

HDP Security Audit Reference 3

Audit Reference

Date of Publish: 2018-07-15

<http://docs.hortonworks.com>

Contents

| | |
|---|----------|
| Managing Auditing in Ranger: Access..... | 3 |
| Managing Auditing in Ranger: Admin..... | 4 |
| Managing Auditing in Ranger: Login Sessions..... | 5 |
| Managing Auditing in Ranger: Plugins..... | 6 |
| Managing Auditing in Ranger: Plugin Status..... | 7 |
| Managing Auditing in Ranger User Sync..... | 8 |

Managing Auditing in Ranger: Access

In Ranger, the Access page provides service activity data for all Policies that have Audit set to On. The default service Policy is configured to log all user activity within the Service. This default policy does not contain user and group access rules.

You can filter the data based on the following criteria:

Table 1: Search Criteria

| Search Criteria | Description |
|----------------------|---|
| Access Enforcer | Ranger (ranger-acl) or Hadoop (hadoop-acl) |
| Access Type | Type of access user attempted (E.G., REVOKE, GRANT, OPEN, USE). |
| Client IP | IP address of the user system that tried to access the resource. |
| Result | Shows whether the operation was successful or not. |
| Service Name / Type | The name and type of the service that the user tried to access. |
| Resource Name / Type | The resource name and type of the service that the user tried to access. For Hive events, this field will display the Hive query the user ran. |
| Start Date, End Date | Filters results for a particular date range. |
| User | Name of the user which tried to access the resource. |
| Cluster Name | Cluster name. Can be defined under Ambari>component>Configs>Advanced>ranger-component-audit file, using <code>ranger.plugin.component.ambari.cluster.name=cluster_name</code> . |

Ranger Access page:

| Policy ID | Event Time | User | Service Name / Type | Resource Name / Type | Access Type | Result | Access Enforcer | Client IP | Cluster Name | Event Count | Tags |
|-----------|------------------------|-------|-------------------------|--------------------------------|--------------|---------|-----------------|---------------|--------------|-------------|------|
| 11 | 08/16/2018 10:41:02 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |
| 11 | 08/16/2018 10:40:57 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |
| 11 | 08/16/2018 10:40:52 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |
| -- | 08/16/2018 10:40:49 AM | yarn | dwweekly_hadoop hdfs | /ats/active path | READ_EXECUTE | Allowed | hadoop-acl | 172.26.240.89 | dwweekly | 1 | -- |
| 11 | 08/16/2018 10:40:47 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |
| 11 | 08/16/2018 10:40:42 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |
| 11 | 08/16/2018 10:40:37 AM | atlas | dwweekly_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 172.26.240.89 | dwweekly | 2 | -- |

Ranger Access showing tag attribute details:

| | | | | | | | | | | |
|---|------------------------|------|--------------|---|--------|---------|------------|---------------|---|---|
| 2 | 04/25/2017 02:24:03 PM | hive | clu_tag_hive | | USE | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 2 | 04/25/2017 12:19:22 PM | hive | clu_tag_hive | | USE | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 2 | 04/25/2017 06:05:59 PM | hive | clu_tag_hive | finance/tax_2010/fed_tax/local_ta_@column | SELECT | Allowed | ranger-aci | 172.22.107.16 | 1 | Attribute Details Key Value expiry date 12/12/2012 time 10:10PM seconds 1000100 |
| 2 | 04/25/2017 06:05:51 PM | hive | clu_tag_hive | finance/tax_2010/ssn | SELECT | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 2 | 04/25/2017 05:49:57 PM | hive | clu_tag_hive | finance/tax_2010/fed_tax/local_ta_@column | SELECT | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 2 | 04/25/2017 05:49:19 PM | hive | clu_tag_hive | finance/tax_2010/ssn | SELECT | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 4 | 04/25/2017 05:46:59 PM | hive | clu_tag_hive | hr/employee/ssn | SELECT | Denied | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 2 | 04/25/2017 05:46:54 PM | hive | clu_tag_hive | finance/tax_2010/ssn | SELECT | Allowed | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |
| 4 | 04/25/2017 04:55:51 PM | hive | clu_tag_hive | hr/employee/ssn | SELECT | Denied | ranger-aci | 172.22.107.16 | 1 | EXPRES_ON , EXP , PII |

Ranger Access showing user 'unixuser1' running a Hive query:

The screenshot shows the Ranger Admin interface with the 'Audit' tab selected. The search filters are set to 'START DATE: 08/16/2018' and 'SERVICE TYPE: HIVE'. The table below shows audit events for user 'unixuser1'.

| Policy ID | Event Time | User | Service Name / Type | Operation | Result | Access Enforcer | Client IP | Cluster Name | Event Count | Tags |
|-----------|------------------------|-----------|---------------------|-----------|---------|-----------------|---------------|--------------|-------------|------|
| 20 | 08/16/2018 10:38:01 AM | unixuser1 | dwweekly_hive | USE | Allowed | ranger-aci | 172.26.240.89 | dwweekly | 1 | -- |
| 20 | 08/16/2018 10:37:26 AM | unixuser1 | dwweekly_hive | UPDATE | Allowed | ranger-aci | 172.26.240.89 | dwweekly | 1 | -- |
| 20 | 08/16/2018 10:19:35 AM | unixuser1 | dwweekly_hive | USE | Allowed | ranger-aci | 172.26.240.89 | dwweekly | 1 | -- |
| 15 | 08/16/2018 10:18:27 AM | hive | dwweekly_hive | USE | Allowed | ranger-aci | 172.26.240.89 | dwweekly | 1 | -- |
| 15 | 08/16/2018 10:18:24 AM | hive | dwweekly_hive | USE | Allowed | ranger-aci | 172.26.240.89 | dwweekly | 1 | -- |

The tooltip for the UPDATE event shows the following Hive query:

```
INSERT INTO TABLE students3 VALUES ('malcolm reynolds', 31, 1.28), ('kvothe reshi', 18, 4.00), ('rob stark', 25, 3.58), ('aretha franklin', 76, 3.28)
```

Managing Auditing in Ranger: Admin

In Ranger, the Admin tab contains all events for the auditing HDP Security Administration Web UI, including Service, Service Manager, Log in, etc. (actions like create, update, delete, password change).

The screenshot shows the Ranger Admin interface with the 'Admin' tab selected. The search bar contains the text 'Search for your access logs...'. The table below shows a list of audit events.

| Operation | Audit Type | User | Date (PST) | Actions | Session Id |
|---|----------------|-------|------------------------|---------|------------|
| Policy updated hbase-test-1-20160202224138 | Ranger Policy | Mal | 02/16/2016 09:51:42 AM | update | 52509 |
| Policy updated Example-Service-1-20160211205602 | Ranger Policy | admin | 02/11/2016 12:56:48 PM | update | 52478 |
| Service updated Example-Service | Ranger Service | admin | 02/11/2016 12:56:34 PM | update | 52478 |
| Policy created New-Service-1-20160211205602 | Ranger Policy | admin | 02/11/2016 12:56:02 PM | create | 52478 |
| Service created New-Service | Ranger Service | admin | 02/11/2016 12:56:02 PM | create | 52478 |
| Policy updated hbase-test-1-20160202224138 | Ranger Policy | admin | 02/11/2016 10:27:15 AM | update | 52461 |
| User updated Mal | XA User | admin | 02/11/2016 10:26:06 AM | update | 52461 |
| Group created UX | XA Group | admin | 02/11/2016 10:25:21 AM | create | 52461 |
| Policy created test-storm-1-20160211016740 | Ranger Policy | admin | 02/10/2016 05:07:40 PM | create | 52391 |

You can filter the data based on the following criteria:

Table 2: Search Criteria

| Search Criteria | Description |
|-----------------|--|
| Action | These are operations performed on resources (actions like create, update, delete, password change). |
| Audit Type | There are three values Resource,asset and xa user according to operations performed on Service,policy and users. |
| End Date | Login time and date is stored for each session. A date range is used to filter the results for that particular date range. |
| Session ID | The session count increments each time you try to login to the system |
| Start Date | Login time and date is stored for each session. A date range is used to filter the results for that particular date range. |
| User | Username who has performed create,update,delete operation. |

Managing Auditing in Ranger: Login Sessions

In Ranger, the Login Sessions tab logs the information related to the sessions for each login.

You can filter the data based on the following criteria:

Table 3: Search Criteria

| Search Criteria | Description |
|----------------------|--|
| Login ID | The username through which someone logs in to the system. |
| Session-id | The session count increments each time the user tries to log into the system. |
| Start Date, End Date | Specifies that results should be filtered based on a particular start date and end date. |
| Login Type | The mode through which the user tries to login (by entering username and password). |
| IP | The IP address of the system through which the user logged in. |
| User Agent | The browser or library version used to login for the specific event (e.g. Mozilla, Java, Python) |
| Result | Logs whether or not the login was successful. Possible results can be Success, Wrong Password, Account Disabled, Locked, Password Expired or User Not Found. |

| Session Id | Login Id | Result | Login Type | IP | User Agent | Login Time (PST) |
|------------|------------------|---------|-------------------|----------------|-----------------------------------|------------------------|
| 52329 | amb_ranger_admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 12:50:32 PM |
| 52328 | admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 12:50:32 PM |
| 52327 | admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 12:50:32 PM |
| 52326 | admin | Success | Username/Password | 192.168.64.1 | Mozilla/5.0 (Macintosh; Intel ... | 02/09/2016 12:39:38 PM |
| 52325 | amb_ranger_admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 10:50:32 AM |
| 52324 | admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 10:50:32 AM |
| 52323 | admin | Success | Username/Password | 192.168.64.101 | Python-urllib/2.6 | 02/09/2016 10:50:32 AM |
| 52322 | rangerusersync | Success | Username/Password | 192.168.64.101 | Java/1.8.0_60 | 02/09/2016 10:21:22 AM |
| 52321 | rangerusersync | Success | Username/Password | 192.168.64.101 | Java/1.8.0_60 | 02/09/2016 10:21:21 AM |
| 52320 | rangerusersync | Success | Username/Password | 192.168.64.101 | Java/1.8.0_60 | 02/09/2016 10:21:21 AM |
| 52319 | rangerusersync | Success | Username/Password | 192.168.64.101 | Java/1.8.0_60 | 02/09/2016 10:21:21 AM |

Managing Auditing in Ranger: Plugins

In Ranger, the Plugins tab shows the upload history of the Security Agents. This module displays all of the services exported from the system.

You can filter the data based on the following criteria:

Table 4: Agents Search Criteria

| Search Criteria | Description |
|----------------------|---|
| Plugin IP | IP Address of the agent that tried to export the service. |
| Plugin ID | Name of the agent that tried to export the service. |
| HTTP Response Code | The HTTP code returned when trying to export the service. |
| Start Date, End Date | Export time and date is stored for each agent. A date range is used to filter the results for that particular date range. |
| Service Name | The service name we are trying to export. |
| Cluster Name | Cluster name. Can be defined under Ambari>component>Configs>Advanced>ranger-component-audit file, using <code>ranger.plugin.component.ambari.cluster.name=cluster_name</code> . |

The screenshot shows the Ranger web interface with the 'Plugin Status' tab selected. A search bar is at the top. Below it is a table with columns: Export Date (PST) *, Service Name, Plugin Id, Plugin IP, Http Response Code, and Status. The status for all entries is 'Policies synced to plugin'.

| Export Date (PST) * | Service Name | Plugin Id | Plugin IP | Http Response Code | Status |
|------------------------|--------------|---|----------------|--------------------|---------------------------|
| 01/05/2017 09:13:09 AM | c6402_hive | hiveServer2@c6402.ambari.apache.org-c6402_hive | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:12:29 AM | c6402_atlas | atlas@c6402.ambari.apache.org-c6402_atlas | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:12:20 AM | c6402_hbase | hbaseRegional@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:12:13 AM | c6402_hbase | hbaseMaster@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:05:19 AM | c6402_hbase | hbaseRegional@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:05:05 AM | c6402_hbase | hbaseMaster@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:03:35 AM | c6402_hive | hiveServer2@c6402.ambari.apache.org-c6402_hive | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:02:48 AM | c6402_hbase | hbaseRegional@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:02:13 AM | c6402_yarn | yarn@c6402.ambari.apache.org-c6402_yarn | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 09:01:02 AM | c6402_hbase | hbaseMaster@c6402.ambari.apache.org-c6402_hbase | 192.168.64.102 | 200 | Policies synced to plugin |
| 01/05/2017 08:59:37 AM | c6402_hadoop | hdfs@c6402.ambari.apache.org-c6402_hadoop | 192.168.64.102 | 200 | Policies synced to plugin |

Managing Auditing in Ranger: Plugin Status

In Ranger, the Plugin Status tab shows policies in effect for each plugin. Includes the relevant host info and when the plugin downloaded and started enforcing the policies.

You can search the data based on the following criteria:

Table 5: Plugin Status Search Criteria

| Search Criteria | Description |
|-----------------|---|
| Host Name | Host, e.g., c6401.ambari.apache.org. |
| Plugin IP | IP Address of the agent that uses the plugin. |
| Service Name | Name of the service that contains the policies, e.g., c6401_yarn. |
| Service Type | Component. |

The screenshot shows the Ranger web interface with the 'Plugin Status' tab selected. A search bar is at the top. Below it is a table with columns: Service Name, Service Type, Host Name, Plugin IP, and two groups of time-based columns: Policy (Time) and Tag (Time). Each group contains Active, Download, and Last Update columns.

| Service Name | Service Type | Host Name | Plugin IP | Policy (Time) | | | Tag (Time) | | |
|--------------|---------------|-------------------------|----------------|------------------------|------------------------|------------------------|--------------|----------|-------------|
| | | | | Active | Download | Last Update | Active | Download | Last Update |
| c6402_atlas | atlas | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 09:12:30 AM | 01/05/2017 09:12:29 AM | 01/05/2017 09:04:33 AM | -- | -- | -- |
| c6402_hadoop | hdfs | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 08:59:39 AM | 01/05/2017 08:59:37 AM | 01/05/2017 08:59:30 AM | -- | -- | -- |
| c6402_hbase | hbaseMaster | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 09:12:13 AM | 01/05/2017 09:12:13 AM | 01/05/2017 09:11:53 AM | -- | -- | -- |
| c6402_hbase | hbaseRegional | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 09:12:20 AM | 01/05/2017 09:12:20 AM | 01/05/2017 09:11:53 AM | -- | -- | -- |
| c6402_hive | hiveServer2 | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 09:13:09 AM | 01/05/2017 09:13:09 AM | 01/05/2017 09:02:55 AM | -- | -- | -- |
| c6402_yarn | yarn | c6402.ambari.apache.org | 192.168.64.102 | 01/05/2017 09:02:14 AM | 01/05/2017 09:02:13 AM | 01/05/2017 09:02:04 AM | -- | -- | -- |

Managing Auditing in Ranger User Sync

In Ranger, the User Sync page provides service activity data for all usersync processes in Ranger. This creates a compliance/audit trail for users and groups synchronized with each run of usersync.

You can filter the data based on the following criteria:

Table 6: Search Criteria

| Search Criteria | Description |
|----------------------|--|
| Start Date, End Date | Filters results for a particular date range. |
| User Name | Name of the user which tried to access the resource. |
| Sync Source | File, LDAP/AD, or Unix. |