Authentication

Authentication is the act of verifying the identity of a user. User login into Jethro is authenticated by an LDAP server (except for the Jethro admin user). When Authentication is enabled, Jethro will enforce all clients to authenticate themselves in order to determine their operations and access policies. If a user is no longer authenticated by the LDAP (after connection), the client connection will drop within a configured time.

While authentication and authorization are closely connected, it is important not to confuse between them, as they are distinct from one another. Authentication verifies the identity of a client, while Authorization determines its operations and access policies. To learn more about Authorization, visit its documentation page.

The following subjects will be covered under this section:

LDAP connectivity configuration

LDAP integration requires the configuration of LDAP connectivity and filtering rules:

- Configure how to connect to the LDAP server
- Configure how to identify Jethro users
- Configure how to identify Jethro groups

In order to set the properties of the required parameters for LDAP connectivity, run the SQL command: 'set global _____' along with each of the following relevant set of parameters:

General LDAP parameters

ldap.enable - 1/0 (True/False). Default is 0. Enables/disables LDAP authorization support.
ldap.uri - String of LDAP URI. Default is empty. Mandatory.
ldap.port - If this parameter is set to 0, Jethro will use a default port according to the protocol chosen to be used (LDAP-389, LDAPS-636). Default value: 0 . Mandatory.
ldap.admin.dn - Default is empty. Mandatory.
ldap.admin.password - Default is empty. Mandatory.
ldap.base.dn - The base location in the LDAP directory tree from which to search for user and group entries. Default is empty. Mandatory.

LDAP users parameters

ldap.user.append.dn - The additional DN to append to the Base DN for the location of user entries. If users are located in multiple locations in the directory, you can separate DNs using pipe (|).Default is empty.
ldap.user.object.class - The object class define the user. Default is user.
ldap.user.unique.id.attribute - This is the name of the LDAP attribute that specifies the unique user ID. Default value: sAMAccountName
ldap.user.filter - General LDAP filter to restrict the search scope for users in the directory tree. Default: empty (no filter).
ldap.user.group.filter - A list of groups which won't appear in search results for user's groups. Default value: empty.

LDAP group parameters

Ldap.group.append.dn - The additional DN to append to the Base DN for the location of group entries. If groups are located in multiple locations in your directory, you can separate DNs using pipe (|). Default value: empty.
Ldap.group.object.class - The object class define the group. Default value: group. Mandatory.
Ldap.group.name.attribute - This is the name of the LDAP attribute that specifies the group. We recommend that group name is unique value,. Default value: name
Ldap.group.filter - An LDAP filter to restrict the search scope for groups in the directory tree. Default is empty.
Ldap.group.members.attribute - Group member attributes. Default is: member. Mandatory

LDAP authentication over SSL/TLS (Version 3.0.3 and up)

ldap.ssl.certificate.path=<path-to-CA-certificate-file> - To use LDAP over SSL/TLS a CA-certificate should be imported by an admin to the trust store on the Jethro host. Once the certificate file is available and readable by jethro user on the host, set the parameter to point to the location of the certificate file. Any update of the certificate file path will require server restart to take effect. Default value: empty.

Note: from version 3.5.0 ldap ssl without certificate is allowed, thus making proving certificate file value **not mandatory**. If certificate is not provided succsuful SSL/TLS connectivity to the LDAP server depend on on LDAP server security settings.

ldap.ssl.enabled - To enable LDAPS (secure LDAP), set the value to 1. When ldap.ssl.enabled is set to 1, the parameter ldap.ssl.certificate.path becomes mandatory. Default value: 0.

ldap.port - If this parameter is set to 0, Jethro will use a default port according to the protocol chosen to be used (LDAP-389, LDAPS-636). Default value: 0.

Examples

```
set global ldap.uri=10.1.1.30;

set global Ldap.port = 389;

set global ldap.admin.dn=CN=Administrator,CN=Users,DC=jethro,DC=LDAP2;

set global ldap.admin.password=Password1212;

set global ldap.base.dn=DC=jethro,DC=LDAP2;

set global ldap.user.append.dn=OU=jethro;

set global ldap.group.append.dn=CN=Users|OU=jethro;

set global ldap.ssl.certificate.path=/home/jethro/jethro_certificate.pem;

set global ldap.ssl.enabled=1;

set global ldap.enable=1;

set global ldap.user.group.filter=Business;

set global ldap.group.filter=!(&(objectCategory=group)(name=data*));

--Example for two groups:

set global ldap.group.filter=(&(objectCategory=group)(|(name=AA)(name=BB)));
```

Impersonation

Impersonation means allowing one user account to act on behalf of another user account. Impersonation support in Jethro allows users to execute queries on external data sources, as the connected user, rather than the super user provided in the external source settings. The main benefit of this feature is it allows administrators to control their data security policy in a single place - their external data source.

Configuring Impersonation in Jethro

In order to Enable/Disable impersonation in Jethro, set the properties of the required parameters in Jethro, by executing the SQL command: 'set global _____', along with the relevant parameter(s) for your use case:

external.connector.hive.impersonation.enable - 1/0 (True/False). Default is 0. Enable/Disable impersonation for Hive external data sources.

external.connector.hdfs.impersonation.enable - 1/0 (True/False). Default is 0. Enable/Disable impersonation for HDFS external data sources.

prerequisites: The external data source should be defined in Jethro using the credentials of a super user.

Configuring Impersonation in external data sources

The procedure required for enabling/disabling impersonation within an external data sources, is different for every data source.

A few examples from Cloudera's documentation:

Configuring Proxy Users to Access HDFS

HiveServer2 Impersonation

From Hortonworks:

https://hortonworks.com/blog/best-practices-for-hive-authorization-using-apache-ranger-in-hdp-2-2/

See also

Auditing

Authorization