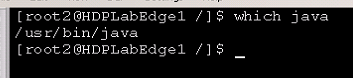
* + 1. **Setup TrustStore**

Follow the below steps to setup TrustStore for Ambari Server.

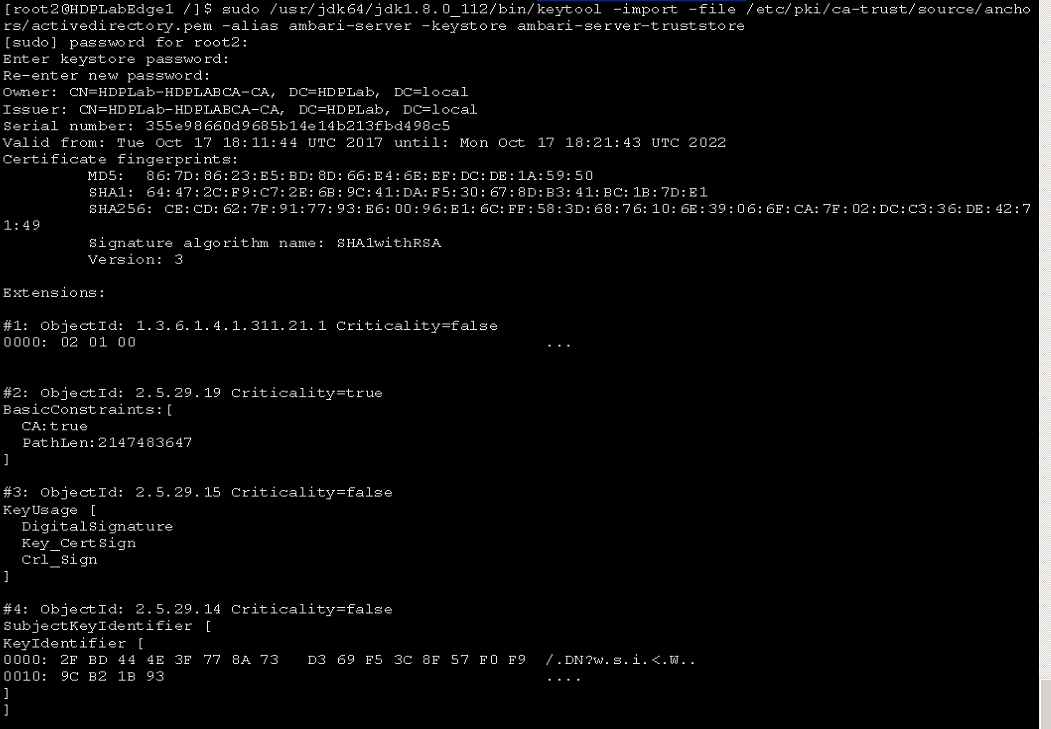
1. Log on to the Ambari Server and Stop the Ambari server using the below command.

ambari-server stop

1. Create a new keystore that will contain the Ambari Server's HTTPS certificate.

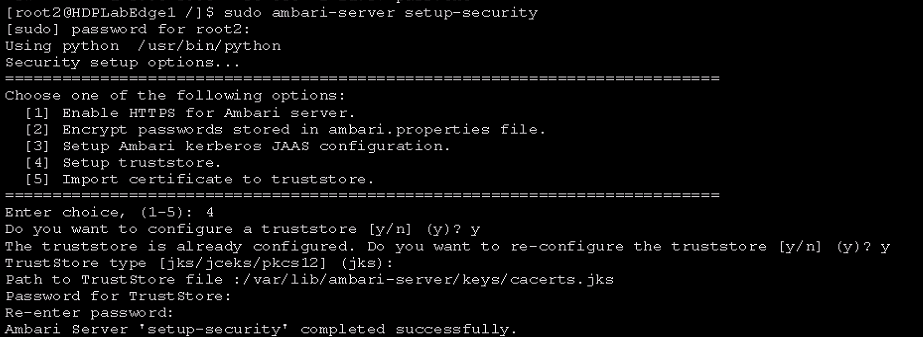


sudo /usr/jdk64/jdk1.8.0\_112/bin/keytool -import -file /etc/pki/ca-trust/source/anchors/activedirectory.pem -alias ambari-server -keystore ambari-server-truststore



When prompted to 'Trust this certificate?' type "yes".

1. Configure the ambari-server to use this new trust store:
2. sudo ambari-server setup-security
3. Choose 4 (setup truststore)



1. Import the certificate (keys) into the trust store (keyring) created above:
   1. sudo ambari-server setup-security
   2. Choose 5 (Import certificate)

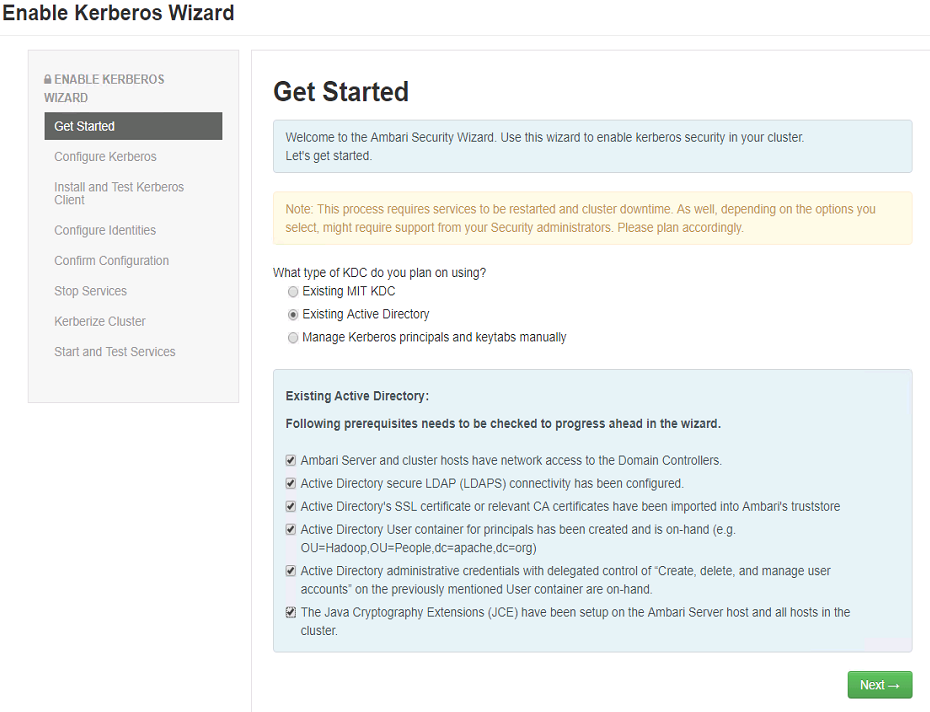


1. Ambari Server must be restarted for the change to take effect.

ambari-server restart

**Configure AD Kerberos Authentication**

1. Log in to Ambari Web and Browse to Admin > Kerberos.
2. Click “Enable Kerberos” to launch the wizard.
3. Select the type of KDC you are using and confirm you have met the prerequisites.

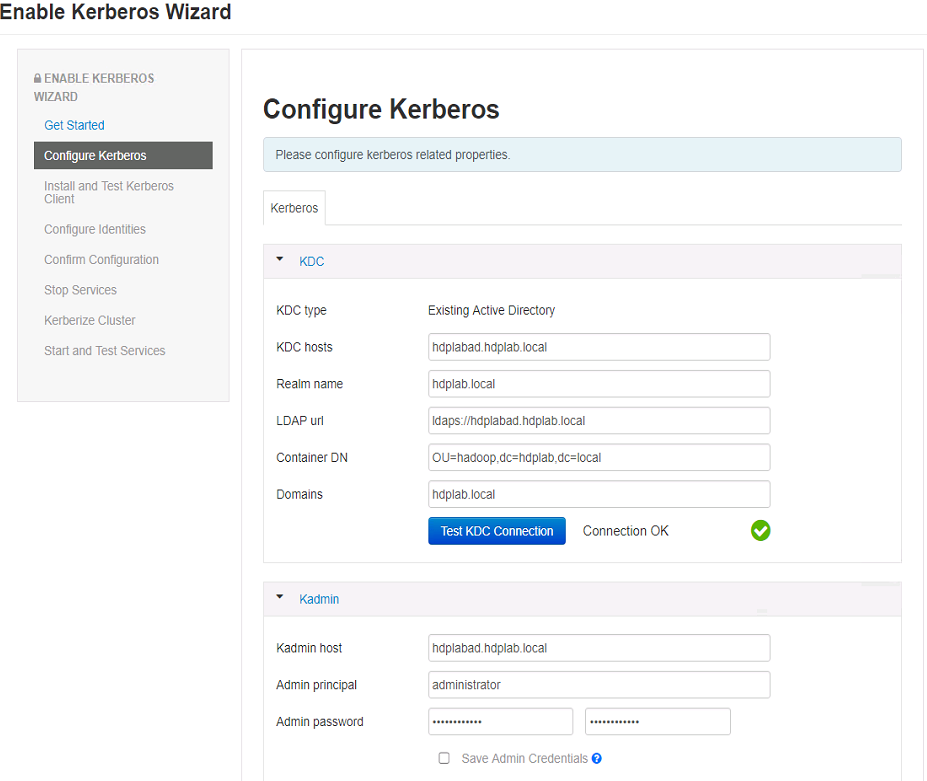


1. Provide information about the KDC and admin account.
   1. In the KDC section, enter the following information:

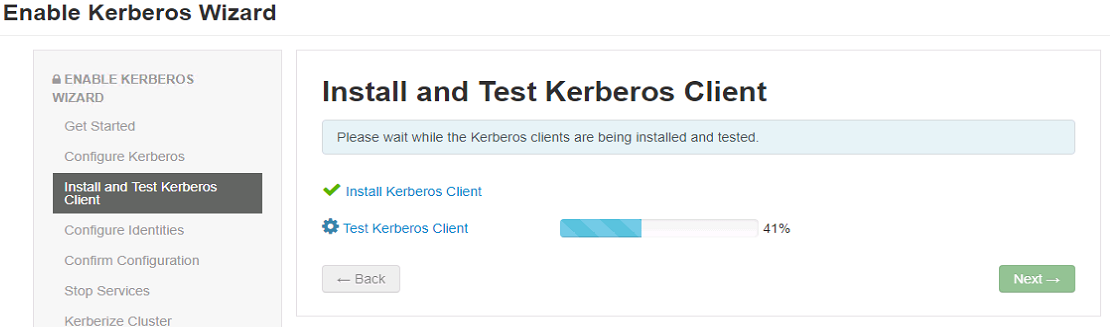
* In the KDC Host field, the IP address or FQDN for the KDC host. Optionally a port number may be included.
* In the Realm name field, the default realm to use when creating service principals. **NOTE:NOTE:NOTE** – this only works upper case. Everything else should be lower case.
* If Load balancing enabled for AD domain controller, provide a list of patterns to use to map hosts in the cluster to the appropriate realm. For example, if your hosts have a common domain in their FQDN such as host1.hortonworks.local and host2.hortonworks.local, you would set this to:

.hortonworks.local,hortonworks.local

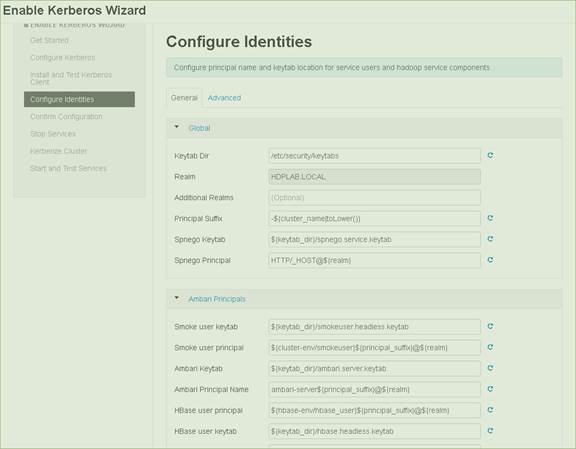
* 1. In the Kadmin section, enter the following information:
* In the Kadmin Host field, the IP address or FQDN for the KDC administrative host. Optionally a port number may be included.
* The Admin principal and password that will be used to create principals and keytabs.

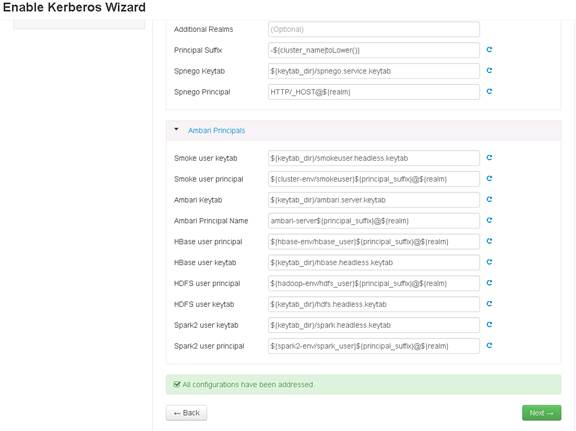


1. Modify any advanced Kerberos settings if needed
2. Proceed with the install.

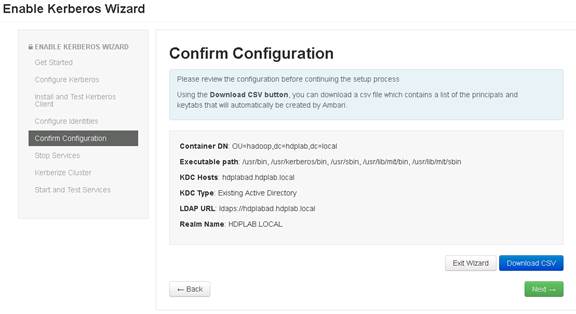


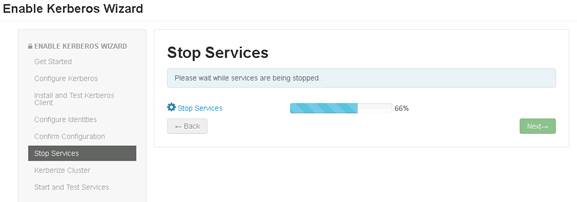
1. Ambari will install Kerberos clients on the hosts and test access to the KDC by testing that Ambari can create a principal, generate a keytab and distribute that keytab.
2. Customize the Kerberos identities used by Hadoop and proceed to kerberize the cluster.



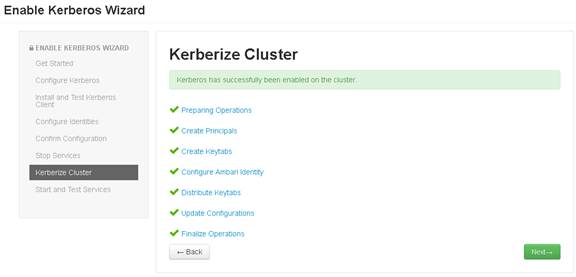


1. Confirm your configuration. You can optionally download a CSV file of the principals and keytabs that Ambari will automatically create.

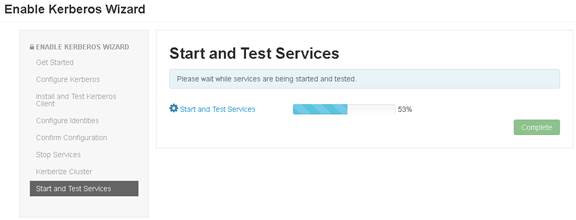




1. Click Next to start the process.



1. After principals have been created and keytabs have been generated and distributed, Ambari updates the cluster configurations, then starts and tests the Services in the cluster.



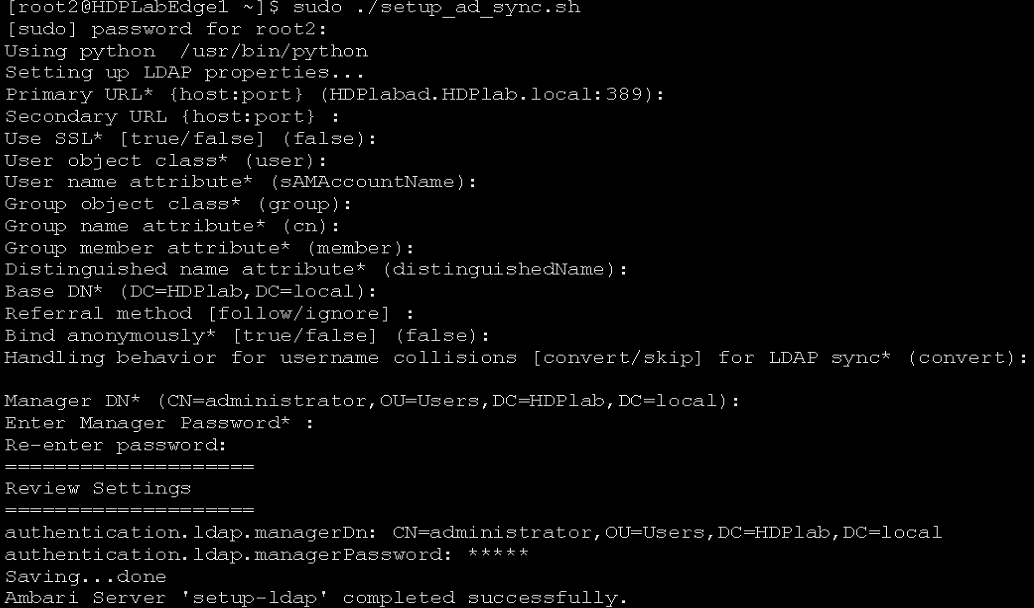
1. Exit the wizard when complete.
2. Finally, Restart Ambari Server.
   1. **Enable LDAP/ AD Authentication**

Run the below mentioned script on the Ambari server to enable LADP/AD Authentication for Ambari. Please make sure to replace the values highlighted in yellow with the actual values.

1. Run the script setup-AD-sync.sh with the following modifications based on information in the table at 12.1.1:
   1. Check ad\_host based on what is in table 12.1.1
   2. ad\_user should reflect the AD admin user sync account ex. Svc\_HadoopSyncDev

sudo ./setup\_ad\_sync.sh





For manager DN\* enter the password for the ad\_user above

1. Restart the Ambari Server

sudo ambari-server restart

1. Run the AD Sync.sh

sudo ./run\_ad\_sync.sh



* + 1. **Ranger User Sync for LDAP/AD**

1. On the Customize Services page, select the Ranger User Info tab.
2. Click Yes under Enable User Sync.
3. Use the Sync Source drop-down to select LDAP/AD.
4. Set the following properties on the Common Configs tab
5. Ensure the Common configs, User Configs and Group configs look like the below screenshots using the following information (except User Config Tab):

Common Config Tab:

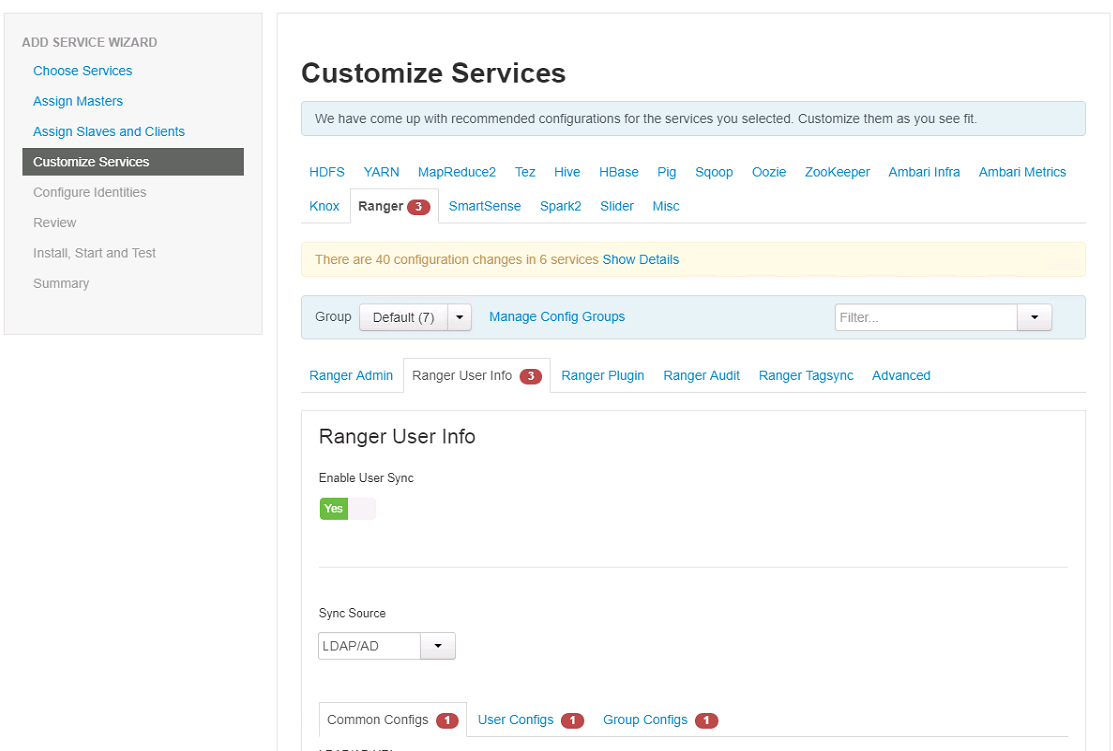
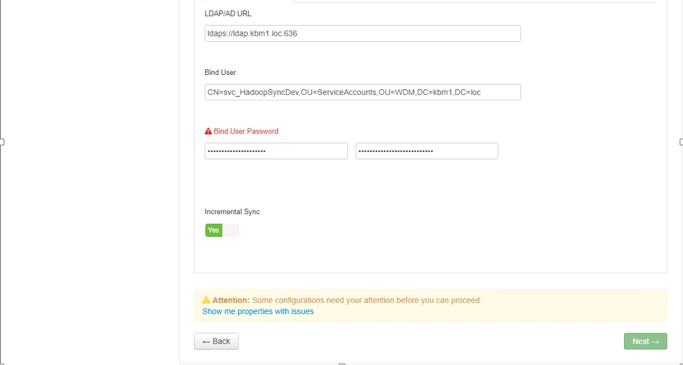
* LDAP/AD URL = ldaps://ldap.kbm1.loc:636 or KBMWDCPV02.kbm1.loc:636
* Bind User = CN=svc\_HadoopSyncDev,OU=ServiceAccounts,OU=WDM,DC=kbm1,DC=loc
* Bind User Password = <lookup in Secret Server>

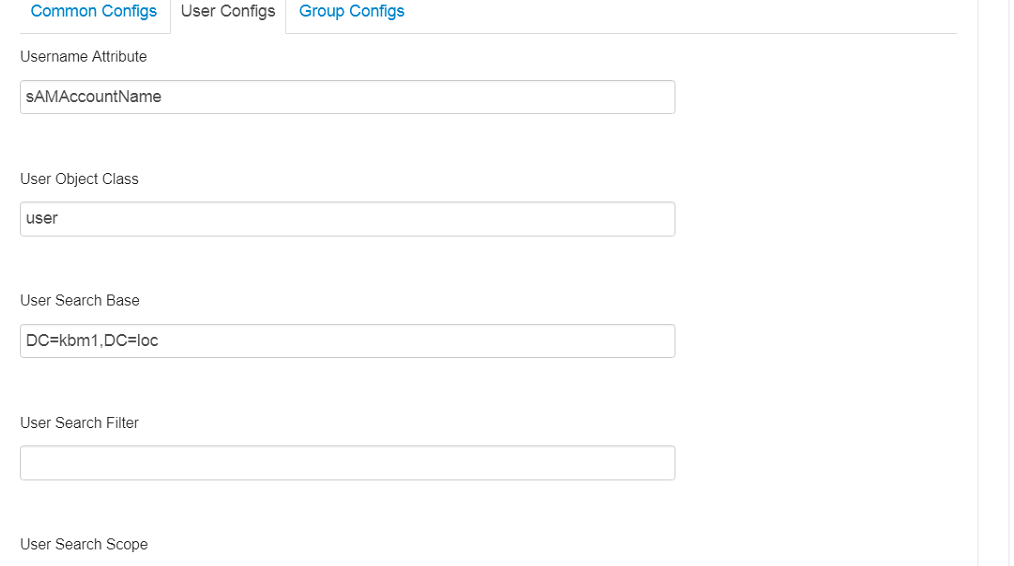
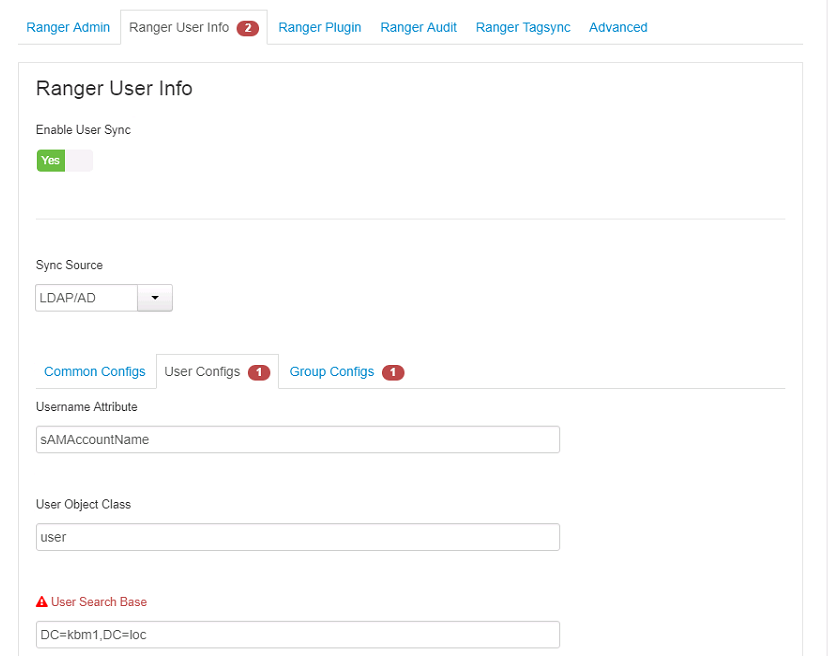
User Config Tab (NOTE this is not necessary):

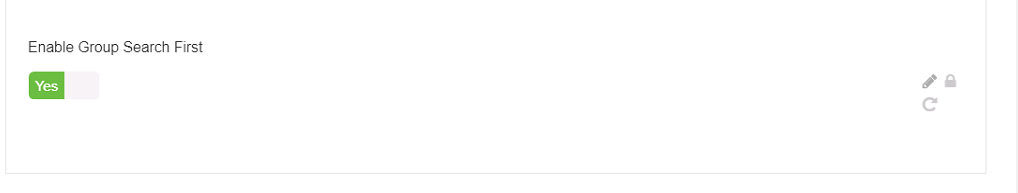
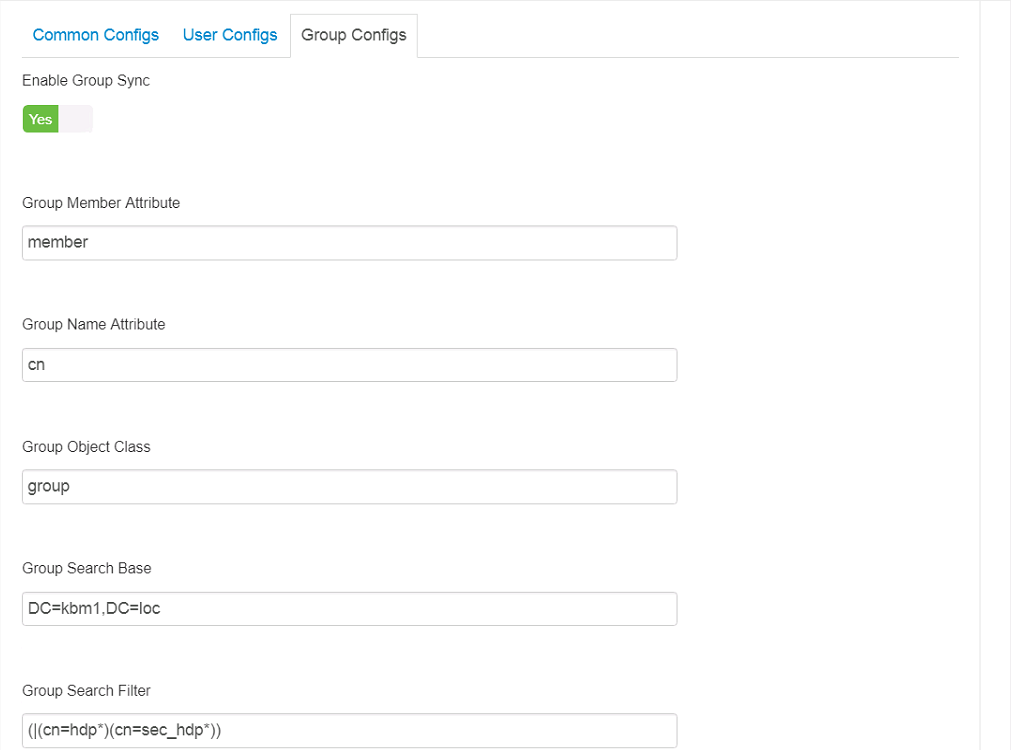
* User Search Base = DC=kbm1,DC=loc
* User Search Filter = (|(&(objectCategory=person)(sAMAccountName=\*)(memberOf=cn=sec\_HDPAccess,OU=Security Groups,OU=Dallas,OU=Groups,OU=KBM,OU=KBMG,DC=kbm1,DC=loc))(&(objectCategory=person)(sAMAccountName=\*)(memberOf=cn=sec\_HDPAdmin,OU=Security Groups,OU=Dallas,OU=Groups,OU=KBM,OU=KBMG,DC=kbm1,DC=loc))(&(objectCategory=person)(sAMAccountName=\*)(memberOf=cn=sec\_HDPDevelopers,OU=Security Groups,OU=Dallas,OU=Groups,OU=KBM,OU=KBMG,DC=kbm1,DC=loc)))

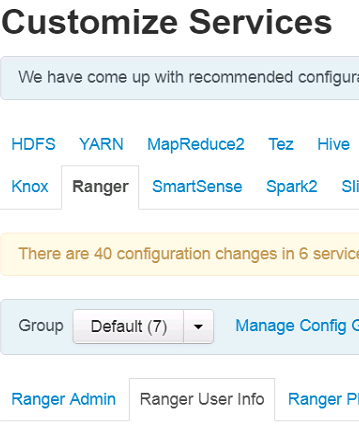
Group Config Tab:

* Group Search Base = DC=kbm1,DC=loc
* Group Search Filter = (|(cn=hdp\*)(cn=sec\_hdp\*)(cn=HDP\*)(cn=sec\_HDP\*))



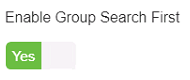




1. Enable Group Search First (Groups tab). . .Note this displays the Enable Users Search button on Users Tab

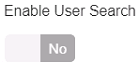
Common Configs user Configs Group Configs 

10/24/2017 12:32 PM - Screen Clipping



1. Disable "User Search" on Users Tab

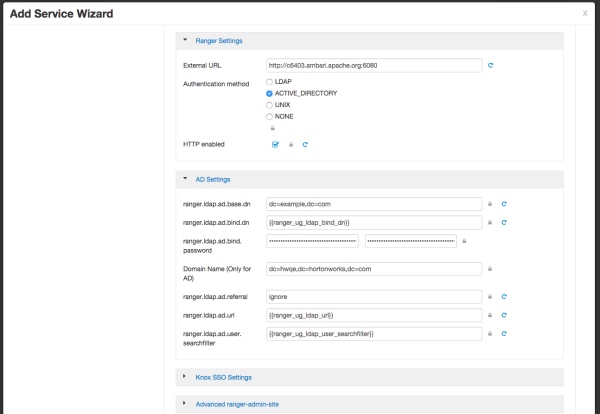
Common Configs user Configs Group Configs 



* + 1. **Ranger Authentication**

Use the following steps to configure Ranger authentication for Active Directory.

1. Select the Advanced tab on the Customize Services page.
2. Under Ranger Settings, specify the Ranger Access Manager/Service Manager host address in the External URL box in the format http://<your\_ranger\_host>:6080.
3. Under Ranger Settings, select ACTIVE\_DIRECTORY.
4. Under AD Settings, set the following properties.



1. Xlick Next at the bottom of the page to continue with the installation.
2. Clear (un-check) the ranger.authentication.method check box, then click OK.

