

Cloudera Runtime 7.0.0

Ranger Auditing

Date published: 2019-08-21

Date modified:

CLOUdera

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

Legal Notice

© Cloudera Inc. 2025. 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.

Exclude Service Users : ☐

Entries : 1 to 25 of 149 Last Updated Time : 07/21/2019 12:24:11 PM

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 > Admin: Update

Ranger Access Manager Audit Security Zone Settings admin

Access Admin Login Sessions Plugins Plugin Status User Sync

START DATE: 07/21/2019

Exclude Service Users: ☐

Entries: 1 to 25 of 25

Policy ID	Policy Version	Event Time	Application	User	Service Name / Type	Resource Name / Type	Access Type	Result	Action
3	1	07/21/2019 12:51:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-
3	1	07/21/2019 12:46:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-
3	1	07/21/2019 12:41:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl dhoyle-7-1-1.vpc.cloudera.com
3	1	07/21/2019 12:36:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl dhoyle-7-1-1.vpc.cloudera.com
3	1	07/21/2019 12:31:31 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl dhoyle-7-1-1.vpc.cloudera.com
3	1	07/21/2019 12:26:30 PM	hbaseMaster	hbase	cm_hbase hbase	--	balance	Allowed	ranger-acl dhoyle-7-1-1.vpc.cloudera.com

Policy Details

Service Name : cm_hbase Service Type : hbase

Policy Details :

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

Allow Condition :

< Version 1 >

OK

The screenshot displays the RANGER Access Manager interface. At the top, there are navigation tabs: "Ranger", "Access Manager", "Admin", "Security Zone", "Settings", and "admin". Below these, a secondary set of tabs includes "Access", "Admin", "Login Sessions", "Plugins", "Plugin Status", and "User Sync".

The main section is titled "Search for your access logs...". Below this, a summary bar indicates "Entries : 1 to 25 of 70" and "Last Updated Time : 07/21/2019 01:09:40 PM".

A table lists various operations. The columns are "Operation", "Audit Type", "User", "Date (Eastern Daylight Time)", "Actions", and "Session Id". The first row shows "Service updated tag_service2" performed by "admin" on "07/21/2019 01:09:34 PM". An arrow points from the "Update" button in the "Actions" column of this row to a modal window.

The modal window, titled "Operation : update", contains 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

At the bottom right of the modal is an "OK" button.

[Ranger](#)
[Access Manager](#)
[Audit](#)
[Security Zone](#)
[Settings](#)
admin

[illegible]

Audit > User Sync: Sync details

The screenshot shows the Ranger web interface with the 'User Sync' tab selected. A search bar at the top indicates 'START DATE: 07/21/2019'. Below the search bar, a status bar shows 'Entries: 1 to 25 of 803' and 'Last Updated Time: 07/21/2019 01:23:45 PM'. The main table displays sync events for 'rangerusersync' from a 'Unix' source. The table columns are: User Name, Sync Source, Number Of New (Users, Groups), Number Of Modified (Users, Groups), Event Time, and Sync Details. A modal window titled 'Sync Details' is open, showing the following information:

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.

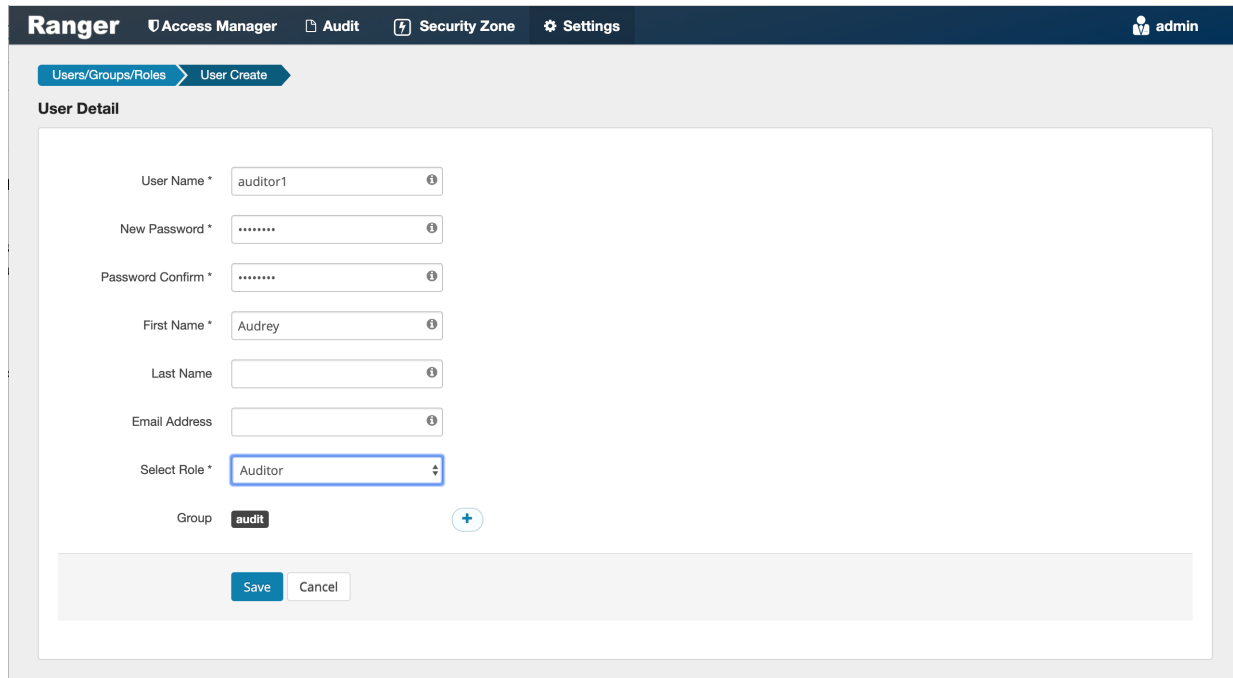
About this task

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 new user. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The breadcrumb trail shows 'Users/Groups/Roles' and '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.