Cloudera Data Visualization 7.2.8

Working with User Roles

Date published: 2020-10-30
Date modified: 2024-10-30

https://docs.cloudera.com/

Legal Notice

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

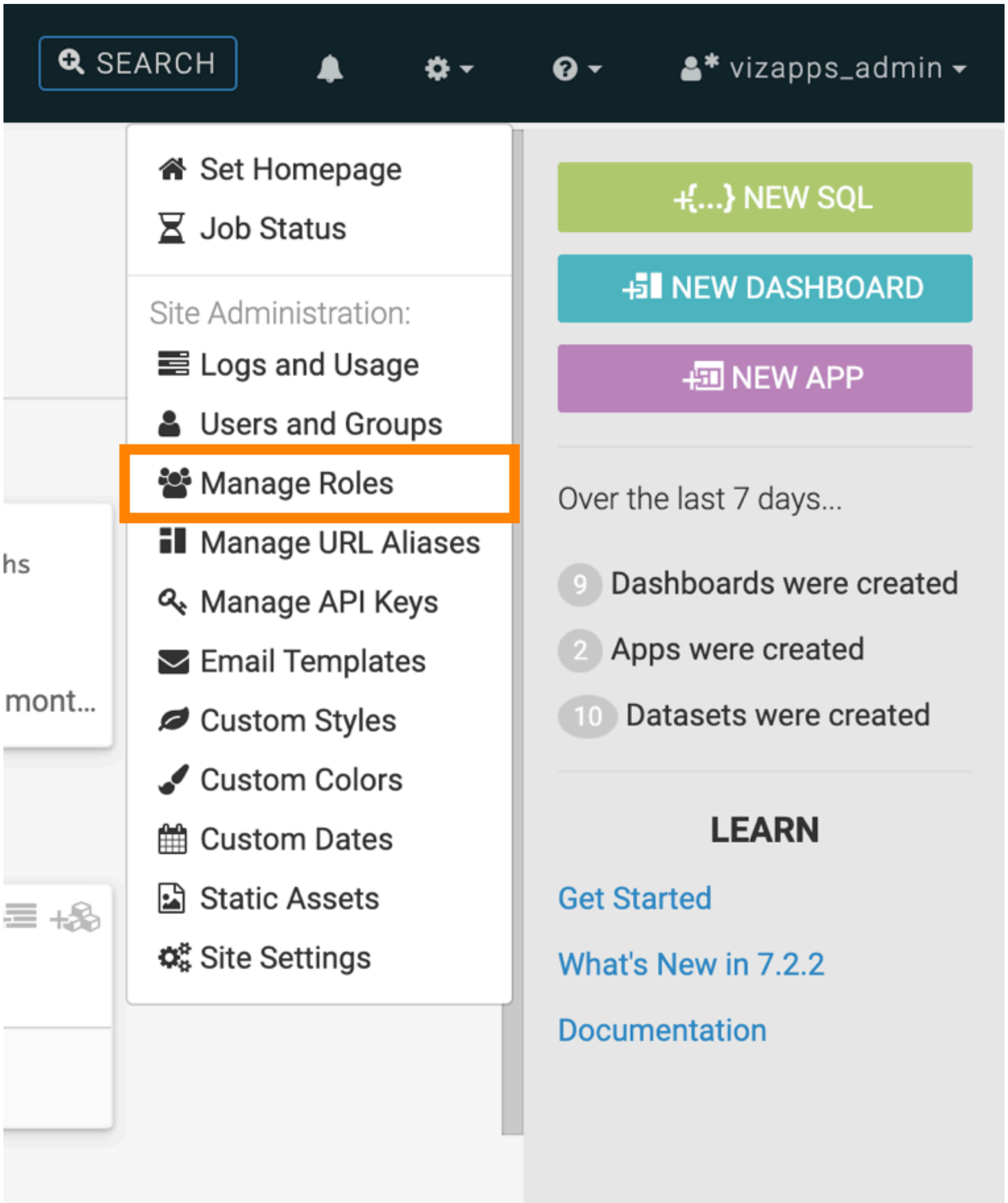
About this task

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

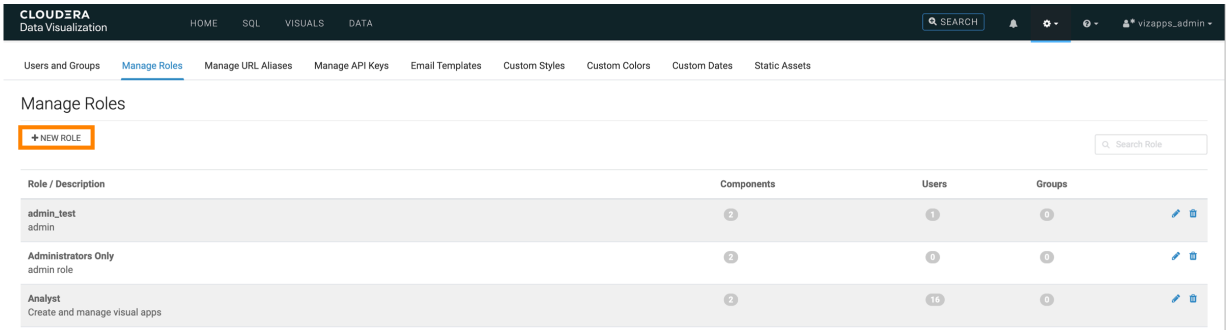
Follow these steps demonstrate to create a new role.

Procedure

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

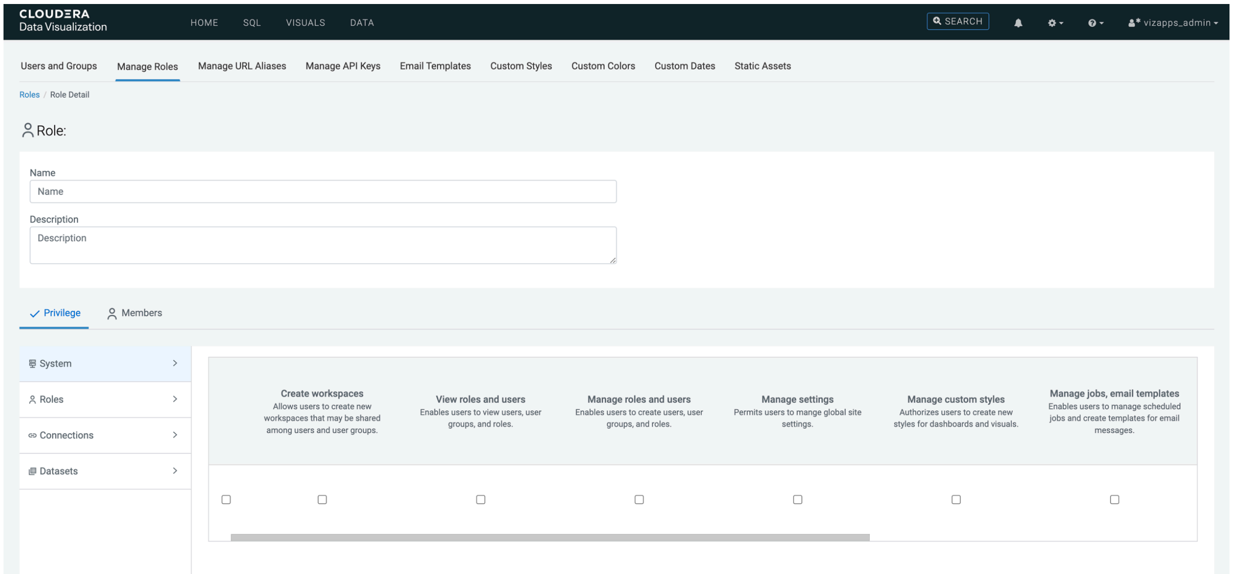


3. Click NEW ROLE.



Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

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

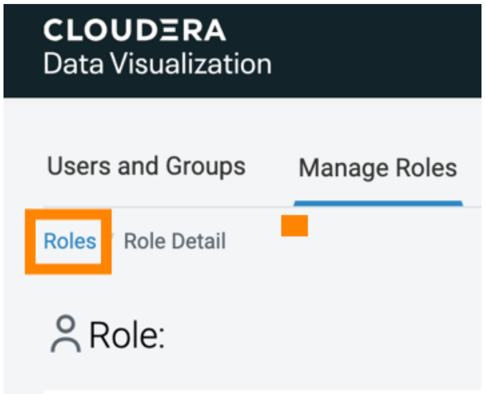


Name: Name

Description: Description

□	**Create workspaces** Allows users to create new workspaces that may be shared among users and user groups.	**View roles and users** Enables users to view users, user groups, and roles.	**Manage roles and users** Enables users to create users, user groups, and roles.	**Manage settings** Permits users to mange global site settings.	**Manage custom styles** Authorizes users to create new styles for dashboards and visuals.	**Manage jobs, email templates** Enables users to manage scheduled jobs and create templates for email messages.
	□	□	□	□	□	□

4. Define role details.
   a) Provide a distinctive name for the new role.
   b) In the Description field, briefly explain the purpose or context of the new role.
   c) Click APPLY CHANGES to save the role.
5. To ensure the role was successfully created, click Roles in the top left corner of the page.



The newly created role should now be visible in the role list.

What to do next

Proceed by defining *role privileges* and *editing role assignments* as needed for the newly created role.

Related Information

Editing role assignments

Role privileges

Adding privileges

Once you have defined a new role in the Role-Based Access Control (RBAC) system of Cloudera Data Visualization, you can start adding privileges to that role.

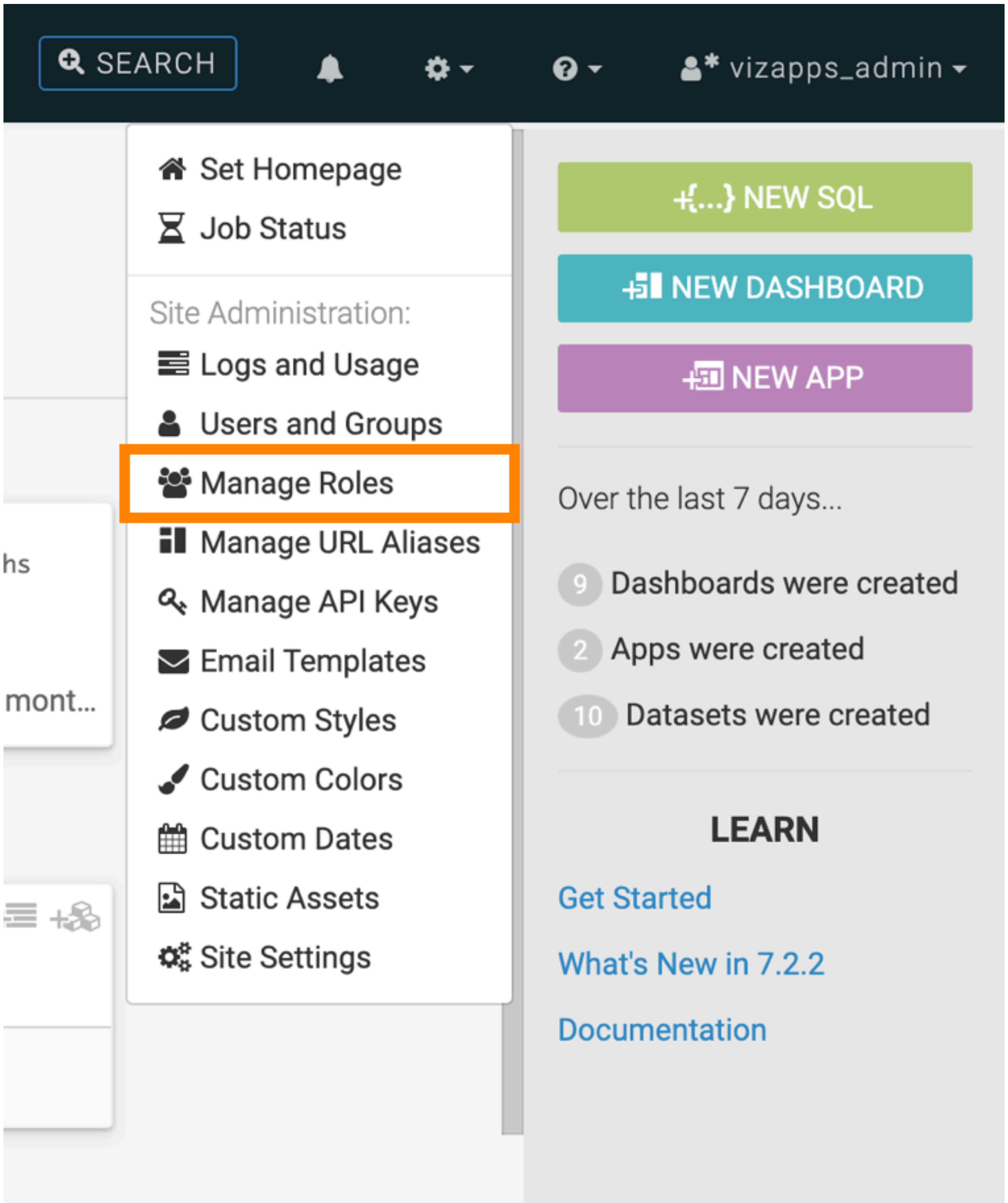
About this task

The following steps show you how to add or modify privileges associated with a specific role.

Procedure

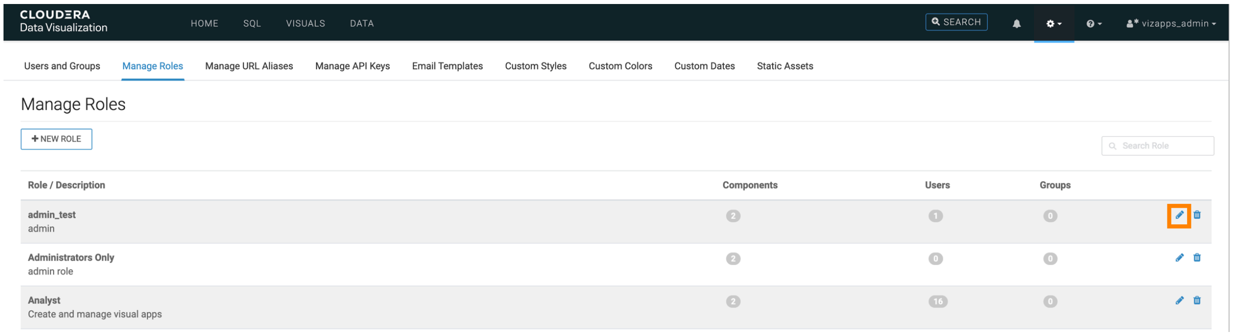
1. On the main navigation bar, click the (gear) icon.

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



3. In the Manage Roles interface, locate the role you wish to edit and click on the (edit) icon next to the respective role.

   You can use the Search Role box to find the role you want to edit.

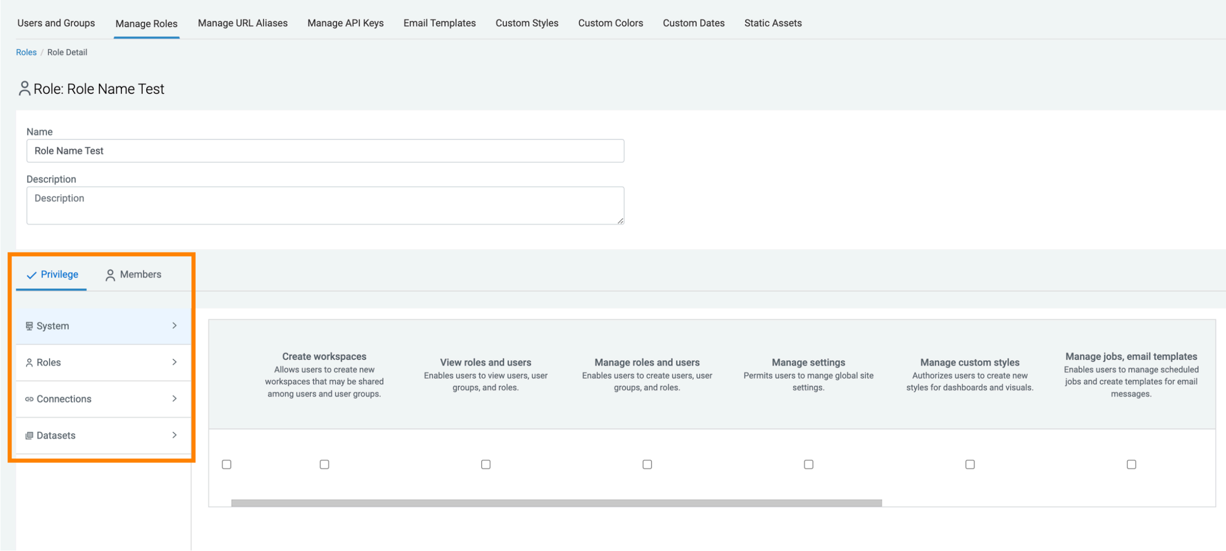


Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

4. On the Role Detail interface, you can set the following groups of privileges:

- *System privileges*
- *Role privileges*
- *Connection privileges*
- *Dataset privileges*



Name: Role Name Test

Description: Description

	Create workspaces Allows users to create new workspaces that may be shared among users and user groups.	View roles and users Enables users to view users, user groups, and roles.	Manage roles and users Enables users to create users, user groups, and roles.	Manage settings Permits users to mange global site settings.	Manage custom styles Authorizes users to create new styles for dashboards and visuals.	Manage jobs, email templates Enables users to manage scheduled jobs and create templates for email messages.
☐	☐	☐	☐	☐	☐	☐

5. After configuring the desired privileges for the role, click APPLY CHANGES to save 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.

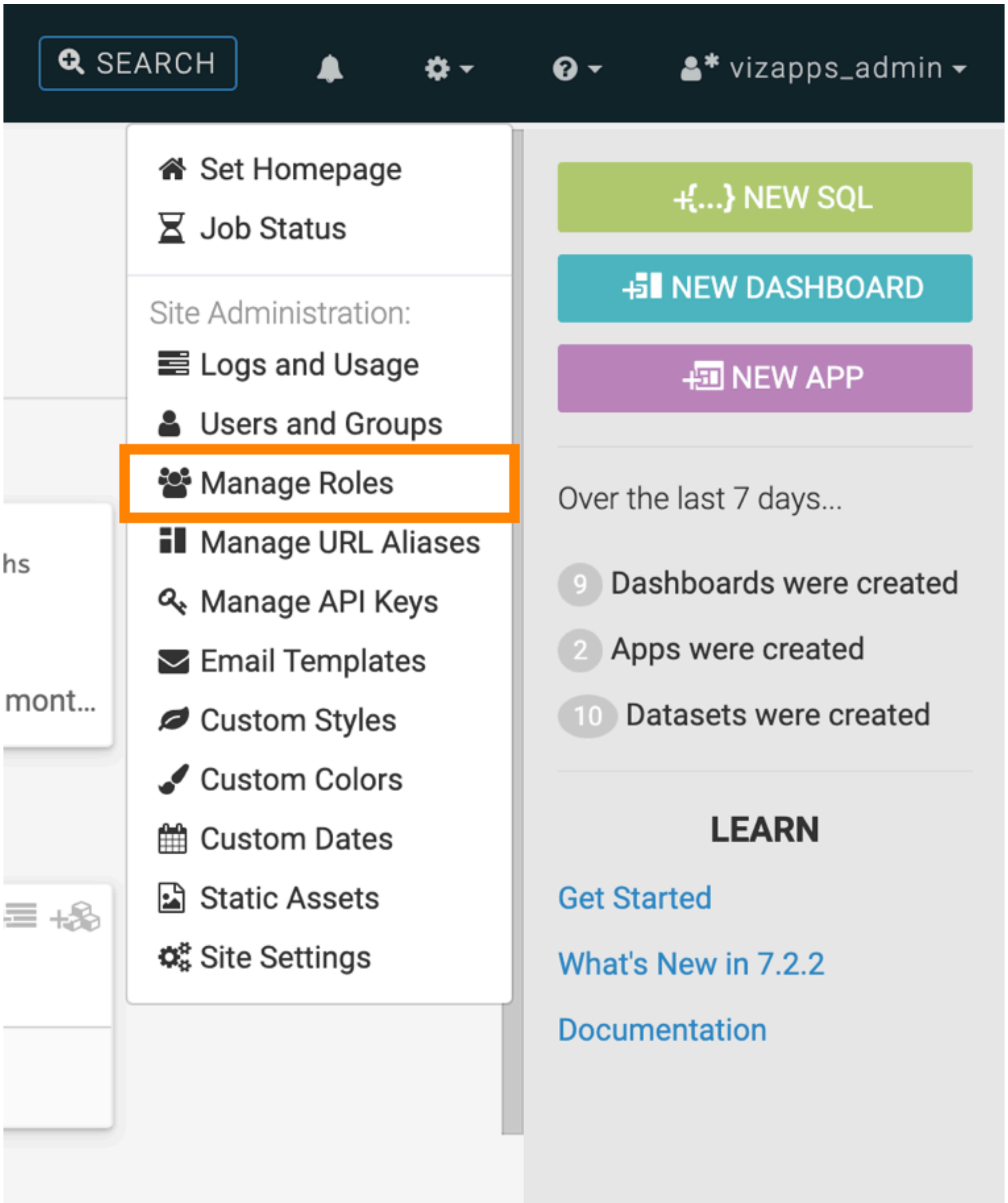
About this task

To configure system-level privileges for a role, follow the steps outlined below.

Procedure

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

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



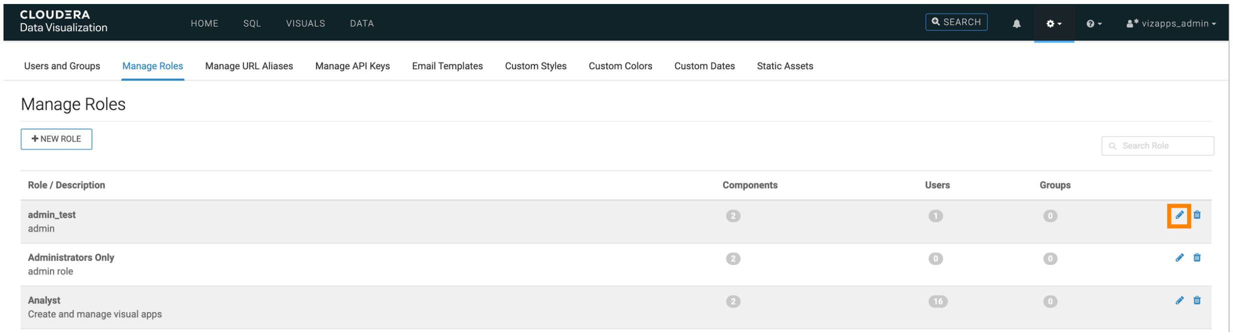
Over the last 7 days...

9 Dashboards were created

2 Apps were created

10 Datasets were created

3. In the Manage Roles interface, find the role you wish to edit and click on the (edit) icon next to the respective role. You can use the Search Role box to find the role you want to edit.



Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

The Role Detail interface is displayed.

4. Locate the System category on the Privilege tab and select the checkboxes for the actions you want to permit for the role.

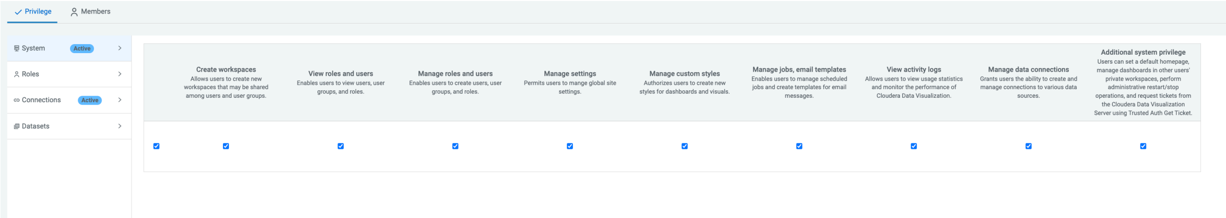
   Click the Select all checkbox, next to the System category name if you want to activate all permissions.

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

   Note:

   Privilege dependency information:

   The View roles and users permission is mandatory if the privilege includes the Manage roles and users permission and cannot be removed. The checkboxes for these permissions are pre-filled and fixed. If Manage roles and users is deselected, the View roles and users permission becomes optional and can also be deselected.



	Create workspaces Allows users to create new workspaces that may be shared among users and user groups.	View roles and users Enables users to view users, user groups, and roles.	Manage roles and users Enables users to create users, user groups, and roles.	Manage settings Permits users to mange global site settings.	Manage custom styles Authorizes users to create new styles for dashboards and visuals.	Manage jobs, email templates Enables users to manage scheduled jobs and create templates for email messages.	View activity logs Allows users to view usage statistics and monitor the performance of Cloudera Data Visualization.	Manage data connections Grants users the ability to create and manage connections to various data sources.	Additional system privilege Users can set a default homepage, manage dashboards in other users' private workspaces, perform administrative restart/stop operations, and request tickets from the Cloudera Data Visualization Server using Trusted Auth Get Ticket.
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

5. Click APPLY CHANGES 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 available 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.

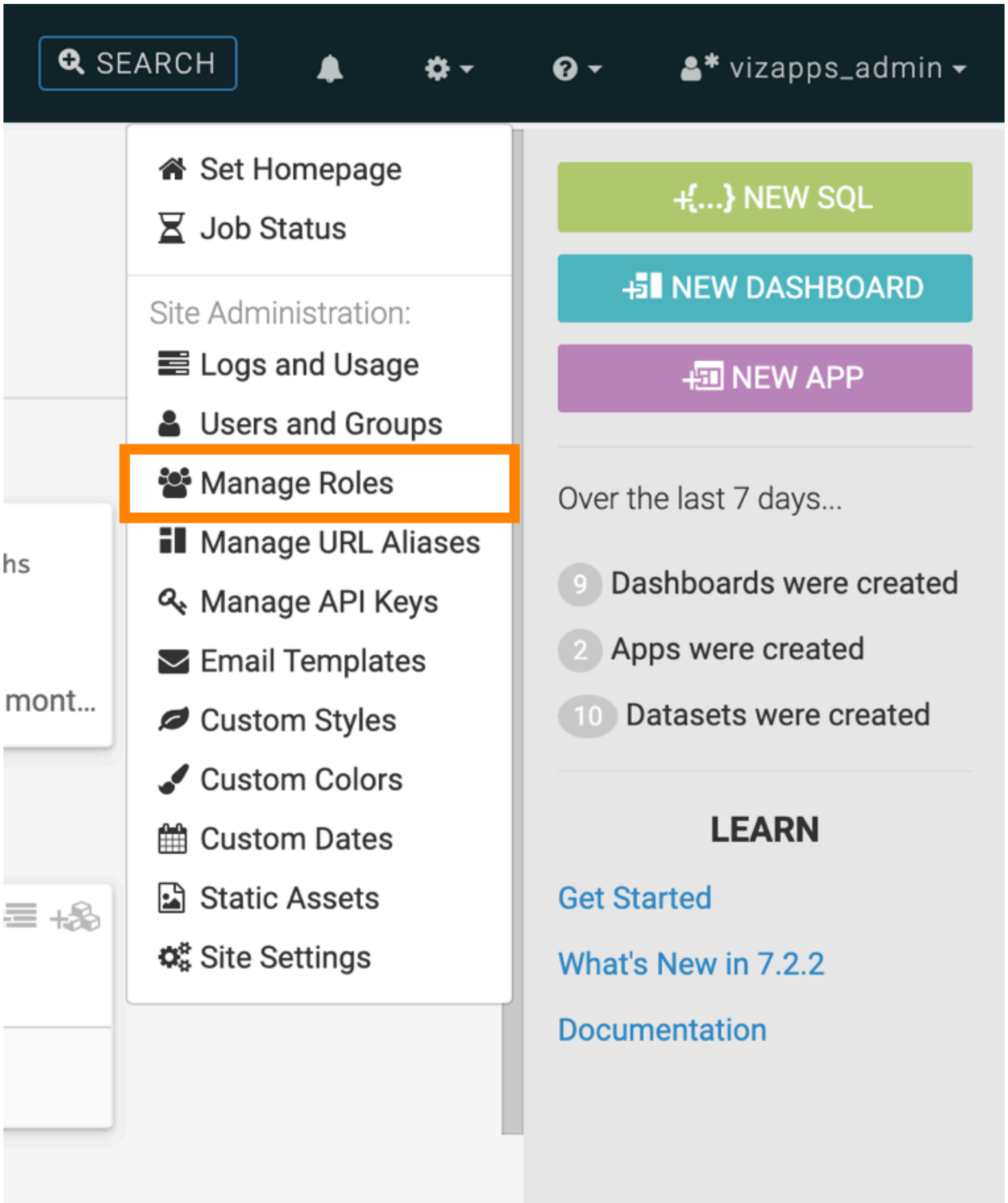
About this task

To add new role privileges to a role, follow the steps outlined below.

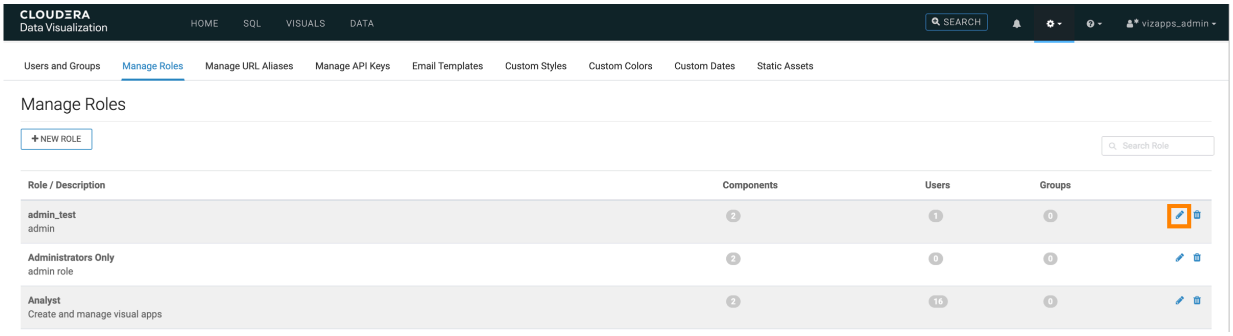
Procedure

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

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



3. In the Manage Roles interface, find the role you wish to edit and click the (edit) icon next to the respective role. You can use the Search Role box to find the role you want to edit.



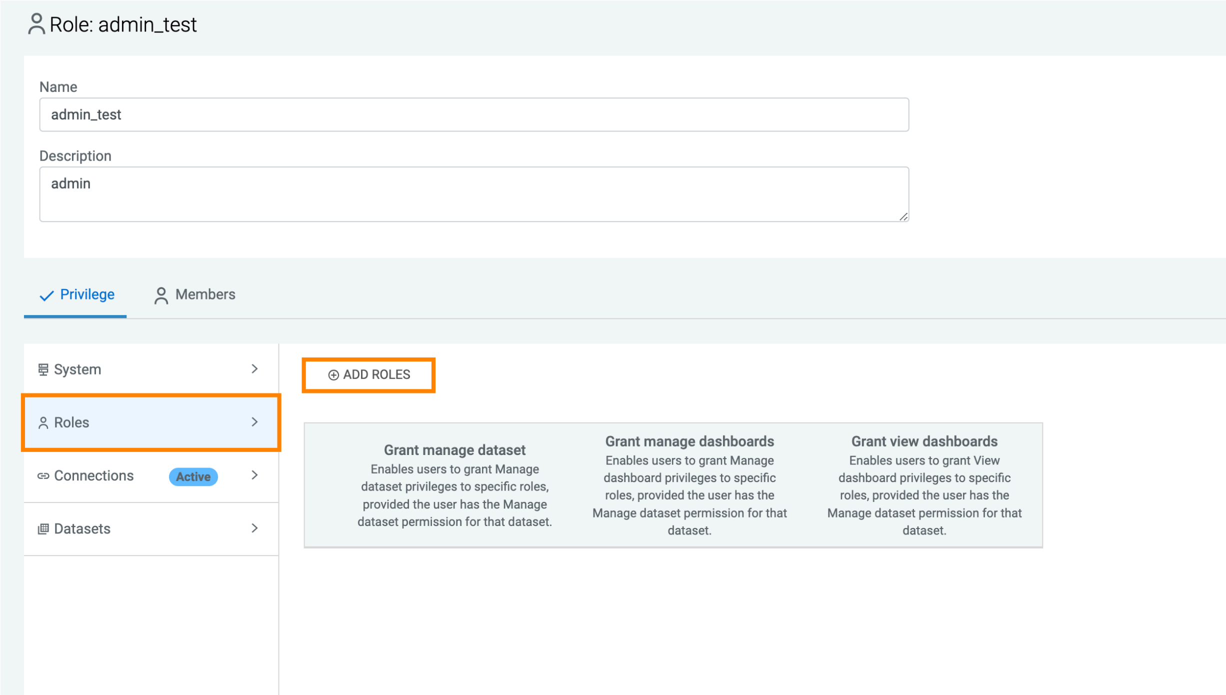
Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

The Role Detail interface is displayed.

4. Switch to the Roles category on the Privilege tab.

5. Add a new role by clicking ADD ROLES.



Grant manage dataset
Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

Grant manage dashboards
Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

Grant view dashboards
Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

The Add Role Privilege modal window appears.

6. Select the required role from the Roles drop-down list and add it.

   When the role is added, by default, all possible privileges are marked for it.

   You can repeat this step to add more roles to the list, if needed.

   You can remove a role from the list by clicking the Delete icon.

7. Select the checkboxes for the actions that you want to permit for the role(s) you have added.

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

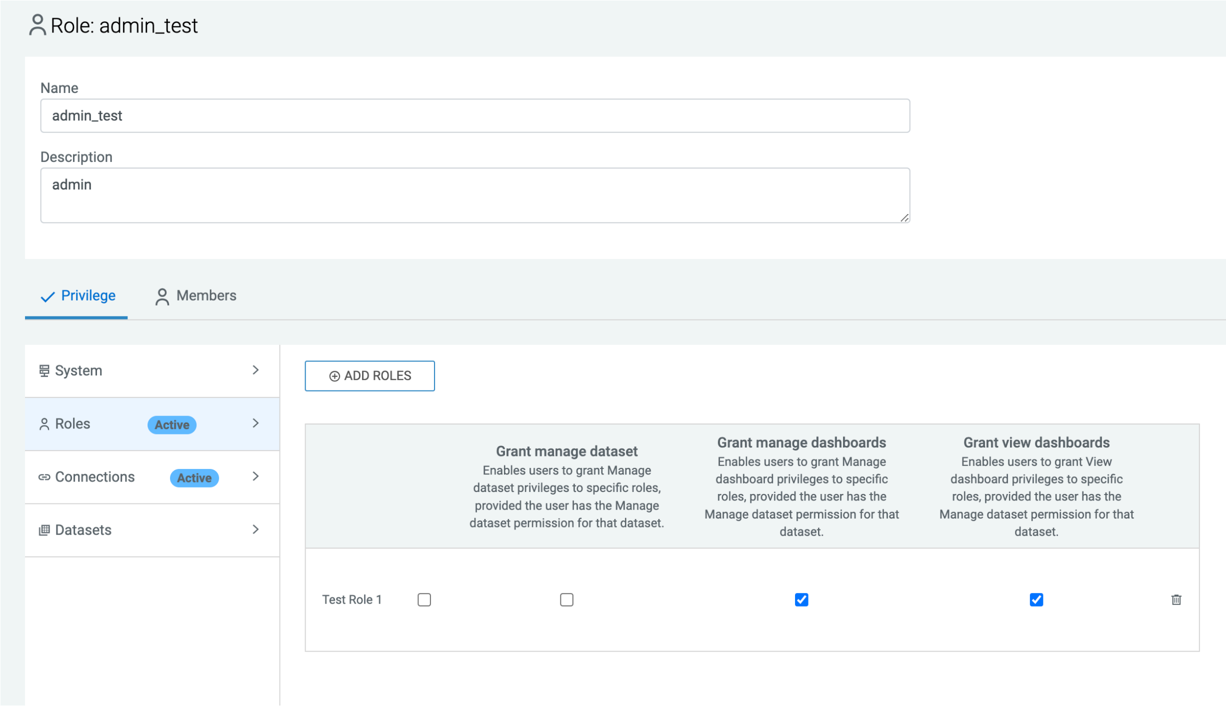
Note:

Privilege dependency information:

The Grant manage dashboards and Grant view dashboards permissions are mandatory if the privilege includes the Grant manage dataset permission and cannot be removed. The checkboxes for these permissions are pre-filled and fixed.

If Grant manage dataset is deselected, Grant manage dashboards becomes optional and can also be deselected. If Grant manage dashboards is deselected, Grant view dashboards becomes optional and can also be deselected.

8. After adding roles and selecting the appropriate role privileges, click APPLY CHANGES.



Role: admin_test

Name

admin_test

Description

admin

		Grant manage dataset Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	Grant manage dashboards Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	Grant view dashboards Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	
Test Role 1	□	□	☑	☑	

Results

- The members assigned to the selected role 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. For example, Test Role 1 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 are integral components of the Role-Based Access Control (RBAC) system in Cloudera Data Visualizationn. These privileges can be configured uniformly across multiple connections or customized for each connection, based on specific business requirements.

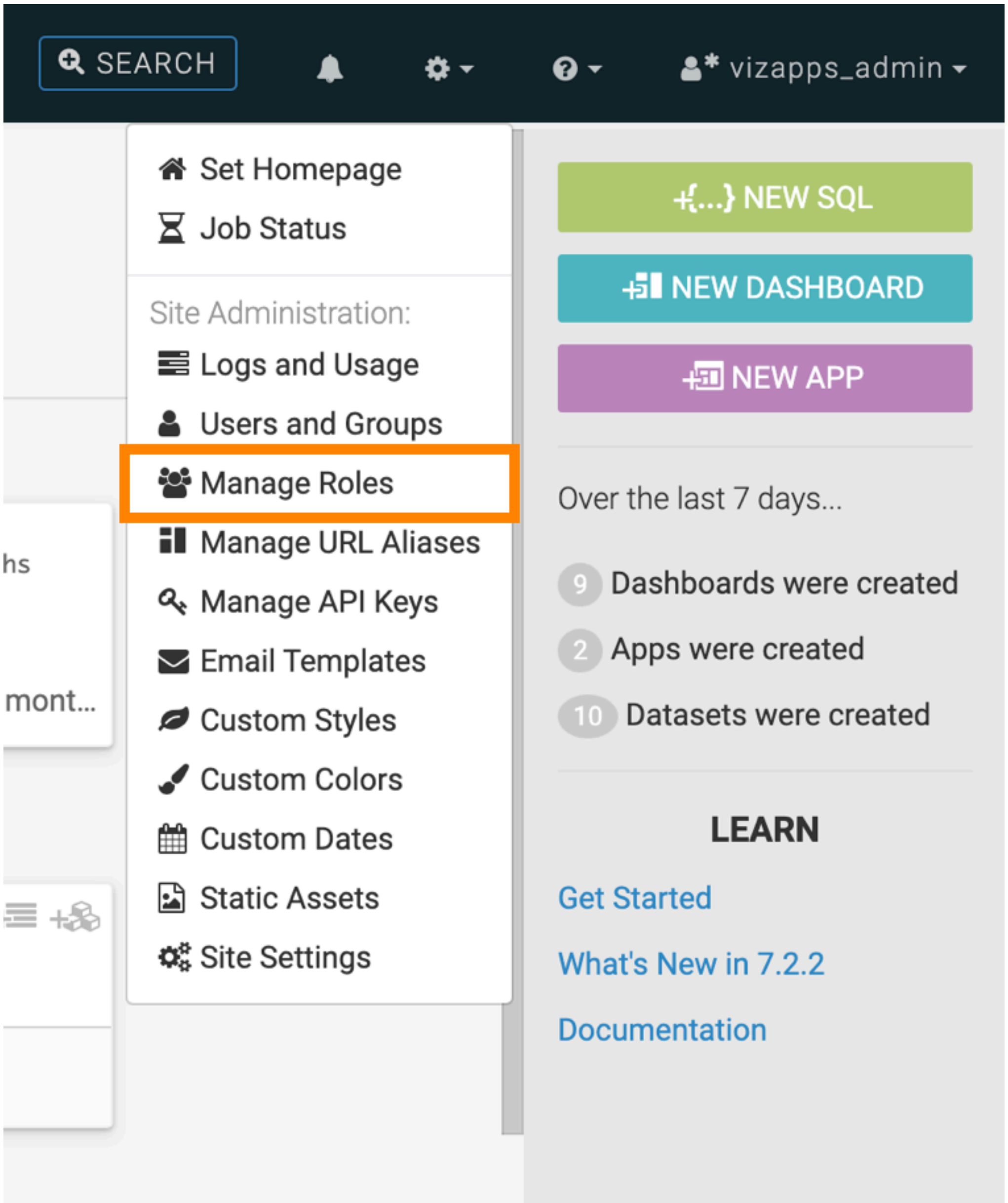
About this task

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

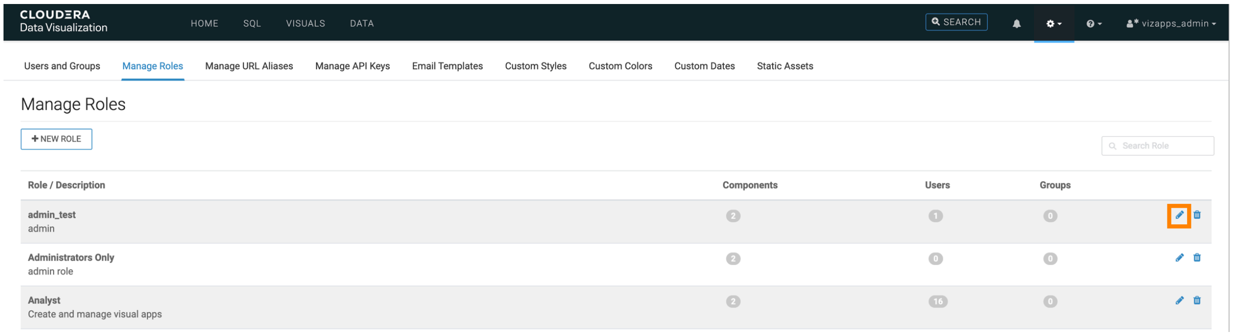
Procedure

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

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



3. In the Manage Roles interface, find the role you wish to edit and click the (edit) icon next to the respective role. You can use the Search Role box to find the role you want to edit.



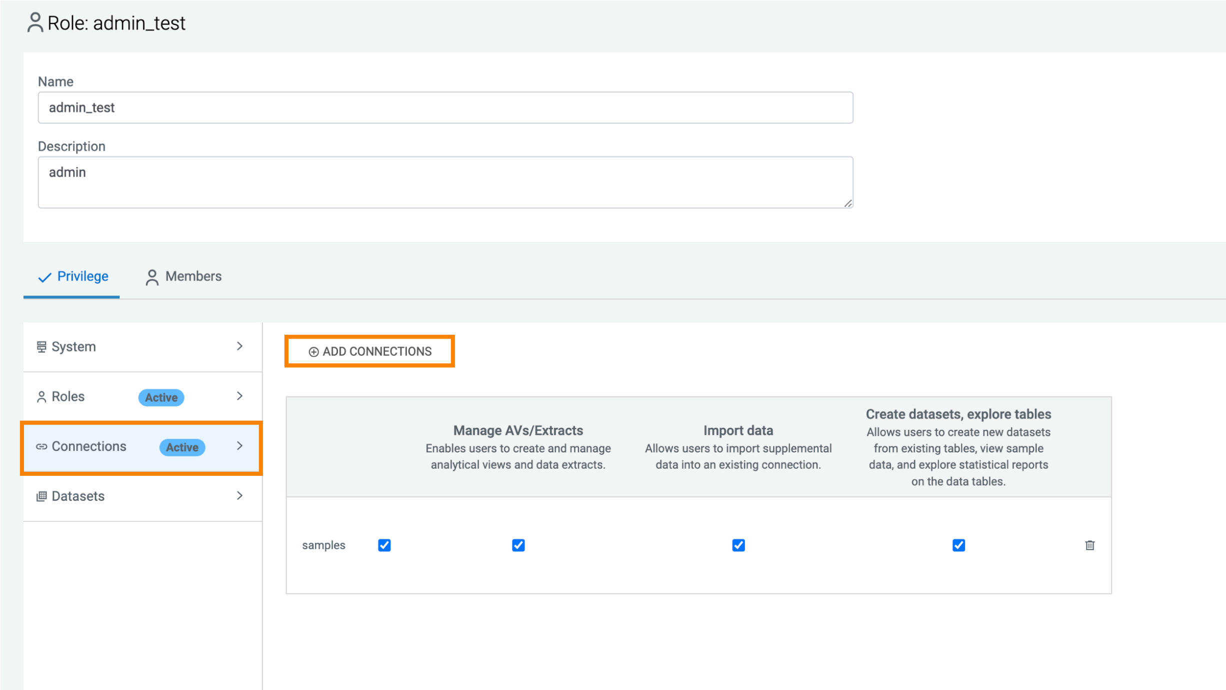
Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

The Role Detail interface is displayed.

4. Switch to the Connections category on the Privilege tab.

5. Add a new connection by clicking ADD CONNECTIONS.



Name: admin_test

Description: admin

	Manage AVs/Extracts Enables users to create and manage analytical views and data extracts.	Import data Allows users to import supplemental data into an existing connection.	Create datasets, explore tables Allows users to create new datasets from existing tables, view sample data, and explore statistical reports on the data tables.	
samples ☑	☑	☑	☑	🗑

   The Add Data connection Privilege modal window appears.

6. From the Connection(s) drop-down menu, select either All connections or one of the individual connections.

   When the connection is added, by default, all possible privileges are marked for it.

   You can repeat this step to include additional connections if necessary.

   You can remove a connection from the list by clicking the Delete icon.

7. Select the checkboxes for the actions that you want to permit for the connection(s) you have added.

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

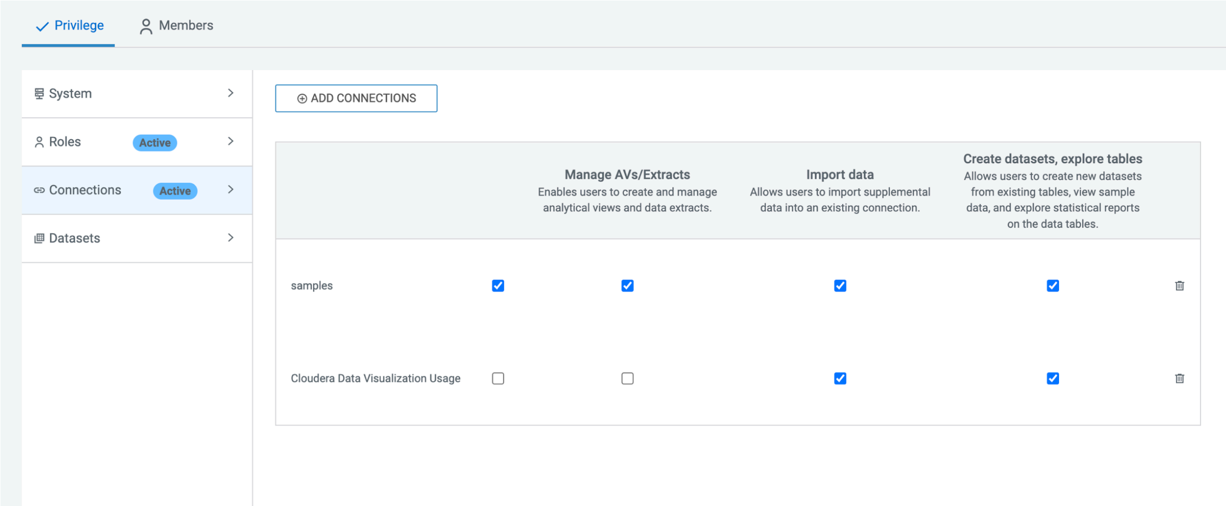
   Note:

   Privilege dependency information:

   Manage AVs/Extracts and Import data are independent privileges, both including the Create datasets, explore tables permission. The Create datasets, explore tables is mandatory if the privilege contains the Manage AVs/Extracts or Import data Connections permission and cannot be removed. The checkboxes for these are pre-filled in and fixed.

   If Manage AVs/Extracts is deselected, Create datasets, explore tables becomes optional and can also be deselected. Similarly, if Import data is deselected, it removes any connection-level access components, Create datasets, explore tables becomes optional and can also be deselected.

8. After adding roles and selecting the appropriate role privileges, click APPLY CHANGES.



		Manage AVs/Extracts Enables users to create and manage analytical views and data extracts.	Import data Allows users to import supplemental data into an existing connection.	Create datasets, explore tables Allows users to create new datasets from existing tables, view sample data, and explore statistical reports on the data tables.	
samples	☑	☑	☑	☑	🗑
Cloudera Data Visualization Usage	□	□	☑	☑	🗑

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 are integral components of the Role-Based Access Control (RBAC) system in Cloudera Data Visualization. These privileges enable fine-grained control over access to datasets, catering to specific business needs. They can be applied uniformly across multiple datasets or customized individually for each dataset.

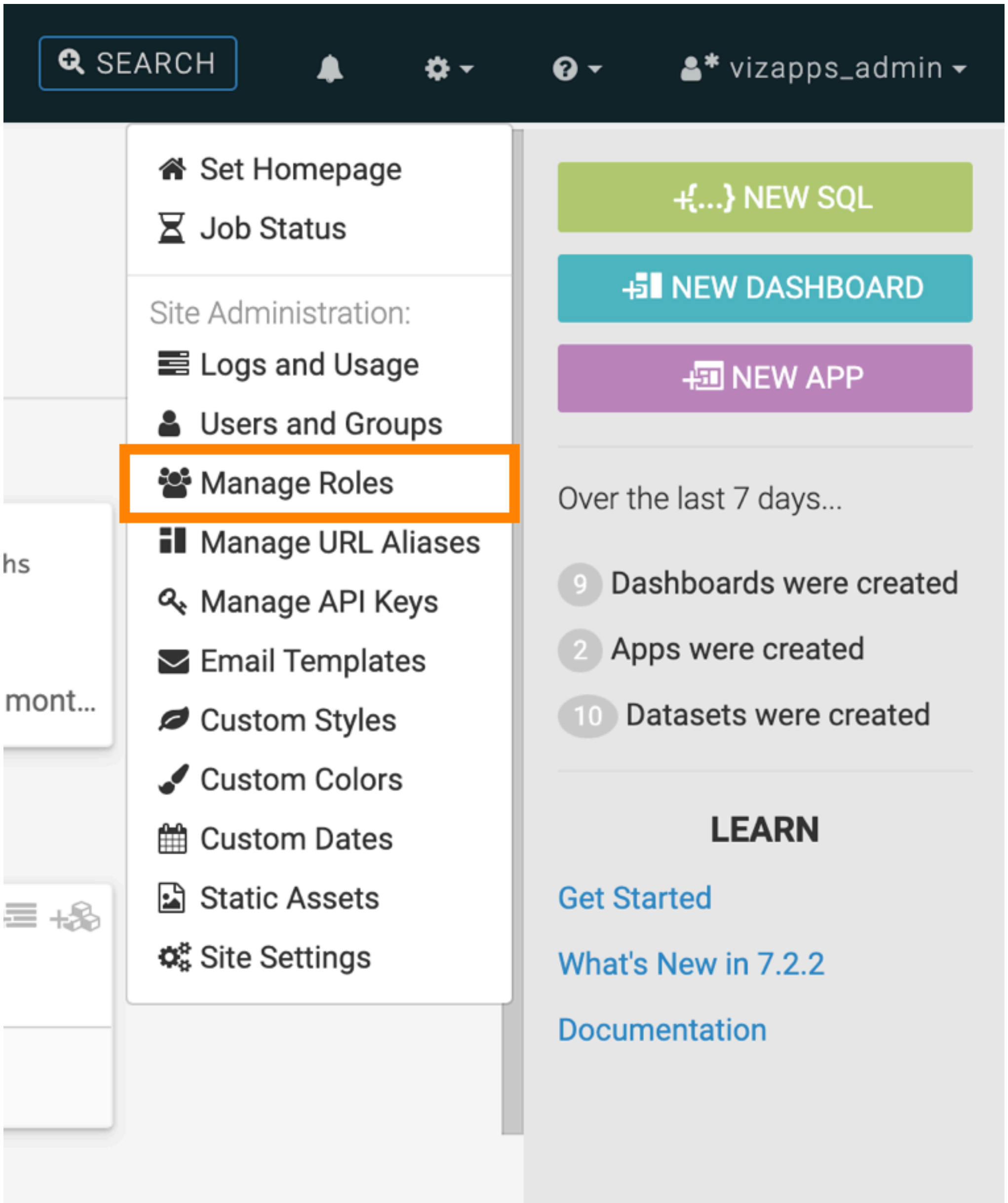
About this task

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

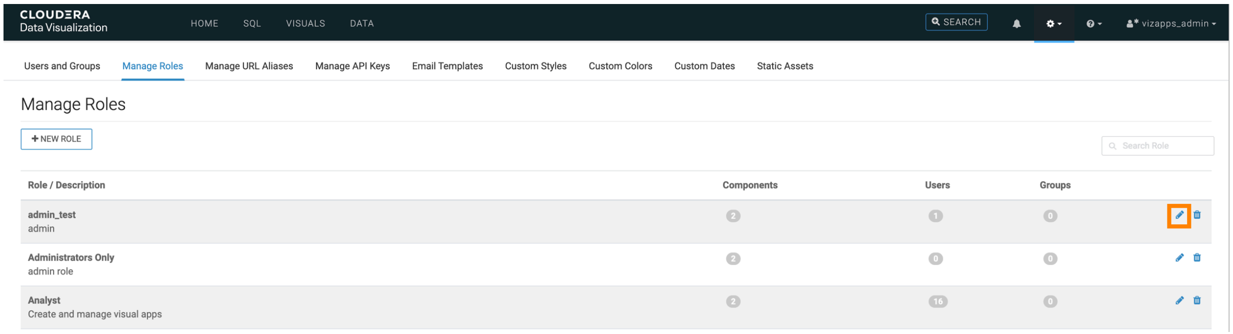
Procedure

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

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



3. In the Manage Roles interface, find the role you wish to edit and click the (edit) icon next to the respective role. You can use the Search Role box to find the role you want to edit.



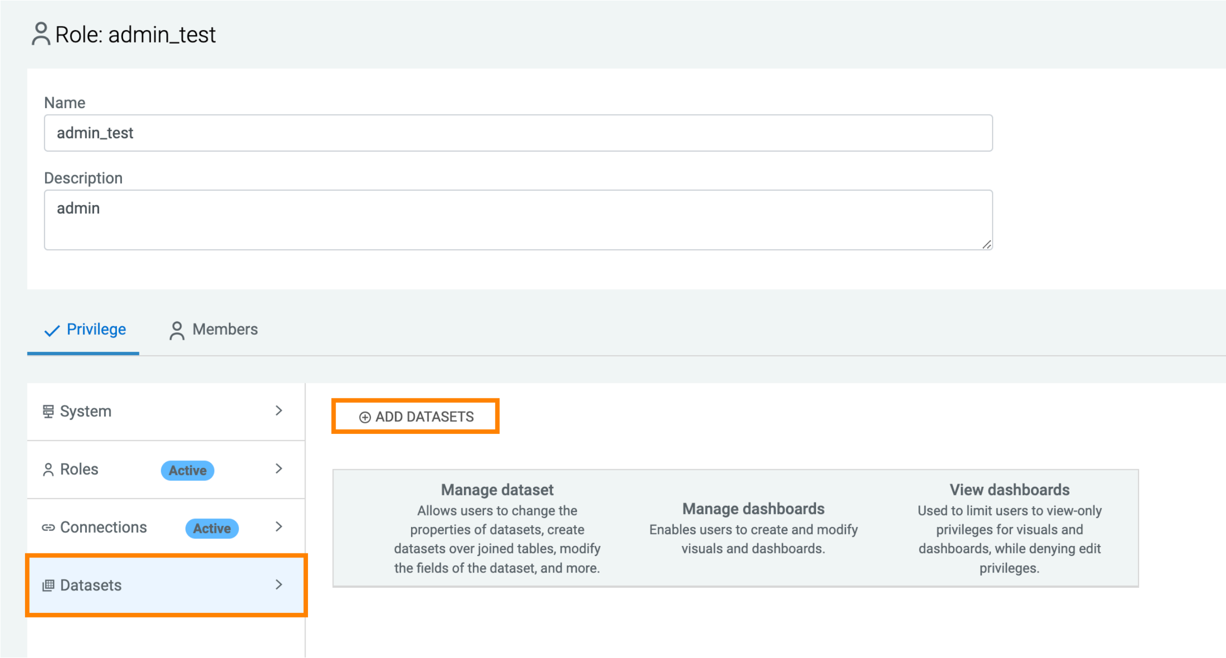
Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

The Role Detail interface is displayed.

4. Switch to the Datasets category on the Privilege tab.

5. Add a new dataset privilege by clicking ADD DATASETS.



Role: admin_test

Name: admin_test

Description: admin

Manage dataset	Manage dashboards	View dashboards
Allows users to change the properties of datasets, create datasets over joined tables, modify the fields of the dataset, and more.	Enables users to create and modify visuals and dashboards.	Used to limit users to view-only privileges for visuals and dashboards, while denying edit privileges.

The Add Dataset Privilege modal window appears.

6. From the Connection(s) drop-down menu, select either All connections or one of the individual connections.
7. From the Datasets(s) drop-down menu, select either All datasets or specific datasets.

   When the dataset is added, by default, all possible privileges are marked for it.

   You can repeat this step to include additional connections if necessary.

   You can remove a connection from the list by clicking the Delete icon.
8. Select the checkboxes for the actions that you want to permit for the connection(s) you have added.

   - Manage dataset
   - Manage dashboards
   - View dashboards

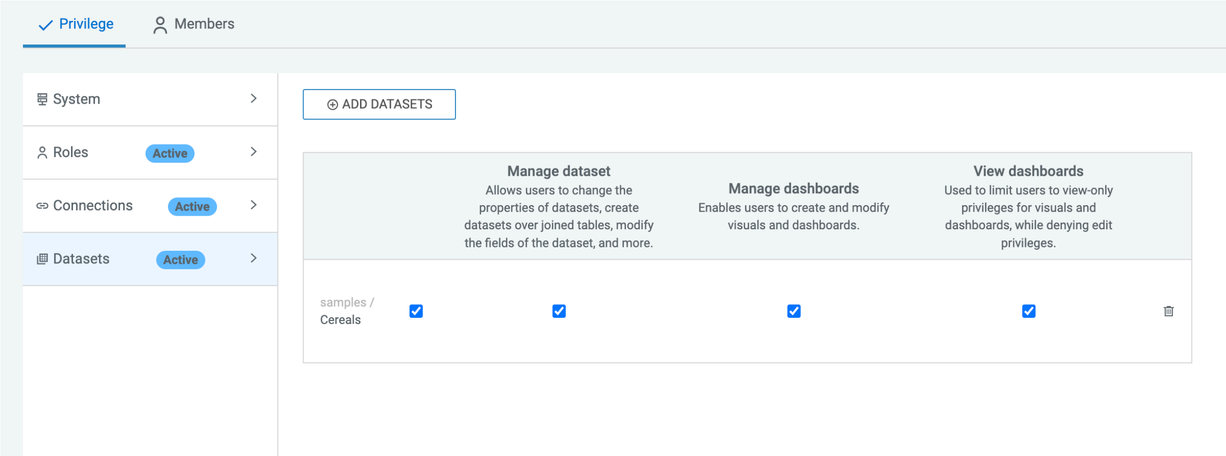
Note:

Privilege dependency information:

The Manage dashboards and View dashboards permissions are mandatory if the privilege includes the Manage dataset permission and cannot be removed. The checkboxes for these permissions are pre-filled and fixed.

If Manage dataset is deselected, Manage dashboards becomes optional and can also be deselected. If Manage dashboards is deselected, View dashboards becomes optional and can also be deselected.

9. After adding roles and selecting the appropriate role privileges, click APPLY CHANGES.



		Manage dataset Allows users to change the properties of datasets, create datasets over joined tables, modify the fields of the dataset, and more.	Manage dashboards Enables users to create and modify visuals and dashboards.	View dashboards Used to limit users to view-only privileges for visuals and dashboards, while denying edit privileges.	
samples / Cereals	☑	☑	☑	☑	

Results

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

Related Information

RBAC permissions

Editing role assignments

About this task

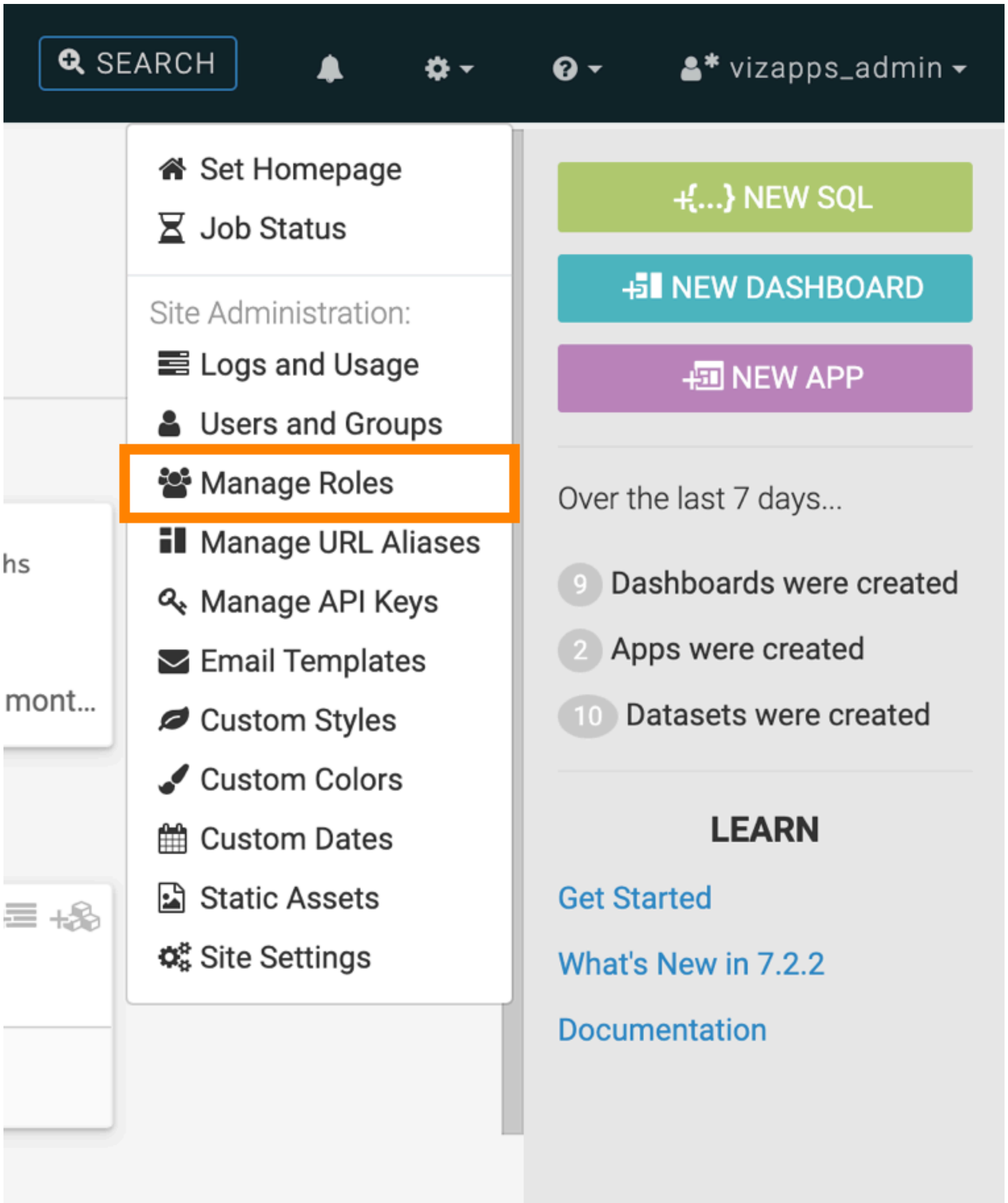
The following steps demonstrate how to edit role assignments for a specific role.

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

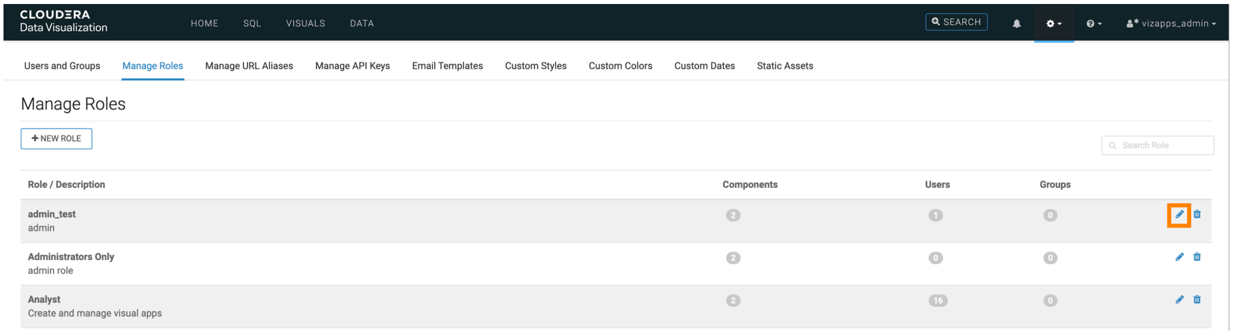
Procedure

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

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



3. In the Manage Roles interface, find the role you wish to edit and click the (edit) icon next to the respective role. You can use the Search Role box to find the role you want to edit.



Manage Roles

Role / Description	Components	Users	Groups
admin_test admin	2	1	0
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

The Role Detail interface is displayed.

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

4. Click the Members tab and proceed to editing 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

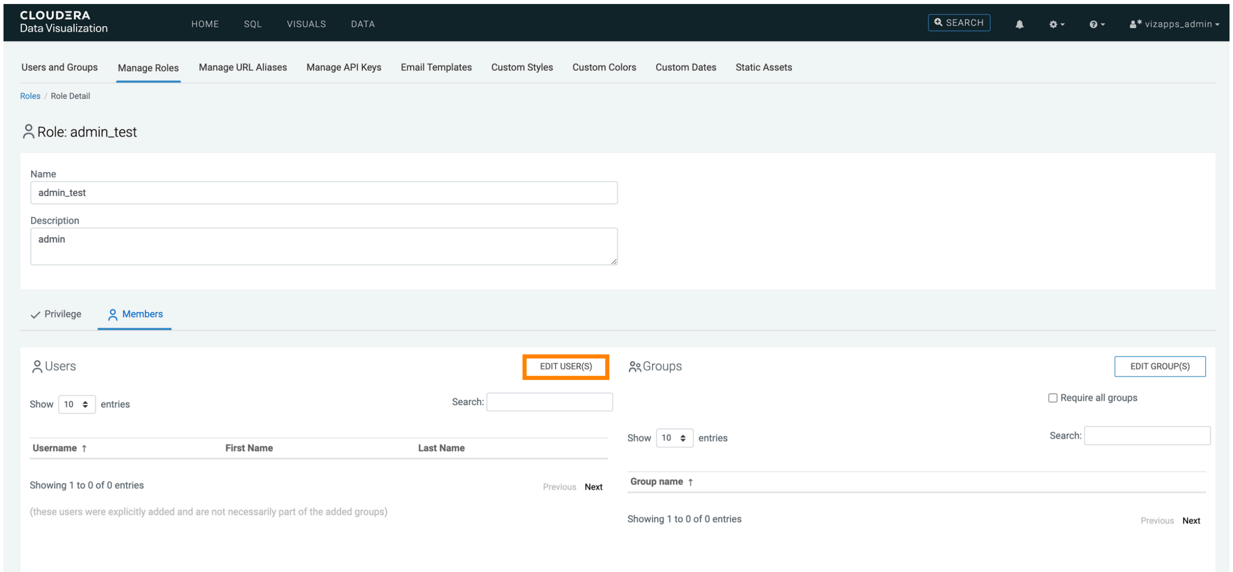
About this task

The following steps demonstrate how to add users to a role.

Procedure

1. Navigate to the Members tab of the Role Detail interface.

2. Click EDIT USER(S).



Role: admin_test

Name: admin_test

Description: admin

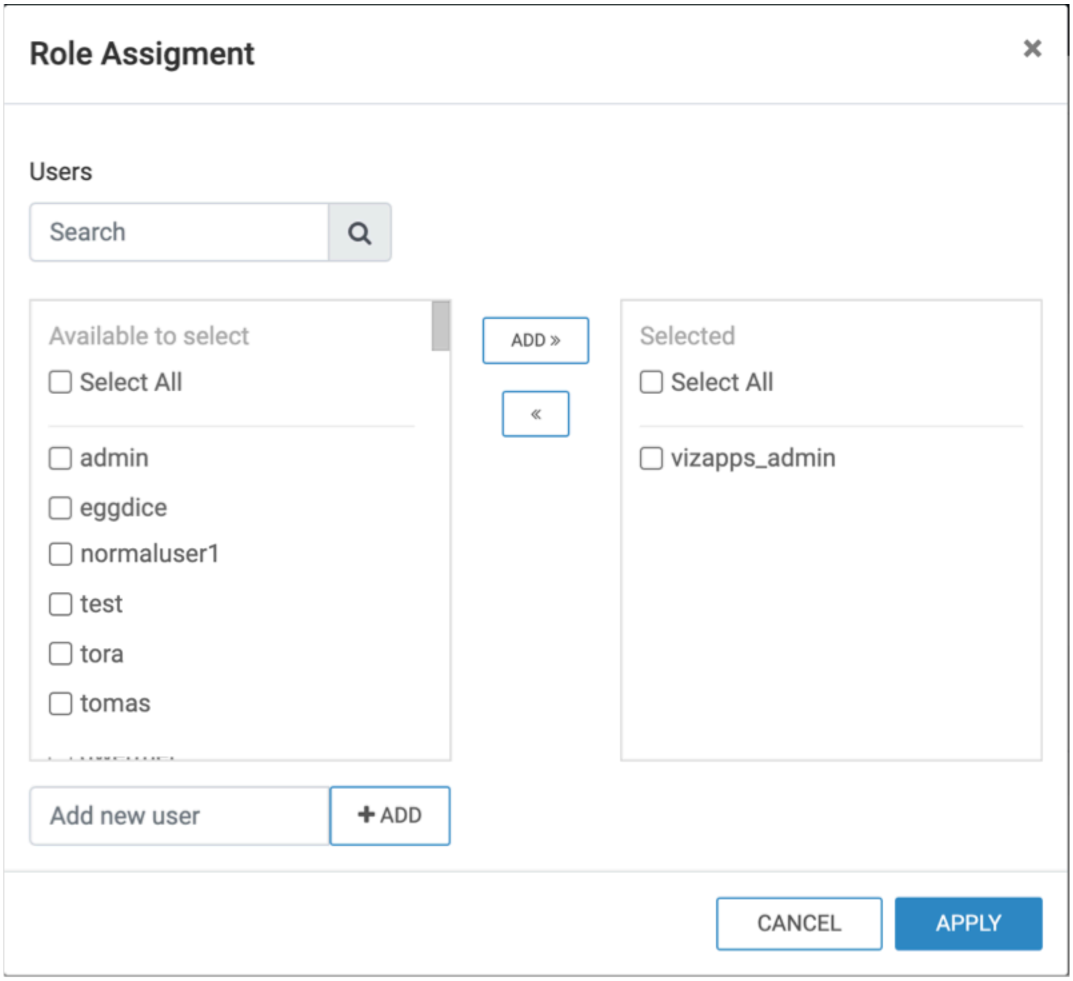
☐ Require all groups

Showing 1 to 0 of 0 entries

(these users were explicitly added and are not necessarily part of the added groups)

Showing 1 to 0 of 0 entries

The Role Assignment modal window is displayed.



Available to select

☐ Select All

☐ admin
☐ eggdice
☐ normaluser1
☐ test
☐ tora
☐ tomas

Selected

☐ Select All

☐ vizapps_admin

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

   - Search

     If you have a long list of users in the Users section, use the Search box to find specific 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 Users 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 Users, mark Select All 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)

     The Role Assignment modal supports adding usernames that are not stored locally. For example, you can add known usernames available through LDAP authentication using this method.

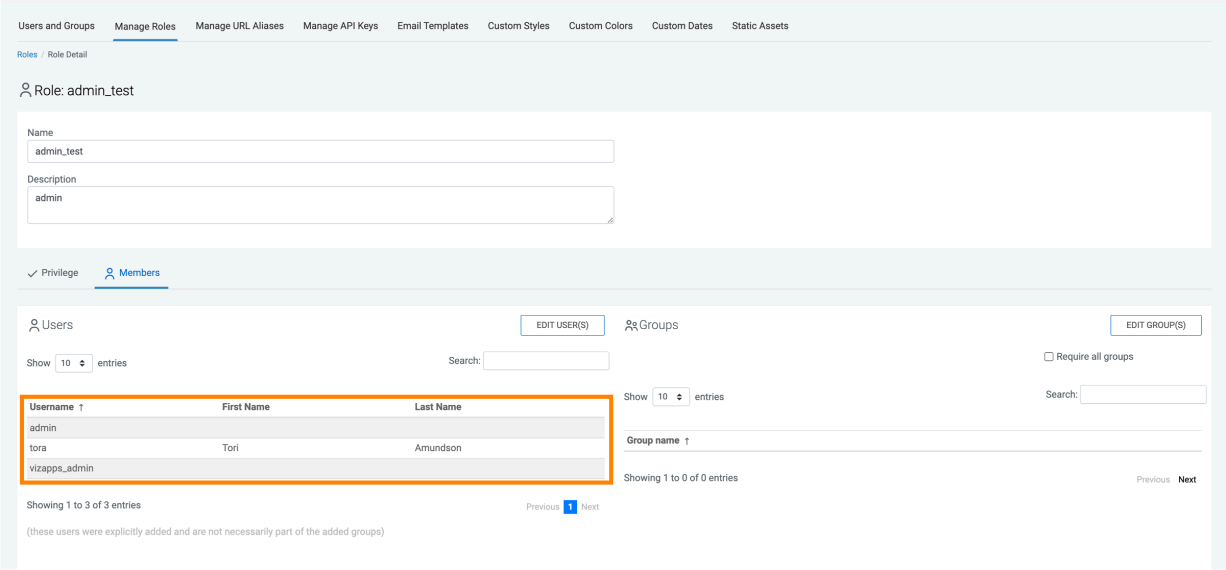
     Enter the new user name and click ADD>> to add externally defined users. After the new user name appears in the Users section, select it and click ADD>> to move the new user to the right side of the modal window.

     When you are ready, click APPLY.
   - Remove

     To remove users from the Users list, select them from the right side panel and click <<.

     When you are ready, click APPLY.
4. Click APPLY CHANGES.

   The Users list is updated.



Role: admin_test

Name: admin_test

Description: admin

Users

Show 10 entries   Search:

Username ↑	First Name	Last Name
admin		
tora	Tori	Amundson
vizapps_admin		

Showing 1 to 3 of 3 entries

(these users were explicitly added and are not necessarily part of the added groups)

Groups

□ Require all groups

Show 10 entries   Search:

Group name ↑

Showing 1 to 0 of 0 entries

Assigning roles to user groups

About this task

The following steps demonstrate how to add user groups to a role.

Procedure

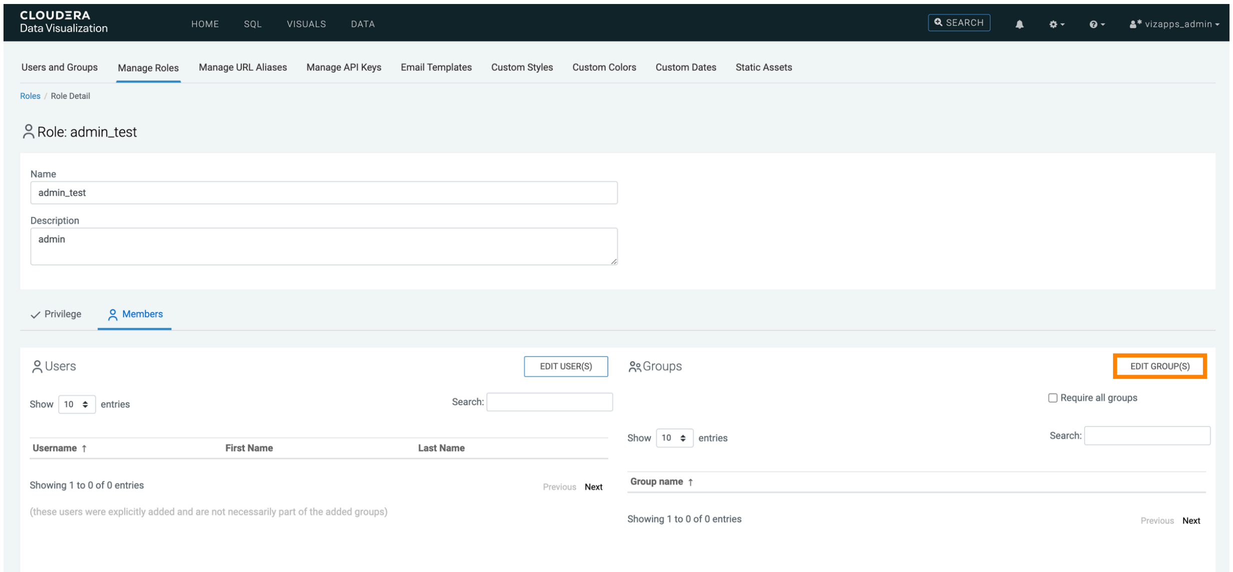
1. Navigate to the Members tab of the Role Detail interface.

The Require all groups option ensures that only members of ALL groups listed in the role membership fields have the role's defined access. It determines whether members must belong to all listed groups or any one of them to access the role's privileges.

Note:

- If Require all groups is checked, only users belonging to both groups will receive the role's privileges.
- Exceptions to group membership include explicitly named users and users imported through Ranger groups.

2. Click EDIT GROUP(S).



Role: admin_test

Name: admin_test

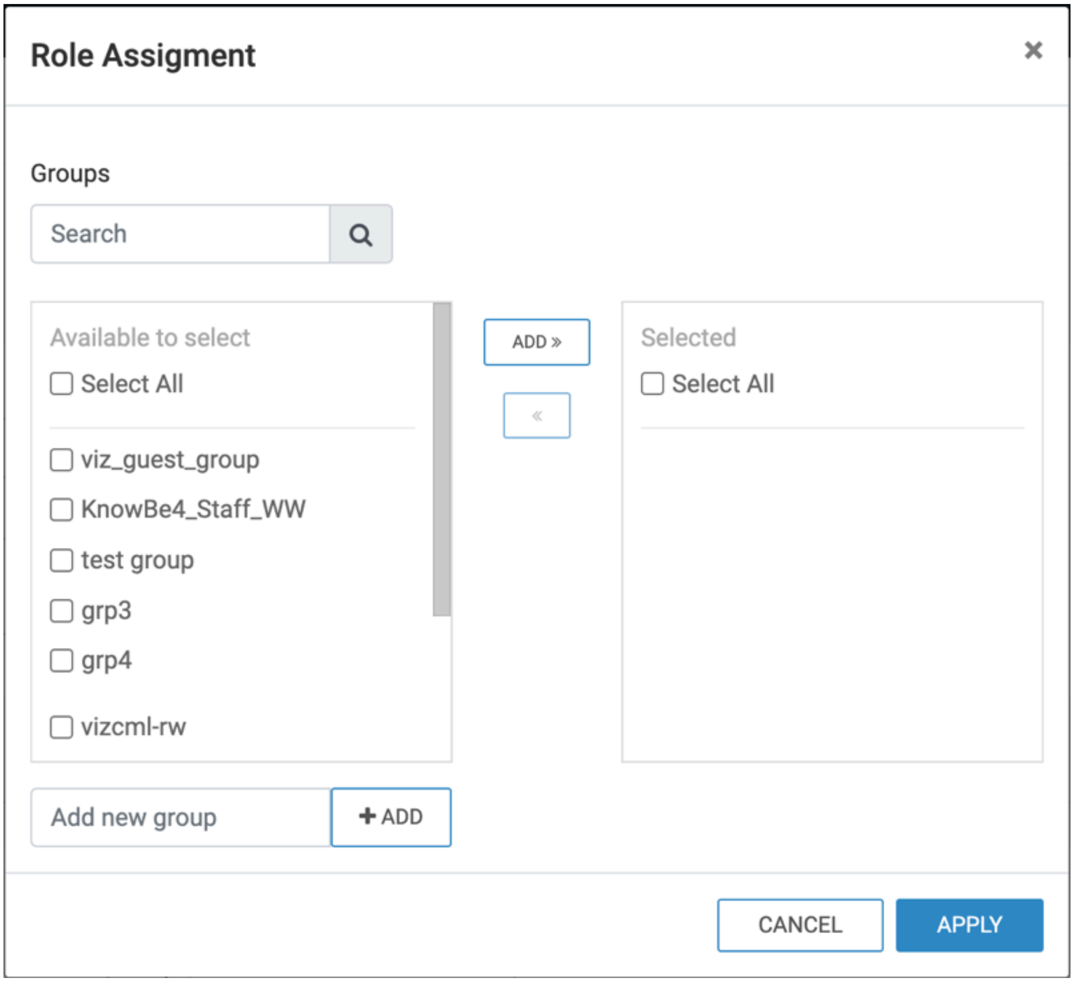
Description: admin

Showing 1 to 0 of 0 entries

(these users were explicitly added and are not necessarily part of the added groups)

Showing 1 to 0 of 0 entries

The Role Assignment modal window is displayed.



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

   - Search

     If you have a long list of groups in the Groups section, use the Search box to find specific 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 Groups 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 Groups, mark Select All 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)

     The Role Assignment modal 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 using this method.

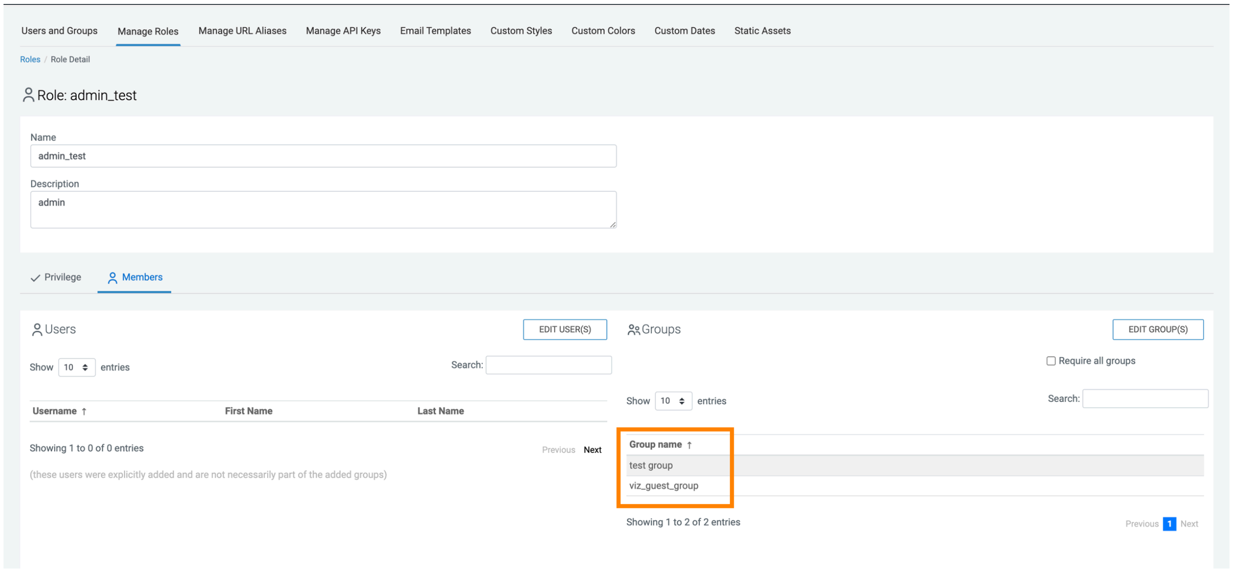
     Enter the new group name and click ADD>>. After the new group name appears in the Members section, select it and click ADD>> to move the new group to the right side of the modal window.

     When you are ready, click APPLY.
   - Remove

     To remove users from the Members list, select them on the right side panel and click <<.

     When you are ready, click APPLY.
4. Click APPLY CHANGES.

   The Users list is updated.



Role: admin_test

Name: admin_test

Description: admin

Users

Show 10 entries Search:

Username ↑	First Name	Last Name

Showing 1 to 0 of 0 entries

(these users were explicitly added and are not necessarily part of the added groups)

Groups

□ Require all groups

Show 10 entries Search:

Group name ↑
test group
viz_guest_group

Showing 1 to 2 of 2 entries

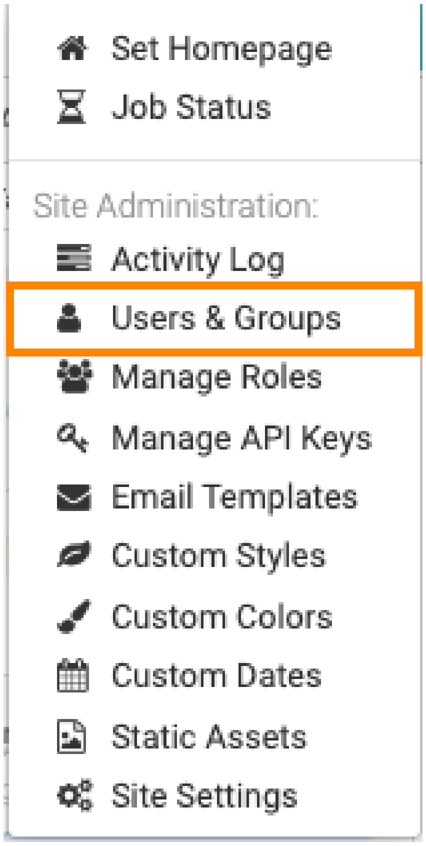
Assigning multiple roles to multiple users

About this task

The following steps demonstrate how to add multiple users to existing roles in the Users & Groups interface of Cloudera Data Visualization.

Procedure

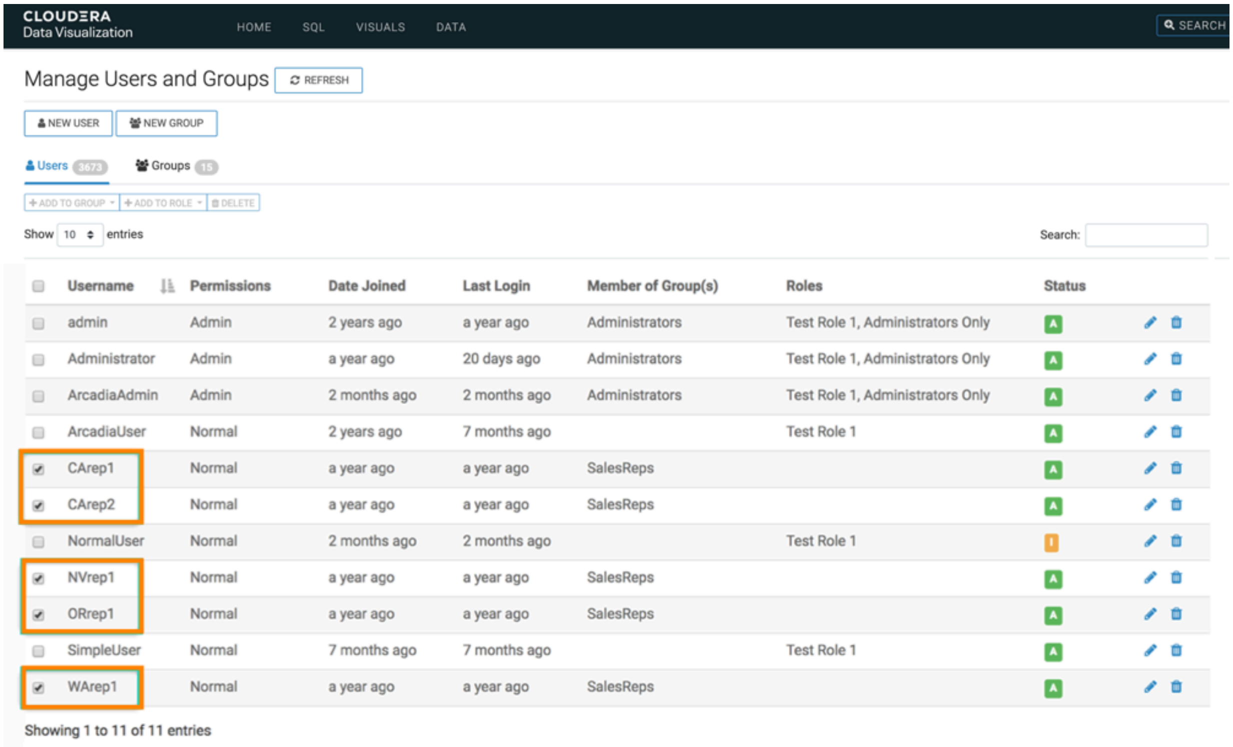
1. Click the Gear icon on the main navigation bar.
2. In the drop-down menu, select Users & Groups.



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

3. Choose the users you wish to assign to roles by selecting their respective checkboxes.

   You can use the Search box to find the users you want to edit.

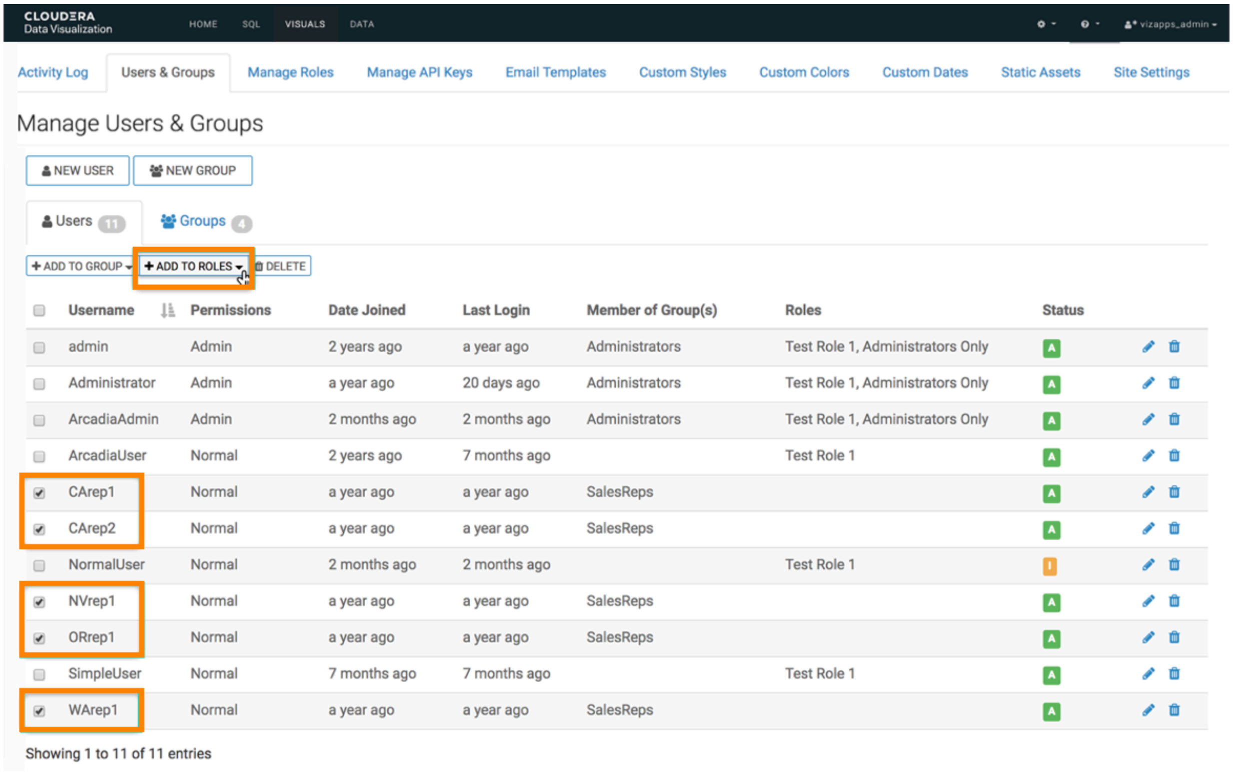


Manage Users and Groups

☐	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
☑	CArep1	Normal	a year ago	a year ago	SalesReps		A
☑	CArep2	Normal	a year ago	a year ago	SalesReps		A
☐	NormalUser	Normal	2 months ago	2 months ago		Test Role 1	!
☑	NVrep1	Normal	a year ago	a year ago	SalesReps		A
☑	ORrep1	Normal	a year ago	a year ago	SalesReps		A
☐	SimpleUser	Normal	7 months ago	7 months ago		Test Role 1	A
☑	WArep1	Normal	a year ago	a year ago	SalesReps		A

Showing 1 to 11 of 11 entries

4. Click ADD TO ROLE.



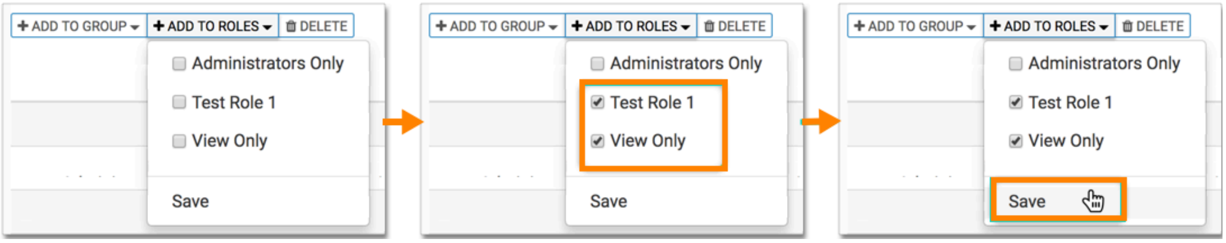
Manage Users & Groups

☐	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
☑	CArep1	Normal	a year ago	a year ago	SalesReps		A
☑	CArep2	Normal	a year ago	a year ago	SalesReps		A
☐	NormalUser	Normal	2 months ago	2 months ago		Test Role 1	!
☑	NVrep1	Normal	a year ago	a year ago	SalesReps		A
☑	ORrep1	Normal	a year ago	a year ago	SalesReps		A
☐	SimpleUser	Normal	7 months ago	7 months ago		Test Role 1	A
☑	WArep1	Normal	a year ago	a year ago	SalesReps		A

Showing 1 to 11 of 11 entries

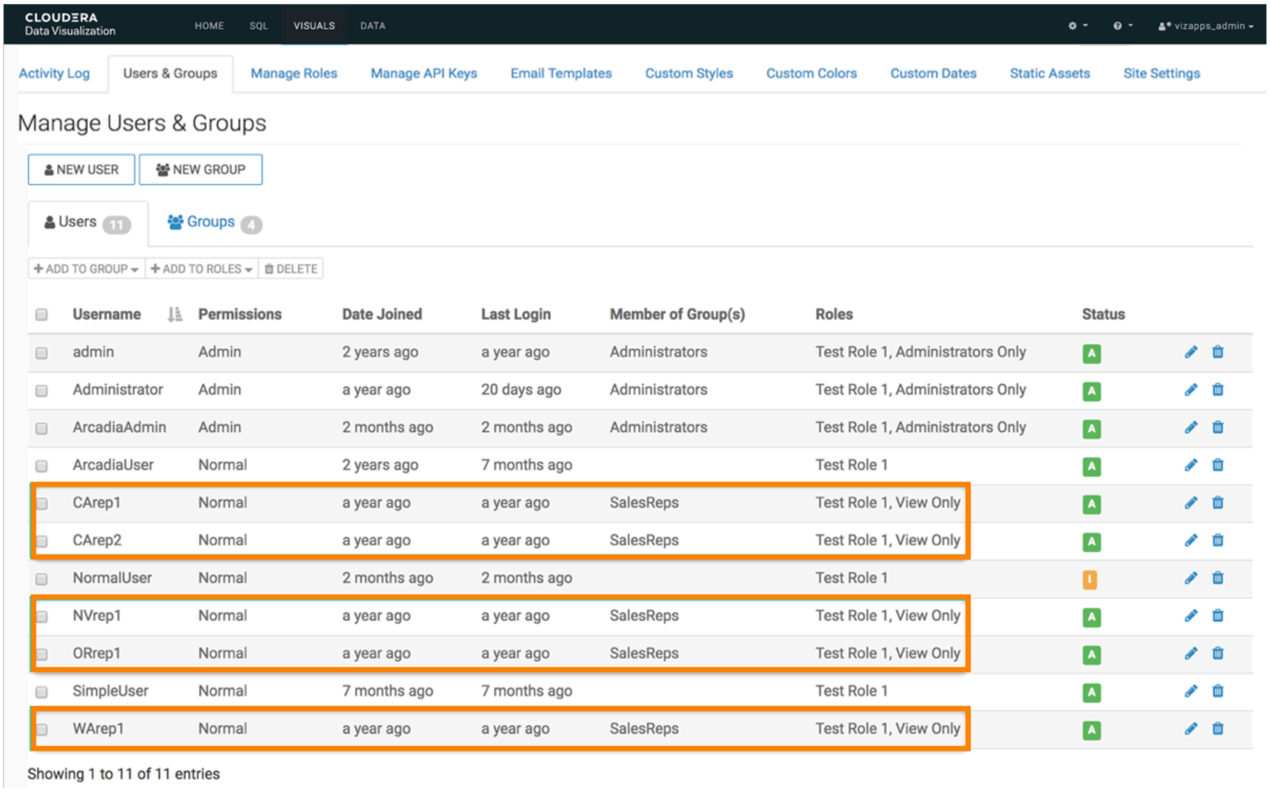
A drop-down menu is displayed, showing a list of available roles.

5. Check the checkboxes next to the roles you want to assign to the selected users and click Save.



Results

You can see the changes to the information in the Users & Groups interface.



Manage Users & Groups

□	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
□	CArep1	Normal	a year ago	a year ago	SalesReps	Test Role 1, View Only	A
□	CArep2	Normal	a year ago	a year ago	SalesReps	Test Role 1, View Only	A
□	NormalUser	Normal	2 months ago	2 months ago		Test Role 1	I
□	NVrep1	Normal	a year ago	a year ago	SalesReps	Test Role 1, View Only	A
□	ORrep1	Normal	a year ago	a year ago	SalesReps	Test Role 1, View Only	A
□	SimpleUser	Normal	7 months ago	7 months ago		Test Role 1	A
□	WArep1	Normal	a year ago	a year ago	SalesReps	Test Role 1, View Only	A

Showing 1 to 11 of 11 entries

Deleting roles

Deleting a role in the role-based access control (RBAC) system is a straightforward process that helps maintain access control efficiency.

About this task

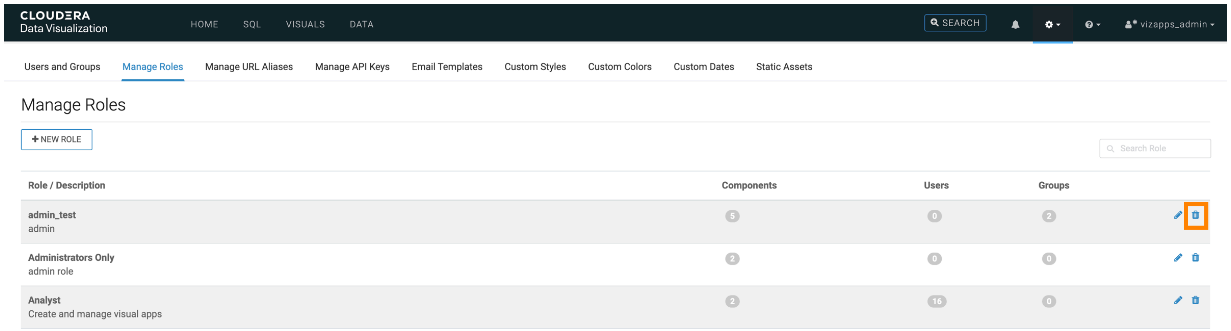
Note: This feature is only available to users with Manage roles and users privileges.

The following steps demonstrate how to add or change privileges defined for a specific role.

Procedure

1. In the Manage Roles interface, identify the role you wish to delete from the list of existing roles.

   You can use the Search Role box to find the role you want to delete.



Role / Description	Components	Users	Groups
admin_test admin	5	0	2
Administrators Only admin role	2	0	0
Analyst Create and manage visual apps	2	16	0

Note: Ensure that the role you are deleting is no longer required and does not impact any ongoing access control configurations.

2. Click the Trash can icon located next to the role.

   A Delete Confirmation modal window will appear, requesting confirmation for the deletion.

3. Click DELETE.

Related Information

Creating new roles