

Working with User Roles

Date published: 2020-10-30

Date modified: 2024-02-29

CLOUDERA

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

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

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

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

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

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

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

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

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

Contents

Creating new roles.....	4
Adding privileges.....	6
Setting system privileges.....	7
Setting role privileges.....	9
Setting connection privileges.....	11
Setting dataset privileges.....	14
Editing role assignments.....	16
Assigning roles to users.....	17
Assigning roles to user groups.....	22
Assigning multiple roles to multiple users.....	28
Deleting roles.....	30

Creating new roles

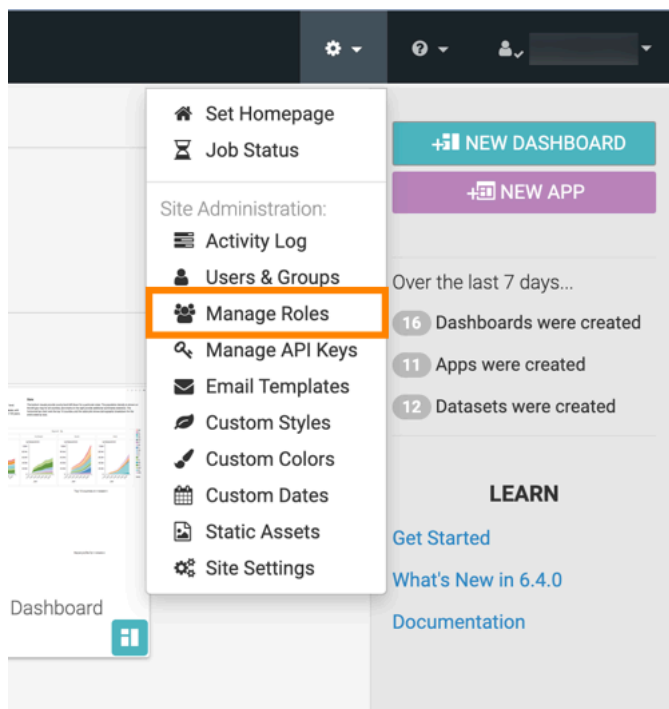
About this task

Administrators with Manage roles and users privilege can introduce new roles into the Role-Based Access Control (RBAC) system.

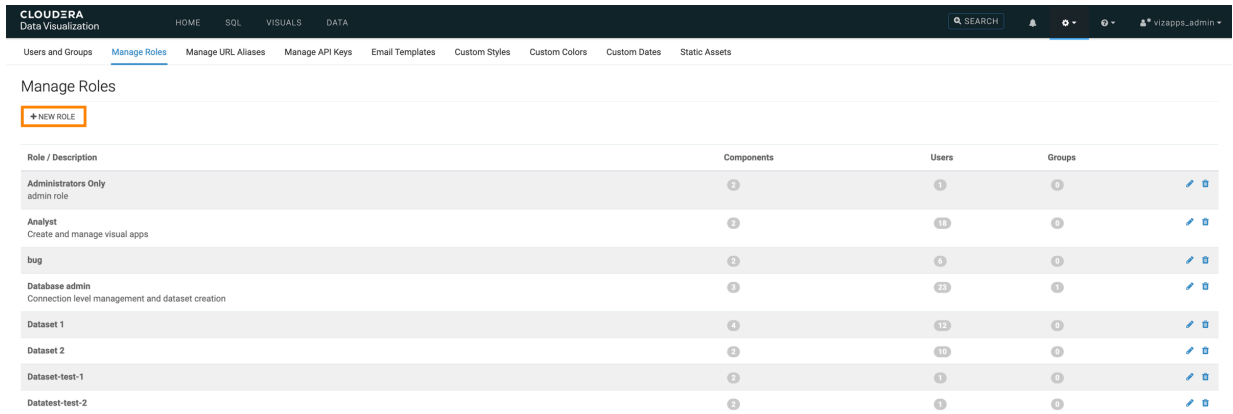
Follow these steps demonstrate to create a new role.

Procedure

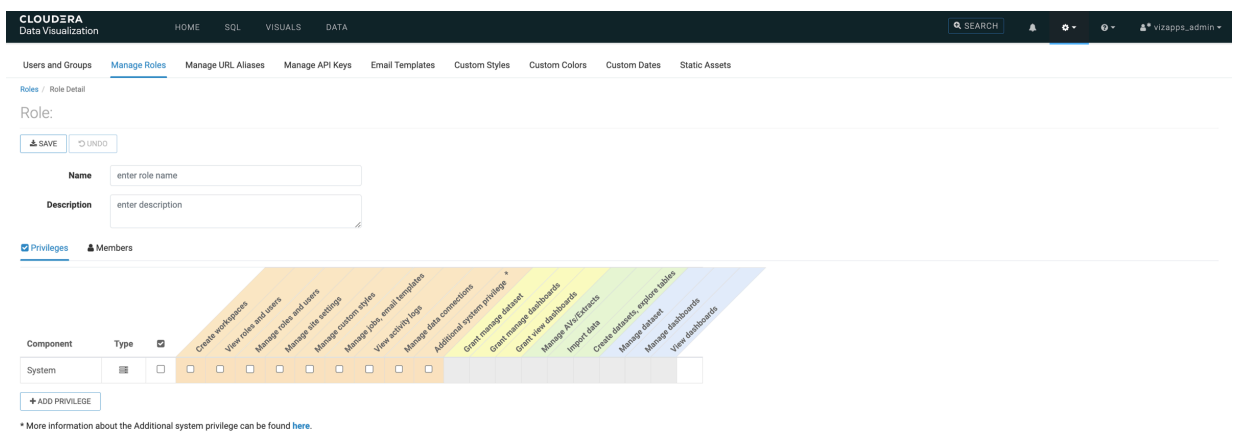
1. On the main navigation bar, click the (gear) icon.
2. Select Manage Roles from the drop-down menu.



3. Click NEW ROLE.



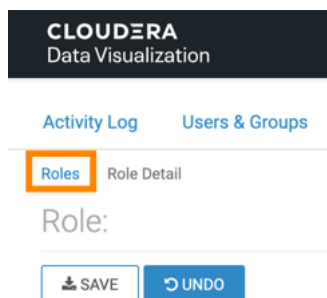
The Role definition interface appears, open on the Privileges tab.



4. Name and save the new role.

- In the Name field, provide a distinctive name for the new role.
In this example, Test Role 1 is used.
- In the Description field, add a brief purpose or context for the new role.
- Click SAVE.

- To verify that the role exists, click Roles at the top of the menu.



You should see the newly created role in the roles list.

 A screenshot of the 'Manage Roles' page in Cloudera Data Visualization. The page has a dark header with 'CLouDERA Data Visualization' and navigation links for 'HOME', 'VISUALS', and 'DATA'. Below the header, there are several sub-navigation tabs: 'Activity Log', 'Users & Groups', 'Manage Roles', 'Manage API Keys', 'Email Templates', 'Custom Styles', 'Custom Colors', 'Custom Dates', 'Static Assets', and 'Site Settings'. The 'Manage Roles' tab is active. Below the navigation, there is a '+ NEW ROLE' button and a table of roles. The table has columns for 'Role / Description', 'Components', 'Users', and 'Groups'. The 'Test Role 1' row is highlighted with an orange border.

Role / Description	Components	Users	Groups
Analyst Create and manage visual apps	2	0	0
Database admin Connection level management and dataset creation	3	1	1
Doc test role	1	1	0
System Admin Full access to all features	3	1	0
Test Role 1 Testing role creation	1	0	0
Visual Consumer View access to visual apps	2	0	0

What to do next

Proceed by defining *Role privileges* and *Editing role assignments* as needed for the newly established role.

Related Information

[Editing role assignments](#)

[Role privileges](#)

Adding privileges

After you declare a new role in the role-based access control (RBAC) system of Cloudera Data Visualization, you can start adding privileges to the role.

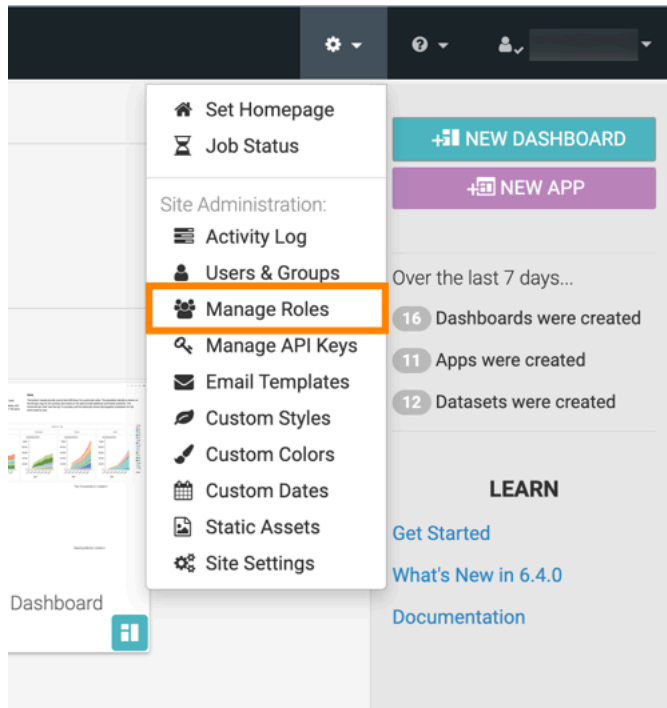
About this task

The following steps demonstrate how to add or change privileges defined for a specific role. In this example, Test Role 1 is used, which was previously defined in *Creating new roles*.

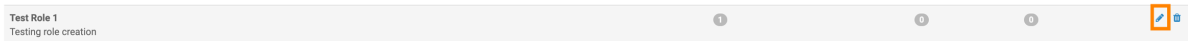
Procedure

- On the main navigation bar, click the (gear) icon.

- In the drop-down menu, click Manage Roles.



- In the Roles interface, next to the role to edit, click the Edit (pencil) icon.



- On the Role definition interface, you can set the following groups privileges:
 - Setting system privileges
 - Setting role privileges
 - Setting connection privileges
 - Setting dataset privileges
- Click SAVE to preserve the new privilege assignments.

Related Information

[Creating new roles](#)

[Setting system privileges](#)

[Setting role privileges](#)

[Setting connection privileges](#)

[Setting dataset privileges](#)

Setting system privileges

System-level privileges are key components of the Role-Based Access Control (RBAC) system in Cloudera Data Visualization.

About this task

To configure system-level privileges for a role, follow the steps outlined below, using "Test Role 1" as an example.

Procedure

1. Activate system privileges.

On the System component line, click the Select all checkbox, next to the System category name.

This action activates the next four checkboxes, granting permissions for the following actions:

- Create workspaces
- View roles and users
- Manage roles and users
- Manage site settings
- Manage custom styles
- Manage jobs, email templates
- View activity logs
- Manage data connections
- Additional system privileges

Privileges Members

Component	Type	<input checked="" type="checkbox"/>	Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant view dashboards	Manage AVs/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards	
System		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
All connections / All datasets		<input checked="" type="checkbox"/>												<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				

[+ ADD PRIVILEGE](#)

* More information about the Additional system privilege can be found [here](#).

To grant only some of the System permissions, deselect the ones not permitted by the new role.

Privileges Members

Component	Type	<input checked="" type="checkbox"/>	Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant view dashboards	Manage AVs/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards	
System		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>										
All connections / All datasets		<input type="checkbox"/>												<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				

[+ ADD PRIVILEGE](#)

* More information about the Additional system privilege can be found [here](#).

2. Click SAVE at the top of the interface to save the changes made to the role.

What to do next

Once system privileges are configured, proceed to *Setting role privileges*.

For more information on possible permissions, see *RBAC permissions*.

Related Information

[Setting role privileges](#)

[RBAC permissions](#)

Setting role privileges

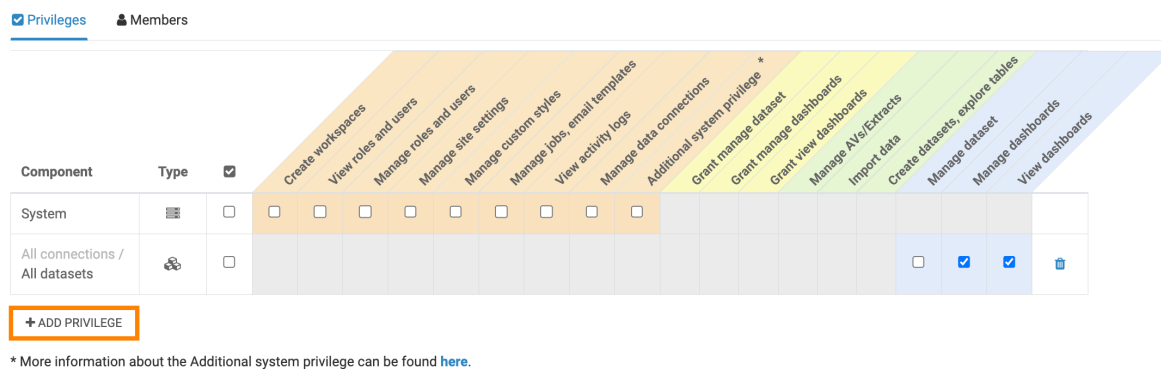
Role privileges are integral components of the Role-Based Access Control (RBAC) system in Cloudera Data Visualization. They define the level of dataset access that a role is allowed to grant to the members of a specified role.

About this task

Follow the steps below to add role privileges to a role, using "Test Role 1" as an example:

Procedure

1. Add a new role privilege by clicking +ADD PRIVILEGE.



The screenshot shows the 'Privileges' tab in the Cloudera Data Visualization interface. At the top, there are tabs for 'Privileges' and 'Members'. Below this is a grid of privilege categories, each with a checkbox. The categories include: Create workspaces, View roles and users, Manage roles and users, Manage site settings, Manage custom styles, Manage jobs, email templates, View activity logs, Manage data connections, Additional system privilege *, Grant manage dataset, Grant manage dashboards, Grant view dashboards, Manage AVs/Extracts, Import data, Create datasets, explore tables, Manage dataset, Manage dashboards, and View dashboards. Below the grid, there are two rows in a table: 'System' and 'All connections / All datasets'. The 'All connections / All datasets' row has checkboxes for 'Grant view dashboards', 'Manage dataset', and 'View dashboards'. Below the table is a '+ADD PRIVILEGE' button. A note below the button states: '* More information about the Additional system privilege can be found [here](#).'

The ADD PRIVILEGE modal window appears.

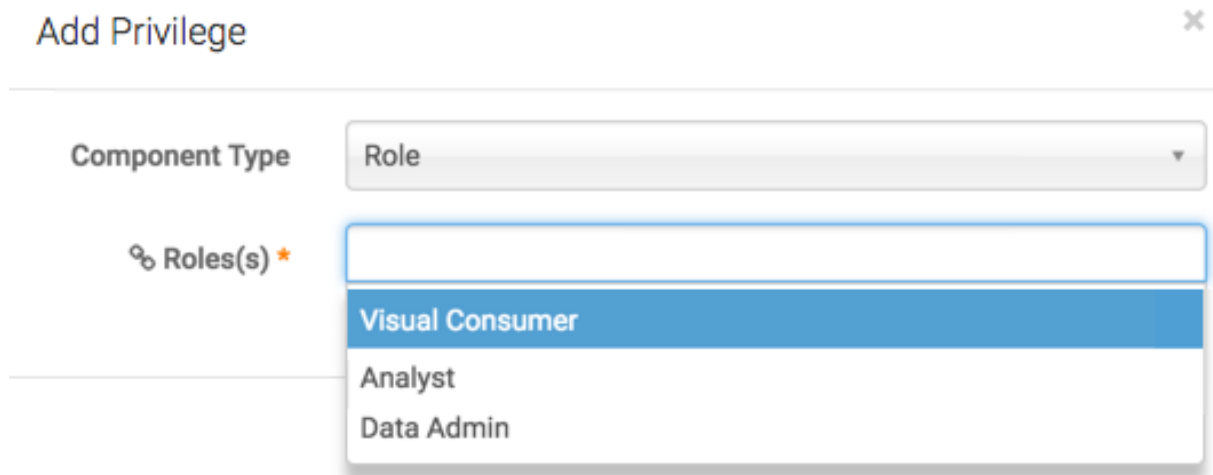


Note: The default privilege type is at the Connection level, but it can be changed by selecting Role or Dataset from the Component Types list.

2. In the Add Privilege modal window, under Component Type, select Role.
3. From Roles(s), choose one of the roles.



Note: You can repeat this step to add more roles to this privilege.



The screenshot shows the 'Add Privilege' modal window. At the top right is a close button (X). Below the title, there is a 'Component Type' dropdown menu with 'Role' selected. Below that is a 'Roles(s) *' field with a magnifying glass icon. A dropdown list is open below this field, showing three roles: 'Visual Consumer' (highlighted in blue), 'Analyst', and 'Data Admin'.

- After selecting the appropriate roles, click CREATE.

Add Privilege ✕

Component Type Role ▾

Roles(s) * Visual Consumer ✕

CANCEL
CREATE

The Role privilege for the selected role appears on the list of privileges.

By default, it contains all possible privileges for a role component:

- Grant manage dataset
- Grant manage dashboards
- Grant view dashboards

Privileges
Members

Component	Type		Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant manage dashboards	Grant view dashboards	Manage AVs/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards
System		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visual Consumer		<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							

+ ADD PRIVILEGE

* More information about the Additional system privilege can be found [here](#).

Additional notes:

- The privilege type is identified with the Roles icon.
 - The Grant view dashboards permission is mandatory if other permissions exist and cannot be removed. If you uncheck both Grant manage dashboards and Grant manage dataset, the Grant view dashboards permission becomes mutable and can be unselected.
 - The Grant manage dashboards permission is mandatory if Grant manage dataset permission is present and cannot be removed. If you uncheck Grant manage dataset, it becomes mutable and can be unselected.
 - The privilege can be deleted by clicking the Delete icon.
- For the role permission on Visual Consumer, select only the Grant view dashboards permission.

6. Repeat the process for Analyst and Data Admin roles, specifying the following permissions:

- For Analyst, specify the Grant manage dashboards and Grant view dashboards permissions.
- For Data Admin, specify all permissions: Grant manage dataset, Grant manage dashboards, and Grant view dashboards.

Privileges Members

Component	Type		Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant manage dashboards	Grant view dashboards	Manage AVE/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards	
System		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
Visual Consumer		<input type="checkbox"/>									<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>
Analyst		<input type="checkbox"/>									<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>
Database admin		<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>

+ ADD PRIVILEGE

* More information about the Additional system privilege can be found [here](#).

7. Click SAVE at the top of the interface to save the updates.

Results

- Members assigned to this role under the Members tab, can now grant dataset access based on the role-based privilege rows.
- The selections in the rows indicate the level of privileges each role receives on the Component line. For example, Analysts can grant Manage and View privileges to users.
- The dataset access permissions are granted to the roles defined on the component line.

What to do next

Proceed to *Setting connection privileges*.

For more information on possible permissions, see *RBAC permissions*.

Setting connection privileges

Connection privileges play a distinct role in the Role-Based Access Control (RBAC) system in Cloudera Data Visualization. They can be specified uniformly for multiple connections simultaneously or individually tailored for each connection, depending on business requirements.

About this task

Follow the below steps to add connection-level privileges to a role, using "Test Role 1" as an example.

Procedure

1. Add a new connection privilege by clicking +ADD PRIVILEGE.

Privileges Members

Component	Type	<input type="checkbox"/>	Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant manage dashboard	Grant view dashboards	Manage AVs/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards	
System		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
Visual Consumer		<input type="checkbox"/>										<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>							
Analyst		<input type="checkbox"/>										<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
Database admin		<input checked="" type="checkbox"/>										<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							

* More information about the Additional system privilege can be found [here](#).

The Add Privilege modal window appears.

2. From Connection(s), choose either All connections or one of the individual connections.

In this example, access to the samples connection is selected. You can repeat this step to add more connections to this privilege.

3. Click CREATE.

The screenshot shows a dialog box titled "Add Privilege". It has a close button (X) in the top right corner. Below the title, there are two input fields: "Component Type" with a dropdown menu currently showing "Connection", and "Connection(s) *" with a text input field containing "samples" and a close button (X). At the bottom right, there are two buttons: "CANCEL" and "CREATE".

The connection privilege for the samples connection is now listed among the role privileges.

By default, all possible privileges for a connection component are selected:

- Manage AVs/Extracts
- Import data
- Create datasets, explore tables

Privileges Members

Component	Type		Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage dataset	Grant manage dashboards	Grant view dashboards	Manage AVs/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards
System	☰	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									
Visual Consumer	👤	<input type="checkbox"/>										<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>						<input type="checkbox"/>
Analyst	👤	<input type="checkbox"/>										<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						<input type="checkbox"/>
Database admin	👤	<input checked="" type="checkbox"/>										<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						<input type="checkbox"/>
samples	🔗	<input checked="" type="checkbox"/>												<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input type="checkbox"/>

+ ADD PRIVILEGE

* More information about the Additional system privilege can be found [here](#).

Additional notes:

- The privilege type is identified with the Connection icon.
 - Manage AVs/Extracts and Import data are independent, and they include the Create datasets, explore tables permission. If you uncheck both of these 'greater' permissions, Create datasets, explore tables becomes mutable and can be unselected. But this removes any connection-level access components.
 - The privilege can be deleted by clicking the Delete icon.
4. Click SAVE at the top of the interface to save the latest changes to the role definition.

What to do next

Proceed to *Setting dataset privileges*.

For more information on possible permissions, see *RBAC permissions*.

Related Information[Setting dataset privileges](#)[RBAC permissions](#)

Setting dataset privileges

Dataset privileges form an integral part of the Role-Based Access Control (RBAC) system in Cloudera Data Visualization. Depending on business requirements, these privileges can be uniformly specified for multiple datasets simultaneously or tailored individually for each dataset.

About this task

Follow these steps to add dataset-level privileges to a role using "Test Role 1" as an example.

Procedure

1. Add a new dataset privilege by clicking +ADD PRIVILEGE.
2. In the Add Privilege modal window, from Component Type, select Dataset.
3. From Connection(s), choose either All connections or one of the individual connections.

In this example, access to the samples connection is selected.

4. From Datasets(s), select either All datasets or one of the individual connections.

To select additional datasets, repeat this step.

In this example, access to the Cereals, Iris, and World Life Expectancy datasets is selected.



Note: The datasets include the dataset ID.

The dataset privilege for the selected datasets appears on the list of privileges for the role.

By default, it contains all possible privileges for a dataset component:

- Manage dataset
- Manage dashboards
- View dashboards

Privileges Members

Component	Type	✓	Create workspaces	View roles and users	Manage roles and users	Manage site settings	Manage custom styles	Manage jobs, email templates	View activity logs	Manage data connections	Additional system privilege *	Grant manage privilege *	Grant manage dataset	Grant view dashboards	Manage AV/Extracts	Import data	Create datasets, explore tables	Manage dataset	Manage dashboards	View dashboards	
System	System	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>											
Visual Consumer	Visual Consumer	<input type="checkbox"/>									<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>
Analyst	Analyst	<input type="checkbox"/>									<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>
Database admin	Database admin	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								<input type="checkbox"/>
samples	samples	<input checked="" type="checkbox"/>												<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					<input type="checkbox"/>
samples / Cereals, Iris, World Life Expectancy	samples / Cereals, Iris, World Life Expectancy	<input checked="" type="checkbox"/>																	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

+ ADD PRIVILEGE

* More information about the Additional system privilege can be found [here](#).

Additional note:

- The Dataset icon specifies the type.
- Two permissions, Manage dashboards and View dashboards, are mandatory if the privilege contains the Manage dataset permission and cannot be removed. The checkboxes in these columns are filled in and fixed.
 - If you unselect Manage dataset, Manage dashboards becomes mutable and can be unselected.
 - If you uncheck Manage dashboards, View dashboards becomes mutable and can be unselected.









- c. You can remove this privilege by clicking the Delete icon.
5. Click SAVE at the top of the interface to save the changes to the role.

Results

The role definition for Test Role 1 is now complete and it has six distinct components.

Roles

+ NEW ROLE

Role / Description	Components	Users	Groups	
Analyst	1	0	0	 
Data Admin	1	0	0	 
Test Role 1 Testing role creation	6	0	0	 
Visual Consumer	1	0	0	 

For more information on possible permissions, see *RBAC permissions*.

Related Information

[RBAC permissions](#)

Editing role assignments

About this task

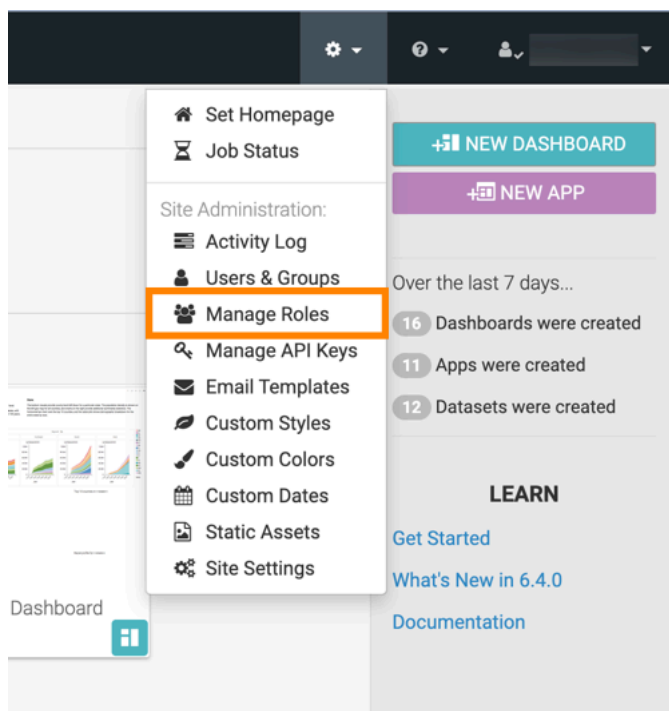
The following steps demonstrate how to edit role assignments for a specific role.

In this example, Test Role 1 is used, which was previously defined in *Creating new roles*.

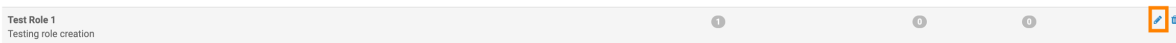
Procedure

1. On the main navigation bar, click the (gear) icon.

- In the drop-down menu, click Manage Roles.



- In the Roles interface, next to the role to edit, click the Pencil icon.



Note: If you do not have any roles defined, see the instructions in *Creating new roles*.

- On the Role definition interface, click Edit.
- Click the Members tab and proceed to edit member roles through one of the following procedures:
 - Assigning roles to a single user
 - Assigning roles to user groups
 - Assigning multiple roles to multiple users

Related Information

[Creating new roles](#)

[Assigning roles to a single user](#)

[Assigning roles to user groups](#)

[Assigning multiple roles to multiple users](#)

Assigning roles to users

About this task

The following steps demonstrate how to add users to a role. In this example, an existing role Test Role 1 is used.

Procedure

1. Under the Members tab, in the Users list, click EDIT USER(S)
The Role Assignment modal window appears.

Role Assignment ✕

Members

🔍

Available to select

- Select All
- Administrator
- ArcadiaAdmin
- ArcadiaUser
- CArep1
- CArep2
- NVrep1
- NormalUser
- ORrep1

ADD >>

<<

Selected

Select users from the left to add to the role's members

+ ADD

CANCEL

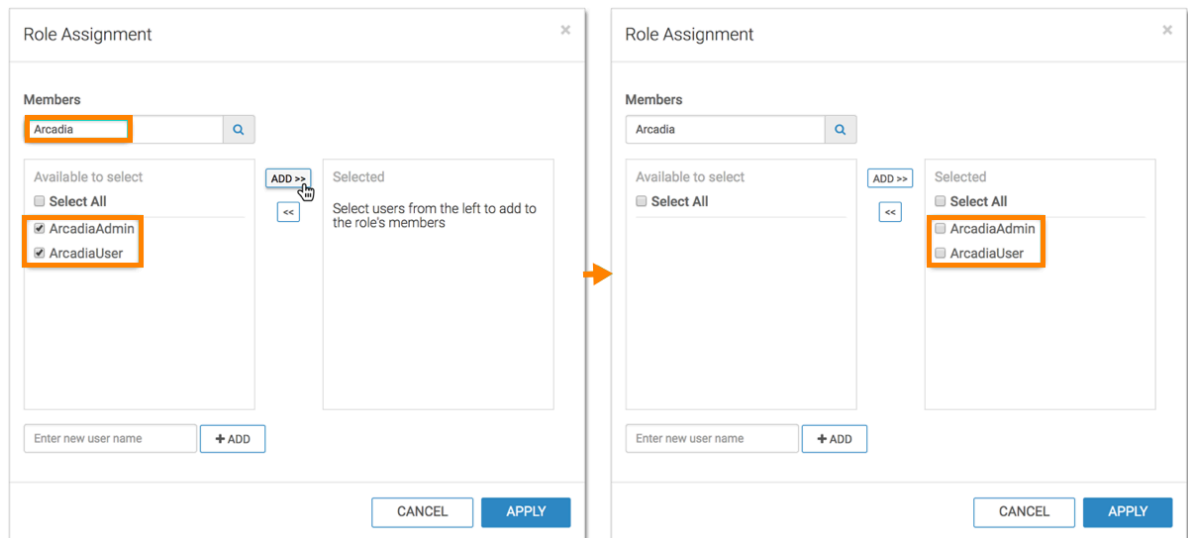
APPLY

2. There are several options to add a user as a member:

- Search

If you have a long list of users in the Members section, use the Search box to find user names, select them from the sub-list, and click ADD>> to move them to the right side of the modal window.

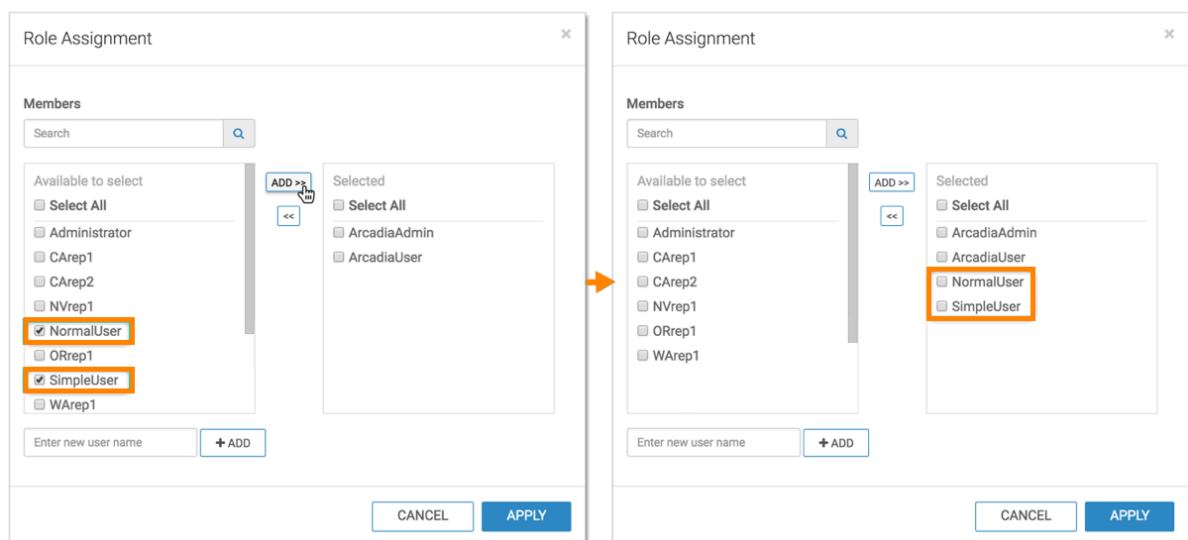
When you are ready, click APPLY.



- Select

In the Members section, select the users to assign to the role and click ADD>> to move them to the right side of the modal window.

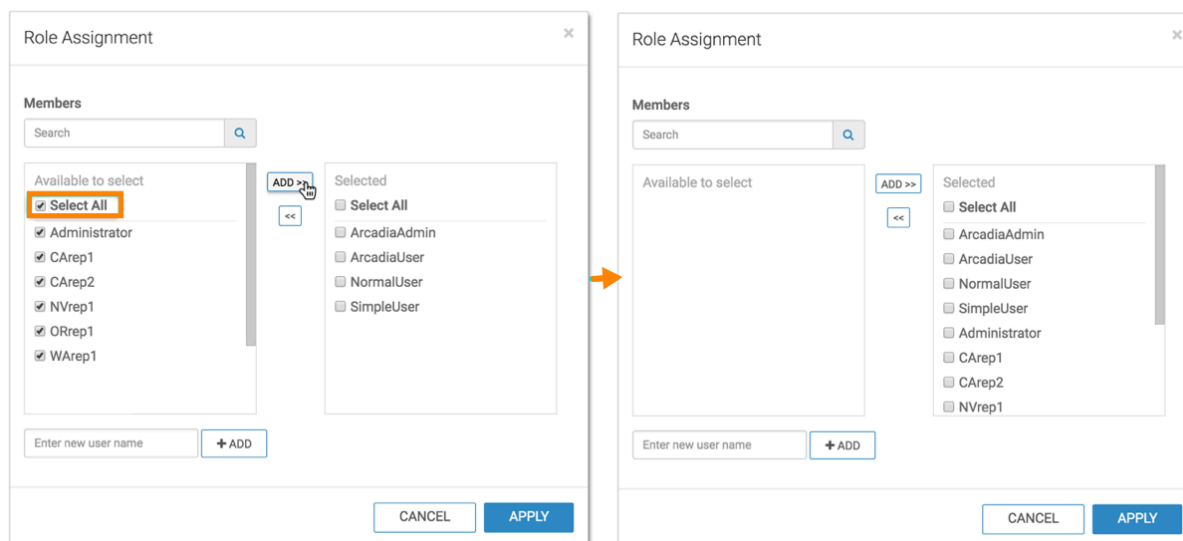
When you are ready, click APPLY.



- Select All

To assign all users to Members, mark Select All to get all user names and click ADD>> to move them to the right side of the modal window.

When you are ready, click APPLY.

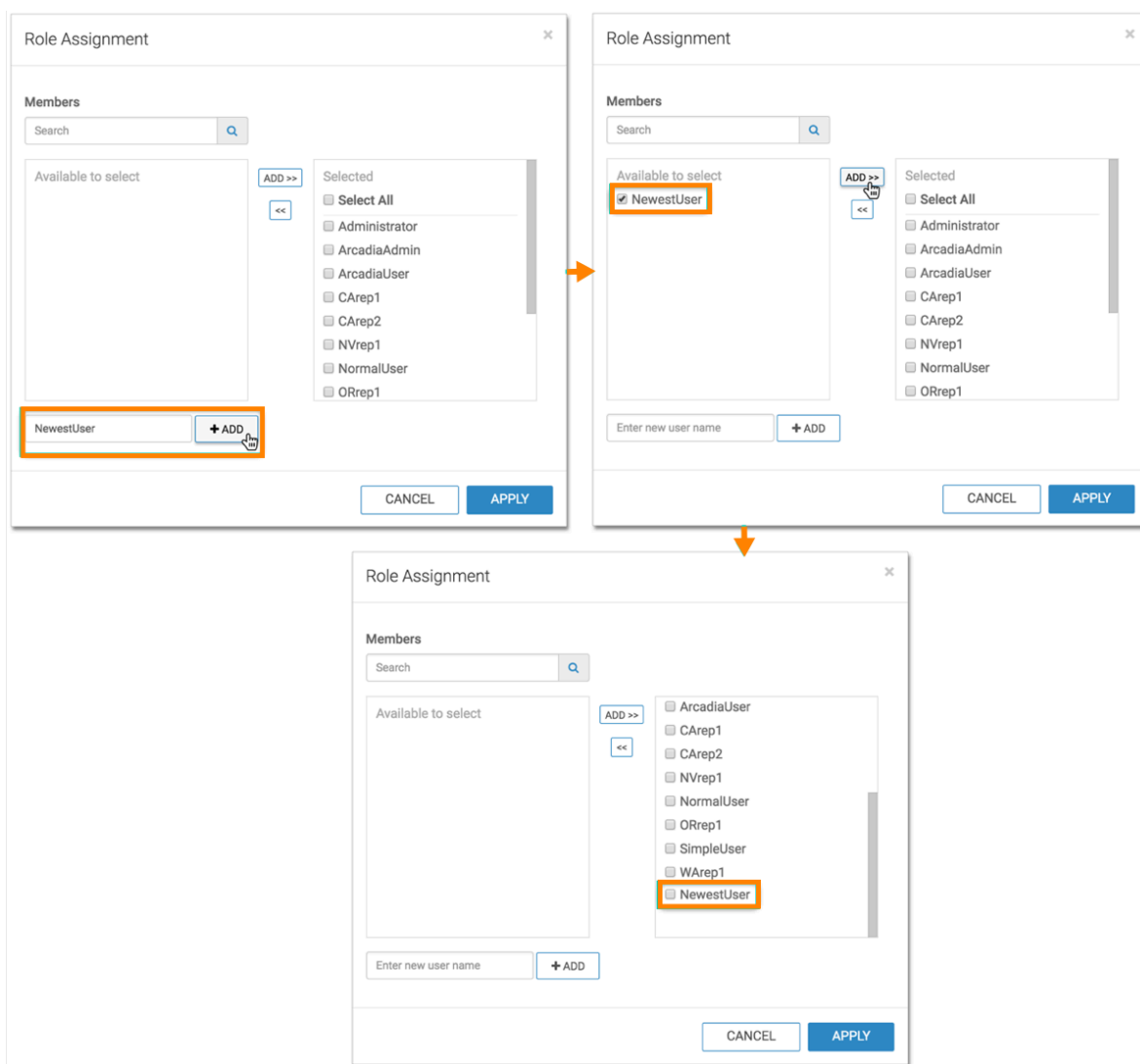


- Adding externally defined users; LDAP authentication

For convenience, the Role Assignment interface supports adding usernames that are not stored locally. For example, you can add known usernames available through LDAP authentication in this manner.

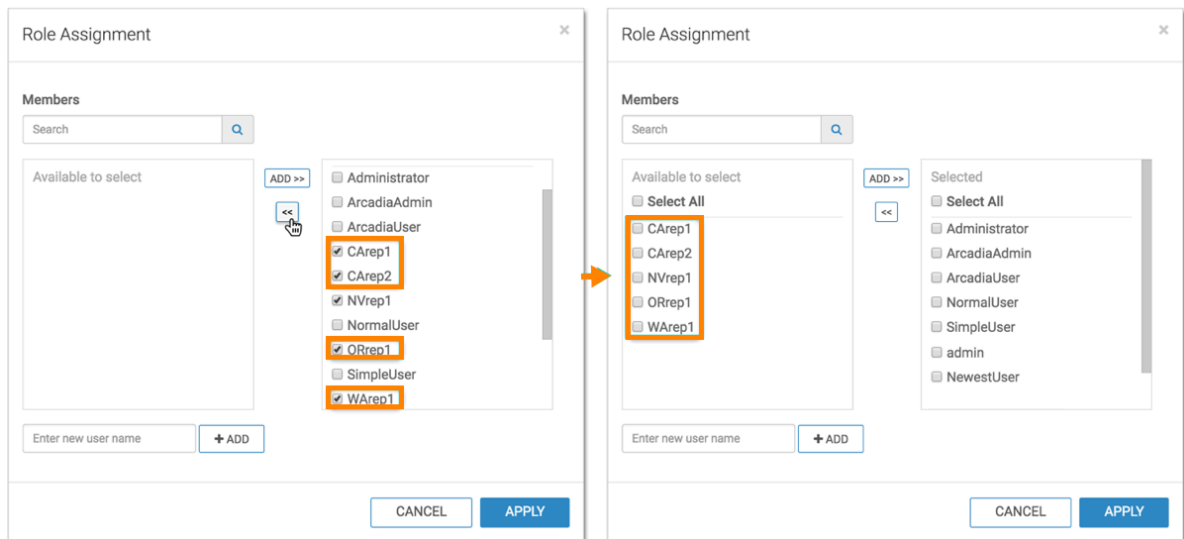
Enter the new user name and click ADD>>. After the new user name appears in the Members section, select it and click ADD>> to move the new user to the right side of the modal window.

When you are ready, click APPLY.



- Remove

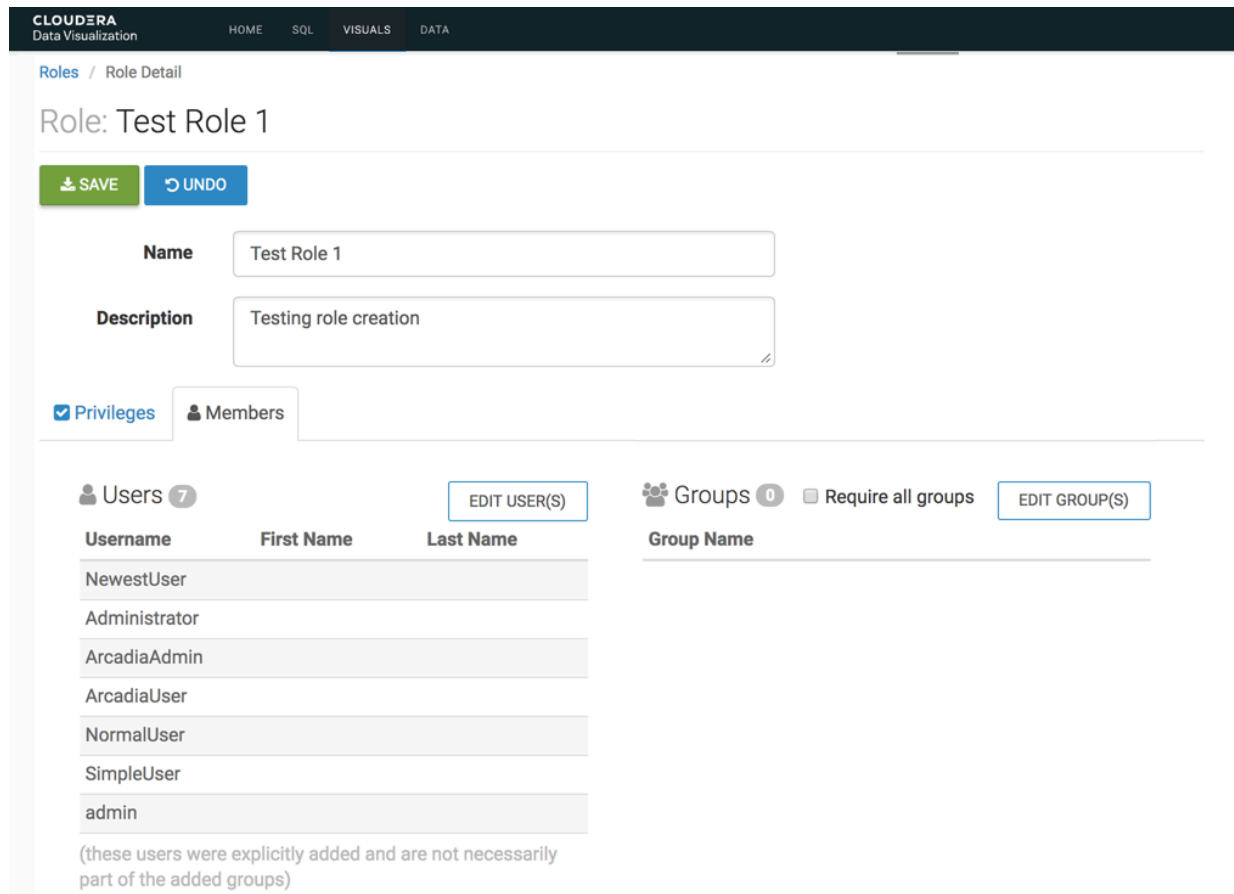
To remove users from the Members list, select the user(s) on the right side panel and click <<. When you are ready, click APPLY.



The list of users assigned to the role appears in the Role: Test Role 1 interface, under the Members tab.

3. Click SAVE.

A confirmation of the role update appears briefly on the screen and the members list is updated.



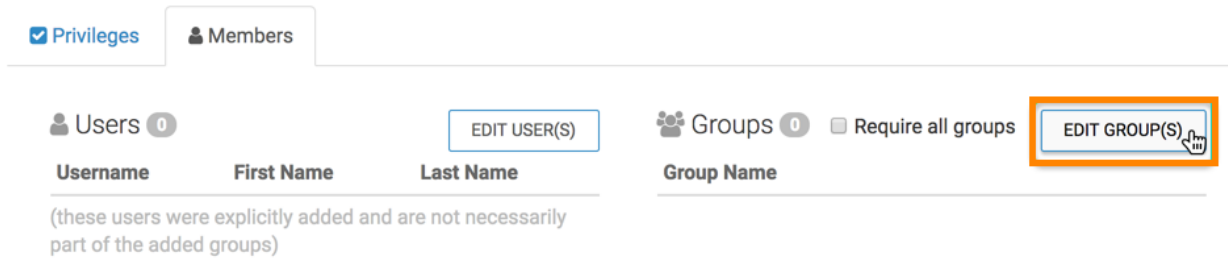
Assigning roles to user groups

About this task

The following steps demonstrate how to add user groups to a role. In this example, an existing role Administrators Only is used.

Procedure

1. Under the Members tab, in the Users list, click EDIT GROUP(S).



The screenshot shows the Cloudera interface with the 'Members' tab selected. At the top, there are two tabs: 'Privileges' (checked) and 'Members'. Below the tabs, there are two sections: 'Users' and 'Groups'. The 'Users' section has a header with 'Users 0' and a button 'EDIT USER(S)'. Below it are columns for 'Username', 'First Name', and 'Last Name'. A note below the columns reads: '(these users were explicitly added and are not necessarily part of the added groups)'. The 'Groups' section has a header with 'Groups 0' and a checkbox 'Require all groups'. Below it is a column for 'Group Name'. A button 'EDIT GROUP(S)' is highlighted with an orange border and a mouse cursor is pointing at it.

The Require all groups option ensures that only members of ALL groups listed in the role membership fields have the role's defined access.

In this example, Administrators Only role is shared by members of both Administrators and Arcadians user groups. The Require all groups should not be selected so that all members of either group get the privileges of the

role. However, if you check the Require all groups option, only users who are members of BOTH user groups get the privileges of the role.

**Note:**

There are two other ways a user can be a member of the role, even when the Require all groups option is on:

- a. If the user is named specifically in the Users section of the membership page.
- b. For roles that are imported, if the Groups section is empty, and the user is a member of ANY Ranger group.

When you click EDIT GROUP(S), the Role Assignment modal window appears.

Role Assignment ✕

Members

Q

Available to select

ADD >>

Select All

Administrators

Arcadians

Everyone

Group One

SalesReps

Selected

Select groups from the left to add to the role's members

Enter new group name

+ ADD

CANCEL

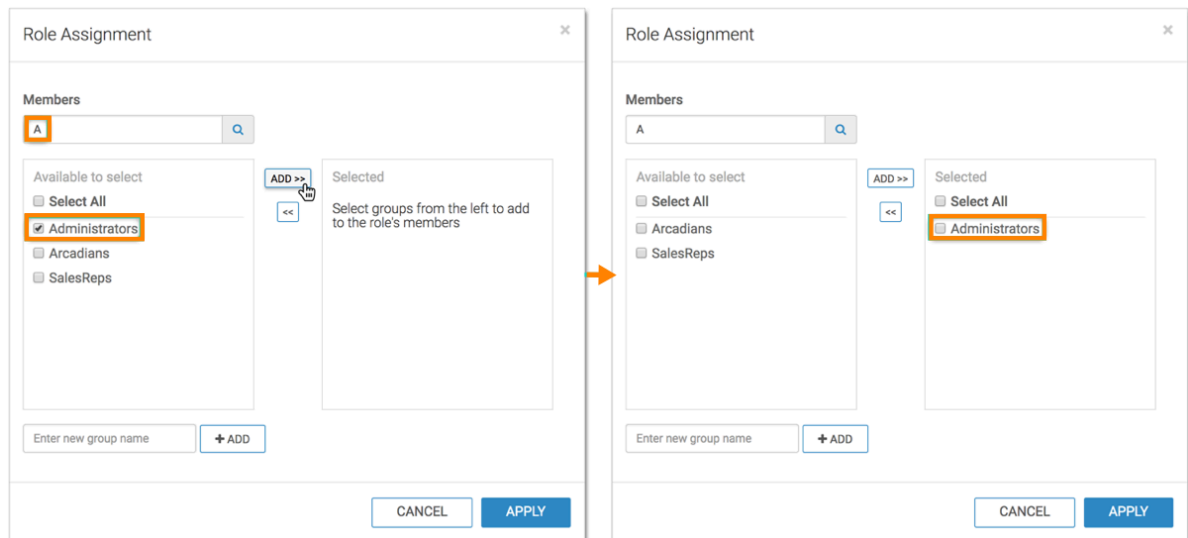
APPLY

2. There are several options to add groups to role membership:

- Search

If you have a long list of groups in the Members section, use the Search box to find group names, select them from the sub-list, and click ADD>> to move them to the right side of the modal window.

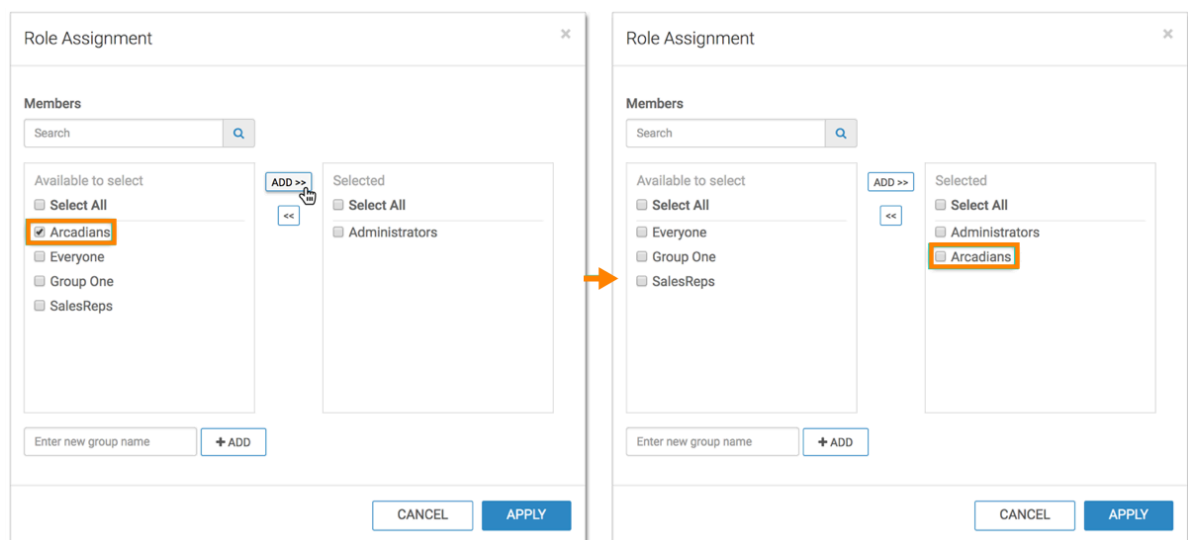
When you are ready, click APPLY.



- Select

In the Members section, select the groups to assign to the role and click ADD>> to move them to the right side of the modal window.

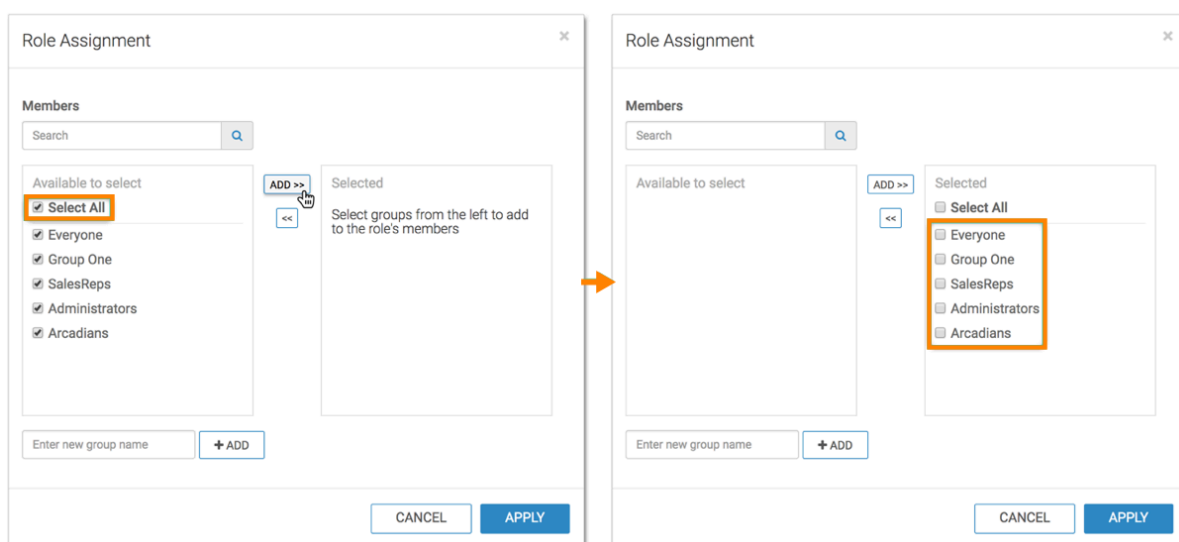
When you are ready, click APPLY.



- Select All

To assign all groups to Members, mark Select All to get all group names and click ADD>> to move them to the right side of the modal window.

When you are ready, click APPLY.

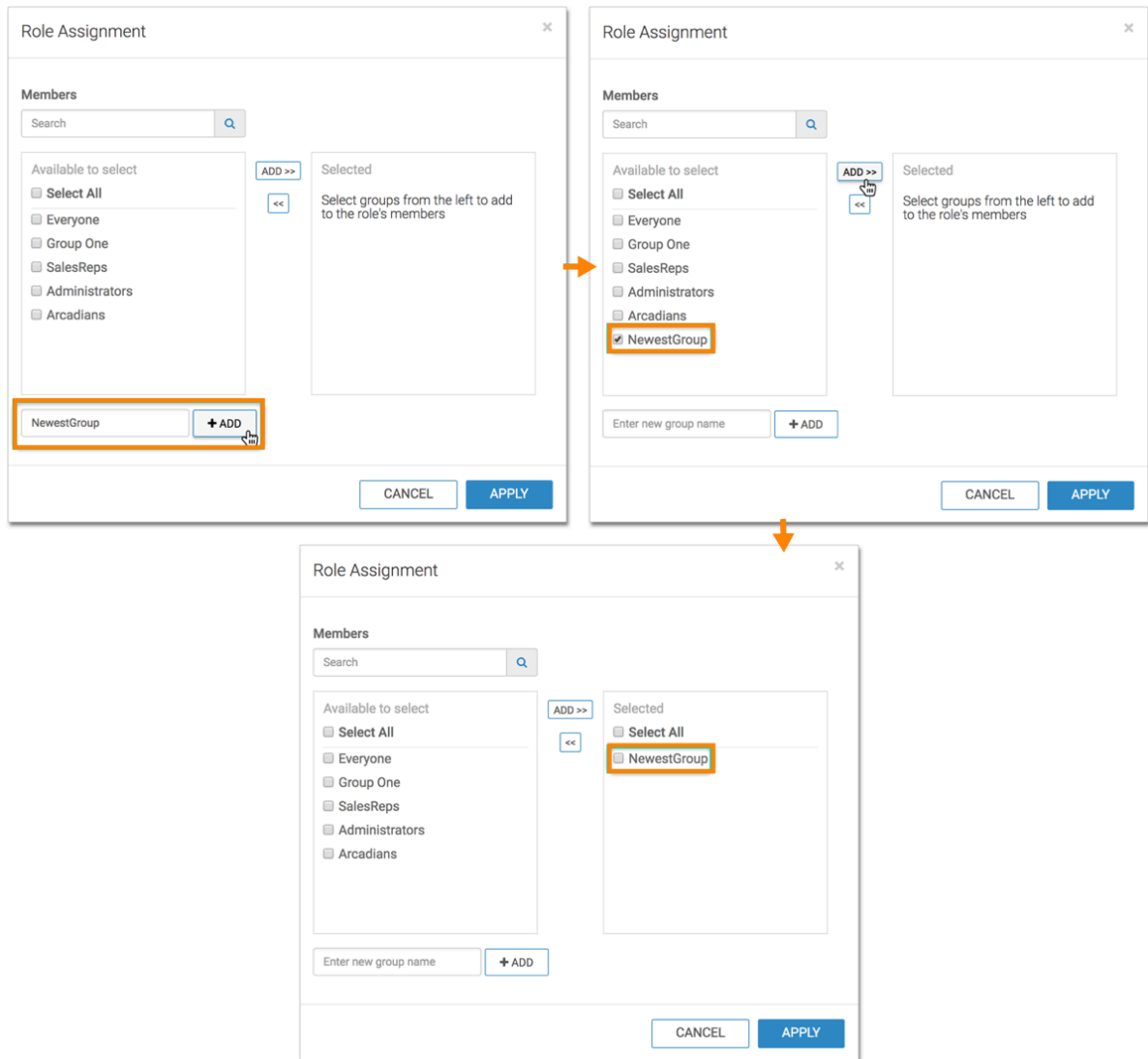


- Adding externally defined users; LDAP authentication

For convenience, the Role Assignment interface supports adding user groups to the list of assignees that are not stored locally. For example, you can add known groups available through LDAP authentication in this manner.

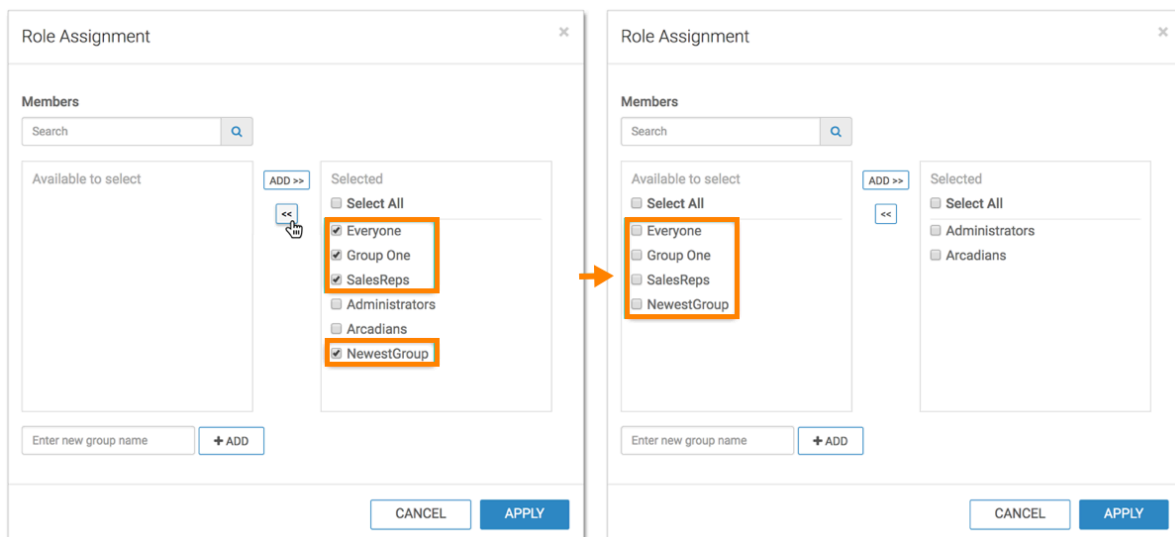
Enter the new group name and click ADD>>. After the new group name appears in the Members section, select it and click ADD>> to move the new group to the right side of the modal window.

When you are ready, click APPLY.



- Remove

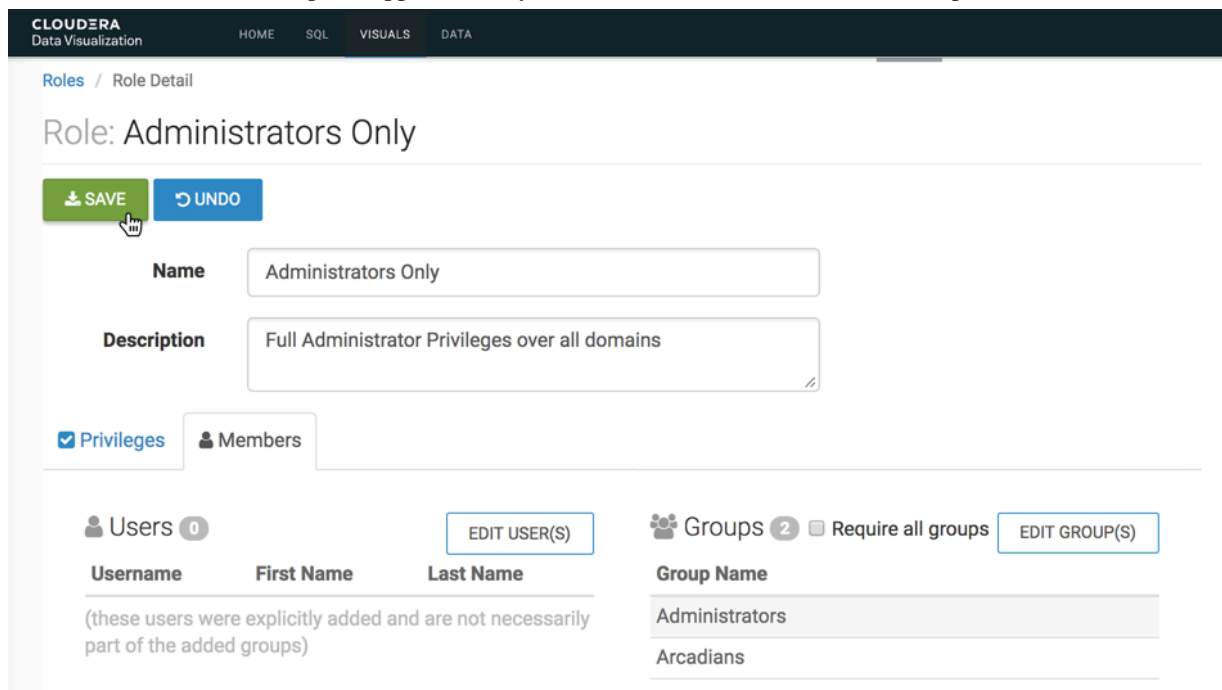
To remove users from the Members list, select the user(s) on the right side panel and click <<. When you are ready, click APPLY.



The list of groups assigned to the role appears in the Role: Administrators Only interface, under the Members tab.

3. Click SAVE.

A confirmation of the role update appears briefly on the screen and the members list is updated.



Assigning multiple roles to multiple users

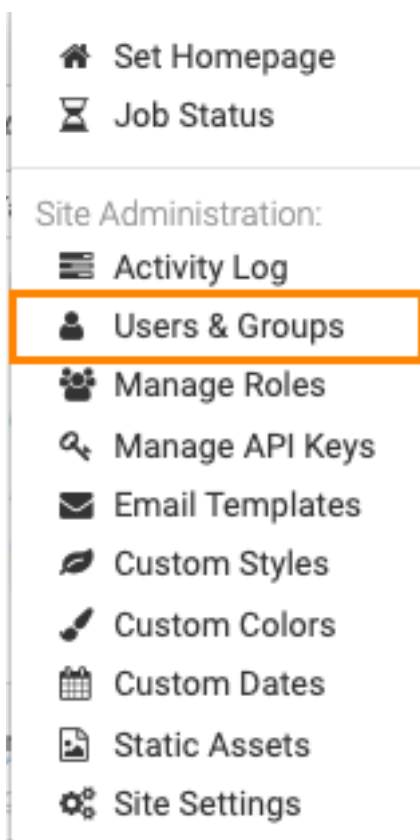
About this task

The following steps demonstrate how to add multiple users to multiple roles in the Users interface. In this example, existing roles Test Role 1 and View Only are used.

To assign multiple users to existing roles, follow these steps:

Procedure

1. On the main navigation bar, click, the Gear icon.
2. In the drop-down menu, click Users & Groups.



The Manage Users & Groups interface appears, open on the Users tab.

3. Select the users that you want to assign to roles.

4. Click ADD TO ROLES.

The screenshot shows the 'Manage Users & Groups' interface. The 'ADD TO ROLES' button is highlighted with an orange box. Below it, a table lists users with their roles. Several users (CArep1, CArep2, NVrep1, ORrep1, WArep1) are selected with checkboxes, and their roles are highlighted with orange boxes.

Username	Permissions	Date Joined	Last Login	Member of Group(s)	Roles	Status
admin	Admin	2 years ago	a year ago	Administrators	Test Role 1, Administrators Only	A
Administrator	Admin	a year ago	20 days ago	Administrators	Test Role 1, Administrators Only	A
ArcadiaAdmin	Admin	2 months ago	2 months ago	Administrators	Test Role 1, Administrators Only	A
ArcadiaUser	Normal	2 years ago	7 months ago		Test Role 1	A
<input checked="" type="checkbox"/> CArep1	Normal	a year ago	a year ago	SalesReps		A
<input checked="" type="checkbox"/> CArep2	Normal	a year ago	a year ago	SalesReps		A
NormalUser	Normal	2 months ago	2 months ago		Test Role 1	I
<input checked="" type="checkbox"/> NVrep1	Normal	a year ago	a year ago	SalesReps		A
<input checked="" type="checkbox"/> ORrep1	Normal	a year ago	a year ago	SalesReps		A
SimpleUser	Normal	7 months ago	7 months ago		Test Role 1	A
<input checked="" type="checkbox"/> WArep1	Normal	a year ago	a year ago	SalesReps		A

Showing 1 to 11 of 11 entries

5. In the drop-down menu, select the roles you plan to assign to the selected users, and click SAVE.

In this example, the roles Test Role 1 and View Only are used.

The sequence of three screenshots shows the 'ADD TO ROLES' dropdown menu. The first shows the menu open with 'Administrators Only', 'Test Role 1', and 'View Only' options. The second shows 'Test Role 1' and 'View Only' selected. The third shows the 'Save' button being clicked.

Results

Note the changes to the information in the Users interface.

Deleting roles

You can easily delete a previously defined role in role-based access control (RBAC) system.

About this task

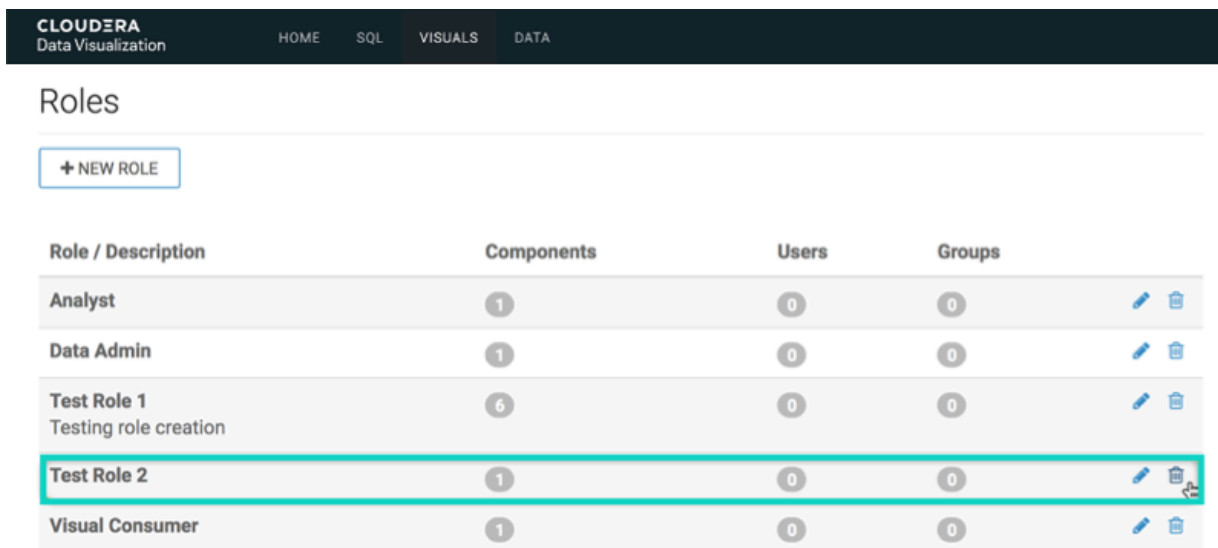


Note: This feature is only available to users with Manage roles and users privileges.











The following steps demonstrate how to add or change privileges defined for a specific role. In this example, Test Role 1 is used, which was previously defined in *Creating new roles*.

Procedure

1. In the Roles interface, click the Trash can icon located next to the role you want to delete.



The screenshot shows the Cloudera Data Visualization Roles interface. At the top, there is a navigation bar with the Cloudera logo and the text "Data Visualization", along with menu items for HOME, SQL, VISUALS, and DATA. Below the navigation bar, the title "Roles" is displayed. A button labeled "+ NEW ROLE" is located at the top left of the main content area. The main content area contains a table with the following columns: "Role / Description", "Components", "Users", "Groups", and an action column with edit and delete icons. The table lists five roles: Analyst, Data Admin, Test Role 1 (Testing role creation), Test Role 2, and Visual Consumer. The "Test Role 2" row is highlighted with a red border, and a mouse cursor is clicking on the delete icon in the action column for this role.

Role / Description	Components	Users	Groups	
Analyst	1	0	0	 
Data Admin	1	0	0	 
Test Role 1 Testing role creation	6	0	0	 
Test Role 2	1	0	0	 
Visual Consumer	1	0	0	 

2. In the Delete Confirmation modal window, click DELETE.

Related Information

[Creating new roles](#)