go to the Browse tab.

### Managing HBase Snapshots

To take a snapshot,

1. Click a table.
2. Click **Take Snapshot**.
Snapshots

3. Specify the name of the snapshot, and click Take Snapshot.

To delete a snapshot, click ▼ and select Delete.

To restore a snapshot, click ▼ and select Restore.

To restore a snapshot to a new table, select Restore As from the menu associated with the snapshot, and provide a name for the new table.

**Warning:** If you "Restore As" to an existing table (that is, specify a table name that already exists) the existing table will be overwritten.

Managing HDFS Directory Snapshots

From the HDFS Browse tab you can:

- Designate HDFS directories to be "snapshottable" so snapshots can be created for those directories.
- Initiate immediate (unscheduled) snapshots of a table.
- View the list of saved snapshots currently being maintained. These may include one-off immediate snapshots, as well as scheduled policy-based snapshots.
- Delete a saved snapshot.
- Restore an HDFS directory or file from a saved snapshot.
- Restore an HDFS directory or file from a saved snapshot to a new directory or file (Restore As)

Browsing HDFS Directories

To browse the HDFS directories to view snapshot activity:

1. From the Clusters tab, select your CDH 5 HDFS service.
2. Go to the Browse tab.

As you browse the directory structure of your HDFS, basic information about the directory you have selected is shown at the right (owner, group, and so on).

Enabling HDFS Snapshots

HDFS directories must be enabled for snapshots in order for snapshots to be created. You cannot specify a directory as part of a snapshot policy unless it has been enabled for snapshotting.

To enable a HDFS directory for snapshots:

1. From the Clusters tab, select your CDH 5 HDFS service.
2. Go to the Browse tab.
3. Verify the Snapshottable Path and click Enable Snapshots.
4. When the command has finished, a Take Snapshot button appears. You may need to refresh the page to see the new state.

**Note:** Once you enable snapshots for a directory, you cannot enable snapshots on any of its subdirectories. Snapshots can be taken only on directories that have snapshots enabled.

To disable snapshots for a directory that has snapshots enabled, use the Disable Snapshots from the drop-down menu button at the upper right. If there are existing snapshots of the directory, they must be deleted before snapshots can be disabled.

Managing HDFS Snapshots

If a directory has been enabled for snapshots:
• The **Take Snapshot** button is present, enabling an immediate snapshot of the directory.
• Any snapshots that have been taken are listed by the time at which they were taken, along with their names and a menu button.

**To take a snapshot**, click **Take Snapshot**, specify the name of the snapshot, and click **Take Snapshot**. The snapshot is added to the snapshot list.

**To delete a snapshot**, click and select **Delete**.

**To restore a snapshot**, click and select **Restore**.

For restoring HDFS data, if a MapReduce or YARN service is present in the cluster, then DistributedCopy (distcp) will be used to restore directories, increasing the speed of restoration. The restore popup for HDFS (under More Options) allows selection of either MapReduce or YARN as the MapReduce service. For files, or if a MapReduce or YARN service is not present, a normal copy will be performed. Use of distcp allows configuration of the following options for the snapshot restoration, similar to what is available when configuring a replication:

• **MapReduce Service** - The MapReduce or YARN service to use.
• **Scheduler Pool** - The scheduler pool to use.
• **Run as** - The user that should run the job. By default this is `hdfs`. If you want to run the job as a different user, you can enter that here. If you are using Kerberos, you *must* provide a user name here, and it must be one with an ID greater than 1000. Verify that the user running the job has a home directory, `/user/<username>`, owned by username:supergroup in HDFS.
• **Log path** - An alternative path for the logs.
• **Maximum map slots** and **Maximum bandwidth** - Limits for the number of map slots and for bandwidth per mapper. The defaults are unlimited.
• **Abort on error** - Whether to abort the job on an error (default is not to do so). This means that files copied up to that point will remain on the destination, but no additional files will be copied.
• **Skip Checksum Checks** - Whether to skip checksum checks (the default is to perform them). If checked, checksum validation will not be performed.
• **Remove deleted files** - Whether to remove deleted files from the target directory if they have been removed on the source. When this option is enabled, files deleted from the target directory are sent to trash if HDFS trash is enabled, or are deleted permanently if trash is not enabled. Further, with this option enabled, if files unrelated to the source exist in the target location, then those files will also be deleted.
• **Preserve** - Whether to preserve the block size, replication count, and permissions as they exist on the source file system, or to use the settings as configured on the target file system. The default is to preserve these settings as on the source.

**Note:** To preserve permissions, you must be running as a superuser. You can use the "Run as" option to ensure that is the case.