Cloudera Data Visualization 7.2.9

Security

Date published: 2020-10-30
Date modified: 2024-12-18

CLOUDERA

Legal Notice

Contents

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 witth 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
• 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	• Grant manage dataset • Grant manage dashboards • Grant view dashboards	• Manage analytical views • Import data • Create datasets, explore tables	• 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.
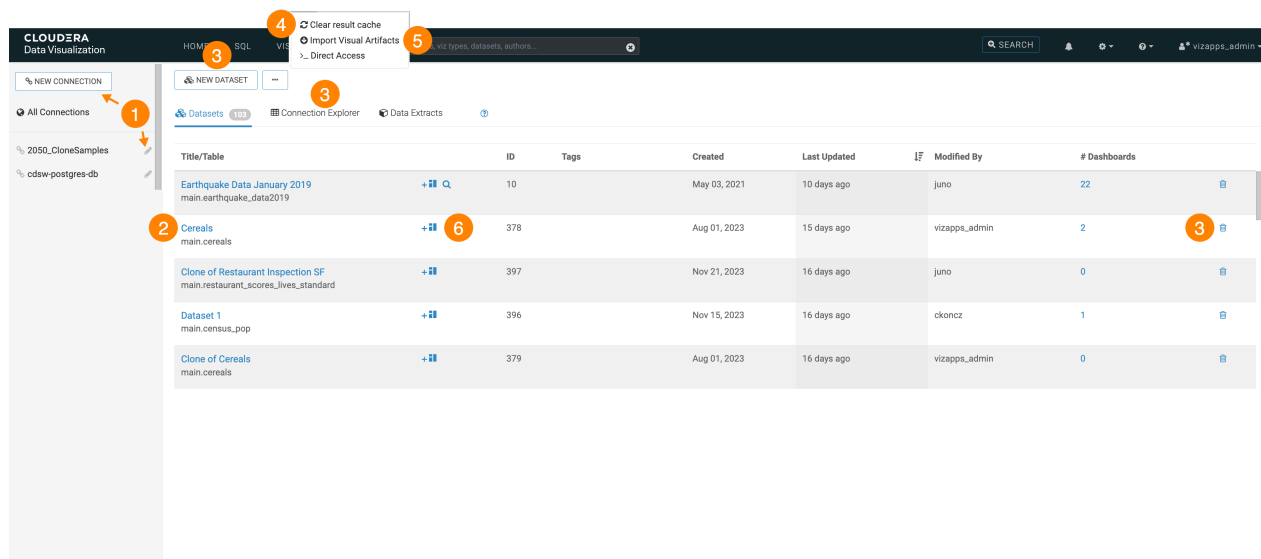
Role privileges

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.
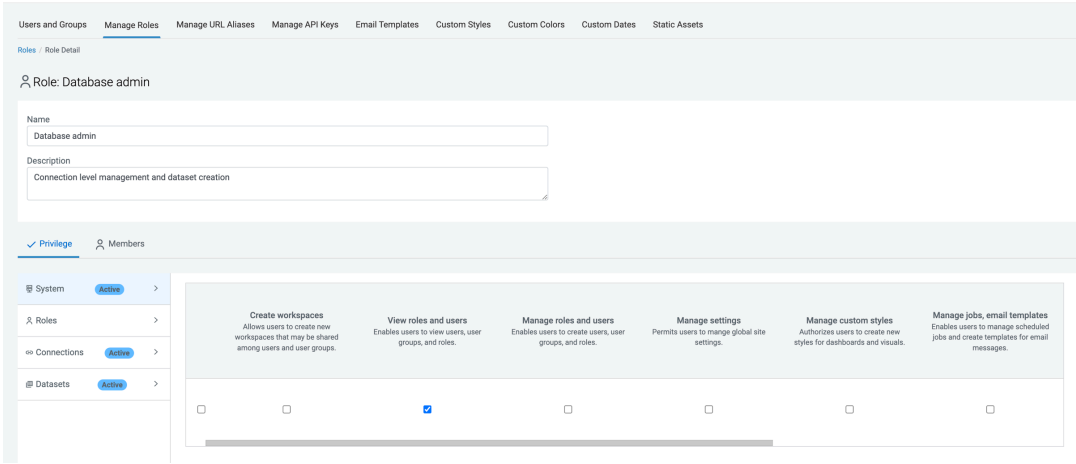
For more information on System privileges, see Create workspaces, View roles and users, Manage roles and users, Manage settings, Manage custom styles, Manage jobs, email templates, View activity logs, Manage data connections, and Additional system privilege.

Roles
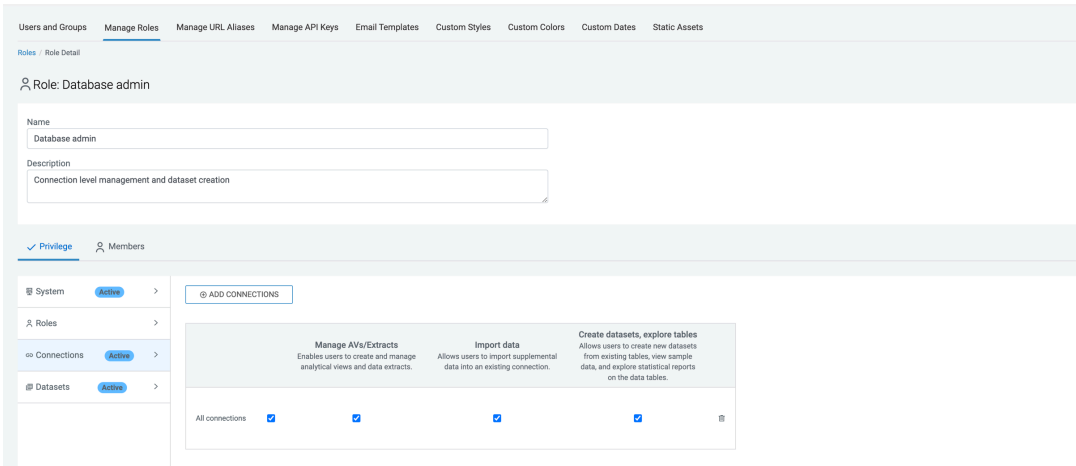
You can see which role-based permissions are enabled.
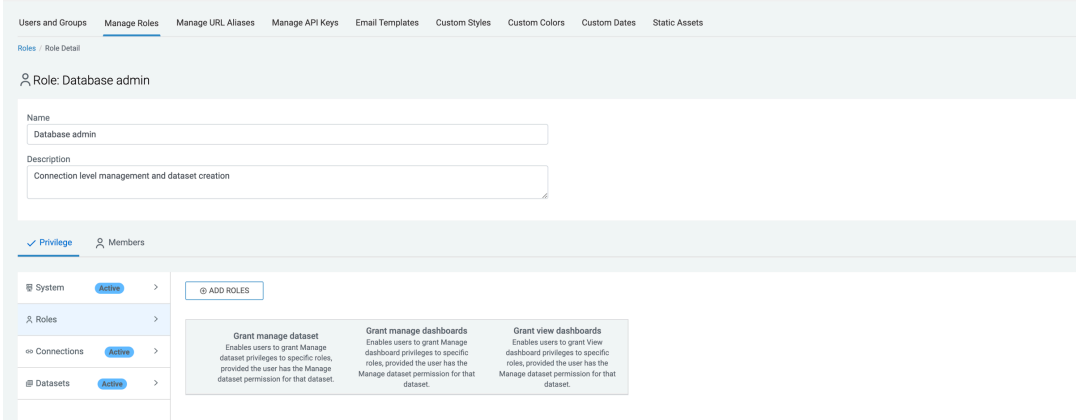
Actions available:

• 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.

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.
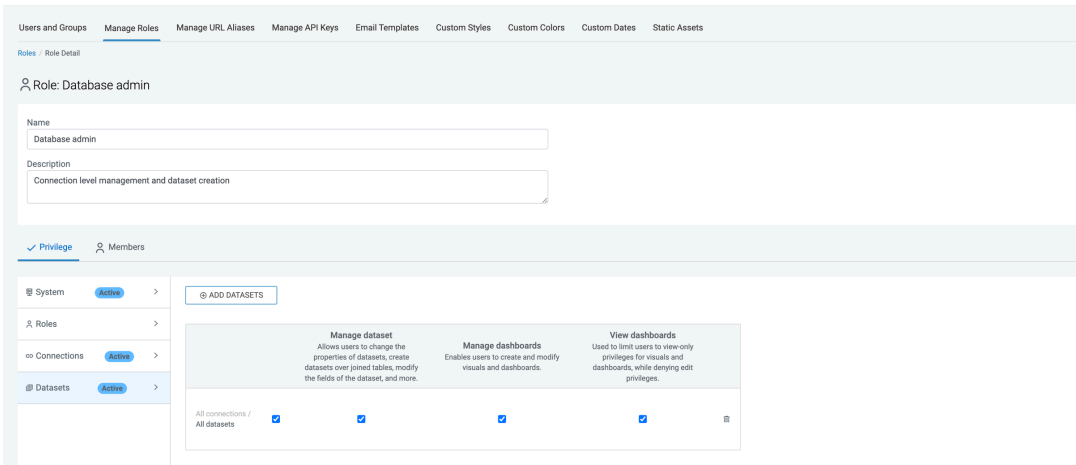
Actions available:

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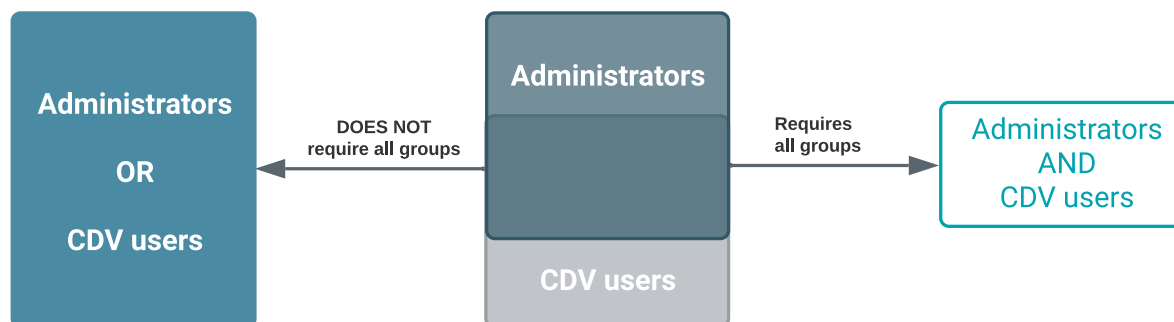
There are two other ways a user can be a member of the role, even when the Require all groups option is on:

- 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