```
root@hadoopnode1 anchors]# tailf  /var/log/ambari-server/ambari-server.log
```

steps 1: cp RootCA_base64.cer /etc/pki/ca-trust/source/anchors/activedirectory.pem

step 2 : update-ca-trust force-enable

step 3 :update-ca-trust extract

step 4 :update-ca-trust check

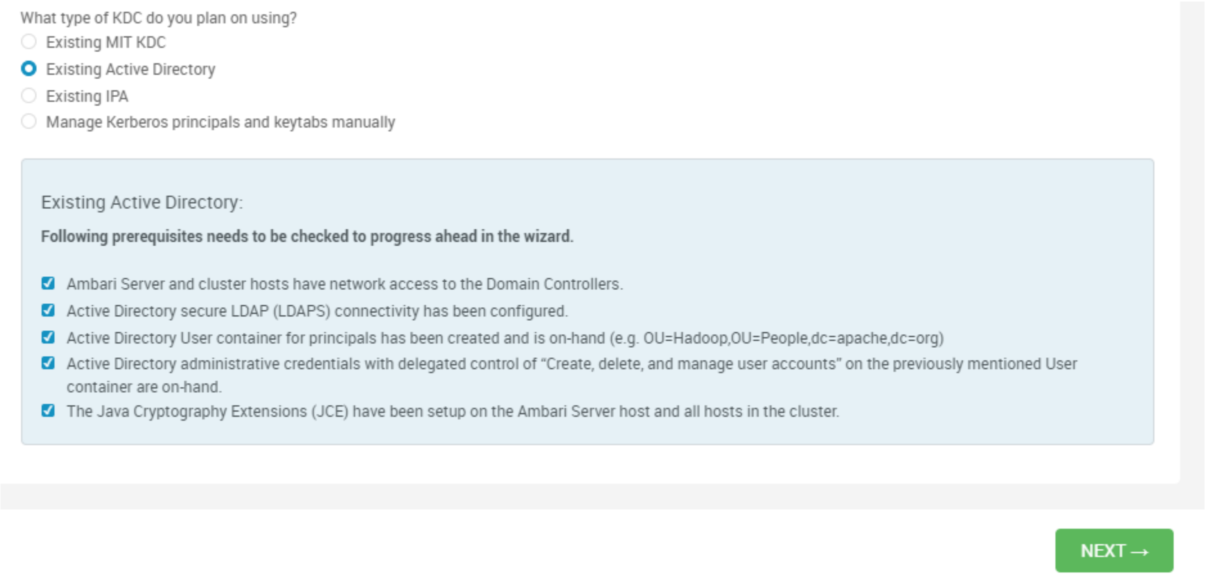
step5 /opt/jdk1.8.0_201/bin/keytool -import -file /etc/pki/ca-trust/source/anchors/activedirectory.pem -alias ambari-server -keystore ambari-server-truststore

step6 : ambari-server setup-security

```
$ ambari-server setup-security
Using python  /usr/bin/python
Security setup options...
================================================================================
Choose one of the following options:
  [1] Enable HTTPS for Ambari server.
  [2] Encrypt passwords stored in ambari.properties file.
  [3] Setup Ambari kerberos JAAS configuration.
  [4] Setup truststore.
  [5] Import certificate to truststore.
================================================================================
Enter choice, (1-5): 4
Do you want to configure a truststore [y/n] (y)? y
The truststore is already configured. Do you want to re-configure the truststore [y/n] (y)? y
TrustStore type [jks/jceks/pkcs12] (jks):
```

```
Path to TrustStore file :/var/lib/ambari-server/keys/cacerts.jks
Password for TrustStore:
Re-enter password:
Ambari Server 'setup-security' completed successfully.



#######################################


# ambari-server setup-security
Using python  /usr/bin/python
Security setup options...
===========================================================================
Choose one of the following options:
  [1] Enable HTTPS for Ambari server.
  [2] Encrypt passwords stored in ambari.properties file.
  [3] Setup Ambari kerberos JAAS configuration.
  [4] Setup truststore.
  [5] Import certificate to truststore.
===========================================================================
Enter choice, (1-5): 5
Do you want to configure a truststore [y/n] (y)? y
Do you want to import a certificate [y/n] (y)? y
Please enter an alias for the certificate: activedirectory
Enter path to certificate: /etc/pki/ca-trust/source/anchors/activedirectory.pem
Ambari Server 'setup-security' completed successfully.

###########################################
```

also enable : Java Cryptography Extensions (JCE) have been setup on the Ambari Server host and all hosts in the cluster.



What type of KDC do you plan on using?

○ Existing MIT KDC

● Existing Active Directory

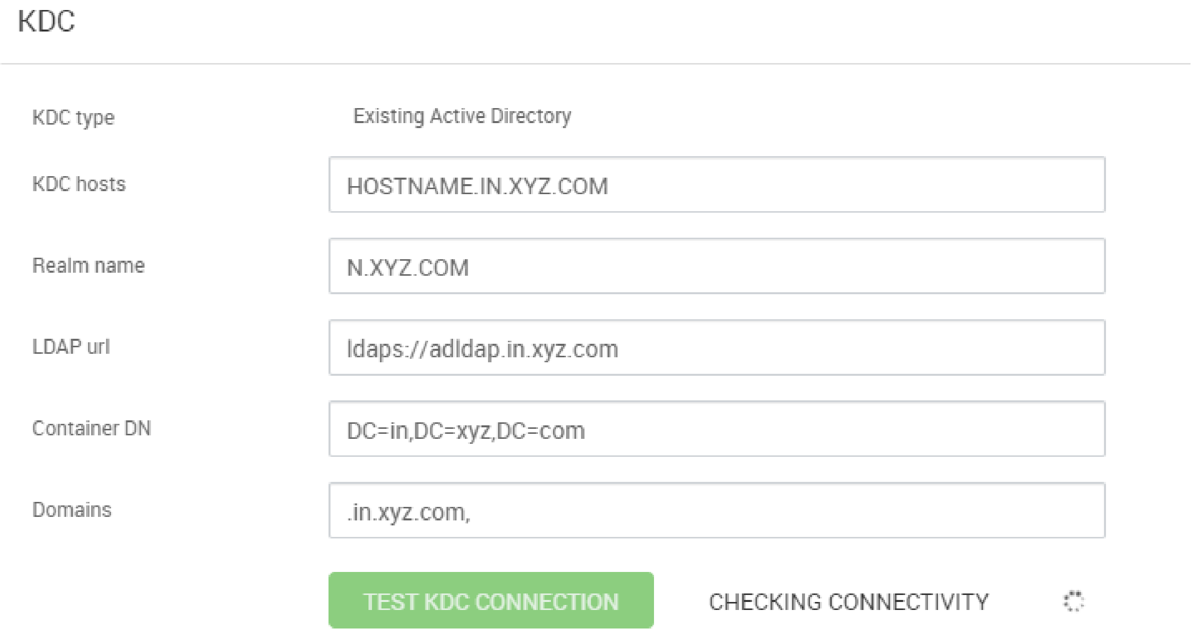
○ Existing IPA

○ Manage Kerberos principals and keytabs manually

Existing Active Directory:

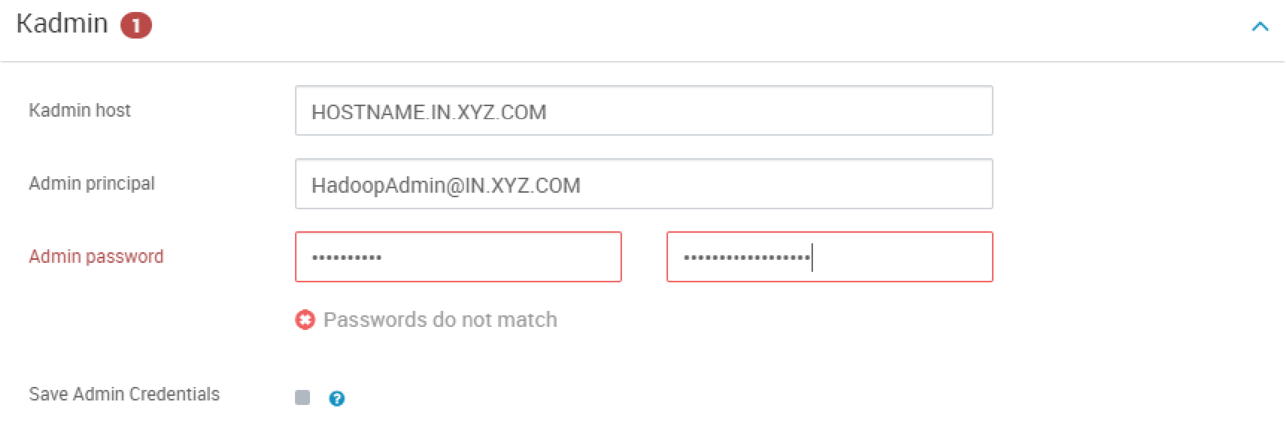
Following prerequisites needs to be checked to progress ahead in the wizard.

- ☑ Ambari Server and cluster hosts have network access to the Domain Controllers.
- ☑ Active Directory secure LDAP (LDAPS) connectivity has been configured.
- ☑ Active Directory User container for principals has been created and is on-hand (e.g. OU=Hadoop,OU=People,dc=apache,dc=org)
- ☑ Active Directory administrative credentials with delegated control of "Create, delete, and manage user accounts" on the previously mentioned User container are on-hand.
- ☑ The Java Cryptography Extensions (JCE) have been setup on the Ambari Server host and all hosts in the cluster.



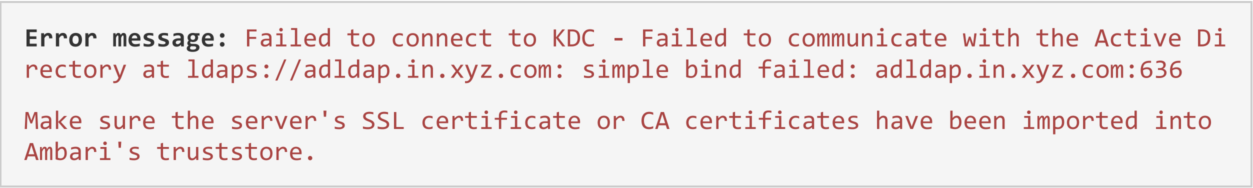
KDC

KDC type	Existing Active Directory
KDC hosts	HOSTNAME.IN.XYZ.COM
Realm name	N.XYZ.COM
LDAP url	ldaps://adldap.in.xyz.com
Container DN	DC=in,DC=xyz,DC=com
Domains	.in.xyz.com,



Kadmin 1

Kadmin host	HOSTNAME.IN.XYZ.COM	
Admin principal	HadoopAdmin@IN.XYZ.COM	
Admin password	••••••••••	••••••••••••••••••
	Passwords do not match	
Save Admin Credentials	□ ?	



```
Error message: Failed to connect to KDC - Failed to communicate with the Active Directory at ldaps://adldap.in.xyz.com: simple bind failed: adldap.in.xyz.com:636

Make sure the server's SSL certificate or CA certificates have been imported into Ambari's truststore.
```

@@@@@@@@@@@@error logs

Error Log as below

```
2019-05-27 15:51:28,677  INFO [ambari-client-thread-45] AmbariManagementControllerImpl:4077 - Received action execution request, clusterName=hadoopcluster1, request=isCommand :true, action :null, command :KERBEROS_SERVICE_CHECK, inputs :{HAS_RESOURCE_FILTERS=true}, resourceFilters: [RequestResourceFilter{serviceName='KERBEROS', componentName='null', hostNames=[]}], exclusive: false, clusterName :hadoopcluster1
```

```
2019-05-27 15:51:29,050  WARN [ambari-client-thread-45] ADKerberosOperationHandler:471 -
Failed to communicate with the Active Directory at ldaps://adldap.x.xyz.com: simple bind failed:
adldap.x.x.com:636

javax.naming.CommunicationException: simple bind failed: adldap.x.x.com:636 [Root exception is
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No name matching
adldap.x.x.com found]


    at sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:459)

    at sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:436)

    at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:200)

    at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:124)

    at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1621)

    ... 142 more

2019-05-27 15:43:09,421 ERROR [ambari-client-thread-42] KerberosHelperImpl:2417 - Cannot
validate credentials:
org.apache.ambari.server.serveraction.kerberos.KerberosInvalidConfigurationException: Failed to
connect to KDC - Failed to communicate with the Active Directory at ldaps://adldap.x.xyz.com:
simple bind failed: adldap.x.x.com:636

Make sure the server's SSL certificate or CA certificates have been imported into Ambari's truststore.

2019-05-27 15:43:09,422 ERROR [ambari-client-thread-42] CreateHandler:80 - Bad request received:
Failed to connect to KDC - Failed to communicate with the Active Directory at
ldaps://adldap.x.xyz.com: simple bind failed: adldap.x.xyz.com:636

Make sure the server's SSL certificate or CA certificates have been imported into Ambari's truststore.
```