Cloudera Runtime 7.2.13

Ranger Auditing

Date published: 2020-07-28
Date modified: 2021-12-13

CLOUDERA

https://docs.cloudera.com/

Legal Notice

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.

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.

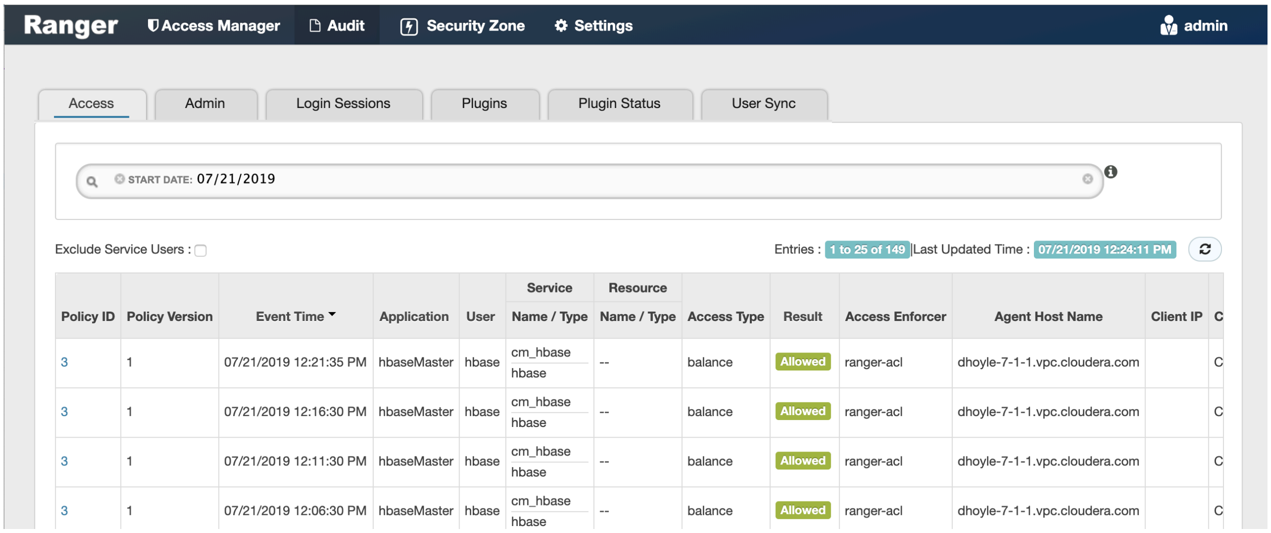
Contents

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

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



START DATE: 07/21/2019

Exclude Service Users : □

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

					Service	Resource						
Policy ID	Policy Version	Event Time	Application	User	Name / Type	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

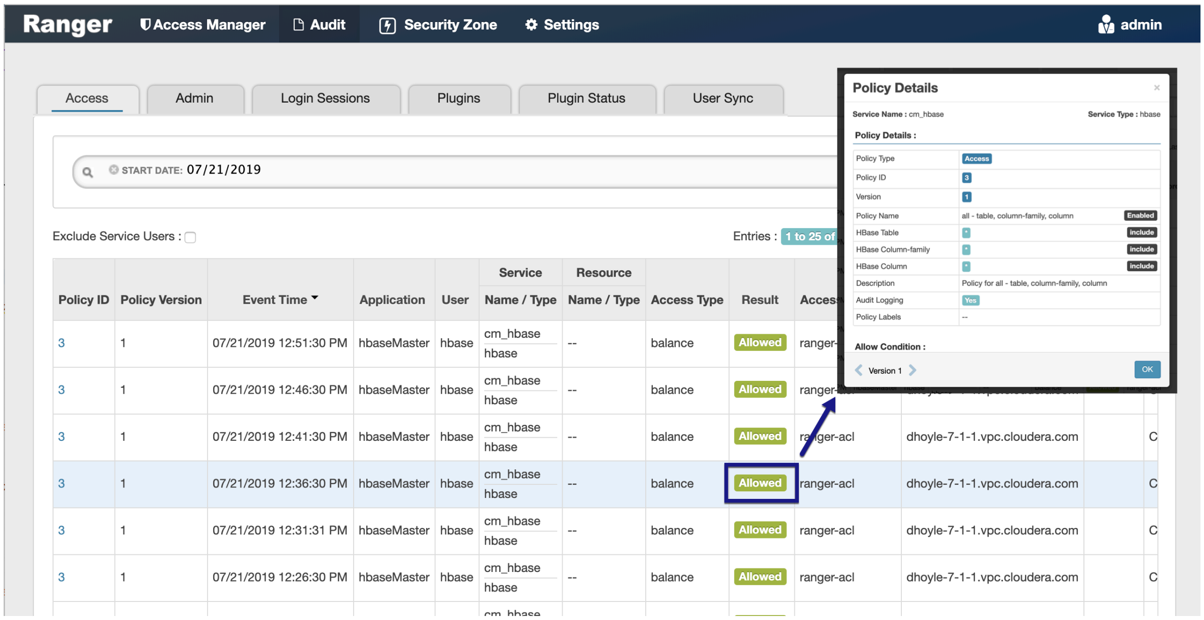
View audit details

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



START DATE: 07/21/2019

Exclude Service Users : □

Entries : 1 to 25 of

Policy ID	Policy Version	Event Time	Application	User	Service Name / Type	Resource Name / Type	Access Type	Result	Acces			
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		C
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		C
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		C
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		C
					cm_hbase							

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	* include
HBase Column-family	* include
HBase Column	* include
Description	Policy for all - table, column-family, column
Audit Logging	Yes
Policy Labels	--

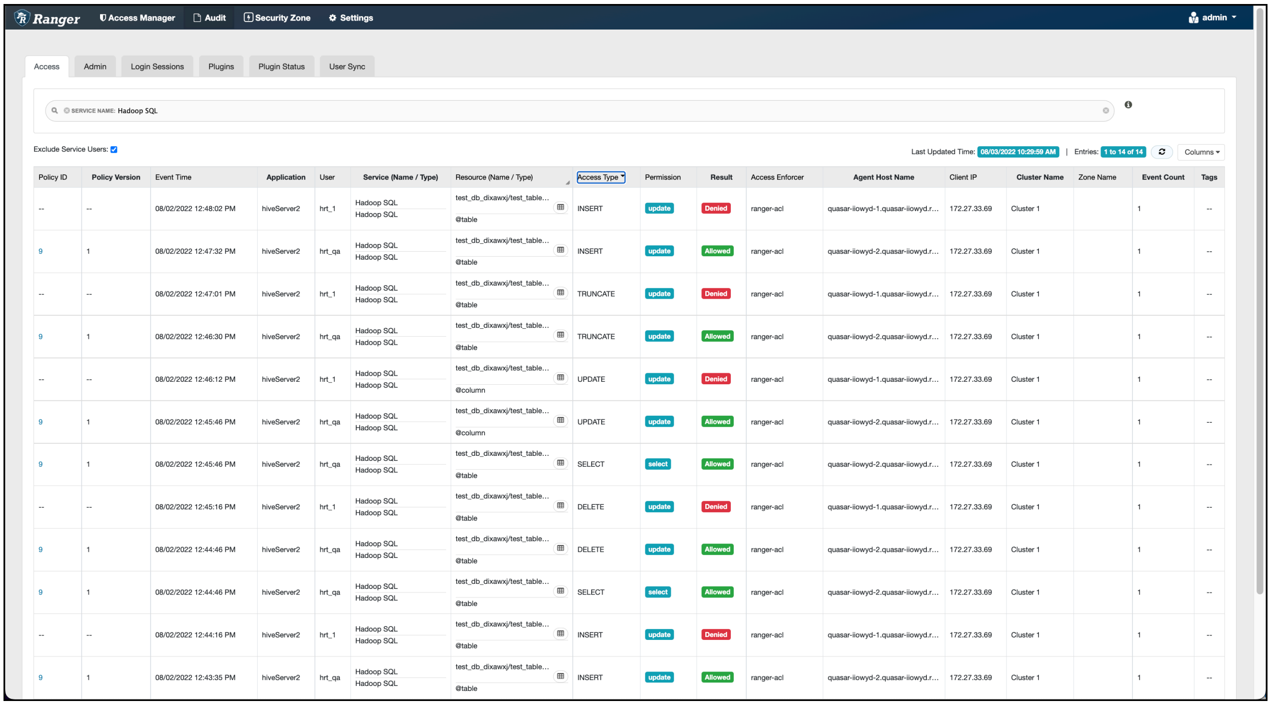
Allow Condition :

Version 1

OK

Audit > Access: HadoopSQL

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



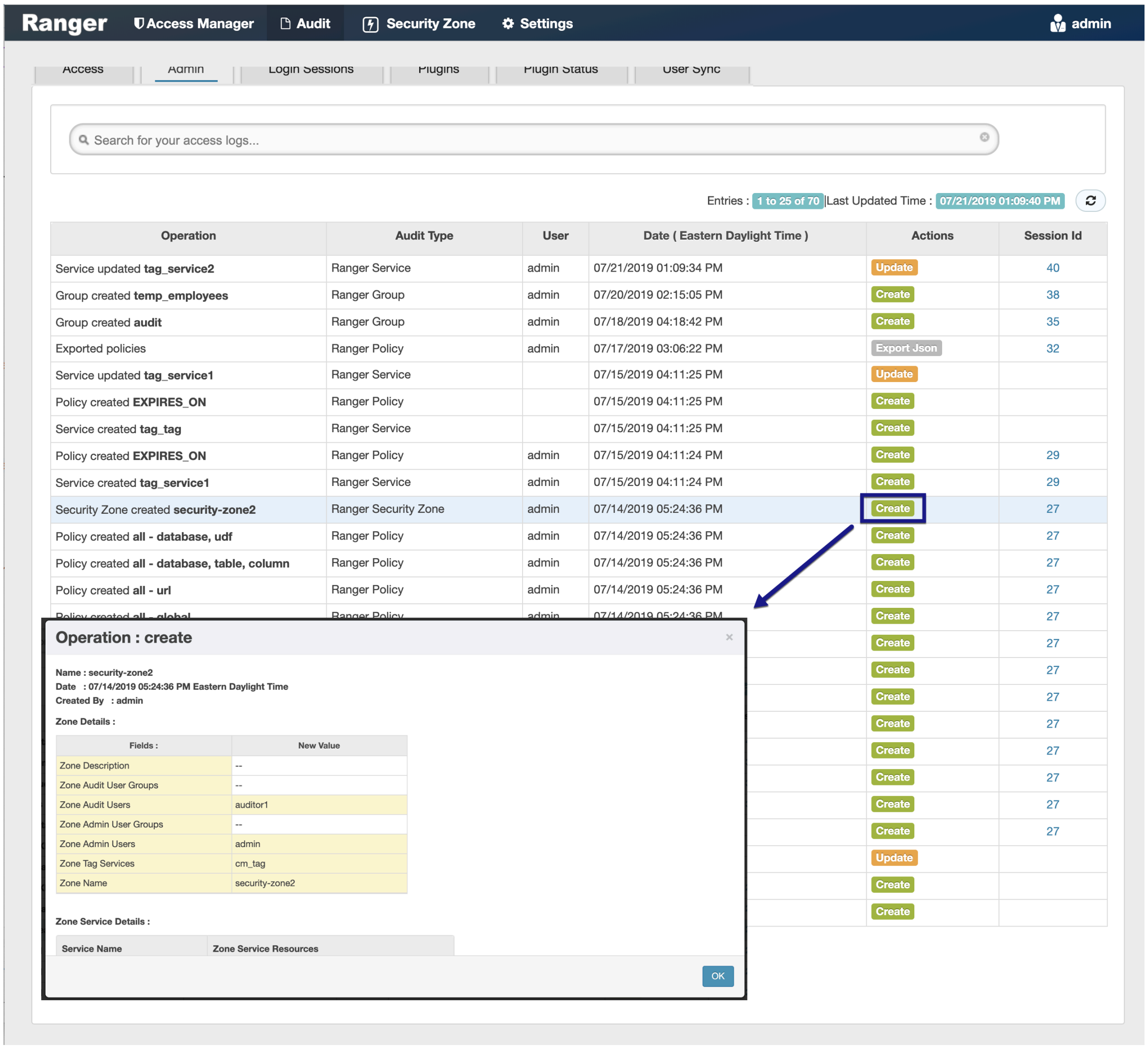
SERVICE NAME: Hadoop SQL

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



Entries : 1 to 25 of 70 |Last Updated Time : 07/21/2019 01:09:40 PM

Operation	Audit Type	User	Date (Eastern Daylight Time)	Actions	Session Id
Service updated **tag_service2**	Ranger Service	admin	07/21/2019 01:09:34 PM	Update	40
Group created **temp_employees**	Ranger Group	admin	07/20/2019 02:15:05 PM	Create	38
Group created **audit**	Ranger Group	admin	07/18/2019 04:18:42 PM	Create	35
Exported policies	Ranger Policy	admin	07/17/2019 03:06:22 PM	Export Json	32
Service updated **tag_service1**	Ranger Service		07/15/2019 04:11:25 PM	Update	
Policy created **EXPIRES_ON**	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Service created **tag_tag**	Ranger Service		07/15/2019 04:11:25 PM	Create	
Policy created **EXPIRES_ON**	Ranger Policy	admin	07/15/2019 04:11:24 PM	Create	29
Service created **tag_service1**	Ranger Service	admin	07/15/2019 04:11:24 PM	Create	29
Security Zone created **security-zone2**	Ranger Security Zone	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - database, udf**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - database, table, column**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - url**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - global**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Update	
				Create	
				Create	

Operation : create

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

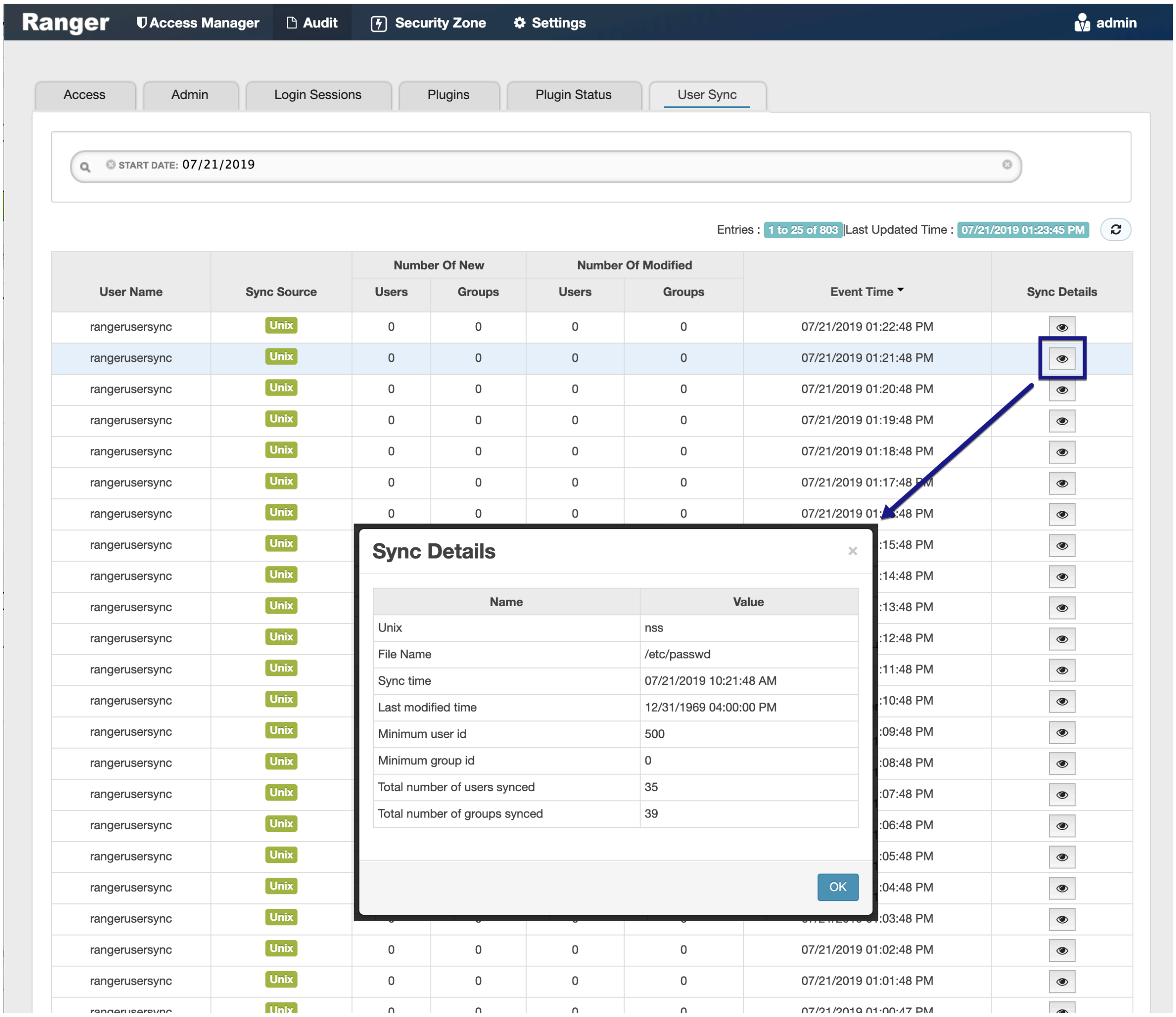
Zone Details :

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

Audit > User Sync: Sync details



Entries : 1 to 25 of 803 |Last Updated Time : 07/21/2019 01:23:45 PM

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

Sync Details

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

OK

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.

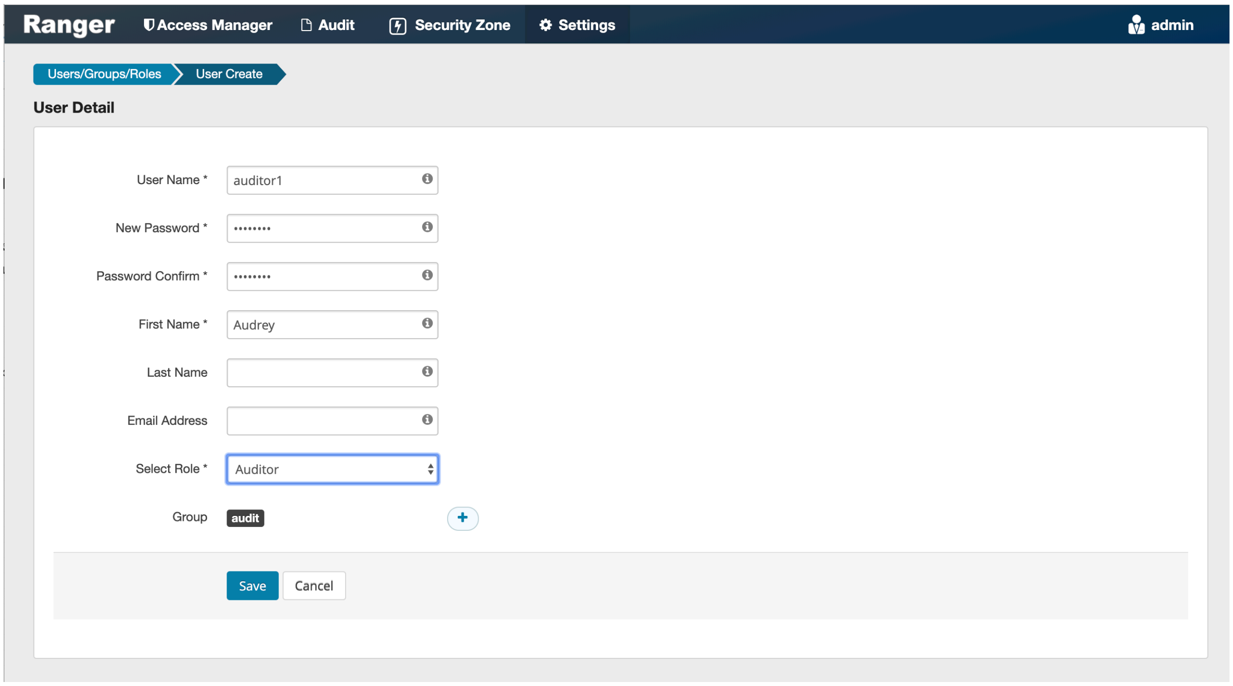
About this task

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:



User Detail

User Name * auditor1

New Password * ••••••••

Password Confirm * ••••••••

First Name * Audrey

Last Name

Email Address

Select Role * Auditor

Group audit

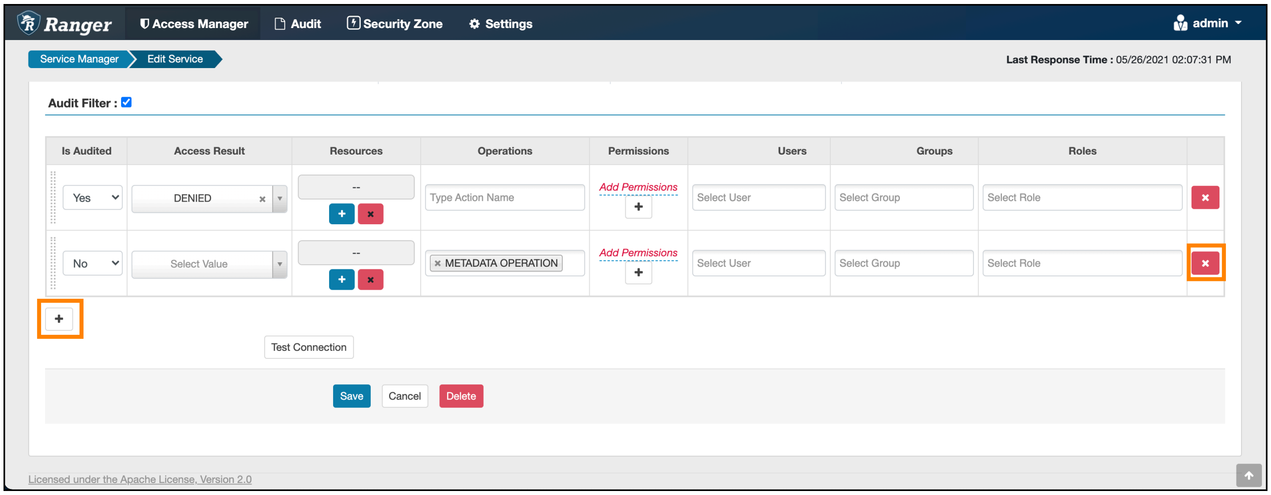
4. Click Save.

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 the in the Ranger Admin web UI Service Manager   Edit Service when you scroll down to Audit Filter. Audit filter is checked (visible) 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 the Hadoop SQL service.



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

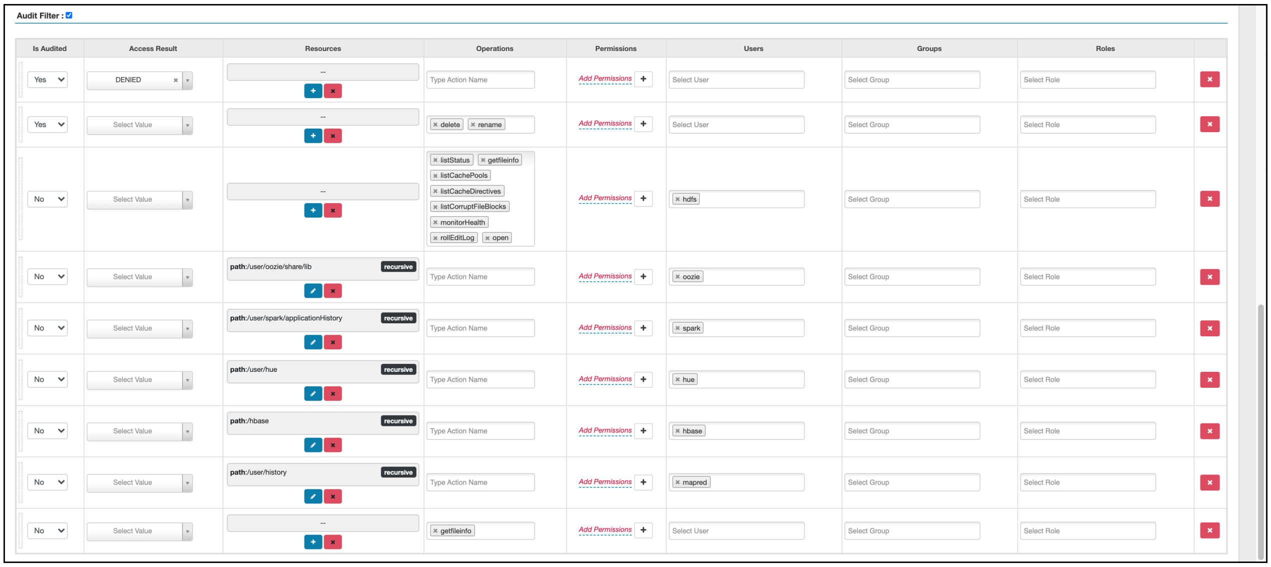
Audit Filter : ☑

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 audit filters

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

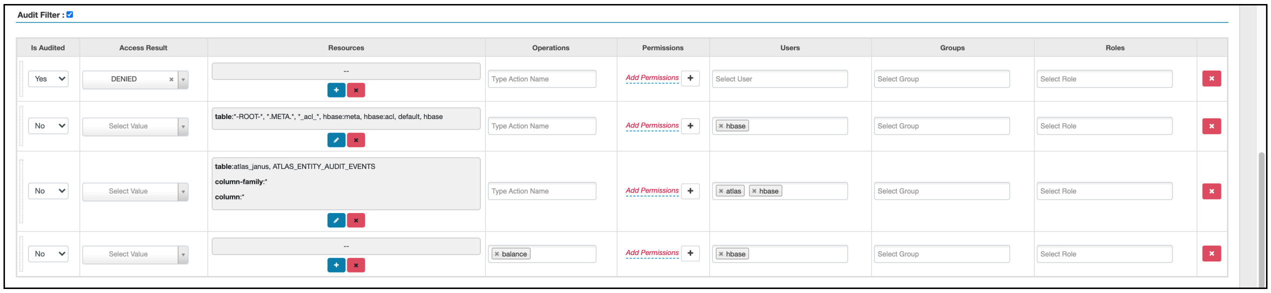
HDFS service:



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

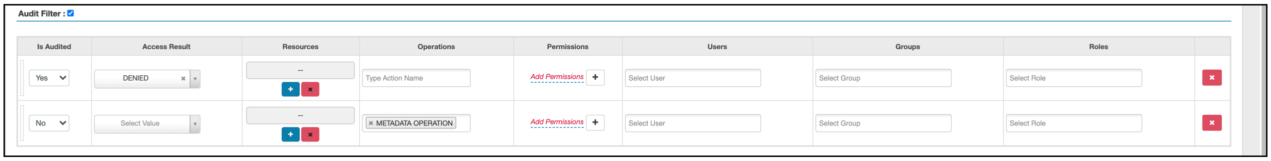
HBase service:



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

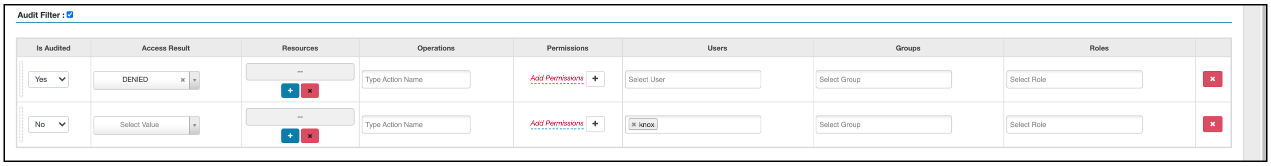
Hadoop SQL service:



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

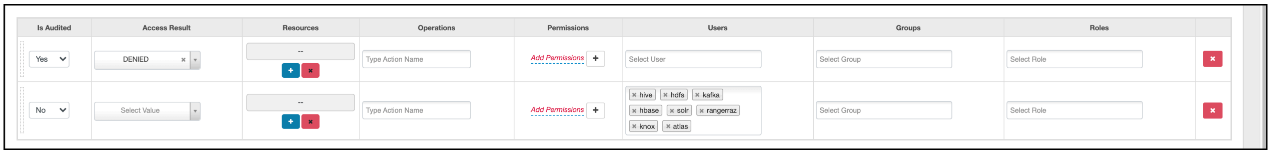
Knox service



Audit Filter : ☑

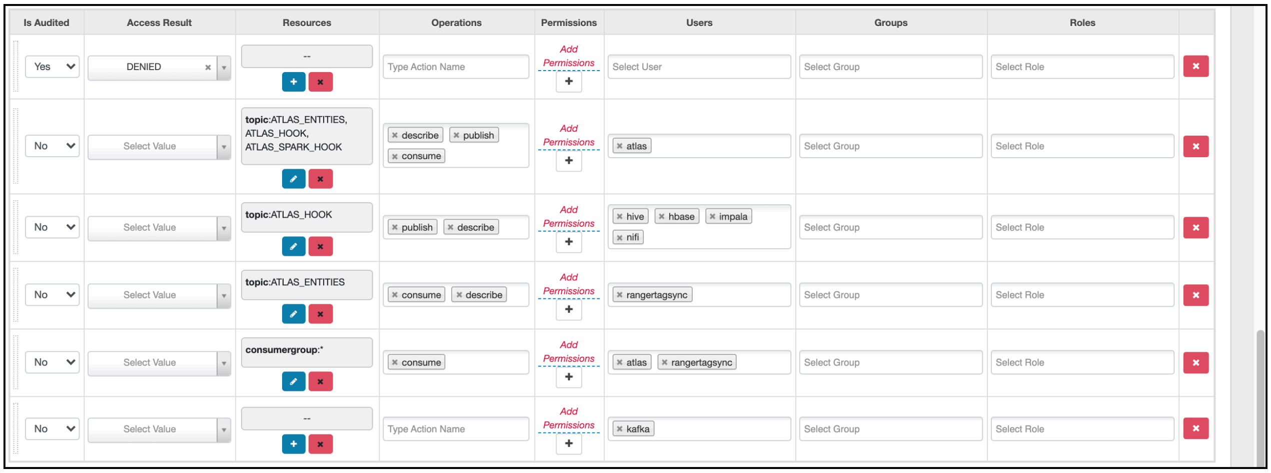
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	knox	Select Group	Select Role

Solr service



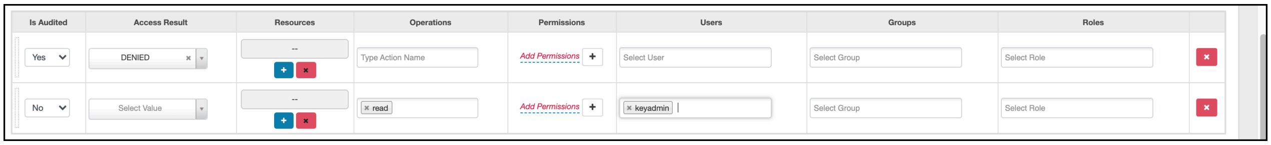
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	hive hdfs kafka hbase solr rangerraz knox atlas	Select Group	Select Role

Kafka service:



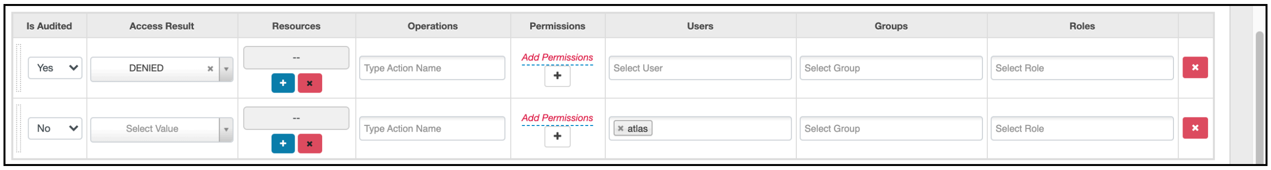
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	topic:ATLAS_ENTITIES, ATLAS_HOOK, ATLAS_SPARK_HOOK	describe publish consume	Add Permissions	atlas	Select Group	Select Role
No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

KMS service



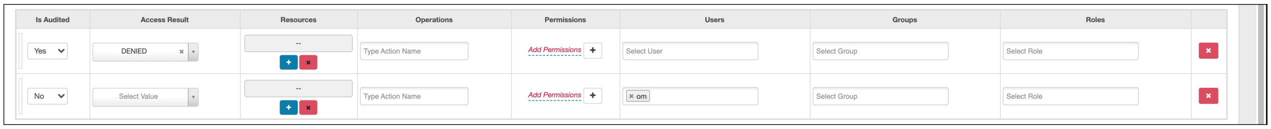
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	read	Add Permissions	keyadmin	Select Group	Select Role

Atlas service



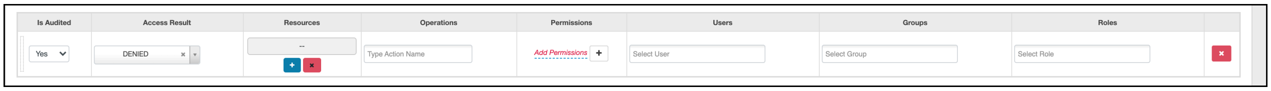
Is Audited	Access Result	Resources	Operations	Permissions	Users	Groups	Roles
Yes	DENIED	--	Type Action Name	Add Permissions	Select User	Select Group	Select Role
No	Select Value	--	Type Action Name	Add Permissions	atlas	Select Group	Select Role

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

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	×

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

Ranger audit filter policy configuration

To configure an audit filter policy, click the Edit icon for either a resource-, or tag-based service in the Ranger Admin web UI. You configure a Ranger audit filter policy by adding (+), deleting (X), or modifying each audit filter row for the service. The preceding example shows the Add and Delete icons for each filter row. To configure each filter in the policy, 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

1. Click + in Permissions to open the Add dialog.
2. 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}
  ```