1. Introduction

In order to maintain consistency of the object and databases/roles created under sentry and to help users to understand in depth details on how to raise sentry service request. This document shows all the naming standards and process to be followed while raising sentry request.

2. Sentry request links

Please find below the link to service now where we can submit sentry request.

Sentry Service Request

(https://allstate.service-now.com/com.glideapp.servicecatalog_cat_item_view.do?v=1&sysparm_id=43166e49132696006a247dcf3244b064&sysparm_link_parent=adafc69441e474004e89d3a4eb4fad22&sysparm_catalog=e0d08b13c3330100c8b837659bba8fb4&sysparm_catalog_view=catalog_default)

Sentry spreadsheet download link -
Linked spreadsheet
(https://start.allstate.com/sites/Hadoop/Hadoop%20COE%20Documents/Onboarding/Sentry%20Request.xlsx)

3. Naming Standards

3.1 Database Name-

Database name should follow the sentry naming standard as per Allstate.

The database name should represent the application or the intended purpose of the database. While the length of a database name can be 128 characters in length, the recommendation is to keep it short but not too much abbreviated to loose clarity. It should start with a 4 character prefix of one among

a. d<env>a for application databases
b. d<env>u for user databases (allowed only on research QA and research TPT environments)

Where env is one among

d – for Enterprise Development cluster t – for Enterprise Test cluster
p – for Enterprise Production cluster q – For Research QA cluster
r – For Research TPT cluster

Database name should be of the form
d<*env*>a_<*application name*> Application Database, POC, Projects

d<*env*>u_<*ntid*> User Database (Research QA and TPT clusters only, not on Production stack)

Ex- dpa_policymdm, dra_ruff, dqu_rbarr.

3.2 Table Name -

The table/view name should represent the data contained in that table/view. While the length of the table/view name can be 128 characters in length, the recommendation is to keep it short but not too much abbreviated to lose clarity.

For the Production stack of clusters, the table name should start with a prefix of two character TCI code7 of the application and 't_'. For a view, the name should start with the two character TCI code of the application and 'v_'.

<TCI Code>t_xxxxxxxx Tables

<TCI Code>v_xxxxxxxx Views

Example: tyt_drw_trip_summary, tyv_drw_trip_info

3.3 View Name -

Length of the index name can be 128 characters in length 5, the recommendation is to keep it short but not too much abbreviated to lose clarity 6. For the production stack of clusters, the index name should start with a prefix of two character TCI code of the application and 'v_'.
Example: tyv_trip_summary_id

3.4 Index Name

While the length of the index name can be 128 characters in length 5, the recommendation is to keep it short but not too much abbreviated to lose clarity 6. For the production stack of clusters, the index name should start with a prefix of two character TCI code of the application and 'i_'.

Example: tyi_trip_summary_id

For a Research stack of clusters or for a POC, where TCI code cannot be obtained, please use blanks for the TCI Code, effectively making the index name to start with 'i_'.

3.5 Role Name

The role name should start with 'role_' and should represent the intended purpose of the Role and the type of privilege that this role has on the database objects (i.e. either SELECT or INSERT etc.). While the length of the role name can be 128 characters in length, the recommendation is to keep it short but not too much abbreviated to lose clarity.

Every role name should start with keyword "role" as prefix followed with database name And ends with role type.

Role types –

Admin (Read write access on entire database tables)
Select (Read access to all tables)
Insert (Insert access to all tables)
Customized (Based on user requirement)

3.5.1 Admin Role

For Admin roles on a particular database role name should start with keyword “role” followed with database name and ends with keyword “admin”.
Ex- for a database “testdb” admin role name should be like “role_testdb_admin” Usage- role_<database_name>_admin

3.5.2 Select Role

For read/select roles on a particular database name should start with keyword “role” followed with database name and ends with keyword “ro”.
Ex- for a database “testdb” select role name should be like “role_testdb_ro” Usage- role_<database_name>_ro

3.5.3 Insert Role

For insert role on particular database name should start with keyword “role” followed with database name and ends with keyword “rw”.
Ex- For a database “testdb” insert role name should be like “role_testdb_rw”
Usage- role_<database_name>_rw

3.5.4 Customized Role

Please contact Admins for any specific requirements on database roles and privileges.

NOTE- Role name naming standard are same for application database or individual user’s database.

4. Sentry group –

4.1 Sentry group for Application id

It’s not mandatory for applications to have their sentry group, application id’s can use their application group to raise sentry request which can be used to accessing the database and tables.But in case if application need to have a separate sentry group then they have to follow naming standards.

Sentry group name - hs<application_id>
Ex - hsclaims

Where “hs” stands as –Hadoop Sentry and “claims” is the name of application.

4.2 Sentry group for User id

In some scenarios where user request for individual database creation and access, then User need to have a separate sentry group mapped to their individual id's to get access to those databases. Sentry group for individual users must be prefixed with "hs" followed with their ntid.

Ex- User with ntid "gparo" want to have a sentry group then group name should be "hsgparo".

Usage- hs<ntid> (Here "hs" stands for "Hadoop Sentry")

4.3 Sentry request links

To get a sentry group with proper naming standard user need to raise New Unix group request followed with UNIX modify id request. Below are the link to raise the request.

1) **UNIX** User Access - Create New **Group**
(https://allstate.service-now.com/com.glideapp.servicecatalog_cat_item_view.do?v=1&sysparm_id=5e97962909225500d0a08f30391c93e2&sysparm_link_parent=1ac0da9441e474004e89d3a4eb4fad1c&sysparm_catalog=e0d08b13c3330100c8b837659bba8fb4&sysparm_catalog_view=catalog_default)

2) **UNIX** User Access - Modify ID
(https://allstate.service-now.com/com.glideapp.servicecatalog_cat_item_view.do?v=1&sysparm_id=c18df870dbe0f2404020d024ce9619ad&sysparm_link_parent=1ac0da9441e474004e89d3a4eb4fad1c&sysparm_catalog=e0d08b13c3330100c8b837659bba8fb4&sysparm_catalog_view=catalog_default)

NOTE – sentry group for individual users are allowed on Research QA and TPT cluster not on Production stack.

5. Sentry Spreadsheet

In the spreadsheet we have two different sheets- 1) Object Setup & 2) Security Setup.

Under Object setup all database, tables, index related details are to be filled in. Under Security setup all roles, access, privileges details need to be filled in.

5.1 Object Setup

5.1.1 Database Details

Database details which needs to be created. It can be application database or user database. (Please follow the naming standard in both the scenarios)

Required details are describe below -

Operation - It can be either "Create" a new database or "Drop" the existing database.
Database Name - As per the naming standard for user's/application database.
Owner - Who owns the database, it can be application name or user name.
Application Name - Name of the application who will be using this database.
Approver - Owner for the database/application

Sample user database request –

Database				
Operation	**Database Name**	**Owner**	**Application Name**	**Approver(s)**
create	dru_gparo	gparo	Hadoop Admin	gparo

5.1.2 Table Details

Update the table details on which any operation need to be performed.

Required details are describe below -

Operation - For a table operation can be either Create, Drop or Alter.
Database Name - Name of database under which table operation need to be performed.
Table Name - Name of the table.
DDL Command - Hive command for the table with required operations. Sample for table creation request –

Table			
Operation	**Database Name**	**Table Name**	**DDL command**
CREATE	dru_gparo	sample	CREATE TABLE sample (id int, name string) ROW FORMAT DELIMITED FIELDS TERMINATED BY ',' STORED AS TEXTFILE ;

5.1.3 View Details

Here you need to update the view details on which any operation need to be performed.

Required details are describe below -

Operation - For a view operation can be either Create, Drop or Alter.
Database Name - Name of database under which view operation need to be performed.
View Name - Name of the view.
DDL Command - Hive command for the view with required operations.

Sample for view creation request

View			
Operation	**Database Name**	**View Name**	**DDL command**
CREATE	dru_gparo	sample_view	CREATE VIEW tyv_emp_30000 AS SELECT * FROM employee WHERE salary>30000;

5.1.4 Index Details

Here you need to update the Index details on which any operation need to be performed.

Required details are describe below –

Operation - For an index operation can be either Create, Drop or Alter.

Database Name - Name of database under which index operation need to be performed.

Table Name - Name of the index.

DDL Command - Hive command for the index with required operations.

Sample for index creation request -

View			
Operation	**Database Name**	**View Name**	**DDL command**
CREATE	dru_gparo	sample_index	CREATE INDEX tyi_inedx_salary ON TABLE employee(salary)

5.2 Security Setup

5.2.1 Role Details

User need to fill in the operation (Create or Drop) & role name following proper naming standards.

Required details are describe below –

Role - Either create or drop

Role name - Role name which need to be created or dropped.

Ex – role_dru_gparo_admin.

Sample for role creation request –

Role name	Operation
role_dru_gparo_admin	create
role_dru_gparo_rw	create
role_dru_gparo_ro	create

5.2.2 Privileges Details

User need to fill in all the required details under privilege tab for map object with required role, to have proper access.

Required details are described below -

DCL Command - Here you need to fill in either Grant or Revoke, which will either create or revoke access for the role mentioned on the required object.

Privilege - Privilege will describe the type of role. It can be either All, Select, Insert where all is used to represent admin role, select represents select/read role and insert represents select/insert role.

Object Type - Object type can be either database, table or view.

Object - Object need to be name of either database or table or view. If Object type is mentioned as table then object name should be "<database_name>.<table_name>"

Role - Here user need to mention the role name.

Sample for privileges and roles on user database-

Privileges				
DCL Command	Privilege	Object Type	Object	Role

Grant	All	database	dru_gparo	dru_gparo_admin
Grant	Insert	database	dru_gparo	dru_gparo_rw
Grant	Select	database	dru_gparo	dru_gparo_ro

5.2.3 Role Assignment

In this section role are mapped to UNIX group. UNIX group should be available for mapping them to required roles.

Required parameters are described below-

DCL Command - It can be either Grant or Revoke, which will add/remove mapping between unix group with required roles.

Role Assignment - User need to fill the Role name created in section 1.

Group - UNIX group name which need to be mapped with required role.

Sample for Role assignment -

Role Assignment		
DCL Command	**Role**	**Group**
grant	dru_gparo_admin	hsgparo
grant	dru_gparo_rw	hsrbarr,hsrgas9
grant	dru_gparo_ro	hshchiw,hshbhay

5.2.4 URI

In this section we are going to grant access to external location which will be used for creation of any external tables.

Required parameters are described below –

DCL Command - It can be wither Grant or Revoke, which will add/remove unix group with required roles.

URI - The URI is the HDFS path to where the external table data will be stored (must be under /data/[ENV]/warehouse)

Role - Role name the URI should be assigned to

Sample on URI –

URI Path for External Tables		
DCL Command	**URI**	**Role**
grant	hdfs://nameservice1/data/res/warehouse/isg/dru_gparo	dru_gparo_admin
grant	hdfs://nameservice1/data/res/warehouse/isg/dru_gparo	dru_gparo_rw

NOTE – Until you have access to URI you are not allowed to create external tables so it's a kind of mandatory column where details need to be fill in.

URI Path – "/data/res/warehouse/" is common for all followed with application or department with database name.

Research Cluster sentry locations for applications

/data/res/warehouse/aft
/data/res/warehouse/ars
/data/res/warehouse/ato
/data/res/warehouse/claims
/data/res/warehouse/das
/data/res/warehouse/drivewise
/data/res/warehouse/encompass
/data/res/warehouse/isg
/data/res/warehouse/mkt
/data/res/warehouse/moae
/data/res/warehouse/qra
/data/res/warehouse/quotes
/data/res/warehouse/ruff
/data/res/warehouse/sph

Enterprise Cluster sentry locations for applications

/data/prod/warehouse/ars

/data/prod/warehouse/drivewise
/data/prod/warehouse/encompass
/data/prod/warehouse/isg
/data/prod/warehouse/quotes
/data/prod/warehouse/siu
/data/prod/warehouse/sph

Please reach out to your teammates or Hadoop admins to get proper path in case you are not sure.

6. Point to Remember

1- If you are requesting for a database creation and requesting for admin roles as well, then the request is applicable for Research QA and Research TPT Cluster, as users individual databases are not allowed on production stack.

2- If you are requesting for admin role for a database then you have full access to create, alter and delete tables, views and index, and hence your request should not contain and table, view, index operation details.

3- For production stack user databases are not allowed and no admin roles are allowed on application databases. User need to raise request in case he needs any table need to be created.

4- Insert and select roles are allowed on databases created on production stack, which gives privileges to alter, load data to a table.

5- Any user request to create role and grant access to existing database (User's db. or application db.) will be processed after approval from the database owner.

6- Please reach out to Hadoop Admins (email- HadoopAdministrationTeam@allstate.com) In case of any concerns.