1. Configure KNOX to use CA certificate

1. Find out the CA certificate for the node . Normally it is in the folder "/home/hdsuser/horton/certs"
2. Make sure you know the KNOX master secret. if not use the following command to rest it forcefully.
   cd $knox_home/bin/knoxcli.sh create-master --force
   #let it be "hadoop"

   In all the below command please replace the hostname where you see zslvedledgdd01 or azslvedledgdd01.d01saedl.manulife.com with your Knox hostname.
3. Backup the files under /var/lib/knox/data-<hdp-version>/security/keystores/ for example /var/lib/knox/data-2.6.5.0-292/security/keystores/
4. Create the new jks file

   cd /var/lib/knox/data-2.6.5.0-292/security/keystores/
   openssl pkcs12 -export -in /home/hdsuser/horton/certs/azslvedledgdd01/edg01.cer -inkey /home/hdsuser/horton/certs/azslvedledgdd01/azslvedledgdd01-pri.key -name azslvedledgdd01.d01saedl.manulife.com -out /home/hdsuser/horton/certs/azslvedledgdd01/azslvedledgdd01.d01saedl.manulife.com.P12

   Use the master secret as password when prompted (say password: hadoop)
5. Import the key store (replace the <master_secret>).
   cd /var/lib/knox/data-2.6.5.0-292/security/keystores/
   keytool -importkeystore -srckeystore /home/hdsuser/horton/certs/azslvedledgdd01/azslvedledgdd01.d01saedl.manulife.com.P12 -srcstoretype PKCS12 -destkeystore gateway.jks -deststoretype jks -srcstorepass <master_secret>-deststorepass <master_secret>-srcalias azslvedledgdd01.d01saedl.manulife.com -destalias gateway-identity -destkeypass <master_secret>
6. If you have multiple nodes where Knox is running the above procedure has to be repeated on each of them.

2. Hiding LDAP Admin Password

1. Create the aliases for the passphrase usage

   /usr/hdp/current/knox-server/bin/knoxcli.sh create-alias gateway-identity-passphrase --value <master_secret>

2. Copy this password phrase for all topologies used

   cd /var/lib/knox/data-2.6.5.0-292/security/keystores/
   cp __gateway-credentials.jceks knoxsso-credentials.jcekscp __gateway-credentials.jceks default-credentials.jceks

   cp __gateway-credentials.jceks manager-credentials.jceks

3. Create the aliases for the ldap manager user password, so that we don't keep the password as open text in Knox topology files. This is the password for the user given as "main.ldapRealm.contextFactory.systemUsername" in Knox topology file (the same one on all 4 lines):
   /usr/hdp/current/knox-server/bin/knoxcli.sh create-alias ldcSystemPassword --cluster manager --value <ldap_password>
   /usr/hdp/current/knox-server/bin/knoxcli.sh create-alias ldcSystemPassword --cluster manager --value <ldap_password>
   /usr/hdp/current/knox-server/bin/knoxcli.sh create-alias ldcSystemPassword --cluster admin --value <ldap_password>
   /usr/hdp/current/knox-server/bin/knoxcli.sh create-alias ldcSystemPassword --cluster knoxsso --value <ldap_password>

4. Restart KNOX.

That's all. Happy KNOXing 🙂

Note: If the master secret is not reset as in step:2 or KNOX is not configured with LDAP, you can skip steps-6,7,8