

Managing the Cloudera Embedded Container Service

Date published: 2023-12-16

Date modified: 2025-11-08



Legal Notice

© Cloudera Inc. 2025. All rights reserved.

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

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

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

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

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

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

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

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

Contents

| | |
|---|----------|
| Managing Cloudera Embedded Container Service..... | 4 |
| Configuring the Cloudera Embedded Container Service..... | 4 |
| Major RHEL Operating System upgrade on Cloudera Embedded Container Service hosts..... | 4 |
| Mixed mode RHEL Operating System upgrade on ECS hosts..... | 7 |
| Upgrading RHEL to a new minor version..... | 10 |
| Mixed mode minor RHEL OS upgrade on the Cloudera Embedded Container Service hosts..... | 10 |
| Adding hosts to a Cloudera Embedded Container Service Cluster..... | 11 |
| Starting, stopping, restarting, and refreshing Cloudera Embedded Container Service Clusters..... | 28 |
| Starting a Cloudera Embedded Container Service Cluster..... | 29 |
| Stopping a Cloudera Embedded Container Service Cluster..... | 29 |
| Restarting a Cloudera Embedded Container Service Cluster..... | 29 |
| Rolling Restart of an Cloudera Embedded Container Service Cluster..... | 29 |
| Configuring Restart for an Cloudera Embedded Container Service cluster..... | 30 |
| Refreshing a Cloudera Embedded Container Service Cluster..... | 30 |
| Monitoring Cloudera Embedded Container Service Clusters..... | 30 |
| Viewing Health Status..... | 30 |
| Viewing the Kubernetes Dashboard..... | 31 |
| Viewing the Cloudera Management Console on premises..... | 31 |
| Performing maintenance of a single host in the Cloudera Embedded Container Service cluster..... | 31 |
| Performing the maintenance of all hosts in the Embedded Container Service cluster..... | 32 |
| Configuring a containerized cluster with SELinux..... | 32 |
| Decommissioning Cloudera Embedded Container Service Hosts..... | 33 |
| Dedicating Cloudera Embedded Container Service nodes for specific workloads..... | 34 |
| Specifying racks for Cloudera Embedded Container Service clusters..... | 36 |
| Unifying time zone for Cloudera Embedded Container Service..... | 49 |
| Adjusting the expiration time of Cloudera Embedded Container Service cluster certificates..... | 50 |
| Rotating internal Cloudera Embedded Container Service certificates..... | 54 |
| Configuring multiple Base clusters with one Cloudera Embedded Container Service cluster..... | 54 |
| Configuring multiple Cloudera Embedded Container Service clusters on a single base cluster..... | 56 |
| Configuring multiple Cloudera Embedded Container Service environments on a single base cluster..... | 57 |
| GPU node labeling on Cloudera Embedded Container Service..... | 57 |

Managing Cloudera Embedded Container Service

Cloudera Manager provides tools for managing and monitoring the on premises Cloudera Embedded Container Service.

The Cloudera Embedded Container Service (ECS) service enables you to run Cloudera Data Services on premises by creating container-based clusters in your data center. In addition to the option to use OpenShift Container Platform, which requires that you deploy and manage the Kubernetes infrastructure, you can also deploy a Cloudera Embedded Container Service cluster, which creates and manages an embedded Kubernetes infrastructure for use with Cloudera Data Services on premises. Installing, configuring, and managing OpenShift is not required. You only need to provide hosts on which to install the service and Cloudera Manager sets up the Cloudera Embedded Container Service cluster and also provides management and monitoring of the cluster.

When you create an Cloudera Embedded Container Service cluster, two new services are added to the cluster:

- Cloudera Embedded Container Service. The Cloudera Embedded Container Service has two roles:
 - Cloudera Embedded Container Service Server -- runs on a single host in the Cloudera Embedded Container Service cluster.
 - Cloudera Embedded Container Service Agent -- runs on all hosts except the host running the Server role in the Cloudera Embedded Container Service Cluster.
- Docker service. The Docker service has a single role:
 - Docker Server -- runs on all hosts in the Cloudera Embedded Container Service Cluster.

If any values in `/etc/dex/secret/dex-secret.yaml`, such as `ldap.bindPass` and `ozoneS3Secret`, contain special characters, then, they must be enclosed in double quotes (") or the `dex-app- . . . pod` fails.

Configuring the Cloudera Embedded Container Service

You use Cloudera Manager to configure the Cloudera Embedded Container Service and clusters.

Procedure

1. Open the Cloudera Manager Admin Console
2. From the Home page, Click on the ECS Cluster
3. Click the Hosts, ECS service, or the Docker service links.
4. Click the Configuration tab.
5. Use the Filters or Search functions to locate the configuration property you are looking for.
6. Enter your change.
7. Click Save Changes.

Related Information

[Modifying Configuration Properties Using Cloudera Manager](#)

Major RHEL Operating System upgrade on Cloudera Embedded Container Service hosts

After installing Cloudera Data Services on premises on a particular RHEL OS, you can now upgrade RHEL OS to a new major version. For example, you can upgrade from RHEL 7.x to RHEL 9.x major version.

About this task

You must perform this task on all Cloudera Embedded Container Service hosts when you are ready for an OS upgrade.

Before you begin

Collect the following information:

- Cloudera Embedded Container Service hosts in the cluster. For example: host-1, host-2.

Navigate to Cloudera Manager > ECS Cluster Name > HOSTS , to collect the host info.

- Version of the ECS running on cluster. For example: 1.5.2

Navigate to Cloudera Manager > DATA SERVICES > Cluster Name , the cluster displays the Version at the bottom of the UI .

- Version of the Operating System (OS) running on those hosts. For example: RHEL 7.9

- Login to all of the hosts in the ECS cluster by executing the following command:

```
cat /etc/redhat-release
```

- Version of the upgraded OS. For example: RHEL 9.4

Verify the ECS version supported on the upgraded OS version here: <https://supportmatrix.cloudera.com/>



Note: The prerequisites assume that your Cloudera Manager/CDH versions and OS version have either been upgraded or do not need to be upgraded and your Cloudera Embedded Container Service cluster is healthy. You must also be familiar with the RedHat upgrade steps to go from your installed version to your final version.

Shutdown of the Cloudera Embedded Container Service Cluster

Perform the following steps:

1. Log in to Cloudera Manager as an Administrator, then navigate to the ECS cluster.
2. Go to the Home Status tab.
3. Click the Actions menu to the right of the Cloudera Embedded Container Service cluster name and select Stop.
4. Click the Stop option in the confirmation screen.

The **Command Details** window shows the progress of the services.

5. SSH into a ECS cluster host as a root user.
6. Verify the OS version by running the following command:

```
cat /etc/redhat-release
```

7. Stop Cloudera Manager agent on all the ECS hosts, by executing the following command:

```
systemctl stop cloudera-scm-agent
```

8. Uninstall Cloudera Manager agent packages on the ECS hosts by executing the following command:

```
yum remove cloudera-manager-agent
```

Major OS Upgrade

Follow the RHEL OS Upgrade documentation for major OS upgrade procedure.



Note: Ensure to check the supported upgrade path for your RHEL OS version.

Verify the upgraded OS version on all Cloudera Embedded Container Service hosts by executing the following command:

```
cat /etc/redhat-release
```

Setup and install new Cloudera Manager agents

Perform the following steps on each host in your cluster:

1. If you have not installed before, install python 3.8 and other dependencies on the Cloudera Embedded Container Service host.

Example: `yum install python3.8 -y`

2. Install the OS compatible Cloudera Manager agent packages.

Example: RHEL 9 package instead of RHEL 7 through commands on the Cloudera Embedded Container Service hosts.

- Change the baseurl= link in the cloudera-manager.repo to point to new RedHat version you upgraded to (from RedHat 7 to RedHat 9).

Example: baseurl=<https://archive.cloudera.com/p/cm7/7.11.3.0/redhat7/yum/>

```
vim /etc/yum.repos.d/cloudera-manager.repo
```

Save the cloudera-manager.repo file.

- To update repositories, execute:

```
yum clean all
```

- To verify the version is available, Example: 7.11.3.26-58725444.el9, execute the following command:

```
yum list available | grep -i cloudera-manager
```

- To install the Cloudera Manager Agent, execute the following command:

```
yum install cloudera-manager-agent
```

- To verify the correct version of the OS compatible Cloudera Manager agent installed, execute the following command:

```
yum list installed | grep -i cloudera-manager-agent
```

3. Restore the Cloudera Manager agent config file, execute the following command:

```
cp /etc/cloudera-scm-agent/config.ini.rpm.save /etc/cloudera-scm-agent/config.ini
```

4. Login to all the ECS host and then start the Cloudera Manager agent by executing the following command:

```
systemctl start cloudera-scm-agent
```

5. To verify the status of the Cloudera Manager agents started, execute the following command:

```
systemctl status cloudera-scm-agent
```

6. Log in to Cloudera Manager as an Administrator.

7. Verify that the Cloudera Manager displays all your hosts before starting ECS Cluster.

Navigate to Cloudera Manager > ECS Cluster Name > HOSTS , to collect the host info.



Note: Verify all the hosts show green indicating good health.

Start the Cloudera Embedded Container Service Cluster

1. To start the Cloudera Embedded Container Service cluster, go to the Home Status tab.
2. Click the Actions menu to the right of the Embedded Container Service cluster name and select Start.
3. Click the Start option.

The **Command Details** window shows the progress of the services.

Wait for all the pods to start. The wait time depends on the number of nodes in the cluster.

4. Navigate to ECS > WEB UI and try accessing: STORAGE UI, ECS WEB UI, and CONSOLE.

If you see a Vault sealed issue, after the start of the ECS service and if it does not unseal itself, then follow the step below to manually unseal it:

In the Cloudera Manager, Go to the ECS CLUSTER NAME > ECS > ACTIONS > UNSEAL VAULT

Mixed mode RHEL Operating System upgrade on ECS hosts

After installing Cloudera Data Services on premises on a particular RHEL OS, you can now upgrade RHEL OS on some of your hosts to a new major version. For example, in a 10 node cluster, you can upgrade any number of hosts from RHEL 7.x to RHEL 9.x major version and keep the other hosts, running RHEL 7.x.

About this task

You must perform this task on all Cloudera Embedded Container Service hosts when you are ready for an OS upgrade.

Before you begin

Collect the following information:

- Cloudera Embedded Container Service hosts in the cluster. For example: host-1, host-2.

Navigate to Cloudera Manager UI > ECS Cluster Name > HOSTS , to collect the host info.

- Version of the ECS running on cluster. For example: 1.5.2

Navigate to Cloudera Manager UI > DATA SERVICES > Cluster Name , the cluster displays the Version at the bottom of the UI .

- Version of the Operating System (OS) running on those hosts. For example: RHEL 7.9

- Login to all of the hosts in the ECS cluster by executing the following command:

```
cat /etc/redhat-release
```

- Version of the upgraded OS. For example: RHEL 9.4

Verify the ECS version supported on the upgraded OS version here: <https://supportmatrix.cloudera.com/>



Note: The prerequisites assume that your Cloudera Manager/CDH versions and OS version have either been upgraded or do not need to be upgraded and your Cloudera Embedded Container Service cluster is healthy. You must also be familiar with the RedHat upgrade steps to go from your installed version to your final version.

Shutdown of the Cloudera Embedded Container Service Cluster and prepare nodes for OS upgrade

Perform the following steps to shutdown the Cloudera Embedded Container Service cluster:

1. Log in to Cloudera Manager as an Administrator, then navigate to the ECS cluster.
2. Go to the **Home Status** tab.
3. Click the Actions menu to the right of the Embedded Container Service (ECS) cluster name and select Stop.
4. Click the Stop option in the confirmation screen.

The **Command Details** window shows the progress of the services.

Perform the following steps ONLY on the hosts you are upgrading:

1. SSH to the ECS host as root.
2. Verify the OS version by running the following command:

```
cat /etc/redhat-release
```

3. Stop Cloudera Manager agent on all the ECS hosts, by executing the following command:

```
systemctl stop cloudera-scm-agent
```

4. Uninstall Cloudera Manager agent packages on the ECS hosts by executing the following command:

```
yum remove cloudera-manager-agent
```

Major OS Upgrade

Follow the RHEL OS Upgrade documentation for major OS upgrade procedure.



Note: Ensure to check the supported upgrade path for your RHEL OS version.

Verify only the hosts you upgraded will show the new OS version on all Cloudera Embedded Container Service hosts by executing the following command:

```
cat /etc/redhat-release
```

Setup and install new Cloudera Manager agents

Perform the following steps on the hosts you upgraded in your cluster:

1. If you have not installed before, install python 3.8 and other dependencies on the ECS host.

Example: `yum install python3.8 -y`

2. Install the OS compatible Cloudera Manager agent packages.

Example: RHEL 9 package instead of RHEL 7 through commands on the ECS hosts.

- Change the baseurl= link in the cloudera-manager.repo to point to new RedHat version you upgraded to (from RedHat 7 to RedHat 9).

Example: baseurl=<https://archive.cloudera.com/p/cm7/7.11.3.0/redhat7/yum/>

```
vim /etc/yum.repos.d/cloudera-manager.repo
```

Save the cloudera-manager.repo file.

- To update repositories, execute:

```
yum clean all
```

- To verify the version is available, Example: 7.11.3.26-58725444.el9, execute the following command:

```
yum list available | grep -i cloudera-manager
```

- To install the Cloudera Manager Agent, execute the following command:

```
yum install cloudera-manager-agent
```

- To verify the correct version of the OS compatible Cloudera Manager agent installed, execute the following command:

```
yum list installed | grep -i cloudera-manager-agent
```

3. Restore the Cloudera Manager agent config file, execute the following command:

```
cp /etc/cloudera-scm-agent/config.ini.rpmsave /etc/cloudera-scm-agent/config.ini
```

4. Start the Cloudera Manager agent by executing the following command:

```
systemctl start cloudera-scm-agent
```

5. To verify the status of the Cloudera Manager agents started, execute the following command:

```
systemctl status cloudera-scm-agent
```

6. Log in to Cloudera Manager as an Administrator.

7. Verify that the Cloudera Manager displays all your hosts before starting ECS Cluster.

Navigate to Cloudera Manager UI > ECS Cluster Name > HOSTS , to collect the host info.



Note: Verify all the hosts show green indicating good health.

Start the Cloudera Embedded Container Service Cluster

1. To start the Cloudera Embedded Container Service cluster, go to the Home Status tab.
2. Click the Actions menu to the right of the Embedded Container Service cluster name and select Start.
3. Click the Start option.

The **Command Details** window shows the progress of the services.

Wait for all the pods to start. The wait time depends on the number of nodes in the cluster.

4. Navigate to ECS > WEB UI and try accessing: STORAGE UI, ECS WEB UI, and CONSOLE.

If you see a Vault sealed issue, after the start of the Cloudera Embedded Container Service and if it does not unseal itself, then follow the step below to manually unseal it:

In the Cloudera Manager UI, Go to the ECS CLUSTER NAME > ECS SERVICE> ACTIONS > UNSEAL VAULT

Upgrading the RHEL Operating System to a new minor version

After installing Cloudera Data Services on premises on a particular RHEL OS, you can now upgrade RHEL OS to a new minor version. For example, in a 9.x OS series, you can upgrade from 9.3 to 9.5 new minor version.

About this task

You must perform this task on all Cloudera Embedded Container Service hosts.

Before you begin

1. Log in to Cloudera Manager as an Administrator, then navigate to the ECS cluster.
2. Go to the Home Status tab.
3. Click the Actions menu to the right of the Embedded Container Service cluster name and select Stop.
4. Click the Stop button in the confirmation screen.

The **Command Details** window shows the progress of the services.

5. SSH into a ECS cluster host as a root user.
6. Verify the OS version by running the following command:

```
cat /etc/redhat-release
```

Procedure

1. Upgrade RHEL from the installed version to the desired minor version on the ECS host. Use the operating system upgrade procedures provided by your RedHat operating system vendor to download and upgrade RHEL.
For example, you can upgrade from RHEL 9.3 version to RHEL 9.5 minor version.
2. Verify the upgraded OS version by running the following command:

```
cat /etc/redhat-release
```

3. Log in to Cloudera Manager as an Administrator.
4. Go to the Home Status tab.
5. Click the Actions menu to the right of the Embedded Container Service cluster name and select Start.
6. Click the Start button that appears in the next screen to confirm.

The **Command Details** window shows the progress of the services.

Wait for all the pods to start. The wait time depends on the number of nodes in the cluster.

Mixed mode minor RHEL OS upgrade on the Cloudera Embedded Container Service hosts

After installing Cloudera Data Services on premises on a particular RHEL OS, you can now upgrade RHEL OS on some of your hosts to a new minor version. For example, in a 10 node cluster running in a RHEL 9.x OS series, you can upgrade any number of hosts from 9.3 to 9.5 new minor version and keep the other hosts running on original RHEL 9.x.

About this task

You must perform this task on all Cloudera Embedded Container Service hosts.

Before you begin

1. Log in to Cloudera Manager as an Administrator, then navigate to the ECS cluster.
2. Go to the **Home Status** tab.
3. Click the **Actions** menu to the right of the Embedded Container Service cluster name and select **Stop**.
4. Click the **Stop** button in the confirmation screen.

The **Command Details** window shows the progress of the services.

5. SSH into an ECS host as root.
6. Verify the OS version by running the following command:

```
cat /etc/redhat-release
```

Procedure

1. Upgrade RHEL from the installed version to the desired minor version on the ECS host you want to upgrade. Use the operating system upgrade procedures provided by your RedHat operating system vendor to download and upgrade RHEL.

For example, you can upgrade from RHEL 9.3 version to RHEL 9.5 minor version.

2. Verify the upgraded OS version by running the following command:

```
cat /etc/redhat-release
```

3. Log in to Cloudera Manager as an Administrator.
4. Go to the **Home Status** tab.
5. Click the **Actions** menu to the right of the Embedded Container Service cluster name and select **Start**.
6. Click the **Start** button that appears in the next screen to confirm.

The **Command Details** window shows the progress of the services.

Wait for all the pods to start. The wait time depends on the number of nodes in the cluster.

Adding hosts to a Cloudera Embedded Container Service Cluster

You can add hosts to a Cloudera Embedded Container Service cluster to increase capacity and performance.

About this task



Note: If the node added was previously a part of the Cloudera Embedded Container Service cluster, it needs to be cleaned up first to remove all residual ECS configurations and data before rejoining the cluster again.



Important: Do not stop the Cloudera Embedded Container Service cluster before adding new hosts. The Cloudera Embedded Container Service cluster must remain running during the host addition process. Stopping Cloudera Embedded Container Service can lead to cluster synchronization and volume attachment issues.

Procedure

1. On the Cloudera Manager home page, click the ECS Cluster, then select Actions > Add Hosts.

The screenshot shows the Cloudera Manager interface for the ECS cluster 152-b883. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Data Services. The main content area shows the cluster status, including a list of hosts (3 Hosts), DOCKER, and ECS. The 'Actions' dropdown menu is open, showing options like Add Service, Add Hosts, Start, Stop, Restart, Refresh Cluster, Upgrade Cluster, Inspect Hosts in Cluster, Rolling Restart, Rename Cluster, Enter Maintenance Mode, and View Maintenance Mode Status. The 'Add Hosts' option is highlighted. Below the status section, there are three charts: Cluster CPU, Cluster Disk IO, and Cluster Network IO, each showing performance metrics over time.

2. On the Add Hosts page, click Add Hosts to Cluster and select the ECS Cluster, then click Continue.

The screenshot shows the 'Add Hosts' wizard in Cloudera Manager. The wizard explains that it allows installing the Cloudera Manager Agent on new hosts. There are two options: 'Add hosts to Cloudera Manager' and 'Add hosts to Cluster'. The 'Add hosts to Cluster' option is selected, and a dropdown menu shows the cluster '152-b883'. At the bottom right, there are 'Back' and 'Continue' buttons.

3. On the Specify Hosts page, hosts that have already been added to Cloudera Manager are listed on the Currently Managed Hosts tab. You can select one or more of these hosts to add to the ECS cluster.

Add Hosts

CDEP Deployment from 2023-Oct-23 11:55

Specify Hosts

Currently Managed Hosts (1/4 Selected) New Hosts

These hosts do not belong to any clusters. Select some to form your cluster.

| <input type="checkbox"/> | Hostname (FQDN) ↑ | IP Address | Rack | Version | Cores |
|-------------------------------------|---------------------------------|---------------|----------|---------|-------|
| <input type="checkbox"/> | dh-centos79m-1.vpc.cloudera.com | 10.65.202.225 | /default | None | 8 |
| <input type="checkbox"/> | dh-centos79m-2.vpc.cloudera.com | 10.65.203.223 | /default | None | 8 |
| <input type="checkbox"/> | dh-centos79m-3.vpc.cloudera.com | 10.65.202.91 | /default | None | 8 |
| <input checked="" type="checkbox"/> | ecst-2.vpc.cloudera.com | 10.65.203.79 | /default | None | 8 |

1 - 4 of 4

Cancel ← Back Continue →

You can also click the New Hosts tab to specify one or more hosts that have not been added to Cloudera Manager. Enter a Fully Qualified Domain Name in the Hostname box, then click Search.



Note: Click the pattern link under the Hostname box to display more information about allowed FQDN patterns.

Add Hosts

CDEP Deployment from 2023-Oct-23 11:55

Specify Hosts

Currently Managed Hosts (1/4 Selected) **New Hosts (1 Selected)**

Hosts should be specified using the same hostname (FQDN) that they will identify themselves with.

Hostname

Hint: Search for hostnames or IP addresses using [pattern](#)

SSH Port Search

2 hosts scanned, 2 running SSH.

| <input type="checkbox"/> | Expanded Query | Hostname (FQDN) ↑ | IP Address | Currently Managed | Result |
|-------------------------------------|-------------------------|-------------------------|--------------|-------------------|--------------------------------|
| <input checked="" type="checkbox"/> | ecst-1.vpc.cloudera.com | ecst-1.vpc.cloudera.com | 10.65.196.65 | No | Host was successfully scanned. |
| <input type="checkbox"/> | ecst-2.vpc.cloudera.com | ecst-2.vpc.cloudera.com | 10.65.203.79 | Yes | Host was successfully scanned. |

1 - 2 of 2

Cancel ← Back Continue →

After you have finished specifying the ECS hosts, click Continue.

4. On the Select Repository page, the applicable Cloudera Manager Agent repository location is selected by default. Click Continue.

CLUSTER DEPLOYMENT CDEP Deployment from 2023-Oct-23 11:55

Add Hosts

- Specify Hosts
- Select Repository**
- Select JDK
- Enter Login Credentials
- Install Agents
- Install Parcels
- Inspect Hosts
- Select Host Template
- Deploy Client Config

Select Repository

Cloudera Manager Agent

Cloudera Manager Agent 7.11.3 (#46431848) needs to be installed on all new hosts.

Repository Location ☐ Cloudera Repository (Requires direct Internet access on all hosts.) ☒ Custom Repository

Example: `http://LOCAL_SERVER/cloudera-repos/cm7/7.11.3`

Do not include operating system-specific paths in the URL. The path will be automatically derived.

[Learn more at How to set up a custom repository.](#)

[Cancel](#) [Back](#) [Continue](#)

5. Select a JDK option on the Select JDK page, then click Continue.

Add Hosts

- Specify Hosts
- Select Repository
- Select JDK**
- Enter Login Credentials
- Install Agents
- Install Parcels
- Inspect Hosts
- Select Host Template
- Deploy Client Config

Select JDK

| CDH Version | Supported JDK Version |
|-----------------|---|
| 7.1.9 and above | OpenJDK 8, 11, 17 or Oracle JDK 8, 11, 17 |
| 7.1.1 to 7.1.8 | OpenJDK 8, 11 or Oracle JDK 8, 11 |
| 7.0 and above | OpenJDK 8 or Oracle JDK 8 |
| 6.3 and above | OpenJDK 8 or Oracle JDK 8 |
| 6.2 | OpenJDK 8 or Oracle JDK 8 |
| 6.1 or 6.0 | Oracle JDK 8 |
| 5.16 and above | OpenJDK 8 or Oracle JDK 8 |
| 5.7 to 5.15 | Oracle JDK 8 |

1 - 8 of 8 [More details on supported JDK version.](#)

If you plan to use JDK 11 with CDH 7.1.x and above or JDK 17 with CDH 7.1.9 and above, you will need to install it manually on all hosts and then select the **Manually manage JDK** option below.

☐ Manually manage JDK

☒ Install a Cloudera-provided version of OpenJDK

By proceeding, Cloudera will install a supported version of OpenJDK version 8.

☐ Install a system-provided version of OpenJDK

By proceeding, Cloudera will install the default version of OpenJDK version 8 provided by the Operating System.

[Cancel](#) [Back](#) [Continue](#)

- On the Enter Login Credentials page, All hosts accept the same password is selected by default. Enter the user name in the SSH Username box, and type in and confirm the password. You can also select the All hosts accept the same private key option and provide the Private Key and passphrase.

The screenshot shows the 'Add Hosts' dialog in Cloudera Manager. The left sidebar contains a progress indicator with steps: Specify Hosts, Select Repository, Select JDK, Enter Login Credentials (current step), Install Agents, Install Parcels, Inspect Hosts, Select Host Template, and Deploy Client Config. Below the progress indicator are links for Parcels, Running Commands, Support, and an admin user icon. The main area is titled 'Enter Login Credentials' and includes a warning about root access. The form fields are: SSH Username (root), Authentication Method (All hosts accept same password selected), Password (masked), Confirm Password (masked), SSH Port (22), and Simultaneous Installations (10). A note explains that simultaneous installations can consume network bandwidth. At the bottom are 'Cancel', 'Back', and 'Continue' buttons.

CLUSTER DEPLOYMENT FROM 2023-OCT-23 11:55

Add Hosts

Enter Login Credentials

Root access to your hosts is required to install the Cloudera packages. This installer will connect to your hosts via SSH and log in either directly as root or as another user with password-less sudo/pbrun privileges to become root.

SSH Username

Authentication Method ☒ All hosts accept same password
☐ All hosts accept same private key

Password

Confirm Password

SSH Port


Simultaneous Installations
(Running a large number of installations at once can consume large amounts of network bandwidth and other system resources)

Cancel

7. The Cloudera Manager agents are installed, and then the Install Parcels page appears. The selected parcel is downloaded to the Cloudera Manager server host, distributed, unpacked, and activated on the ECS cluster hosts. Click Continue.

The screenshot shows the Cloudera Manager interface during the 'Add Hosts' process. On the left is a dark sidebar with the Cloudera Manager logo and a list of navigation items: Parcels, Running Commands, Support, and an 'admin' user profile. The main content area is titled 'Add Hosts' and features a vertical progress bar on the left with steps 1 through 9. Step 6, 'Install Parcels', is the current active step. The main panel displays the 'Install Parcels' section with the text: 'The selected parcels are being downloaded and installed on all the hosts in the cluster.' Below this, a progress bar for 'Embedded Container Service ...' shows four stages: 'Downloaded: 100%', 'Distributed: ...', 'Unpacked: 4/4', and 'Activated: 4/4'. At the bottom of the interface, there is a 'Cancel' button on the left and 'Back' and 'Continue' buttons on the right. A status bar at the very bottom shows the version '7.11.3' and a double-left arrow icon.

8. Review the Validations list on the Inspect Hosts page. If issues are detected, you can fix the issues, then click Run Again to repeat the host inspection. Click Continue.



CLOUDERA
Manager

- Parcels
- Running Commands
- Support
- admin

7.11.3

Add Hosts

- Specify Hosts
- Select Repository
- Select JDK
- Enter Login Credentials
- Install Agents
- Install Parcels
- 7
Inspect Hosts- Select Host Template
- Deploy Client Config

Inspect Hosts

[Run Again](#)

| Status | Description |
|--------|---|
| ✓ | Inspector ran on all 4 hosts. |
| ✓ | Individual hosts resolved their own hostnames correctly. |
| ✓ | No errors were found while looking for conflicting init scripts. |
| ✓ | No errors were found while checking /etc/hosts. |
| ✓ | All hosts resolved localhost to 127.0.0.1. |
| ✓ | All hosts checked resolved each other's hostnames correctly and in a timely manner. |
| ✓ | Host clocks are approximately in sync (within ten minutes). |
| ✓ | Host time zones are consistent across the cluster. |
| ✓ | No users or groups are missing. |
| ✓ | No conflicts detected between packages and parcels. |
| ✓ | No kernel versions that are known to be bad are running. |
| ✓ | No problems were found with /proc/sys/vm/swappiness on any of the hosts. |
| ⚠ | Transparent Huge Page Compaction is enabled and can cause significant performance problems. Run "echo never > /sys/kernel/mm/transparent_hugepage/defrag" and "echo never > /sys/kernel/mm/transparent_hugepage/enabled" to disable this, and then add the same command to an init script such as /etc/rc.local so it will be set on system reboot. The following hosts are affected: > View Details |
| ⚠ | Hue Python version dependency is satisfied. Starting with CDH 6, PostgreSQL-backed Hue requires Psycopg2 version to be at least 2.5.4, see the documentation for more information. The following hosts are missing a compatible version of the Psycopg2 library: > View Details |
| ✓ | A compatible version of the operating system is installed on the hosts in a Private Cloud Containerized Cluster. |
| ✓ | Ports 80 and 443 are available for use on the hosts in a Private Cloud Containerized Cluster. |

[Cancel](#)

← Back
Continue →

9. The Select Host Template page lists available host templates. Click Create.

**Note:**

The following three steps describe how to create a host template to assign the Docker Server and Ecs Agent role groups to the new host. You can also select None and add these role instances after adding the new host to the cluster, as described at the end of this topic.

The screenshot shows the Cloudera Manager interface during the 'Add Hosts' process. On the left is a dark sidebar with the Cloudera Manager logo and a list of navigation items: Parcels, Running Commands, Support, and a user profile for 'admin'. The main area is titled 'Add Hosts' and shows a progress bar with steps 1 through 9. Step 8, 'Select Host Template', is the current step and is highlighted. Below the progress bar, the 'Select Host Template' section contains the instruction: 'Select a host template to apply to the new hosts in order to populate them with role instances.' There is a radio button selected for 'None' and a 'Create...' button. At the bottom of the main area are 'Cancel', 'Back', and 'Continue' buttons. A status bar at the very bottom shows the version '7.11.3' and a back arrow.

10. On the Create New Host Template pop-up, enter a template name and select the Docker Server and Ecs Agent role groups, then click Create.

The screenshot shows the 'Add Hosts' page in Cloudera Manager. A modal window titled 'Create New Host Template For 152-b883' is open. The 'Template Name' field contains 'ecsworker'. Under 'Select Role Groups to Include:', the 'DOCKER' section has 'Docker Server' checked with a dropdown set to 'Docker Server Default Group'. The 'ECS' section has 'Ecs Agent' checked with a dropdown set to 'Ecs Agent Default Group', and 'Ecs Server' is unchecked. The modal has 'Cancel' and 'Create' buttons at the bottom right. The background shows the 'Add Hosts' progress bar and navigation buttons.

11. On the Select Host Template page, select the new template, then click Continue.

The screenshot shows the 'Add Hosts' page in Cloudera Manager, specifically the 'Select Host Template' step. The progress bar on the left indicates the current step is '8 Select Host Template'. The main content area has the title 'Select Host Template' and the instruction 'Select a host template to apply to the new hosts in order to populate them with role instances.' There are two radio buttons: 'None' and 'ecsworker', with 'ecsworker' selected. A 'Create...' button is next to the 'ecsworker' option. Below this, there is a checked checkbox for 'Start newly created roles after applying the host template.' At the bottom, there are 'Cancel', 'Back', and 'Continue' buttons.

12. The Apply Host Template page appears. After the roles have successfully started, click Continue.

CLOUDERA
Manager

Parcels
Running Commands
Support
admin

Add Hosts

Specify Hosts

Select Repository

Select JDK

Enter Login Credentials

Install Agents

Install Parcels

Inspect Hosts

Select Host Template

Apply Host Template

Deploy Client Config

Cancel

Continue →

CDEP Deployment from 2023-Oct-23 11:55

Apply Host Template

Start Roles on Hosts When Free Command

Status Finished Dec 12, 10:20:41 PM 48.4s


Successfully started all the roles on selected hosts.

Completed 3 of 3 step(s).

☒ Show All Steps ☐ Show Only Failed Steps ☐ Show Only Running Steps

| | | | |
|--|------------------------|---------------------|--------|
| > Wait for Service Commands | DOCKER | Dec 12, 10:20:41 PM | 99ms |
| > Wait for Service Commands | ECS | Dec 12, 10:20:41 PM | 100ms |
| > Starts all the roles on the selected hosts. | | Dec 12, 10:20:41 PM | 48.25s |

13. The Deploy Client Config page appears. After all client configurations have been successfully deployed, click Finish.

CLOUDERA
Manager

Parcels

Running Commands

Support

admin

7.11.3

Add Hosts

Specify Hosts

Select Repository

Select JDK

Enter Login Credentials

Install Agents

Install Parcels

Inspect Hosts




Select Host Template

Apply Host Template

10 Deploy Client Config

Deploy Client Config

Deploy Client Configuration Command

Status Finished Context [152-b883](#)   Dec 12, 10:26:12 PM  59ms


Successfully deployed all client configurations.

Completed 1 of 1 step(s).

Show All Steps

Show Only Failed Steps

Show Only Running Steps

>  Execute DeployClusterClientConfig for {} in parallel.

Dec 12, 10:26:12 PM

57ms

Cancel

Back

Finish

14. The new host is listed on the ECS cluster Hosts page.

152-b883

CDEP Deployment from 2023-Oct-23 11:55

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Data Services New

Hosts

Configuration

Add Hosts

Review Upgrade Status

Inspect Hosts in Cluster

Inspect Cluster Network Performance

Q Search

Filters

Last Updated: Dec 12, 10:29:36 PM UTC

Columns: 11 Selected

Filters

STATUS

Good Health 4

CLUSTERS

CORES

COMMISSION STATE

LAST HEARTBEAT

LOAD (1 MINUTE)

LOAD (5 MINUTES)

LOAD (15 MINUTES)

MAINTENANCE MODE

UPGRADE DOMAIN

RACK

SERVICE

Actions for Selected

| <input type="checkbox"/> | Status | Name | IP | Roles | Tags | Commission State | Last He |
|--------------------------|--------|--------------------------------|---------------|---------|-------|------------------|---------|
| <input type="checkbox"/> | ✓ | dh-centos79-1.vpc.cloudera.com | 10.65.203.160 | 2 Roles | | Commissioned | |
| <input type="checkbox"/> | ✓ | dh-centos79-2.vpc.cloudera.com | 10.65.194.119 | 2 Roles | | Commissioned | |
| <input type="checkbox"/> | ✓ | dh-centos79-3.vpc.cloudera.com | 10.65.194.114 | 2 Roles | | Commissioned | |
| <input type="checkbox"/> | ✓ | ecst-1.vpc.cloudera.com | 10.65.217.129 | 2 Roles | 1 Tag | Commissioned | |

1 - 4 of 4

- 15.** If your ECS hosts are running the CentOS 8.4, OEL 8.4, RHEL 7.9, or RHEL 8 operating systems, you must install iptables on all the ECS hosts.

For CentOS 8.4, OEL 8.4, or RHEL 8, run the following command on each ECS host:

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

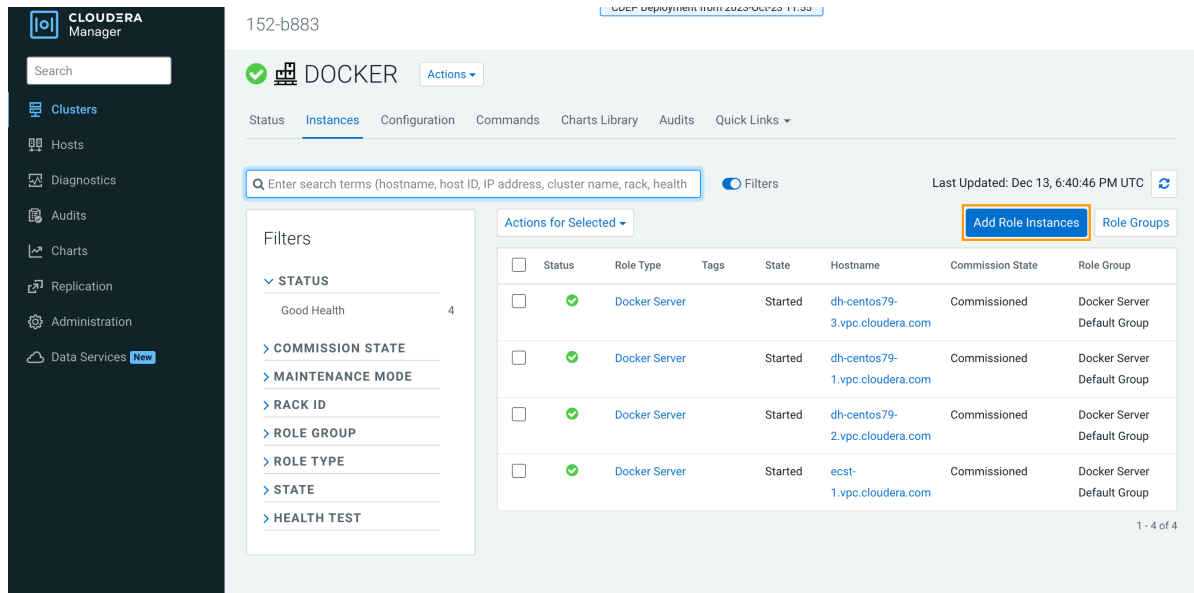
For RHEL 7.9, run the following command on each ECS host:

```
yum install -y iptables
```

16. If you did not apply a host template to assign roles, perform the following steps to assign the Docker Server and Ecs Agent role groups to the new host.

To assign the Docker Server role group:

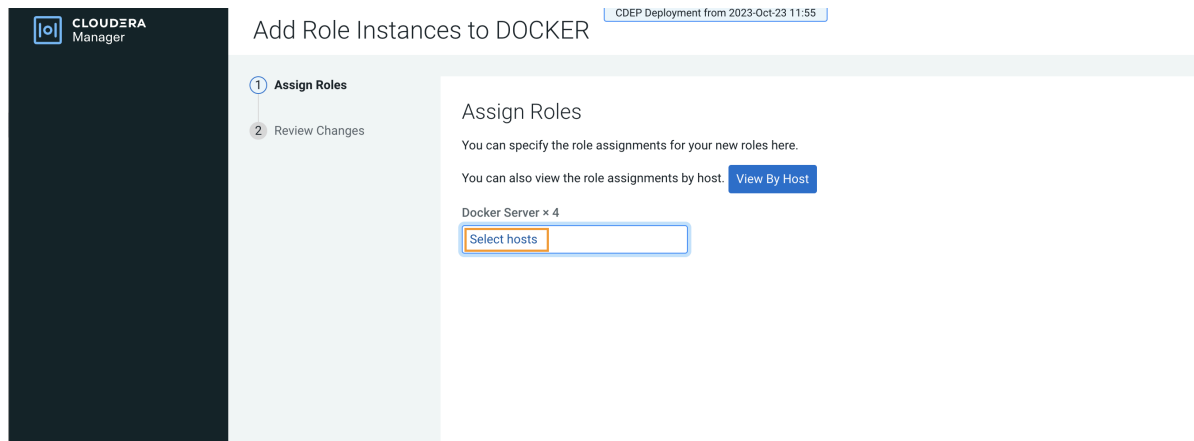
a. Click DOCKER on the ECS cluster home page, select Instances, then click Add Role Instances.



The screenshot shows the Cloudera Manager interface for a DOCKER cluster. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Data Services. The main content area displays the cluster status as 'Good Health' with 4 instances. A table lists the instances with columns for Status, Role Type, Tags, State, Hostname, Commission State, and Role Group. The 'Add Role Instances' button is highlighted in the top right corner.

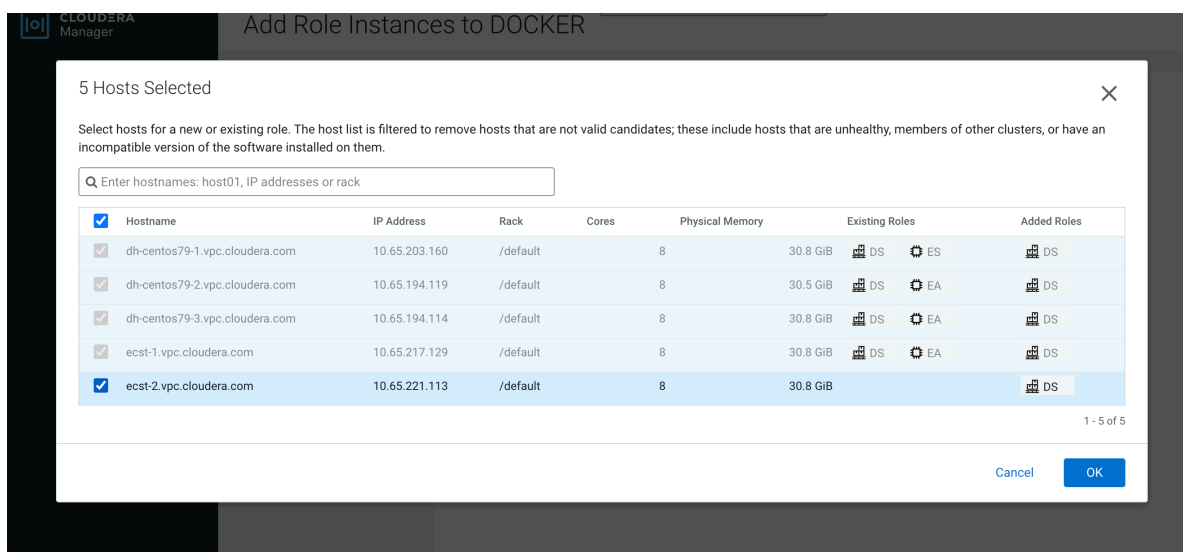
| Status | Role Type | Tags | State | Hostname | Commission State | Role Group |
|--------|---------------|------|---------|--------------------------------|------------------|-----------------------------|
| ✓ | Docker Server | | Started | dh-centos79-3.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| ✓ | Docker Server | | Started | dh-centos79-1.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| ✓ | Docker Server | | Started | dh-centos79-2.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| ✓ | Docker Server | | Started | ecst-1.vpc.cloudera.com | Commissioned | Docker Server Default Group |

b. On the Add Role Instances to DOCKER page, click Select hosts.

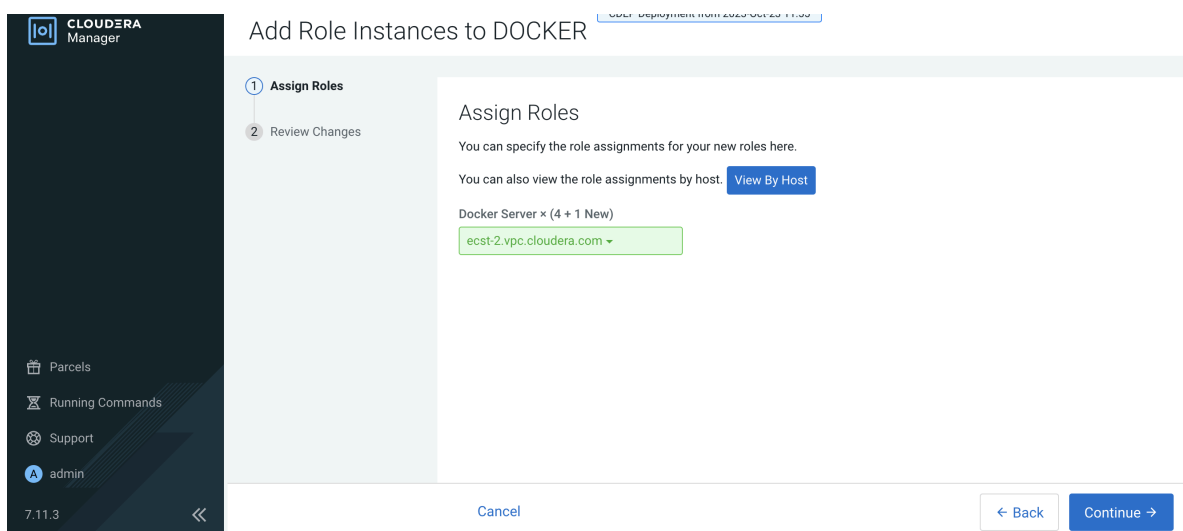


The screenshot shows the 'Add Role Instances to DOCKER' page. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Data Services. The main content area displays the 'Assign Roles' step, which includes a 'Select hosts' button. The 'Review Changes' step is also visible.

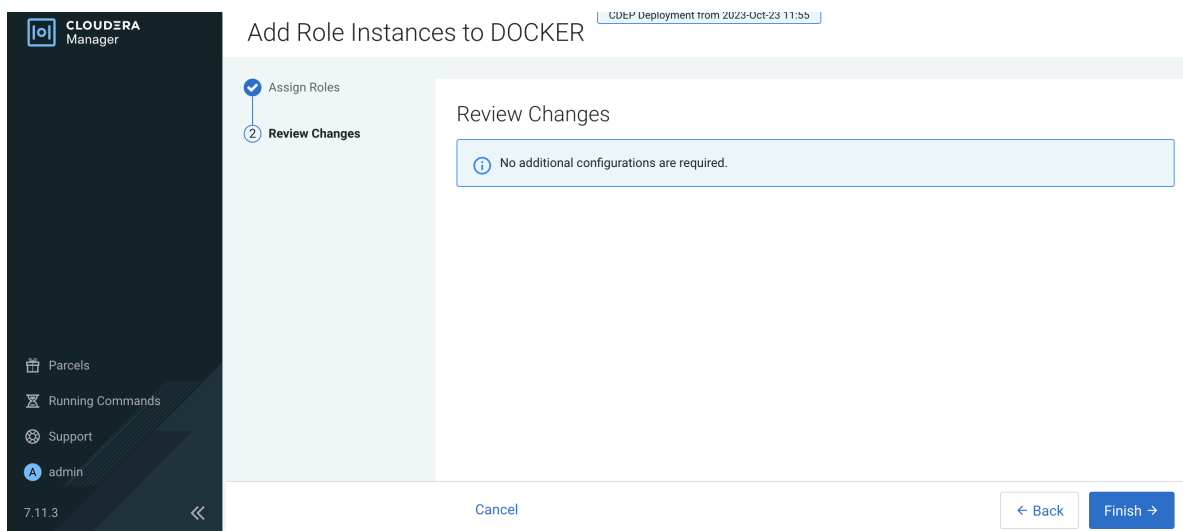
c. On the Hosts Selected pop-up, select the new host, then click OK.



- d. On the Assign Roles page, click Continue.



- e. On the Review Changes page, click Finish.



- f. The new host is listed on the Docker Instances page.

152-b883

CDEP Deployment from 2023-Oct-23 11:25

DOCKER Actions

Status Instances Configuration Commands Charts Library Audits Quick Links

Q Enter search terms (hostname, host ID, IP address, cluster name, rack, health s) Filters Last Updated: Dec 13, 7:00:56 PM UTC

Filters

STATUS

Good Health 4
Stopped 1

COMMISSION STATE

MAINTENANCE MODE

RACK ID

ROLE GROUP

ROLE TYPE

STATE

HEALTH TEST

Actions for Selected

Add Role Instances Role Groups

| Status | Role Type | Tags | State | Hostname | Commission State | Role Group |
|--------------------------|---------------|------|---------|--------------------------------|------------------|-----------------------------|
| <input type="checkbox"/> | Docker Server | | Started | dh-centos79-3.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| <input type="checkbox"/> | Docker Server | | Started | dh-centos79-1.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| <input type="checkbox"/> | Docker Server | | Started | dh-centos79-2.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| <input type="checkbox"/> | Docker Server | | Stopped | ecst-2.vpc.cloudera.com | Commissioned | Docker Server Default Group |
| <input type="checkbox"/> | Docker Server | | Started | ecst-1.vpc.cloudera.com | Commissioned | Docker Server Default Group |

1 - 5 of 5

To assign the ECS Agent role group:

- Click ECS on the ECS cluster home page, select Instances, then click Add Role Instances.

152-b883

CDEP Deployment from 2023-Oct-23 11:55

ECS Actions

Status Instances Configuration Commands Charts Library Audits Web UI Quick Links

This entity is currently running with an outdated configuration. Restart the service (or the instance) for the changes to take effect.

Q Enter search terms (hostname, host ID, IP address, cluster name, rack, health st) Filters Last Updated: Dec 13, 7:07:48 PM UTC

Filters

STATUS

Good Health 4

COMMISSION STATE

MAINTENANCE MODE

RACK ID

ROLE GROUP

ROLE TYPE

STATE

HEALTH TEST

Actions for Selected

Add Role Instances Role Groups

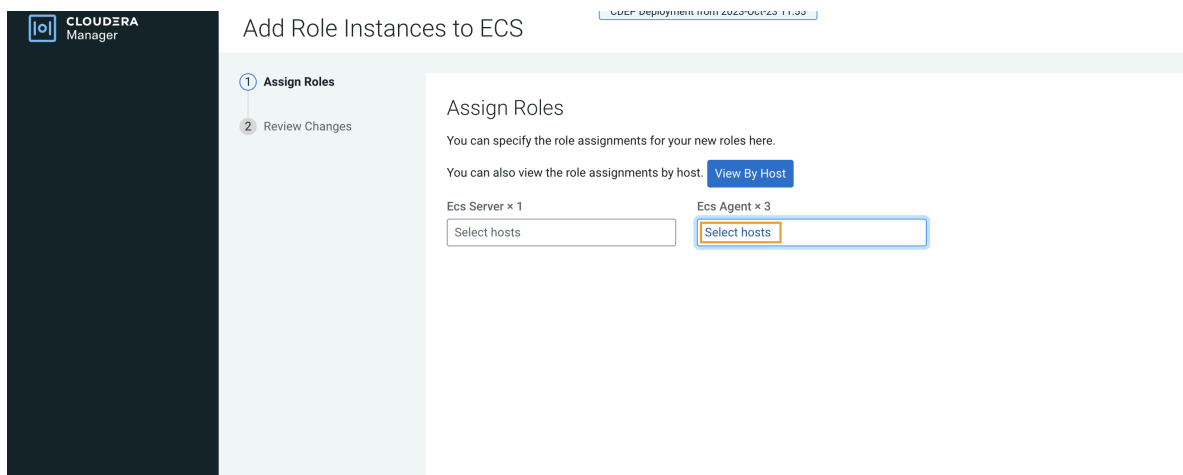
| Status | Role Type | Tags | State | Hostname | Commission State | Role Group |
|--------------------------|------------|------|-------------------------------------|--------------------------------|------------------|--------------------------|
| <input type="checkbox"/> | Ecs Agent | | Started | dh-centos79-3.vpc.cloudera.com | Commissioned | Ecs Agent Default Group |
| <input type="checkbox"/> | Ecs Agent | | Started | dh-centos79-2.vpc.cloudera.com | Commissioned | Ecs Agent Default Group |
| <input type="checkbox"/> | Ecs Agent | | Started | ecst-1.vpc.cloudera.com | Commissioned | Ecs Agent Default Group |
| <input type="checkbox"/> | Ecs Server | | Started with Outdated Configuration | dh-centos79-1.vpc.cloudera.com | Commissioned | Ecs Server Default Group |

1 - 4 of 4

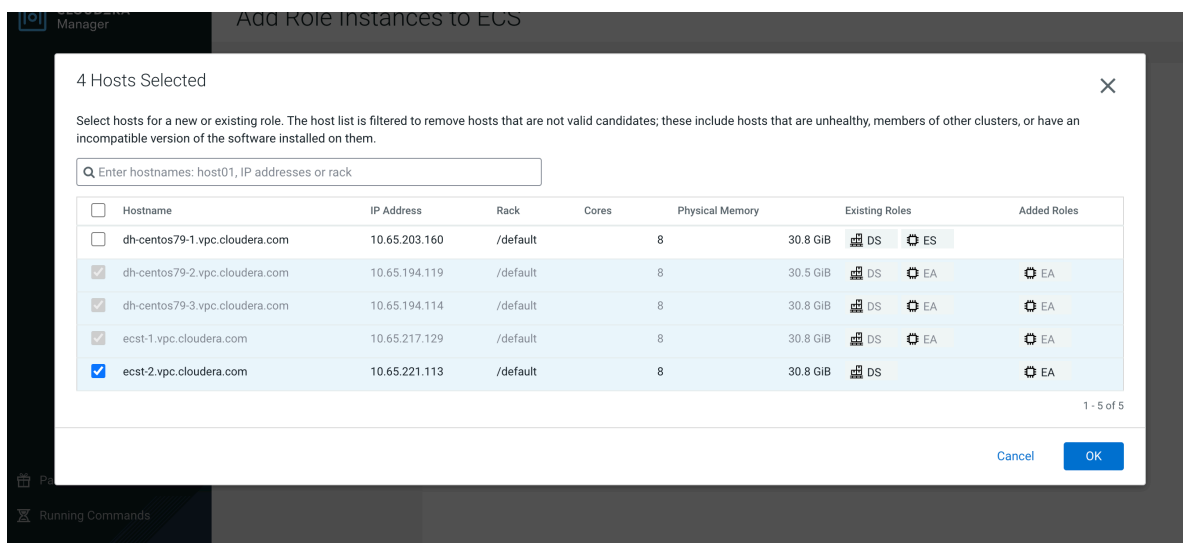
- On the Add Role Instances to ECS page, in the Ecs Agent box, click Select hosts.



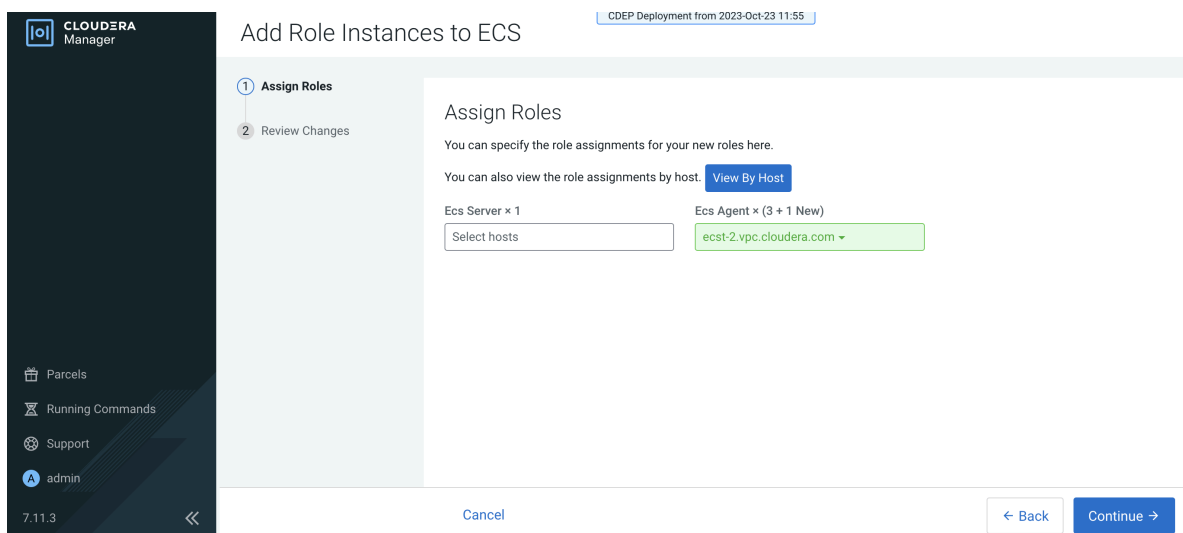
Important: Be sure to click Select hosts in the Ecs Agent box – do not click the link in the Ecs Server box.



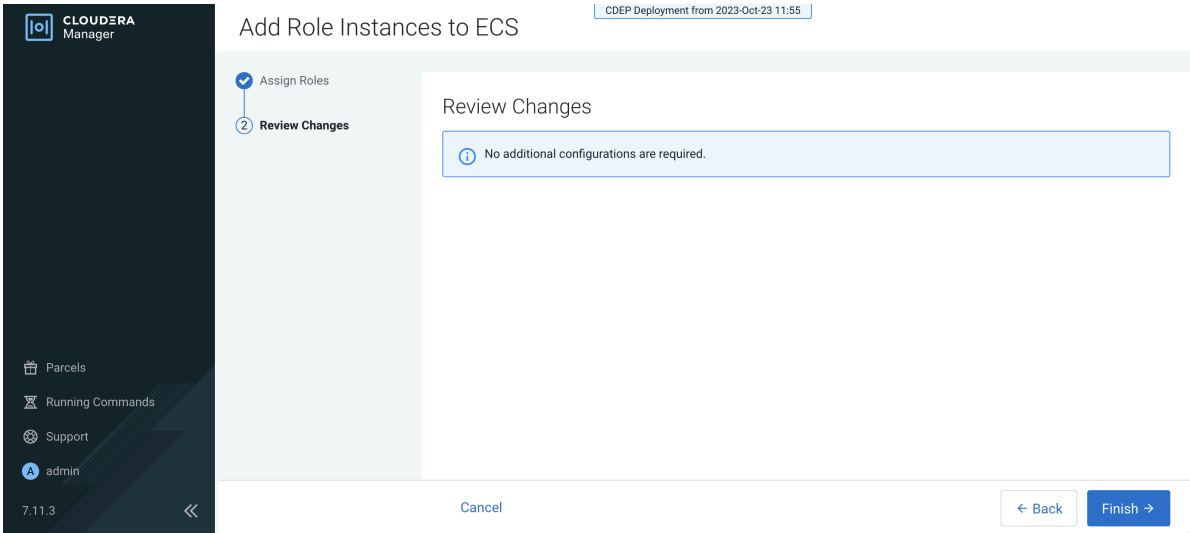
- c. On the Hosts Selected pop-up, select the new host, then click OK.



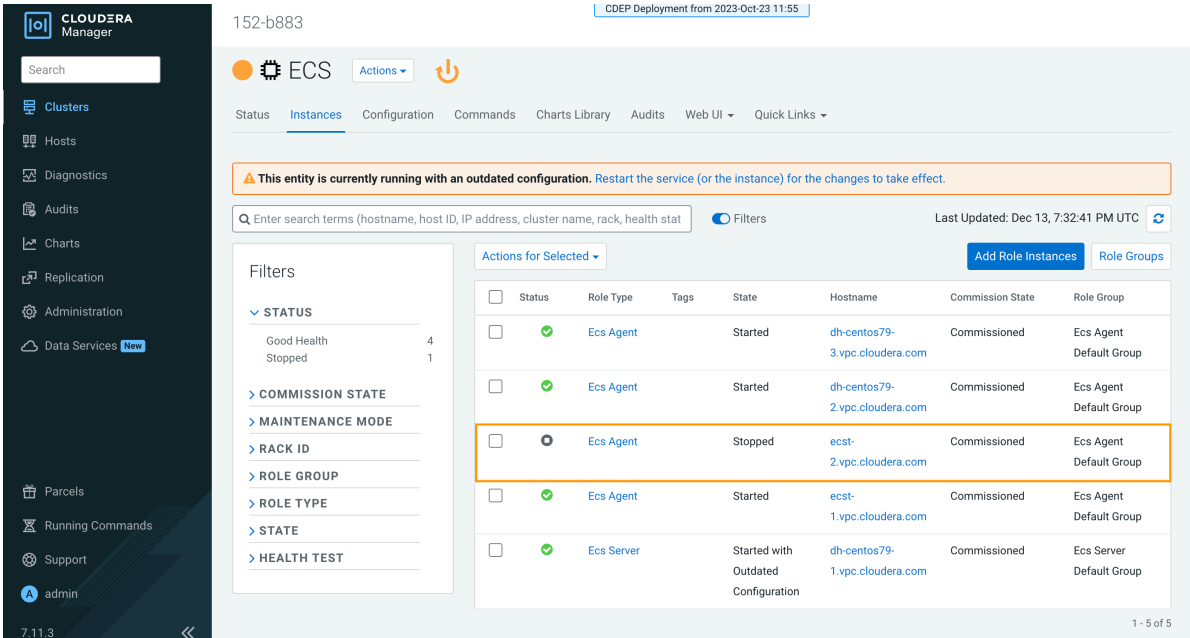
- d. On the Assign Roles page, click Continue.



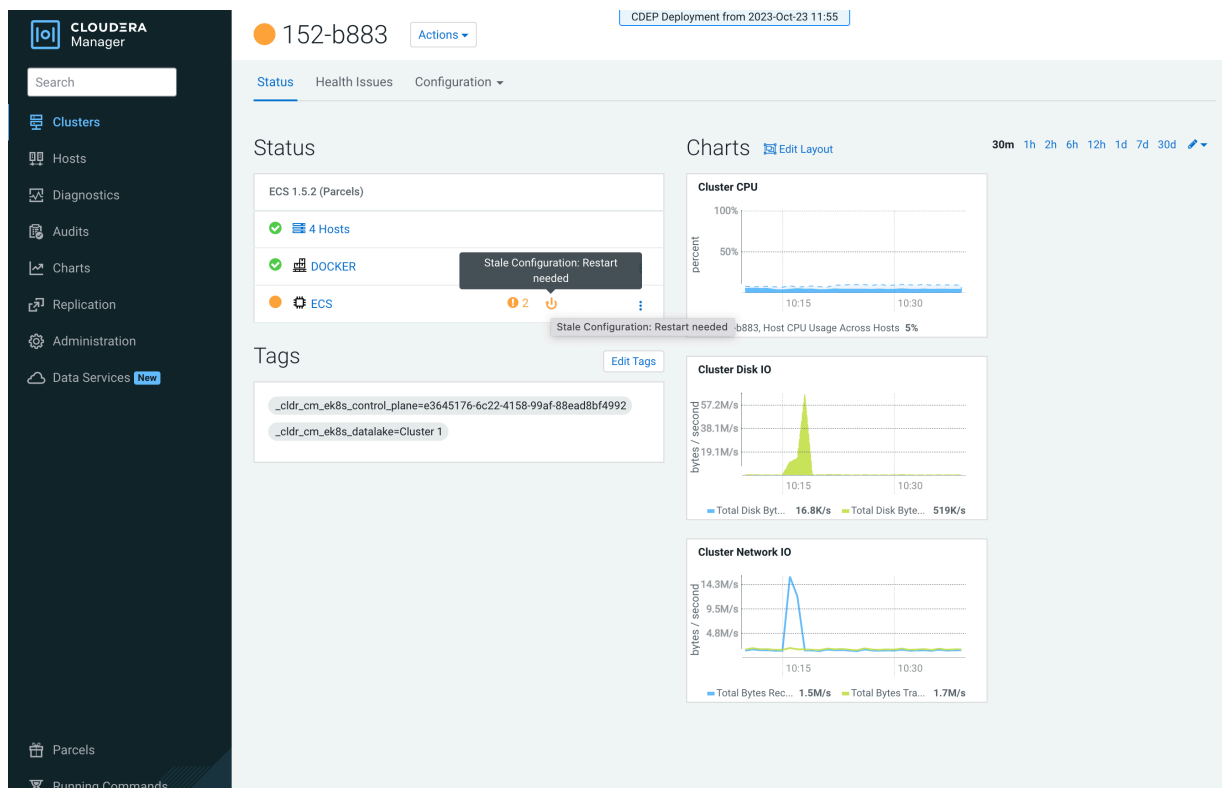
- e. On the Review Changes page, click Finish.



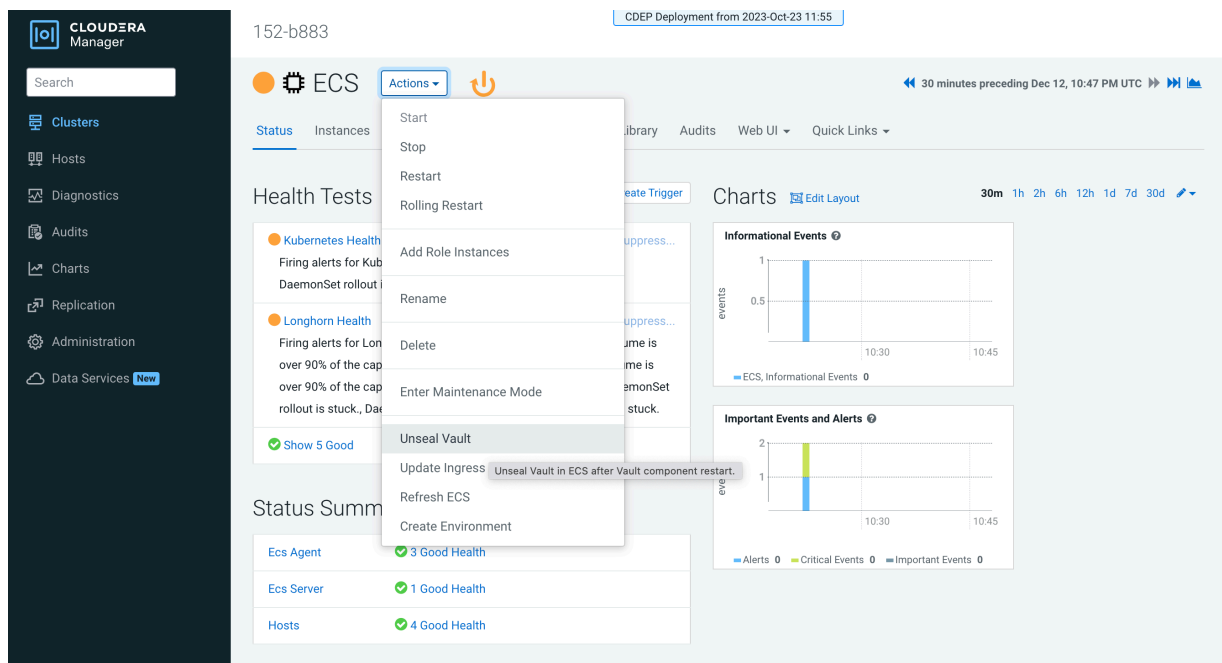
f. The new host is listed on the ECS Instances page.



17. Restart the ECS cluster by clicking the ECS Restart icon, or by selecting Actions > Restart on the ECS cluster home page.



18. Click ECS on the ECS cluster home page, then select Actions > Unseal Vault.



Starting, stopping, restarting, and refreshing Cloudera Embedded Container Service Clusters

Procedures to start, stop, restart, and refresh Cloudera Data Services on premises clusters

Starting a Cloudera Embedded Container Service Cluster

Procedure

1. On the Home Status tab, click the Actions Menu to the right of the Embedded Container Service cluster name and select Start.
2. Click the Start button that appears in the next screen to confirm. The Command Details window shows the progress of starting services.

Results

When the All services successfully started message appears, the task is complete and you can close the Command Details window.

Stopping a Cloudera Embedded Container Service Cluster

Procedure

1. On the Home Status tab, click the Actions Menu to the right of the Embedded Container Service cluster name and select Stop.
2. Click the Stop button in the confirmation screen. The Command Details window shows the progress of stopping services.

Results

When the All services successfully stopped message appears, the task is complete and you can close the Command Details window.



Note: The cluster-level Stop action does not stop the Cloudera Management Service. You must stop the Cloudera Management Service separately.

Restarting a Cloudera Embedded Container Service Cluster

Procedure

1. On the Home Status tab, click the Actions Menu to the right of the cluster name and select Restart.
2. Click the Restart button that appears in the next screen to confirm.
The Command Details window shows the Rolling Restart of services in the cluster. When all the services are restarted successfully, the task is complete and you can close the Command Details window.
3. Click Actions Unseal Vault

Rolling Restart of an Cloudera Embedded Container Service Cluster

Procedure

1. On the Home Status tab, click the Actions Menu to the right of the cluster name and select Rolling Restart.
2. Click the Rolling Restart button that appears in the next screen to confirm. On this screen, you can select the services (Docker or /and ECS), Roles (Workers only, Non-workers only, All Roles).



Note: Workers only refers to ECS agents, Non-workers only refers to all docker roles and ECS server.

The Command Details window shows the progress of rolling restart of a batch of nodes. Here, batch size refers to the number of worker roles that can be restarted in parallel. The Batch size is 1 by default.

3. Click Actions Unseal Vault

Configuring Restart for an Cloudera Embedded Container Service cluster

Procedure

1. Navigate to the ECS service, Home Configuration tab.
2. Select Node Readiness Timeout OR Drain Node Timeout configurations to configure overall restart time for an ECS cluster.



Note: Node Readiness Timeout is the maximum time for rescheduling workloads on a new node. This is 5 minutes by default.



Note: Drain Node Timeout is the time out to drain a node. This is 5 minutes by default.

Table 1: ECS Cluster Actions and Performance Impact

| ECS Cluster action | Affects Availability | Impact |
|---|---|------------------------|
| Stop and Start | Yes | All nodes |
| Restart | Least | one node at a time |
| Rolling restart (if the agent batch size is 1 then it is similar to Restart). | Inversely proportional to the batch size. | Depends on batch size. |

Refreshing a Cloudera Embedded Container Service Cluster

Procedure

To refresh a cluster, in the Home Status tab, click the Actions Menu to the right of the cluster name and select Refresh Cluster.



Note:

Refreshing an Cloudera Embedded Container Service cluster, runs a cluster refresh action to bring the configuration up to date without restarting all services.

Monitoring Cloudera Embedded Container Service Clusters

Procedures to monitor Embedded Container Service clusters

Related Information

[Monitoring Services](#)

[Monitoring Clusters](#)

[Docker Server Health Tests](#)

[Cloudera Embedded Container Service Health Tests](#)

[Cloudera Embedded Container Service Agent Health Tests](#)

[Cloudera Embedded Container Service Server Health Tests](#)

[Docker Server Metrics](#)

[Cloudera Embedded Container Service Agent Metrics](#)

[Cloudera Embedded Container Service Server Metrics](#)

Viewing Health Status

Procedure

1. Open the Cloudera Manager Admin Console.

2. From the Home page, Click on the Embedded Container Service cluster.
3. Click on the ECS or Docker service.

Results

The Service status page displays the Health Test, Status Summary and Health History of the services.

Viewing the Kubernetes Dashboard

About this task

The Kubernetes Dashboard displays configuration and other information about the embedded Kubernetes infrastructure used in the Cloudera Embedded Container Service cluster. Although you can make configuration changes using the dashboard (if you have the appropriate permissions), you should not make any changes using the dashboard. Cloudera Support may use the dashboard to diagnose problems with the cluster.

Procedure

1. In the Cloudera Manager Admin Console, go to the ECS service.
2. Click Web UI ECS Web UI

Results

The Kubernetes Dashboard displays.

Viewing the Cloudera Management Console on premises

Procedure

1. In the Cloudera Manager Admin Console, go to the ECS service.
2. Click Web UI Console

Results

The Cloudera Management Console displays.

Performing maintenance of a single host in the Cloudera Embedded Container Service cluster

You can perform maintenance on the nodes in your Cloudera Embedded Container Service cluster by shutting down the nodes one at a time.

Before you begin

- The containerized cluster must be configured for Cloudera Embedded Container Service Server high availability to reduce the downtime.
- You must be able to log into the nodes as root or have sudo privileges.
- The node to be maintained must have a status of Ready. A status of NotReady may suggest the node is having other complicating issues. Run the following command on an Cloudera Embedded Container Service server node to verify status of the nodes.

```
/var/lib/rancher/rke2/bin/kubectl --kubeconfig=/etc/rancher/rke2/rke2.yaml  
get nodes
```

Procedure

1. Log in to the Cloudera Manager Admin Console.

2. Stop the ECS role and the Docker server role on the host.
 - Click the Hosts tab.
 - Select the Host->Action->Stop roles on the host.
3. Perform the maintenance on the host.
4. Reboot the host.
5. Log in to the Cloudera Manager Admin Console.
6. Click the Action menu next to the ECS cluster and select Start roles on the host.
7. Click Actions Refresh ECS Cluster.
8. Go to the ECS service page and verify that the Vault is not sealed. This information displays in the Health Tests section.
9. If the Vault is sealed, click Actions Unseal Vault .

Performing the maintenance of all hosts in the Embedded Container Service cluster

If you want to perform the maintenance of all hosts in the ECS cluster follow below steps:

Procedure

1. Log in to the Cloudera Manager Admin Console.
2. Click the Action menu next to the ECS cluster and select Stop.
3. Perform the maintenance on all the hosts.
4. Reboot the hosts.
5. Log in to the Cloudera Manager Admin Console.
6. Click the Action menu next to the ECS cluster and select Start.
7. Click Actions Refresh ECS Cluster .
8. Go to the ECS service page and verify that the Vault is not sealed. This information displays in the Health Tests section.
9. If the Vault is sealed, click Actions Unseal Vault .

Configuring a containerized cluster with SELinux

This section provides the steps required to run the Cloudera Embedded Container Service with SELinux enabled. If you are not planning to enable SELinux, you do not need to follow these instructions.

Before you begin



Note:

Enabling SELinux enhances system security by enforcing strict access controls, limiting the potential damage from compromised processes. This means even if an application is exploited, SELinux restricts its actions, preventing it from accessing sensitive data or impacting other system components.

1. Ensure that the hosts you use for the containerized cluster meet all [hardware](#) and [software](#) requirements for use with Cloudera Data Services on premises.
2. Ensure SELinux is disabled on your ECS hosts. You can use the `getenforce` command to check its status.

Procedure

1. Ensure system compatibility: Verify your system meets all [hardware](#) and [software](#) requirements.
2. Enable SELinux in Permissive mode by updating the `/etc/selinux/config` file on all ECS hosts by running the following commands:

```
sed -i 's/SELINUX=disabled/SELINUX=permissive/' /etc/selinux/config
```

```
reboot
```

These commands update the SELinux configuration to permissive mode.



Note: Setting the mode to permissive initially allows you to install the Rancher-provided `rke2-selinux` RPM and continue with ECS installation without any issues. The reason for enabling SELinux in permissive mode initially is to avoid a restart when switching from SELinux disabled mode to SELinux enabled mode. When switching from permissive to enforcing mode (That is, SELinux is enabled in both cases), a reboot of the host is not required.

3. Install the SELinux policies provided by RKE2 by installing the RPMs on all ECS hosts. Use the following commands:

```
yum localinstall -y
http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm
wget https://github.com/rancher/rke2-selinux/releases/download/v0.8.stable.2/rke2-selinux-0.8-2.el7.noarch.rpm
yum install -y rke2-selinux-0.8-2.el7.noarch.rpm
```

These commands install the necessary SELinux policies to support ECS.

4. Uninstall the `nsd` service by running the following command on all ECS hosts :

```
yum erase -y nsd
```



Note: Uninstalling the `nsd` service is required to prevent issues with Cloudera Manager Agent heartbeats (on ECS hosts) sent to Cloudera Manager Server.

5. Install a containerized cluster on all hosts. See [Adding a Cloudera on Premises Data Services cluster](#).
6. Enable SELinux in Enforced mode by running the following commands on all ECS hosts:

```
setenforce 1
```

You can confirm that SELinux is running in Enforced mode by running the following command:

```
getenforce
```

This command switches SELinux from permissive to enforcing mode without a reboot.

7. Check the SELinux status with `getenforce`.
8. Verify that the ECS cluster hosts are sending heartbeats to the Cloudera Manager server.
 - a) Open the Cloudera Manager Admin Console.
 - b) Click Hosts All Hosts .
 - c) Check the Last Heartbeat column for heartbeat status.
9. Verify that your workloads are functioning as expected.

Decommissioning Cloudera Embedded Container Service Hosts

You can decommission Cloudera Embedded Container Service hosts and remove them from the cluster.

About this task

1. Cordon the node. Longhorn will automatically disable the node scheduling when a Kubernetes node is cordoned. Run the following command on any Cloudera Embedded Container Service host:

```
kubectl cordon [***NODE***]
```

2. Drain the node to move the workload to somewhere else. Run the following command on any ECS Server host:

```
kubectl drain [***NODE***] --ignore-daemonsets --pod-selector='app!=csi-attacher,app!=csi-provisioner' --delete-emptydir-data
```

3. Detach all the volumes on the node. Navigate to the ECS Service page on Cloudera Manager UI.
 - a. In the Web UI dropdown, select Storage UI to open the Longhorn UI.
 - b. Under the Volume tab in Longhorn UI, select the volumes on this node. Click Detach and select Yes on the screen prompt.

If the node has been drained, all the workloads should be migrated to another node already.

If there are any other volumes remaining attached, detach them before continuing.

4. Remove the node from Longhorn using the Delete in the Node tab. Or, remove the node from Kubernetes. Run the following command on any ECS Server host:

```
kubectl delete node [***NODE-NAME***]
```

Longhorn will automatically remove the node from the cluster.

5. Uninstall ECS and Docker artifacts from the host. Run below commands on the host:

```
cd /opt/cloudera/parcels/ECS/bin
./rke2-killall.sh # usually 2 times is sufficient
./rke2-uninstall.sh
rm -rf /ecs/* # assumes the default defaultDataPath and IsoDataPath
rm -rf /var/lib/docker_server/* # deletes the auth and certs
rm -rf /etc/docker/certs.d/* # delete the ca.crt
rm -rf /docker # assumes the default defaultDataPath for docker
```

6. Go to the Hosts page for the ECS Cluster, select that host, and under Actions for Selected, click Begin Maintenance (Suppress Alerts/Decommission)



Note: The node hosting Docker Server role cannot be decommissioned even if an external docker registry is used.



Note: Removing a host with the embedded docker registry is not supported.

If you are decommissioning a host on an Cloudera Embedded Container Service, ensure that the host is not an embedded docker registry host. Here are the two approaches to follow to check if a host has the embedded docker registry:

- a. Find the latest process directory of ECS-Server and check the config under registries.yaml:

```
cd $(ls -lrt /var/run/cloudera-scm-agent/process/*ECS_SERVER | tail -1) && awk '/^configs:/,0' registries.yaml
```

- b. From Cloudera Manager database, run the below query to identify the registry hosts details:

```
SELECT config_id, role_id, attr, value FROM configs WHERE attr LIKE '%docker%';
```

Dedicating Cloudera Embedded Container Service nodes for specific workloads

You use Cloudera Manager to dedicate Cloudera Embedded Container Service cluster nodes for specific workloads. You can dedicate GPU nodes for Cloudera AI Workbenches, and NVME nodes for Cloudera Data Warehouse workloads.

Dedicating Cloudera Embedded Container Service nodes when creating a new cluster

1. Check the [ECS installation requirements](#).
2. [Add the new hosts to Cloudera Manager](#).
3. In Cloudera Manager, click Hosts > All Hosts, then select one or more of the new ECS hosts.
4. Click the Configuration tab, then use the Search box to locate the node_taint configuration property.
5. Select Dedicated GPU Node to dedicate the node for Cloudera AI Workbenches, or select Dedicated NVME node to dedicate the node for Cloudera Data Warehouse workloads.

When either of these options are selected, no other workload pods will be allowed to run on the dedicated node.

6. Click Save Changes.
7. Run the following command to label the dedicated NVME node for Cloudera Data Warehouse workloads:

```
kubectl label node <node name> cdw.cloudera.com/dedicated-executor-host=
<any value>
```

8. Repeat the previous steps to add the other Cloudera Embedded Container Service hosts to Cloudera Manager and assign workload types.
9. Follow the [ECS installation procedure](#). When you reach the Specify Hosts page in the installation wizard, the hosts you added to Cloudera Manager appear. Select the hosts, click Continue, then proceed through the rest of the installation wizard.
10. After the installation is complete, the applicable workloads will only run on the specified dedicated nodes.

Dedicating Cloudera Embedded Container Service nodes in an existing cluster

1. Open the Cloudera Manager Admin Console.
2. On the Home page, click the ECS Cluster.
3. Click Hosts, select one or more of the ECS hosts, then click the Configuration tab.
4. Click the Configuration tab, then use the Search box to locate the node_taint configuration property.

5. Select Dedicated GPU Node to dedicate the node for CML workloads, or select Dedicated NVME node to dedicate the node for CDW workloads.

When either of these options are selected, no other workload pods will be allowed to run on the dedicated node.

6. Click Save Changes.
7. Run the following command to label the dedicated NVME node for Cloudera Data Warehouse workloads:

```
kubectl label node <node name> cdw.cloudera.com/dedicated-executor-host=
<any value>
```

8. Repeat the previous steps to assign workload types to the other ECS hosts.
9. On the ECS Cluster landing page, click Actions > Refresh Cluster.
10. After the Refresh is complete, click Actions > Rolling Restart.

Specifying racks for Cloudera Embedded Container Service clusters

You use Cloudera Manager to assign Cloudera Embedded Container Service cluster hosts to different racks.

About this task

- Each rack needs a different name and hence hosts in an Cloudera Embedded Container Service cluster will have different rack names.
- Cloudera Embedded Container Service cluster hosts with no specified rack name are assigned the default rack name value. The default value means that no rack name has been specified for the ECS cluster hosts.

Specifying a rack name for an Cloudera Embedded Container Service cluster

1. In Cloudera Manager, select the ECS cluster, then click Hosts.

2. In the Hosts list, click the top checkbox to select all of the cluster hosts.

CLUSTERA
Manager

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Data Services New

152-b813

CDEP Deployment from 2023-Sep-26 08:29

Cust

Hosts

ConfigurationAdd HostsReview Upgrade StatusInspect Hosts in ClusterInspect Cluster Network Performance

Search

Filters

Last Updated: Oct 1, 7:41:54 PM UTC

Columns: 11 Selected

Filters

STATUS

Good Health3

CLUSTERS

CORES

COMMISSION STATE

LAST HEARTBEAT

LOAD (1 MINUTE)

LOAD (5 MINUTES)

LOAD (15 MINUTES)

MAINTENANCE MODE

UPGRADE DOMAIN

RACK

SERVICE

Actions for Selected (3)

| Status | Name | IP | Roles | Tags | Commission Stat |
|-------------------------------------|--------------------------------|---------------|---------|------|-----------------|
| <input checked="" type="checkbox"/> | dh-centos79-1.vpc.cloudera.com | 10.65.201.209 | 2 Roles | | Commissioned |
| <input checked="" type="checkbox"/> | dh-centos79-2.vpc.cloudera.com | 10.65.194.34 | 2 Roles | | Commissioned |
| <input checked="" type="checkbox"/> | dh-centos79-3.vpc.cloudera.com | 10.65.200.38 | 2 Roles | | Commissioned |

1 - 3 of 3

3. Click Actions for Selected, then click Assign Rack.

CLUSTERA
Manager

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Data Services New

152-b813

CDEP Deployment from 2023-Sep-26 08:29

Cust

Hosts

ConfigurationAdd HostsReview Upgrade StatusInspect Hosts in ClusterInspect Cluster Network Performance

Search

Filters

Last Updated: Oct 1, 7:47:54 PM UTC

Columns: 11 Selected

Filters

STATUS

Good Health3

CLUSTERS

CORES

COMMISSION STATE

LAST HEARTBEAT

LOAD (1 MINUTE)

LOAD (5 MINUTES)

LOAD (15 MINUTES)

MAINTENANCE MODE

UPGRADE DOMAIN

RACK

SERVICE

Actions for Selected (3)

Assign Rack

Assign Upgrade Domain

Regenerate Keytab

Apply Host Template

Start Roles on Hosts

Stop Roles on Hosts

Begin Maintenance (Suppress Alerts/Decommission)

End Maintenance (Enable Alerts/Recommission)

Edit Tags

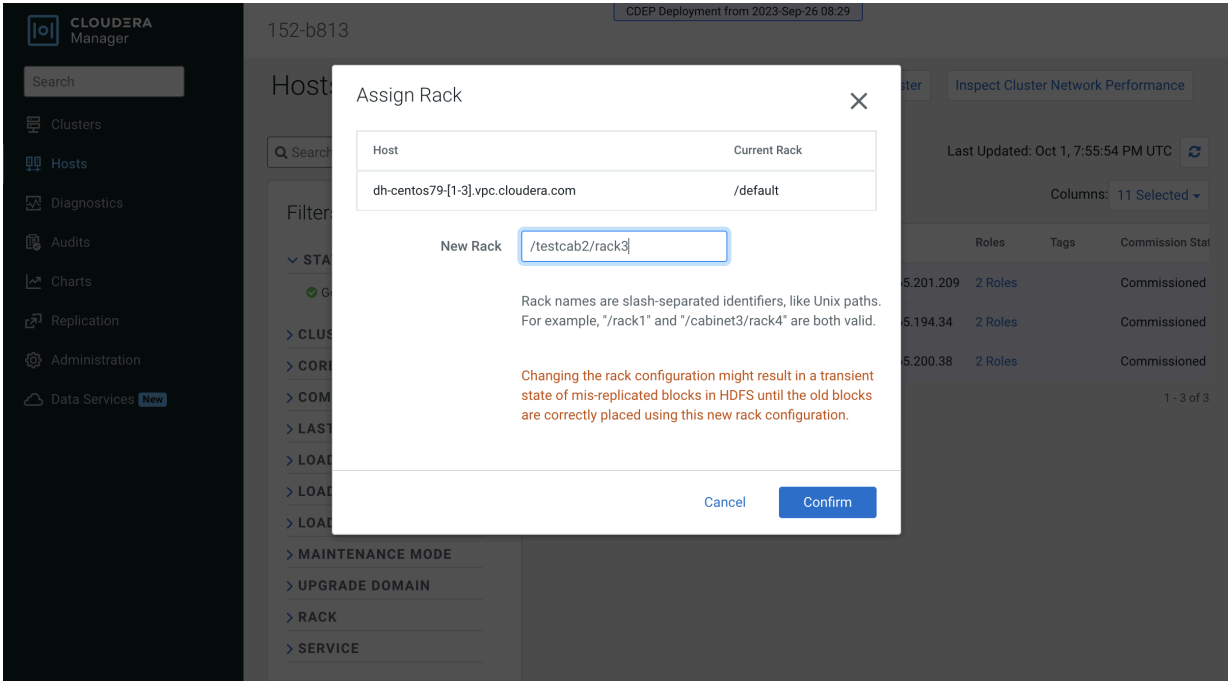
Remove From Cluster

Remove From Cloudera Manager

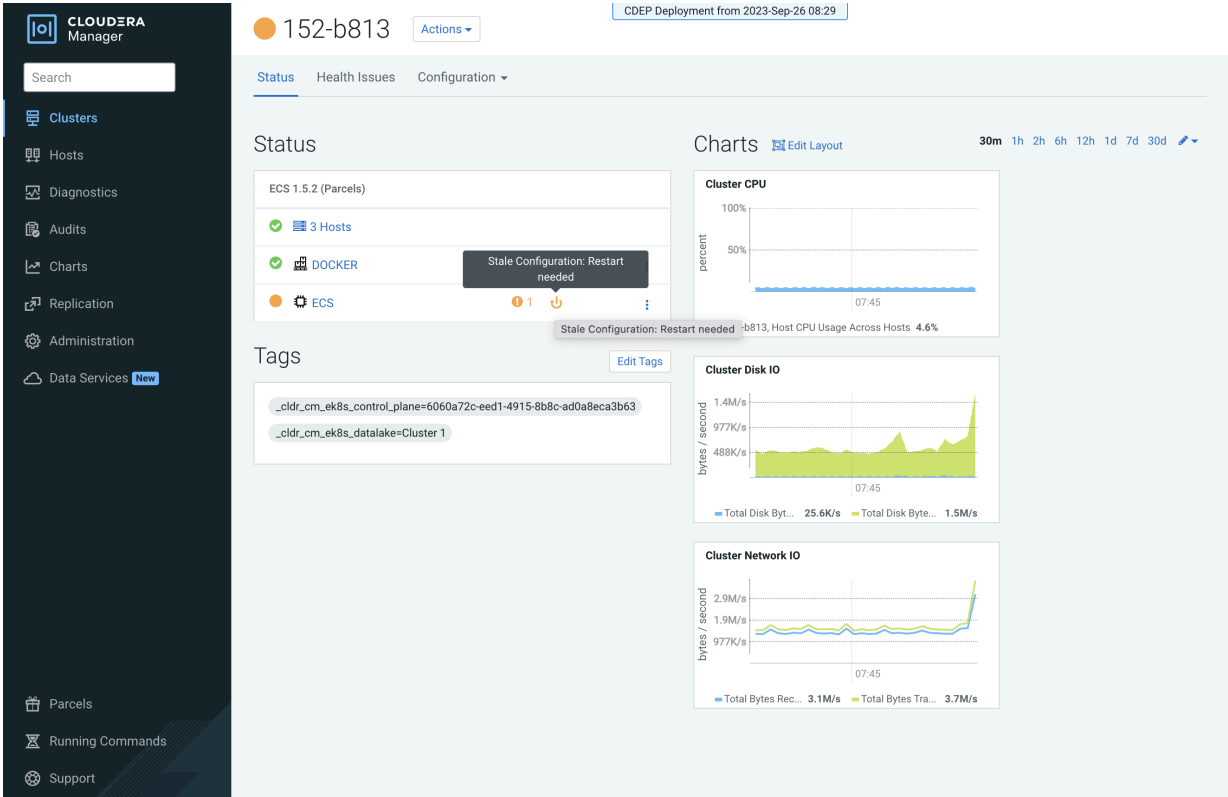
| Roles | Tags | Commission Stat |
|-----------------|------|-----------------|
| 201.209 2 Roles | | Commissioned |
| .194.34 2 Roles | | Commissioned |
| .200.38 2 Roles | | Commissioned |

1 - 3 of 3

4. On the Assign Rack popup, enter a rack name in the New Rack box, then click Confirm.



5. Cloudera Manager detects this configuration change, and displays a Stale Configuration warning. You must restart the cluster in order for the updated configuration to take effect.



- Click the Stale Configuration icon, then click Restart Stale Services and click through the Restart wizard.

152-b813

CDEP Deployment from 2023-Sep-26 08:29

Stale Configurations

Filters [Clear All](#)

- FILE**
 - File: config.yaml 3
- SERVICE** [Clear](#)
 - ECS 3
- ROLE TYPE**
 - Ecs Agent 2
 - Ecs Server 1

File: config.yaml [ecs\(1\)](#) [Show](#)

```

... .. @@ -1,7 +1,7 @@
1 1 node-label:
2 2 - "ecs_role=master"
3 3 - "rack=default"
4 4 + "rack=testcab2.rack3"
5 5 private-registry:
6 6 - "${CONF_CONF_DIR}/registries.yaml"
7 7 node-taint:
8 8 - "node-role.kubernetes.io/control-plane=true:NoSchedule"

```

File: config.yaml [ecs\(1\)](#) [Show](#)

```

... .. @@ -6,6 +6,6 @@
6 6 - "kubelet-cgroups=/systemd/system.slice/cloudera-scm-supervisord.service"
7 7 node-name:
8 8 - "dh-centos79-2.vpc.cloudera.com"
9 9 node-label:
10 10 - "rack=default"
11 11 + "rack=testcab2.rack3"

```

File: config.yaml [ecs\(1\)](#) [Show](#)

```

... .. @@ -6,6 +6,6 @@
6 6 - "kubelet-cgroups=/systemd/system.slice/cloudera-scm-supervisord.service"
7 7 node-name:
8 8 - "dh-centos79-3.vpc.cloudera.com"
9 9 node-label:
10 10 - "rack=default"
11 11 + "rack=testcab2.rack3"

```

[Restart Stale Services](#)

- When the Restart is complete, you can use the Assign Rack popup to confirm that the new rack name has been applied to the ECS cluster hosts.

152-b813

CDEP Deployment from 2023-Sep-26 08:29

Hosts

Search

Filters

STATUS

CLUSTER

CORES

COMMISSIONED

LAST HEARTBEAT

LOAD (1)

LOAD (5)

LOAD (1)

MAINTENANCE MODE

UPGRADE DOMAIN

RACK

Assign Rack

Host: dh-centos79-[1-3].vpc.cloudera.com

Current Rack: /testcab2/rack3

New Rack:

Rack names are slash-separated identifiers, like Unix paths. For example, "/rack1" and "/cabinet3/rack4" are both valid.

Changing the rack configuration might result in a transient state of mis-replicated blocks in HDFS until the old blocks are correctly placed using this new rack configuration.

[Cancel](#) [Confirm](#)

- You can also use the ECS Web UI to view cluster host rack assignments. Select the ECS cluster, click ECS, then click Web UI > ECS Web UI . In the Web UI, select the CDP namespace, then click Nodes.

Note that in Kubernetes periods are used as separators (rather than slashes) in the rack name path. The leading slash is also not used in Kubernetes.

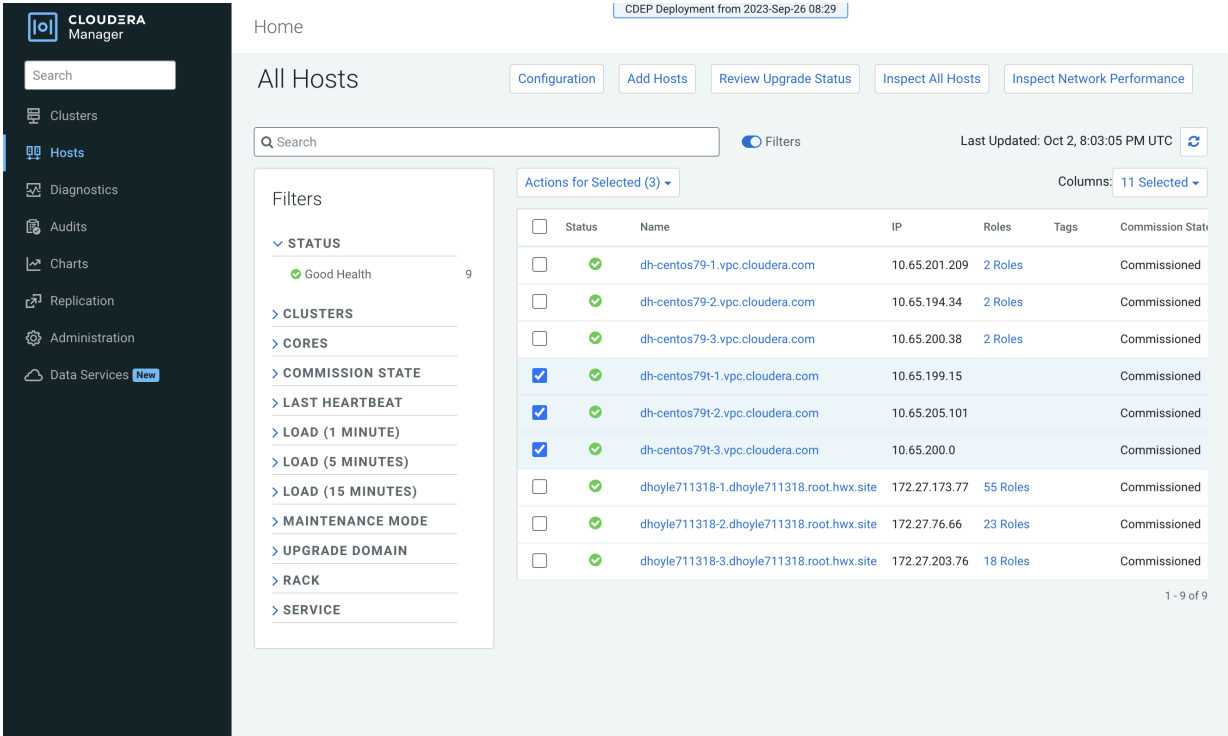
| Name | Labels | CPU Ready requests (cores) | CPU limits (cores) | CPU capacity (cores) | Memory requests (bytes) | Memory limits (bytes) | Memory capacity (bytes) | Pods |
|--------------------------------|--|----------------------------|--------------------|----------------------|-------------------------|-----------------------|-------------------------|--------------------|
| dh-centos79-3.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 beta.kubernetes.io/os: linux kubernetes.io/arch: amd64 kubernetes.io/hostname: dh-centos79-3.vpc.cloudera.com kubernetes.io/os: linux rack: testcab2.rack3 | True | 6.07 (75.81%) | 6.95 (86.88%) | 8.00 | 8.82Gi (28.61%) | 29.13Gi (94.54%) | 30.81Gi 39 (7.8) |
| dh-centos79-2.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 beta.kubernetes.io/os: linux kubernetes.io/arch: amd64 kubernetes.io/hostname: dh-centos79-2.vpc.cloudera.com kubernetes.io/os: linux rack: testcab2.rack3 | True | 7.92 (99.01%) | 7.55 (94.38%) | 8.00 | 13.78Gi (45.21%) | 28.98Gi (95.07%) | 30.48Gi 48 (9.6) |
| dh-centos79-1.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 beta.kubernetes.io/os: linux ecs_role: master kubernetes.io/arch: amd64 kubernetes.io/hostname: dh-centos79-1.vpc.cloudera.com kubernetes.io/os: linux node-role.kubernetes.io/control-plane: true node-role.kubernetes.io/etcd: true node-role.kubernetes.io/master: true rack: testcab2.rack3 | True | 7.97 (99.63%) | 11.35 (141.88%) | 8.00 | 11.36Gi (36.88%) | 29.85Gi (96.90%) | 30.81Gi 57 (11.40) |

Specifying a rack name when creating a new ECS cluster

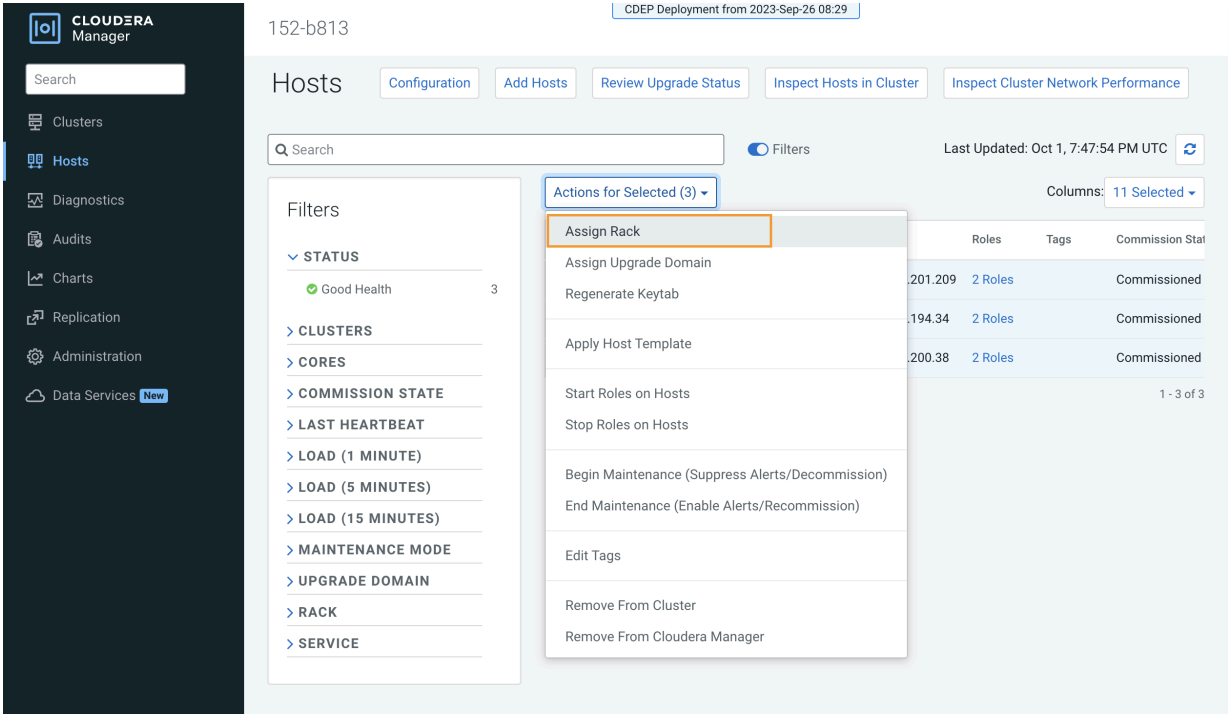
Currently the ECS installation wizard does not enable you to assign rack names when creating a new ECS cluster. Therefore, you should first add the new set of ECS hosts to Cloudera Manager, and then assign the rack name in Cloudera Manager. You can then use the ECS installation wizard to create a new ECS cluster using these hosts.

- Check the [ECS installation requirements](#).
- [Add the new hosts to Cloudera Manager](#).

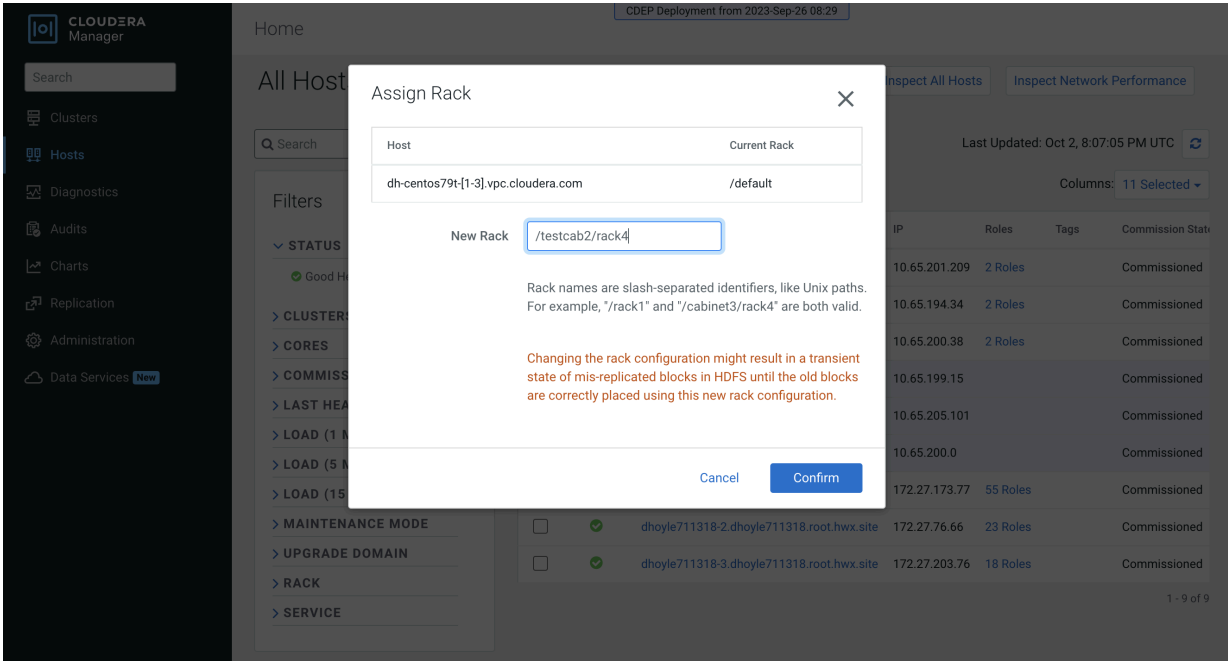
3. In Cloudera Manager, click Hosts > All Hosts, then select the hosts you just added.



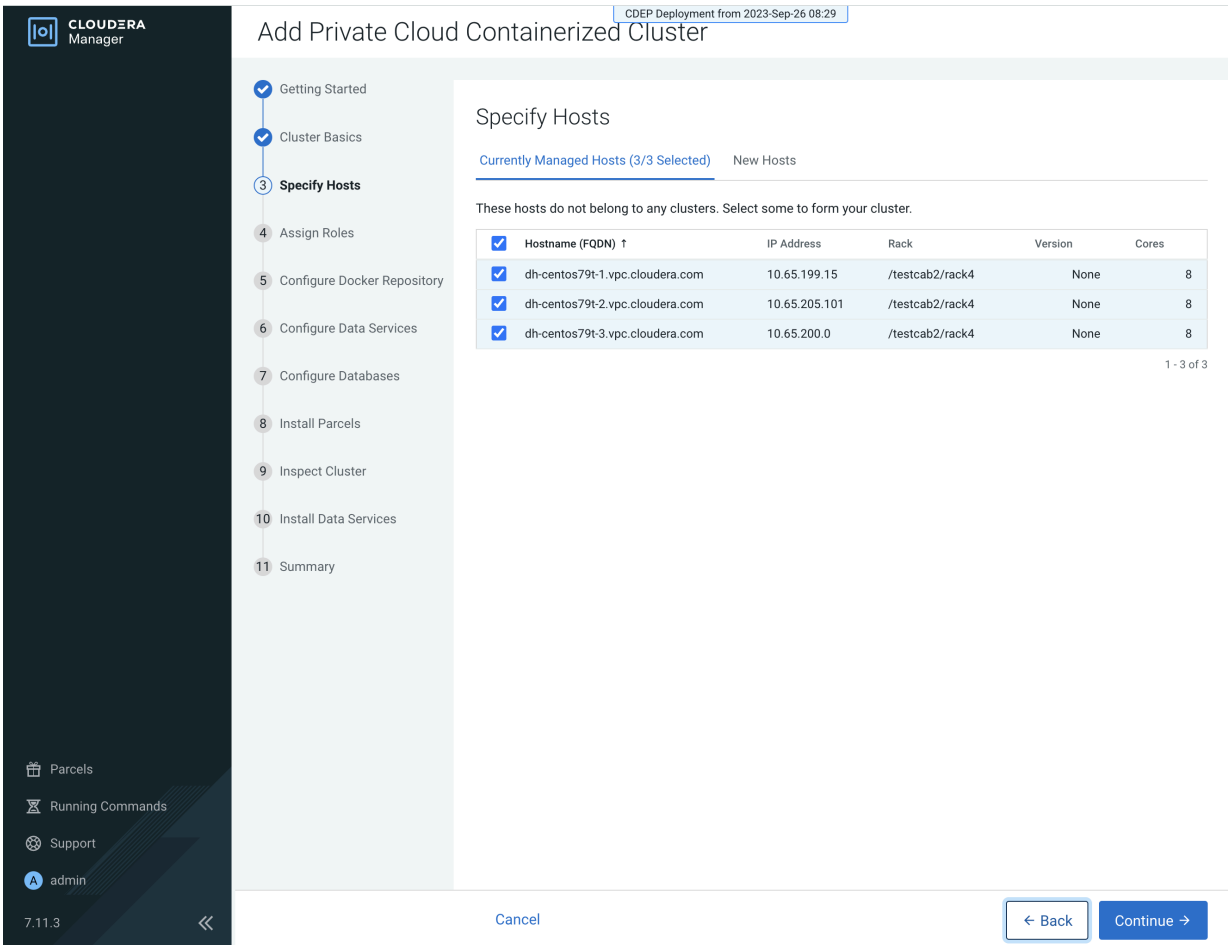
4. Click Actions for Selected, then click Assign Rack.



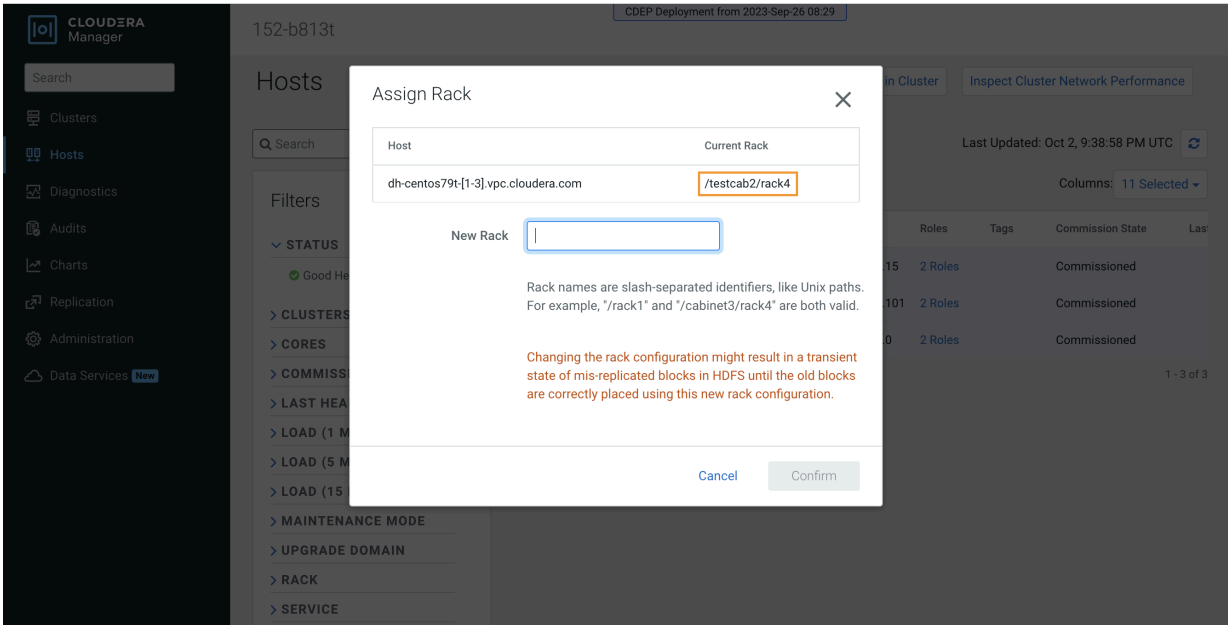
5. On the Assign Rack popup, enter a rack name in the New Rack box, then click Confirm.




6. Follow the [ECS installation procedure](#). When you reach the Specify Hosts page in the installation wizard, the hosts you added to Cloudera Manager appear. Select the hosts, click Continue, then proceed through the rest of the installation wizard.







- 7. After the installation is complete, you can use the Assign Rack popup or the ECS Web UI to view the rack assignments for the ECS cluster hosts.



kubernetes

cdp

 Search



Cluster > Nodes

Daemon Sets

Deployments

Jobs

Pods

Replica Sets

Replication Controllers

Stateful Sets

Service

Ingresses

Ingress Classes

Services

Config and Storage

Config Maps

Persistent Volume Claims

Secrets

Storage Classes

Cluster

Cluster Role Bindings

Cluster Roles

Events

Namespaces

Network Policies

Nodes

Persistent Volumes

Role Bindings

Roles




Service Accounts

Custom Resource Definitions

Settings

About

Nodes

| Name | Labels | Ready | CPU requests (cores) | CPU limits (cores) | CPU capacity (cores) | Memory requests (bytes) | Memory limits (bytes) | Memory capacity (bytes) | Pods |
|---|---|-------|----------------------|--------------------|----------------------|-------------------------|-----------------------|-------------------------|-------------|
|  dh-centos79t-2.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 | True | 7.44 (93.03%) | 5.10 (63.75%) | 8.00 | 26.18Gi (85.88%) | 21.64Gi (70.99%) | 30.48Gi | 49 (9.80%) |
| | beta.kubernetes.io/os: linux | | | | | | | | |
| | kubernetes.io/arch: amd64 | | | | | | | | |
| | kubernetes.io/hostname: dh-centos79t-2.vpc.cloudera.com | | | | | | | | |
| | kubernetes.io/os: linux | | | | | | | | |
| rack: testcab2.rack4 | Show less | | | | | | | | |
|  dh-centos79t-3.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 | True | 7.62 (95.26%) | 8.35 (104.38%) | 8.00 | 10.48Gi (34.40%) | 36.83Gi (120.83%) | 30.48Gi | 52 (10.40%) |
| | beta.kubernetes.io/os: linux | | | | | | | | |
| | kubernetes.io/arch: amd64 | | | | | | | | |
| | kubernetes.io/hostname: dh-centos79t-3.vpc.cloudera.com | | | | | | | | |
| | kubernetes.io/os: linux | | | | | | | | |
| rack: testcab2.rack4 | Show less | | | | | | | | |
|  dh-centos79t-1.vpc.cloudera.com | beta.kubernetes.io/arch: amd64 | True | 6.40 (79.94%) | 9.40 (117.50%) | 8.00 | 8.91Gi (28.93%) | 25.66Gi (83.30%) | 30.81Gi | 47 (9.40%) |
| | beta.kubernetes.io/os: linux | | | | | | | | |
| | ecs_role: master | | | | | | | | |
| | kubernetes.io/arch: amd64 | | | | | | | | |
| | kubernetes.io/hostname: dh-centos79t-1.vpc.cloudera.com | | | | | | | | |
| kubernetes.io/os: linux | | | | | | | | | |
| node-role.kubernetes.io/control-plane: true | | | | | | | | | |
| node-role.kubernetes.io/etcid: true | | | | | | | | | |
| node-role.kubernetes.io/master: true | | | | | | | | | |
| rack: testcab2.rack4 | | | | | | | | | |

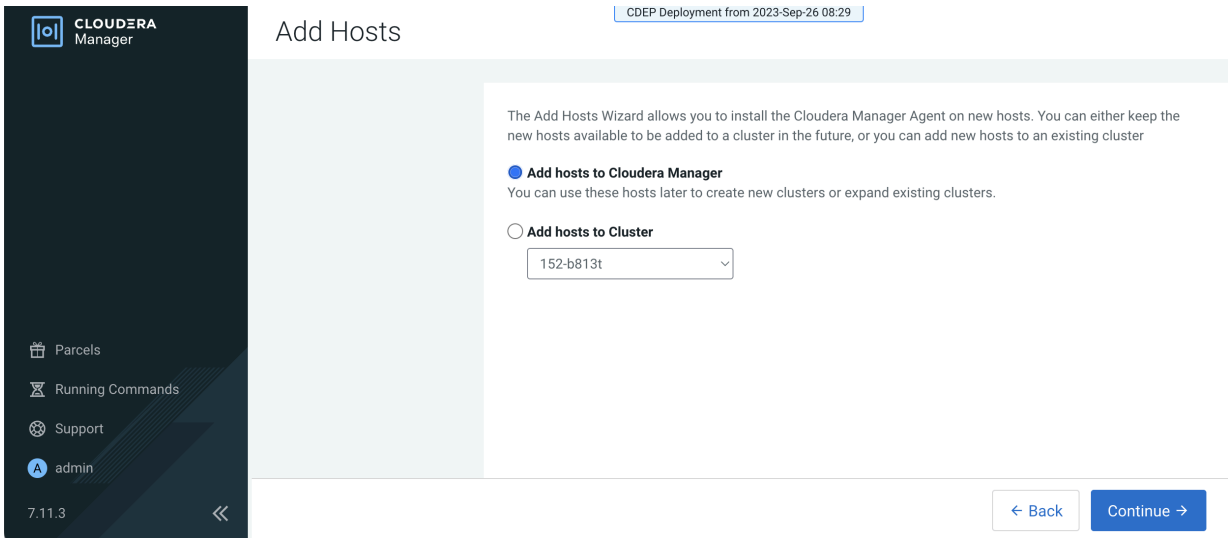
Adding a host to an ECS cluster with a previously specified rack name

When you add a host directly to an ECS cluster, there is no way to specify a rack name for the new host, so it will be assigned the default rack name. A configuration error will occur if you try to add a new host directly to an ECS cluster with a previously specified rack name, since the default rack name of the new host does not match the rack name previously assigned to the other cluster hosts.

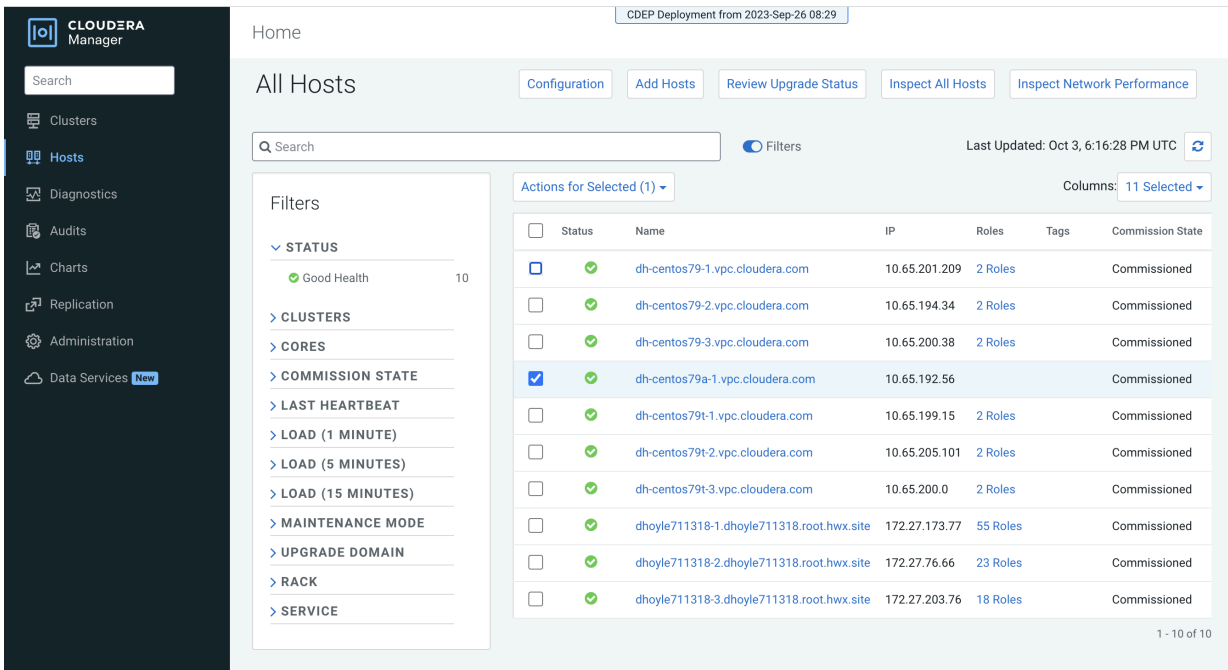
Therefore, you should first add the new ECS host to Cloudera Manager, and then use Cloudera Manager to assign the same rack name as the other ECS cluster hosts to the new host. You can then add the new host to the ECS cluster.

1. Check the [ECS installation requirements](#).

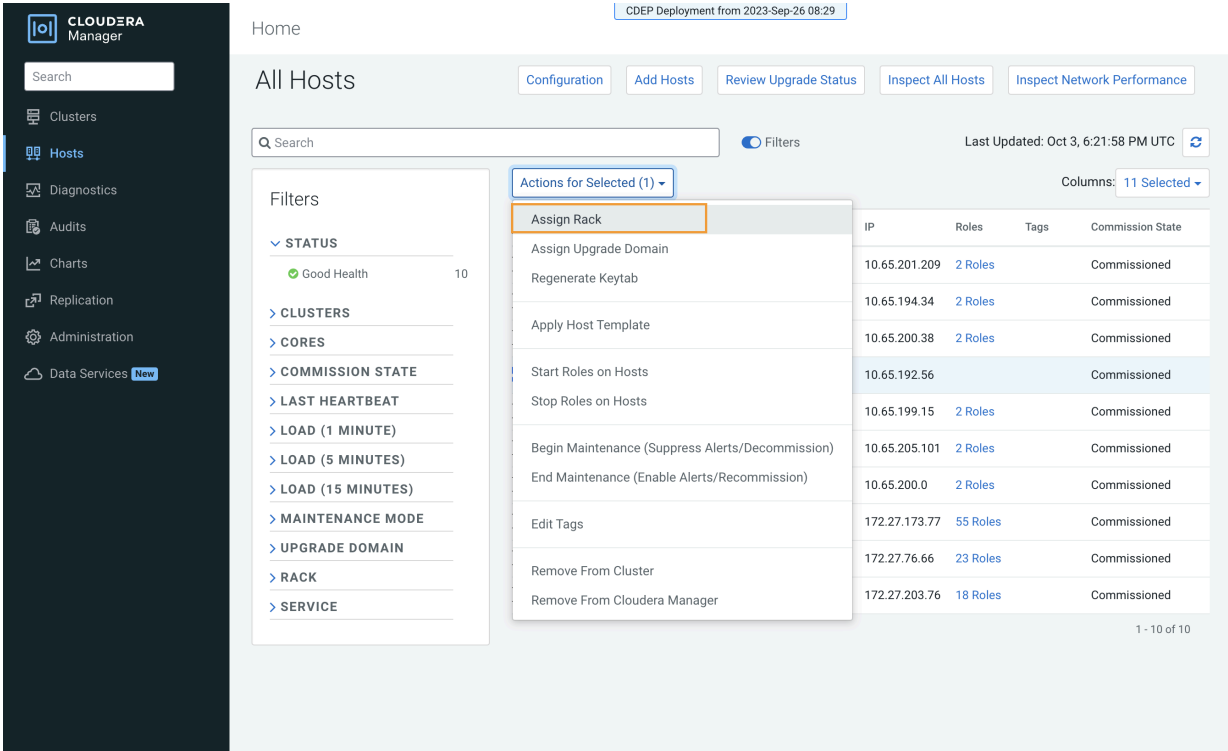
2. [Add the new hosts to Cloudera Manager](#). You can also access the Add Hosts wizard by clicking Hosts in the ECS cluster, and then clicking Add Hosts. Select Add hosts to Cloudera Manager.



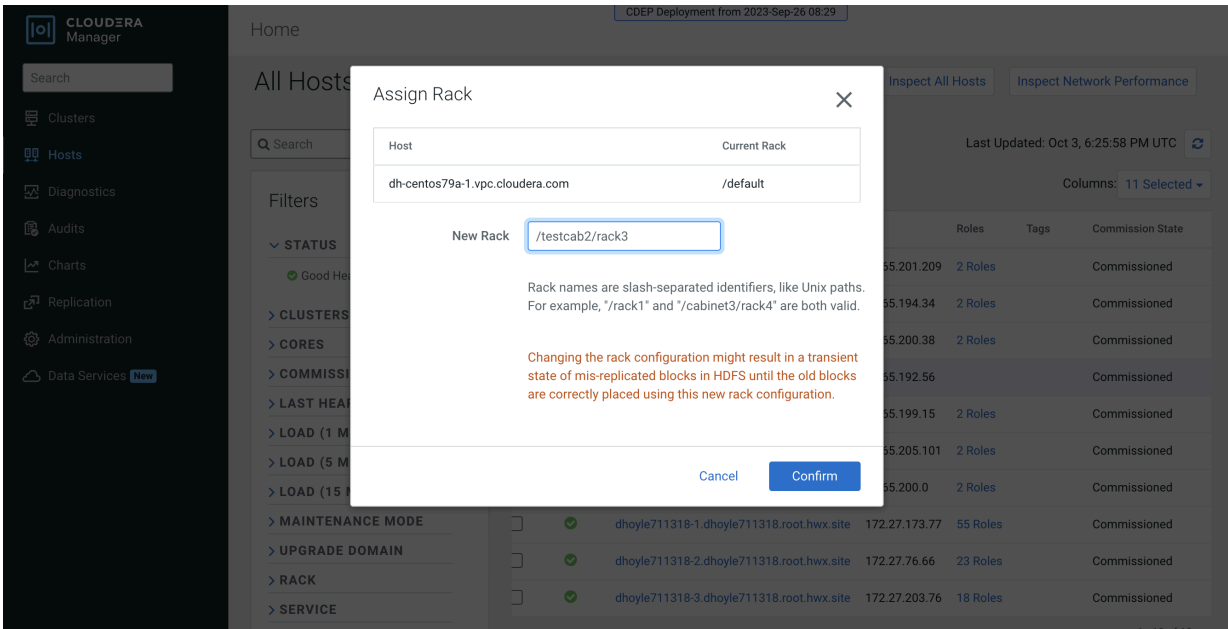
3. In Cloudera Manager, click Hosts, then select the host you just added.



4. Click Actions for Selected, then click Assign Rack.



5. On the Assign Rack popup, enter the same rack name assigned to the other ECS cluster hosts in the New Rack box, then click Confirm.



6. In the ECS cluster, click Hosts, then click Add Hosts. Select Add hosts to Cluster, then click Continue.

CLOUDERA Manager

Add Hosts

CDEP Deployment from 2023-Sep-26 08:29

The Add Hosts Wizard allows you to install the Cloudera Manager Agent on new hosts. You can either keep the new hosts available to be added to a cluster in the future, or you can add new hosts to an existing cluster

☐ Add hosts to Cloudera Manager
You can use these hosts later to create new clusters or expand existing clusters.

☒ Add hosts to Cluster


152-b813

Parcels
Running Commands
Support
admin

7.11.3

← Back Continue →

8. After the Add Host wizard is completed, the new host appears on the ECS cluster Hosts page.

 **CLOUDERA**
Manager

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Data Services New

152-b813

CDEP Deployment from 2023-Sep-26 08:29

Hosts

ConfigurationAdd HostsReview Upgrade StatusInspect Hosts in ClusterInspect Cluster Network Performance

Q Search

Filters

Last Updated: Oct 3, 6:56:46 PM UTC

Filters

STATUS

Good Health4

CLUSTERS

CORES

COMMISSION STATE

LAST HEARTBEAT

LOAD (1 MINUTE)

LOAD (5 MINUTES)

LOAD (15 MINUTES)

MAINTENANCE MODE

UPGRADE DOMAIN

RACK

SERVICE

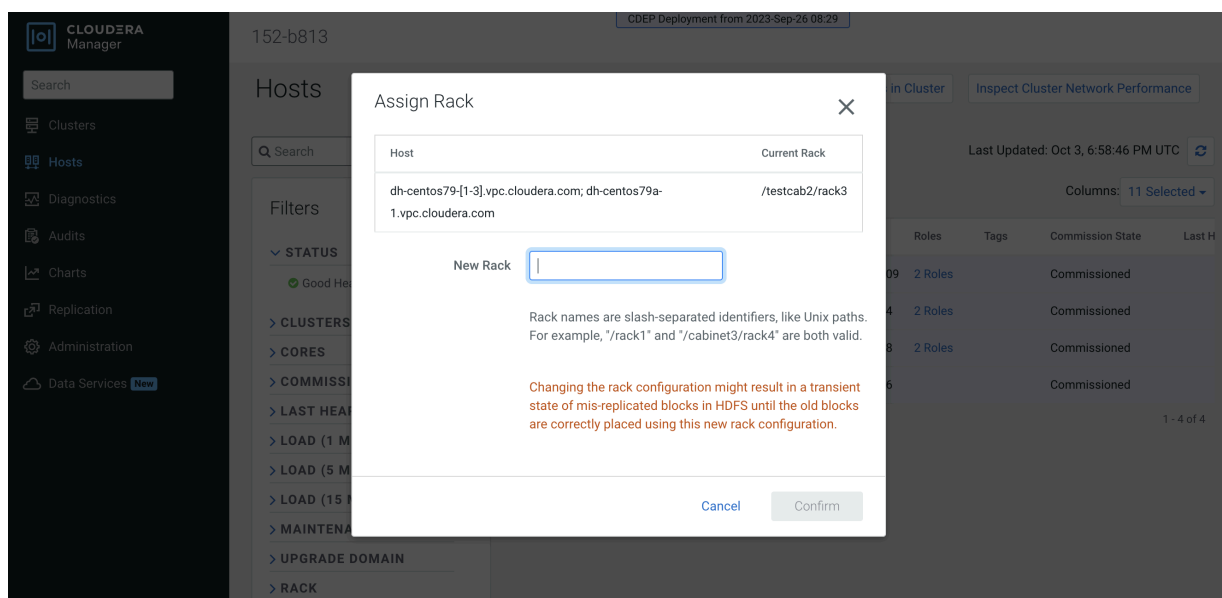
Actions for Selected (1)

Columns: 11 Selected

| <input type="checkbox"/> | Status | Name | IP | Roles | Tags | Commission State | Last H |
|-------------------------------------|--------|---------------------------------|---------------|---------|------|------------------|--------|
| <input type="checkbox"/> | ✓ | dh-centos79-1.vpc.cloudera.com | 10.65.201.209 | 2 Roles | | Commissioned | |
| <input type="checkbox"/> | ✓ | dh-centos79-2.vpc.cloudera.com | 10.65.194.34 | 2 Roles | | Commissioned | |
| <input type="checkbox"/> | ✓ | dh-centos79-3.vpc.cloudera.com | 10.65.200.38 | 2 Roles | | Commissioned | |
| <input checked="" type="checkbox"/> | ✓ | dh-centos79a-1.vpc.cloudera.com | 10.65.192.56 | | | Commissioned | |

1 - 4 of 4

9. You can use the Assign Rack popup to view the rack assignments for the ECS cluster hosts and confirm that the rack name for the new host matches the rack name of the other cluster hosts.



Unifying time zone for Cloudera Embedded Container Service

You can synchronize the Cloudera Embedded Container Service cluster time zone with the Cloudera Manager Base time zone.

In Cloudera Data Services on premises versions earlier than 1.5.2, containers running on an Cloudera Embedded Container Service Kubernetes cluster did not inherit the time zone settings from the Cloudera Manager Base host. In most cases, Kubernetes containers use Coordinated Universal Time (UTC) by default.

In Cloudera Data Services on premises 1.5.2 and higher versions, you can unify the time zone in the Cloudera Embedded Container Service cluster with the Cloudera Manager Base time zone. All workload pods in the Cloudera Embedded Container Service cluster run under the Cloudera Manager time zone, and workload logs on the Cloudera Embedded Container Service cluster are correlated with the Cloudera Manager Base logs. Timestamp-related SQL queries are also correlated.

- Unified time zone is enabled by default for new Cloudera Data Services on premises 1.5.2+ installs.
- When upgrading from earlier versions of Cloudera Data Services on premises to 1.5.2+, unified time zone is disabled by default to avoid affecting timestamp-sensitive logic.

You can enable or disable unified time zone using the following script in the Cloudera Embedded Container Service parcel:

```
bash /opt/cloudera/parcels/ECS/k8tz-webhook/configure-k8tz-webhook.sh -h
```

This script modifies the k8tz webhook settings.

Syntax:

```
configure-k8tz-webhook.sh [-i|-h]
```

Options:

- **i** – This option enables the unified time zone feature
- **No options** – To disable the unified time zone feature, run the `configure-k8tz-webhook.sh` script without any options.
- Use the **-h** flag to print Help information

To complete the process of enabling the unified time zone feature:

- Restart the workload pods where you want the Cloudera Manager Server timezone to be applied.

-OR-

- Initiate an Cloudera Embedded Container Service cluster rolling restart. This will inject the time zone information into all workload pods.

When the unified time zone feature is disabled, all running pods are not affected. To apply the new disabled setting so they run with the default UTC time zone, a pod restart or a rolling restart is required.

Adjusting the expiration time of Cloudera Embedded Container Service cluster certificates

The RKE Kubernetes, Vault, and Cloudera Embedded Container Service webhook certificate expiration times are set to one year by default. To avoid certificate expiration errors, you may want to extend the expiration times.

About this task

- These steps describe how to adjust the expiration time of internal cluster certificates in an existing Cloudera Embedded Container Service cluster.
- For a new cluster, if the nodes have been added to Cloudera Manager before creating the Cloudera Embedded Container Service cluster, you can edit the `cluster_signing_duration` configuration property in Cloudera Manager before creating the Cloudera Embedded Container Service cluster.

Adjusting the expiration time of the RKE Kubernetes cluster certificate



Note:

This topic only applies to internal certificates within Cloudera Embedded Container Service. It does not apply to the ingress controller certificate.

1. In Cloudera Manager, select the ECS cluster, then click ECS.
2. Click the Configuration tab, then use the Search box to locate the `cluster_signing_duration` configuration property.

- The `cluster_signing_duration` configuration property sets the expiration time for the RKE Kubernetes, Vault, and ECS webhook certificates, and is set to 1 year (365 days) by default. In the example below, the certificate expiration has been reset to 5 years (1825 days):

The screenshot shows the Cloudera Manager interface for an ECS cluster (ID: 153-b278). The left sidebar contains navigation options: Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Data Services (New), Parcels, Running Commands, Support, and a user profile for 'admin'. The main panel is titled 'ECS' and includes tabs for Status, Instances, Configuration (selected), Commands, Charts Library, Audits, Web UI, and Quick Links. A search bar at the top of the main panel contains 'cluster_signing_duration'. Below the search bar, there are filters for SCOPE (ECS (Service-Wide), Ecs Agent, Ecs Server) and CATEGORY (Main, Advanced, Monitoring, Performance, Ports and Addresses, Resource Management, Security). The STATUS filter shows Error (0), Warning (0), Edited (1), Non-Default (1), and Include Overrides (0). The main configuration area shows the 'Cluster Signing Duration' property set to 'ECS (Service-Wide)' with a value of '1825'. A 'Show All Descriptions' link is visible. At the bottom, a '1 Edited Value' message indicates a change, with a 'Reason for change' field containing 'Modified Cluster Signing Duration' and a 'Save Changes(CTRL+S)' button.

- Click Save Changes.
- On the ECS Cluster landing page, click Actions > Refresh Cluster.
- For versions:
 - Upto 1.5.4 SP1 after the Refresh is complete, click Actions > Rolling Restart.
 - From 1.5.4 SP2 and later, after the Refresh is complete, click Actions > Restart.
- After the restart is complete, the certificate expiration time is reset to the new value. You can also use the CLI to verify the new certificate expiration setting.

Adjusting the expiration time of the Vault certificate

- In Cloudera Manager, select the ECS cluster, then click ECS.
- Click the Configuration tab, then use the Search box to locate the `cluster_signing_duration` configuration property.

- The `cluster_signing_duration` configuration property sets the expiration time for the RKE Kubernetes, Vault, and ECS webhook certificates, and is set to 1 year (365 days) by default. In the example below, the certificate expiration has been reset to 5 years (1825 days):

The screenshot shows the Cloudera Manager interface for an ECS cluster (ID: 153-b278). The left sidebar contains navigation options: Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Data Services (New), Parcels, Running Commands, Support, and a user profile for 'admin'. The main panel is titled 'ECS' and has tabs for Status, Instances, Configuration (selected), Commands, Charts Library, Audits, Web UI, and Quick Links. A search bar at the top of the main panel contains 'cluster_signing_duration'. Below the search bar, there are filters for SCOPE, CATEGORY, and STATUS. The SCOPE filter shows 'ECS (Service-Wide)' selected. The CATEGORY filter shows 'Main' selected. The STATUS filter shows 'Non-Default' selected. The main configuration area displays the 'Cluster Signing Duration' property, which is set to 'ECS (Service-Wide)' and has a value of '1825'. A 'Save Changes(CTRL+S)' button is at the bottom right. A status bar at the bottom indicates '1 Edited Value' and 'Reason for change: Modified Cluster Signing Duration'.

- Click Save Changes.



Note: Manual execution of `rotate-vault-cert.sh` and `rotate-webhook-cert.sh` are deprecated from Cloudera Data Services on premises 1.5.4 CHF3.

- Certificate rotation must be performed through the Cloudera Manager. For more information, see [Rotating internal ECS certificates](#).
- You can use the CLI to verify the new certificate expiration setting:

```
root      49076    48970    2 16:49 ?        00:00:10 kube-controller-mana
ger
--flex-volume-plugin-dir=/var/lib/kubelet/volumeplugins --terminated-pod-
gc-threshold=1000 --permit-port-sharing=true
--allocate-node-cidrs=true --authentication-kubeconfig=/var/lib/rancher/
rke2/server/cred/controller.kubeconfig
--authorization-kubeconfig=/var/lib/rancher/rke2/server/cred/controller.
kubeconfig --bind-address=127.0.0.1
--cluster-cidr=10.42.0.0/16 --cluster-signing-duration=43800h
<snip!>
```

Adjusting the expiration time of the Cloudera Embedded Container Service webhook certificate

- In Cloudera Manager, select the ECS cluster, then click ECS.
- Click the Configuration tab, then use the Search box to locate the `cluster_signing_duration` configuration property.

- The `cluster_signing_duration` configuration property sets the expiration time for the RKE Kubernetes, Vault, and ECS webhook certificates, and is set to 1 year (365 days) by default. In the example below, the certificate expiration has been reset to 5 years (1825 days):

The screenshot shows the Cloudera Manager interface for cluster 153-b278. The left sidebar contains navigation options: Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Data Services (New), Parcels, Running Commands, Support, and a user profile for 'admin'. The main panel is titled 'ECS' and shows the 'Configuration' tab. A search bar contains 'cluster_signing_duration'. The 'Filters' section on the left lists various categories and their counts. The main configuration area shows 'Cluster Signing Duration' set to 'ECS (Service-Wide)' with a value of '1825'. A 'Save Changes(CTRL+S)' button is at the bottom right.

Filters

- SCOPE**
 - ECS (Service-Wide) 1
 - Ecs Agent 0
 - Ecs Server 0
- CATEGORY**
 - Main 1
 - Advanced 0
 - Monitoring 0
 - Performance 0
 - Ports and Addresses 0
 - Resource Management 0
 - Security 0
- STATUS**
 - Error 0
 - Warning 0
 - Edited 1
 - Non-Default 1
 - Include Overrides 0

Cluster Signing Duration ECS (Service-Wide) Undo

`cluster_signing_duration` 1825

1 Edited Value Reason for change: Modified Cluster Signing Duration Save Changes(CTRL+S)

- Click Save Changes.



Note: Manual execution of `rotate-vault-cert.sh` and `rotate-webhook-cert.sh` are deprecated from Cloudera Data Services on premises 1.5.4 CHF3.

- Certificate rotation must be performed through the Cloudera Manager. For more information, see [Rotating internal ECS certificates](#).
- Check for any pods in the Pending state whose status shows that they cannot tolerate the `node-role.kubernetes.io/control-plane` toleration. Restart those pods.
- You can use the CLI to verify the new certificate expiration setting:

```
root      49076   48970   2 16:49 ?        00:00:10 kube-controller-mana
ger
--flex-volume-plugin-dir=/var/lib/kubelet/volumeplugins --terminated-pod-
gc-threshold=1000 --permit-port-sharing=true
--allocate-node-cidrs=true --authentication-kubeconfig=/var/lib/rancher/
rke2/server/cred/controller.kubeconfig
--authorization-kubeconfig=/var/lib/rancher/rke2/server/cred/controller.
kubeconfig --bind-address=127.0.0.1
--cluster-cidr=10.42.0.0/16 --cluster-signing-duration=43800h
<snip!>
```

Rotating internal Cloudera Embedded Container Service certificates

Perform the below steps to rotate the control plane certificates for vault, tolerations webhook, embedded database, and ingress certificate, if the cluster is using the default certificate for ingress.

Before you begin



Note: Ensure that Cloudera Manager and ECS both are upgraded to the appropriate 1.5.5 versions. That is, Cloudera Manager is upgraded to minimum version of *7.13.1 CHF3* and ECS to *1.5.5*.

1. In Cloudera Manager UI, select the ECS cluster, then click ECS Service.
2. Under Actions, click Rotate Internal ECS Certificates.
3. A prompt appears requesting confirmation regarding the certificates that will be rotated as part of this command. Proceed by clicking Rotate Internal ECS Certificates.
4. The command will rotate certificates for vault, ingress controller, and restart related pods.



Note: You will notice some additional pods getting restarted as well, this is done by the cdp-reloader service, which restarts certain pods which have annotations regarding the kubernetes secrets and/or configmaps the pod utilizes.

5. After the command executes, you must wait for all control plane pods to run again (same state prior to running the command) and then proceed with your regular use.



Note: For Cloudera Data Warehouse, ensure that you refresh your Environment, Cloudera Data Catalog, and Virtual Warehouses after you have updated the certificate.

Configuring multiple Base clusters with one Cloudera Embedded Container Service cluster

You can configure one Cloudera Embedded Container Service cluster to work with multiple Cloudera Base on premises clusters managed by separate instances of Cloudera Manager. In order to do this you must first create a combined truststore .pem file that contains the ECS Control Plane truststore .pem file appended with the certificate files of each of the Cloudera Base on premises clusters.

About this task



Note:

Either, all Cloudera Manager instances must share the same root CA (in which case only one upload of the root CA is required), or the certificates of all Cloudera Manager instances need to be manually concatenated, and the combined .pem file is uploaded as the Datalake.

Use the following steps to configure one Cloudera Embedded Container Service cluster to work with multiple Cloudera Base on premises clusters:

1. Append the ECS Control Plane truststore .pem file with the certificate files from the additional Cloudera Base on premises clusters.
2. Register an ECS environment with each of the additional Cloudera Base on premises clusters.
3. Create data services within each environment.

Step 1: Append the Cloudera Embedded Container Service Control Plane truststore .pem file with the certificate files from the Base clusters

1. On the ECS Control Plane, run the following kubectl command to get the contents of the configmap:

```
kubectl get configmap cdp-private-installer-truststore -n cdp -o yaml >
cdp-private-installer-truststore.yaml
```

2. Copy the `truststorePEM` content, decode it, and store it in a file. For example:

```

echo LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURhakNDQWxJQ0NRRG5iNnhmK0d
QRl16QU5CZ22txaGtpRz13MEJBUXNGQURCWk1Rc3dDUV
1EV1FRROV3S1YKVXpFTElBa0dBmVVFQ0F3Q1EwRXhDekFKQmdOVk1JBY01BbE5ETVEwd0N3WU
RWUvFLREFSRFRFU1NNUXd3Q2dZRAPWUvFMREFOQ1RGS
XhFekFSQmdOVk1JBTU1DaW91YUhhNExuTnBkR1V3SGhjTk1qTXhNVEV3TVRRME1qUXdXaGNOC
klqUXhNVEE1TVRRME1qUXdXakFWTVJNd0VRWURWUvFE
REFvUxtaDN1QzV6YVhSbElJSUJvakFOQmdrcWhraUcK0XcwQkFRRUZBQU9DQVk4QU1JSUJp
Z0tdQV1lFQS91Zk1JTk05IQtdWUTFM05qk3ZoRGFRV0p
JcUhfBvCxoFlpYgpbQUdiYmlvYi9YYnY0aTRINU81MXV3Sjj1cWowaktUM3dBu3l0UG0yS0p
1RE9vVXMveWhJc0xuK3VOW1Mzd292CkNxSk5RcWpRT3
N2RUVITU5ZZ3JOWExMc1hlbHZHTX14aG16bVFlSEhHTkZhcldENVkwd1laMVVlaG00a0pUUT
UKTFhoZml1JVJj1TUJieE4ySVB2WU1TV1AvYmo4ekF3a
k500HQvVUhaFRTEw1jUktEWitsMGxoeGt0cHpzdmxmcQo4eXNCVTBBQ2MvbWp2bGNWS0xyN
VVRSTRadVNfb2ZRK1QyaEpITEZNQ0N4bFJvcWN5aFo0
Qmt1ZmZwaUhIOGJHcm9kd2tSaHRRMVFCFFxSk1CLytcCOWNZbKfjYlBfah1Xekh1TG1qak15
VTZOYzV3SmpoTGL1SVmptRmpWNzNvZmgKanJ4V1BtVyt
FSDJZODRWK3RpOvdiZE5LQW9KNzU4bzZaSmJsc3ZBRVBNVytBVmw2clFMtTFPZXN1UTNtczc
xMwpWOENObFBWVEQ0UGdpaythOG1YV3FWZkVZN2F1V3
N1YnIwUkIyeFl1WHBhd2lWdWxrSjdYRURHOEpmN2hFNzRqCkRhM1JaeWN5YXdScGF3SXV2V1
kwWGtoSktOOTNBZ01CQUFFd0RRWUpLb1pJaHZjTkFRR
UxCUUFEEZ2dFQkFdcTcKSdu5R2lnky9iUVB3enhmUmF6dlhXM09mT3M1UjNnU0hGeDRmS1BXV
lN5TjEwaW5Obmdxejd4R2dYVnBpRDdWNApQRGVXZFRZ
MjdHN2w3ZHBjek1FS2ptN25XOUp3RW05S3dyRndRwH00WEzNjVvUnhqTzA3Y09VanZYaEwy
dkxlCnk1eHRYZl1JyZl1Pa1NmZDVxcn1KV1BoMDBHb0N
UWTViMy9wK25saWJUUmNkY29mQkFTU0VhbnhaVDJoc1B2V3kKSG9PVkVGSmlrTnVxRHJhS2Y
ySlFfXrRnR4aGs0MFIvUW9LVUpKUTgzUWIXZHBmWVVCdE
91WXRvNExmQWV3Y0RuRwpFWUQvYVp1blgwU2cxRTRoRS9NaUNFN2R6ZzY4TVVPeWVBVlpCel
JuMHBEZ1VtanpTOUNndi9GQ240MjV0QnR5Cis5anY1W
it3TVNkd1VZL2VudEE9C10tLS0tRU5EIEFUF1RJRklDQVRFLS0tLS0KLS0tLS1CRUdJTiBDR
VJUSUZJQ0FURS0tLS0tCk1JSURlekNDQW1PZ0F3SUJB
Z01VQWRide1lQ3JycVRMY1UzRzhPakZRUW5YNGY4d0RRWUpLb1pJaHZjTkFRRUwKQlFBdldU
RUxNQCtHdQTVFVUj0TUNWVkl4Q3pBSk1JnTlZCQWdnQWt
OQk1Rc3dDUV1lEVlFRSERBS1RRekVOTUFzRwpBMVVFQ2d3RVeweEVVakVNTUUFvR0ExVUVDd3d
EUWt4U01STXdFUV1lEVlFRREBb3FmbWgzZUM1emFYUm
xNQjRYCkRUSXpNVEV4TURFek1UTXpOVm9YRFRJMU1URXdPVEV6TVRNEk5Wb3dXVEVMTUFRrR0
ExVUVCaElDVLzNeEN6QUoKQmdOVk1JBZ01Ba05CTVFzdz
0NRWURWUvFIREFkVFF6RU5NQXNHQTFVRUNnd0VRMhHfVWpFTU1Bb0dBmVVFQ3d3RApRa3hTT
VJNd0VRWURWUvFEREFvUxtaDN1QzV6YVhSbElJSUJJ
akFOQmdrcWhraUc5dzBCQVFFRkFBT0NBUTHBCK1JSUJdZ0tdQVFFQXczQXBYeXg4dkxXSvZq
SlpLZ2Npb29XcGdtNjZwN2gxWCTrWUvVZ0Q0VEc3dkZ
2OGNucKhKdzlaZ1ZVpcW1zUTVJRlZxRk5lcEFpSFbteUxscDl1d1RhTEthdm9IZ2pXU0p1K2d
waUdiMHJiR1hkM3ltYkw5Rwp2Sm1pNmtPZW9SeHpQbk
N5SVVEa3NmU3kzdE5pWlNRRFRubmhUWk9Zc2tmbDdZK1VYaVJVS2NBNEExkWTBWSTVJcNpmRl
R0cw5qm0o4SnJ6d0dJdlNoK0ZNdHRYWFQ5WFI5bzVpL
0M2cWh0L1JwbEx3QTB6ZV1YSDhkNj12Ykw4TlEKemREeXZlcmptRXZjs3F1bGo4NU1CSTZwc
VRGb21QcEp5Vv1xS0cwN2U1WDN0QmZiVzk2QXdxYT1BT
Sfd0QlpndwppeTVFbzRxWVRJMGZmYlFCS3ZIVElZyTdT3T0xmRzAvK3J3SURBUUFCh3pzd09U
QUxCZ05WSFE4RUJBTUNCREF3CkV3WURWUjBsQkF3d0N
nwU1Ldl1CQlFVSEF3RXdGUv1lEVlIwUk1JBNhdESU1LS2k1b2QzZ3VjMmwWw1RBTk1Jna3EKaGt
pRz13MEJBUXNGQURFQ0FRUvTEkZfZUlg5M2k1Q1FPQ1
FIVVZ2Y2M1OWFMb2Y3SnJxcGNaN0NOaGJXMzc4Zgo3RTNpTjhBY1BNQ0dvZllTeWFrblQxVl
kwdDNIvXhtSTFSdxDEUXNDU3U1MmlhYnhIVUhrOFBEQ
jk5NTRxL3RtCkh4MXpVR0VURkZaZhdKb0dDMk14U19WdU9wbExza2hEc0ZJZmpaZC81clVrL
1QvMUxUaC8zMeXBBGhPVzNtek8KZFJWWC9LR2QyWGZ3
SFNzQ3FRTFk4WGZQM0d3WHgrTmVUY09vTEQycXyYw1kMnY1dlVtdXpONzErZjR3bXVvbWpa
Z1JiYk9OSkMvdzVzV3MvWVRaODd1M1JNUWExd2gvck1
Ymk1QMzNTMG1SeHJkSX1pEGMxamF6ZTYxWmRUUnk5Ck9NQ2RmZEPGNFE1RndmOddWSWpYZXd
PemdQVnFJVGVGNVW1vcy9HR0p0UT09C10tLS0tRU5EIE
NFU1RJRklDQVRFLS0tLS0= | base64 -d > cdp-private-installer-truststore.pem

```

3. Obtain the truststore .pem file from the first additional Cloudera Manager host from `/var/lib/cloudera-scm-agent/agent-cert/cm-auto-global_cacerts.pem` or `/opt/cloudera/CMCA/trust-store/cm-auto-global_cacerts.pem` and copy the contents.
4. Append the `cdp-private-installer-truststore.pem` file created previously with the contents of the Cloudera Manager .pem file.
5. Repeat the previous two steps for all additional Cloudera Manager hosts you would like to register environments with.
6. Log in to the ECS cluster Cloudera Management Console and click Administration > CA Certificates. Select Datalake in the CA Certificate Type drop-down, click Choose File, then select the appended `cdp-private-installer-truststore.pem` file and click Upload. Click Save to save your changes.

You can also use the following CLI commands to upload the `cdp-private-installer-truststore.pem` file and update the global truststore with the encoded certificate file content:

```
cat cdp-private-installer-truststore.pem | base64
cdp environments --set-environment-setting --settings truststorePEM=<base64
4 encoded CM cert> --no-verify-tls
```



Note: Create a new file with both merged certificates and then upload the certificate. You can now view that the Cloudera Manager connection is successful.

Step 2: Register an Cloudera Embedded Container Service environment with each of the additional Base clusters

1. Log in to the ECS cluster Management Console and [Register an environment](#) for the first additional Base cluster using the applicable Cloudera Manager URL and credentials.
2. Repeat the previous step for the rest of the additional Base clusters.

Step 3: Create data services within each environment

Refer to the following topics to create the data services of your choice in each environment:

- [Adding a Cloudera Data Engineering service](#)
- [Activate ECS environments](#) (Cloudera Data Warehouse)
- [Provision an AI Workspaces](#)

Configuring multiple Cloudera Embedded Container Service clusters on a single base cluster

This section provides details on configuring multiple Cloudera Embedded Container Service clusters on a single Base cluster from Cloudera Manager.

About this task

Use the following steps to configure multiple Cloudera Embedded Container Service clusters on a single base cluster:

1. Login to the Cloudera Manager UI.
2. Follow the steps to configure the ECS cluster here: [Configuring ECS](#).
3. Log in to the Cloudera Embedded Container Service cluster Management Console and [Register an environment](#) for the existing Base cluster.
4. Install the required Data Services in that environment: Cloudera Data Warehouse, Cloudera Data Engineering, Data Catalog, Cloudera AI, and Replication Manager.
 - [Adding a Cloudera Data Engineering service](#)
 - [Activate ECS environments](#) (Cloudera Data Warehouse)
 - [Provision an AI Workspaces](#)

5. If you want to configure multiple Cloudera Embedded Container Service, follow steps 2 to 4 on different clusters.

Configuring multiple Cloudera Embedded Container Service environments on a single base cluster

This section provides details on configuring multiple Cloudera Embedded Container Service environments on a single Base cluster from Cloudera Manager.

About this task

Use the following steps to configure multiple Cloudera Embedded Container Service environments on a single base cluster:

1. Login to the Cloudera Manager UI.
2. Follow the steps to configure the ECS cluster here: [Configuring ECS](#).
3. Log in to the Cloudera Embedded Container Service cluster Management Console and [Register an environment](#) for the existing Base cluster.
4. Install the required Data Services in that environment: Cloudera Data Warehouse, Cloudera Data Engineering, Data Catalog, Cloudera AI, and Replication Manager.
 - [Adding a Cloudera Data Engineering service](#)
 - [Activate ECS environments](#) (Cloudera Data Warehouse)
 - [Provision an AI Workspaces](#)
5. If you want to configure multiple Cloudera Embedded Container Service Environments with the same base cluster, follow steps 3 and 4.

GPU node labeling on Cloudera Embedded Container Service

You can use NVIDIA Feature Discovery to generate labels for the set of GPUs available on ECS nodes. You can use these node labels to assign workloads to specific GPU devices. This feature is enabled by default on Cloudera Embedded Container Service.

Using GPU node labeling on Cloudera Embedded Container Service

Information about using GPU node labeling is available on the [NVIDIA GPU feature discovery](#) page.

Known Issues and Limitations

- GPU node labeling is only supported for GPU cards manufactured by NVIDIA.
- If an Cloudera Embedded Container Service node has [multiple GPUs](#), not all of the GPUs will be labeled. The last GPU as per lspci will be labeled.
- If an Cloudera Embedded Container Service node is provisioned from a provisioner with virtual GPUs (AWS, Azure, etc.) the nodes will not be labeled with the GPU information.