1.4.0

Installing CDP Private Cloud Data Services with the Embedded Container Service

Date published: 2021-10-04
Date modified: 2022-05-20

https://docs.cloudera.com/

Legal Notice

Contents

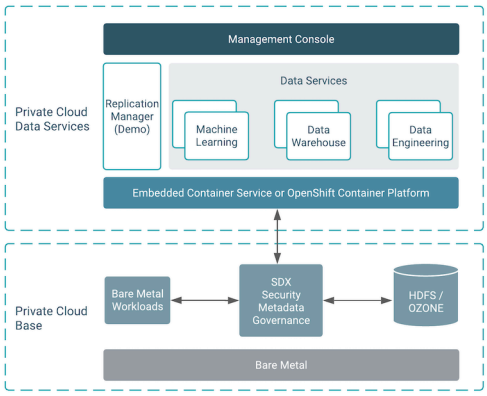
CDP Private Cloud Data Services installation overview

CDP Private Cloud Data Services works on top of CDP Private Cloud Base and is the on-premise offering of CDP that brings many of the benefits of the public cloud deployments to the on-premise CDP deployments. Like the cloud native applications, the CDP Private Cloud Data Services are designed to be easy to use, offer tenant-level isolation and self-service with auto-scale. All of this is made possible by the new Embedded Container Service (ECS) which manages the compute infrastructure and ease of deployment for the Data Services.

Note: To install CDP Private Cloud Data Services on OpenShift, see Installing on OpenShift.

An installation of CDP Private Cloud Base is required to deploy CDP Private Cloud Data Services. A base cluster deployed in CDP Private Cloud Baseserves as a Data Lake for the Data Services. CDP Private Cloud Data Services is the on-premise offering of CDP that brings many of the benefits of public cloud deployments to on-premise CDP deployments. CDP Private Cloud Data Services allows you to deploy the Cloudera Data Warehouse (CDW), Cloudera Machine Learning (CML), and Cloudera Data Engineering(CDE) data services.

The CDP Private Cloud Data Services rely and work with customer's existing data storage and governance clusters, which we refer to as Private Cloud Base Cluster. The data services, once deployed, seamlessly and securely connect with the Private Cloud Base cluster. The following diagram is a typical example of a CDP Private Cloud Data Services deployment:



Before you can install CDP Private Cloud Data Services, you need a running instance of CDP Private Cloud Base. You need an isolated hardware environment with dedicated infrastructure and networking for CDP Private Cloud Data Services.

Requirements

CDP Private Cloud Base Software Requirements

The software requirements for the nodes on which CDP Private Cloud Data Services are deployed are identical to CDP Private Cloud Base.

Your Private Cloud Base cluster must have the operating system, JDK, database, CDP components, and CDP Runtime version compatible with CDP Private Cloud Data Services.

You can install your Private Cloud Base cluster independently. Cloudera recommends that you first set up the Private Cloud Base cluster with data and then install the Private Cloud Containerized cluster. To know the requirements for the Private Cloud Base cluster, see Requirements and Supported Versions.

Ensure that you have CDP Private Cloud Base 7.1.6, 7.1.7, or 7.1.7 SP1 with a Data Lake cluster. (CDP Private Cloud Base 7.1.7 SP1 is compatible with CDP Private Cloud Data Services 1.4.0/1.4.0-H1 if you upgrade to Cloudera Manager 7.6.5). For the Private Cloud Base cluster setup, you can use the latest version of Cloudera Manager 7.6.5.

Note: The current Cloudera Manager version supports the Private Cloud Base cluster. You must upgrade the current Cloudera Manager to Cloudera Manager 7.6.5 to install the Private Cloud Containerized cluster.

The following CDP Private Cloud Base cluster services are required to fully access the Data Services:

- Hive Metastore (HMS)
- Ranger
- Atlas
- HDFS
- Ozone
- YARN
- Kafka
- Solr

CDP Private Cloud Data Services Hardware Requirements

Minimum and recommended hardware to successfully install and run Private Cloud Data Services.

In addition to the resources required for the Control Plane, additional resources will be required depending on the Data Service(s) you intend to run. Minimum and recommended additional resource requirements for each of the Data Services can be found in the pages below. To calculate the total minimum or recommended resource requirements for your CDP Private Cloud Data Services cluster, add the resources required for the Control Plane to the total minimum or recommended additional resources for your chosen Data Service(s).

You can also use the CDP Private Cloud Data Services Spreadsheet to model the number and specification of hosts required for a deployment. See How to use the CDP Private Cloud Data Services sizing spreadsheet on page 7.

Requirements for HA and Non-HA Control Plane

Standard resource mode requirements for standalone HA and Non-HA Control Plane.

Component	Minimum	Recommended
Node Count	1 (Non-HA) **Note:** The Control Plane does not require a dedicated node.	3 (HA)
CPU	8 core	8 core (per node)
Memory	16 GB	16 GB (per node)
Storage	300 GB	1 TB (per node)
Network Bandwidth	1GB/s to all nodes and base cluster	1GB/s to all nodes and base cluster

Note: You must not use embedded or external NFS for high-scale input or output. For example, large data sets. Input or output data should be stored in HDFS or Ozone. Using NFS for small project artifacts is fine.

Additional resource requirements for Cloudera Data Warehouse

Standard resource mode requirements for Cloudera Data Warehouse.

The following table lists the minimum and recommended compute (processor), memory, storage, and network bandwidth required for each OpenShift or ECS worker node using the Standard Resource Mode for production use case. Note that the actual node still needs some extra resources to run the operating system, Kubernetes engine, and Cloudera Manager agent on ECS.

Component	Minimum	Recommended
Node Count	10	20
CPU per worker	16 cores [or 8 cores or 16 threads that have Simultaneous Multithreading (SMT) enabled]	32+ cores (can also be achieved by enabling SMT)
Memory per worker	128 GB per node	384 GB* per node
FAST (Fully Automated Storage Tiering) Cache - Locally attached SCSI device(s) on every worker. Preferred: NVMe and SSD. OCP uses Local Storage Operator. ECS uses Local Path Provisioner.	1.2 TB* SATA, SSD per host	1.2 TB* NVMe/SSD per host
Persistent Volume (PV) Block Storage. On OCP, block from a Container Storage Interface (CSI)-compliant block provider, such as OpenShift Container Storage. ECS uses an embedded distributed block provider that aggregates local disks of workers. Other Data Services additionally have added capacity requirements on this service.	Approximately 100 GB per Virtual Warehouse	Approximately 100 GB per Virtual Warehouse
Network Bandwidth	1 GB/s guaranteed bandwidth to every CDP Private Cloud Base node	10 GB/s guaranteed bandwidth to every CDP Private Cloud Base node

Important: When you add memory and storage, it is very important that you add it in the increments as follows:

- Increments of 128 GB of memory
- Increments of 600 GB of locally attached SSD/NVMe storage
- Increments of 100 GB (in 5 chunks of 20 GB each) of persistent volume storage per Virtual Warehouse

If you add memory or storage that is not in the above increments, the memory and storage that exceeds these increments is not used for executor pods. Instead, the extra memory and storage can be used by other pods that require fewer resources.

For example, if you add 200 GB of memory, only 128 GB is used by the executor pods. If you add 2 TB of locally attached storage, only 1.8 TB is used by the executor pods.

Additional resource requirements for Cloudera Data Engineering

Standard resource mode requirements for standalone Cloudera Data Engineering.

Component	Minimum	Recommended
Node Count	3	5
CPU	16 cores for CDE workspace (base and virtual cluster) and 8 cores for workload	16 cores for CDE workspace (base and virtual cluster) and 32 cores (you can extend this depending upon the workload size)

* Depending on the number of executors you want to run on each physical node, the per-node requirements change proportionally. For example, if you are running 3 executor pods per physical node, you require 384 GB of memory and approximately 1.8TB (600GB per executor) of locally attached SSD/NVMe storage for FAST Cache.

Component	Minimum	Recommended
Memory	64 GB for CDE workspace (base and virtual cluster) and 32 GB (you can extend this depending upon the workload size)	64 GB for CDE workspace (base and virtual cluster) and 64 GB (you can extend this depending upon the workload size)
Storage	200 GB block storage and 500 GB NFS storage	200 GB block storage and 500 GB NFS storage
Network Bandwidth	1 GB/s to all nodes and base cluster	10 GB/s to all nodes and base cluster

Additional resource requirements for Cloudera Machine Learning

Standard resource mode requirements for standalone Cloudera Machine Learning. Node count should not be a limiting factor assuming the other MEM and CPU mins are reached.

Component	Minimum	Recommended
Node Count	1	1 per workspace + additional nodes depending on expected user workloads
CPU	16 Cores Per Workspace+ additional Cores depending on expected user workloads	32 Cores Per workspace + addtitional Cores depending on expected user workloads
Memory	32 GB + addtitional memory depending on the expected workloads	64 GB Per Workspace + addtitional memory depending on the expected workloads
Storage	600 GB Block storage + 1000 GB NFS storage (Block if internal and NFS if external)	4500 GB Block storage+ 1000 GB NFS storage if external
Network Bandwidth	1GB/s to all nodes and base cluster	1GB/s to all nodes and base cluster

Additional Resources for User Workloads:

Component	Minimum	Recommended
CPU	1 Core per concurrent workload	2–16 cores per concurrent workload (dependent on use cases)
Memory	2 GB per concurrent workload	4–64 GB per concurrent workload (dependent on use cases)

How to use the CDP Private Cloud Data Services sizing spreadsheet

You can use the sizing spreadsheet to model the hardware requirements for a CDP Private Cloud Data Services deployment.

Overview

The CDP Private Cloud Data Services Sizing spreadsheet is a spreadsheet that you can use to model the quantity and specifications for worker hosts required in a CDP Private Cloud Data Services deployment.

This spreadsheet is intended to use information about workloads you are planning to run and hardware specifications for worker nodes to arrive at an approximate number of worker nodes required for your deployment. Due to the complexity of estimating workloads, Cloudera recommends you review any sizing or purchasing decisions with Cloudera Professional Services before committing to those decisions.

How to access the spreadsheet

You can access the spreadsheet here: CDP Private Cloud Data Services Sizing. The file is in Microsoft Excel format. You can open the file in Excel, or upload it to Google Sheets.

There are three tabs in the spreadsheet. You will make your inputs only on the Worker Node Totals tab. Do not modify the following tabs (these tabs contain data used to calculate values in the spreadsheet and should not be modified):

- Component Lookup

- K8s Resources

Important: Do not modify any cells except for the ones indicated below. Modifying the formulas in other cells will result in inaccurate calculations.

Workload inputs

The spreadsheet calculates the total amount vcores, RAM, and storage required based on information you enter about the combined workloads you intend to deploy. Then based on the hardware specifications entered, calculates the number of worker nodes required, which is displayed in cell E25.

The following sections describe values you must enter into the spreadsheet. Values are required for each Data Service you intend to deploy, and values to enter for the hardware specifications for your worker nodes.

Cloudera Data Warehouse (CDW)

If you will deploy CDW, on the Worker Node Totals tab, enter the following information:

Label	Cell	Description
CDW Data Catalog (min 1 per env)	B5	Enter the number of Data Catalogs you will need in your deployment. You must have at least one Data Catalog.
CDW LLAP warehouses	B6	Enter the number of LLAP warehouses you will need for each Virtual Warehouse in your deployment.
-- LLAP Executors	B7	Enter the total number of LLAP Executors you will need in your deployment.
CDW Impala warehouses	B8	Enter the number of CDW Impala warehouses for each Virtual Warehouse you will need in your deployment.
-- Impala Coordinators (2 x for HA)	B9	Enter the number of Impala Warehouses you will need in your deployment. If you have enabled high availability, enter twice the number of Warehouses.
-- Impala Executors	B10	Enter the number of Impala Executors you will need in your deployment.
-- CDW Data Cache	B11	Enter the amount of CDW Cache space for each coordinator and executor (Default 600)

For more information about sizing Cloudera Data Warehouse deployments, see:

- (OCP) CDE hardware requirements.
- (ECS) Additional resource requirements for Cloudera Data Engineering

Cloudera Machine Learning (CML)

Sizing for a CML deployment depends on the number of concurrent jobs you expect to run and the number of Workspaces you provision.

Label	Cell	Description
CML Workspace (min of 1)	B13	Enter the number of workspaces you need in your deployment.
-- CML Small session	B14	Enter the number of concurrent small-sized sessions you intend to run.
-- CML Medium session	B15	Enter the number of concurrent medium-sized sessions you intend to run.

Label	Cell	Description
-- CML Large session	B16	Enter the number of concurrent large-sized sessions you intend to run.

For more information about sizing the Cloudera Data Engineering service, see the following topics:

- Additional resource requirements for Cloudera Machine Learning.
- (OCP) Cloudera Machine Learning requirements
- (ECS)Cloudera Machine Learning requirements

Cloudera Data Engineering (CDE)

Label	Cell	Description
CDE Service (min/max 1 per cluster)	B18	Enter the number of CDE clusters you will need in your deployment.
CDE Virtual Cluster	B19	Enter the number of CDE Virtual Clusters you will need in your deployment.
-- CDE Small jobs	B20	Enter the number of concurrent small-sized jobs you intend to run.
-- CDE Avg Jobs	B21	Enter the number of concurrent average-sized jobs you intend to run.

For more information about sizing the Cloudera Data Engineering service, see Additional resource requirements for Cloudera Data Engineering.

Worker node hardware specifications

Based on the inputs you supplied for your workloads, the spreadsheet totals the number of vcores, RAM, and storage required for the cluster in cells C20-C26. Then, based on the worker node hardware specifications you enter in cells B26-B29, divides the totals for vcores, RAM and storage by each of the worker node specifications to arrive at the required number of nodes for vcores, RAM and storage shown in cells D5-D29. The final number, in cell E27 chooses the higher value of these cells.

You may notice that the calculated values in cells D26 and D27 are different. This indicates that some nodes are oversubscribed for RAM or vcores. Adjust the hardware specifications for CPU and RAM until the two cells are closer together in value. Changing these values may also change the calculated number of worker nodes.

Label	Cell	Description
CPU recommend 32+ cores (64vcores)	B26	Enter the number of vcores for each worker node.
RAM (GB) recommend 384GB RAM	B27	Enter the amount of RAM, in gigabytes, for each worker node.
Disk (GB) Block (OCP CSI block, ECS Longhorn)	B28	Enter the number of gigabytes Block required for: - OpenShift Container Platform: CSI block - Embedded Container Service: ECS Longhorn
Disk (GB) Fast Cache for CDW (nvme,ssd)	B29	Enter the number of gigabytes of Fast Cache used in Cloudera Data Warehouse.
NFS (GB) (choose 1 from below)	B31	Enter required storage in either cell B30 or cell B31:
-- Embedded nfs - (subtract from Block provider) non-prod	B32	Enter the number of gigabytes storage for an embedded NFS.
-- External nfs	B33	Enter the number of gigabytes of storage for an External NFS.

Label	Cell	Description
		If you are using the Embedded Container Service, you will also need to provision a host for the ECS Master Node (a node running the ECS Server component). The information below contains Cloudera's recommendations for specifications for the ECS Master node.
NEW* ECS Master Node spec	B35	8 vcores
	B36	16 GB RAM
	B37	1 TB HDD (For a "proof-of-concept" cluster, 300GB is adequate.)

CDP Private Cloud Data Services Software Requirements

The software requirements for the nodes on which CDP Private Cloud Data Services are deployed are identical to CDP Private Cloud Base. The most basic requirement is the operating system and JDK support.

This release ships with Cloudera Manager 7.6.5. This new version of Cloudera Manager has the support to create and manage the ECS cluster. If you have an existing Base cluster setup, managed by Cloudera Manager, you must first upgrade Cloudera Manager to version 7.6.5.

For this release, the ECS nodes will support:

- CentOS 8.4, 7.9, Red Hat Enterprise Linux 8.4. 7.9, Oracle Linux 7.9, and CentOS 8.2 (CDW only)
- JDK 11 (any distribution)
- For CML, you must install nfs-utils in order to mount longhorn-nfs provisioned mounts. The nfs-utils package is required on every node of the ECS cluster. Run this command `yum install nfs-utils` to install nfs-utils.
- If you have nodes with GPU, ensure that the GPU hosts have nVidia Drivers and nvidia-container-runtime installed. You must confirm that drivers are properly loaded on the host by executing the command `nvidia-smi`. You must also install the nvidia-container-toolkit package.

Additionally, you must perform the following:

- You must have a minimum of one agent node for ECS.
- Set up Kerberos on these clusters using an Active Directory or MIT KDC.
- Enable TLS on the Cloudera Manager cluster for communication with components and services.
- Configure PostgreSQL database as an external database for the Private Cloud Base cluster components[*].
- If you do not have entitlements, contact your Cloudera account team to get the necessary entitlements.
- The default docker service uses /docker folder. Whether you wish to retain /docker or override /docker with any other folder, you must have a minimum of 200 GB space.
- Ensure all the hosts in the ECS cluster have 100 gigabytes free in the /var/lib directory at the time of installation.
- The cluster generates multiple hosts and host based routing is used in the cluster in order to route it to the right service. You must decide on a domain for the services which Cloudera Manager by default points to one of the hostnames on the cluster. However, during the installation, you should check the default domain and override the default domain (only if necessary) with what you plan to use as the domain. The default domain must have a wildcard DNS entry. For example, "*.apps.myhostname.com".
- It is recommended that you leave IPv6 enabled at the OS level on all ECS nodes.

[*] Cloudera Data Warehouse (CDW) supports MariaDB, MySQL, PostgreSQL version 12, and Oracle databases for the Hive Metastore (HMS) on the base CDP cluster (Cloudera Manager side). Support for Oracle database (whether SSL-enabled or not) is in technical preview and not recommended for production deployments.

Installation

Preparing CDP Private Cloud Base

Use Cloudera Manager to configure your Private Cloud Base cluster in preparation for the Private Cloud Data Services installation.

1. Configure the Private Cloud Base cluster to use TLS.Configuring TLS Encryption for Cloudera Manager Using Auto-TLS.
2. Configure Cloudera Manager with a JKS-format (not PKCS12) TLS truststore.Database requirements.
3. Configure Cloudera Manager to include a root certificate that trusts the certificate for all Cloudera Manager server hosts expected to be used with the Private Cloud, LDAP server (if you are using LDAP), and the Postgres DB of all Hive Metastores that you use with Private Cloud. If a single CA is used to sign all of them, then just that single CA must be imported.
   a. Import the necessary certificates into the truststore configured in Configure Administration > Settings > Security > Cloudera Manager TLS/SSL Client Trust Store File.
4. Enable Kerberos for all the services in the cluster.Enabling Kerberos for authentication.
5. Configure Ranger and LDAP for user authentication. Ensure that you have configured Ranger user synchronization.Configure Ranger authentication for LDAP and Ranger usersync.
6. Configure LDAP using Cloudera Manager. Only Microsoft Active Directory (AD) and OpenLDAP are currently supported.Configure authentication using an LDAP-compliant identity service.
7. Check if all the running services in the cluster are healthy. To check this using Cloudera Manager, go to Cloudera Manager > Clusters > [***CLUSTER NAME***] > Health Issues. If there are no health issues, the No Health Issues message is displayed.
8. If you want to reuse data from your legacy CDH or HDP deployment in your Private Cloud, copy the data from your CDH or HDP deployments into the CDP Private Cloud Base cluster that will be accessed by CDP Private Cloud Data Services. For more information about data migration, see the Data Migration Guide.
9. For installing CDP Private Cloud Base, see Install CDP Private Cloud Base

Adding a CDP Private Cloud Data Services cluster

Using the new Cloudera Manager 7.6.5, you can either install Private Cloud Data Services by downloading the repository from the Internet or you can do an air gap installation if your Cloudera Manager does not have access to the Internet.

Before you begin:

- Ensure you have Cloudera Manager 7.6.5 installed and you have the entitlements to the CDP Private Cloud Data Services product.
- Only TLS 1.2 is supported for authentication with Active Directory/LDAP. You require TLS 1.2 to authenticate the CDP control plane with your LDAP directory service like Active Directory.
- When the system logs you out after some period of inactivity and the Add Cluster wizard is not yet finished, you must either restart Cloudera Manager or from the Home screen > select Add Cluster > choose CDP Private Cloud Base cluster > Click Continue, and then just click Cancel to leave the wizard.
- The Kubeconfig file is available in /etc/rancher/rke2/rke2.yaml
- If the installer fails, do not cancel the installation. For more information, see Manually uninstalling ECS from a cluster.
- If you are installing ECS on RHEL 8.4, step 2 and its substeps available in the next section are mandatory.

Note: While installing the ECS cluster using the Cloudera Manager UI, do not provide the unsupported characters in the app-domain. The supported characters are:

- Lower case alphanumeric characters
- '-' or '.'
- It must start and end with an alphanumeric character. For example, 'example.com', and regex used for validation is '[a-z0-9]([-a-z0-9][a-z0-9])?(\.[a-z0-9]([-a- z0-9][a-z0-9])?)*')

Installing CDP Private Cloud Data Services

Follow the steps in this topic to install CDP Private Cloud Data Services.

Procedure

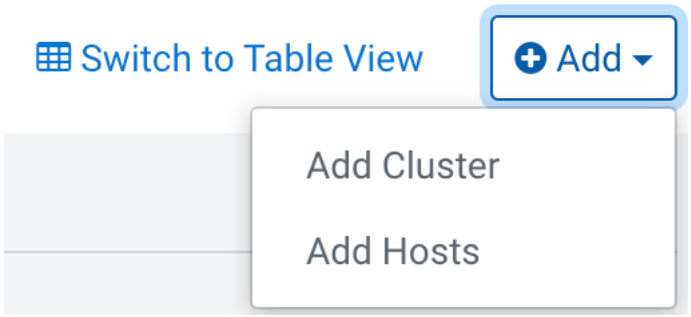
1. If your ECS hosts are running the CentOS 8.4 or OEL 8.4 operating systems, you must install iptables on all the ECS hosts. (This step is not required when running RHEL 8.4.) Run the following command on each ECS host:

```
yum --setopt=tsflags=noscripts install -y iptables
```

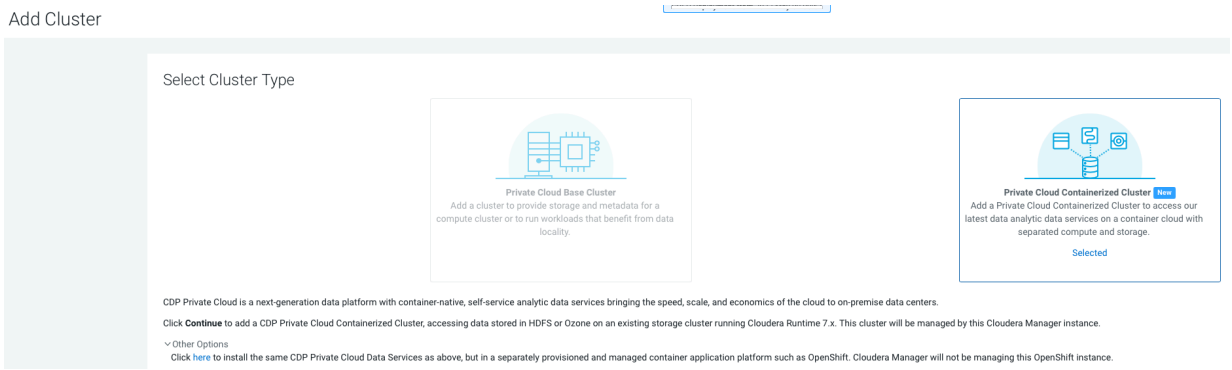
2. If you are installing ECS on RHEL 8.x:,
   a) Add the hosts you intend to use for ECS to Cloudera Manager, without specifying a cluster. See Add New Hosts To Cloudera Manager.
   b) If you are using RHEL 8.4, and if the nm-cloud-setup.service and nm-cloud-setup.timer services are enabled, disable them by running the following command on each host you added:

```
systemctl disable nm-cloud-setup.service nm-cloud-setup.timer
```

   For more information, see Known issues and limitations.
   c) If you disabled the nm-cloud-setup.service and nm-cloud-setup.timer services, reboot the added hosts.
3. In Cloudera Manager, on the top right corner, click Add > Add Cluster. The Select Cluster Type page appears.

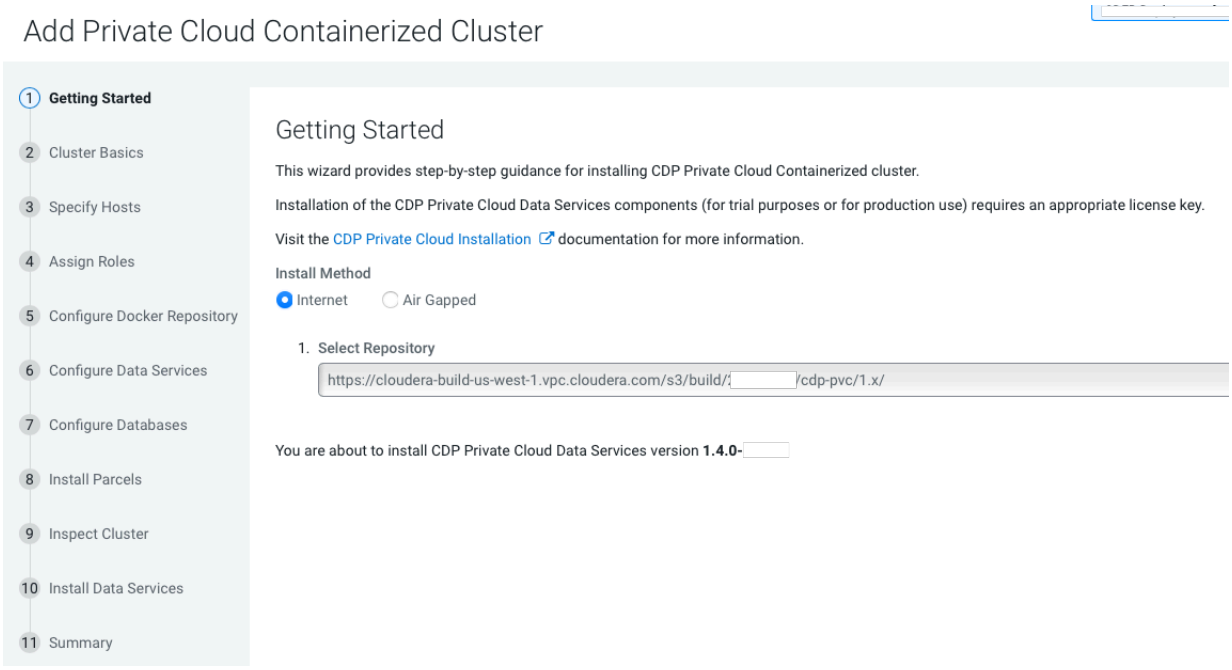


4. In the Select Cluster Type page, select the cluster type as Private Cloud Containerized Cluster and click Continue.

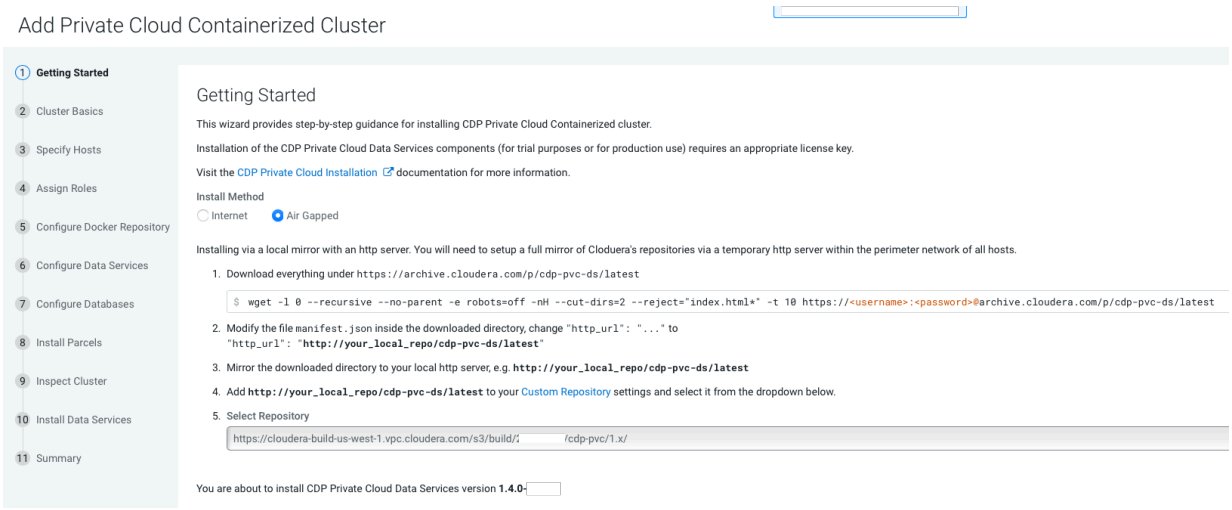


5. On the Getting Started page of the installation wizard, select Internet or Air Gapped as the Install Method. To use a custom repository link provided to you by Cloudera, click Custom Repository. Click Continue.

   Internet install method:

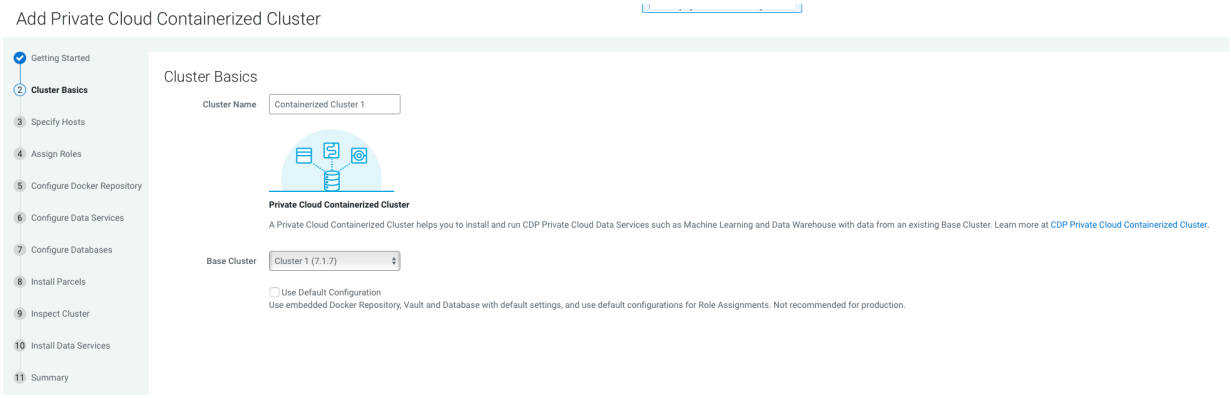


   Air Gapped install method:



   Click Continue.

6. In the Cluster Basics page, type a name for the Private Cloud cluster that you want to create in the Cluster Name field. From the Base Cluster drop-down list, select the cluster that has the storage and SDX services that you want this new Private Cloud Data Services instance to connect with. Click Continue.

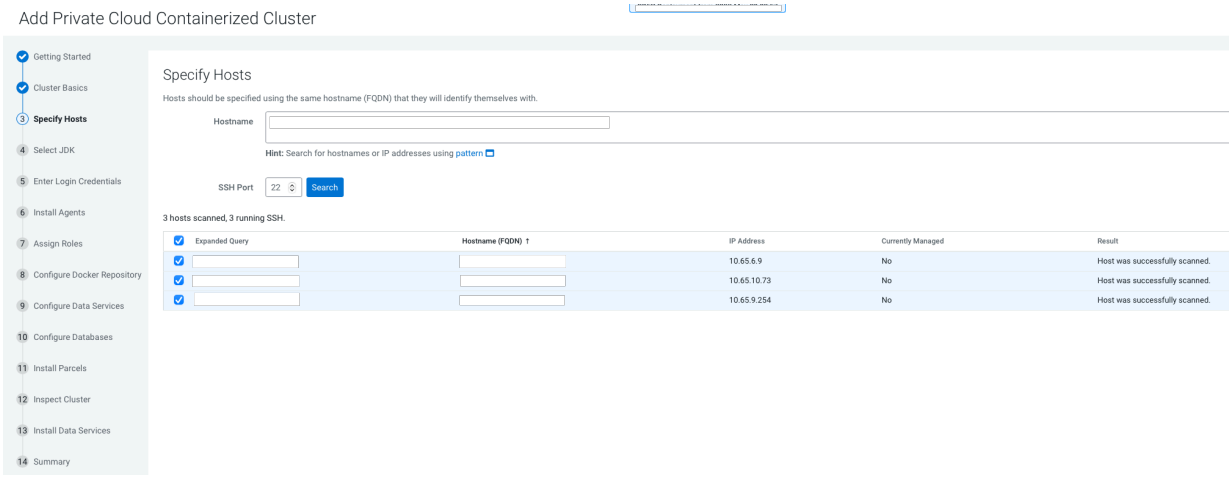


7. In the Specify Hosts page, provide a list of available hosts or you can add new hosts. (If you already added the hosts to Cloudera Manager, enter the Fully Qualified Domain Name (FQDN) for those hosts.) You can provide the FQDN in the following patterns:

   You can specify multiple addresses and address ranges by separating them by commas, semicolons, tabs, or blank spaces, or by placing them on separate lines. Use this technique to make more specific searches instead of searching overly wide ranges.

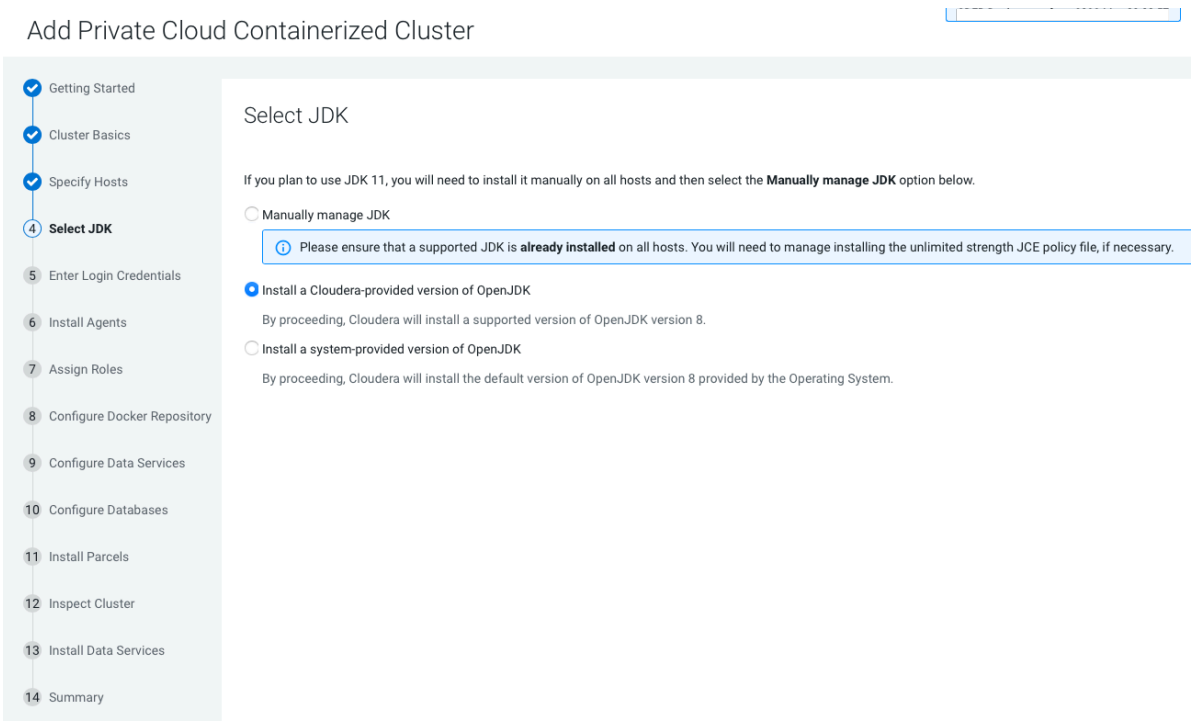
   For example, use host[1-3].network.com to specify these hosts: host1.network.com, host2.network.com, host3.network.com.

   Click Continue.

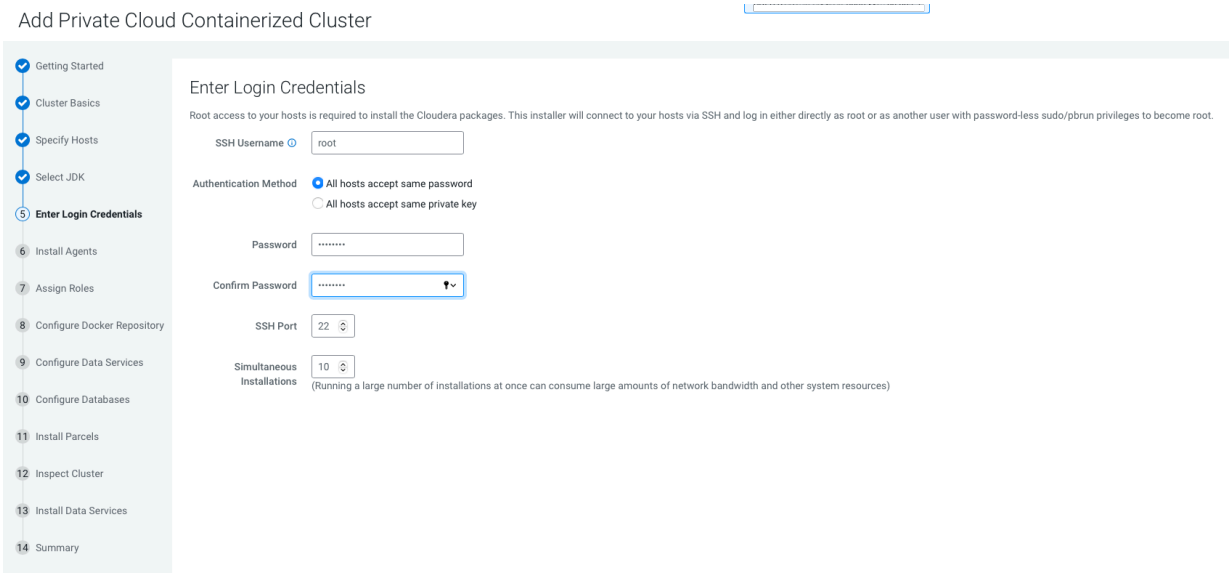


8. In the Select JDK page, select any one from the below options:

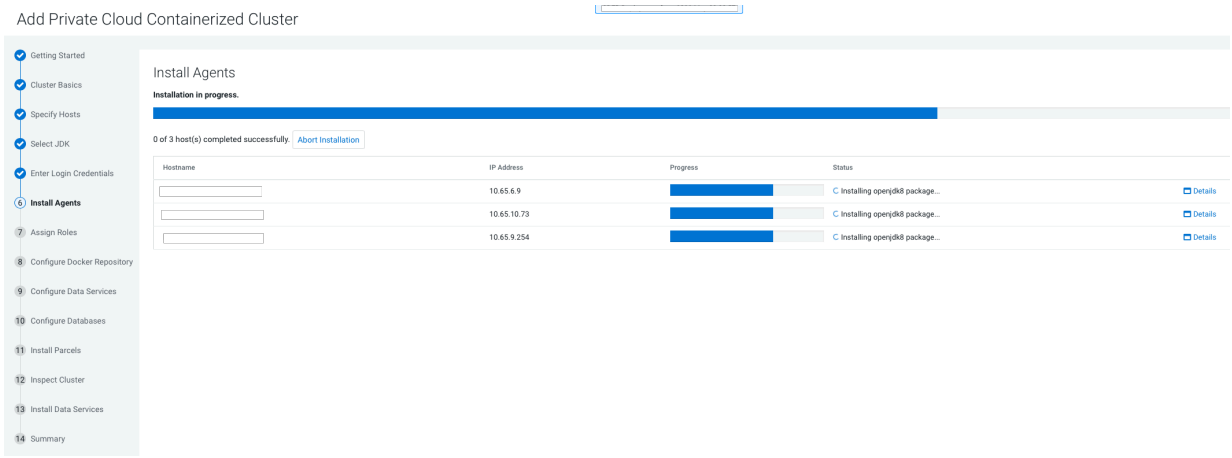
a) Manually manage JDK
b) Install a Cloudera-provided version of OpenJDK
c) Install a system-provided version of OpenJDK



9. In the Enter Login Credentials page select the SSH Username and provide the password.

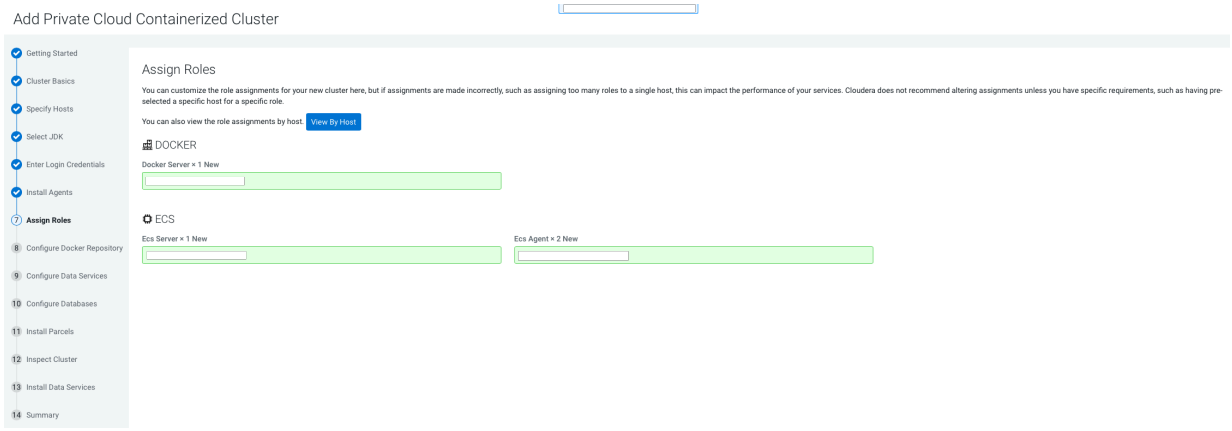


10. The Install Agents page appears.



11. In the Assign Roles page, you can customize the roles assignment for your new Private Cloud Containerized cluster.

Important: Cloudera does not recommend altering assignments unless you have specific requirements such as having selected a specific host for a specific role.



Click Continue.

12. In the Configure Docker Repository page, you must select one of the Docker repository options.

Use an embedded Docker Repository - Copies all images (Internet or AirGapped) to the embedded registry.

Use Cloudera's default Docker Repository - Copies images from Internet to the embedded registry. This uses the default repository that is in manifest.json

Note:

a. Use Cloudera's default Docker Repository option can be selected only if you have selected Internet as the install method.

b. You must ensure that the following ports are opened and allowed. This is required for completing the ECS installation.

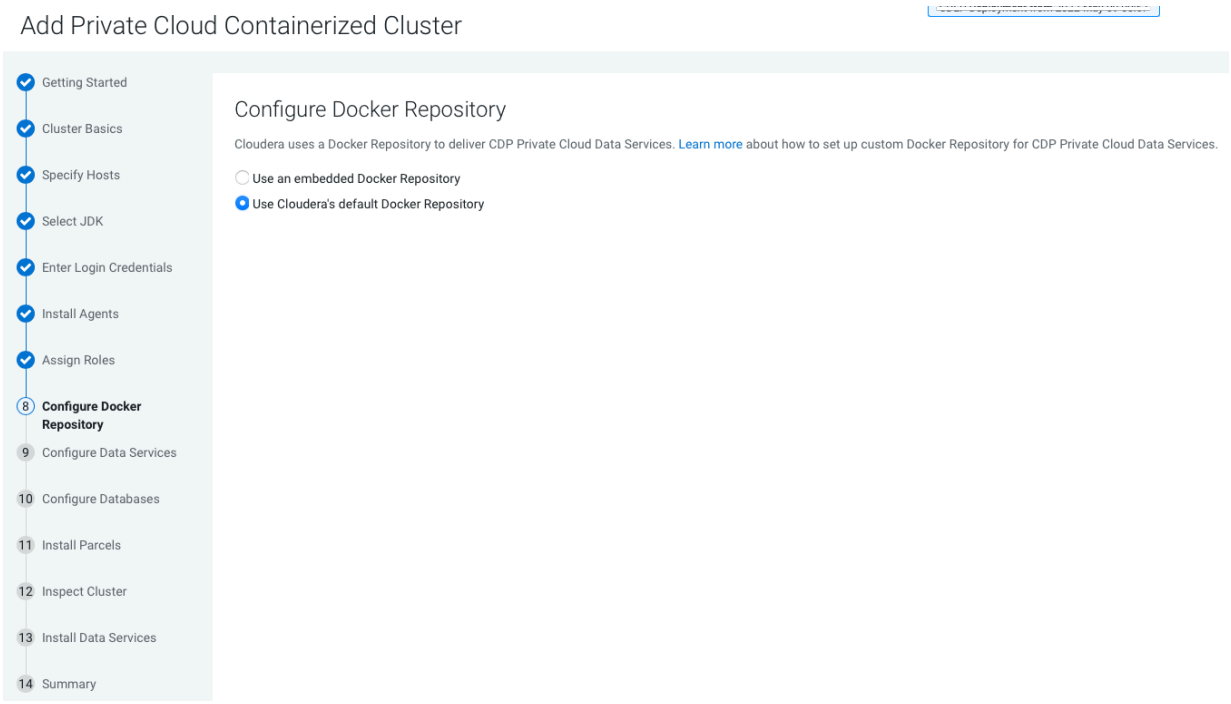
Protocol	**Port**
TCP	7180-7192
TCP	19001
TCP	5000
TCP	9000

c. Inbound rules for ECS Server nodes.

Protocol	**Port**
TCP	9345
TCP	6443
UDP	8472
TCP	10250
TCP	2379
TCP	2380
TCP	30000-32767

d. Inbound Rules for ECS Agent.

Protocol	**Port**
UDP	4789

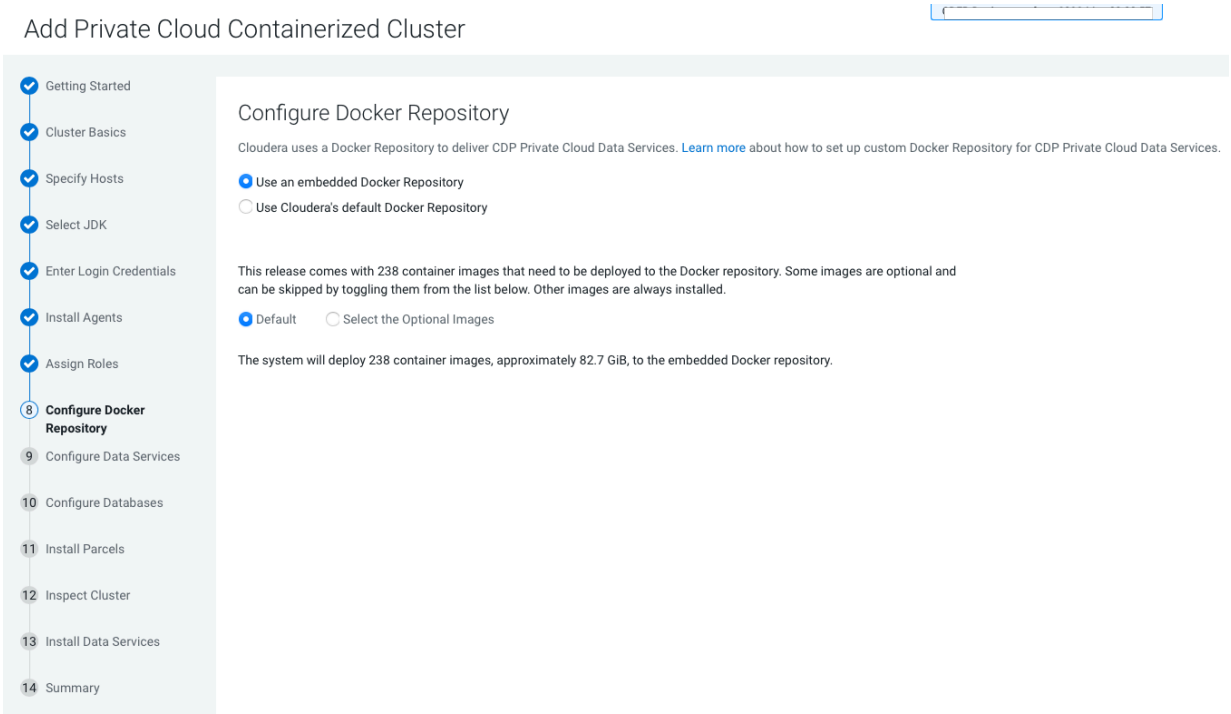


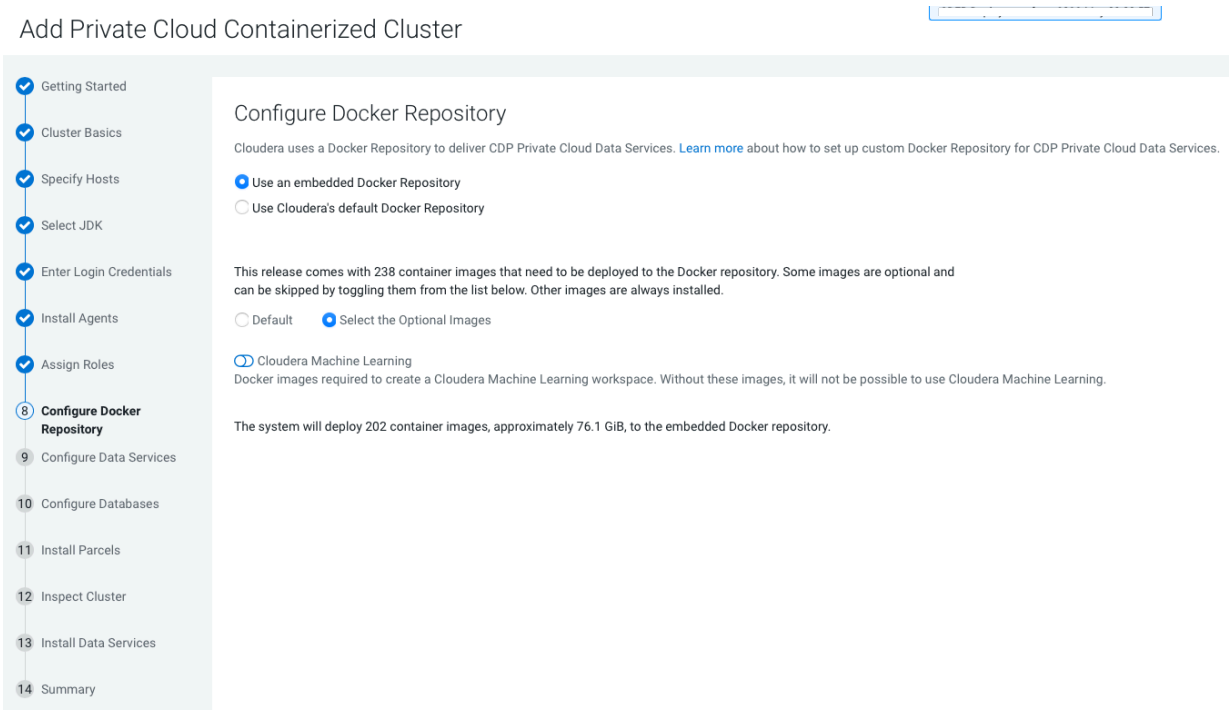
If you select Use an embedded Docker Repository option, then you can download and deploy the Data Services that you need for your cluster.

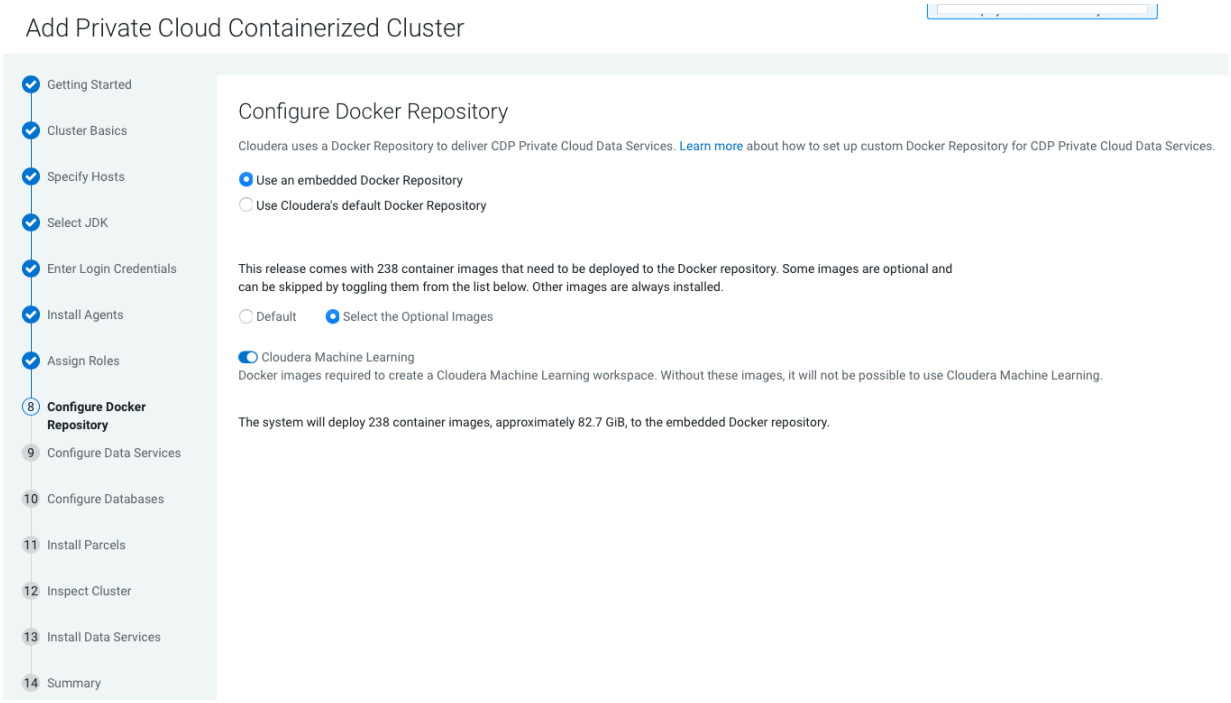
a. By selecting Default, all the data services will be downloaded and deployed.

b. By selecting Select the optional images:

- If you switch off the Machine Learning toggle key, then the Machine Learning runtimes will not be installed.
- If you switch on the Machine Learning toggle key, then the Machine Learning runtimes will be installed.





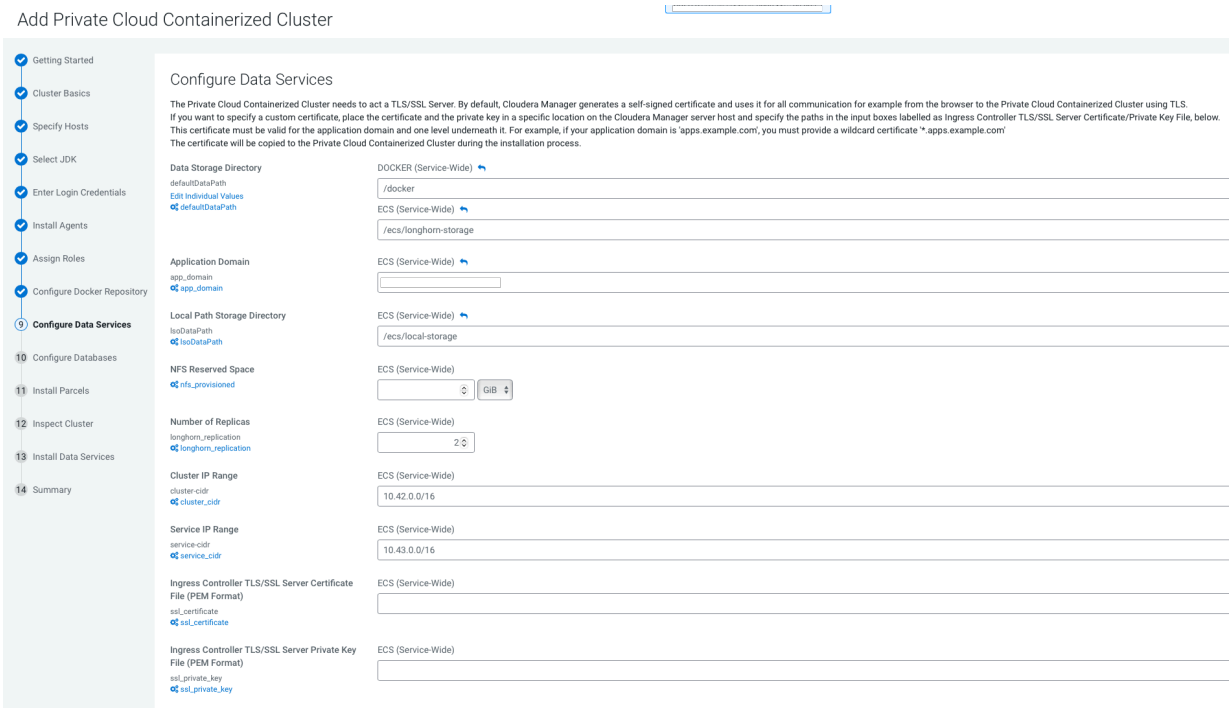


Click Continue.

13. In the Configure Data Services page, you can modify configuration settings such as the data storage directory, number of replicas, and so on. If there are multiple disks mounted on each host with different characteristics (HDD and SSD), then Local Path Storage Directory must point to the path belonging to the optimal storage. Ensure that you have reviewed your changes. If you want to specify a custom certificate, place the certificate and the private key in a specific location on the Cloudera Manager server host and specify the paths in the input boxes

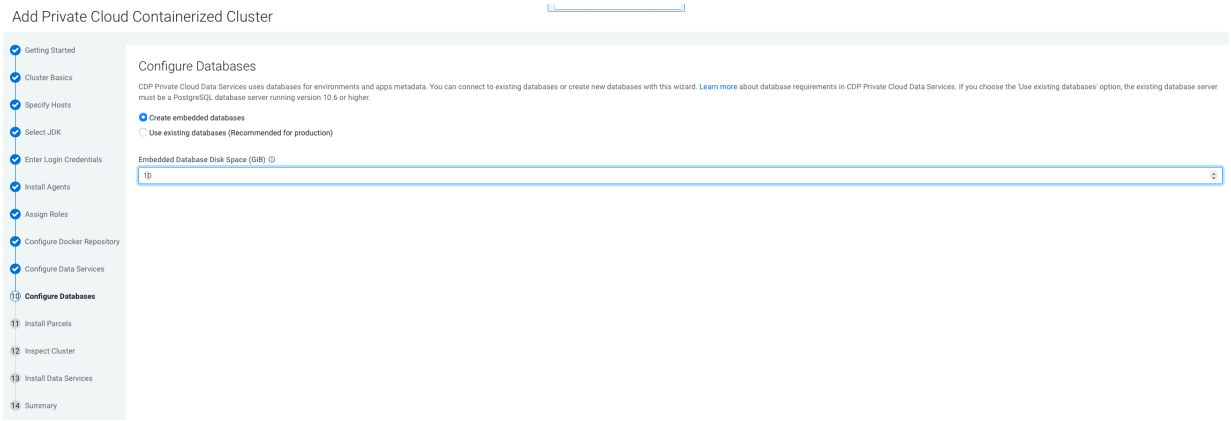
labelled as Ingress Controller TLS/SSL Server Certificate/Private Key File below. This certificate will be copied to the Control Plane during the installation process.

Click Continue.



14. In the Configure Databases page, follow the instructions in the wizard to use your external existing databases with CDP Private Cloud.

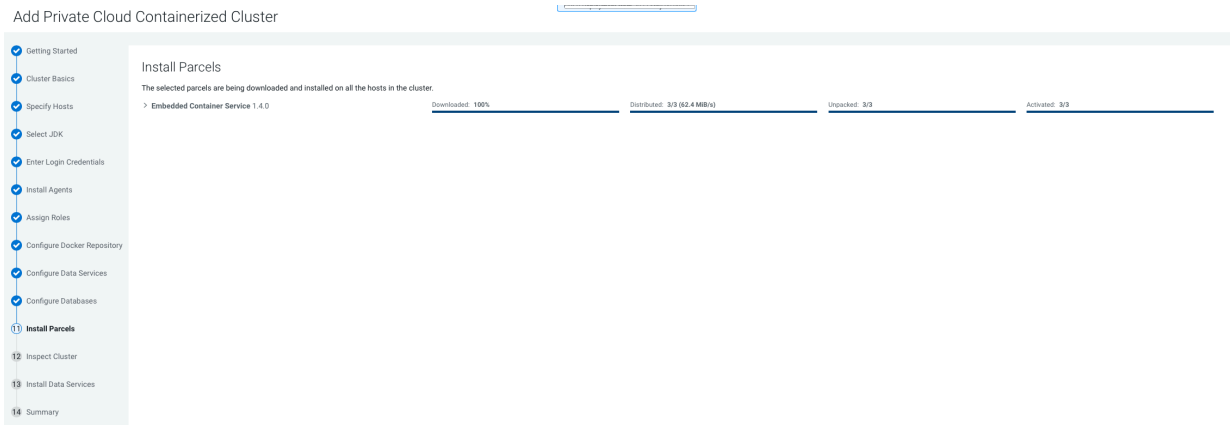
Click Continue.



For production environments, Cloudera recommends that you use databases that you have previously created. These databases must all be on the same host and that host must be a PostgreSQL database server running version 10 or 12.

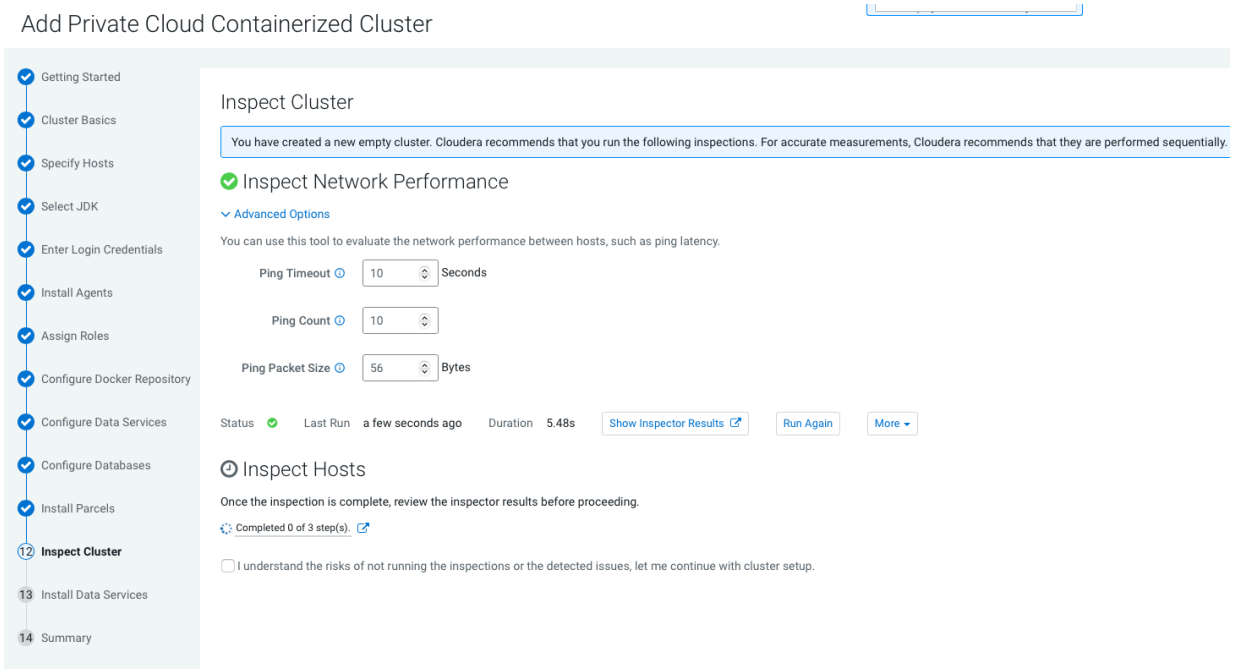
Ensure that you have selected the Use TLS for Connections Between the Control Plane and the Database option if you have plans to use Cloudera Data Warehouse (CDW). Enabling the Private Cloud Base Cluster PostgreSQL database to use an SSL connection to encrypt client-server communication is a requirement for CDW in CDP Private Cloud.

15. In the Install Parcels page, the selected parcels are downloaded and installed on the host cluster. Click Continue.

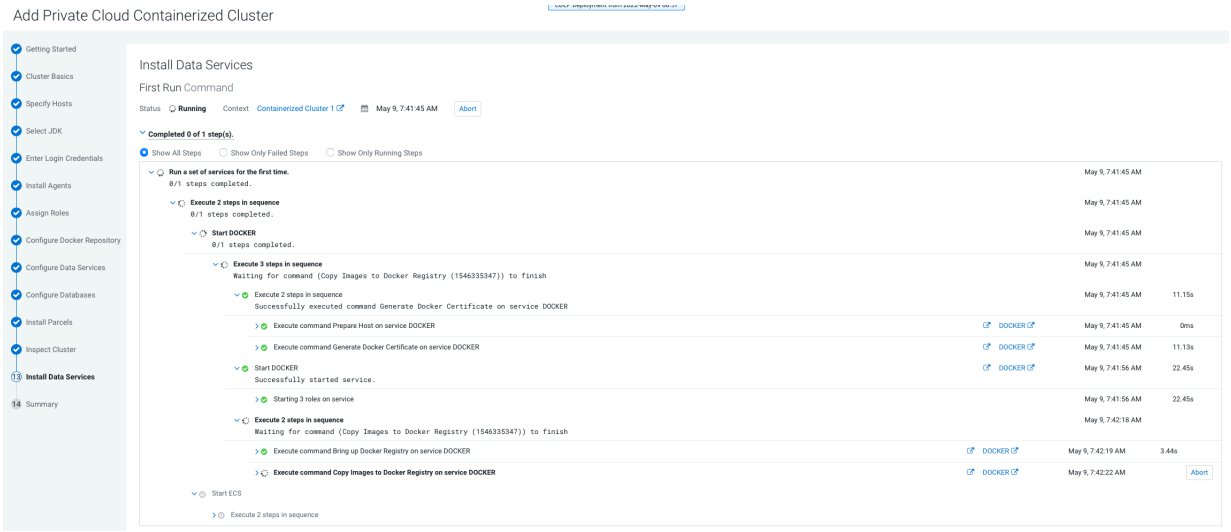


16. In the Inspect Cluster page, you can inspect your network performance and hosts. If the inspect tool displays any issues, you can fix those issues and run the inspect tool again.

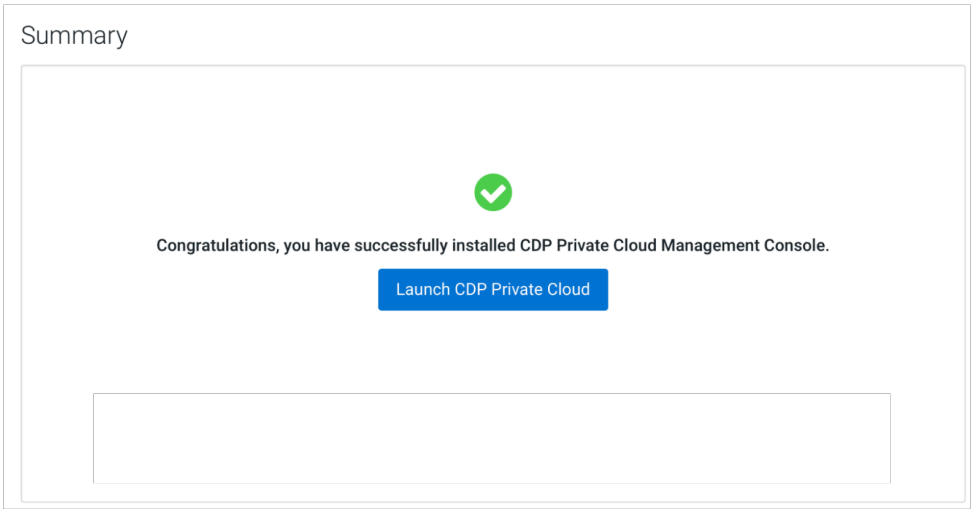
Click Continue.



17. In the Install Data Services page, you will see the installation process.



18. After the installation is complete, you will see the Summary image. You can Launch CDP Private Cloud.



19. After the installation is complete, you can access your Private Cloud Data Services instance from Cloudera Manager > click Open Private Cloud Data Services.

If the installation fails, and you see the following error message in the stderr output during the Install Longhorn UI step, retry the installation by clicking the Resume button.

```
++ openssl passwd -stdin -apr1 + echo 'cm-longhorn:$apr1$gp2nrbtq$1KYPGI0QNl
FJ2lo5sV62l0' + kubectl -n longhorn-system create secret generic basic-auth
--from-file=auth + rm -f auth + kubectl -n longhorn-system apply -f /opt/clo
udera/cm-agent/service/ecs/longhorn-ingress.yaml Error from server (Internal
```

```
Error): error when creating "/opt/cloudera/cm-agent/service/ecs/longhorn-ing
ress.yaml":
Internal error occurred: failed calling webhook "validate.nginx.ingress.kub
ernetes.io": Post "https://rke2-ingress-nginx-controller-admission.kube-syst
em.svc:443/networking/v1/ingresses?timeout=10s": x509: certificate signed by
 unknown authority
```

What to do next

- Click Open Private Cloud Data Services to launch your Private Cloud Experiences instance.
- Log in using the default username and password admin.
- In the Welcome to CDP Private Cloud page, click Change Password to change the Local Administrator Account password.
- Set up external authentication using the URL of the LDAP server and a CA certificate of your secure LDAP. Follow the instructions on the Welcome to CDP Private Cloud page to complete this step.
- Click Test Connection to ensure that you are able to connect to the configured LDAP server.
- Create your first Virtual Warehouse in the CDW Data Service
- Provision an ML Workspace in the CML Data Service
- Add a CDE service in the CDE Data Service

ECS Server High Availability

If you want to enable ECS Server for High Availability after installing ECS, then you must proceed with this section. If you do not want to enable ECS HA, you can safely ignore this section. You must review the note section and unserstand the ECS Server scenarios that are supported before you proceed to the next section.

Note:

- Longhorn replication defaults to two replicas. This can be set only during the installation time. Three or more replicas potentially have performance issues.
- Kubectl delete node <host> permanently removes host from cluster and any data on the host is lost. You must reformat the host before reading to the cluster.
- Single node failure may cause the Control Plane or any other management service to be unavailable. In 1.3.4 or later, it will take several minutes to recover automatically.

ECS Server scenarios

Clusters with only two servers are not supported. This is only for the temporary transition from a single server cluster to a three server cluster.

1. Three or more servers
   - Redundancy requirements:
     - One failure requires three or more servers
     - Two failures require five or more servers
     - For more information see, Fault Tolerance
   - To recover, you must scale-up the ECS Server roles. For more information on adding ECS node to a cluster, see the following section.

2. Two servers to one server
   - Only after a double failure in a three server cluster
   - To recover:
     - Stop the ECS service
     - Remove both the failed ECS server roles and hosts from cluster
     - On the surviving server, run the following command `/opt/cloudera/parcels/ECS/bin/rke2 server --cluster-reset`
     - Start the ECS service
3. Single server
   - No failure supported

Enable ECS Server HA Post Installation

If you want to enable ECS Server for High Availability after installing ECS, then you must proceed with this section. If you do not want to enable ECS HA, you can safely ignore this section.

As a prerequisite, during the installation, you must have installed ECS with 1 master (with app_domain as Load Balancer URL) + agents. When you are adding more masters, ensure that you add Docker server as well.

Adding hosts to the containerised cluster

You must add hosts to the containerised cluster.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Click the Actions drop-down.
4. Click the Add Hosts button. The Add Hosts page appears.
5. Select the Add hosts to cluster option.
6. Select the cluster where you want to add the host from the drop-down list. Click Continue.
7. In the Specify Hosts page, provide a list of available hosts or you can add new hosts. You can provide the Fully Qualified Domain Name (FQDN) in the following patterns: You can specify multiple addresses and address ranges by separating them by commas, semicolons, tabs, or blank spaces, or by placing them on separate lines. Use this technique to make more specific searches instead of searching overly wide ranges.

   For example, use host[1-3].network.com to specify these hosts: host1.network.com, host2.network.com, host3.network.com.

   Click Continue.
8. In the Select Repository page, you must specify the repository location. Choose any one of the following:
   a. Cloudera Repository (Requires direct internet access on all hosts)
   b. Custom Repository
9. In the Select JDK page, select any one from the below options:
   a. Manually manage JDK
   b. Install a Cloudera-provided version of OpenJDK
   c. Install a system-provided version of OpenJDK
10. In the Enter Login Credentials page select the SSH Username and provide the password.
11. The Install Agents page appears. Click Continue.
12. In the Install Parcels page, the selected parcels are downloaded and installed on the host cluster. Click Continue.
13. In the Inspect Hosts page, you can inspect your hosts. If the inspect tool displays any issues, you can fix those issues and run the inspect tool again. Click Continue.
14. In the Select Host Template page, select the hosts.
15. The Deploy Client Config page appears. Click Finish.

Adding Role Instances to Docker Server

You must add role instances to the docker server.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Open Docker Server.
4. Click the Actions drop-down.
5. Click the Add Role Instances button.
6. Select the hosts.
7. Click OK.

Adding Role Instances to Containerised Cluster

You must add the role instances to the containerised cluster.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Click the Actions drop-down.
4. Click the Add Role Instances button. The Add Role Instances page appears.
5. In the Assign Roles page, specify the role assignments for your new roles. Click Continue.
6. In the Review Changes page, click Finish.

Starting Docker Server on Nodes

You must start the Docker server on nodes.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Open Docker Server.
4. Click the Actions for Selected drop-down.
5. Click Start. Docker Server starts.

Starting ECS Server on Nodes

You must start the ECS server on nodes.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Click the Instances tab.
4. Select the nodes by clicking the checkbox
5. Click the Actions for Selected drop-down.
6. Click Start. ECS Server starts.

Refreshing ECS

You must refresh the ECS servers.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Click the Actions drop-down.
4. Click the Refresh button.

Checking Nodes and Pods in the UI

You must check the nodes and pods in the UI.

1. Log in to Cloudera Manager.
2. Navigate to the ECS service.
3. Click the Web UI drop-down.
4. Click ECS Web UI. The Kubernetes web UI page opens in a new tab.
5. Check the Nodes and Pods on the Web UI.

Enable ECS Server HA and promote agents Post ECS Installation

If you want to enable ECS Server for High Availability after installing ECS, then you must proceed with this section.
If you do not want to enable ECS HA, you can safely ignore this section.

As a prerequisite, during the installation, you must have installed ECS with 1 master (with app_domain as Load Balancer URL) + agents. This allows you to promote Agents as masters.

Enabling ECS Server deployment for High Availability

Learn how to enable ECS Server deployment for High Availability by installing a Load Balancer and promoting the existing ECS Agents to ECS Server. By performing this procedure, you will be able to deploy HA on your existing ECS Server.

If you have a production quality ECS cluster, then Cloudera recommends you to use ECS Server High Availability. You can also consider having an ECS Server HA for any non-production ECS cluster that you expect to be available long-term.

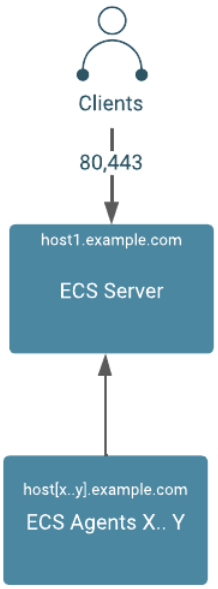
If you have Cloudera Manager 7.5.4, then you must have an ECS cluster installed and configured with a single ECS Server.

You can enable an ECS cluster and convert it to a cluster protected by ECS Server HA. Enabling ECS Server deployment for High Availability involves preparing your cluster, configuring DNS wildcard entry, adding a Load Balancer into the topology, and promoting ECS Agents to the ECS Server. An ECS High Availability cluster must consist of:

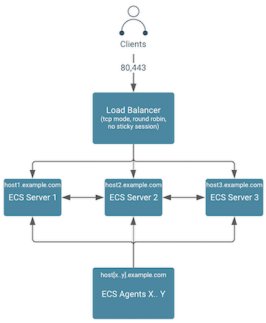
- An odd number of server nodes that will run etcd, the Kubernetes API, and other control plane services. Cloudera recommends a minimum of three ECS Server nodes.
- Two or more agent nodes that are designated to run CDP data services.
- A software or hardware Load balancer using TCP mode (non-terminating https).

Note: A Load Balancer is required for the ECS Server HA. This documentation uses HAProxy as an example. However, Cloudera recommends that you use your production quality Load Balancer technology from commercial vendors.

Architecture of CDP Private Cloud Experiences on single ECS Server



Architecture of CDP Private Cloud Experiences on High Availability



Preparing the cluster for High Availability:

Review the table to understand the requirements for enabling the High Availability.

1. This process has been tested with a minimum of five ECS hosts. However, Cloudera recommends six or more hosts.
2. DNS requirements for ECS High Availability must be fulfilled.

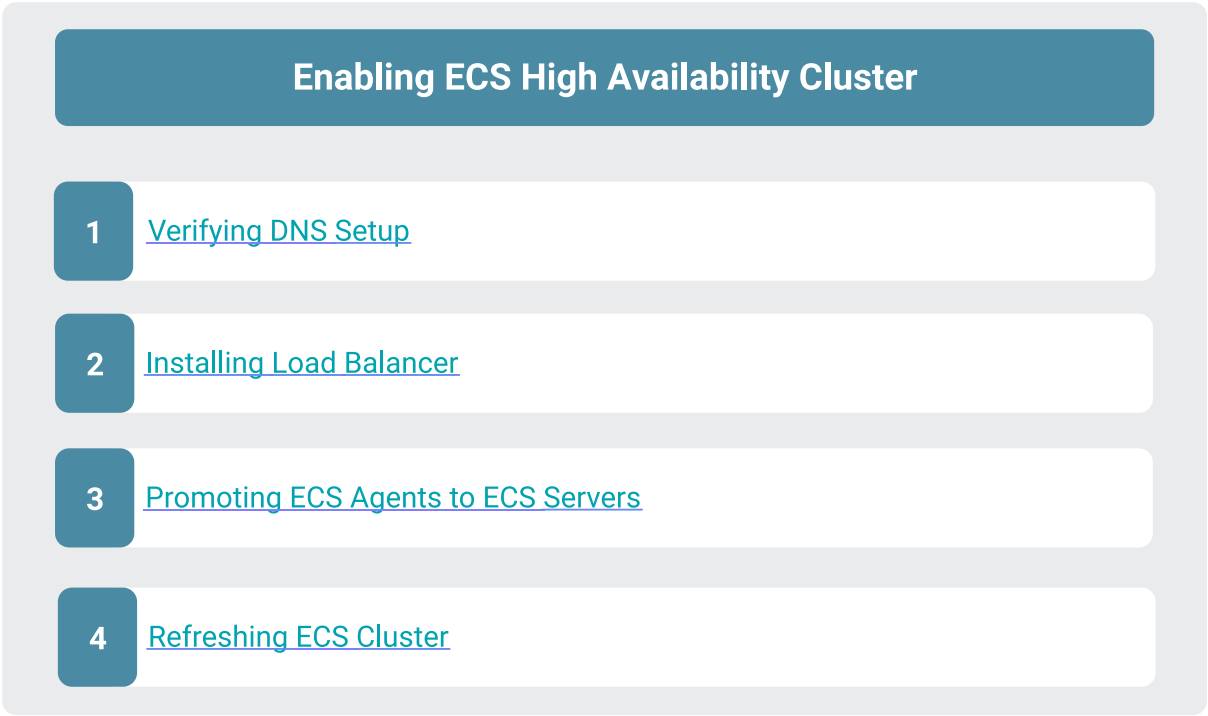
Hostname	Subdomain	Expected Roles	DNS ForwardZone	Reverse Zone PTR
“Wildcard” (hostname = *)	apps.ecs.example.com The string “apps” is required, “ecs” is up to user	Virtual app domain wildcard	“A Record” wildcard (hostname = *), may be a CNAME on certain DNS systems that use text-based config. Resolves to fixed IP of ha_proxy (or VIP of some commerical LB’s)	N
“apps alias”	apps.ecs.example.com	Virtual app domain alias	“CNAME” alias points to A Record of ha_proxy (or VIP). Alternatively, this can be an ARecord with IP of ha_proxy (or VIP)	N/A
HAProxy (or commercial LB)	<domain of your LB>	HA Load Balancer	Depends on vendor/ software	
ecs-master1	example.com	ECS Server 1 Docker server	“A Record” resolves to IP of ecs-master1	Y
ecs-master2	example.com	ECS Server 2 Docker server	“A Record” resolves to IP of ecs-master2	Y
ecs-master3	example.com	ECS Server 3 Docker server	“ARecord” resolves to IP of ecs-master3	Y
ecs-agentN	example.com	ECS Agent N Docker server N	“ARecord” resolves to IP of ecs-agentN	Y

Note:

1. The above table uses a consistent subdomain (“example.com”) but this is not mandatory. To support multiple domains, you must follow certain steps to ensure that the domains are forward and reverse resolvable using DNS, from all Base cluster and ECS cluster hosts (that is through forest/domain level trusts and/or hosts level /etc/resolv.conf config). You must avoid the use of /etc/hosts entries.
2. A predefined wildcard DNS record allows the resolution of *.apps.<app domain name> to the IP address of the Load Balancer. You cannot proceed further until this is in place.

High Level steps to enable an ECS High Availability cluster

Review the high level steps to understand the steps in enabling High Availability.



Note:

1. You must have installed an ECS with one ECS server and other nodes that are ECS Agents.
2. You must have a DNS wildcard record that has an IP address pointing to your Load Balancer (hostname or VIP). For more information, see the KB article.

Verifying DNS setup

You must verify the DNS setup to ensure that the app domain DNS hostname points to the Load Balancer.

Procedure

1. Verify that the app domain DNS hostname has moved from single non-HA ECS Server to the Load Balancer.

Hostname	Expected Roles	DNS
ecs-loadbalancer.example.com	Load Balancer	Resolves to IP of LB host (or VIP). The example uses 10.10.0.99. Both *.apps.ecs.example.com and apps.ecs.example.com resolve to 10.10.0.99.

2. Verify the DNS setup with nslookup.

   Note: You must verify that a random hostname resolves in the wildcard entry. In this example, Cloudera uses foobar.apps.ecs.example.com as the random name. Both entries should resolve to the same IP address.

   For example,

```
$ hosts="apps.ecs.example.com foobar.apps.ecs.example.com"
$ for target in $hosts; do nslookup $target; done

Server: 10.10.xx.xx
Address: 10.10.xx.xx#53

apps.ecs.example.com canonical name = ecs-loadbalancer.example.com.
Name: ecs-loadbalancer.example.com
```

```
Address: 10.10.0.99

Server: 10.10.xx.xx
Address: 10.10.xx.xx#53

Name: foobar.apps.ecs.example.com
Address: 10.10.0.99
```

Results
DNS setup is verified.

What to do next
You must now install the Load Balancer.

Installing Load Balancer
To install the HAProxy Load Balancer, Cloudera uses an example that uses a single instance of HAProxy, configured with round robin balancing and TCP mode. This allows for non-terminating https (https passthrough). The HAProxy service can be configured for High Availability using keepalived.

Before you begin

You must consult your operating system vendor's documentation for requirements and the install guide for configuring HAproxy with keepalived.

To install a HAProxy Load Balancer, you must ssh into the HAProxy host, install, and then configure HAProxy:

Procedure

1. `sudo su -`
2. `yum install haproxy -y`
3. `cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.bak`
4. `cat > /etc/haproxy/haproxy.cfg << EOF`

   global

log	127.0.0.1 local2
chroot	/var/lib/haproxy
pidfile	/var/run/haproxy.pid
user	haproxy
group	haproxy
daemon	

   defaults

mode	tcp
log	global
option	tcplog
option	dontlognull
option	redispatch
retries	3
maxconn	5000

timeout connect	5s
timeout client	50s
timeout server	50s

listen stats

```
bind *:8081
mode http
stats enable
stats refresh 30s
stats uri /stats
monitor-uri /healthz
```

frontend fe_k8s_80

```
bind *:80
default_backend be_k8s_80
```

backend be_k8s_80

```
balance roundrobin
mode tcp
server ecs-server1.example.com 10.10.0.1:80 check
server ecs-server2.example.com 10.10.0.2:80 check
server ecs-server3.example.com 10.10.0.3:80 check
```

frontend fe_k8s_443

```
bind *:443
default_backend be_k8s_443
```

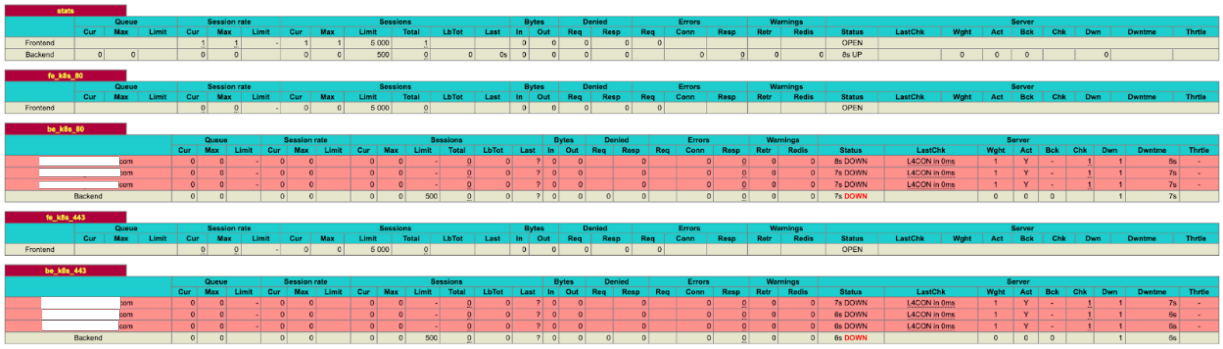
backend be_k8s_443

```
balance roundrobin
mode tcp
server ecs-server1.example.com 10.10.0.1:443 check
server ecs-server2.example.com 10.10.0.2:443 check
server ecs-server3.example.com 10.10.0.3:443 check
```

EOF

```
systemctl enable haproxy
systemctl restart haproxy
systemctl status haproxy
```

5. You can verify that all the hosts are shown from the HAproxy UI. However, at this point the hosts are not listening to the configured ports.



Important: Since you already have an ECS cluster running, you must alter your DNS wildcard to point to the IP address of the HAProxy server. You cannot change the Application Domain configured through the ECS wizard. So you must ensure that you send all ingress traffic to the HAProxy IP address by making that change in the IP address of your wildcard DNS Record.

Note:

a. Application Domain (app_domain property in Cloudera Manager) maps to your wildcard DNS record (For example, app_domain ecs.example.com maps to your DNS entry *.apps.ecs.example.com)

b. The resolved IP address must be the host IP (or VIP) of your Load Balancer. For more information, see the Verify DNS Step 5 above.

Results

Load Balancer is now installed.

Promoting ECS Agents to ECS Servers

You must promote ECS Agents to ECS Servers.

About this task

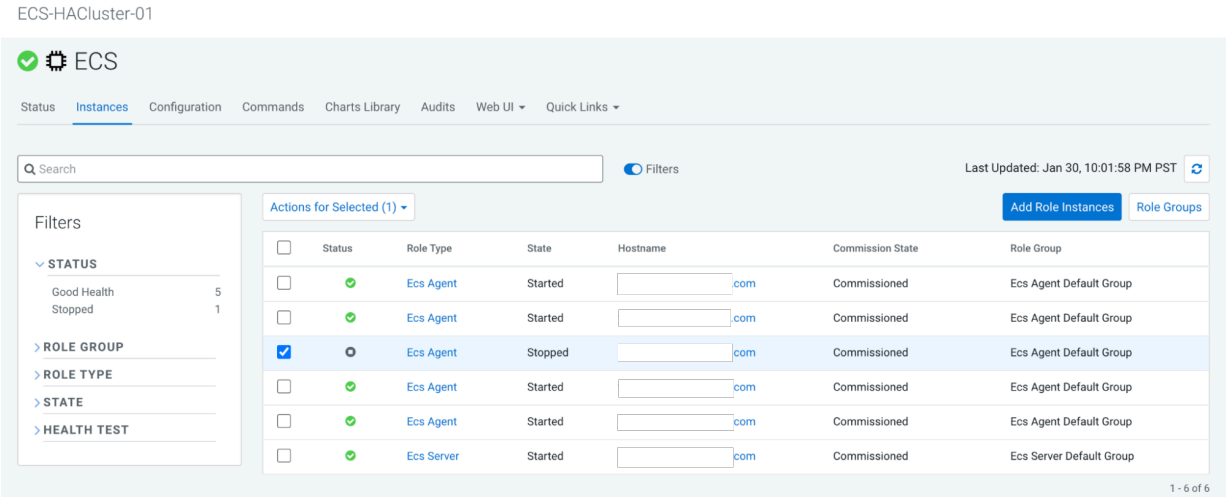
After installing the Load Balancer, you must reconfigure the existing ECS Agents to ECS Servers. This process is called Promoting the agents to Servers. You must promote only one agent at a time. This procedure is explained using an example where you promote the ECS agent on agent1.example.com and then promote the ECS agent on agent2.example.com.

Procedure

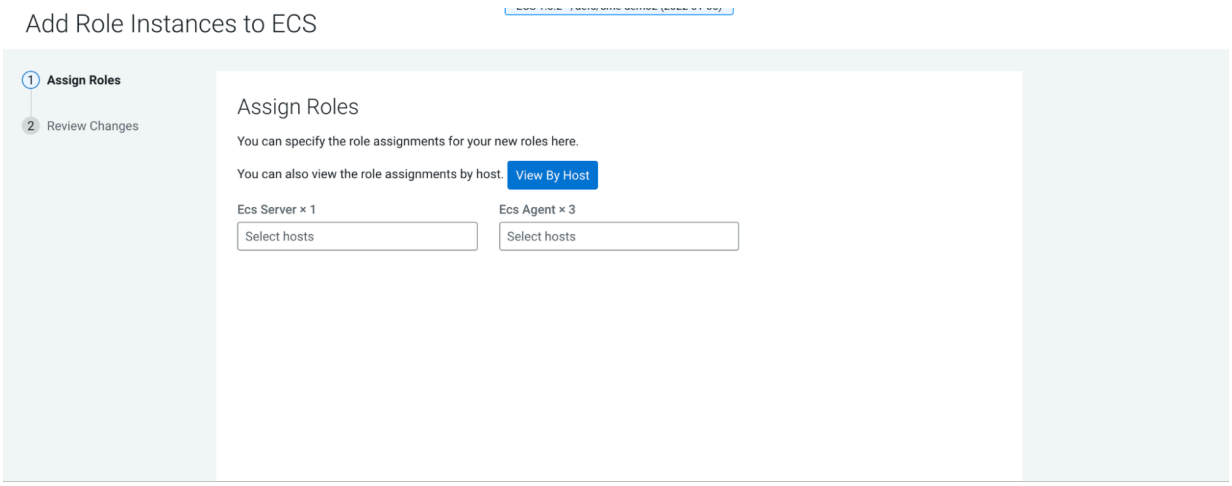
1. Prepare the agent node for promotion by running the following commands on the command line of your ECS Server host. `sudo /var/lib/rancher/rke2/bin/kubectl --kubeconfig=/etc/rancher/rke2/rke2.yaml get nodes sudo /var/lib/rancher/rke2/bin/kubectl --kubeconfig=/etc/rancher/rke2/rke2.yaml drain agent1.example.com --ignore-daemonsets --delete-emptydir-data.`

Note: This may take a few minutes.

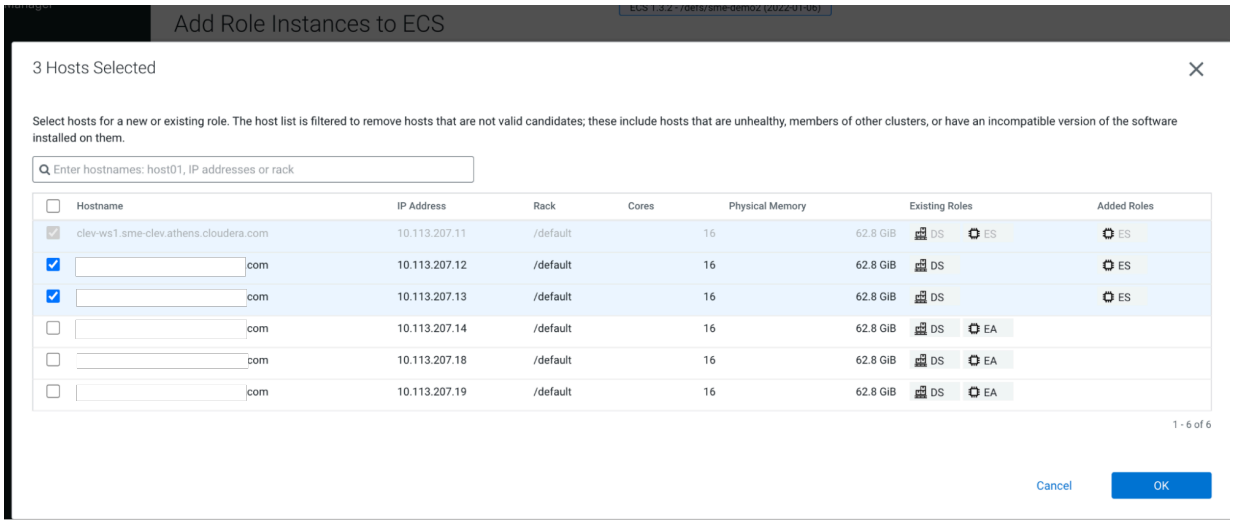
2. In Cloudera Manager, navigate to ECS Cluster >> ECS. Stop the ECSAgent running on agent1 and then delete the agent.

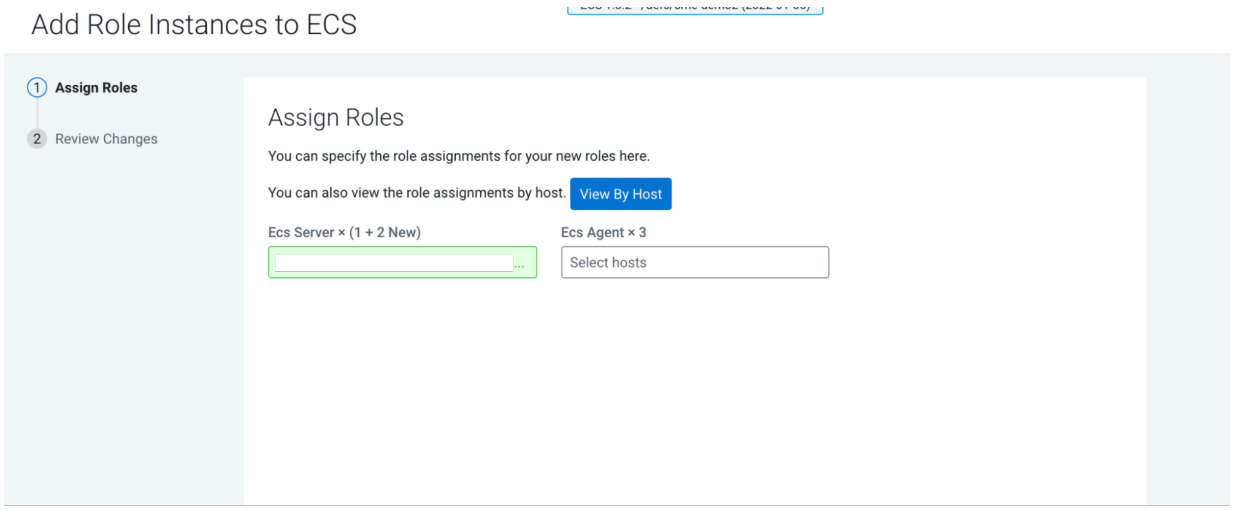


3. In Cloudera Manager, navigate to ECS Cluster >> ECS. Click Add Role Instances.

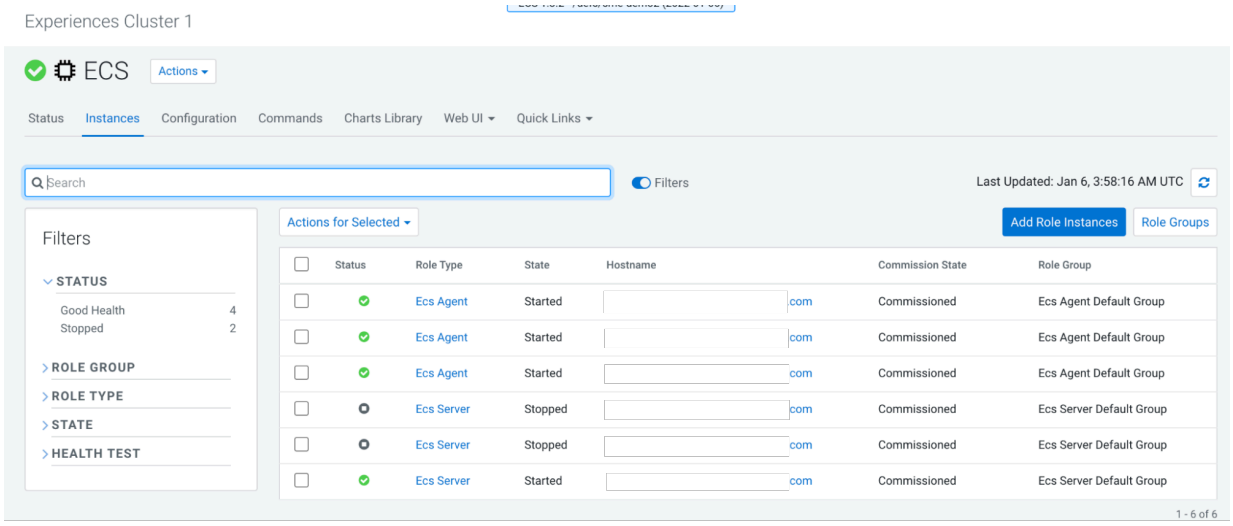


4. Add the available host agent1 as an ECS Server in the Add Role Instances to ECS pop-up. Click Ok.

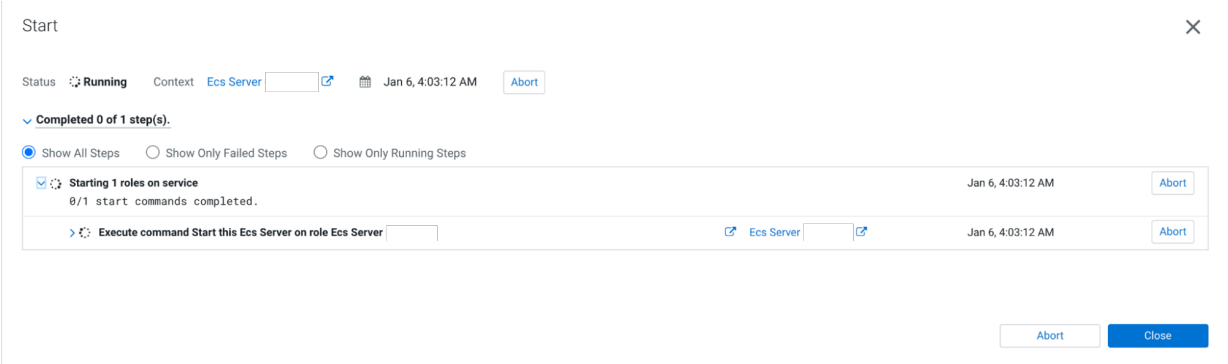




5. Click Continue.

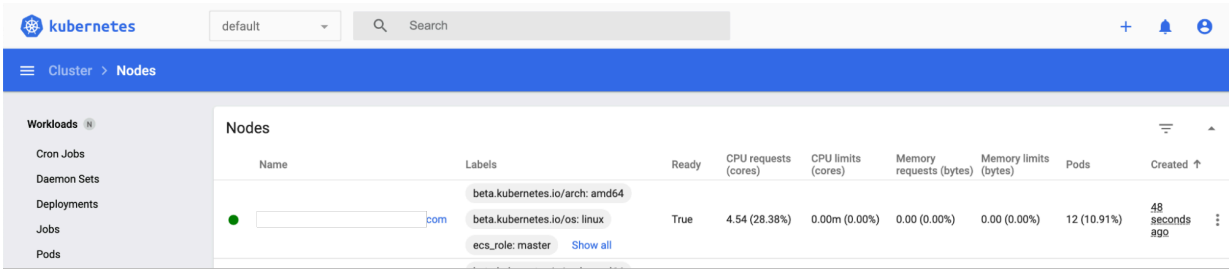


6. Start the new ECS Server from ECS Instances view. For example, start ECSServer on agent1.



7. On the command line, uncordon the node by running the following command: `sudo /var/lib/rancher/rke2/bin/kubectl --kubeconfig=/etc/rancher/rke2/rke2.yaml uncordon agent1.example.com`
8. Confirm the node's status from webUI or the command line by running the command `sudo /var/lib/rancher/rke2/bin/kubectl --kubeconfig=/etc/rancher/rke2/rke2.yaml get nodes`.

Note: Do not proceed until node status is Ready. This may take several minutes.



What to do next

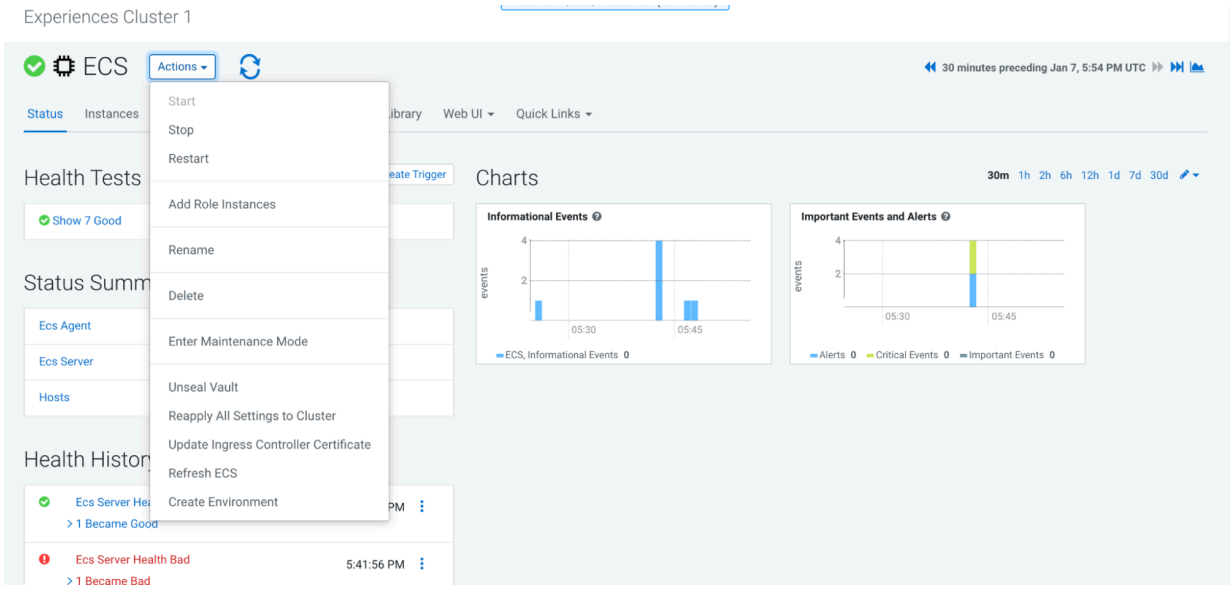
When agent1 is ready, you can promote the next agent agent2. To promote the next agent, you must perform steps 1-8 again, the example uses agent2.example.com.

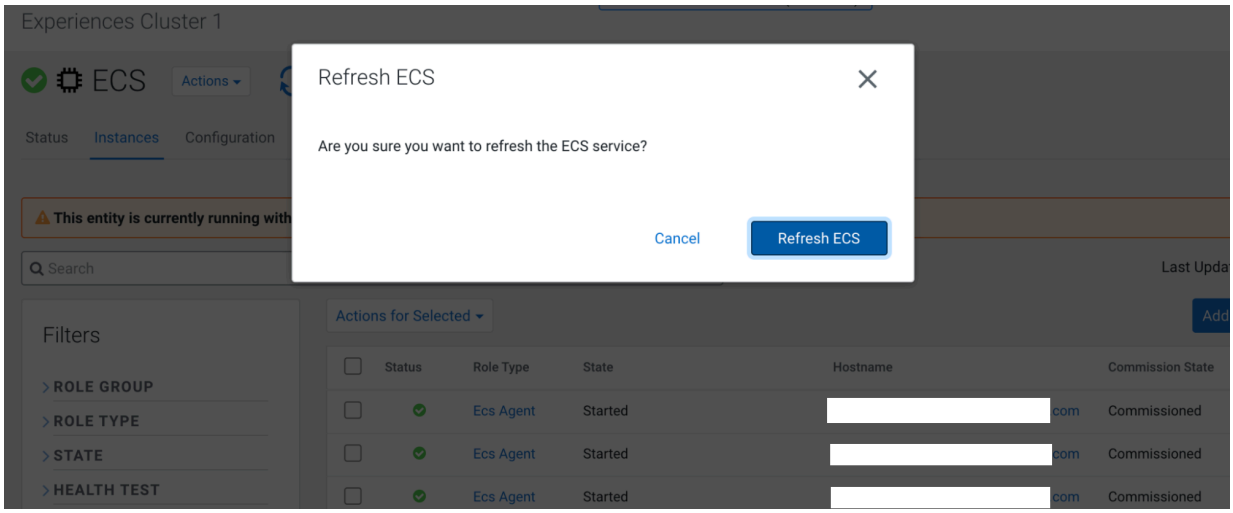
Refreshing ECS

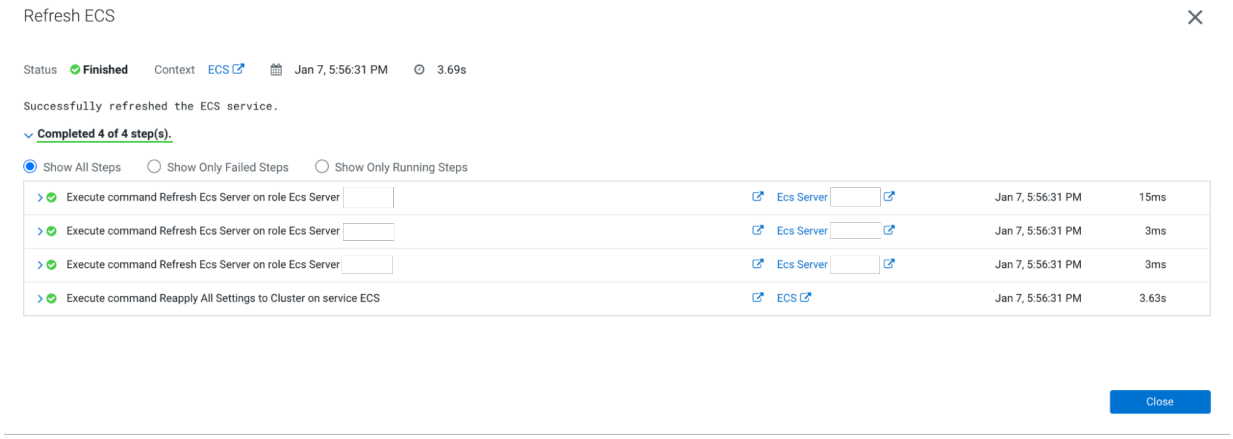
After all the ECS Agents are promoted to ECS Servers, you must log in to Cloudera Manager and refresh the ECS cluster.

Procedure

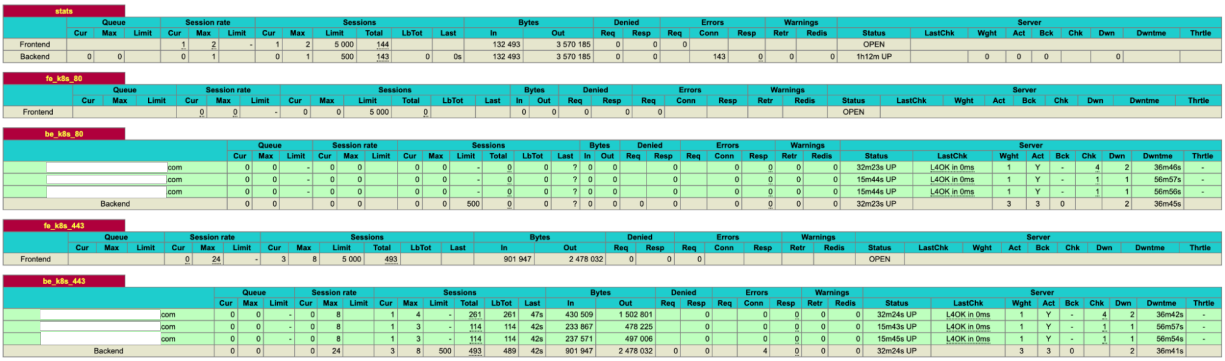
1. Navigate to ECS Cluster >> ECS view >> Actions >> Refresh ECS. This sets the ingress proxy so that all three servers are eligible to process incoming commands.







2. Confirm that all backends of HAProxy display the status UP. This may take several minutes.



stats																																						
	Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server																	
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle								
Frontend				1	2	-	1	2	5 000	144			132 493	3 570 185	0	0	0					OPEN																
Backend	0	0		0	1		0	1	500	143	0	0s	132 493	3 570 185	0	0		143	0	0	0	1h12m UP		0	0	0		0									

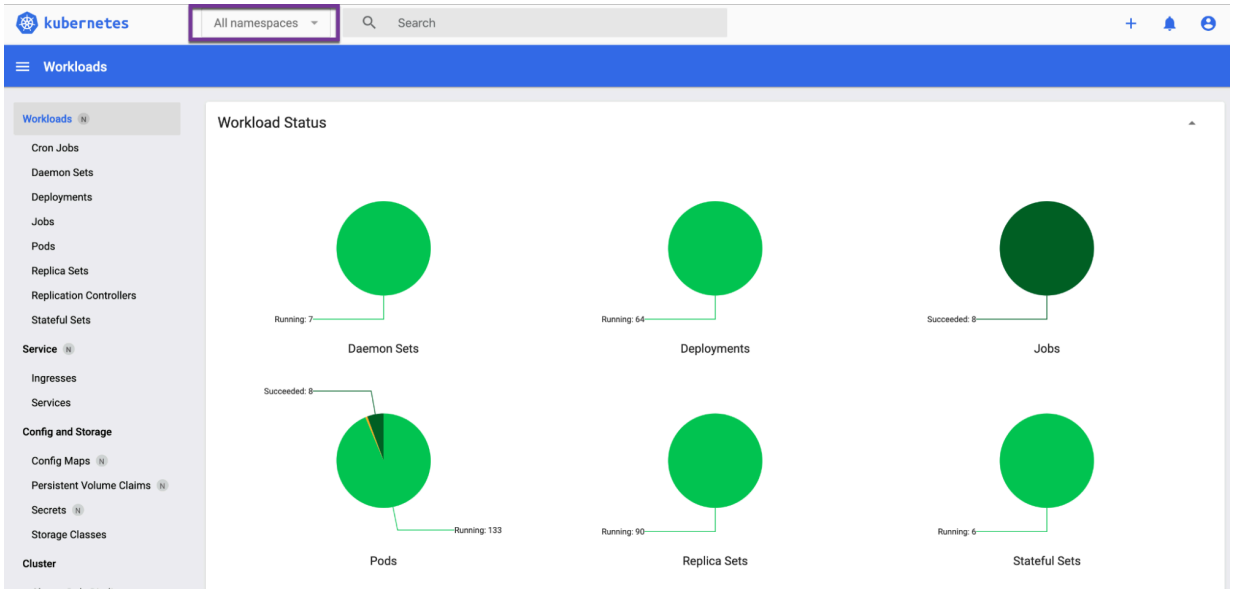
fe_k8s_80																																						
	Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server																	
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle								
Frontend				0	0	-	0	0	5 000	0			0	0	0	0	0					OPEN																

be_k8s_80																																						
		Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server																	
		Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle								
	com	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	32m23s UP	L4OK in 0ms	1	Y	-	4	2	36m46s	-							
	com	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	15m44s UP	L4OK in 0ms	1	Y	-	1	1	56m57s	-							
	com	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	15m44s UP	L4OK in 0ms	1	Y	-	1	1	56m56s	-							
Backend		0	0		0	0		0	0	500	0	0	?	0	0		0		0	0	0	0	32m23s UP		3	3	0		2	36m45s								

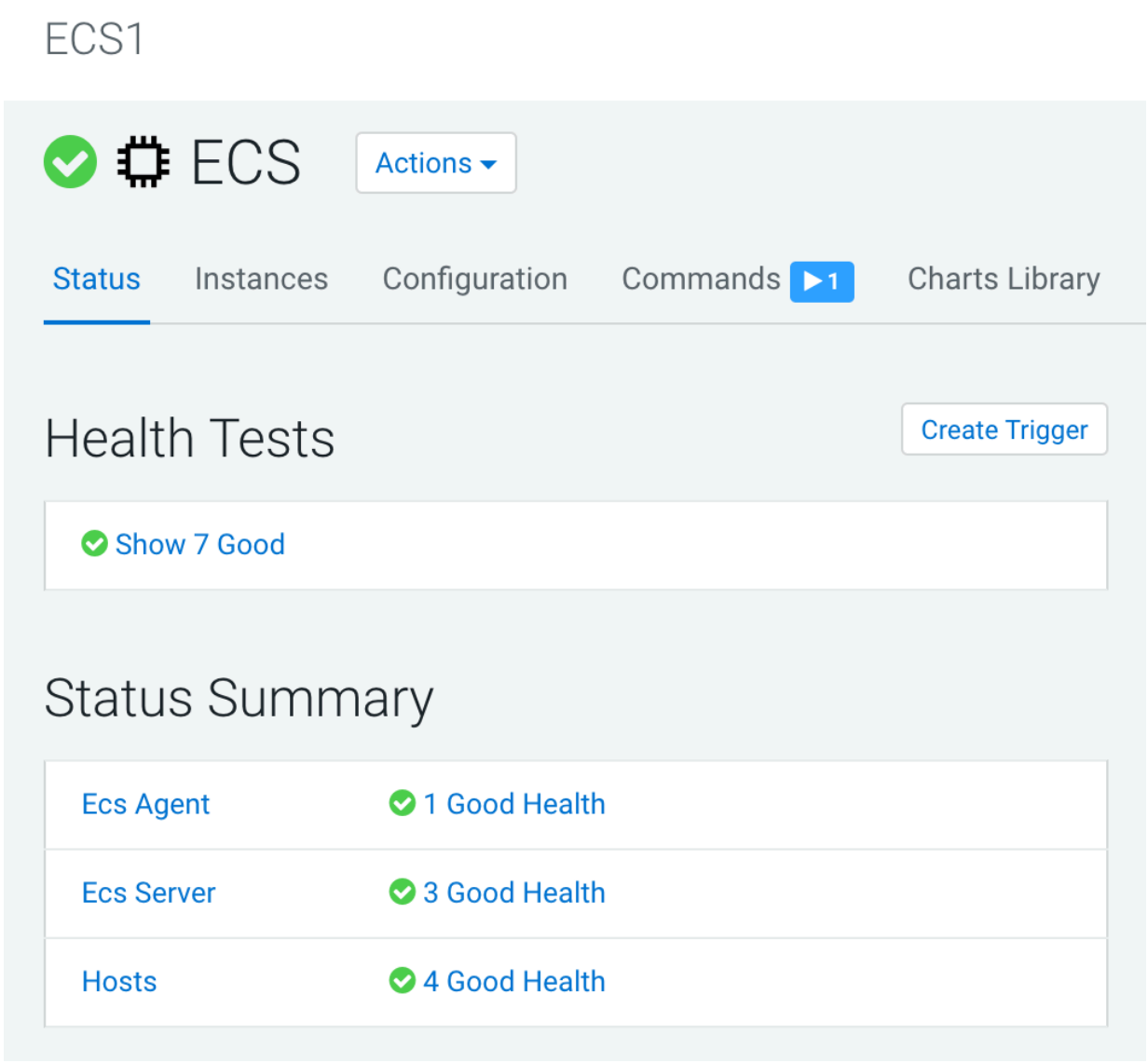
fe_k8s_443																																						
	Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server																	
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle								
Frontend				0	24	-	3	8	5 000	493			901 947	2 478 032	0	0	0					OPEN																

be_k8s_443																																						
		Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server																	
		Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle								
	com	0	0	-	0	8		1	4	-	261	261	47s	430 509	1 502 801		0		0	0	0	0	32m24s UP	L4OK in 0ms	1	Y	-	4	2	36m42s	-							
	com	0	0	-	0	8		1	3	-	114	114	42s	233 867	478 225		0		0	0	0	0	15m43s UP	L4OK in 0ms	1	Y	-	1	1	56m57s	-							
	com	0	0	-	0	8		1	3	-	114	114	42s	237 571	497 006		0		0	0	0	0	15m45s UP	L4OK in 0ms	1	Y	-	1	1	56m54s	-							
Backend		0	0		0	24		3	8	500	493	489	42s	901 947	2 478 032	0	0		4	0	0	0	32m24s UP		3	3	0		2	36m41s								

3. Confirm that all pods are green in the ECS webUI >> (All Namespaces) >> Workloads.



4. Confirm that there are no alerts in the ECS service.



Results

High Availability is now deployed on your ECS cluster.

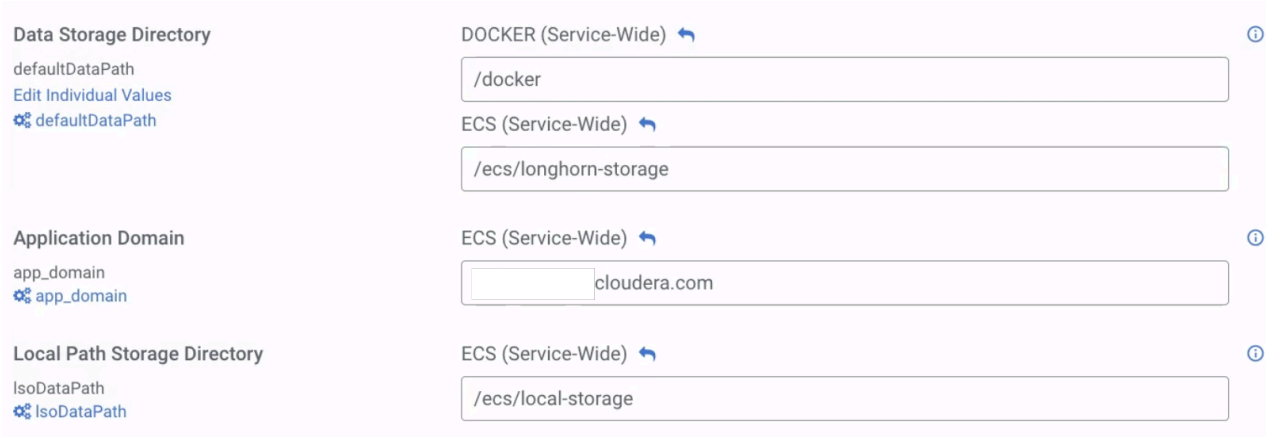
Manually uninstalling ECS from a cluster

You can manually uninstall ECS from your cluster.

Before you begin

Before performing this procedure, ensure that you have activated the ECS parcel on the cluster hosts.

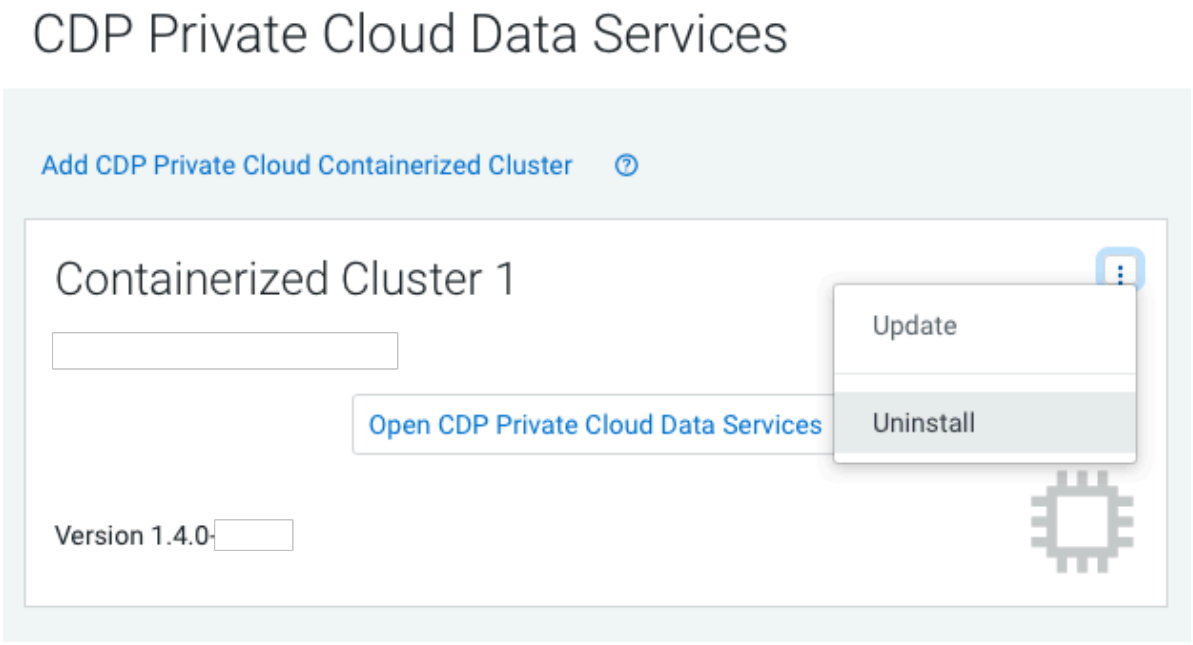
During the installation time of ECS, the directory for Longhorn and the LSO are decided by Cloudera Manager and defaults to /ecs.



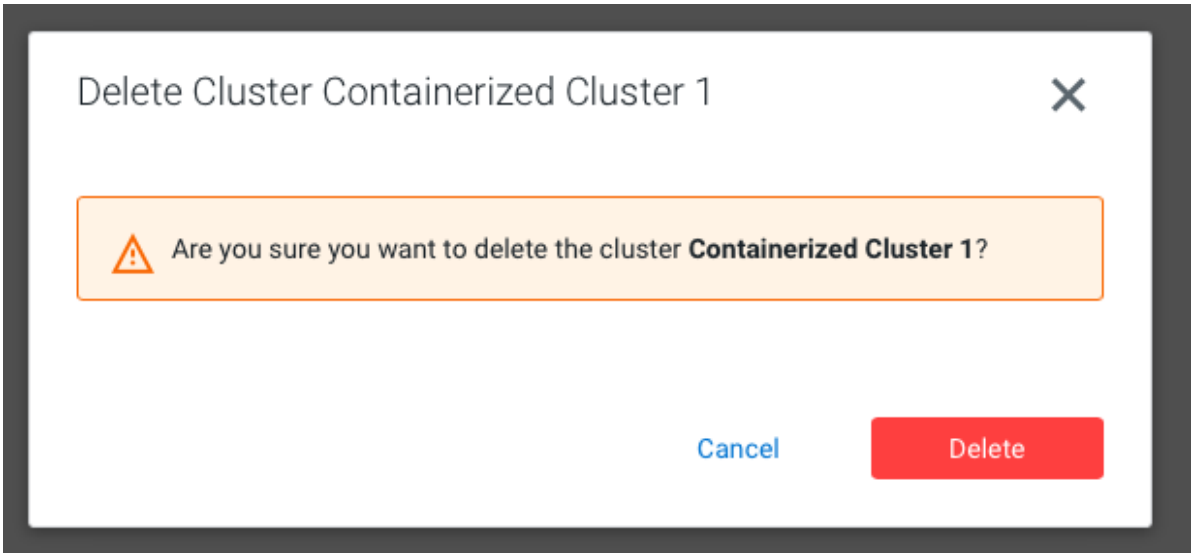
Procedure

1. On each host in the cluster:
   a) /opt/cloudera/parcels/ECS/docker/docker container stop registry
   b) /opt/cloudera/parcels/ECS/docker/docker container rm -v registry
   c) /opt/cloudera/parcels/ECS/docker/docker image rm registry:2
2. Stop the ECS cluster in Cloudera Manager
3. On each host:
   a) cd /opt/cloudera/parcels/ECS/bin
   b) ./rke2-killall.sh # usually 2 times is sufficient
   c) ./rke2-uninstall.sh
   d) rm -rf /ecs/* # assumes the default defaultDataPath and lsoDataPath
   e) rm -rf /var/lib/docker_server/* # deletes the auth and certs
   f) rm -rf /etc/docker/certs.d/* # delete the ca.crt
   g) rm -rf /docker # assumes the default defaultDataPath for docker

4. Delete the ECS cluster in Cloudera Manager.
   a) In Cloudera Manager, navigate to CDP Private Cloud Data Services 1.4.0/1.4.0-H1 and click . Click Uninstall.



   b) The Delete Cluster wizard appears. Click Delete.



5. Clean IPtables on each host:

```
echo "Reset iptables to ACCEPT all, then flush and delete all other chai
ns";
                        declare -A chains=( [filter]=INPUT:FORWARD:OUTPUT
 [raw]=PREROUTING:OUTPUT [mangle]=PREROUTING:INPUT:FORWARD:OUTPUT:POSTROUT
ING [security]=INPUT:FORWARD:OUTPUT [nat]=PREROUTING:INPUT:OUTPUT:POSTRO
UTING );
                        for table in "${!chains[@]}"; do
                        echo "${chains[$table]}" | tr : $"\n" | while IFS=
 read -r;
                        do sudo iptables -t "$table" -P "$REPLY" ACCEPT
```

```
                        done
                        sudo iptables -t "$table" -F
                        sudo iptables -t "$table" -X
                        done
```

Note: Alternatively, an experimental script is available. This script combines steps three through five. The script is available here: https://github.com/cloudera-labs/snippets/blob/main/private-cloud/kill-2-rke .sh script

6. Reboot the host(s).
7. Before you install ECS again, ensure that the IP tables list is empty by executing the following command: #iptable s -L

Upgrading

Upgrading Cloudera Manager

You must use the Cloudera Manager version 7.6.5 to set up the Private Cloud Experiences cluster.

If you already have a Private Cloud Base cluster setup using an earlier version of Cloudera Manager, you must first upgrade the Cloudera Manager version to Cloudera Manager 7.6.5 release and then begin the ECS installation.

For more information, see Upgrading Cloudera Manager.

Related Information

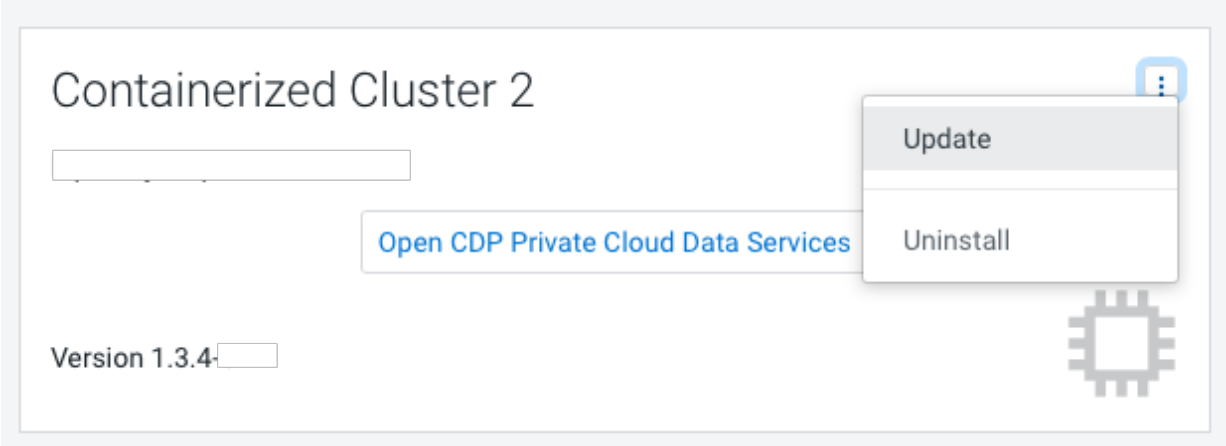
Upgrading Cloudera Manager

Update from 1.4.0 to 1.4.0-H1

You can update your existing CDP Private Cloud Data Services 1.4.0 to 1.4.0-H1 without requiring an uninstall.

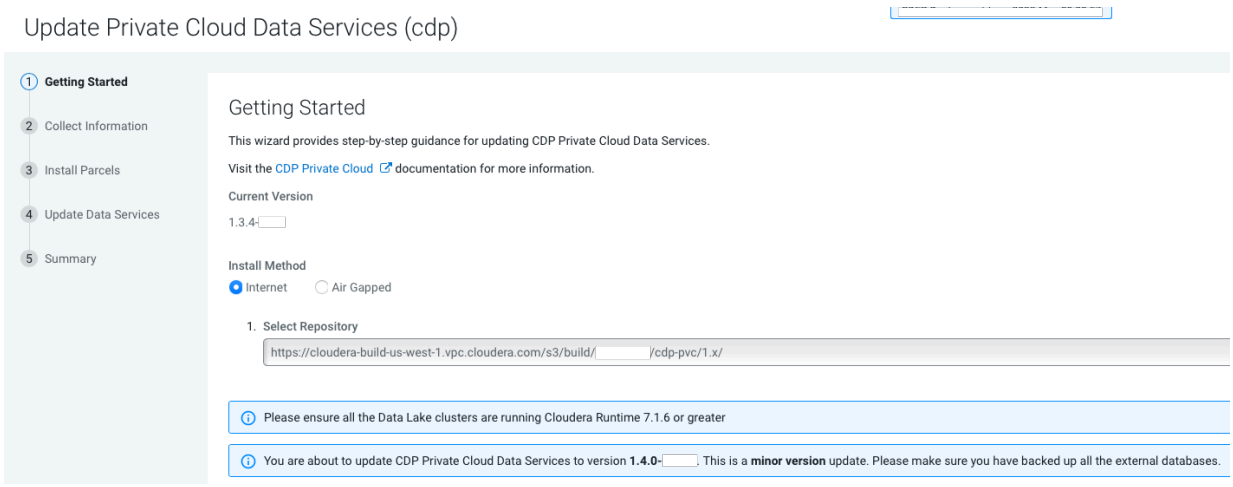
Procedure

1. In Cloudera Manager, navigate to CDP Private Cloud Data Services 1.4.0 and click . Click Update.

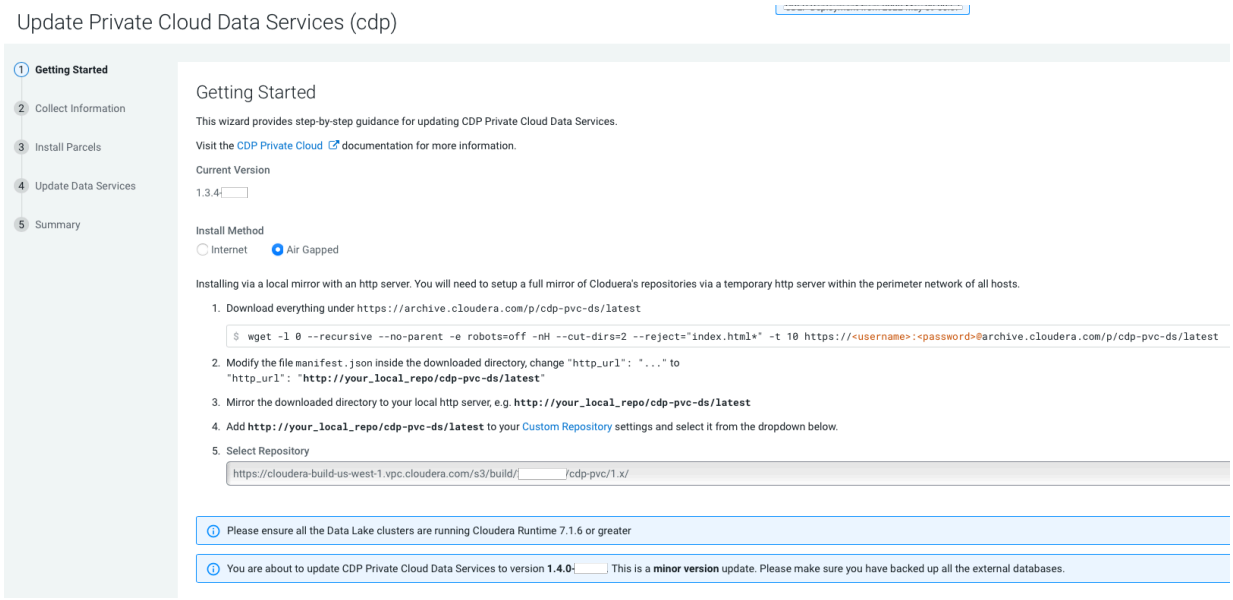


2. On the Getting Started page, you can select the Install method - Air Gapped or Internet and proceed.

   Internet install method

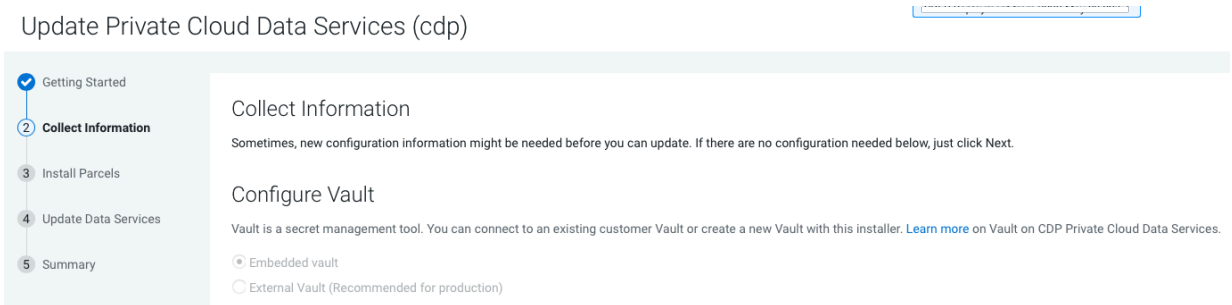


   Air Gapped install method

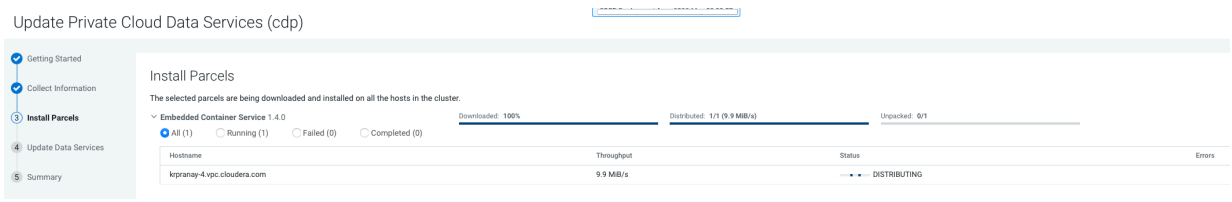


   Click Continue.

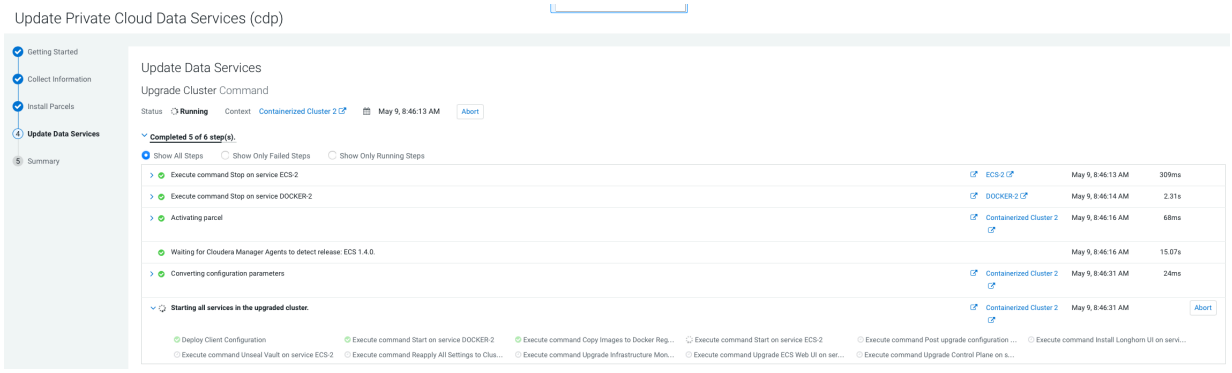
3. On the Collect Information page, click Continue.



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: Unable to start ECS server role on ECS server host.

  Workaround:

  a. SSH to the affected host.
  b. Search for the rke2-killall.sh script and run it.
  c. Start the ECS server role on the host from Cloudera Manager.
  d. Resume the upgrade by running any command that was affected by the upgrade failure.
- Error message: Code: 503. Errors: * Vault is sealed.

  Workaround: Longhorn repairs by itself. Wait until the Longhorn repair is complete.
- 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
  ```

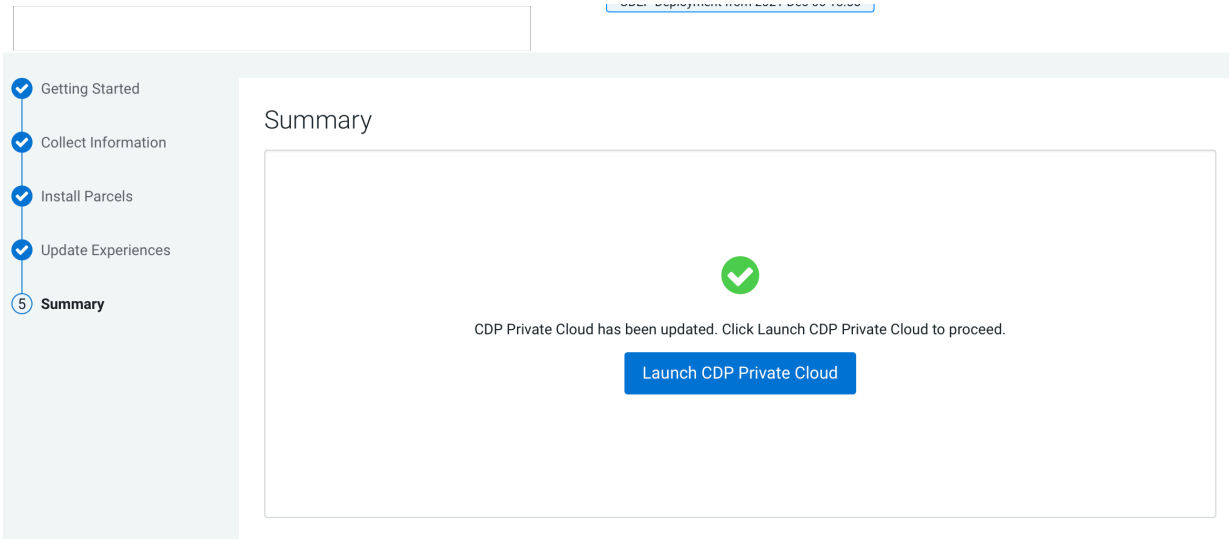
```
ecs-abc-4.vpc.myco.com   NotReady   <none>
 3h45m   v1.21.8+rke2r2
```

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.

1. If the upgrade stalls, do the following:

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

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

b. 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.

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

The Longhorn dashboard opens.

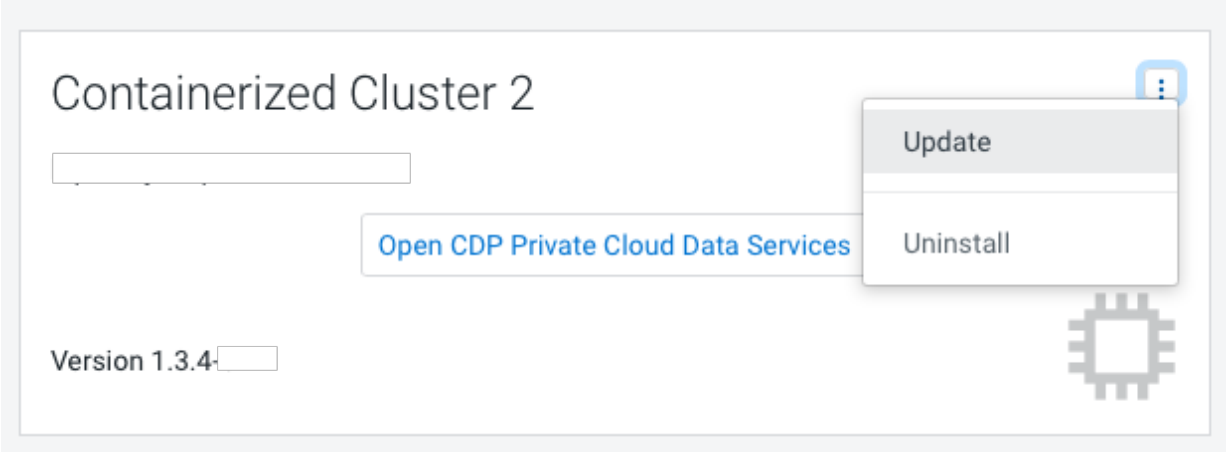
d. Check the "in Progress" section of the dashboard to see whether there are any volumes stuck in the attaching/detaching state in. If a volume is that state, reboot its host.

Update from 1.3.4 to 1.4.0/1.4.0-H1

You can update your existing CDP Private Cloud Data Services 1.3.4 to 1.4.0 or 1.4.0-H1 without requiring an uninstall.

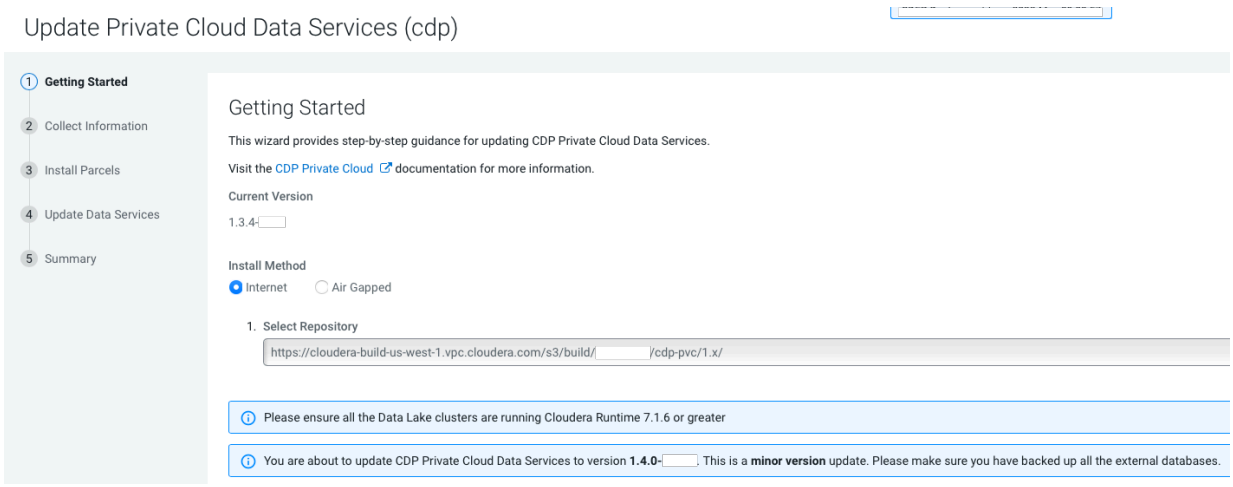
Procedure

1. In Cloudera Manager, navigate to CDP Private Cloud Data Services 1.3.4 and click  . Click Update.

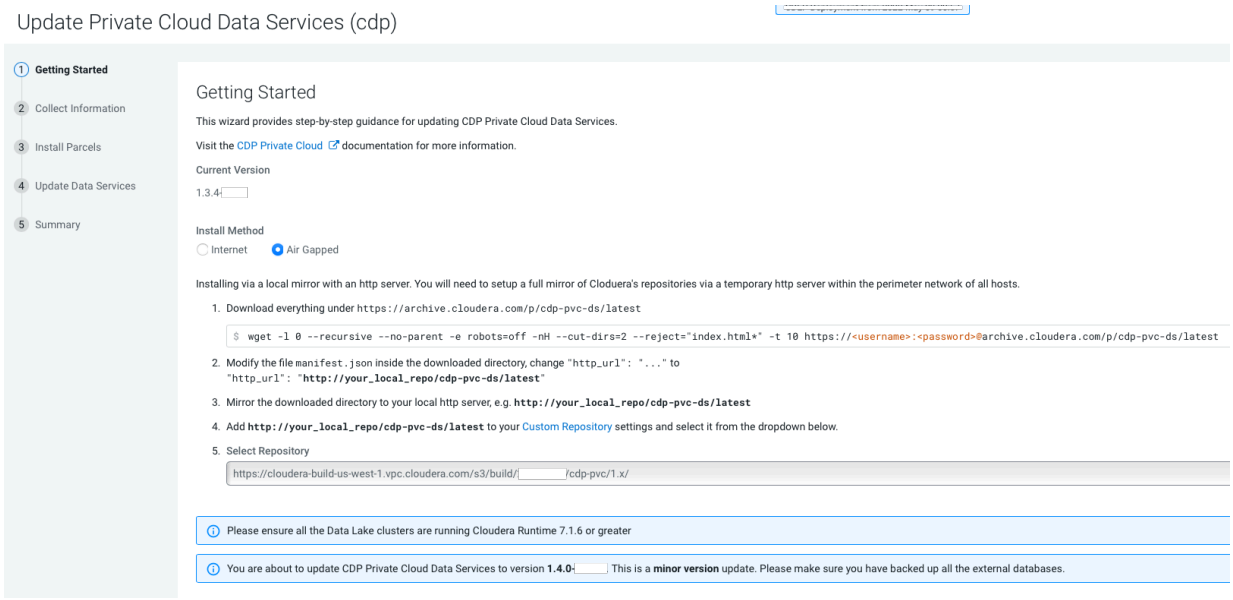


2. On the Getting Started page, you can select the Install method - Air Gapped or Internet and proceed.

   Internet install method

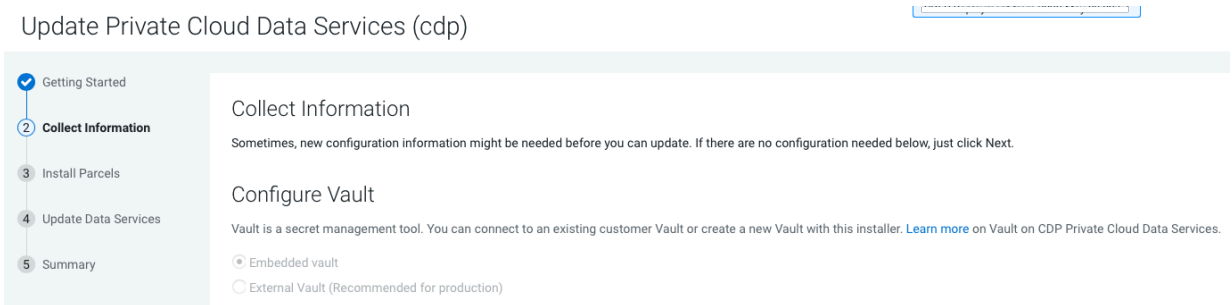


   Air Gapped install method

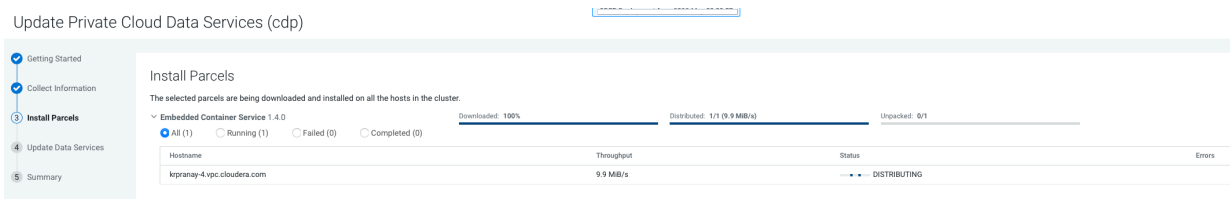


   Click Continue.

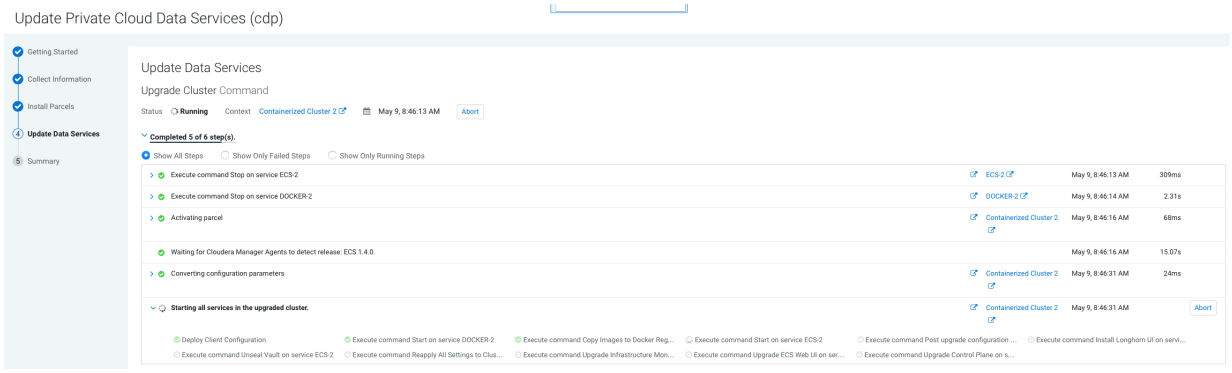
3. On the Collect Information page, click Continue.



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: Unable to start ECS server role on ECS server host.

  Workaround:

  a. SSH to the affected host.
  b. Search for the rke2-killall.sh script and run it.
  c. Start the ECS server role on the host from Cloudera Manager.
  d. Resume the upgrade by running any command that was affected by the upgrade failure.
- Error message: Code: 503. Errors: * Vault is sealed.

  Workaround: Longhorn repairs by itself. Wait until the Longhorn repair is complete.
- 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
  ```

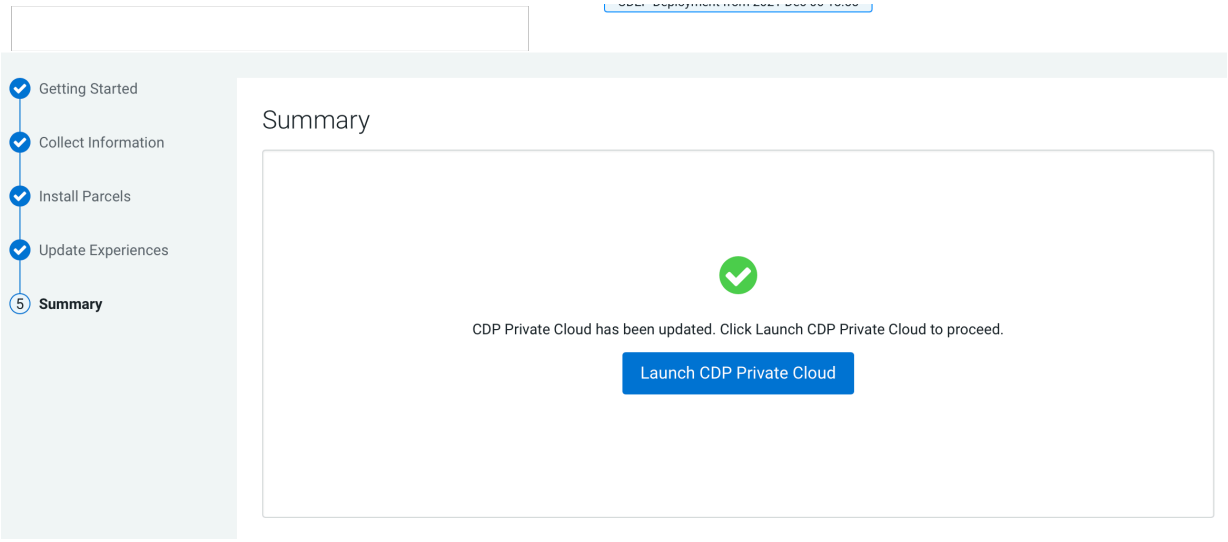
```
ecs-abc-4.vpc.myco.com   NotReady   <none>
 3h45m   v1.21.8+rke2r2
```

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.

- Upgrade failure with Cloudera's public registry

  On installation of CDP Private Cloud Data Services 1.3.4, the user can use an embedded registry or Cloudera's public registry. Upgrades using Cloudera's public registry will fail.

  Upgrade is not possible in this scenario. If an upgrade was attempted, activating the 1.3.4 parcel will restore the cluster.

Update from 1.3.3 to 1.4.0/1.4.0-H1

You can update your existing CDP Private Cloud Data Services 1.3.3 to 1.4.0 or 1.4.0-H1 without requiring an uninstall.

Before you begin

Important: Before beginning the update, you must first do the following:

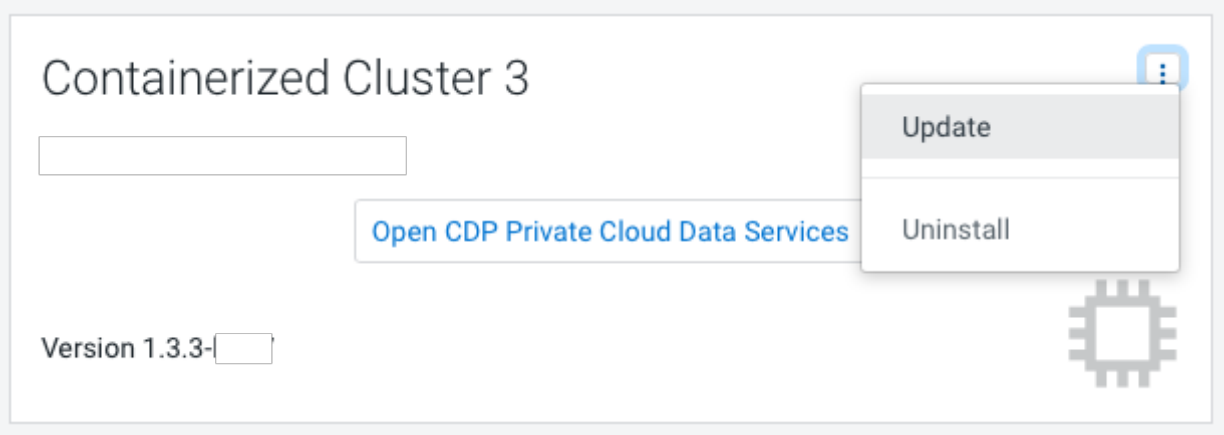
1. Log in to the Cloudera Manager Admin Console.
2. Go to Clusters Experience Cluster ECSQuick Links ECSWebUI.
3. Select the CDP namespace. For example: cdp.
4. Select the configmap named "cdp-pvc-truststore" and EDIT the deployment associated with this configmap.
5. If you find the line "END CERTIFICATE----------BEGIN CERTIFICATE" from the list of certificates, insert a new line using \n. For example:

```
END CERTIFICATE-----\n-----BEGIN CERTIFICATE
```

6. Save the configmap.
7. Continue with the update steps below.

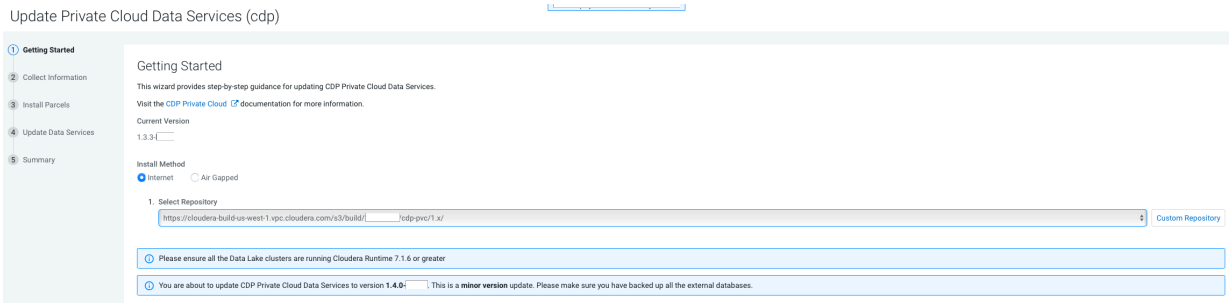
Procedure

1. In Cloudera Manager, navigate to CDP Private Cloud Experiences 1.3.3 and click . Click Update.

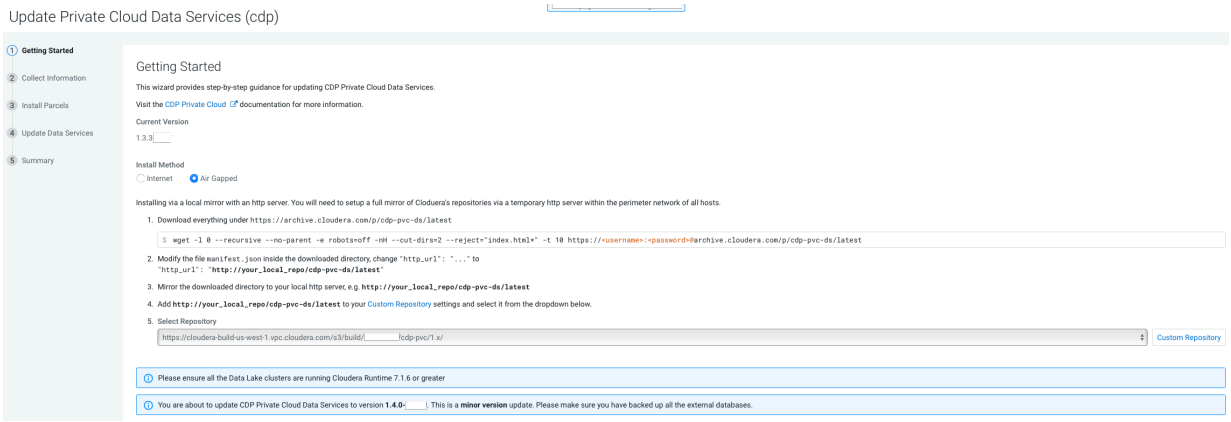


2. On the Getting Started page, you can select the Install method - Air Gapped or Internet and proceed.

   Internet install method

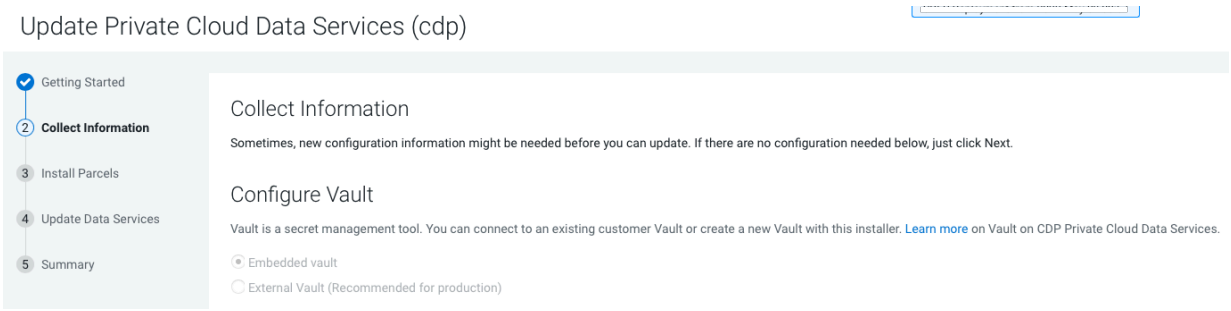


   Air Gapped install method

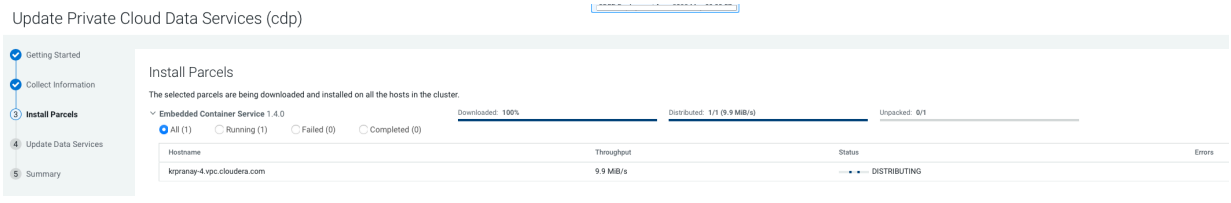


   Click Continue.

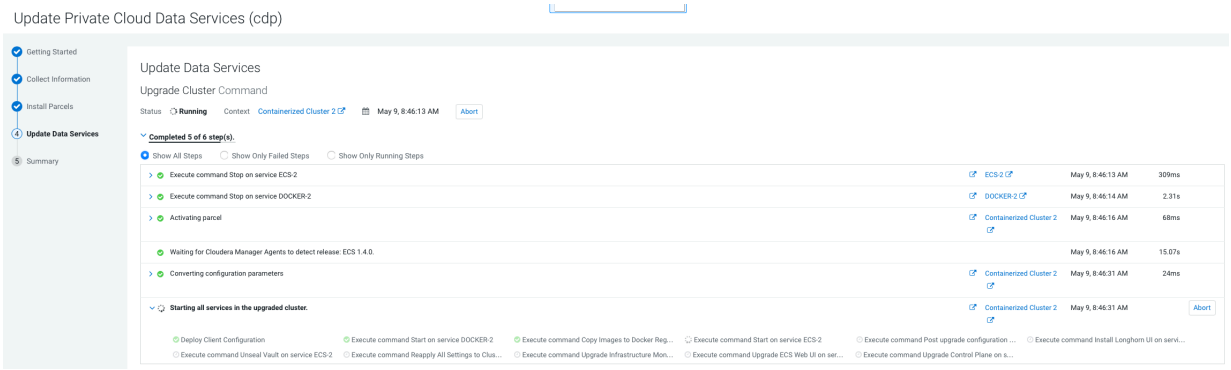
3. On the Collect Information page, click Continue.



4. On the Install Parcels page, click Continue.



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



If you encounter an error message in the Upgrade Cluster Command output, during the Execute command Install Tolerations Webhook on service ECS-3 step that mentions a failure waiting for kube-proxy to come up, do the following:

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
```

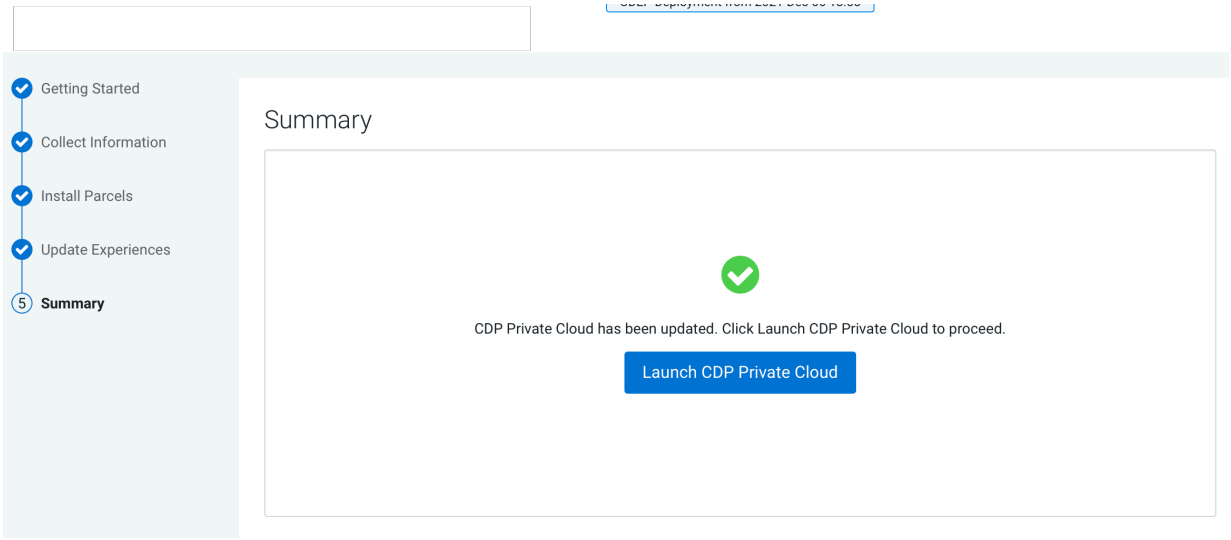
The output will look similar to the following:

```
NAME                              STATUS     ROLES                       AG
E     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.

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



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

- After the upgrade, the version of YuniKorn may not match the version that should be used with Private Cloud version 1.3.4. The YuniKorn version should be: 0.10.4-b25. If this version is not deployed, do the following to correct this:

  1. Log in to any node with access to the ECS cluster using ssh. The user must have the correct administration privileges to execute these commands.
  2. Run the following command to find the YuniKorn scheduler pod:

     ```
     kubectl get pods -n yunikorn | grep yunikorn-scheduler
     ```

     The first value on the line is the scheduler pod ID. Copy that text and us it in the following command to describe the pod:

     ```
     kubectl describe pod **yunikorn-scheduler-ID** -n yunikorn : grep "Ima
     ge:"
     ```

     A completed upgrade for 1.3.4 shows the image version:

     ```
     docker-private.infra.cloudera.com/cloudera/cloudera-scheduler:0.10.4-b25
     ```

     The correct version is 0.10.4-b25. If it still shows an older version like 0.10.3-b10, then the upgrade has failed.

     In case of a failed upgrade you must manually upgrade to the correct version. Continue with the remaining steps.
  3. Scale the YuniKorn deployment down to 0:

     ```
     kubectl scale deployment yunikorn-scheduler -n yunikorn --replicas=0
     ```
  4. Wait until all pods are terminated. you can check this by listing the pods in the unikorn namespace:

     ```
     kubectl get pods -n yunikorn
     ```
  5. Edit the deployment to update the version:

     ```
     kubectl edit deployment yunikorn-scheduler
     ```
  6. Replace all the references to the old version with the new updated version. There should be 3 references in the deployment file:

     - ADMISSION_CONTROLLER_IMAGE_TAG
     - Two lines with the "Image:" tag

     Replace all occurrences of the old version with the new version. For example: replace 0.10.3-b10 with 0.10.4-b25
  7. Save the changes.
  8. Scale the deployment back up:

     ```
     kubectl scale deployment yunikorn-scheduler -n yunikorn --replicas=1
     ```

- 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.
- If the upgrade fails, or constantly retries the upgrade, do the following:
  1. Open the ECS Web UI (Kubernetes Dashboard):
     a. In the Cloudera Manager Admin Console, go to the ECS service.
     b. Click Web UI ECS Web UI.
  2. If you see an error message similar to the following after the upgrade for the alertmanager pod, perform the steps below. If it is another pod, skip to Step 3 below.

     ```
     Warning  FailedAttachVolume  2s (x5 over 20s)  attachdetach-controller
     AttachVolume.Attach failed for volume "pvc-6b2bc988-cbdf-4b4a-a005-dee7a
     1b26cf5" : rpc error: code = DeadlineExceeded desc = volume pvc-6b2bc988
     -cbdf-4b4a-a005-dee7a1b26cf5 failed to attach to node ecs-bcrgq6-3.vpc.m
     yco.com
     ```

     a. Restart the pod with the error message:

        ```
        kubectl delete pod <pod name and number as shown in the error
         message>
        ```

        The pod will restart.
     b. If the pod still reports the error, log in to one of the ECS hosts and run the following command to delete the pvc:

        ```
        kubectl delete pvc storage-volume-monitoring-prometheus-alertmanager-
        <number> -n <namespace>
        ```

     c. Restart the pod with the error message:

        ```
        kubectl delete pod <pod name and number as shown in the error
         message>
        ```

        The pod will restart.

d. There will be two instances of alertmanager, cdp-release-prometheus-alertmanager-0 and cdp-release-prometheus-alertmanager-1, Run the following command, using the instance of the pod with the error message to restart the pod:

```
kubectl delete pod cdp-release-prometheus-alertmanager-<number> -
n <namespace>
```

3. If the same error happens with a pod that is not the alertmanager, but one that is not running in a statefulset, but in a deployment (like prometheus or grafana), save the pvc before deleting it and re-add it after it has terminated:

a. Log in to one of the ECS hosts and run the following command to save the pvc:

```
kubectl get pvc storage-volume-monitoring-prometheus-alertmanager-
<number> -n <namespace> -o yaml > mybackup.yaml
```

4. Run the following command to start the pvc:

```
kubectl apply -f mybackup.yaml  -n <namespace>
```