Cloudera Runtime 7.1.8

Ranger Auditing

Date published: 2020-07-28
Date modified: 2022-12-15

CLOUDERA

https://docs.cloudera.com/

Legal Notice

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

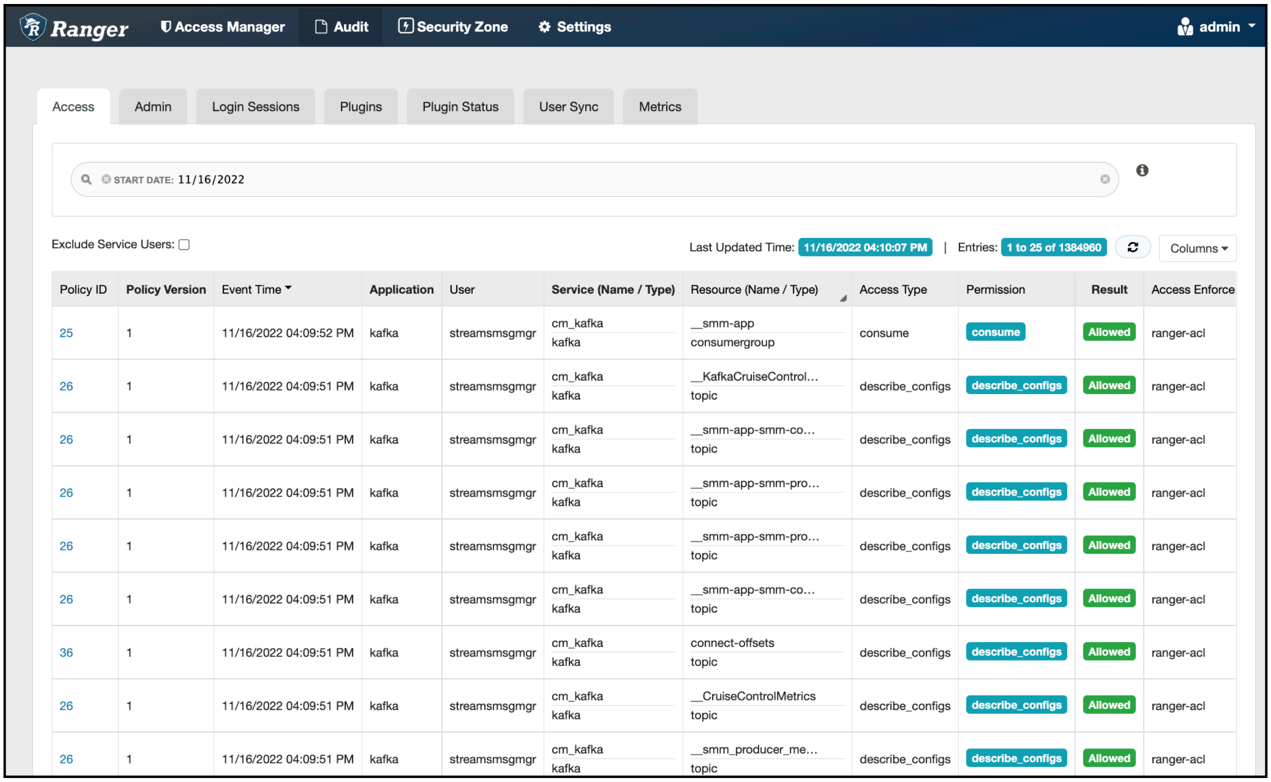
Audit Overview

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

You can manage auditing using the Audit page in the Ranger Admin Web UI.

To explore options for auditing policies, click Audit in the top menu of the Ranger Admin Web UI.



START DATE: 11/16/2022

Exclude Service Users: □

Last Updated Time: 11/16/2022 04:10:07 PM | Entries: 1 to 25 of 1384960

Policy ID	Policy Version	Event Time	Application	User	Service (Name / Type)	Resource (Name / Type)	Access Type	Permission	Result	Access Enforce
25	1	11/16/2022 04:09:52 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm-app consumergroup	consume	consume	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__KafkaCruiseControl… topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm-app-smm-co… topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm-app-smm-pro… topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm-app-smm-pro… topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm-app-smm-co… topic	describe_configs	describe_configs	Allowed	ranger-acl
36	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	connect-offsets topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__CruiseControlMetrics topic	describe_configs	describe_configs	Allowed	ranger-acl
26	1	11/16/2022 04:09:51 PM	kafka	streamsmsgmgr	cm_kafka kafka	__smm_producer_me… topic	describe_configs	describe_configs	Allowed	ranger-acl

Seven tabs sub-divide the Audit page:

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

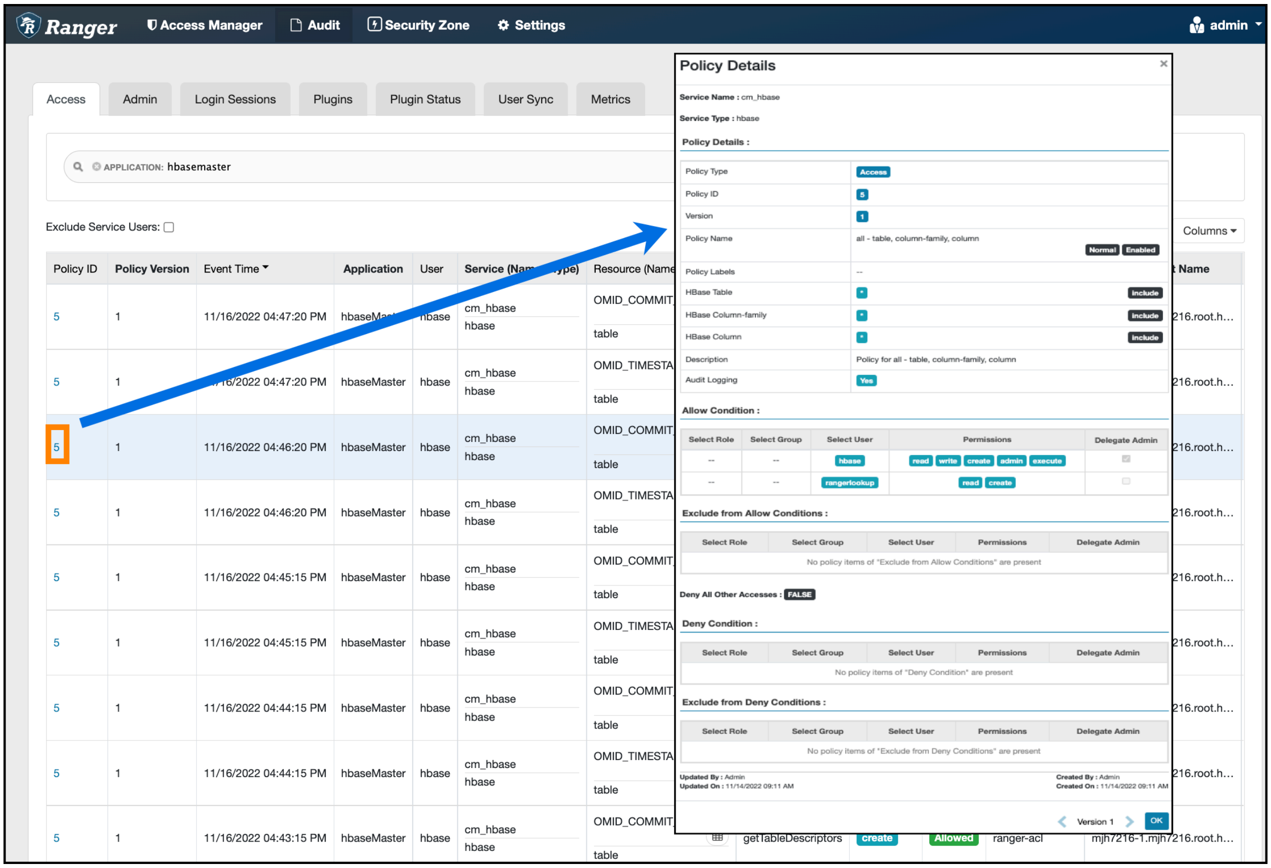
Viewing audit details

How to view policy and audit log details in Ranger audits.

Procedure

To view policy details for a specific audit log, click Access Policy ID .

Audit > Access: hbasemaster



APPLICATION: hbasemaster

Exclude Service Users: □

Policy ID	Policy Version	Event Time	Application	User	Service (Name / Type)	Resource (Name	t Name
5	1	11/16/2022 04:47:20 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_COMMIT table	216.root.h...
5	1	11/16/2022 04:47:20 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_TIMESTA table	216.root.h...
5	1	11/16/2022 04:46:20 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_COMMIT table	216.root.h...
5	1	11/16/2022 04:46:20 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_TIMESTA table	216.root.h...
5	1	11/16/2022 04:45:15 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_COMMIT table	216.root.h...
5	1	11/16/2022 04:45:15 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_TIMESTA table	216.root.h...
5	1	11/16/2022 04:44:15 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_COMMIT table	216.root.h...
5	1	11/16/2022 04:44:15 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_TIMESTA table	216.root.h...
5	1	11/16/2022 04:43:15 PM	hbaseMaster	hbase	cm_hbase hbase	OMID_COMMIT table	mjh7216-1.mjh7216.root.h...

getTableDescriptors create Allowed ranger-acl

Policy Details

Service Name : cm_hbase

Service Type : hbase

Policy Details :

Policy Type	Access
Policy ID	5
Version	1
Policy Name	all - table, column-family, column Normal Enabled
Policy Labels	--
HBase Table	* include
HBase Column-family	* include
HBase Column	* include
Description	Policy for all - table, column-family, column
Audit Logging	Yes

Allow Condition :

Select Role	Select Group	Select User	Permissions	Delegate Admin
--	--	hbase	read write create admin execute	☑
--	--	rangerlookup	read create	□

Exclude from Allow Conditions :

Select Role	Select Group	Select User	Permissions	Delegate Admin
No policy items of "Exclude from Allow Conditions" are present				

Deny All Other Accesses : FALSE

Deny Condition :

Select Role	Select Group	Select User	Permissions	Delegate Admin
No policy items of "Deny Condition" are present				

Exclude from Deny Conditions :

Select Role	Select Group	Select User	Permissions	Delegate Admin
No policy items of "Exclude from Deny Conditions" are present				

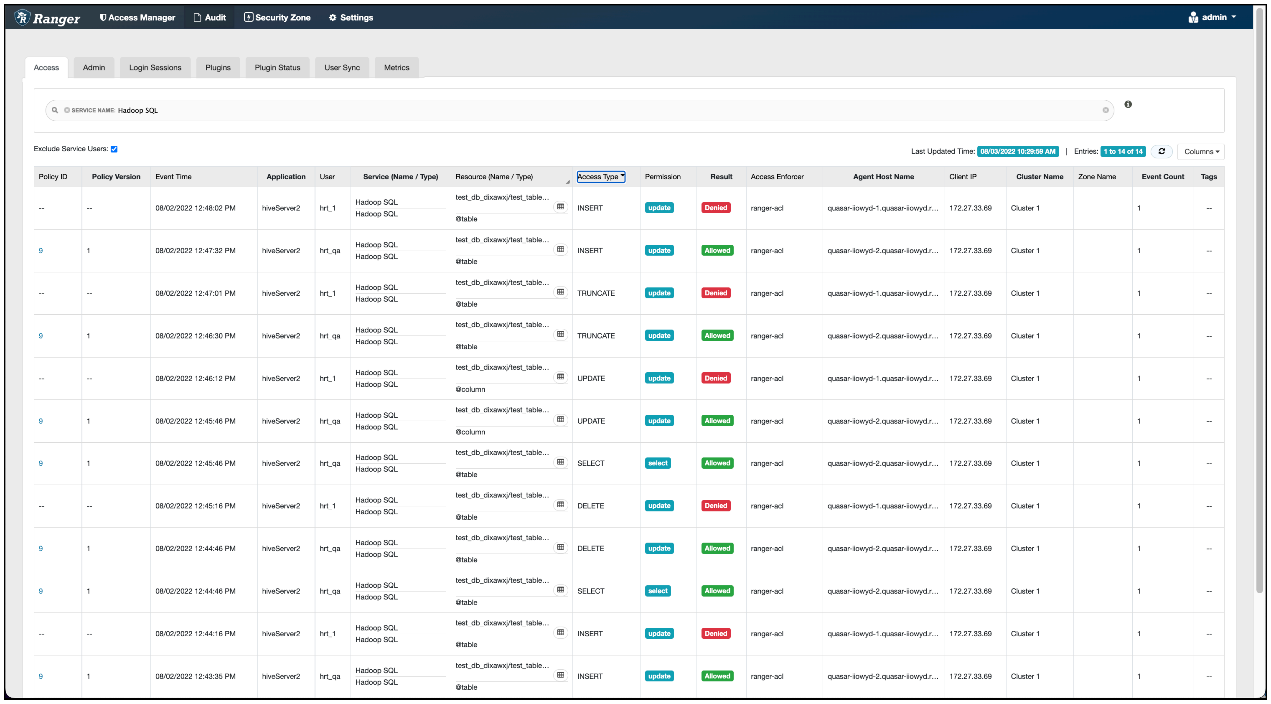
Updated By : Admin
Updated On : 11/14/2022 09:11 AM

Created By : Admin
Created On : 11/14/2022 09:11 AM

Version 1 OK

Audit > Access: HadoopSQL

Note: The Hive plugin audit handler now logs UPDATE operations as INSERT, UPDATE, DELETE, and TRUNCATE specifically.

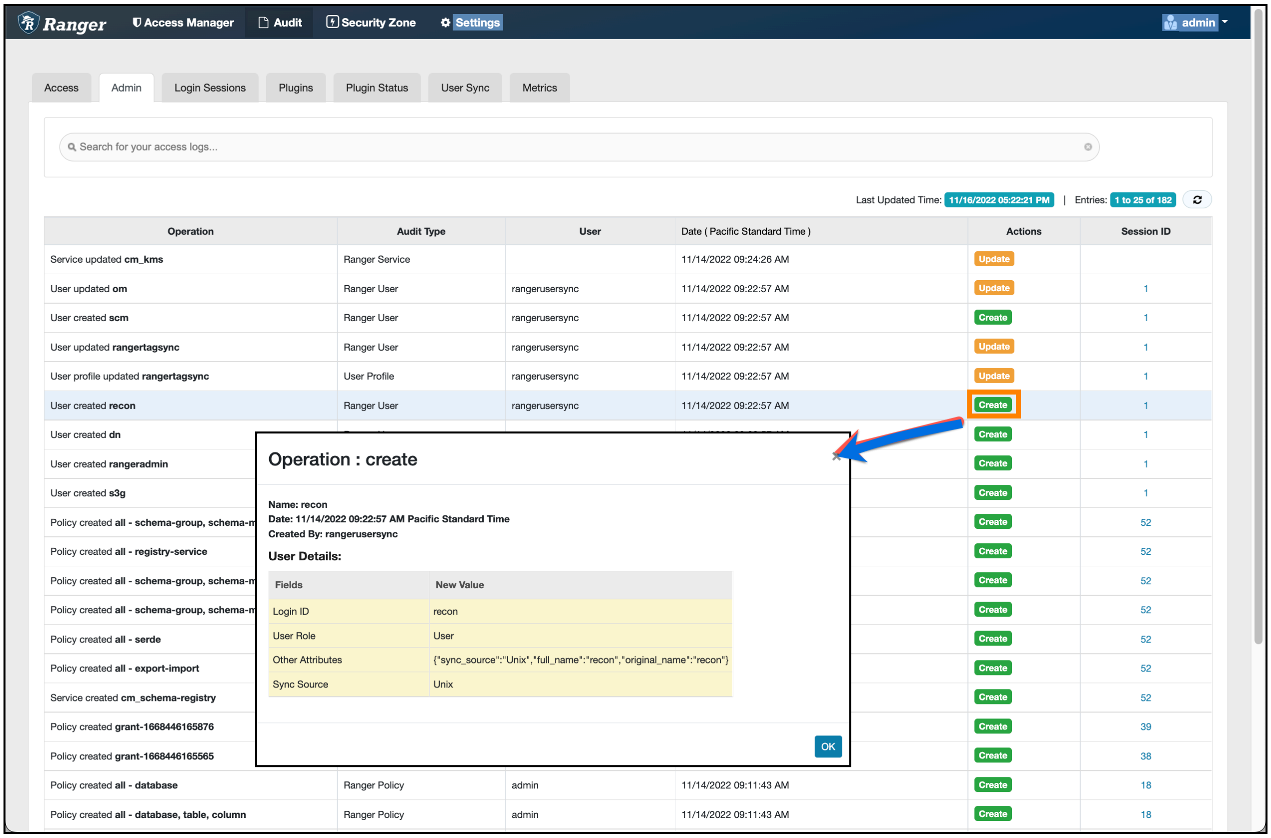


Exclude Service Users: ☑

Last Updated Time: 08/03/2022 10:29:59 AM | Entries: 1 to 14 of 14

Policy ID	Policy Version	Event Time	Application	User	Service (Name / Type)	Resource (Name / Type)	Access Type	Permission	Result	Access Enforcer	Agent Host Name	Client IP	Cluster Name	Zone Name	Event Count	Tags
--	--	08/02/2022 12:48:02 PM	hiveServer2	hrt_1	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	INSERT	update	Denied	ranger-acl	quasar-iiowyd-1.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:47:32 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	INSERT	update	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
--	--	08/02/2022 12:47:01 PM	hiveServer2	hrt_1	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	TRUNCATE	update	Denied	ranger-acl	quasar-iiowyd-1.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:46:30 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	TRUNCATE	update	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
--	--	08/02/2022 12:46:12 PM	hiveServer2	hrt_1	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @column	UPDATE	update	Denied	ranger-acl	quasar-iiowyd-1.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:45:46 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @column	UPDATE	update	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:45:46 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	SELECT	select	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
--	--	08/02/2022 12:45:16 PM	hiveServer2	hrt_1	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	DELETE	update	Denied	ranger-acl	quasar-iiowyd-1.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:44:46 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	DELETE	update	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:44:46 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	SELECT	select	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
--	--	08/02/2022 12:44:16 PM	hiveServer2	hrt_1	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	INSERT	update	Denied	ranger-acl	quasar-iiowyd-1.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--
9	1	08/02/2022 12:43:35 PM	hiveServer2	hrt_qa	Hadoop SQL Hadoop SQL	test_db_dixawxj/test_table... @table	INSERT	update	Allowed	ranger-acl	quasar-iiowyd-2.quasar-iiowyd.r...	172.27.33.69	Cluster 1		1	--

Audit > Admin: Create



Last Updated Time: 11/16/2022 05:22:21 PM | Entries: 1 to 25 of 182

Operation	Audit Type	User	Date (Pacific Standard Time)	Actions	Session ID
Service updated **cm_kms**	Ranger Service		11/14/2022 09:24:26 AM	Update	
User updated **om**	Ranger User	rangerusersync	11/14/2022 09:22:57 AM	Update	1
User created **scm**	Ranger User	rangerusersync	11/14/2022 09:22:57 AM	Create	1
User updated **rangertagsync**	Ranger User	rangerusersync	11/14/2022 09:22:57 AM	Update	1
User profile updated **rangertagsync**	User Profile	rangerusersync	11/14/2022 09:22:57 AM	Update	1
User created **recon**	Ranger User	rangerusersync	11/14/2022 09:22:57 AM	Create	1
User created **dn**				Create	1
User created **rangeradmin**				Create	1
User created **s3g**				Create	1
Policy created **all - schema-group, schema-m**				Create	52
Policy created **all - registry-service**				Create	52
Policy created **all - schema-group, schema-m**				Create	52
Policy created **all - schema-group, schema-m**				Create	52
Policy created **all - serde**				Create	52
Policy created **all - export-import**				Create	52
Service created **cm_schema-registry**				Create	52
Policy created **grant-1668446165876**				Create	39
Policy created **grant-1668446165565**				Create	38
Policy created **all - database**	Ranger Policy	admin	11/14/2022 09:11:43 AM	Create	18
Policy created **all - database, table, column**	Ranger Policy	admin	11/14/2022 09:11:43 AM	Create	18

Operation : create

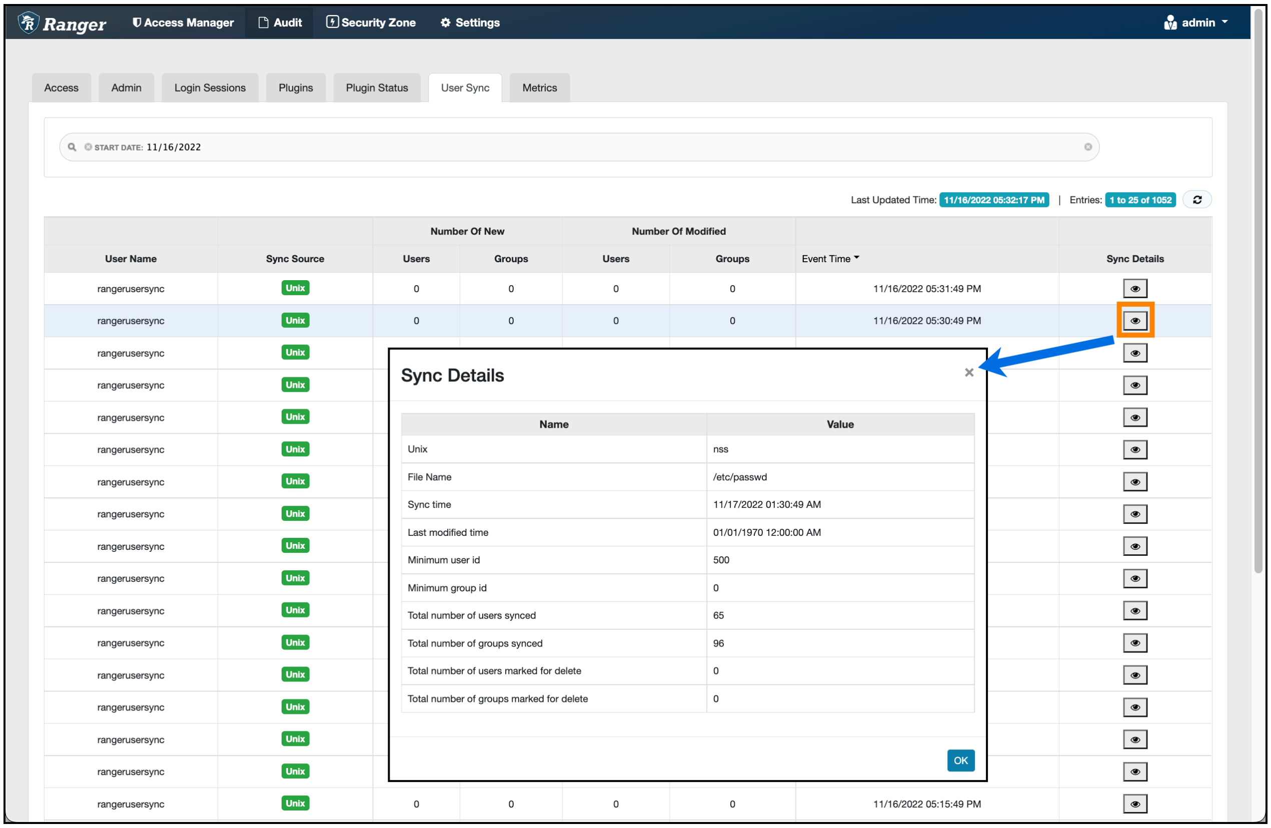
Name: recon
Date: 11/14/2022 09:22:57 AM Pacific Standard Time
Created By: rangerusersync

User Details:

Fields	New Value
Login ID	recon
User Role	User
Other Attributes	{"sync_source":"Unix","full_name":"recon","original_name":"recon"}
Sync Source	Unix

OK

Audit > User Sync: Sync details



START DATE: 11/16/2022

Last Updated Time: 11/16/2022 05:32:17 PM | Entries: 1 to 25 of 1052

		Number Of New		Number Of Modified			
User Name	Sync Source	Users	Groups	Users	Groups	Event Time	Sync Details
rangerusersync	Unix	0	0	0	0	11/16/2022 05:31:49 PM	👁
rangerusersync	Unix	0	0	0	0	11/16/2022 05:30:49 PM	👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix						👁
rangerusersync	Unix	0	0	0	0	11/16/2022 05:15:49 PM	👁

Sync Details

Name	Value
Unix	nss
File Name	/etc/passwd
Sync time	11/17/2022 01:30:49 AM
Last modified time	01/01/1970 12:00:00 AM
Minimum user id	500
Minimum group id	0
Total number of users synced	65
Total number of groups synced	96
Total number of users marked for delete	0
Total number of groups marked for delete	0

Viewing audit metrics

How to view audit metrics information using the Ranger Admin Web UI.

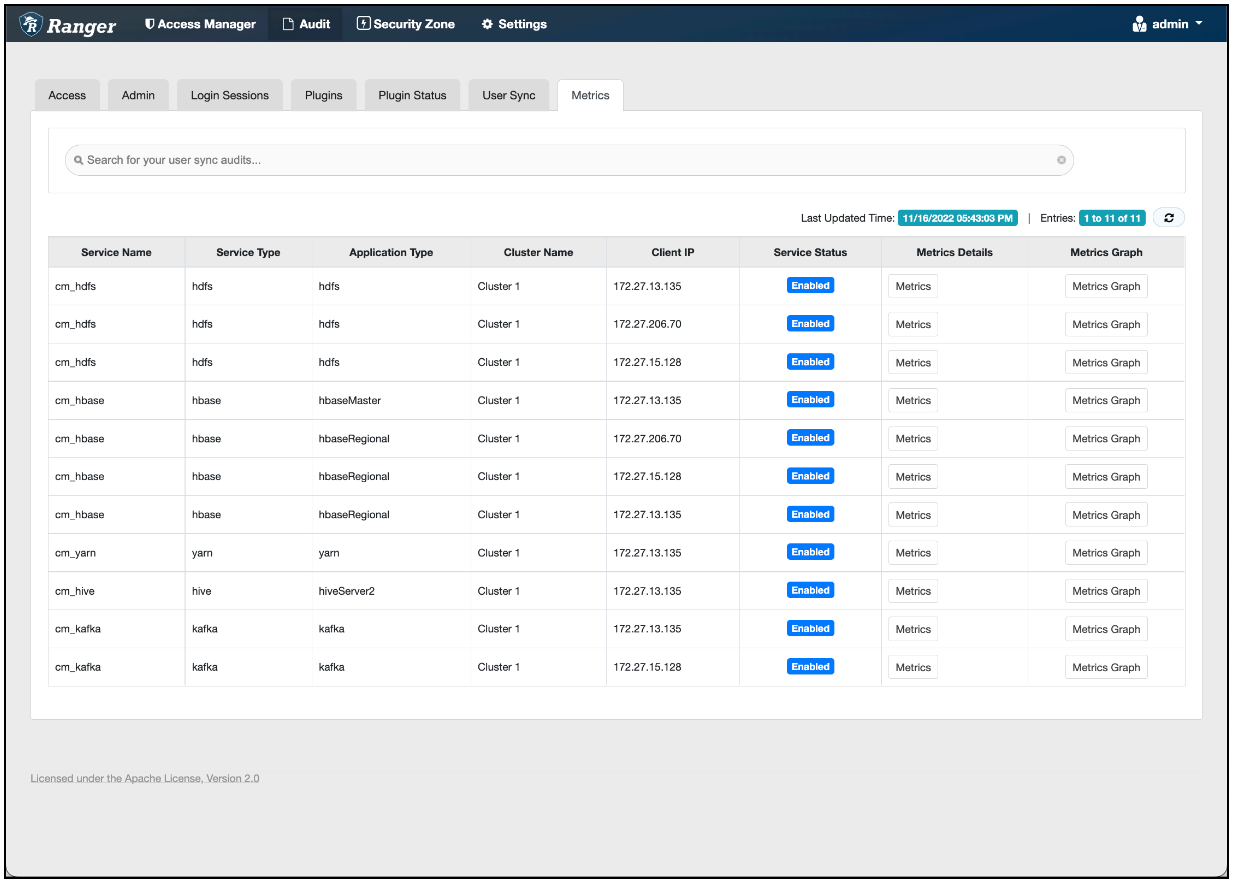
About this task

Metrics provides a high-level view of audit logs as they generate and update in Ranger. Ranger captures audit metrics throughput from the following Ranger services:

- Atlas
- HBase
- Hdfs
- Hive
- Impala
- Kafka
- Knox
- Kudu
- NiFi
- Schema-registry
- Solr
- Streams Messaging Manager
- Yarn

Procedure

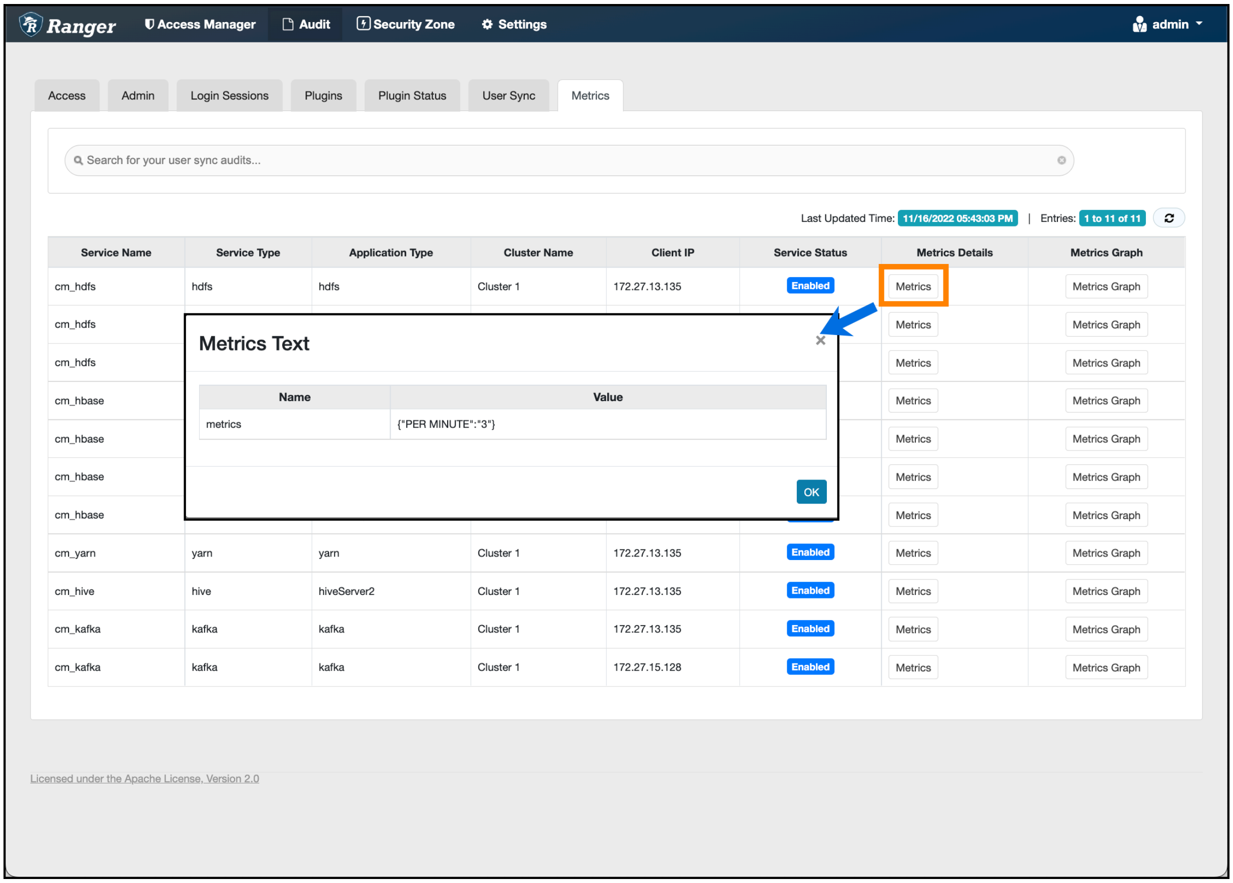
1. To view audit metrics, in the Ranger Admin Web UI, click Audit Metrics .



Last Updated Time: 11/16/2022 05:43:03 PM | Entries: 1 to 11 of 11

Service Name	Service Type	Application Type	Cluster Name	Client IP	Service Status	Metrics Details	Metrics Graph
cm_hdfs	hdfs	hdfs	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hdfs	hdfs	hdfs	Cluster 1	172.27.206.70	Enabled	Metrics	Metrics Graph
cm_hdfs	hdfs	hdfs	Cluster 1	172.27.15.128	Enabled	Metrics	Metrics Graph
cm_hbase	hbase	hbaseMaster	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hbase	hbase	hbaseRegional	Cluster 1	172.27.206.70	Enabled	Metrics	Metrics Graph
cm_hbase	hbase	hbaseRegional	Cluster 1	172.27.15.128	Enabled	Metrics	Metrics Graph
cm_hbase	hbase	hbaseRegional	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_yarn	yarn	yarn	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hive	hive	hiveServer2	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_kafka	kafka	kafka	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_kafka	kafka	kafka	Cluster 1	172.27.15.128	Enabled	Metrics	Metrics Graph

2. To view metrics details for a specific service, click Metrics.



Last Updated Time: 11/16/2022 05:43:03 PM | Entries: 1 to 11 of 11

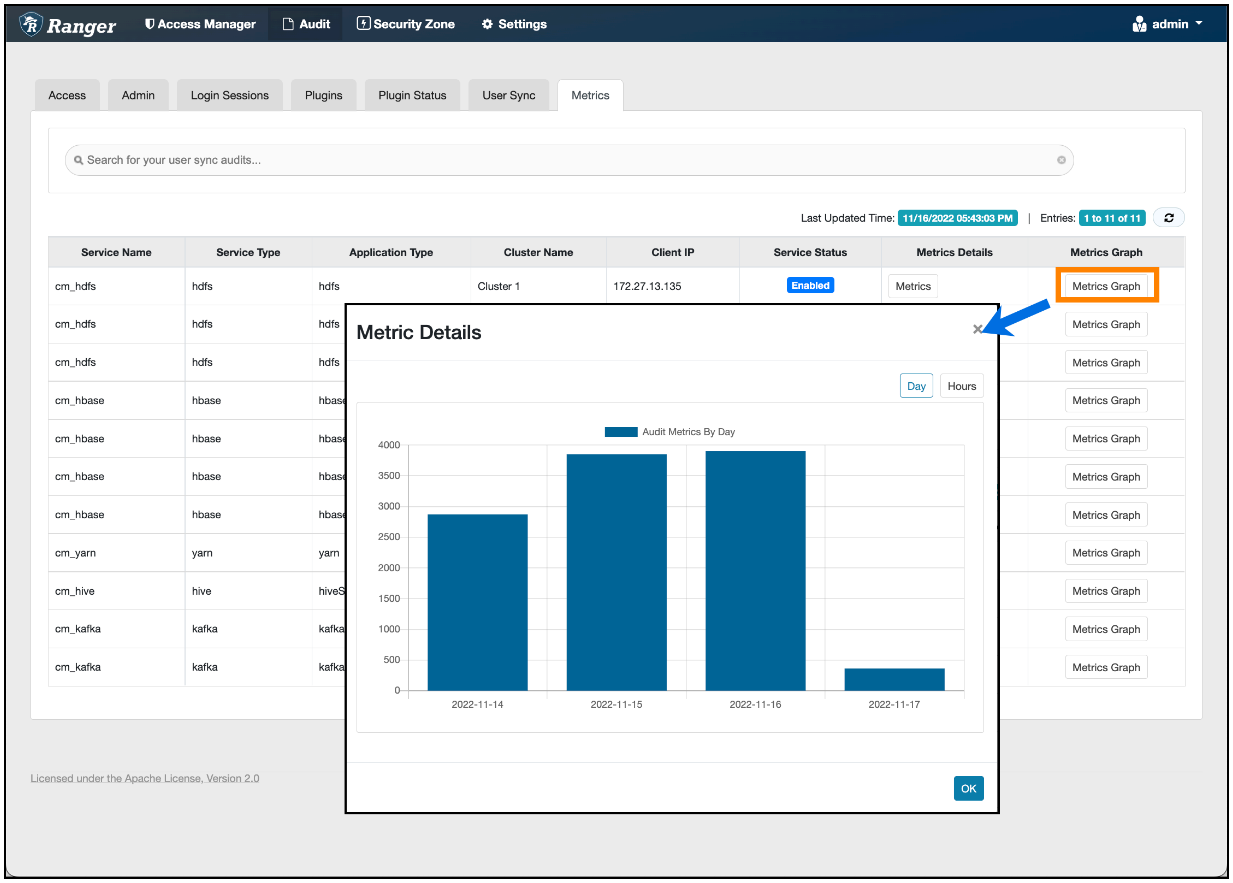
Service Name	Service Type	Application Type	Cluster Name	Client IP	Service Status	Metrics Details	Metrics Graph
cm_hdfs	hdfs	hdfs	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hdfs						Metrics	Metrics Graph
cm_hdfs						Metrics	Metrics Graph
cm_hbase						Metrics	Metrics Graph
cm_hbase						Metrics	Metrics Graph
cm_hbase						Metrics	Metrics Graph
cm_hbase						Metrics	Metrics Graph
cm_yarn	yarn	yarn	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hive	hive	hiveServer2	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_kafka	kafka	kafka	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_kafka	kafka	kafka	Cluster 1	172.27.15.128	Enabled	Metrics	Metrics Graph

Metrics Text

Name	Value
metrics	{"PER MINUTE":"3"}

Licensed under the Apache License, Version 2.0

3. To view hourly or daily metrics as a graphic for a specific service, click Metrics Graph.



Last Updated Time: 11/16/2022 05:43:03 PM | Entries: 1 to 11 of 11

Service Name	Service Type	Application Type	Cluster Name	Client IP	Service Status	Metrics Details	Metrics Graph
cm_hdfs	hdfs	hdfs	Cluster 1	172.27.13.135	Enabled	Metrics	Metrics Graph
cm_hdfs	hdfs	hdfs					Metrics Graph
cm_hdfs	hdfs	hdfs					Metrics Graph
cm_hbase	hbase	hbas					Metrics Graph
cm_hbase	hbase	hbas					Metrics Graph
cm_hbase	hbase	hbas					Metrics Graph
cm_hbase	hbase	hbas					Metrics Graph
cm_yarn	yarn	yarn					Metrics Graph
cm_hive	hive	hiveS					Metrics Graph
cm_kafka	kafka	kafka					Metrics Graph
cm_kafka	kafka	kafka					Metrics Graph

Metric Details

Creating 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.

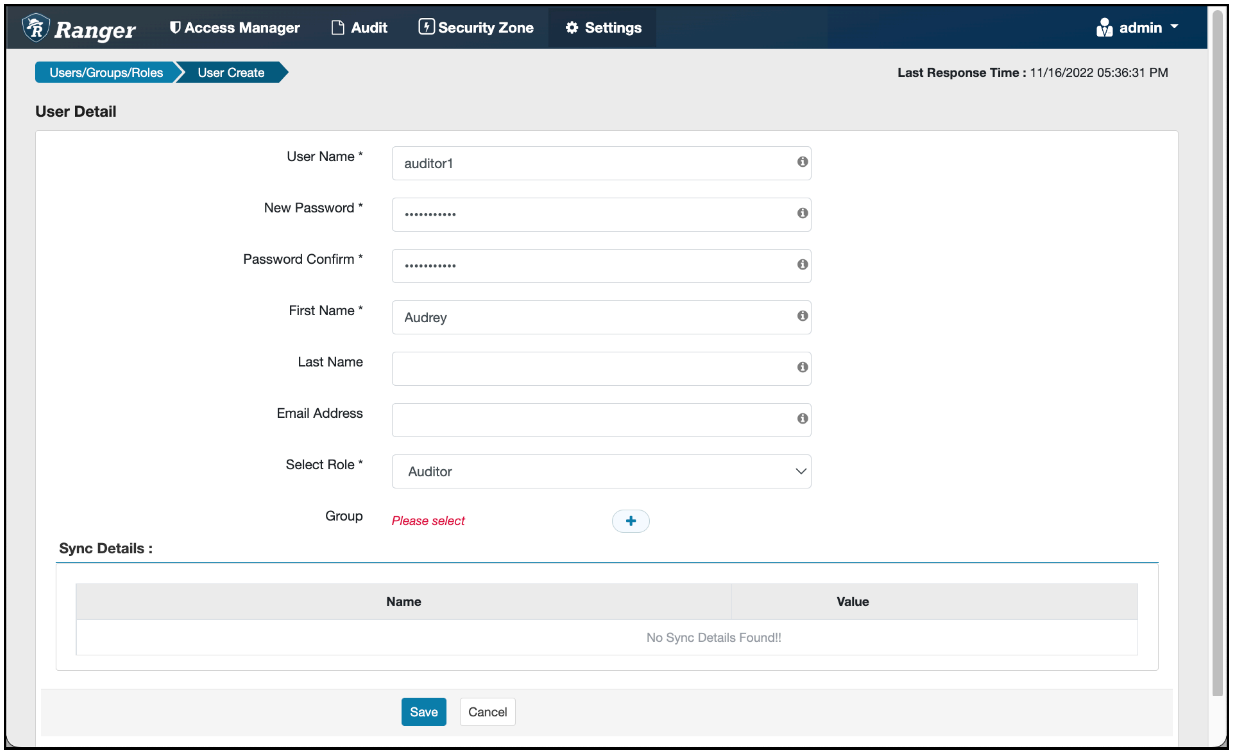
About this task

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:



Last Response Time : 11/16/2022 05:36:31 PM

User Detail

User Name * auditor1

New Password * ....

Password Confirm * ....

First Name * Audrey

Last Name

Email Address

Select Role * Auditor

Group Please select

Sync Details :

Name	Value
No Sync Details Found!!	

4. Click Save.

Updating Ranger audit configration parameters

How to change the default time settings that control how long Ranger keeps audit data collected by solr.

About this task

You can configure parameters that control how much data collected by solr that Ranger will store for auditing purposes.

Table 1: Ranger Audit Configuration Parameters

Parameter Name	Description	Default Setting	Units
ranger.audit.solr.config.ttl	Time To Live for Solr Collection of Ranger Audits	90	days
ranger.audit.solr.config.delete.trigger	Auto Delete Period in seconds for Solr Collection of Ranger Audits for expired documents	1	days (configurable)

Note: "Time To Live for Solr Collection of Ranger Audits" is also known as the Max Retention Days attribute.

Procedure

1. From Cloudera Manager choose Ranger Configuration .
2. In Search, type ranger.audit.solr.config, then press Return.
3. In ranger.audit.solr.config.ttl, set the the number of days to keep audit data.
4. In ranger.audit.solr.config.delete.trigger set the number and units (days, minutes, hours, or seconds) to keep data for expired documents

5. Refresh the configuration, using one of the following two options:
   a) Click Refresh Configuration, as prompted or, if Refresh Configuration does not appear,
   b) In Actions, click Update Solr config-set for Ranger, then confirm.

Triggering HDFS audit files rollover

How to configure when HDFS audit files close for each service.

About this task

By default, the Ranger Audit framework closes audit files created in HDFS or other cloud storage inline with audit event triggers. In other words, when an audit event occurs, Ranger checks the configured rollout time and then closes the file if the threshold has reached. Default audit rollout time is 24 hours. If no audit event occurs in a 24 hour period, files remain open beyond the 24 hour period. In some environments, audit log analysis that encounter an audit file open beyond the current date can cause system exceptions. If you want the files to be closed every day, so that the audit log file will have only that day's log and the next day’s log will be in the next day's file, you can configure the audit framework to close files every day. To do this, you must add several configuration parameters to the ranger-<service_name>-audit.xml (safety valve) file for each service, using Cloudera Manager.

Procedure

1. From Cloudera Manager choose <service_name> Configuration .
2. In <service_name> Configuration Search , type ranger-<service_name>, then press Return.
3. In <service_name> Server Advanced Configuration Snippet (Safety Valve) for ranger-<service_name>-audit.xml, do the following steps:
   a) Click + (Add).
   b) In Name, type xasecure.audit.destination.hdfs.file.rollover.enable.periodic.rollover
   c) In Value, type true.

      When this is enabled Ranger Audit Framework will spawn a Scheduler thread which monitors the occurrence of closing threshold and closes the file. By default every night the file gets closed.
   d) Click + (Add another).
   e) In Name, type xasecure.audit.destination.hdfs.file.rollover.sec
   f) In Value, type an integer value in seconds.

      This is the time in seconds when the file has to be closed. The default value is 86400 sec (1 day) which triggers the file to be closed at midnight and opens a new audit log for the next day. You can override the default value can be overridden by setting this parameter. For example, if you set the value 3600 (1 hr), the file gets closed every hour.

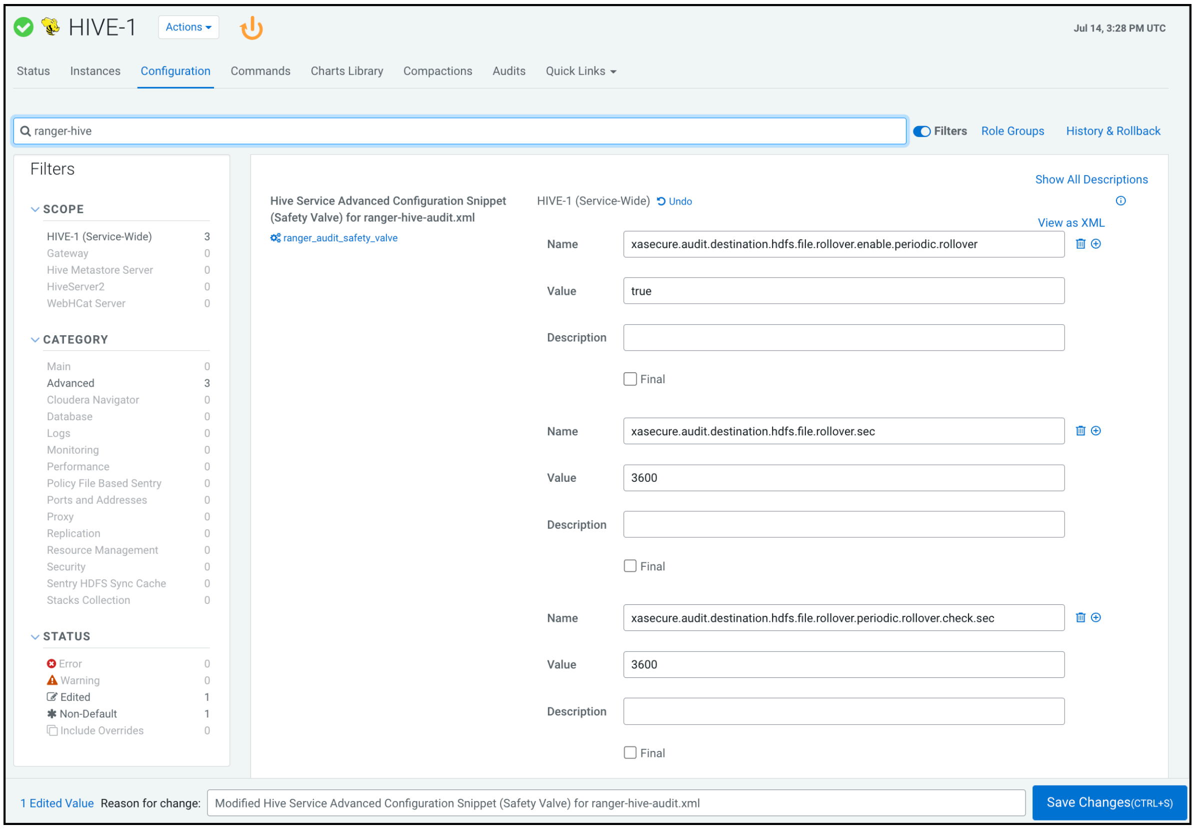
g) Click + (Add another).

h) In Name, type xasecure.audit.destination.hdfs.file.rollover.periodic.rollover.check.sec

i) In Value, type an integer value in seconds.

This is the time frequency of the check to be done whether the threshold time for rollover has occurred. By default the check is done every 60 secs. You can configure this parameter to delay the check time.

Figure 1: Example: Hive service configured to trigger rollover of hdfs audit files



ranger-hive

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

ranger_audit_safety_valve

HIVE-1 (Service-Wide)

Name: xasecure.audit.destination.hdfs.file.rollover.enable.periodic.rollover
Value: true
Description:
□ Final

Name: xasecure.audit.destination.hdfs.file.rollover.sec
Value: 3600
Description:
□ Final

Name: xasecure.audit.destination.hdfs.file.rollover.periodic.rollover.check.sec
Value: 3600
Description:
□ Final

1 Edited Value Reason for change: Modified Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

j) Click Save Changes (CTRL+S).

4. Repeat steps 1-3 for each service.

5. Restart the service.

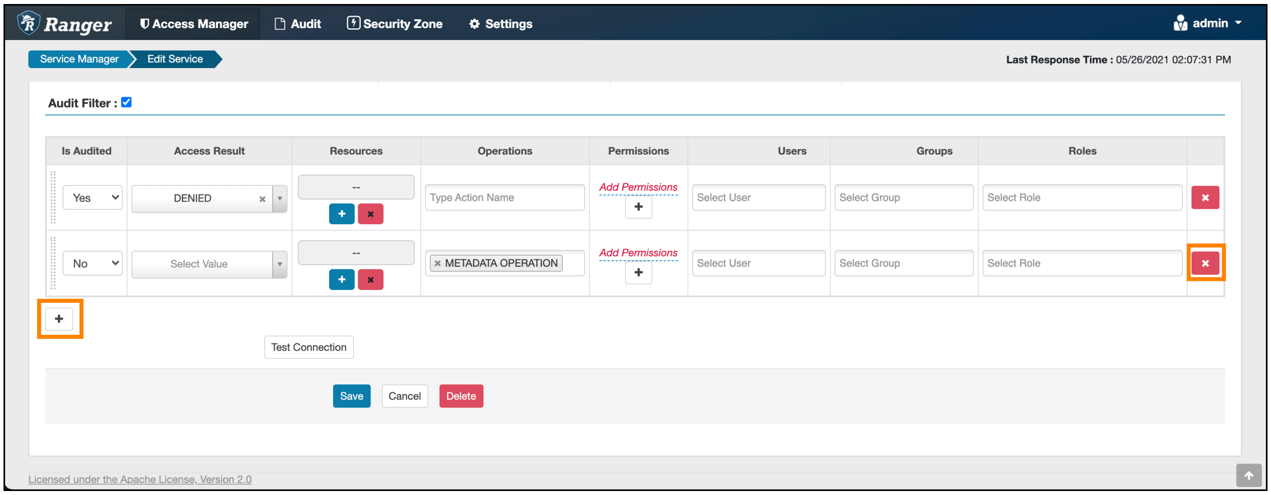
Ranger Audit Filters

You can use Ranger audit filters to control the amount of audit log data collected and stored on your cluster.

About Ranger audit filters

Ranger audit filters allow you to control the amount of audit log data for each Ranger service. Audit filters are defined using a JSON string that is added to each service configuration. The audit filter JSON string is a simplified form of the Ranger policy JSON. Audit filters appear as rows in the Audit Filter section of the Edit Service view for each service. The set of audit filter rows defines the audit log policy for the service. For example, the default audit log policy for the Hadoop SQL service appears in Ranger Admin web UI Service Manager Edit Service when you scroll down to Audit Filter. Audit Filter is checked (enabled) by default. In this example, the top row defines an audit filter that causes all instances of "access denied" to appear in audit logs. The lower row defines a filter that causes no metadata operations to appear in audit logs. These two filters comprise the default audit filter policy for Hadoop SQL service.

Figure 2: Default audit filter policy for the Hadoop SQL service



Last Response Time : 05/26/2021 02:07:31 PM

Audit Filter : ☑

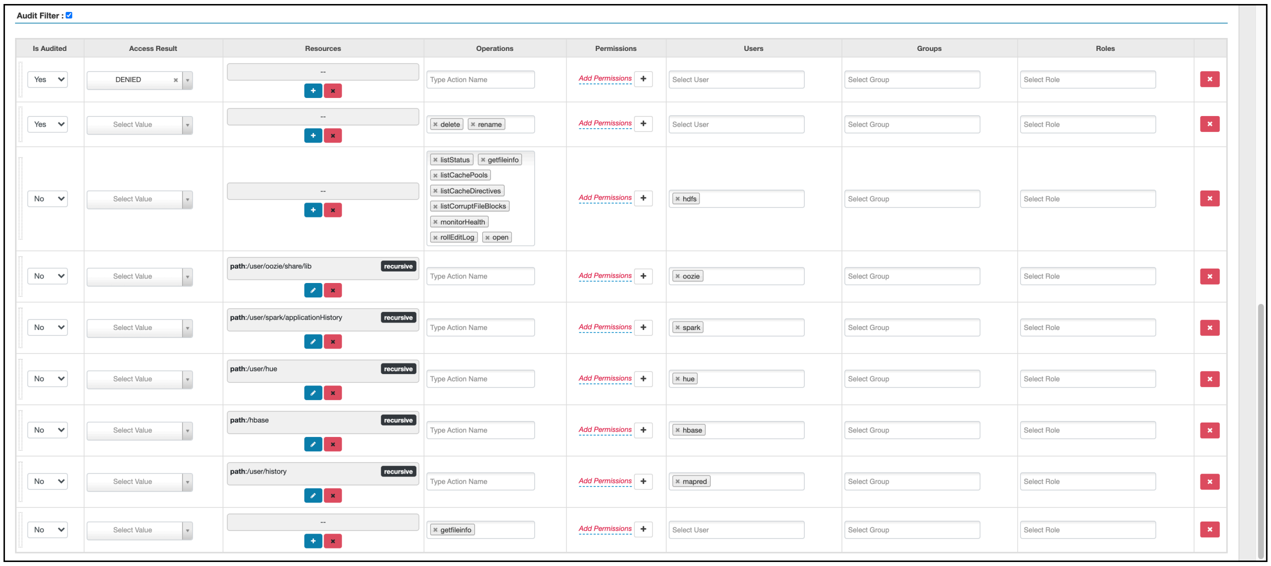
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	METADATA OPERATION	Add Permissions	Select User	Select Group	Select Role

Default Ranger audit filters

Default audit filters for the following Ranger service appear in Edit Services and may be modified as necessary by Ranger Admin users.

HDFS

Figure 3: Default audit filters for HDFS service

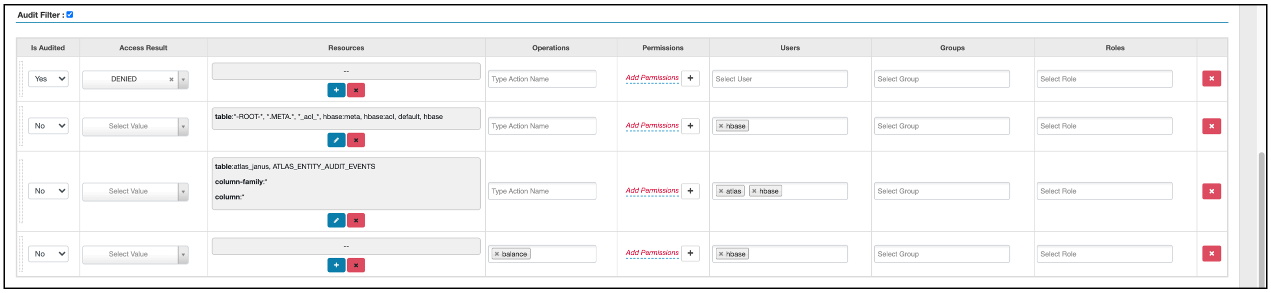


Audit Filter : ☑

Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
Yes	Select Value	--	delete rename	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	listStatus getfileinfo listCachePools listCacheDirectives listCorruptFileBlocks monitorHealth rollEditLog open	Add Permissions	hdfs	Select Group	Select Role
No	Select Value	path:/user/oozie/share/lib recursive	Type Action Name	Add Permissions	oozie	Select Group	Select Role
No	Select Value	path:/user/spark/applicationHistory recursive	Type Action Name	Add Permissions	spark	Select Group	Select Role
No	Select Value	path:/user/hue recursive	Type Action Name	Add Permissions	hue	Select Group	Select Role
No	Select Value	path:/hbase recursive	Type Action Name	Add Permissions	hbase	Select Group	Select Role
No	Select Value	path:/user/history recursive	Type Action Name	Add Permissions	mapred	Select Group	Select Role
No	Select Value	--	getfileinfo	Add Permissions	Select User	Select Group	Select Role

Hbase

Figure 4: Default audit filters for the Hbase service

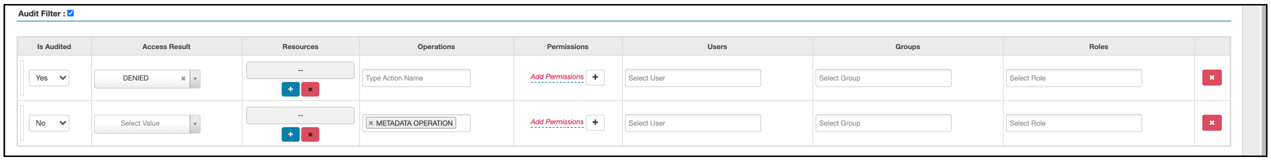


Audit Filter : ☑

Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED	--	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×
No	Select Value	**table**:*-ROOT-*, *.META.*, *_acl_*, hbase:meta, hbase:acl, default, hbase	Type Action Name	Add Permissions +	× hbase	Select Group	Select Role	×
No	Select Value	**table**:atlas_janus, ATLAS_ENTITY_AUDIT_EVENTS **column-family**:* **column**:*	Type Action Name	Add Permissions +	× atlas × hbase	Select Group	Select Role	×
No	Select Value	--	× balance	Add Permissions +	× hbase	Select Group	Select Role	×

Hadoop SQL

Figure 5: Default audit filters for the Hadoop SQL service

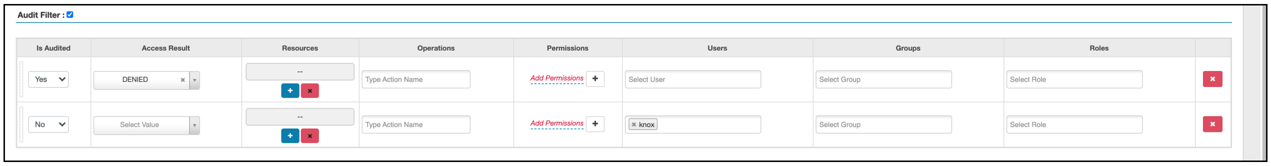


Audit Filter : ☑

Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED	--	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×
No	Select Value	--	× METADATA OPERATION	Add Permissions +	Select User	Select Group	Select Role	×

Knox

Figure 6: Default audit filters for the Knox service

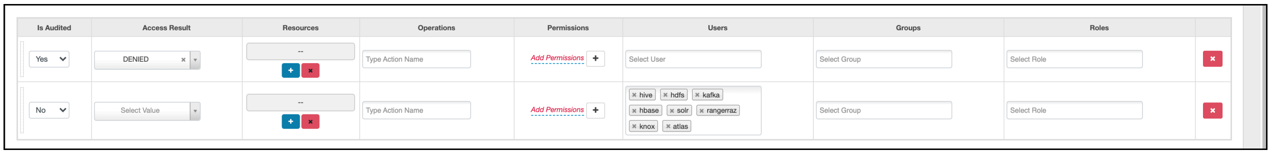


Audit Filter : ☑

Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED	--	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×
No	Select Value	--	Type Action Name	Add Permissions +	× knox	Select Group	Select Role	×

Solr

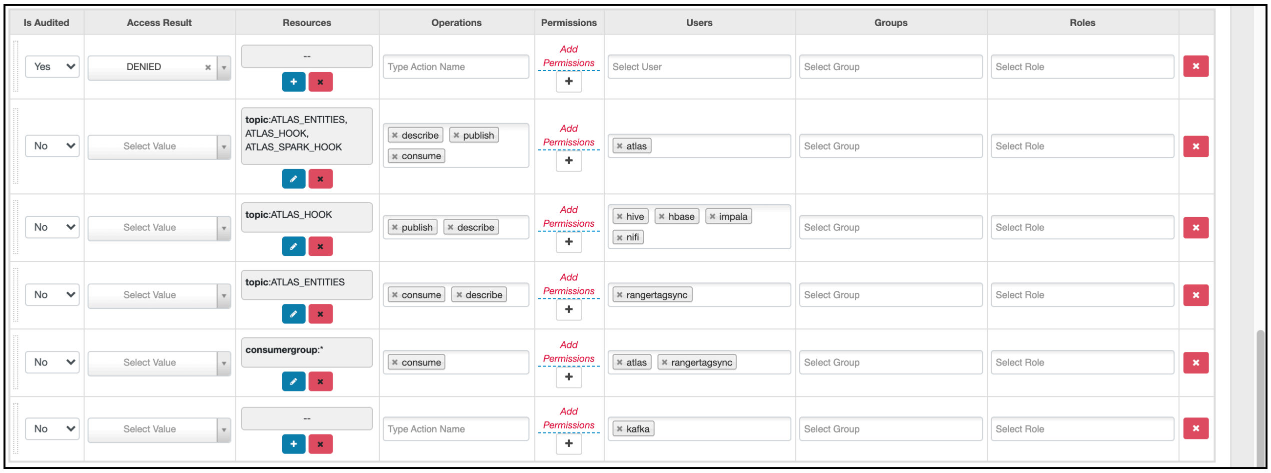
Figure 7: Default audit filters for the Solr service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED	--	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×
No	Select Value	--	Type Action Name	Add Permissions +	× hive × hdfs × kafka × hbase × solr × rangerraz × knox × atlas	Select Group	Select Role	×

Kafka

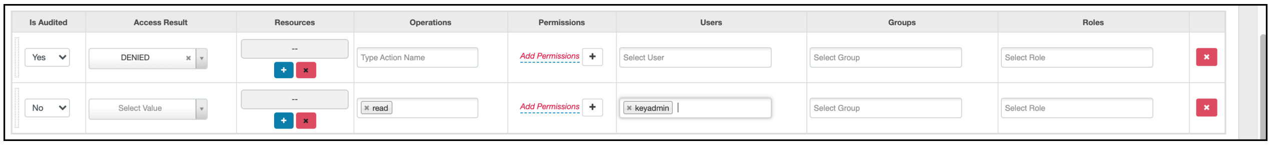
Figure 8: Default audit filters for the Kafka service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	topic:ATLAS_ENTITIES, ATLAS_HOOK, ATLAS_SPARK_HOOK	describe publish consume	Add Permissions	atlas	Select Group	Select Role
No	Select Value	topic:ATLAS_HOOK	publish describe	Add Permissions	hive hbase impala nifi	Select Group	Select Role
No	Select Value	topic:ATLAS_ENTITIES	consume describe	Add Permissions	rangertagsync	Select Group	Select Role
No	Select Value	consumergroup:*	consume	Add Permissions	atlas rangertagsync	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	kafka	Select Group	Select Role

Ranger KMS

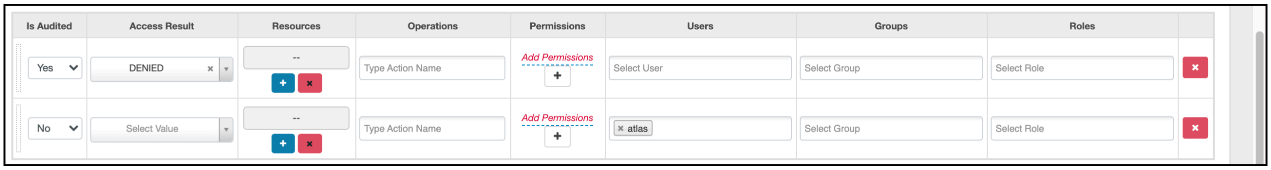
Figure 9: Default audit filters for the Ranger KMS service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	read	Add Permissions	keyadmin	Select Group	Select Role

Atlas

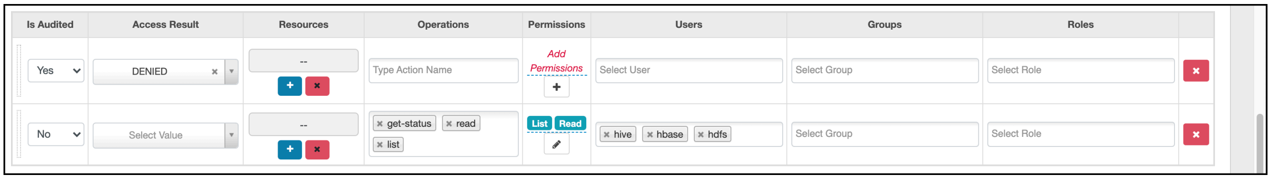
Figure 10: Default audit filters for the Atlas service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	atlas	Select Group	Select Role

ADLS

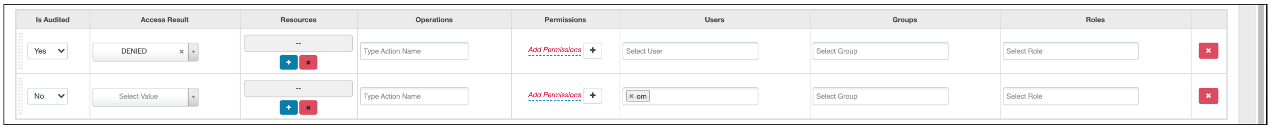
Figure 11: Default audit filters for the ADLS service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	get-status read list	List Read	hive hbase hdfs	Select Group	Select Role

Ozone

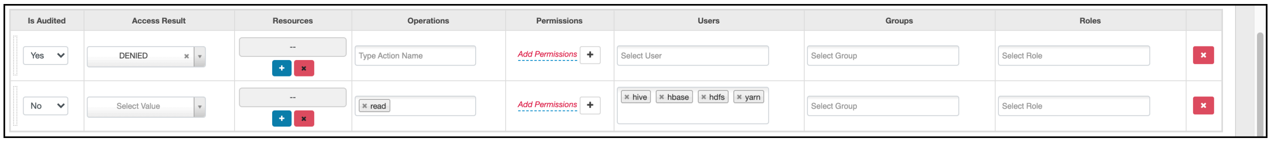
Figure 12: Default audit filters for the Ozone service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	om	Select Group	Select Role

S3

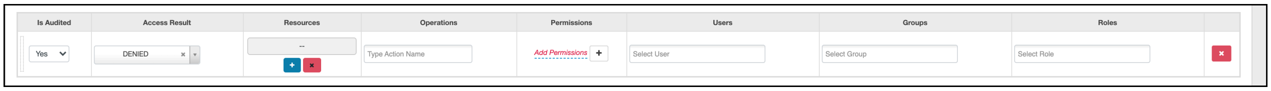
Figure 13: Default audit filters for the S3 service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED ×	-- + ×	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×
No	Select Value	-- + ×	× read	Add Permissions +	× hive × hbase × hdfs × yarn	Select Group	Select Role	×

Tag-based services

Figure 14: Default audit filters for a tag-based service



Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	DENIED ×	-- + ×	Type Action Name	Add Permissions +	Select User	Select Group	Select Role	×

Note:

Default audit filter policies do not exist for Yarn, NiFi, NiFi Registry, Kudu, or schema registry services.

Configuring a Ranger audit filter policy

You can configure an audit filter as you add or edit a resource- or tag-based service.

To configure an audit filter policy:

1. In Ranger Admin web UI Service Manager clcik Add or Edit for either a resource-, or tag-based service.
2. Scroll down to Audit Filter.
3. Click Audit Filter flag.

   You configure a Ranger audit filter policy by adding (+), deleting (X), or modifying each audit filter row for the service.

4. Use the controls in the filter row to edit filter properties. For example, you can configure:

   Is Audited: choose Yes or No

   to include or not include a filter in the audit logs for a service

   Access Result: choose DENIED, ALLOWED, or NOT_DETERMINED

   to include that access result in the audit log filter

   Resources: Add or Delete a resource item

   to include or remove the resource from the audit log filter

   Operations: Add or Remove an action name

   to include the action/operation in the audit log filter

   (click x to remove an existing operation)

   Permissions: Add or Remove permissions

   a. Click + in Permissions to open the Add dialog.
   b. Select/Unselect required permissions.

   For example, in HDFS service select read, write, execute, or All permissions.

   Users: click Select User to see a list of defined users

   to include one or multiple users in the audit log filter

   Groups: click Select Group to see a list of defined groups

   to include one or multiple groups in the audit log filter

   Roles: click Select Role to see a list of defined roles

   to include one or multiple roles in the audit log filter

Audit filter details

- When you save the UI selections described in the preceding list, audit filters are defined as a JSON list. Each service references a unique list.
- For example, ranger.plugin.audit.filters for the HDFS service includes:

```
[

               {
               "accessResult":"DENIED",
               "isAudited":true
               },
               {
               "users":[
               "unaudited-user1"
               ],
               "groups":[
               "unaudited-group1"
               ],
               "roles":[
               "unaudited-role1"
               ],
               "isAudited":false
               },
               {
               "actions":[
               "listStatus",
               "getfileinfo"
               ],
               "accessTypes":[
               "execute"
               ],
               "isAudited":false
               },
               {
               "resources":{
               "path":{
               "values":[
               "/audited"
               ],
               "isRecursive":true
               }
               },
               "isAudited":true
               },
               {
               "resources":{
               "path":{
               "values":[
               "/unaudited"
               ],
               "isRecursive":true
               }
               },
               "isAudited":false
               }
               ]
```

- Each value in the list is an audit filter, which takes the format of a simplified Ranger policy, along with access results fields.
- Audit filters are defined with rules on Ranger policy attributes and access result attributes.
  - Policy attributes: resources, users, groups, roles, accessTypes
  - Access result attributes: isAudited, actions, accessResult
- The following audit filter specifies that accessResult=DENIED will be audited.

  The isAudited flag specifies whether or not to audit.

  ```
  {"accessResult":"DENIED","isAudited":true}
  ```
- The following audit filter specifies that “resource => /unaudited” will not be audited.

  ```
  {"resources":{"path":{"values":["/
  unaudited"],"isRecursive":true}},"isAudited":false}
  ```
- The following audit filter specifies that access to resource database=> sys table=> dump by user “use2” will not be audited.

  ```
  {"resources":{"database":{"values":["sys"]},"table":{"values":
  ["dump"]}},"users":["user2"],"isAudited":false}
  ```
- The following audit filter specifies that access result in actions => listStatus, getfileInfo and accessType => execute will not be audited.

  ```
  {"actions":["listStatus","getfileinfo"],"accessTypes":
  ["execute"],"isAudited":false}
  ```
- The following audit filter specifies that access by user "superuser1" and group "supergroup1" will not be audited.

  ```
  {"users":["superuser1"],"groups":["supergroup1"],"isAudited":false}
  ```
- The following audit filter specifies that access to any resource tagged as NO_AUDIT will not be audited.

  ```
  {"resources":{"tag":{"values":["NO_AUDIT"]}},"isAudited":false}
  ```

How to set audit filters in Ranger Admin Web UI

You can set specific audit filter conditions for each service, using Create/Edit Service .

About this task

Creating audit filters for a service using the Ranger Admin Web UI can prevent audit logs from being sent to destinations like SOLR and HDFS.

Procedure

1. In the Ranger Admin Web UI Service Manager , click Add New Service or Edit (existing service).
2. On Create/Edit Service, scroll down to Audit Filters.
   a) Verify that Audit Filter is checked.

      Optionally, define any of the following to include in the filter definition:

      Is Audited

      Defines whether audit logs are stored or not.

      Is Audited=Yes: stores audit records in the defined audit destination.

      Is Audited=No: do not store audit records.

      Access Results

      Denied, Allowed, or Not Determined

      select to filter access=denied, access=allowed or all by selecting access=Not determined.

      Resource

      use Resource Details to include or exclude specific resources such as databases, tables, or columns.

      Operations

      select specific operations to filter

      Permissions

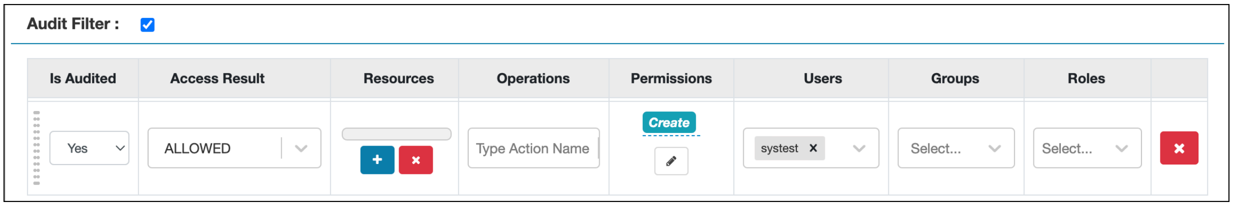
      select specific permissions

      Users, Groups, Roles

      select specific users, groups, and roles

   b) Click Save.

Figure 15: Adding an audit filter that stores user systest, access=Allowed logs for Hive service



Audit Filter : ☑

Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles	
Yes	ALLOWED	+ ×	Type Action Name	Create	systest ×	Select...	Select...	×

3. Test your filters to verify that defined audit filters perform as expected.

Results

Defining specific filtering properties can prevent access logs for service users from being stored in the configured audit destination, if Is Audited = No.

Filter service access logs from Ranger UI

You can limit display of system access/audit log records generated by service users in each service.

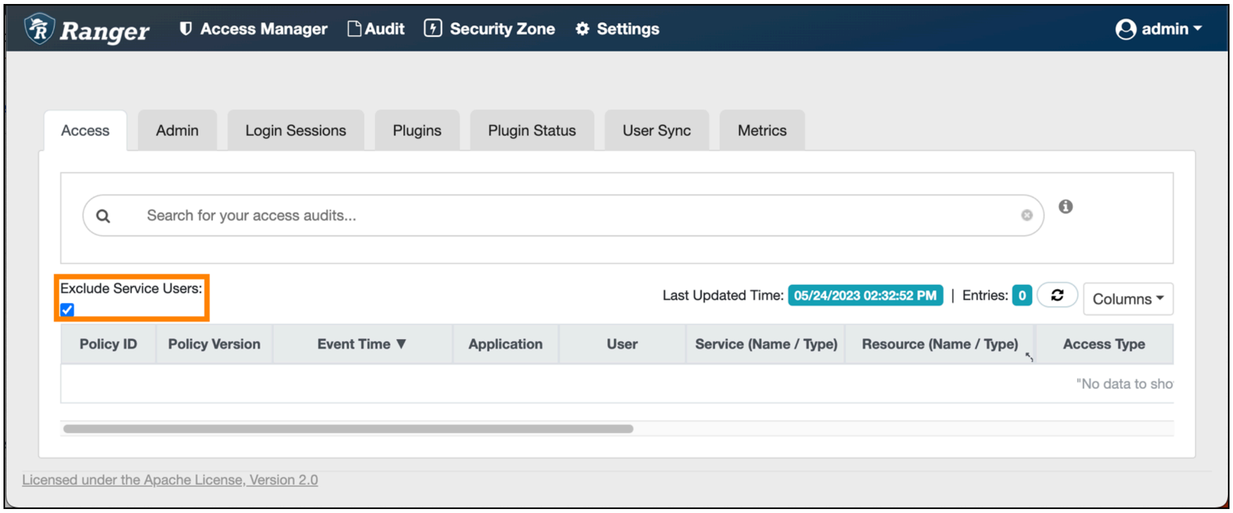
About this task

This topic describes how to limit the display of access log records on the Access tab in the Ranger Admin Web UI.

Procedure

1. Go to Ranger Admin Web UI Audit Access .
2. Check the Exclude Service Users box, as shown in:

Figure 16: Setting the Exclude Service Users flag to true



Exclude Service Users: ☑

Last Updated Time: 05/24/2023 02:32:52 PM | Entries: 0

Policy ID	Policy Version	Event Time ▼	Application	User	Service (Name / Type)	Resource (Name / Type)	Access Type
							"No data to sho

3. Define specific component services and users for access logs to filter out, in ranger-admin-site.xml.
   a) Go to Cloudera Manager Ranger Configuration
   b) In Search, type ranger-admin-site.
   c) Define the following properties:

      Name

      ranger.plugins.<service_name>.serviceuser

      Value

      <service_name>

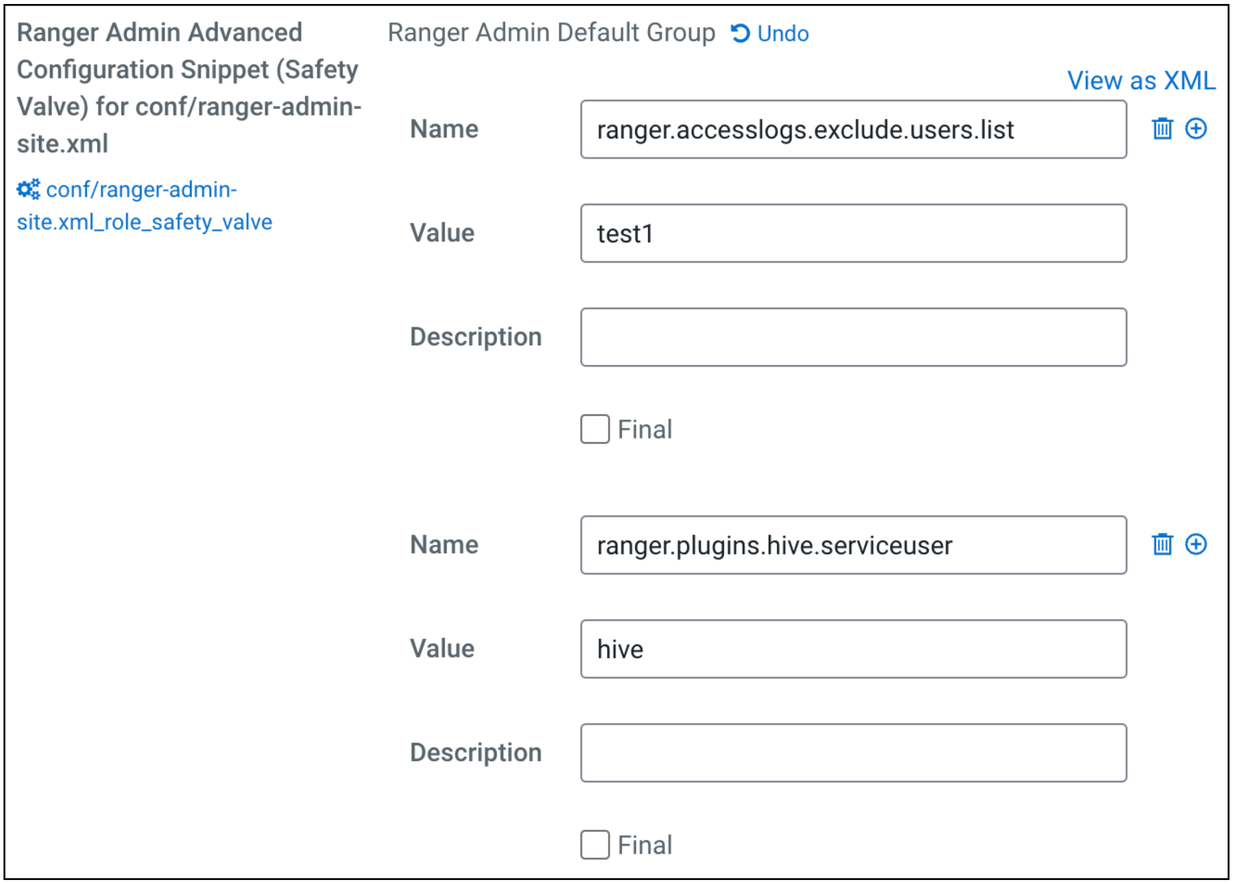
      Name

      ranger.accesslogs.exclude.users.list

      Value

      user1, user2

Figure 17: Filtering out service and user logs for Hive service



Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml

conf/ranger-admin-site.xml_role_safety_valve

Ranger Admin Default Group

Name: ranger.accesslogs.exclude.users.list

Value: test1

Description:

□ Final

Name: ranger.plugins.hive.serviceuser

Value: hive

Description:

□ Final

4. Click Save Changes (CTRL+S).
5. Restart the Ranger service.

Results

Setting Exclude Service Users to true and defining specific filtering properties prevents audit logs from service users from appearing on Ranger Admin Web UI Audit Access , but does NOT prevent access logs for service users from being generated in Solr.

Excluding audits for specific users, groups, and roles

You can exclude audit records for specific users, groups, and roles from each service from appearing in the Ranger UI.

About this task

Ranger default log functionality creates audit log records for access and authorization requests, specifically around service accounts such as hbase, atlas and solr. Writing so much data to solr can limit the availability of Solr for further usage. This topic describes how to exclude audit records for specific users, groups, and roles from each service from appearing in the Ranger UI. Excluding specific users, groups or roles is also known as creating a blacklist for Ranger audits.

Procedure

1. In the Ranger Admin Web UI Service Manager , click Add New Service or Edit (existing service).
2. On Create/Edit Service, scroll down to Config Properties Add New Configurations .
3. Remove all audit filters from the existing service.

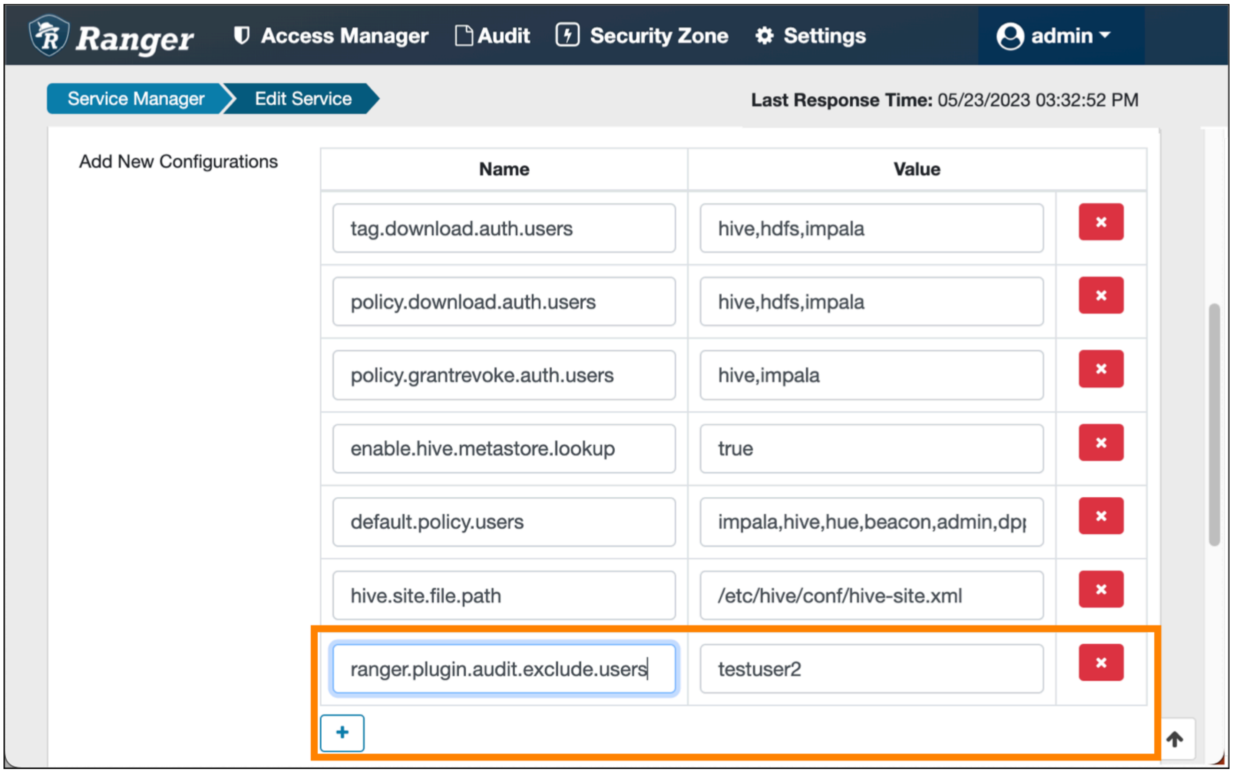
4. Click +, then type one of the following property names:

   - ranger.plugin.audit.exclude.users
   - ranger.plugin.audit.exclude.groups
   - ranger.plugin.audit.exclude.roles

   followed by one or more values.

   Note: You can include multiple values for each exclude property using a comma-separated list.

Figure 18: Adding an exclude users property to the HadoopSQL service



Last Response Time: 05/23/2023 03:32:52 PM

Add New Configurations

Name	Value
tag.download.auth.users	hive,hdfs,impala
policy.download.auth.users	hive,hdfs,impala
policy.grantrevoke.auth.users	hive,impala
enable.hive.metastore.lookup	true
default.policy.users	impala,hive,hue,beacon,admin,dp
hive.site.file.path	/etc/hive/conf/hive-site.xml
ranger.plugin.audit.exclude.users	testuser2

After adding the above configuration; if testuser2 user performs any actions for HadoopSQL service, Audit Access logs will not appear in the Ranger UI, but are still sent to Solr.

Similarly, you can exclude (or blacklist) users belonging to a particular group or role by adding a user-specific or role-specific configuration.

Configuring Ranger audits to show actual client IP address

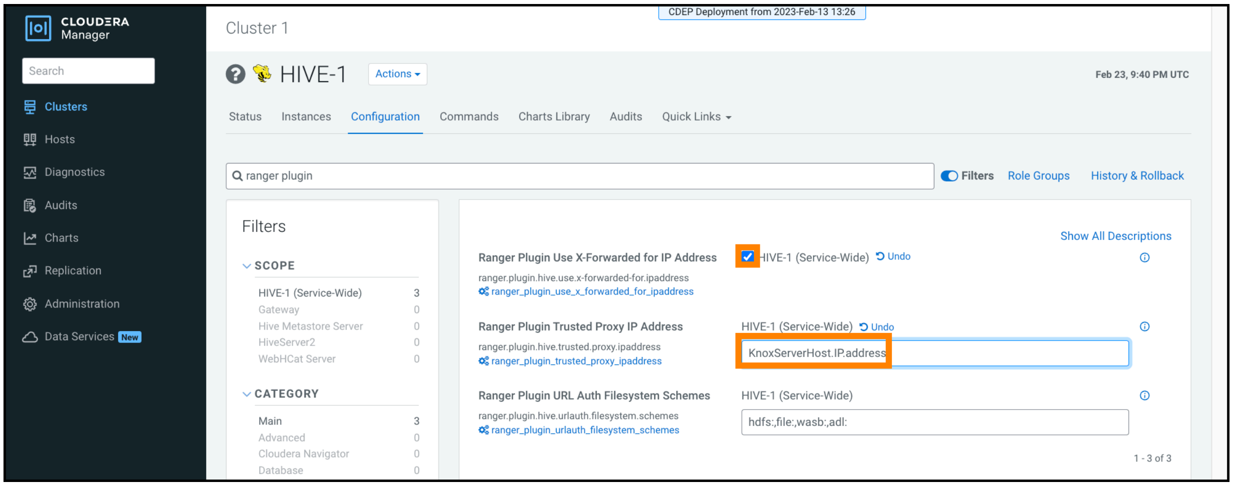
How to forward the actual client IP address to audit logs generated from a Ranger plugin.

About this task

Ranger audit logs record the IP address through which Ranger policies grant/authorize access. When Ranger is set up behind a Knox proxy server, the proxy server IP address appears in the audit logs generated for each Ranger plugin. You can configure each plugin to forward the actual client IP address on which that service runs, so that the audit logs for that service more specifically reflect access/authorization activity. You must configure each plugin individually. This topic uses the Hive (Hadoop SQL) service as an example.

Procedure

1. From Cloudera Manager choose <service_name> Configuration .
2. In <service_name> Configuration Search , type ranger-plugin, then press Return.
3. In Ranger Plugin Use X-Forwarded for IP Address, check the box.
4. In Ranger Plugin Trusted Proxy IP Address, type the IP address of the Knox proxy server host.



ranger plugin

Ranger Plugin Use X-Forwarded for IP Address
ranger.plugin.hive.use.x-forwarded-for.ipaddress
ranger_plugin_use_x_forwarded_for_ipaddress
☑ HIVE-1 (Service-Wide)

Ranger Plugin Trusted Proxy IP Address
ranger.plugin.hive.trusted.proxy.ipaddress
ranger_plugin_trusted_proxy_ipaddress
HIVE-1 (Service-Wide): KnoxServerHost.IP.address

Ranger Plugin URL Auth Filesystem Schemes
ranger.plugin.hive.urlauth.filesystem.schemes
ranger_plugin_urlauth_filesystem_schemes
HIVE-1 (Service-Wide): hdfs:,file:,wasb:,adl:

Results

Hive audit logs will now show the IP address of the host on which Hive service runs.