CDP Private Cloud Data Services 1.5.0

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

**Date published: 2020-12-16**
**Date modified: 2023-1-24**

**https://docs.cloudera.com/**

# Legal Notice

# Contents

# Upgrading

## Upgrading Cloudera Manager

You must use Cloudera Manager version 7.9.5 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 7.9.5 release before proceeding with the CDP Private Cloud Data Services update.

A hotfix version of Cloudera Manager is required for Cloudera Runtime 7.1.7 SP2 for the following two use cases:

- If you are updating from CDP Private Cloud Data Services 1.4.0-H1 or 1.4.1 and you would like to use Cloudera Runtime 7.1.7 SP2, you must first upgrade the Cloudera Manager version to the Cloudera Manager 7.9.5-h1 hotfix release before proceeding with the CDP Private Cloud Data Services update.
- If you are upgrading from earlier Cloudera Manager versions that did not support CDP Private Cloud Data Services (such as Cloudera Manager 7.6.7) and you would like to use Cloudera Runtime 7.1.7 SP2, you must first upgrade the Cloudera Manager version to the Cloudera Manager 7.9.5-h1 hotfix release before proceeding with the CDP Private Cloud Data Services installation.

### Related Information

Upgrading Cloudera Manager

## Update from 1.4.0-H1 or 1.4.1 to 1.5.0 (ECS)

You can update your existing CDP Private Cloud Data Services 1.4.0-H1 or 1.4.1 to 1.5.0 without performing an uninstall.

### Before you begin

**Important:**

If you are updating from CDP Private Cloud Data Services 1.4.0-H1 or 1.4.1 and you would like to use Cloudera Runtime 7.1.7 SP2, you must first upgrade the Cloudera Manager version to the Cloudera Manager 7.9.5-h1 hotfix release before proceeding with the CDP Private Cloud Data Services update.

- 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"
```

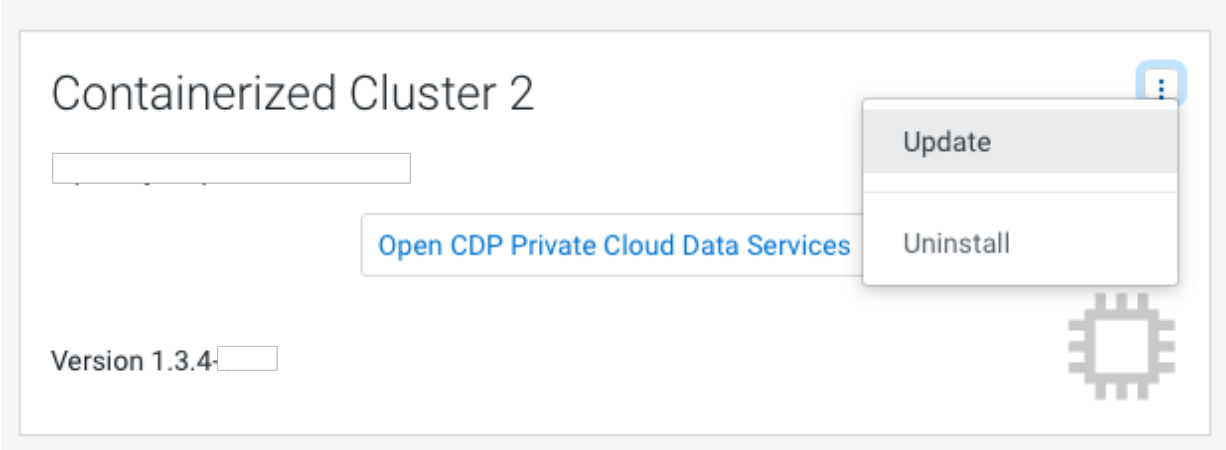
- Upgrading the Embedded Container Service (ECS) version, while CDE service is enabled, it fails to launch the Jobs page in the old CDE virtual cluster. You must back up CDE jobs in the CDE virtual cluster, and then delete the CDE service and CDE virtual cluster. Restore it after the upgrade. For more information about backup and restore CDE jobs, see Backing up and restoring CDE jobs.

### About this task

**Note:** This procedure requires down time during the upgrade.

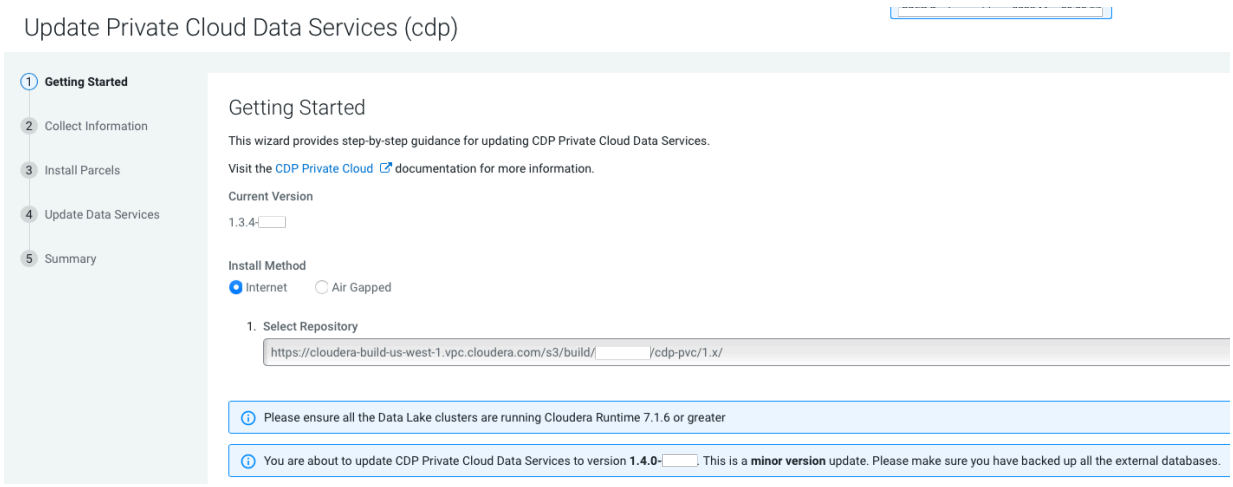
## Procedure

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

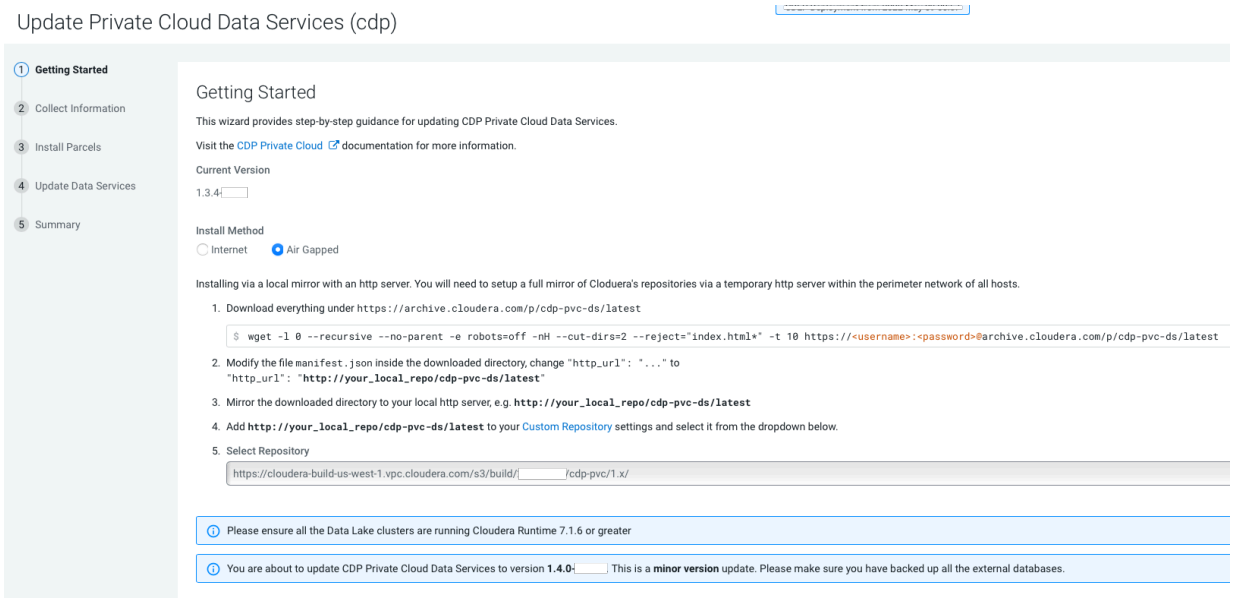


2. On the Getting Started page, you can select the Install method - Air Gapped or Internet and proceed.

   Internet install method

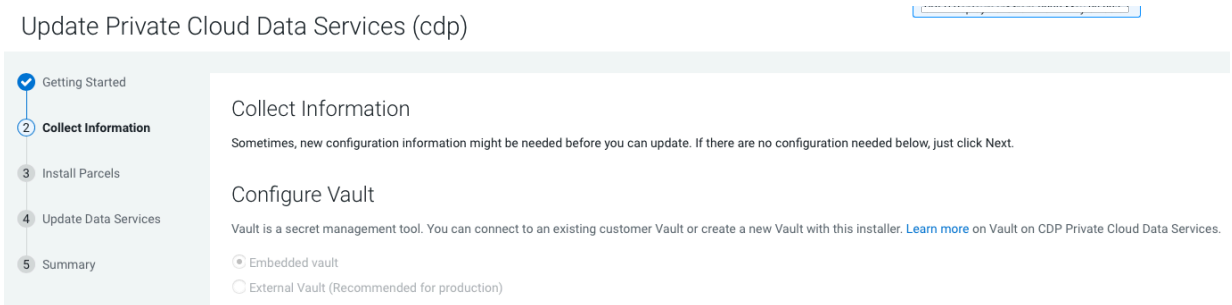



   Air Gapped install method

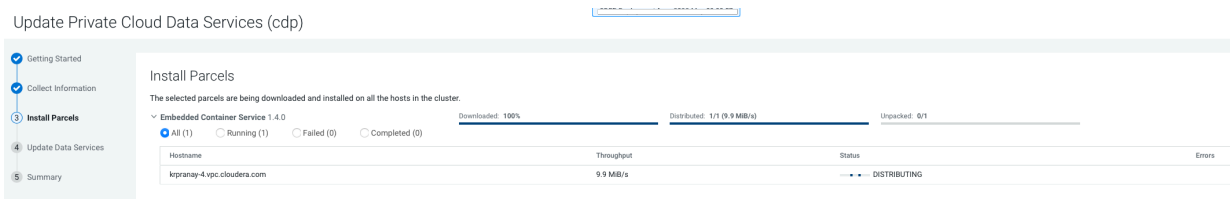



   Click Continue.

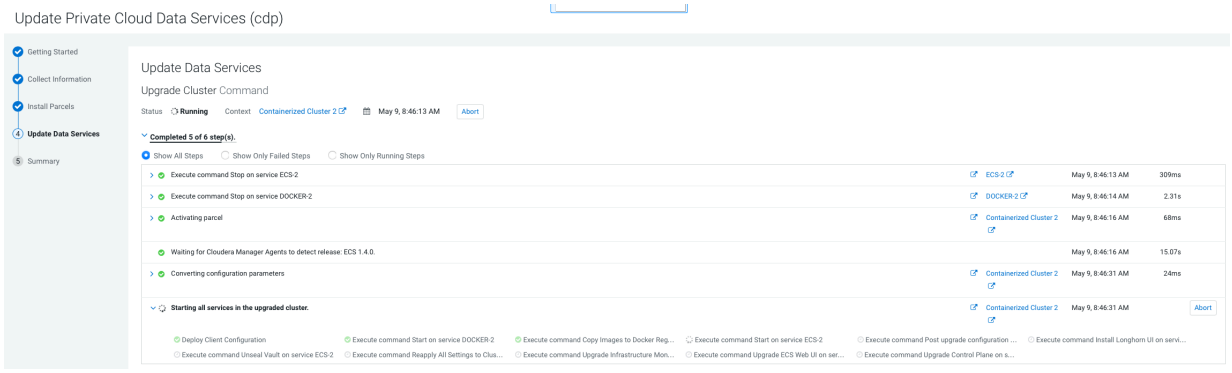
3. On the Collect Information page, click Continue.



4. On the Install Parcels page, click Continue.



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



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

  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:

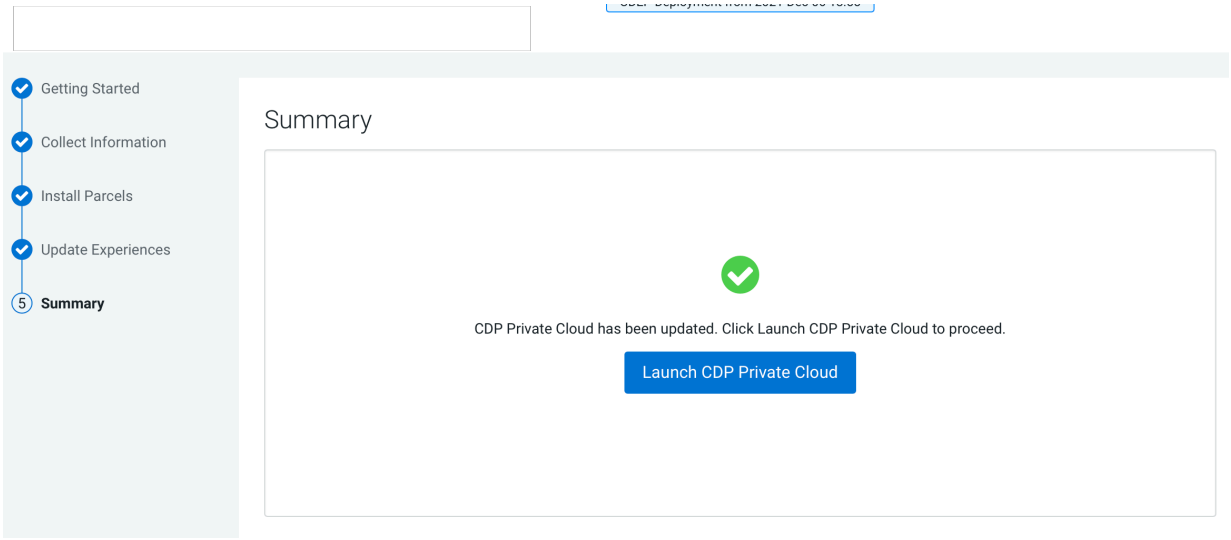
  ```
  NAME                      STATUS     ROLES
  AGE     VERSION
  ecs-abc-1.vpc.myco.com   Ready      control-plane,etcd,master
  3h47m   v1.21.11+rke2r1
  ecs-abc-2.vpc.myco.com   NotReady   <none>
  3h45m   v1.21.8+rke2r2
  ecs-abc-3.vpc.myco.com   NotReady   <none>
   3h45m   v1.21.8+rke2r2
  ecs-abc-4.vpc.myco.com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

  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 –force
     ```

     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-s
   ystem
   ```

4. Resume the upgrade.

### What to do next

- 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.

## Migrating CDE Service Endpoint

You can now manually migrate an old CDE service endpoint to another new CDE service seamlessly. Migration provides endpoint stability and enables you to access the new CDE version with the previous endpoint. In upgrade scenarios, you can use the latest CDE version with the existing endpoints without changing configurations at the application level.

Contact your Cloudera Account team to help you in migrating your CDE Service endpoint manually.