Audit Reference

Date of Publish: 2018-07-15

http://docs.hortonworks.com

Contents

Managing Auditing in Ranger: Access

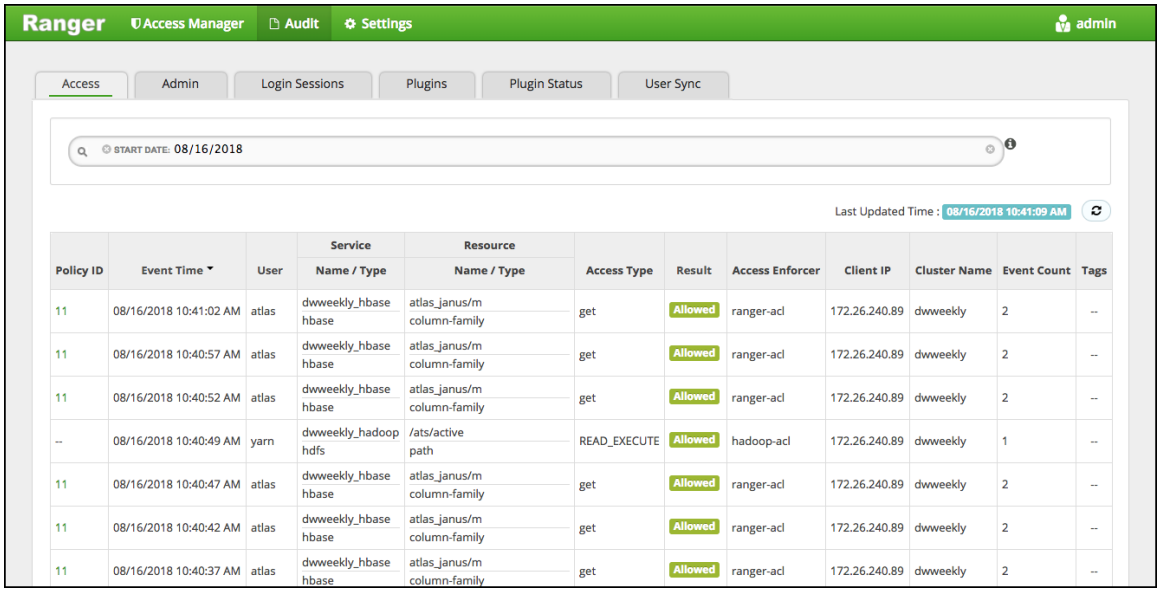
In Ranger, the Access page provides service activity data for all Policies that have Audit set to On. The default service Policy is configured to log all user activity within the Service. This default policy does not contain user and group access rules.

You can filter the data based on the following criteria:

Table 1: Search Criteria

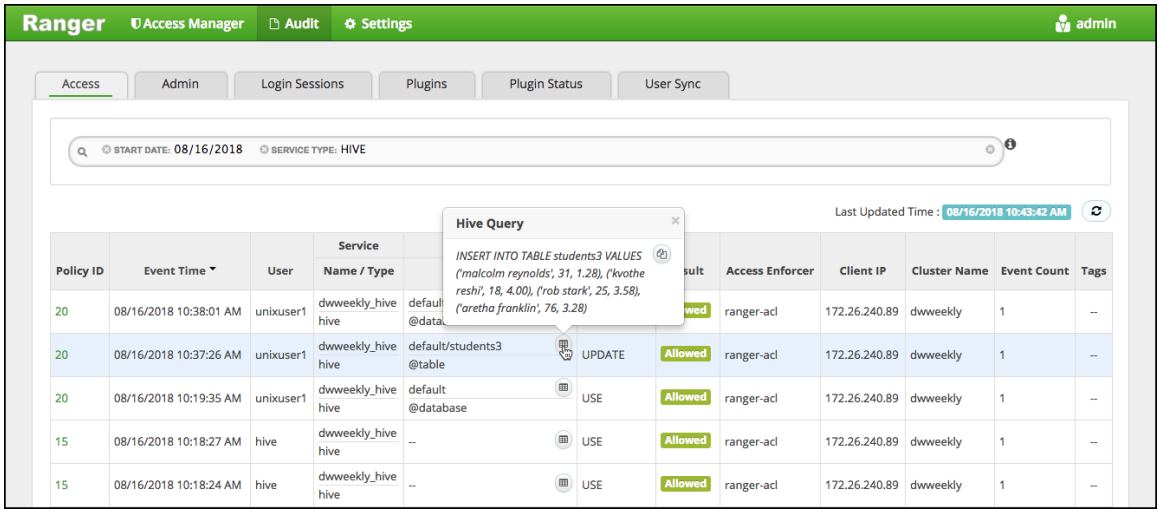
Search Criteria	Description
Access Enforcer	Ranger (ranger-acl) or Hadoop (hadoop-acl)
Access Type	Type of access user attempted (E.G., REVOKE, GRANT, OPEN, USE).
Client IP	IP address of the user system that tried to access the resource.
Result	Shows whether the operation was successful or not.
Service 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 ranger.plugin.component.ambari.cluster.name=cluster_name .

Ranger Access page:



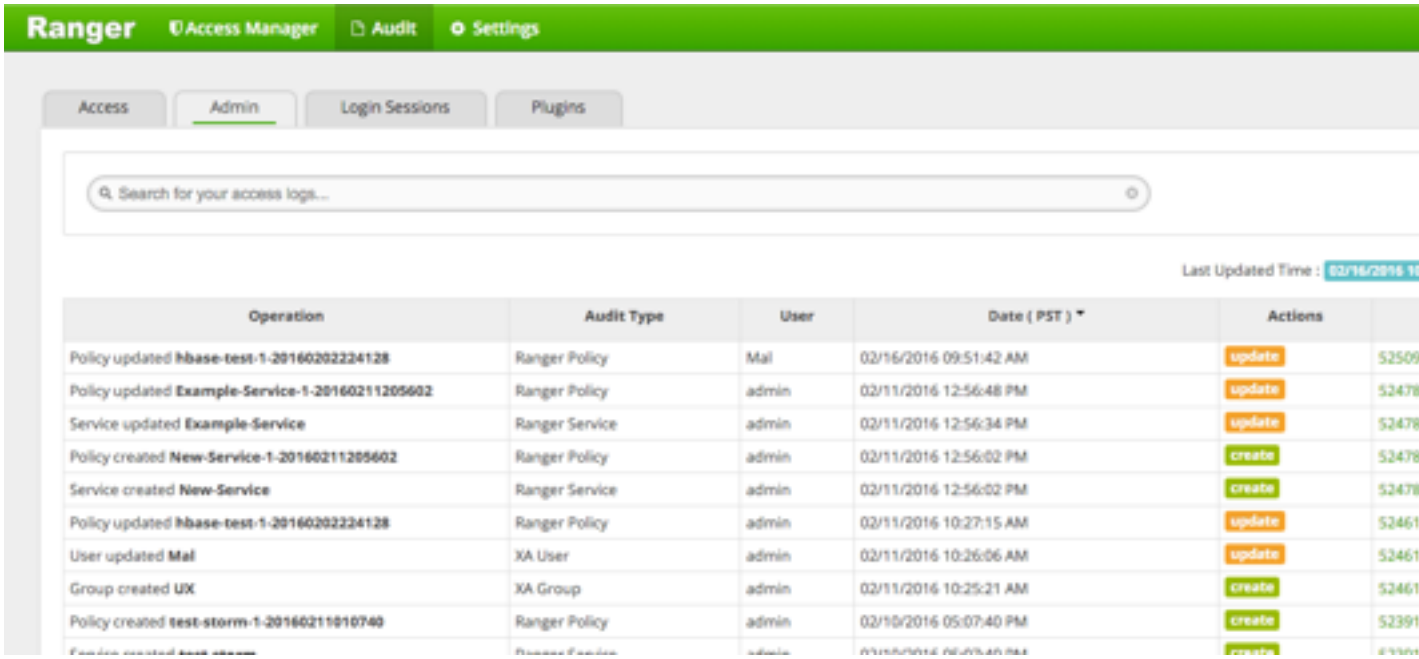
Ranger Access showing tag attribute details:

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



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).



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

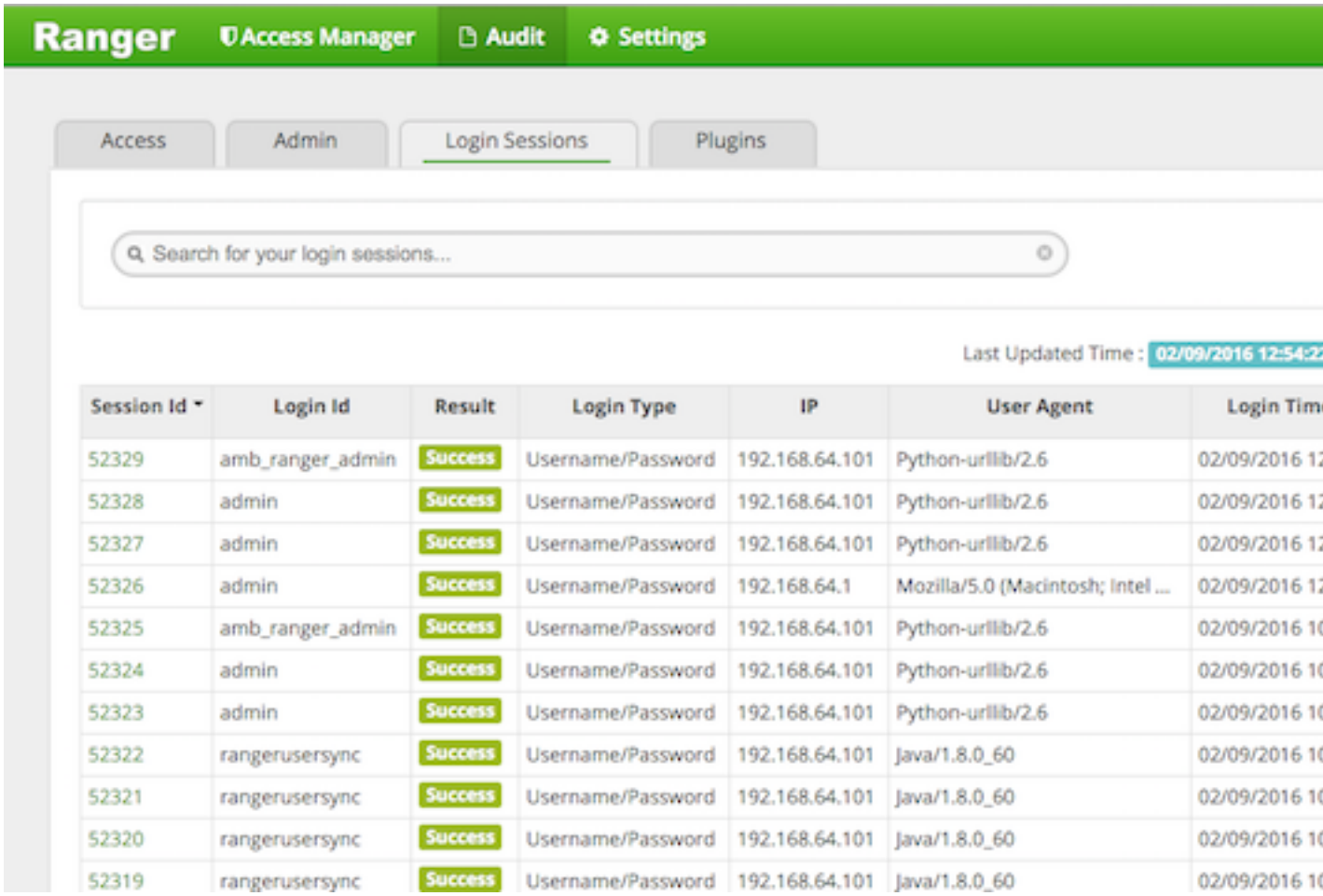
In Ranger, the Login Sessions tab logs the information related to the sessions for each login.

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.

Search Criteria	Description
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.



Managing Auditing in Ranger: Plugins

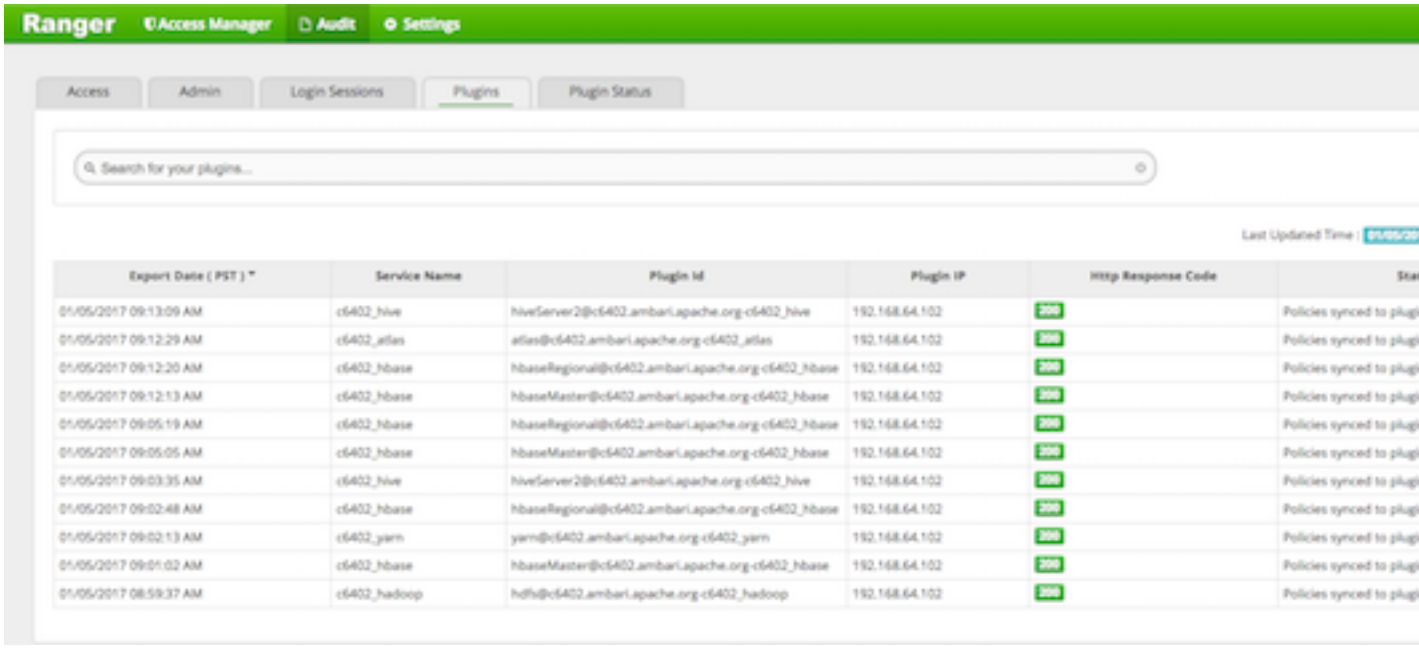
In Ranger, the Plugins tab shows the upload history of the Security Agents.This module displays all of the services exported from the system.

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.

Search Criteria	Description
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 ranger.plugin.component.ambari.cluster.name=cluster_name .



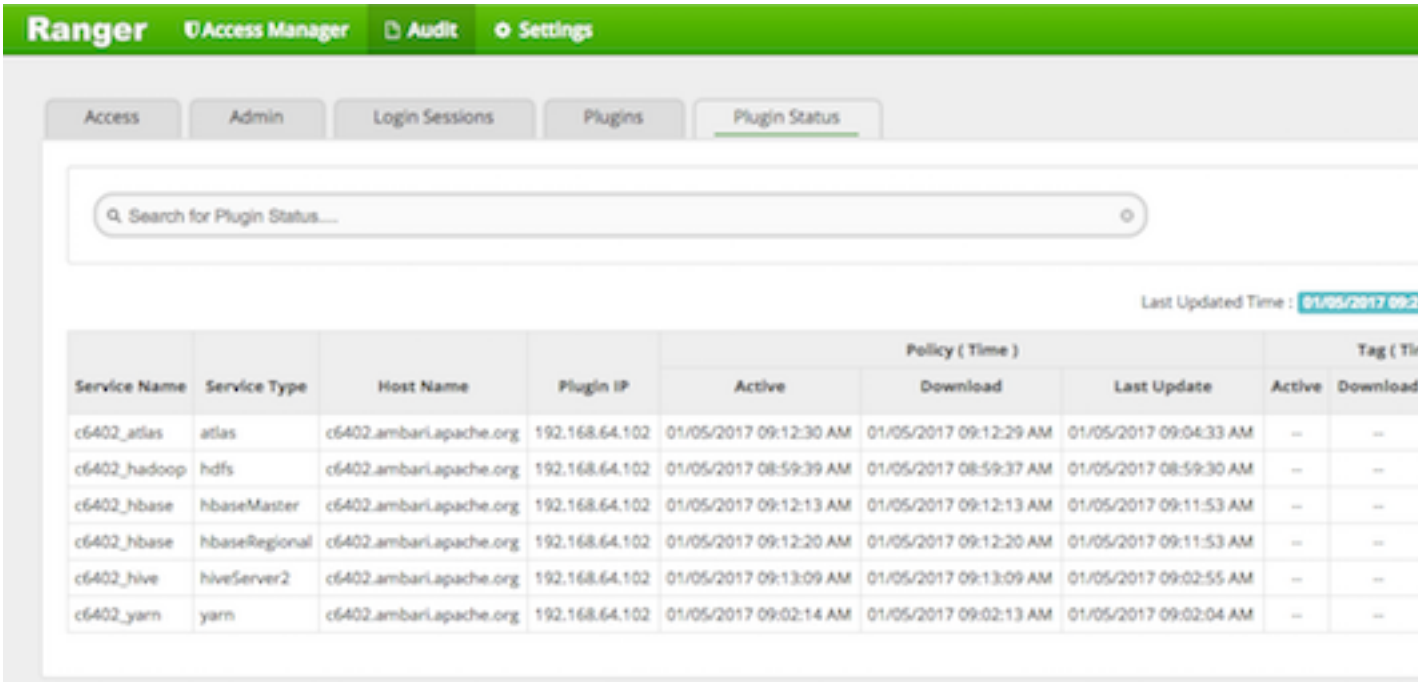
Managing Auditing in Ranger: Plugin Status

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.



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 userync.

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.