

Data Recovery Service (DRS)

Date published: 2020-07-30

Date modified: 2026-09-30



Legal Notice

© Cloudera Inc. 2026. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Data Recovery Service overview.....	4
Backup and restore Cloudera Data Engineering using Data Recovery Service.....	4

Data Recovery Service overview

The Data Recovery Service (DRS) is a microservice in Cloudera Data Services on premises. It allows you to backup and restore Cloudera Data Engineering compute clusters. This enables you to protect Cloudera Data Engineering services, Virtual Clusters (VCs), job definitions, and job execution metadata against datacenter failures or infrastructure migrations.



Important:

- DRS is supported in Cloudera Data Engineering from Cloudera Data Services on premises 1.5.5 SP4 release onwards.
- DRS backs up and restores the Cloudera Data Engineering control plane and compute entities. It does not perform disaster recovery for the underlying Cloudera Base on premises Base cluster (Cloudera Manager, HDFS, or Base Ozone object storage). Base cluster data lake recovery is managed independently through Base Cluster backup procedures.
- In Cloudera Data Engineering, DRS is only supported on Cloudera Embedded Container Service clusters only. It is not supported on OpenShift Container Platform clusters.

DRS in Cloudera Data Engineering is natively integrated into the Cloudera Management Console. It provides automated, policy-driven backup and point-in-time recovery capabilities for Cloudera Data Engineering compute workloads and Cloudera Control Plane states. By capturing consistent snapshots of Cloudera Data Engineering services, Virtual Clusters (VCs), job definitions, application resources, and execution metadata, DRS ensures business continuity and rapid recovery during unexpected datacenter outages, regional infrastructure failures, cluster corruption, or planned environment migrations.

For more information about DRS, see [Data Recovery Service \(DRS\) overview](#).

Supported restore scenarios

Cloudera Data Engineering DRS supports three primary backup and restore topologies:

Table 1: Supported recovery scenarios

Scenario	Description
Same Cloudera Embedded Container Service cluster and same Cloudera Base on premises Base cluster.	Point-in-time state recovery on the same Cloudera Embedded Container Service cluster. Preserves all Cloudera Base on premises Base cluster connections, logs, and historical job metrics.
Different Cloudera Embedded Container Service cluster and same Cloudera Base on premises Base cluster.	Restores Cloudera Data Engineering state to a secondary Cloudera Embedded Container Service cluster connected to the same underlying Cloudera Base on premises Base cluster. Job logs, storage paths, and Cloudera Base on premises Base cluster integrations remain intact.
Different Cloudera Embedded Container Service cluster and different Cloudera Base on premises Base cluster.	Restores Cloudera Data Engineering state to a new Cloudera Embedded Container Service cluster linked to a new Cloudera Base on premises Base cluster. Requires re-mapping Cloudera Manager endpoints, updating Kerberos keytabs, and configuring certificates. Historical job run logs stored in the original Base cluster will not be visible unless the Base Cluster itself was also replicated.

Backup and restore Cloudera Data Engineering using Data Recovery Service

Learn how to perform backup and restore of Cloudera Data Engineering using the Data Recovery Service (DRS).

About this task



Important: If you switch to a secondary Cloudera Base on premises base cluster without performing a backup and restore of the original base cluster, logs for pre-backup runs (stderr, stdout, fgstatus, and event logs) will not be visible.

Procedure

1. [Create a backup of the Cloudera Data Engineering services and virtual clusters.](#)
2. Delete all the Cloudera Data Engineering Services and Virtual Clusters that are already created in the secondary Cloudera Base on premises Base cluster.
3. If any dedicated Cloudera Embedded Container Service cluster nodes were setup for Cloudera Data Engineering before backup, then setup the dedicated Cloudera Embedded Container Service cluster nodes again. For instructions, see [Dedicating Cloudera Embedded Container Service nodes for Cloudera Data Engineering.](#)
4. [Restore the Cloudera Data Engineering services and virtual clusters.](#)
5. To see if the restore operation is successful, perform the following steps:
 - a) In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
 - b) Click Administration in the left navigation menu. The **Administration** page displays.
 - c) In the Services column, select the environment for which you want to see the logs.
 - d) Click Monitoring Logs and check if the Config restart is successful.
 - e) If the Config restart failed, then restart the Cloudera Data Engineering restore using DRS again.
6. If you restored the Cloudera Data Engineering to a new Cloudera Base on premises secondary base cluster, then update the keytab in Cloudera Data Engineering service only if the keytab on the secondary cluster has changed. If the keytab is unchanged, you do not need to update it. For instructions, see [Updating Hadoop Authentication.](#)
7. Configure the TLS certificates again. For instructions about how to configure TLS certificates for Cloudera Data Engineering service, see [Updating the Control Plane certificates in Cloudera Data Engineering services](#) and for virtual clusters, see [Updating the Control Plane certificates in Cloudera Data Engineering Virtual Clusters.](#)



Important: If you experience issues accessing the Spark UI after a restore operation, clear your browser cookies and cache, or click the Spark UI link again to refresh the session.