

Cloudera Runtime 7.0.0

Ranger Auditing

Date published: 2019-08-21

Date modified:

CLouDERA

<https://docs.cloudera.com/>

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

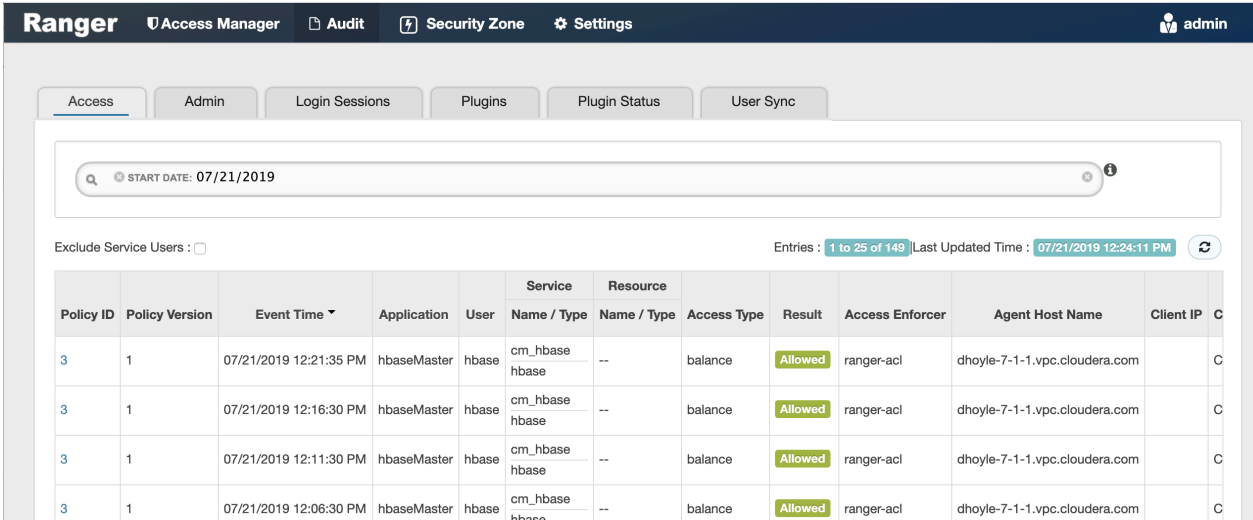
| | |
|--|----------|
| Audit Overview..... | 4 |
| Managing Auditing with Ranger..... | 4 |
| View audit details..... | 4 |
| Create a read-only Admin user (Auditor)..... | 7 |

Audit Overview

Apache Ranger provides a centralized framework for collecting access audit history and reporting data, including filtering on various parameters. Ranger enhances audit information obtained from Hadoop components and provides insights through this centralized reporting capability.

Managing Auditing with Ranger

To explore options for auditing policies in Ranger, click Audit in the top menu.



The screenshot shows the Ranger web interface. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user is logged in as 'admin'. Below the navigation bar are tabs for 'Access', 'Admin', 'Login Sessions', 'Plugins', 'Plugin Status', and 'User Sync'. The 'Audit' tab is active, displaying a search bar with 'START DATE: 07/21/2019'. Below the search bar, there is a table of audit entries. The table has columns for Policy ID, Policy Version, Event Time, Application, User, Service Name / Type, Resource Name / Type, Access Type, Result, Access Enforcer, Agent Host Name, Client IP, and a 'C' column. The table shows four entries, all with a result of 'Allowed'.

| Policy ID | Policy Version | Event Time | Application | User | Service Name / Type | Resource Name / Type | Access Type | Result | Access Enforcer | Agent Host Name | Client IP | C |
|-----------|----------------|------------------------|-------------|-------|---------------------|----------------------|-------------|---------|-----------------|-------------------------------|-----------|---|
| 3 | 1 | 07/21/2019 12:21:35 PM | hbaseMaster | hbase | cm_hbase hbase | -- | balance | Allowed | ranger-acl | dhoyle-7-1-1.vpc.cloudera.com | | C |
| 3 | 1 | 07/21/2019 12:16:30 PM | hbaseMaster | hbase | cm_hbase hbase | -- | balance | Allowed | ranger-acl | dhoyle-7-1-1.vpc.cloudera.com | | C |
| 3 | 1 | 07/21/2019 12:11:30 PM | hbaseMaster | hbase | cm_hbase hbase | -- | balance | Allowed | ranger-acl | dhoyle-7-1-1.vpc.cloudera.com | | C |
| 3 | 1 | 07/21/2019 12:06:30 PM | hbaseMaster | hbase | cm_hbase hbase | -- | balance | Allowed | ranger-acl | dhoyle-7-1-1.vpc.cloudera.com | | C |

There are six tabs on the Audit page:

- Access
- Admin
- Login sessions
- Plugins
- Plugin Status
- User Sync

View audit details

How to view operation details in Ranger audits.

Procedure

To view details for a particular operation, click any tab, then Policy ID, Operation name, or Session ID.

Audit > Access: HBase Table

The screenshot shows the Ranger interface with the 'Audit' tab selected. A search filter for 'START DATE: 07/21/2019' is applied. The main table displays access logs with columns for Policy ID, Policy Version, Event Time, Application, User, Service Name / Type, Resource Name / Type, Access Type, Result, and Access. One entry is highlighted with a blue box, and a modal window titled 'Policy Details' is open over it. The modal shows the following information:

- Service Name: cm_hbase
- Service Type: hbase
- Policy Type: Access
- Policy ID: 3
- Version: 1
- Policy Name: all - table, column-family, column
- HBase Table: --
- HBase Column-family: --
- HBase Column: --
- Description: Policy for all - table, column-family, column
- Audit Logging: Yes
- Policy Labels: --

Audit > Admin: Update

The screenshot shows the Ranger interface with the 'Admin' tab selected. The main table displays administrative operations with columns for Operation, Audit Type, User, Date, Actions, and Session Id. One entry is highlighted with a blue box, and a modal window titled 'Operation : update' is open over it. The modal shows the following information:

- Name: tag_service2
- Date: 07/21/2019 01:09:34 PM Eastern Daylight Time
- Updated By: admin
- Service Details:

| Fields | Old Value | New Value |
|---------------------|-----------|--------------|
| Service Description | -- | -- |
| Service Name | tag_tag | tag_service2 |

Audit > Admin: Create

The screenshot displays the Ranger Admin interface. At the top, the navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The 'Audit' tab is active. Below the navigation bar, there is a search box for 'Search for your access logs...'. The main content area shows a table of audit entries with columns for Operation, Audit Type, User, Date, Actions, and Session Id. The entry for 'Security Zone created security-zone2' is highlighted, and its 'Create' button is circled in red. A blue arrow points from this button to a modal dialog box titled 'Operation : create'. The dialog box contains the following details:

- Name : security-zone2
- Date : 07/14/2019 05:24:36 PM Eastern Daylight Time
- Created By : admin

Zone Details :

| Fields : | New Value |
|------------------------|----------------|
| Zone Description | -- |
| Zone Audit User Groups | -- |
| Zone Audit Users | auditor1 |
| Zone Admin User Groups | -- |
| Zone Admin Users | admin |
| Zone Tag Services | cm_tag |
| Zone Name | security-zone2 |

Zone Service Details :

| Service Name | Zone Service Resources |
|--------------|------------------------|
| | |

An 'OK' button is located at the bottom right of the dialog box.

Audit > User Sync: Sync details

The screenshot shows the Ranger Admin console with the 'User Sync' tab selected. The table below displays the sync events, and the 'Sync Details' modal is open for one of the entries.

| User Name | Sync Source | Number Of New | | Number Of Modified | | Event Time | Sync Details |
|----------------|-------------|---------------|--------|--------------------|--------|------------------------|--------------|
| | | Users | Groups | Users | Groups | | |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:22:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:21:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:20:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:19:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:18:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:17:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:16:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:15:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:14:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:13:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:12:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:11:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:10:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:09:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:08:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:07:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:06:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:05:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:04:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:03:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:02:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:01:48 PM | [Eye Icon] |
| rangerusersync | Unix | 0 | 0 | 0 | 0 | 07/21/2019 01:00:47 PM | [Eye Icon] |

| Name | Value |
|-------------------------------|------------------------|
| Unix | nss |
| File Name | /etc/passwd |
| Sync time | 07/21/2019 10:21:48 AM |
| Last modified time | 12/31/1969 04:00:00 PM |
| Minimum user id | 500 |
| Minimum group id | 0 |
| Total number of users synced | 35 |
| Total number of groups synced | 39 |

Create a read-only Admin user (Auditor)

Creating a read-only Admin user (Auditor) enables compliance activities because this user can monitor policies and audit events, but cannot make changes.

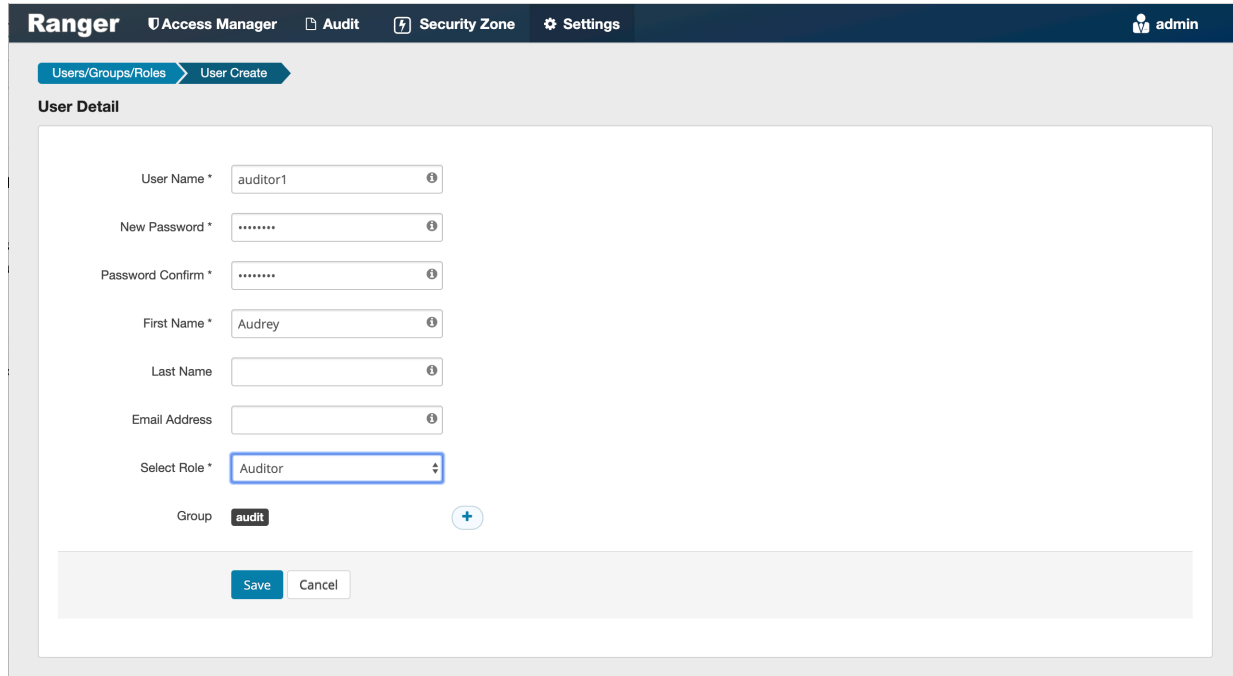
About this task

When a user with the Auditor role logs in, they see a read-only view of Ranger policies and audit events. An Auditor can search and filter on access audit events, and access and view all tabs under Audit to understand access events. They cannot edit users or groups, export/import policies, or make changes of any kind.

Procedure

1. Select Settings > Users/Groups/Roles.
2. Click Add New User.

3. Complete the **User Detail** section, selecting Auditor as the role:



The screenshot shows the Ranger web interface for creating a user. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings', with a user profile icon for 'admin'. The breadcrumb trail is 'Users/Groups/Roles > User Create'. The 'User Detail' section contains the following fields:

- User Name *: auditor1
- New Password *: [masked]
- Password Confirm *: [masked]
- First Name *: Audrey
- Last Name: [empty]
- Email Address: [empty]
- Select Role *: Auditor (highlighted with a blue border)
- Group: audit (with a plus icon to add more groups)

At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Click Save.