

Security

Date published: 2020-10-30

Date modified: 2024-10-30

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

Security model.....	4
Role-based access control.....	4
Permissions.....	5
Role privileges.....	6
All groups requirement.....	8
RBAC setup for dataset publishing.....	9

Security model

Security in Cloudera Data Visualization means robust authentication and granular permission control. This comprehensive security approach involves various components, including role-based access control, which enables you to have precise control over data and feature access.

Administrative configuration

As an administrator, you have the authority to configure roles, privileges, and members, providing a foundation for robust security controls. For more information, see *Working with user roles*.

Role-based access control (RBAC)

You can manage privileges and members of a role with the help of RBAC. Utilize RBAC to effectively manage privileges and members associated with specific roles, ensuring a tailored access control environment. For more information, see the *Role-based access control* documentation.

User roles for dataset control

You can leverage user roles to facilitate dataset creators and managers in sharing curated datasets within their organization. This includes the implementation of three levels of access control. For more information, see *Publishing datasets*.

Access control for defined data segments

You can restrict a user's access to defined data segments, ensuring a granular control mechanism. For more information, see *Setting segments*.

Advanced configuration options

You can further enhance security by configuring LDAP authentication. For more information, see *Enabling LDAP authentication*.

Related Information

[Role-based access control](#)

[Working with user roles](#)

[Publishing datasets](#)

[Setting segments](#)

[Enabling LDAP authentication](#)

Role-based access control

Role-Based Access Control (RBAC) is a functional system in Cloudera Data Visualization that helps to manage user access rights. By setting permissions and privileges, RBAC ensures that only authorized users can access specific functionalities, defined by their roles in the system.



Note: This feature is only available to users with administrative privileges.

RBAC provides administrators with precise control over data and feature access, based on different user roles. Roles come with distinct sets of rights, creating a structured and secure access system. For more information, see *Role privileges*.

Components of RBAC:

Permissions

Permissions regulate access to visuals, datasets, data connections, and system-level functions. They fall into four categories: system, role, connection, and dataset. For more information, see *Permissions*.

Privileges

Privileges are sets of permissions of a specific type, tied to associated components. For example, a privilege may contain the permission to View visuals and dashboards on the component specifier Connection default / All datasets.

Members

Members are a users and user groups assigned to a particular role.

Roles

Roles serve as collections of privileges, each with its associated members possessing these privileges.

Related Information

[Role privileges](#)

Permissions

Permissions define access to visuals, datasets, data connections, and system-level functions. There are four categories of permissions: system, role, connection, and dataset.

When defining privileges, the following default permissions exist at each level:

System-level permissions: site-level capabilities	Role-level permissions: defined separately for each role	Connection-level permissions: defined separately for each data connection	Dataset-level permissions: defined separately for each dataset
<ul style="list-style-type: none"> • Create workspaces • View roles and users • Manage roles and users • Manage site settings • Manage custom styles • Manage jobs, email templates • Manage data connections • View activity logs • Additional system privileges 	<ul style="list-style-type: none"> • Grant manage dataset • Grant manage dashboards • Grant view dashboards 	<ul style="list-style-type: none"> • Manage analytical views • Import data • Create datasets, explore tables 	<ul style="list-style-type: none"> • Manage dataset • Manage dashboards • View dashboards

DATA interface interpretations

To connect the permissions to what options are available in the DATA interface of Cloudera Data Visualization, consider the following:

1. System-level Manage data connections permission

Necessary to access the NEW CONNECTION button for creating new connections and the Pencil icon for editing existing connections.

2. Dataset-level View visuals and dashboards permission

Required for a specific dataset to appear in the list of datasets for the selected connection.

3. Connection-level Create datasets, explore tables permission

Necessary to access the:

- NEW DATASET button over the list of datasets
- Connection Explorer tab
- Delete icon on the dataset row

4. Connection-level Manage data connections and dataset-level Manage dataset permissions

Essential for the visibility of the Clear result cache option in the Supplemental menu.

5. System-level Manage styles and settings, connection-level Create datasets, explore tables, and dataset-level Manage dataset and Manage visuals and dashboards permissions

May all be required for the visibility of the Import Visual Artifacts option in the Supplemental menu, depending on the type of import.

6. Dataset-level Manage visuals and dashboards permission

Necessary to access the New Dashboard and New Visual icons on the specified dataset rows.

Title/Table	ID	Tags	Created	Last Updated	Modified By	# Dashboards
Earthquake Data January 2019 main.earthquake_data2019	10		May 03, 2021	10 days ago	juno	22
Cereals main.cereals	378		Aug 01, 2023	15 days ago	vizapps_admin	2
Clone of Restaurant Inspection SF main.restaurant_scores_lives_standard	397		Nov 21, 2023	16 days ago	juno	0
Dataset 1 main.census_pop	396		Nov 15, 2023	16 days ago	ckoncz	1
Clone of Cereals main.cereals	379		Aug 01, 2023	16 days ago	vizapps_admin	0

Role privileges

Privileges are sets of permissions of a particular type and the associated components on which the permissions are granted. Administrators can define role privileges at various levels within Cloudera Data Visualization. This allows precise control over system access for different roles.



Note: This feature is only available to users with administrative privileges.

Privileges for a role may be defined on one of the following levels:

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

The Role Detail interface shows a table matrix of privilege components and specific permissions granted to a role for each component. Each privilege type (system, roles, connections, or datasets) tab shows the relevant permissions.

System

You can see which system-level permissions are enabled.

Users and Groups **Manage Roles** Manage URL Aliases Manage API Keys Email Templates Custom Styles Custom Colors Custom Dates Static Assets

Roles / Role Detail

🔍 Role: Database admin

Name
Database admin

Description
Connection level management and dataset creation

✓ Privilege 👤 Members

System	Active	Privilege														
System	Active	<table border="1"> <thead> <tr> <th>Privilege</th> <th>Enabled</th> </tr> </thead> <tbody> <tr> <td>Create workspaces Allows users to create new workspaces that may be shared among users and user groups.</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>View roles and users Enables users to view users, user groups, and roles.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Manage roles and users Enables users to create users, user groups, and roles.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Manage settings Permits users to manage global site settings.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Manage custom styles Authorizes users to create new styles for dashboards and visuals.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Manage jobs, email templates Enables users to manage scheduled jobs and create templates for email messages.</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Privilege	Enabled	Create workspaces Allows users to create new workspaces that may be shared among users and user groups.	<input checked="" type="checkbox"/>	View roles and users Enables users to view users, user groups, and roles.	<input type="checkbox"/>	Manage roles and users Enables users to create users, user groups, and roles.	<input type="checkbox"/>	Manage settings Permits users to manage global site settings.	<input type="checkbox"/>	Manage custom styles Authorizes users to create new styles for dashboards and visuals.	<input type="checkbox"/>	Manage jobs, email templates Enables users to manage scheduled jobs and create templates for email messages.	<input type="checkbox"/>
Privilege	Enabled															
Create workspaces Allows users to create new workspaces that may be shared among users and user groups.	<input checked="" type="checkbox"/>															
View roles and users Enables users to view users, user groups, and roles.	<input type="checkbox"/>															
Manage roles and users Enables users to create users, user groups, and roles.	<input type="checkbox"/>															
Manage settings Permits users to manage global site settings.	<input type="checkbox"/>															
Manage custom styles Authorizes users to create new styles for dashboards and visuals.	<input type="checkbox"/>															
Manage jobs, email templates Enables users to manage scheduled jobs and create templates for email messages.	<input type="checkbox"/>															
Roles																
Connections	Active															
Datasets	Active															

For more information on System privileges, see [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](#), and [Additional system privilege](#).

Roles

You can see which role-based permissions are enabled.

Users and Groups **Manage Roles** Manage URL Aliases Manage API Keys Email Templates Custom Styles Custom Colors Custom Dates Static Assets

Roles / Role Detail

🔍 Role: Database admin

Name
Database admin

Description
Connection level management and dataset creation

✓ Privilege 👤 Members

⊕ ADD ROLES

System	Active	Privilege								
System	Active	<table border="1"> <thead> <tr> <th>Privilege</th> <th>Enabled</th> </tr> </thead> <tbody> <tr> <td>Grant manage dataset Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Grant manage dashboards Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Grant view dashboards Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Privilege	Enabled	Grant manage dataset Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>	Grant manage dashboards Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>	Grant view dashboards Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>
Privilege	Enabled									
Grant manage dataset Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>									
Grant manage dashboards Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>									
Grant view dashboards Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.	<input type="checkbox"/>									
Roles										
Connections	Active									
Datasets	Active									

Actions available:

- **ADD ROLES** to add a new role privilege

For more information on Role privileges, see [Grant manage dataset](#), [Grant manage dashboards](#), and [Grant view dashboards](#).

Connections

You can see what permissions are enabled for which connections.

Users and Groups **Manage Roles** Manage URL Aliases Manage API Keys Email Templates Custom Styles Custom Colors Custom Dates Static Assets

Roles / Role Detail

🔍 Role: Database admin

Name
Database admin

Description
Connection level management and dataset creation

✓ Privilege 👤 Members

🔍 System **Active** > @ ADD CONNECTIONS

🔍 Roles >

	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.
All connections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

🔍 Connections **Active** >

🔍 Datasets **Active** >

Actions available:

- ADD CONNECTIONS to add a new data connection role privilege
- Delete to remove a connection component

For more information on Connection privileges, see [Manage AVs/Extracts](#), [Import data](#), and [Create datasets, explore tables](#).

Datasets

You can see what permissions are enabled for which datasets.

Users and Groups **Manage Roles** Manage URL Aliases Manage API Keys Email Templates Custom Styles Custom Colors Custom Dates Static Assets

Roles / Role Detail

🔍 Role: Database admin

Name
Database admin

Description
Connection level management and dataset creation

✓ Privilege 👤 Members

🔍 System **Active** > @ ADD DATASETS

🔍 Roles >

	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.
All connections / All datasets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

🔍 Connections **Active** >

🔍 Datasets **Active** >

Actions available:

- ADD DATASETS to add a new dataset role privilege
- Delete to remove a dataset component

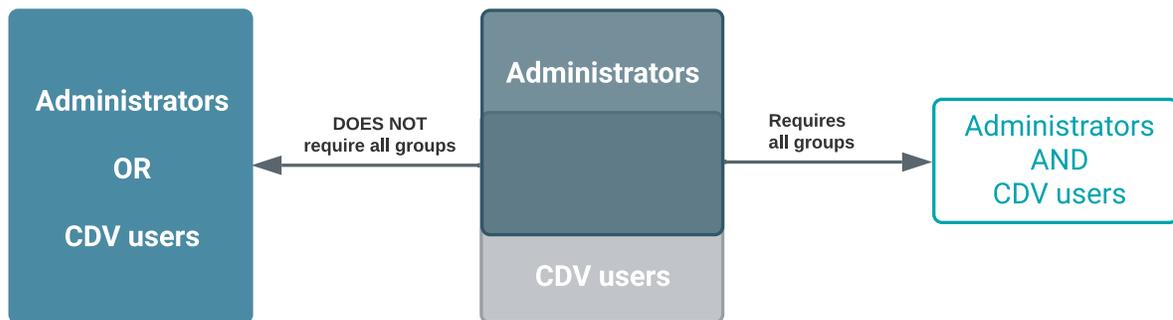
For more information on Dataset privileges, see [Manage dataset](#), [Manage dashboards](#), and [View dashboards](#).

All groups requirement

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, the role Administrators Only is shared by members of both Administrators and CDV users user groups. If you do not select the Require all groups option, all members of either group get the privileges of the role.

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



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

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

RBAC setup for dataset publishing

Role-Based Access Control (RBAC) empowers dataset creators to share or 'publish' their datasets securely by leveraging role-based privileges. The dataset creators can grant specific roles access using permissions like [Grant manage dataset](#), [Grant manage dashboards](#), and [Grant view dashboards](#).



Note:

- Only users with Manage roles and users role privilege (typically system administrators) can set up roles and permissions and define users and user groups.

Consider the following practical scenario to demonstrate how dataset publishing works:

- **Teams**
 - Marketing
 - Sales
 - Operations
- **Access levels in each team**
 - Data admins
 - Analysts
 - Visual consumers

To set up the required permissions, roles, groups, and users, see the documentation listed in the Related information section.

After you have completed the RBAC setup steps, Data Admins can proceed to publish their datasets, following the instructions in Publishing datasets documentation.

Related Information

[Setting the dataset recipient roles](#)

[Setting the dataset publisher role](#)

[Define groups for teams and access levels](#)

[Assign groups to roles](#)

[Assign users to groups](#)

[Publishing datasets](#)