Security 3

Streaming Analytics Manager Authorization

Date of Publish: 2020-12-15

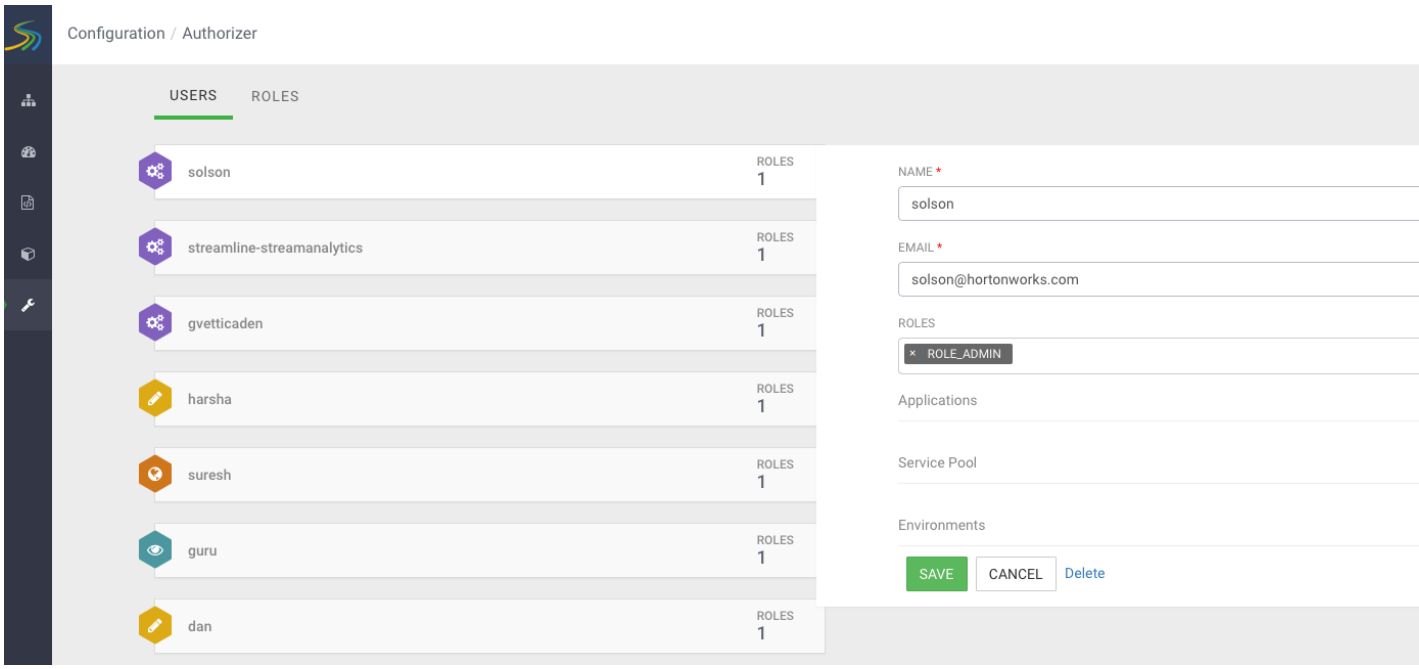
https://docs.cloudera.com/

Contents

SAM Authorization

After you have logged in as the streamline user, you can access the SAM UI. The streamline user is assigned the **Admin** role and can manage users and security permissions. After logging in with this user, go to the menu item **Configuration** and select **Authorizer**.

You can use the **Authorizer** dialog to create users and assign them to roles.



Roles and Permissions

SAM provides four out of the box roles which map to the 3 different personas that SAM provides capabilities for and then a Admin user.

- Admin Role – The Admin Role is a super user who has access to all of SAM's system roles and privileges.
- Application Developer Role – The Application Developer Role has the privileges necessary to create and submit applications.
- Operations Role – The Operations Role has the privileges necessary to create service pools and environments and to submit applications.
- Analyst Role – The Analyst Role has access to specific applications and dashboards.

A role provides permissions (Read,Write, Execute) to 5 different resources in SAM:

- Applications
- Service Pools
- Environments
- User Management / Security
- Dashboards

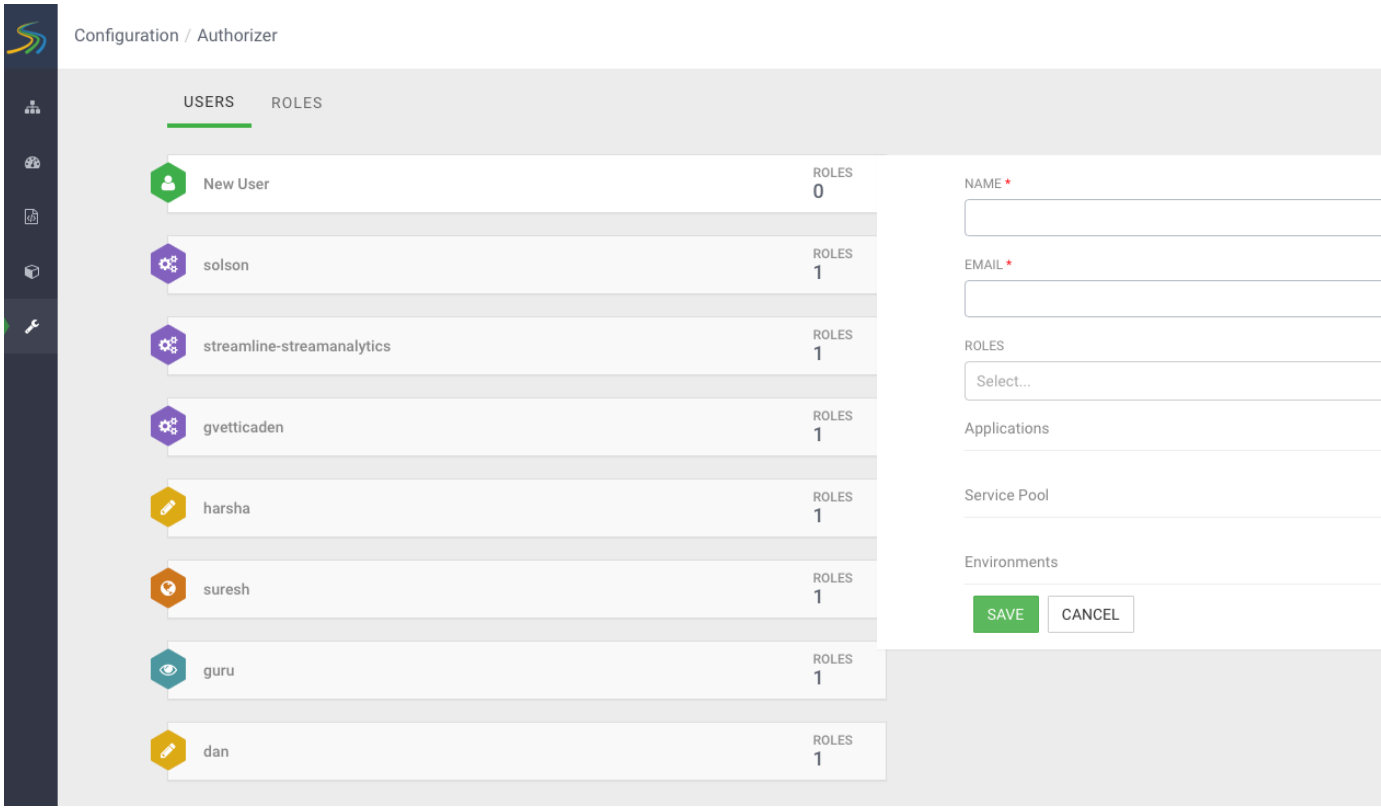
Table 1: Role and Permission Matrix

Resources	Admin Role Access	Application Developer Role Access	Operations Role Access	Analyst Role Access
Streamline Resources				
User Mgmt	All Access	No Access	No Access	No Access
Role Mgmt	All Access	No Access	No Access	No Access
Topology	All Access	U: R W X	All: R W X	No Access
Customer Processor	All Access	U: R W	All: R W	No Access
Service Pools	All Access	All: R	All: R W	No Access
Environments	All Access	U: R W	All: R W	No Access
System Artifacts: Notifier UDF UDAF Component Defs	All Access (includes edit access to component defs)	Read to All	Read to All	No Access
Custom Artifacts: Notifier UDF UDAF	All Access	U: R, W	All: R W	No Access
Dashboards				Has LInk to Menu
Schema Registry Resources				
Schemas		All: R W	All: R W	All: -
Model Registry Resources				
Models	All: R	U: R W O: R		

Creating Users and Assigning Them to Roles

Using the streamline user to initially go into SAM, you can create other admin roles in the system that can administer user accounts for the rest of the organization. To create new admin account for user gvetticaden, perform the following steps:

1. From Menu, select **Configuration** and then **Authorizer**.
2. From the **Users** tab, select the + icon.
3. Enter information about the new user account.



4. Click **Save**.

Result

You are able to see the user you just created in the user list, on the left side of the **SAM Configuration | Authorizer** view.

You do not have to provide any password. This is because SAM relies on a Kerberos/KDC to do the authentication. The principal is then passed to SAM when accessing the SAM UI. The principal name as part of the kerberos ticket must match a user in SAM. Then SAM looks up the role for that user and provides access based on the roles permissions.

Sharing Resources

SAM allows users to share different resources with other users to provide a collaborative team environment. A user who has edit access to a resource can share that resource with another user. When a resource is shared, the user can configure if the resource being shared can be just viewed or edited.

SAM allows the following resources to be shared:

- Environments
- Applications

Sharing an Environment

By default, only the user who created an application can see that it. However, it is common for applications to be shared amongst a group of users. To do this, the user who created the application must share that it with other users.

1. From the left-hand menu select **Configuration**, then **Environment**.
2. From the environment you want to share, click the **Configuration** ellipses at the top right and click **Share**.
3. In the **Share Environment** dialog, select the users with whom you want to share the environment.
4. Specify whether you want to give them **View** or **Edit** privileges and click **Ok**.

Sharing an Application

By default, only the user who created an application can see that it. However, it is common for applications to be shared amongst a group of users. To do this, the user who created the application must share that it with other users.

1. From the left-hand menu select **My Applications**.
2. From the application you want to share, click the **Configuration** ellipses at the top right and click **Share**.
3. In the **Share Application** dialog, select the users with whom you want to share the application.
4. Specify whether you want to give them **View** or **Edit** privileges and click **Ok**.

SAM Authorization Limitations

- SAM's roles and access control policies are maintained in SAM.
- Creation of users and assignment to roles must be done using the SAM UI. There is no support to import users from KDC/AD.
- Role assignment is at a user level. Assigning roles to a group is not supported.
- New Roles or editing the out of the box role cannot be allows. However, the collaboration sharing features allow you to share each of the 5 resources across users meeting most use case requirements.