Launch One Windows Server in same vpc

Change Name of server as = hadoop-ad

Install – DNS server

Install – AD services

Root Domain – HADOOPSECURITY.LOCAL

Install – AD certificate

1. Create organization unit – hadoop
2. Create users -
3. Create delegation control

If you are using Active Directory: 1. Create an Organizational Unit (OU) in your AD setup where all the principals used by your CDH cluster will reside. 2. Add a new user account to Active Directory, for example, @YOUR-REALM.COM. The password for this user should be set to never expire. 3. Use AD's Delegate Control wizard to allow this new user to Create, Delete and Manage User Accounts

Note: Each account must have a user ID that is greater than or equal to 1000. In the /etc/hadoop/conf/taskcontroller.cfg file, the default setting for the banned.users property is mapred, hdfs, and bin to prevent jobs from being submitted via those user accounts. The default setting for the min.user.id property is 1000 to prevent jobs from being submitted with a user ID less than 1000, which are conventionally Unix super users

EDIT hosts file with AD private ip And host name

# The following lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

ff02::3 ip6-allhosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

10.0.0.90 hadoop-ad.hadoopsecurity.local

AD server in the hosts file on every node in the cluster.

./putnmove.sh hosts /etc/hosts

------------------------------------------------------------

Edit krb5.conf

[libdefaults]

default\_realm = HADOOPSECURITY.LOCAL

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

default\_tgs\_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5

default\_tkt\_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5

permitted\_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5

[realms]

HADOOPSECURITY.LOCAL = {

kdc = hadoop-ad.hadoopsecurity.local

admin\_server = hadoop-ad.hadoopsecurity.local

}

Install open ldap and workstation on all hosts

Install openldap-clients and krb5-workstation if it's not there.

For ubuntu

./clustercmd.sh sudo apt-get install ldap-utils

./clustercmd.sh sudo apt-get install krb5-user

RHEL

./clustercmd.sh sudo yum install openldap-clients -y

./clustercmd.sh sudo yum install krb5-workstation -y

Move krb5.conf

./putnmove.sh krb5.conf /etc/krb5.conf

Mova all policy files (RHEL)

./putnmove.sh US\_export\_policy.jar /usr/java/jdk1.7.0\_67-cloudera/jre/lib/security

./putnmove.sh local\_policy.jar /usr/java/jdk1.7.0\_67-cloudera/jre/lib/security

Ubuntu

./putnmove.sh US\_export\_policy.jar /usr/lib/jvm/j2sdk1.6-oracle/jre/lib/security

./putnmove.sh local\_policy.jar /usr/lib/jvm/j2sdk1.6-oracle/jre/lib/security

OR

./putnmove.sh local\_policy.jar /usr/lib/jvm/java-7-oracle-cloudera/jre/lib/security

./putnmove.sh US\_export\_policy.jar /usr/lib/jvm/java-7-oracle-cloudera/jre/lib/security

CONFIGURE HUE WITH KERBEROS

**Authentication Backend**

backend

Hue (Service-Wide)



**Enable LDAP TLS**

use\_start\_tls

Hue (Service-Wide)

**LDAP URL**

ldap\_url

Hue (Service-Wide)



**LDAP Search Base**

base\_dn

Hue (Service-Wide)



**Create LDAP users on login**

create\_users\_on\_login

Hue (Service-Wide)

**LDAP Bind User Distinguished Name**

bind\_dn

Hue (Service-Wide)



**LDAP Bind Password**

bind\_password

Hue (Service-Wide)



**Active Directory Domain**

nt\_domain

Hue (Service-Wide)



Add user in white listed list of YARN

Jus search white list

And add hue user

Login hue and add new hue user in hue

Key tab

Location:

/var/run/cloudera-scm-agent/process/

Ticket cache: FILE:/tmp/krb5cc\_998

Default principal: yarn@HADOOPSECURITY.LOCAL

Valid starting Expires Service principal

08/05/2017 00:39:05 08/05/2017 10:39:05 krbtgt/HADOOPSECURITY.LOCAL@HADOOPSECURITY.LOCAL

renew until 08/12/2017 00:39:01, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96