Cloudera Data Engineering 1.5.5

User Access Management

Date published: 2020-07-30
Date modified: 2025-11-08

https://docs.cloudera.com/

Legal Notice

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

Overview

Users must be assigned roles on Cloudera Data Engineering Services and Virtual Clusters to provide them with specific access to the Service or the Virtual Cluster.

Important: Starting from Cloudera Data Engineering on premises 1.5.5 release, User Access Management including the new roles (Service Admin, Service User, VC Admin, VC User, and VC Viewer) is supported only for Cloudera Data Engineering Service installation using Embedded Container Service.

For Cloudera Data Engineering Service installation using OpenShift Container Platform, the user accesses the Services and the Virtual Clusters with the DEAdmin and DEUser roles only. User Access Management is not applicable for Cloudera Data Engineering Service and Virtual Clusters in OpenShift Container Platform. Assigning the roles to manage and access the Service and Virtual Clusters is not applicable.

User Access Management allows you to assign the roles to manage and access the Cloudera Data Engineering Service and Virtual Clusters by defining the access levels for a particular user or groups. With User Access Management, you can define whether a user or a group of users can administer or view a Service or a Virtual Cluster. For more information about User Management, onboarding new users, or assigning roles, see User Management.

Limitations

- When a user or a group is added to or removed from Cloudera Data Services on premises, you must clear the browser cache or open the same URL in a new tab to refresh the users or groups list.
- In the Cloudera Data Engineering UI, to assign a role on a Virtual Cluster in the Service, the user must at least be assigned a Service User role at that Service. Cloudera Data Engineering CLI or API allows you to directly assign a role in a Virtual Cluster even though you do not have any role assigned in the Service. But, you cannot access the Virtual Cluster because you do not have access to the Service itself. This will not result in an effective role management as users first need to be assigned a role on the Service before assigning a role on a Virtual Cluster.
- The roles assigned as part of the User Access Management are not applicable for Airflow deployments. Any user who can submit an Airflow DAG can access all the DAGs available in the Cloudera Data Engineering environment irrespective of the role they are assigned. To disable creating the Airflow jobs in the Virtual Cluster, update the configmap after creating the Virtual Cluster by executing the following command:

  ```
  DEX_APP_NAMESPACE=<***DEX_APP_NAMESPACE***> && \
  MODIFIED_VALUE=$( \
      set -o pipefail; \
      kubectl get configmap ${DEX_APP_NAMESPACE}-api-cm -n ${DEX_APP_NAME
  SPACE} \
          -o go-template='{{index .data "dex.yaml"}}' | \
      yq eval '.airflowJobsEnabled = false' - | \
      jq -R -s '.' \
  ) && \
  [ "${MODIFIED_VALUE}" != "\"\"" ] && \
  kubectl patch configmap ${DEX_APP_NAMESPACE}-api-cm -n ${DEX_APP_NAMESPACE
  } \
      --type='json' \
      -p="[{\"op\": \"replace\", \"path\": \"/data/dex.yaml\", \"value\":
  ${MODIFIED_VALUE}}]" && \
  kubectl rollout restart deployment ${DEX_APP_NAMESPACE}-api -n ${DEX_APP_N
  AMESPACE} && \
  kubectl scale deployment --replicas=0 ${DEX_APP_NAMESPACE}-airflow-webser
  ver -n ${DEX_APP_NAMESPACE}
  ```

  To identify <***DEX_APP_NAMESPACE***>, do the following steps:

  1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
  2. Click Administration in the left navigation menu. The Administration page displays.

3. In the Services column, select the Service containing the virtual cluster for which you want to identify the namespace.
4. In the Virtual Clusters column on the right, click the Cluster Details icon for the virtual cluster for which you want to identify the namespace. In the Cluster Details, VC-ID is your <***DEX_APP_NAMESPACE***>.

Access roles in Cloudera Data Engineering

Learn about role-based access in Cloudera Data Engineering.

> **Important:** If you upgrade from Cloudera Data Engineering 1.5.4 or earlier, you use either the **DEAdmin** or the **DEUser** roles. A user with the **DEAdmin** role has the same Administrator level permissions in Cloudera Data Engineering 1.5.5 as well. Starting from the Cloudera Data Engineering 1.5.5 release, the **DEUser** role is deprecated. A user assigned with a **DEUser** role in a particular environment can access all the Cloudera Data Engineering Services and Virtual Clusters of that environment. Cloudera recommends you to unassign the **DEUser** role and assign one of the relevant new roles for the users.

Access roles available in Cloudera Data Engineering:

> **Important:** Artifacts refer to jobs, resources, repositories, job runs, and sessions.

- **DE Admin**: A DEAdmin user has full access to all the components in the Cloudera Data Engineering including the Services and the Virtual Clusters within a specific environment. A DEAdmin can view and manage the artifacts created by any user in the environment.
- **Roles at Cloudera Data Engineering Service**:
  - **Service Admin**: A Service Admin can manage a specific Service with full access to the underlying Virtual Clusters, including the associated artifacts. By default, a Service Admin gets full-access to all the Virtual Clusters and the associated artifacts in a specific Service even though they are not assigned any role in the Virtual Cluster.
  - **Service User**: A Service User can only view the details of a specific Service. A Service User cannot update or delete a Service. Also, a Service User cannot implicitly view the underlying Virtual Clusters or the artifacts within a Virtual Cluster, unless they are explicitly assigned at least a VC User role in the Virtual Cluster.
- **Roles at Cloudera Data Engineering Virtual Cluster**:
  - **VC Admin**: A VC Admin can manage a specific Virtual Cluster with full access to all its associated artifacts.
  - **VC User**: A VC User can access a specific Virtual Cluster to create and manage the artifacts that are owned by them or explicitly shared with them by another user.
  - **VC Viewer**: A VC Viewer can access a specific Virtual Cluster with view-only access to all the artifacts in the Virtual Cluster. A VC Viewer cannot run, delete, or change any artifacts. Cloudera recommends using the VC Viewer role for view-only scenarios. For example, support-related scenarios, where a Support Executive has to view the artifacts and the logs to debug any issue.

⚠ **Important:**

- In a Cloudera Data Engineering Virtual Cluster, you must have at least one of the following roles to access the Virtual Cluster:
  - DEAdmin
  - DEUser (deprecated)
  - Service Admin
  - VC Admin
  - VC Uset
  - VC Viewer
- A DEAdmin and Service Admin can assign a role in a Cloudera Data Engineering Service.
- A DEAdmin, Service Admin, and VC Admin can assign a role in a Cloudera Data Engineering Virtual Cluster.
- For a user or a group to appear in the search while assigning a role in the Virtual Cluster, the user or group must have a role assigned in the corresponding Cloudera Data Engineering Service. You must have at least a Service User role to assign a role in the Virtual Cluster. For example, if you want to assign user-01 as VC Admin for the VC-01 (Virtual Cluster) in the Service-01 (Service), then user-01 must at least be a Service User in Service-01.
- A Service User can only access the Virtual Cluster only if they have a role assigned in the Virtual Cluster. A Service User with a VC Admin role can view, update, and delete the specific Virtual Cluster. Whereas, a Service User with either a VC User or VC Viewer role can only view a Virtual Cluster.

Role-based access for Services

The following table lists the roles and actions a user can perform in the Cloudera Data Engineering Service:

Role	Create	View	Update	Delete
DE Admin	Yes	Yes	Yes	Yes
Service Admin	No	Yes	Yes	Yes
Service User	No	Yes	No	No
VC Admin	No	Yes	No	No
VC User	No	Yes	No	No
VC Viewer	No	Yes	No	No

⚠ **Important:** A role assigned in a Virtual Cluster is effective only if a role is assigned to the user or the group in the respective Service (at least Service User).

Role-based access for Virtual Clusters

The following table lists the roles and actions a user can perform in the Cloudera Data Engineering Virtual Cluster:

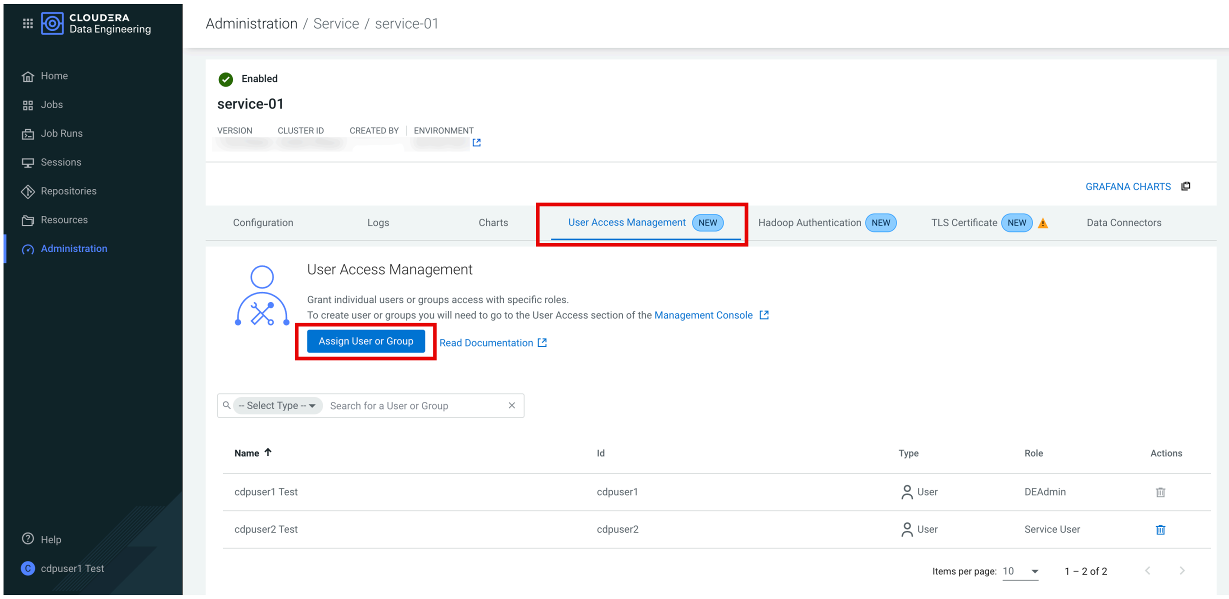
Role	Create	View	Update	Delete
DE Admin	Yes	Yes	Yes	Yes
Service Admin	Yes	Yes	Yes	Yes
VC Admin	No	Yes	Yes	Yes
VC User	No	Yes	No	No
VC Viewer	No	Yes	No	No

Assigning a role in a Cloudera Data Engineering Service

Learn about how to assign a new role for a user or a group in a Cloudera Data Engineering Service.

Procedure

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Administration in the left navigation menu. The Administration page displays.
3. In the Services column, select the Service for which you want to assign a new role and click Service Details.
4. Click User Access Management.
5. Click Assign User or Group.



service-01

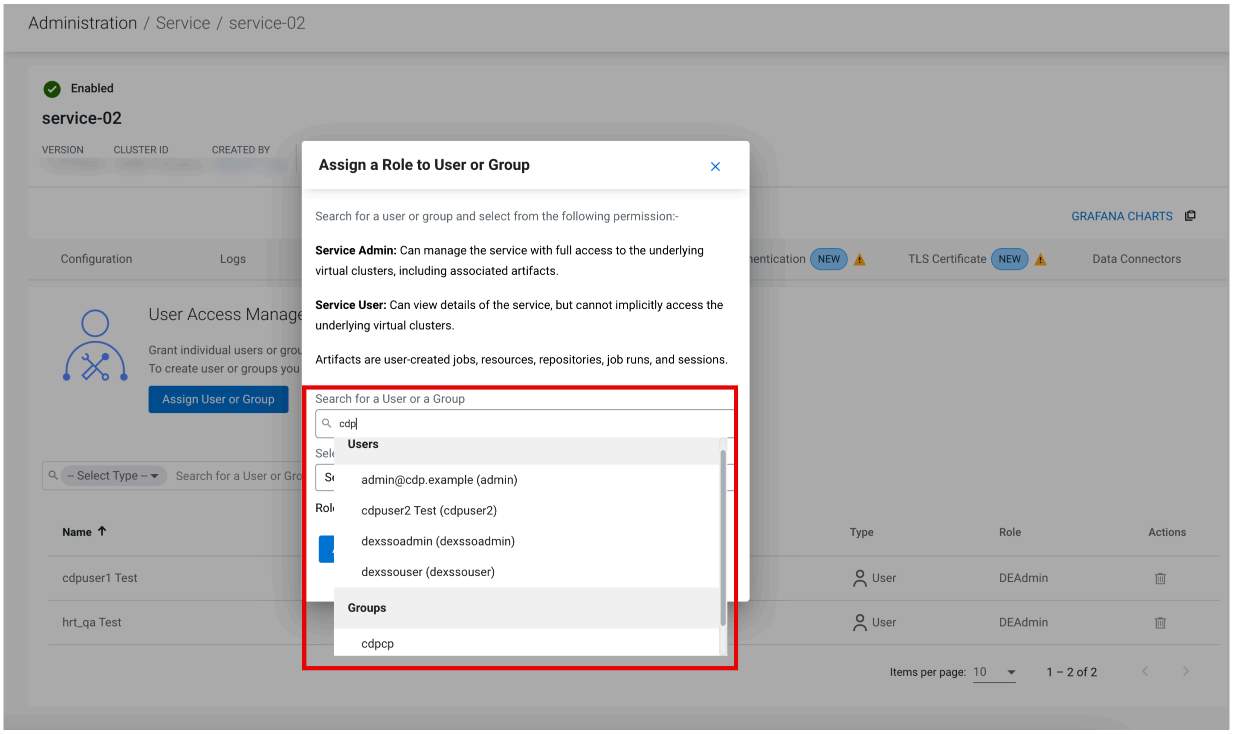
VERSION CLUSTER ID CREATED BY ENVIRONMENT [redacted]

User Access Management

Grant individual users or groups access with specific roles.
To create user or groups you will need to go to the User Access section of the Management Console

Name ↑	Id	Type	Role	Actions
cdpuser1 Test	cdpuser1	User	DEAdmin	🗑
cdpuser2 Test	cdpuser2	User	Service User	🗑

6. In the Search for a User or a Group field, search for the user or the group you want to assign the new role to and select the relevant user or the user group from the search results.



Assign a Role to User or Group

Search for a user or group and select from the following permission:-

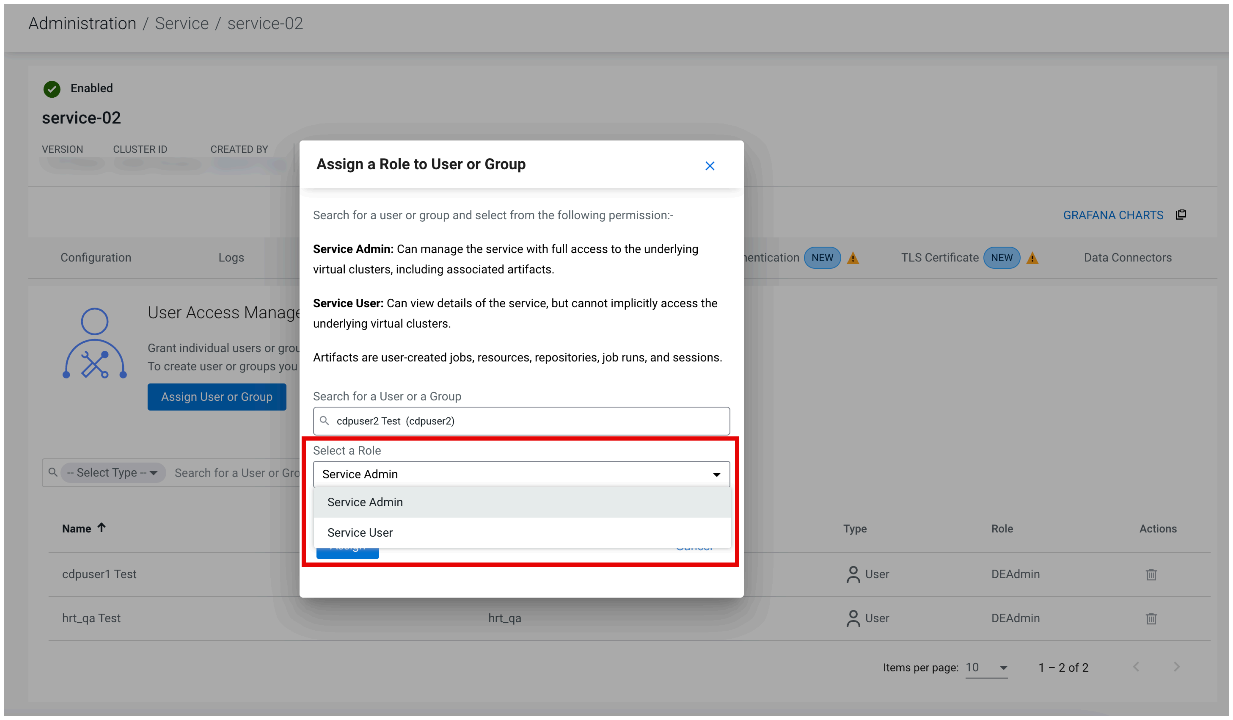
Service Admin: Can manage the service with full access to the underlying virtual clusters, including associated artifacts.

Service User: Can view details of the service, but cannot implicitly access the underlying virtual clusters.

Artifacts are user-created jobs, resources, repositories, job runs, and sessions.

Search for a User or a Group: cdp

7. In the Select a Role drop-down list, select the role that you want to assign.



Assign a Role to User or Group

Search for a user or group and select from the following permission:-

Service Admin: Can manage the service with full access to the underlying virtual clusters, including associated artifacts.

Service User: Can view details of the service, but cannot implicitly access the underlying virtual clusters.

Artifacts are user-created jobs, resources, repositories, job runs, and sessions.

Search for a User or a Group: cdpuser2 Test (cdpuser2)

Select a Role: Service Admin

8. Click Assign.

Unassigning a role in a Cloudera Data Engineering Service

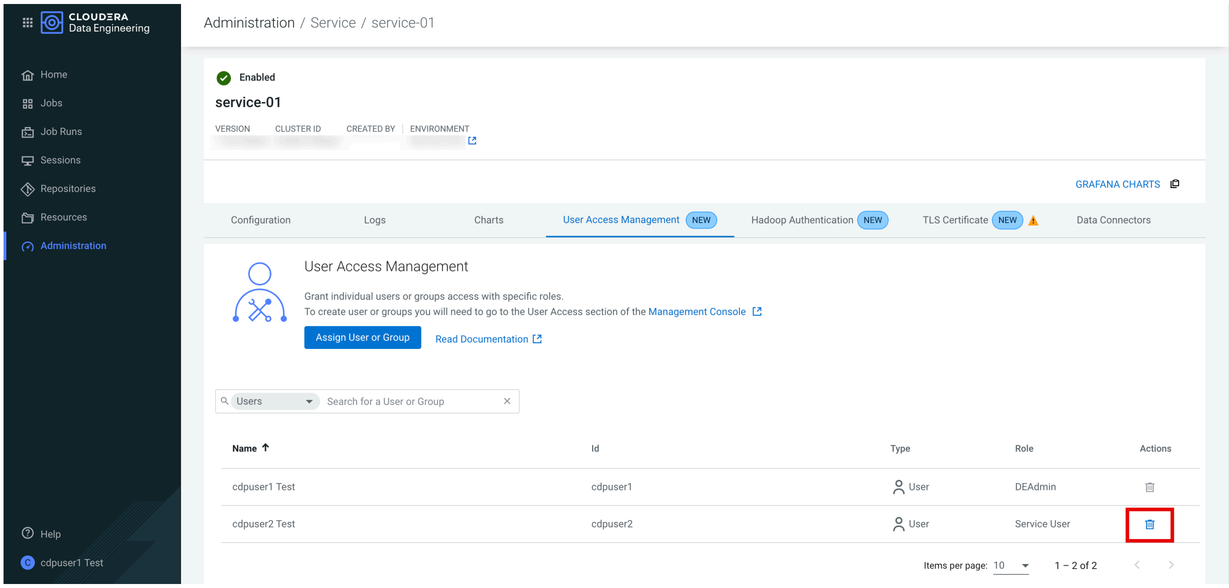
Learn about how to unassign a role for a user or a group in a Cloudera Data Engineering Service.

Procedure

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Administration in the left navigation menu. The Administration page displays.
3. In the Services column, select the Service where you want to unassign a role and click Service Details.
4. Click User Access Management.
5. In the Search field, select one of the following options depending on for which you want to unassign the role:

   - Users
   - Machine Users
   - Groups

   Depending on the option you select, a relevant list of users or groups appear.
6. In the table, go to the Actions column and click the Remove icon for the user or group for which you want to unassign the role.



[redacted]

Grant individual users or groups access with specific roles.
To create user or groups you will need to go to the User Access section of the Management Console

Name ↑	Id	Type	Role	Actions
cdpuser1 Test	cdpuser1	User	DEAdmin	🗑
cdpuser2 Test	cdpuser2	User	Service User	🗑

7. Click Confirm.

Assigning a role in a Cloudera Data Engineering Virtual Cluster

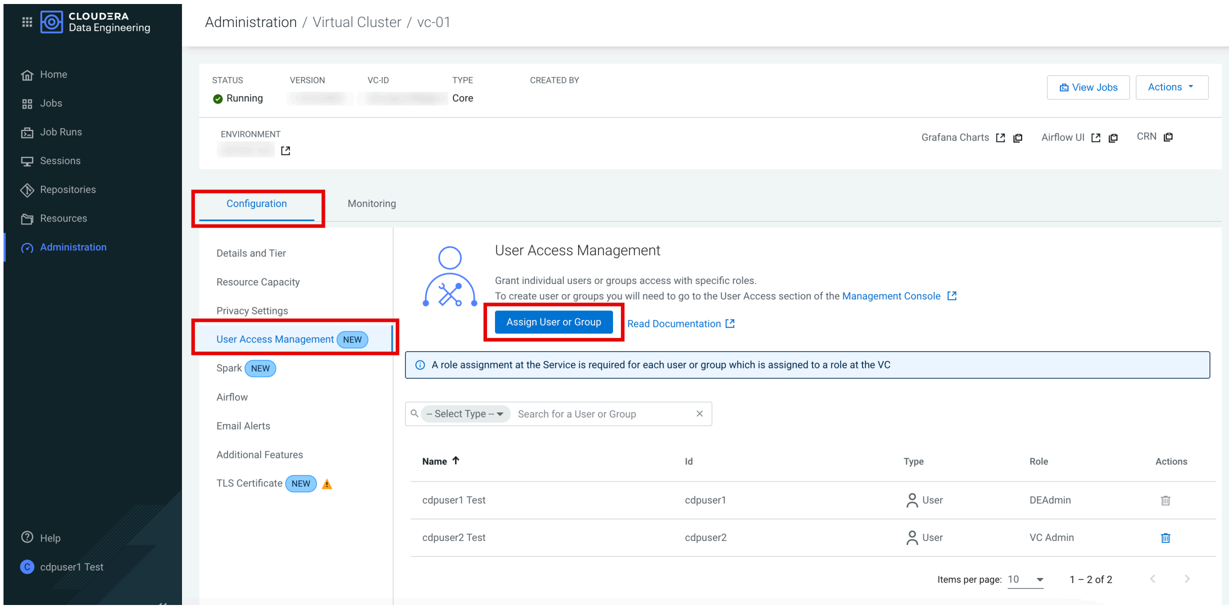
Learn about how to assign a new role for a user or a group in Cloudera Data Engineering Virtual Cluster.

Before you begin

Make sure that the user or the group has a role (at least a Service User) assigned in the corresponding Service.

Procedure

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Administration in the left navigation menu. The Administration page displays.
3. In the Services column, select the Service containing the Virtual Cluster where you want to assign a new role.
4. In the Virtual Clusters column on the right, click the Cluster Details icon for the Virtual Cluster for which you want to assign the role.
5. Click Configurations User Access Management .



STATUS: Running | VERSION: [redacted] | VC-ID: [redacted] | TYPE: Core | CREATED BY

ENVIRONMENT: [redacted]

User Access Management

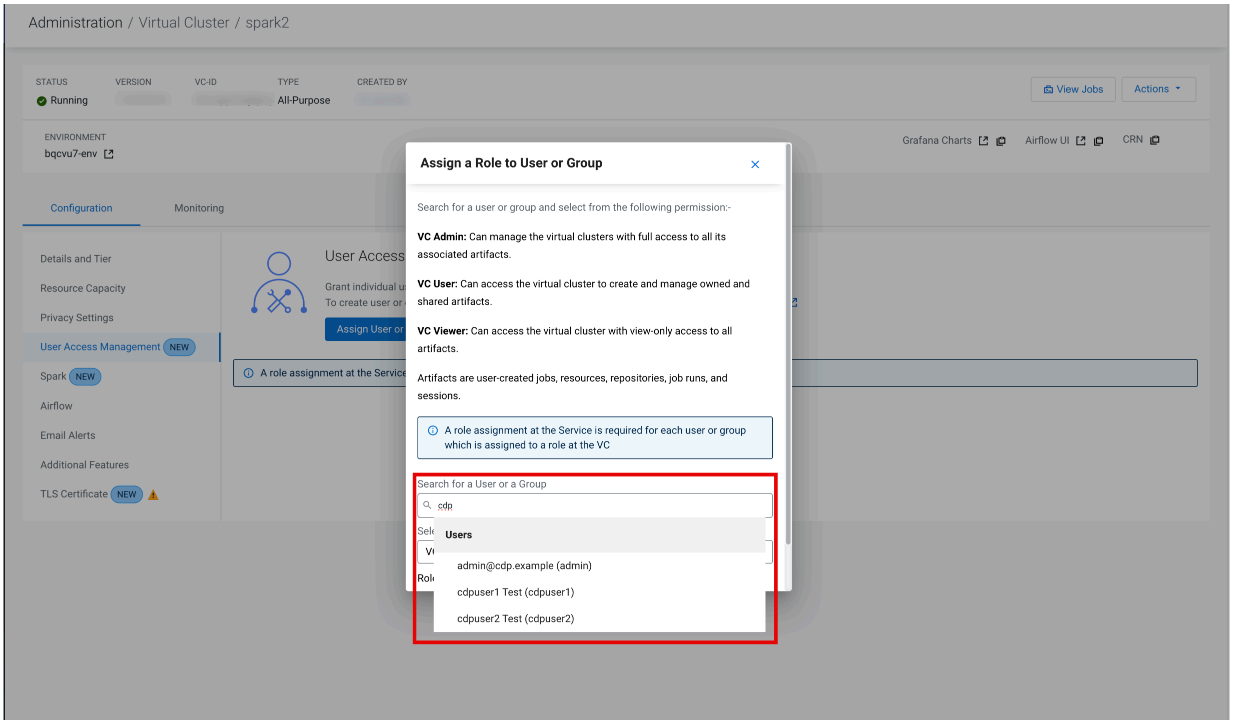
Grant individual users or groups access with specific roles.
To create user or groups you will need to go to the User Access section of the Management Console

A role assignment at the Service is required for each user or group which is assigned to a role at the VC

Name ↑	Id	Type	Role	Actions
cdpuser1 Test	cdpuser1	User	DEAdmin	
cdpuser2 Test	cdpuser2	User	VC Admin	

Items per page: 10 1 – 2 of 2

6. Click Assign User or Group.
7. In the Search for a User or a Group field, search for the user or the user group you want to assign the new role and select the relevant user or user group from the search results.



STATUS: Running | VERSION: [redacted] | VC-ID: [redacted] | TYPE: All-Purpose | CREATED BY: [redacted]

ENVIRONMENT: bqcvu7-env

Assign a Role to User or Group

Search for a user or group and select from the following permission:-

VC Admin: Can manage the virtual clusters with full access to all its associated artifacts.

VC User: Can access the virtual cluster to create and manage owned and shared artifacts.

VC Viewer: Can access the virtual cluster with view-only access to all artifacts.

Artifacts are user-created jobs, resources, repositories, job runs, and sessions.

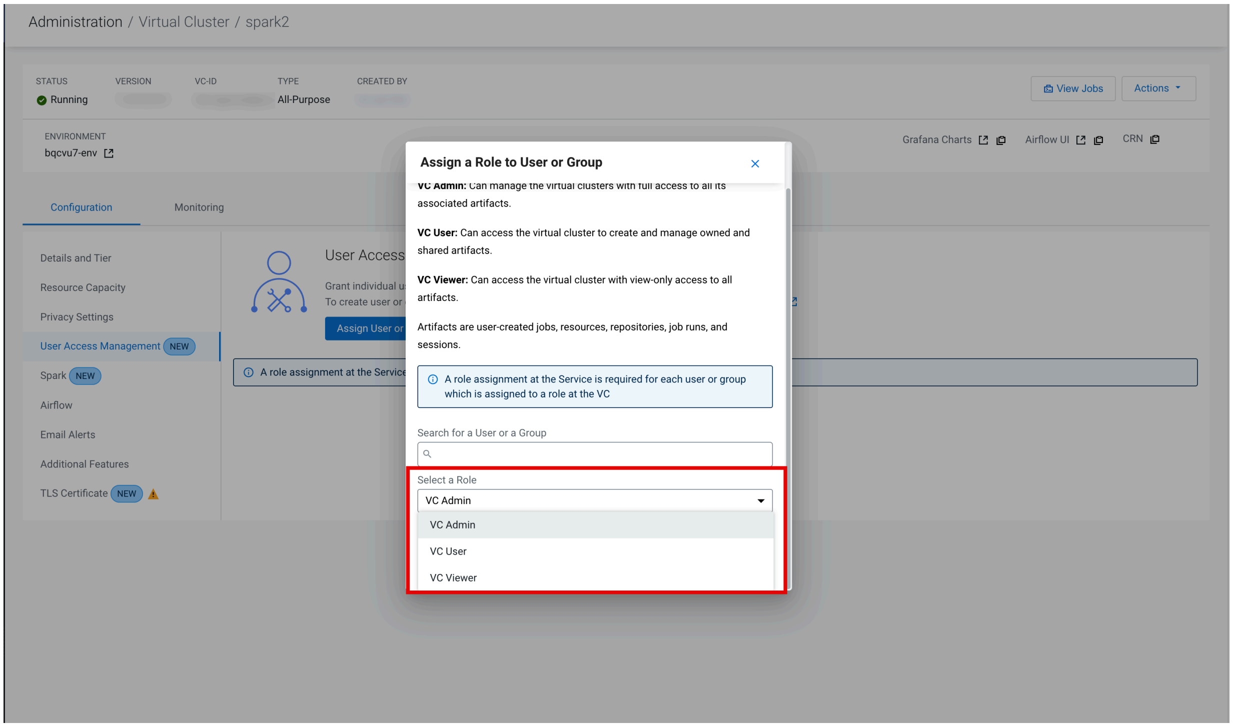
A role assignment at the Service is required for each user or group which is assigned to a role at the VC

Search for a User or a Group: cdp

Users

- admin@cdp.example (admin)
- cdpuser1 Test (cdpuser1)
- cdpuser2 Test (cdpuser2)

8. In the Select a Role drop-down list, select the role that you want to assign.



Assign a Role to User or Group

VC Admin: Can manage the virtual clusters with full access to all its associated artifacts.

VC User: Can access the virtual cluster to create and manage owned and shared artifacts.

VC Viewer: Can access the virtual cluster with view-only access to all artifacts.

Artifacts are user-created jobs, resources, repositories, job runs, and sessions.

A role assignment at the Service is required for each user or group which is assigned to a role at the VC

Search for a User or a Group

Select a Role: VC Admin

- VC Admin
- VC User
- VC Viewer

9. Click Assign.

Unassigning a role in a Cloudera Data Engineering Virtual Cluster

Learn about how to unassign a role for a user or a group in Cloudera Data Engineering Virtual Cluster.

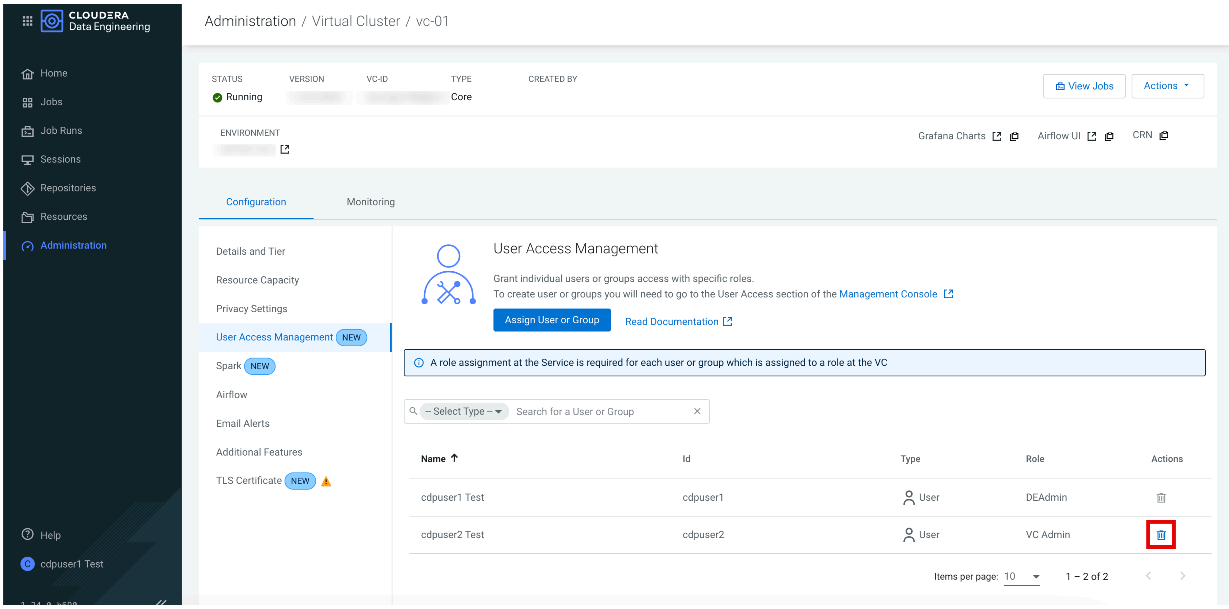
Procedure

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Administration in the left navigation menu. The Administration page displays.
3. In the Services column, select the Service containing the Virtual Cluster where you want to unassign the role.
4. In the Virtual Clusters column on the right, click the Cluster Details icon for the virtual cluster where you want to unassign the role.
5. Click Configurations User Access Management .
6. In the Search field, select one of the following options depending on for which you want to unassign the role:

   - Users
   - Machine Users
   - Groups

   Depending on the option you select, a relevant list of users or groups appear.

7. In the table, go to the Actions column and click the Remove icon for the user or the group for which you want to unassign the role.



Administration / Virtual Cluster / vc-01

STATUS: Running
VERSION: [redacted]
VC-ID: [redacted]
TYPE: Core
CREATED BY:
ENVIRONMENT: [redacted]

User Access Management

Grant individual users or groups access with specific roles.
To create user or groups you will need to go to the User Access section of the Management Console

A role assignment at the Service is required for each user or group which is assigned to a role at the VC

Name ↑	Id	Type	Role	Actions
cdpuser1 Test	cdpuser1	User	DEAdmin	🗑
cdpuser2 Test	cdpuser2	User	VC Admin	🗑

Items per page: 10 1 – 2 of 2

8. Click Confirm.