**LDAP Authentication in HS2**

**(HIVE-7193)**

There are two important functional deficiencies in the current LDAP Authentication provider implementation.

**Group membership**: This enables HiveServer to enforce group membership for users. The authentication request will succeed if the user belongs to one or more of the groups listed in the hive configuration file. If the user does not belong to atleast on of the groups listed, the user authentication fails.

To support group membership based authentication, two new parameters will be added.

hive.server2.authentication.ldap.groupBaseDN : This value represents “base distinguished name” for groups in the directory. This value could be just the delta from the baseDN or could include the baseDN.

Ex1:

<property>

<name>hive.server2.authentication.ldap.groupBaseDN</name>

<value>OU=Groups</value>

</property>

So the full DN for a group named “group1” becomes

“CN=group1,OU=Groups,DC=foo,DC=apache,DC=org”

Ex2:

<property>

<name>hive.server2.authentication.ldap.groupBaseDN</name>

<value>CN=Users,DC=foo,DC=apache,DC=org</value>

</property>

Full DN, for group “group2” would then be “CN=group2,CN=Users,DC=foo,DC=apache,DC=org”

hive.server2.authentication.ldap.groupFilter: This value represents the group name filter that is to be enforced by the Atn provider. The user MUST belong to one or more of these groups for the authentication request to succeed.

Ex:

<property>

<name>hive.server2.authentication.ldap.groupFilter</name>

<value>group1,group2</value>

</property>

**User search list:** This enables HiveServer to restrict access to a specified list of users. If the user, being authenticated, is not part of this userlist, access will be denied.

To support this feature, two new parameters will be added.

a) hive.server2.authentication.ldap.userBaseDN:

This value represents “base distinguished name” for users in the directory. This value could be just the delta from the baseDN or could include the baseDN.

Ex1:

<property>

<name>hive.server2.authentication.ldap.userBaseDN</name>

<value>CN=Users</value>

</property>

So the full DN for a user named “user1” becomes

“CN=<username>,” + <userBaseDN> + “,” + <baseDN>

“CN=user1,CN=Users,DC=foo,DC=apache,DC=org”

Ex2:

CN=Users,DC=foo,DC=apache,DC=org

Full DN for usr “user2” would then be “CN=user2,CN=Users,DC=foo,DC=apache,DC=org”

b) hive.server2.authentication.ldap.userFilter: This is a comma separated list of usernames to grant access to. The Atn provider grants access if the user being authenticated is part of this list, denies access otherwise.

Ex :

<property>

<name>hive.server2.authentication.ldap.userFilter</name>

<value>hive-admin,hive,hivetest,hive-user</value>

</property>

**Implementation**:

The group membership parameters can used in conjunction with the user lists to enforce a stricter access. LDAP Atn provider renders decision according to the following criterion

1. if GroupFilter and UserFilter are both specified in the configuration file, access is granted IFF the user being authenticated satisfies BOTH conditions, access is denied otherwise. So the user has to be listed in the UserFilter AND the user MUST also belong to one of the groups listed in the GroupFilter.

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>DC=foo,DC=apache,DC=org</value>

</property>

<property>

<name>hive.server2.authentication.ldap.groupBaseDN

</name>

<value>CN=Users</value>

</property>

<property>

<name>hive.server2.authentication.ldap.groupFilter

</name>

<value>Foo,Domain Admins,Group Policy Creator Owners,

Administrators,hive\_AD</value>

</property>

<property>

<name>hive.server2.authentication.ldap.userBaseDN</name>

<value>CN=Users</value>

</property>

<property>

<name>hive.server2.authentication.ldap.userFilter</name>

<value>cm-admin,hive,hivetest,hive-user</value>

</property>

1. If only the GroupFilter is specified, the provider checks for group membership for the given user. Access is granted if the user belongs to atleast one of the groups, denied otherwise.

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>DC=foo,DC=apache,DC=org</value>

</property>

<property>

<name>hive.server2.authentication.ldap.groupBaseDN

</name>

<value>CN=Users</value>

</property>

<property>

<name>hive.server2.authentication.ldap.groupFilter

</name>

<value>Foo,Domain Admins,Group Policy Creator Owners,

Administrators,hive\_AD</value>

</property>

1. If only the UserFilter is specified, the provider checks if the user belongs to the list of users. Access is granted if user is part of the UserFilter list, denied otherwise.

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>DC=foo,DC=apache,DC=org</value>

</property>

<property>

<name>hive.server2.authentication.ldap.userBaseDN</name>

<value>CN=Users</value>

</property>

<property>

<name>hive.server2.authentication.ldap.userFilter</name>

<value>cm-admin,hive,hivetest,hive-user</value>

</property>

1. If neither GroupFilter nor UserFilter is specified in the configuration file, the Atn provider adjudicates a grant/deny decision based on whether or not the user is defined in the directory.

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>DC=foo,DC=apache,DC=org</value>

</property>