

# Upgrading CDP Private Cloud Data Services on the Embedded Container Service

Date published: 2020-12-16

Date modified: 2023-06-08

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with a stylized 'E' that has three horizontal bars.

# Legal Notice

© Cloudera Inc. 2024. 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

<b>Upgrading.....</b>	<b>4</b>
Pre-upgrade - Upgrading CDE Service with Endpoint Stability.....	4
Prerequisites for upgrading CDE Service with endpoint stability.....	4
Backing up CDE service using the docker image.....	5
Pre-upgrade - Regenerate external DB cert as SAN (if applicable).....	7
Upgrading Cloudera Manager.....	8
Update from 1.4.1 or 1.5.0 to 1.5.1 (ECS).....	8
Post-upgrade - Ozone Gateway validation.....	15
Post-upgrade - Restoring CDE Service for Endpoint Stability.....	17
Restoring a CDE service.....	17
Rolling back the CDE Service Endpoint migration.....	19
Limitations.....	20
Post-upgrade - Data Warehouse runtime upgrade.....	20

# Upgrading

## Pre-upgrade - Upgrading CDE Service with Endpoint Stability

You can seamlessly upgrade an old Cloudera Data Engineering (CDE) service to a new version with endpoint stability. This enables you to access the CDE service of the new version with the previous endpoint. Thus, you can use the existing endpoints without changing configurations at the application level.

The CDE service endpoint migration process lets you migrate your resources, jobs, job run history, spark jobs' logs and event logs from your old cluster to the new cluster.

### Prerequisites for upgrading CDE Service with endpoint stability

You must first download the docker image and create the `cde-upgrade-util.properties` file to back up the Cloudera Data Engineering (CDE) service.

#### Procedure

1. Download the [dex-upgrade-utils](#) docker image tarball. The file naming convention is `dex-upgrade-utils-<version-number>-<build-number>.tar.gz`.
2. Load the downloaded image into the host machine docker runtime:

```
docker load < dex-upgrade-utils-<version-number>-<build-number>.tar.gz
```

Example:

```
docker load < dex-upgrade-utils-1.19.1-b184.tar.gz
```

3. Create a directory in the host machine and export that path as `BASE_WORK_DIR`.

```
mkdir <host_machine_path>  
export BASE_WORK_DIR=<host_machine_path>
```

Example:

```
mkdir /opt/backup-restore  
export BASE_WORK_DIR=/opt/backup-restore
```

4. Create backup and secrets directories in the `BASE_WORK_DIR` directory and update the access permissions. The secrets directory stores the kubeconfig and CDP DE Admin credentials files. The backup directory will store the backup file which will be generated when you backup the CDE Service.

```
cd $BASE_WORK_DIR  
mkdir backup secrets  
chmod 775 backup
```

5. Place the CDP credentials file of the `DEAdmin` user and `administrator` kubeconfig file in the `$BASE_WORK_DIR/secrets` directory.
6. Create the `cde-upgrade-util.properties` file with the information described below and save it in the `$BASE_WORK_DIR` directory.

```
cdp_k8s_namespace:<CDP control plane k8s namespace>  
cdp_endpoint:<CDP control plane endpoint>  
credential_file_path:<Path to the DEAdmin user CDP credentials file>  
de_admin_user:<DEAdmin user-id>
```

```
de_admin_password:<DEAdmin user's password must be in base64 encoded form
at. Use the echo -n <password> | base64 command to encode the password. >
tls_insecure:<Keep it false if you are using a self-signed certificate>
auto_unpause_jobs: <Specify it as "true" if you want to automatically re
sume the jobs that were paused during the backup phase. The jobs will be
resumed after you restore the CDE service.>
platform_type:<Platform type, can be ECS (Embedded Container Service) or
OCF (OpenShift Container Platform)>
```

Example:

```
$ cat $BASE_WORK_DIR/cde-upgrade-util.properties


cdp_k8s_namespace=cdp-test
cdp_endpoint=https://console-cdp-test.apps.cluster.example.com
credential_file_path=/home/dex/.cdp/credentials
de_admin_user=user
de_admin_password=cGFzc3dvcmQ=
tls_insecure=true
auto_unpause_jobs=true
platform_type=ECS
```



**Note:** You must always set the value of the `credential_file_path` property as `/home/dex/.cdp/credentials` and should not be changed.



**Warning:** You can specify the `cdp_env_override:<environment-name>` optional property in the `cde-upgrade-util.properties` file, if you want to change the environment of the CDE service that is being restored. But, if you change the environment during restore, it will lead to loss of old spark jobs' logs and event logs that were there in the old virtual clusters.

7. Make a note of the details of the CDE service that is being migrated. This information is required if you are using a CDP database that is external and is not accessible from the container which is running the `cde-upgrade` endpoint stability commands. Identify the cluster endpoint:
  - a. In the Cloudera Data Platform (CDP) console, click the Data Engineering tile. The CDE Home page displays.
  - b. Click Administration in the left navigation menu. The Administration page displays.
  - c.
    - In the Services column on the left, click  icon corresponding to the CDE service whose endpoint you want to migrate.
  - d. Make a note of the CDE cluster ID.
8. During the restore operation, both old and the new CDE services use the same resources allocated to existing CDE service. Hence, you must double the resource pool size using the Quota Management option. For example, if `root.default.sales` is the pool that is used for the old or existing CDE service, you must double the CPU and memory resources of this pool. Also, make sure that you have sufficient hardware when doubling the resource pool size.

### What to do next

You must now expand the resource pool, and then upgrade your CDP platform before you restore the CDE service. For information about configuring resource pool and capacity, see *Managing cluster resources using Quota Management*

### Related Information

[Upgrading CDP on the Embedded Container Service](#)

[Managing cluster resources using Quota Management](#)

## Backing up CDE service using the docker image

You must run the docker image to take backup of a Cloudera Data Engineering (CDE) service. It takes backup of all the active virtual clusters in that CDE service. You can take backup of only an active CDE service.

### Before you begin

You must download the `dex-upgrade-utils` docker image and create the `cde-upgrade-util.properties` file before backing up jobs as described in the *Prerequisites for upgrading CDE Service with endpoint stability* section.



**Warning:** You must make sure to allocate sufficient downtime before you proceed further. If you start the backup procedure, you cannot create, edit, or run jobs in the existing CDE service and its associated virtual clusters until the backup is complete. The virtual clusters will be in the read-only mode after you backup the service and until you restore it.



**Important:** It is recommended to copy the logs of the commands run from the terminal and save them on your machine. This will be helpful in debugging or when raising a support ticket. You can also increase the terminal buffer size and save the terminal logs of each command for reference.

### Procedure

Run the `dex-upgrade-utils` docker image on the host machine:

```
$ export BACKUP_OUTPUT_DIR=/home/dex/backup

$ docker run \
-v <kubeconfig_file_path>:/home/dex/.kube/config:ro \
-v <cdp_credential_file_path>:/home/dex/.cdp/credentials:ro \
-v <cde-upgrade-util.properties_file_path>:/opt/cde-backup-restore/scripts/
backup-restore/cde-upgrade-util.properties:ro \
-v <local_backup_directory>:$BACKUP_OUTPUT_DIR \
-e KUBECONFIG=/home/dex/.kube/config \
<docker_image_name>:<docker_image_version> prepare-for-upgrade -s <cde-clust
er-id> -o $BACKUP_OUTPUT_DIR
```



**Important:** All the paths to the right side of colon (:) in volume mounts, that is, paths inside the container are fixed paths and must not be changed. Here `-s` is the CDE service ID and `-o` is the backup output directory path in the container. The backup output directory value must always be `$BACKUP_OUTPUT_DIR` and should not be changed.

Example:

```
$ docker run \

-v $BASE_WORK_DIR/secrets/kubeconfig:/home/dex/.kube/config:ro \
-v $BASE_WORK_DIR/secrets/credentials:/home/dex/.cdp/credentials:ro \
-v $BASE_WORK_DIR/cde-upgrade-util.properties:/opt/cde-backup-restore/scr
ipts/backup-restore/cde-upgrade-util.properties:ro \
-v $BASE_WORK_DIR/backup:$BACKUP_OUTPUT_DIR \
-e KUBECONFIG=/home/dex/.kube/config \
docker-private.infra.cloudera.com/cloudera/dex/dex-upgrade-utils:1.19.1 pr
epare-for-upgrade -s cluster-c2dhkp22 -o $BACKUP_OUTPUT_DIR
```

### Results

You have now taken the CDE service backup as a ZIP file. You can make a note of the Zip file name from the logs to use it while restoring the CDE service.

### What to do next

You must now expand the resource pool, and then upgrade your Cloudera Data Platform (CDP) before you restore the CDE service. For information about configuring resource pool and capacity, see *Managing cluster resources using Quota Management*.

### Related Information

[Managing cluster resources using Quota Management](#)

[Prerequisites for migrating CDE endpoints](#)

## Pre-upgrade - Regenerate external DB cert as SAN (if applicable)

If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1, and you were previously using an external Control Plane metadata database, you must regenerate the DB certificate with SAN before upgrading to CDP Private Cloud Data Services 1.5.1.

### Procedure

1. Generate certificates with SAN for the external Control Plane metadata database, for example `server.crt` and `server.key`.
2. Take a backup of the previous certificates and copy them to postgres.

The certificates will be available in the `/var/lib/pgsql/12/data` directory on the Private Cloud Base cluster host.

3. Use the following command format to change the owner to postgres:

```
chown postgres:postgres <file_name>
```

For example:

```
chown postgres:postgres server.crt
chown postgres:postgres server.key
```

4. Restart postgres:

```
systemctl restart postgresql-12
```

5. Update the certificates in all Cloudera Manager agents and restart the agents:

Get the truststore password from the `/etc/hadoop/conf.cloudera.HDFS-1/ssl-client.xml` file.

- a) To view the certificates in the truststore:

```
keytool -list -rfc -keystore /var/lib/cloudera-scm-agent/agent-cert/cm-
auto-global_truststore.jks -storetype JKS -storepass <truststore_pass
word>
```

- b) Delete the existing postgres certificate:

```
keytool -delete -alias postgresql -rfc -keystore /var/lib/cloudera-scm-a
gent/agent-cert/cm-auto-global_truststore.jks -storetype JKS -storepass
<truststore_password>
```

- c) Import the new certificate into the truststore:

```
keytool -import -file <cert_location> -alias postgresql -rfc -keystore /
var/lib/cloudera-scm-agent/agent-cert/cm-auto-global_truststore.jks -sto
retype JKS -storepass <truststore_password>
```

- d) Restart the agent:

```
systemctl restart cloudera-scm-agent
```

6. In the Private Cloud Management Console UI, update the certificate via: Administration > CA Certificates > Certificate type = External Database.

## 7. Perform the following additional steps for CDW and CML:

### a) CDW:

When any certificate is updated using the Management console, you must perform a refresh DBC operation.

On the CDW Overview page, select Default DBC Options > Refresh.

### b) CML:

Once the certificate is updated, the MLX service should be restarted at the K8s level. Restart the following pods in the <CDP> namespace:

```
dp-mlx-control-plane-app-XXX
dp-cadence-worker-XXX
dp-health-poller-XXX
```

## Upgrading Cloudera Manager

You must use Cloudera Manager version 7.10.1 to set up the CDP Private Cloud Data Services cluster.

If you already have a CDP Private Cloud Base cluster set up using an earlier version of Cloudera Manager, you must first upgrade the Cloudera Manager version to Cloudera Manager 7.10.1 release before proceeding with the CDP Private Cloud Data Services update.

### Related Information

[Upgrading Cloudera Manager](#)

## Update from 1.4.1 or 1.5.0 to 1.5.1 (ECS)

You can update your existing CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 without performing an uninstall.

### Before you begin

- Review the [Software Support Matrix for ECS](#).
- Run the following commands on the ECS server hosts:

```
TOLERATION='{ "spec": { "template": { "spec": { "tolerations": [ { "effect": "NoSchedule", "key": "node-role.kubernetes.io/control-plane", "operator": "Exists" } ] } } } }'
```

```
kubectl patch deployment/yunikorn-admission-controller -n yunikorn -p "$TOLERATION"
```

```
kubectl patch deployment/yunikorn-scheduler -n yunikorn -p "$TOLERATION"
```

- As of CDP Private Cloud Data Services 1.5.1, external metadata databases are no longer supported. If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1, and you were previously using an external Control Plane database, you must run the following psql commands to create the required databases. You should also ensure that the three new databases are owned by the common database users known by the control plane.

```
CREATE DATABASE db-dss-app;
CREATE DATABASE db-cadence;
CREATE DATABASE db-cadence-visibility;
```

- If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1, and you were previously using an external Control Plane database, you must regenerate the DB certificate with SAN before upgrading to CDP Private Cloud Data Services 1.5.1. For more information see [Pre-upgrade - Regenerate external DB cert as SAN \(if applicable\)](#) on page 7.



### About this task



**Note:** ECS services will be unavailable to users for a period of time during this upgrade procedure. However, you should not stop the ECS cluster prior to upgrade. Upgrade requires the ECS cluster to be running and in a healthy state.

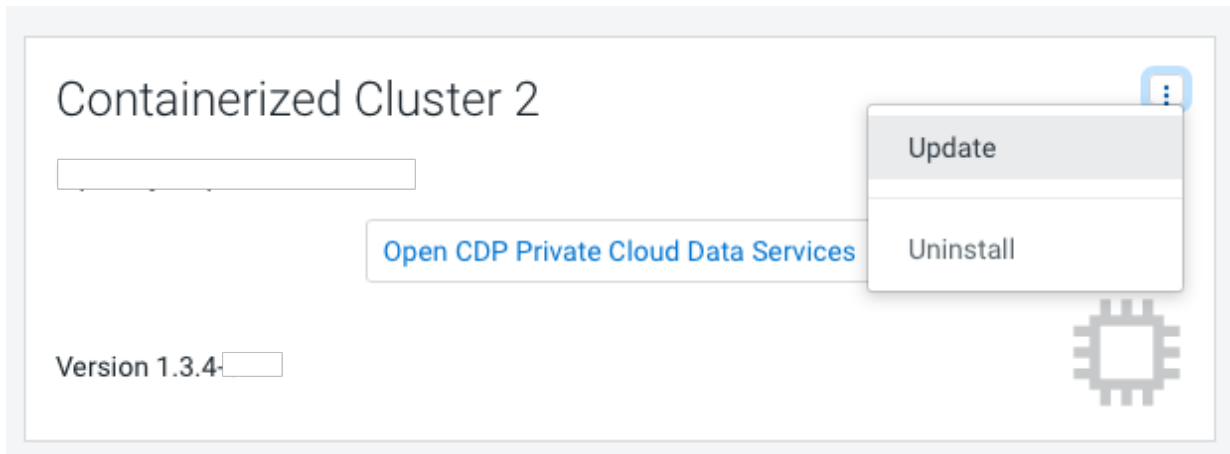


**Important:** When the control plane is upgraded from 1.4.1 to 1.5.1, the Kubernetes version changes to 1.24. The Livy pods running in existing Virtual Clusters (VCs) use a deprecated networking API for creating ingress for Spark driver pods. Because the old networking API is deprecated and does not exist in Kubernetes 1.24, any new job run will not work for the existing VCs.

### Procedure

1.

In Cloudera Manager, navigate to CDP Private Cloud Data Services and click the  icon, then click Update.



2. On the Getting Started page, you can select the Install method - Air Gapped or Internet and proceed.

### Internet install method

Update Private Cloud Data Services (cdp)

Getting Started

This wizard provides step-by-step guidance for updating CDP Private Cloud Data Services. Visit the [CDP Private Cloud](#) documentation for more information.

Current Version  
1.3.4

Install Method  
 Internet  Air Gapped

1. Select Repository

Please ensure all the Data Lake clusters are running Cloudera Runtime 7.1.6 or greater

You are about to update CDP Private Cloud Data Services to version 1.4.0. This is a **minor version** update. Please make sure you have backed up all the external databases.

### Air Gapped install method

Update Private Cloud Data Services (cdp)

Getting Started

This wizard provides step-by-step guidance for updating CDP Private Cloud Data Services. Visit the [CDP Private Cloud](#) documentation for more information.

Current Version  
1.3.4

Install Method  
 Internet  Air Gapped

Installing via a local mirror with an http server. You will need to setup a full mirror of Cloudera's repositories via a temporary http server within the perimeter network of all hosts.

1. Download everything under <https://archive.cloudera.com/p/cdp-pvc-ds/latest>

```
$ wget -l 0 --recursive --no-parent -e robots=off -nH --cut-dirs=2 --reject="index.html*" -t 10 https://<username>:<password>@archive.cloudera.com/p/cdp-pvc-ds/latest
```

2. Modify the file manifest.json inside the downloaded directory, change "http\_url": "." to "http\_url": "http://your\_local\_repo/cdp-pvc-ds/latest"

3. Mirror the downloaded directory to your local http server, e.g. [http://your\\_local\\_repo/cdp-pvc-ds/latest](http://your_local_repo/cdp-pvc-ds/latest)

4. Add [http://your\\_local\\_repo/cdp-pvc-ds/latest](http://your_local_repo/cdp-pvc-ds/latest) to your [Custom Repository](#) settings and select it from the dropdown below.

5. Select Repository

Please ensure all the Data Lake clusters are running Cloudera Runtime 7.1.6 or greater

You are about to update CDP Private Cloud Data Services to version 1.4.0. This is a **minor version** update. Please make sure you have backed up all the external databases.

Click Continue.

3. On the Collect Information page, click Continue.

Update Private Cloud Data Services (cdp)

Collect Information

Sometimes, new configuration information might be needed before you can update. If there are no configuration needed below, just click Next.

Configure Vault

Vault is a secret management tool. You can connect to an existing customer Vault or create a new Vault with this installer. [Learn more](#) on Vault on CDP Private Cloud Data Services.

Embedded vault  
 External Vault (Recommended for production)

4. On the Install Parcels page, click Continue.

Update Private Cloud Data Services (cdp)

Install Parcels

The selected parcels are being downloaded and installed on all the hosts in the cluster.

Embedded Container Service 1.4.0

Downloaded: 100%    Distributed: 1/1 (3.9 MB/s)    Unpacked: 0/1

All (1)    Running (1)    Failed (0)    Completed (0)

Hostname	Throughput	Status	Errors
kpranay-4.vpc.cloudera.com	9.9 MB/s	DISTRIBUTING	

- On the Update Progress page, you can see the progress of your update. Click Continue after the update is complete .

Update Private Cloud Data Services (cdp)

- Getting Started
- Collect Information
- Install Parcels
- Update Data Services
- Summary

### Update Data Services

Upgrade Cluster Command

Status: Running Context: [Containerized Cluster 2](#) May 9, 8:46:13 AM [Abort](#)

**Completed 5 of 6 step(s).**

Show All Steps  Show Only Failed Steps  Show Only Running Steps

Execute command Stop on service ECS-2	<a href="#">ECS-2</a>	May 9, 8:46:13 AM	309ms
Execute command Stop on service DOCKER-2	<a href="#">DOCKER-2</a>	May 9, 8:46:14 AM	2.31s
Activating parcel	<a href="#">Containerized Cluster 2</a>	May 9, 8:46:16 AM	68ms
Waiting for Cloudera Manager Agents to detect release ECS 1.4.0.		May 9, 8:46:16 AM	15.07s
Converting configuration parameters	<a href="#">Containerized Cluster 2</a>	May 9, 8:46:31 AM	24ms
<b>Starting all services in the upgraded cluster.</b>		<a href="#">Containerized Cluster 2</a>	May 9, 8:46:31 AM <a href="#">Abort</a>
<ul style="list-style-type: none"> <li style="margin-right: 10px;"><input type="checkbox"/> Deploy Client Configuration</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Start on service DOCKER-2</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Copy Images to Docker Reg...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Start on service ECS-2</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Post upgrade configuration ...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Install Longhorn UI on servi...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Unseal Vault on service ECS-2</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Reapply All Settings to Clus...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Upgrade Infrastructure Mon...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Upgrade ECS Web UI on set...</li> <li style="margin-right: 10px;"><input type="checkbox"/> Execute command Upgrade Control Plane on s...</li> </ul>			



**Note:** The upgrade might occasionally fail with error messages or conditions such as the following:

- Error message: During the following step: Execute command Install Tolerations Webhook on service ECS-3 the Upgrade progress page mentions a failure waiting for kube-proxy to come up.

Workaround:

- a. Log in using ssh to one of the ECS Server nodes and run the following command:

```
/var/lib/rancher/rke2/bin/kubectl get nodes
```

The output will look similar to the following:

NAME	STATUS	ROLES
ecs-abc-1.vpc.myco.com 4h50m v1.21.8+rke2r2	Ready	control-plane,etcd,master
ecs-abc-2.vpc.myco.com 4h48m v1.20.8+rke2r1	NotReady	<none>
ecs-abc-3.vpc.myco.com 4h48m v1.21.8+rke2r2	Ready	<none>
ecs-abc-4.vpc.myco.com 4h48m v1.20.8+rke2r1	NotReady	<none>
ecs-abc-5.vpc.myco.com 4h48m v1.20.8+rke2r1	NotReady	<none>

If any of the version numbers in the last column are lower than the expected version, reboot those nodes. (For example, v1.20.8 in the output above.)

- b. In the Command Output window, in the step that failed, click Resume.
- Upgrade hangs on the Execute command Post upgrade configuration on service ECS step for more than an hour.

Workaround:

- a. Log in to one of the ECS server nodes and run the following command:

```
kubectl get nodes
```

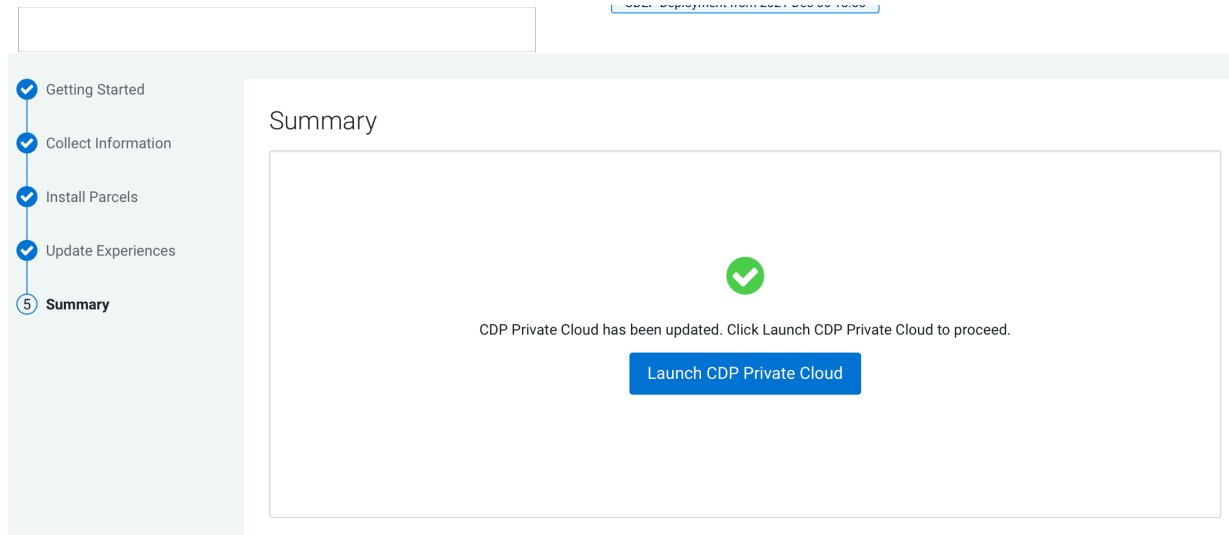
The output looks similar to the following:

NAME	STATUS	ROLES
ecs-abc-1.vpc.myco.com 3h47m v1.21.11+rke2r1	Ready	control-plane,etcd,master
ecs-abc-2.vpc.myco.com 3h45m v1.21.8+rke2r2	NotReady	<none>
ecs-abc-3.vpc.myco.com 3h45m v1.21.8+rke2r2	NotReady	<none>
ecs-abc-4.vpc.myco.com 3h45m v1.21.8+rke2r2	NotReady	<none>

If you any nodes display a status of NotReady, click the Abort button in the command output window.

- b. Reboot all nodes showing NotReady.
- c. Check the node status again as shown above. After all the nodes show Ready, click the Resume button in the command output window to continue with the upgrade.

6. After the update is complete, the Summary page appears. You can now Launch CDP Private Cloud from here.



If you see a Longhorn Health Test message about a degraded Longhorn volume, wait for the cluster repair to complete.

Or you can navigate to the CDP Private Cloud Data Services page and click Open CDP Private Cloud Data Services.

CDP Private Cloud Data Services opens up in a new window.

- If the upgrade stalls, do the following:

1. Check the status of all pods by running the following command on the ECS server node:

```
kubectl get pods --all-namespaces
```

2. If there are any pods stuck in “Terminating” state, then force terminate the pod using the following command:

```
kubectl delete pods <NAME OF THE POD> -n <NAMESPACE> --grace-period=0 -f orce
```

If the upgrade still does not resume, continue with the remaining steps.

3. In the Cloudera Manager Admin Console, go to the ECS service and click Web UIStorage UI.

The Longhorn dashboard opens.

4. Check the "in Progress" section of the dashboard to see whether there are any volumes stuck in the attaching/detaching state in. If a volume is that state, reboot its host.

- You may see the following error message during the Upgrade Cluster > Reapplying all settings > kubectl-patch :

```
kubectl rollout status deployment/rke2-ingress-nginx-controller -n kube-system --timeout=5m
error: timed out waiting for the condition
```

If you see this error, do the following:

1. Check whether all the Kubernetes nodes are ready for scheduling. Run the following command from the ECS Server node:

```
kubectl get nodes
```

You will see output similar to the following:

```
NAME STATUS ROLES AGE VERSION
```

```
<node1> Ready,SchedulingDisabled control-plane,etcd,master 103m v1.21.11+rke2r1
<node2> Ready <none> 101m v1.21.11+rke2r1
<node3> Ready <none> 101m v1.21.11+rke2r1
<node4> Ready <none> 101m v1.21.11+rke2r1
```

2. Run the following command from the ECS Server node for the node showing a status of SchedulingDisabled:

```
kubectl uncordon
```

You will see output similar to the following:

```
<node1>node/<node1> uncordoned
```

3. Scale down and scale up the rke2-ingress-nginx-controller pod by running the following command on the ECS Server node:

```
kubectl delete pod rke2-ingress-nginx-controller-<pod number> -n kube-system
```

4. Resume the upgrade.

### What to do next

- After upgrade, the Cloudera Manager admin role may be missing the Host Administrators privilege in an upgraded cluster. The cluster administrator should run the following command to manually add this privilege to the role.

```
ipa role-add-privilege <cmadminrole> --privileges="Host Administrators"
```

- If you specified a custom certificate, select the ECS cluster in Cloudera Manager, then select Actions > Update Ingress Controller. This command copies the cert.pem and key.pem files from the Cloudera Manager server host to the ECS Management Console host.

## Post-upgrade - Ozone Gateway validation

If you are using CDE, after upgrading CDP Private Cloud Data Services you must validate that the Ozone Gateway is working as expected. This procedure applies to both 1.4.1 to 1.5.1 and 1.5.0 to 1.5.1 upgrades.. You can run the following commands to get the types of logs that are available with the job run:

### Command 1

```
cde run logs --id <run_id> --show-types --vcluster-endpoint <job_api_url> --cdp-endpoint <cdp_control_plane_endpoint> --tls-insecure
```

For example,

```
cde run logs --id 8 --show-types --vcluster-endpoint https://76fsk4rz.cde-fm
ttv45d.apps.apps.shared-rke-dev-01.kcloud.cloudera.com/dex/api/v1 --cdp-endpoint
https://console-cdp-keshaw.apps.shared-rke-dev-01.kcloud.cloudera.com --tls-insecure
```

Log:

TYPE	ENTITY	STREAM	ENTITY DEFAULT
driver/stderr	Driver	stderr	True
driver/stdout	Driver	stdout	False

TYPE	ENTITY	STREAM	ENTITY DEFAULT
executor_1/stderr	Executor 1	stderr	True
executor_2/stdout	Executor 2	stdout	False

## Command 2

```
cde run logs --id <run_id> --type <log_type> --vcluster-endpoint <job_api_url>
--cdp-endpoint <cdp_control_plane_endpoint> --tls-insecure
```

For example,

```
cde run logs --id 8 --type driver/stderr --vcluster-endpoint https://76fsk4r
z.cde-fmttv45d.apps.apps.shared-rke-dev-01.kcloud.cloudera.com/dex/api/v1 --
cdp-endpoint https://console-cdp-keshaw.apps.shared-rke-dev-01.kcloud.cloude
ra.com --tls-insecure
```

Log:

```
Setting spark.hadoop.yarn.resourcemanager.principal to hive
23/05/22 09:27:28 INFO SparkContext: Running Spark version 3.2.3.1.19.71720
00.0-38
23/05/22 09:27:28 INFO ResourceUtils: =====
=====
23/05/22 09:27:28 INFO ResourceUtils: No custom resources configured for sp
ark.driver.
23/05/22 09:27:28 INFO ResourceUtils: =====
=====
23/05/22 09:27:28 INFO SparkContext: Submitted application: PythonPi
23/05/22 09:27:28 INFO ResourceProfile: Default ResourceProfile created, e
xecutor resources: Map(cores -> name: cores, amount: 1, script: , vendor: ,
memory -> name: memory, amount: 1024, script: , vendor: , offHeap -> name: o
ffHeap, amount: 0, script: , vendor: ), task resources: Map(cpus -> name: cp
us, amount: 1.0)
23/05/22 09:27:29 INFO ResourceProfile: Limiting resource is cpus at 1 tasks
per executor
23/05/22 09:27:29 INFO ResourceProfileManager: Added ResourceProfile id: 0
23/05/22 09:27:29 INFO SecurityManager: Changing view acls to: sparkuser,c
dpuser1
23/05/22 09:27:29 INFO SecurityManager: Changing modify acls to: sparkuser,c
dpuser1
23/05/22 09:27:29 INFO SecurityManager: Changing view acls groups to:
23/05/22 09:27:29 INFO SecurityManager: Changing modify acls groups to:
23/05/22 09:27:29 INFO SecurityManager: SecurityManager: authentication en
abled; ui acls disabled; users with view permissions: Set(sparkuser, cdpuse
r1); groups with view permissions: Set(); users with modify permissions: Se
t(sparkuser, cdpuser1); groups with modify permissions: Set()
.....
.....
```

## Results

- If you can see the driver pod logs, then Ozone Gateway is working as expected and you can go ahead with the upgrade.
- If the logs do not appear, then you can try restarting the Ozone Gateway and get Spark job's driver log to validate if Ozone gateway is healthy or not.
- If you do not get the Spark job driver log, then you must contact Cloudera Support.
- For more information about configuring CDE CLI, see [Using the Cloudera Data Engineering command line interface](#)



## Post-upgrade - Restoring CDE Service for Endpoint Stability

After you take backup of the CDE service and upgrade your CDP platform, you can restore the Cloudera Data Engineering (CDE) service with same endpoints.

### Restoring a CDE service

You can restore the Cloudera Data Engineering (CDE) service with its jobs, resources, job run history, and job logs from a backed-up ZIP file.

#### Before you begin

You must back up the CDE service, you must expand the resource pool, and then upgrade your Cloudera Data Platform (CDP) to restore the CDE service. You must validate that the Ozone Gateway is working as expected by performing the steps listed in the *Post upgrade - Ozone Gateway validation* topic.



**Important:** It is recommended to copy the logs of the commands run from the terminal and save them on your machine. This will be helpful in debugging or when raising a support ticket. You can also increase the terminal buffer size and save the terminal logs of each command for reference.

#### Procedure

1. If you have exited from the previous terminal where the pre-upgrade commands were run for CDE Service being upgraded, then you have to export these variables before running any docker command.

```
export BASE_WORK_DIR=<host_machine_path>
export BACKUP_OUTPUT_DIR=/home/dex/backup
```

2. Run the dex-upgrade-utils docker image to restore the service on the same machine where you have completed the prerequisite steps.

```
$ docker run \
-v <kubeconfig_file_path>:/home/dex/.kube/config:ro \
-v <cdp_credential_file_path>:/home/dex/.cdp/credentials:ro \
-v <cde-upgrade-util.properties_file_path>:/opt/cde-backup-restore/scripts/backup-restore/cde-upgrade-util.properties:ro \
-v <local_backup_directory>:$BACKUP_OUTPUT_DIR \
-e KUBECONFIG=/home/dex/.kube/config \
<docker_image_name>:<docker_image_version> restore-service -s <cde-cluster-id> -f $BACKUP_OUTPUT_DIR/<backup-zip-file-name>
```

Here -s is the CDE service ID and -f is the backup output filepath in the container.

Example:

```
$ docker run \
-v $BASE_WORK_DIR/secrets/kubeconfig:/home/dex/.kube/config:ro \
-v $BASE_WORK_DIR/secrets/credentials:/home/dex/.cdp/credentials:ro \
-v $BASE_WORK_DIR/cde-upgrade-util.properties:/opt/cde-backup-restore/scripts/backup-restore/cde-upgrade-util.properties:ro \
-v $BASE_WORK_DIR/backup:$BACKUP_OUTPUT_DIR \
-e KUBECONFIG=/home/dex/.kube/config \
docker-private.infra.cloudera.com/cloudera/dex-upgrade-utils:1.19.1
restore-service -s cluster-c2dhkp22 -f $BACKUP_OUTPUT_DIR/cluster-c2dhkp22-2023-03-10T06_00_05.zip
```

3. [Optional] If you are using a CDP database that is external and is not accessible from the container which is running the CDE upgrade command, then the following SQL statements are displayed in the logs.

Example:

```
2023-05-17 13:02:29,551 [INFO] CDP control plane database is external and
not accessible
2023-05-17 13:02:29,551 [INFO] Please rename the old & new cde service
name manually by executing below SQL statement
2023-05-17 13:02:29,551 [INFO]      update cluster set name = 'cde-base-
service-1' where id = 'cluster-92c2fkgb';
      2023-05-17 13:02:29,551 [INFO]      update cluster set name = 'cde-
base-service-1-18-1' where id = 'cluster-rtc234g8';
2023-05-17 13:02:29,551 [INFO] Please update the lastupdated time of ol
d cde service in db to extend the expiry interval of db entry for suppor
ting CDE CLI after old CDE service cleanup
2023-05-17 13:02:29,551 [INFO]      update cluster set lastupdated =
'2023-05-05 06:16:37.786199' where id = 'cluster-rtc234g8';
-----
```

You must execute the above SQL statements to complete the restore process.

If you have closed the terminal or do not have this information, run the following SQL statements and specify the cluster details. Use the cluster ID that you noted when performing the steps listed in the *Prerequisites for upgrading CDE Service with endpoint stability* section.

- a. Rename old CDE service to a different name.

```
update cluster set name = '<modified_service_name>' where id = '<old_cde
_cluster_id>';
```

Example:

```
update cluster set name = 'cde-base-service-1' where id = 'cluster-92c2f
kgb'
```

- b. Rename the new CDE service to the old CDE service name.

```
update cluster set name = '<old_cde_service_name>' where id = '<new_cde_
_cluster_id>';
```

Example:

```
update cluster set name = 'cde-base-service-1-18-1' where id = 'cluster-
rtc234g8'
```

- c. Run the following command so that when the old CDE service is deleted/disabled then it is not cleared from the database for the next two years. The timestamp format must be the same and should be two years of the current time.

```
update cluster set lastupdated = 'YYYY-MM-DD hh:mm:ss[.nnn]' where id =
'<old_cde_cluster_id>';
```


Example:

```
update cluster set lastupdated = '2023-05-05 06:16:37.786199' where id =
'cluster-rtc234g8'
```

4. [Optional] When the cluster is restored, self-signed certificates are automatically added to the new virtual clusters. To use a signed certificate and private key, perform the following:

a. Identify the virtual cluster endpoint:

1. In the Cloudera Data Platform (CDP) console, click the Data Engineering tile. The CDE Home page displays.
2. Click Administration in the left navigation menu. The Administration page displays.
- 3.

In the Services column on the left, click  corresponding to the CDE service whose endpoint you want to migrate.

4. Click the JOBS API URL link to copy the URL to your clipboard.
5. Paste the URL into a text editor to identify the endpoint host. For example, the URL is similar to the following:

```
http://dfdj6kgx.cde-2cdxw5x5.ecs-demo.example.com/dex/api/v1
```

The endpoint host is `dfdj6kgx.cde-2cdxw5x5.ecs-demo.example.com`.

- b. Provide a signed certificate and private key. Make sure that the certificate is a wildcard certificate for the cluster endpoint. For example, `*.dfdj6kgx.cde-2cdxw5x5.ecs-demo.example.com`.

```
./cdp-cde-utils.sh init-virtual-cluster -h <endpoint_host> -c /path/to/cert -k /path/to/keyfile
```

For example, using the previous example URL, the endpoint host is `dfdj6kgx.cde-2cdxw5x5.ecs-demo.example.com`:

```
./cdp-cde-utils.sh init-virtual-cluster -h dfdj6kgx.cde-2cdxw5x5.ecs-demo.example.com -c /tmp/cde-pvc.crt -k /tmp/cde-pvc.key
```

You must perform this procedure for each virtual cluster you use.

5. After the restore operation completes, validate that the jobs and resources are restored by running the `cde job list` and `cde resource list` CLI commands or check the virtual cluster job UI. In the Administration page of the CDE UI, you can see the old CDE service is appended with a version number. For example, if the old CDE service name was `cde-sales`, after the restore, the old CDE service name is something similar to `cde-sales-1-18.2`.
6. [Optional] You can now delete the old CDE service after validating that everything is working as expected. If you delete the old CDE service, then you can shrink the resource pool size back to its initial value which you expanded in the *Prerequisite* steps.

### Related Information

[Upgrading CDP on the Embedded Container Service](#)

[Ozone Gateway validation](#)

## Rolling back the CDE Service Endpoint migration

You can use the rollback command to delete the new CDE service and restore the old CDE service in working condition.



**Important:** It is recommended to copy and save the logs of the commands run from the terminal and save them on your machine. This will be helpful in debugging or when raising a support ticket. You can also increase the terminal buffer size and save the terminal logs of each command for reference.

To rollback, the state of the CDE service must be in the Failed or Installed state before you restore it.

## Procedure

Run the `rollback-restore-service` command.

```
./cdp-cde-utils.sh rollback-restore-service -s <new-new-service-id> -f <path-to-the-backup-file>
```

Example:

```
./cdp-cde-utils.sh rollback-restore-service -s cluster-j8nmkxh4 -f /home/dex/backup/cluster-sijoeKds-2023-05-23T07_57_57.zip
```

## Limitations

This page lists the current limitations that you might run into while migrating your CDE service endpoint.

- Airflow job logs of the old cluster will be lost after the Restore operation.
- The Spark UI tab for a completed job does not work on the first click. As a workaround, do the following:
  1. Click the Spark UI tab. Nothing is displayed.
  2. Click on some other tab. For example, the Logs tab.
  3. Click the Spark UI tab again. The Spark UI loads now.

## Post-upgrade tasks for Cloudera Data Warehouse

Post-upgrade steps for Cloudera Data Warehouse (CDW) vary depending on whether you are upgrading from 1.4.1 or 1.5.0. Perform the steps that are applicable to you.

### Before you upgrade

Review the [Release Notes](#) to learn about the new features, fixes, and known issues in this release, and more importantly, the [upgrade-related known issues](#).

### Upgrading from 1.4.1

If you are upgrading from CDP Private Cloud Data Services 1.4.1, then in-place upgrade cannot be performed. You must deactivate and reactivate the environment in CDW and recreate Virtual Warehouses with the desired configurations. All customization and configurations are lost when you deactivate an environment. Perform the following steps after upgrading the platform:

1. Log in to the Data Warehouse service as DWAdmin.
2. Note any custom configurations or settings that you have made in CDW.
3. Deactivate the environment in CDW.
4. Reactivate the environment in CDW.
5. Create Virtual Warehouses with your desired configuration.






**Attention:** If you upgrade the platform from 1.4.1 to 1.5.1, but you do not deactivate and reactivate your environment in CDW, you won't be able to create new Virtual Warehouses. Hue will also stop working. However, existing Virtual Warehouses will continue to operate using the existing runtime version and you will be able to query data using SQL client such as Beeline, `impala-shell`, or any other JDBC/ODBC client tools.

### Upgrading from 1.5.0

If you are upgrading from CDP Private Cloud Data Services 1.5.0, then you can perform in-place upgrade. In an in-place upgrade, you can directly upgrade the Database Catalog and Virtual Warehouses from the CDW UI without having to deactivate your environment. Perform the following steps after upgrading the platform:

1. Log in to the Data Warehouse service as DWAdmin.

2. Upgrade the Database Catalog by clicking  Upgrade .
3. Upgrade individual Virtual Warehouses by clicking  Upgrade .
4. Verify whether the upgrade is successful by checking the version information on the Database Catalog or Virtual Warehouse details page by clicking  Edit on the Database Catalog or Virtual Warehouse tile.

### What changes after the upgrade

- Starting with 1.5.1, Data Analytics Studio (DAS) has been deprecated and completely removed from CDW. After you upgrade the platform, any running DAS instances will be removed from the cluster. Cloudera recommends that you use Hue for querying and exploring data in CDW.
- If you upgrade the platform from 1.5.0 to the latest release, then the configuration of an existing environments stays the same as before. Configurations such as default file format, compression type, and transactional type are not copied from the base cluster. To copy configurations from the base cluster, you must reactivate the environment.

### Related Information

[Learn more about the CDW upgrade process](#)

[Activating OpenShift environments on CDW](#)

[Activating Embedded Container Service environments in CDW](#)