1. **prerequisites**
2. Set up and configure Hadoop (HDP 2.x) with all necessary services.
3. **Make** sure that all hosts in the realm time-synchronized.
4. **Enable Domain and Trust in Active Directory**
5. Configure network security and enable network encryption for Kerberos in the active or default local domain policy
6. In the Active Directory console, go to:  
   *Server Manager > Group Policy Management > Domain > Group Policy Objects > Default or Active Domain Policy and Edit*

*<image>*

1. Navigate to below mentioned path, and chose all the necessary encryptions.

*Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options and configure Network security: Configure Encryption types allowed for Kerberos.*

*<image>*

1. Run these commands in PowerShell to configure Windows Kerberos with realms in Linux.

*ksetup /addkdc NAMENODE.COM namenode.com  
netdom trust NAMENODE.COM /Domain: IDA.COM /add /realm /passwordt:Siemens1234  
ksetup /SetEncTypeAttr NAMENODE.COM DES-CBC-CRC DES-CBC-MD5 RC4-HMAC-MD5 AES128-CTS-HMAC-SHA1-96 AES256-CTS-HMAC-SHA1-96*

*(The password should be same as that of realm krbtgt/NAMENODE.COM@IDA.COM)*

1. **Configure Kerberos KDC**
2. Install Kerberos with latest version on NameNode.

*yum install krb5-server krb5-libs krb5-auth-dialog krb5-workstation*

1. Install Kerberos with latest version on all other nodes in the cluster

*yum -y install krb5-libs krb5-auth-dialog krb5-workstation*

1. Edit Kerberos configuration file (/etc/krb5.conf) as file attached below.

Where, HDP Cluster realm = NAMENODE.COM

And Windows Domain = IDA.COM



1. /usr/sbin/kdb5\_util create -s
2. Edit KDC configuration file (*/var/Kerberos/krb5kdc/kdc.conf*) as file attached below.

[kdcdefaults]

kdc\_port = 88

kdc\_tcp\_ports = 88

[realms]

HADOOP.COM = {

#master\_key\_type = aes256-cts

acl\_file = /var/kerberos/krb5kdc/kadm5.acl

dict\_file = /usr/share/dict/words

admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab

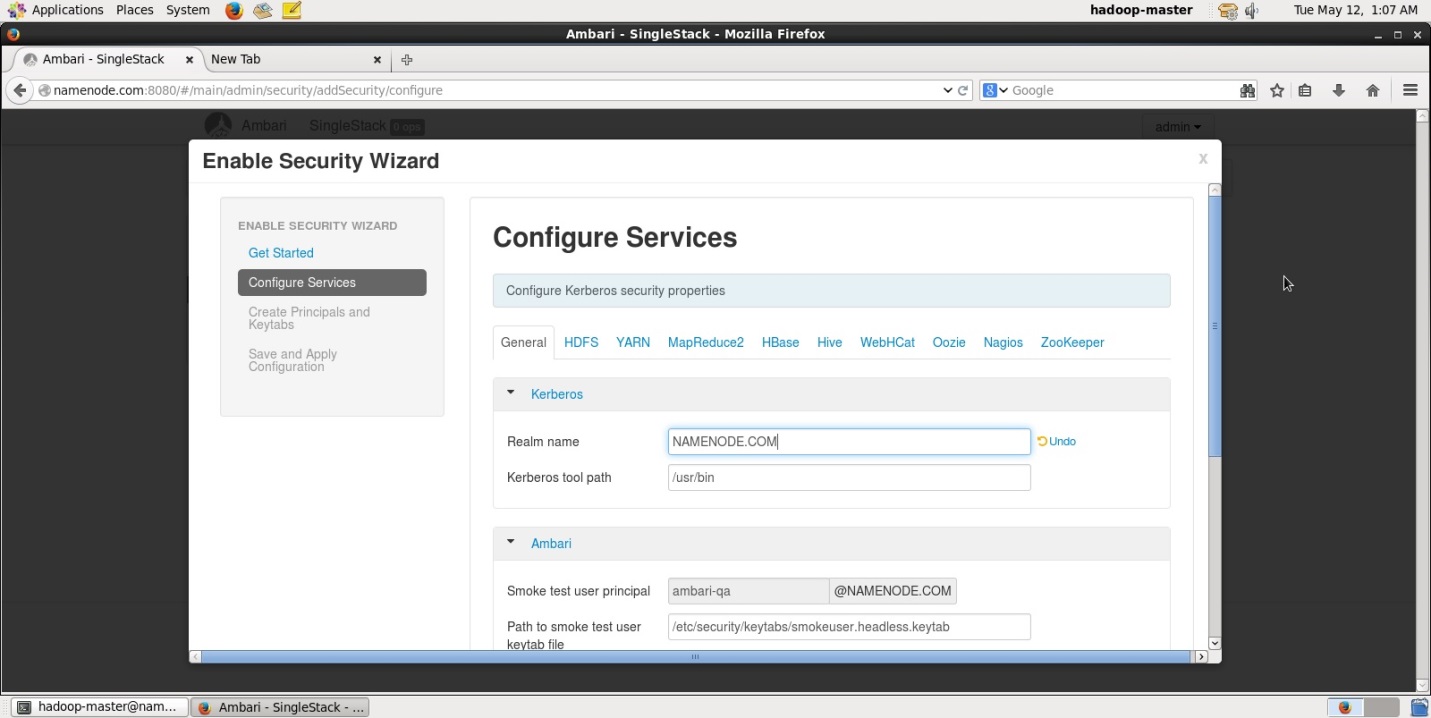
supported\_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal

}

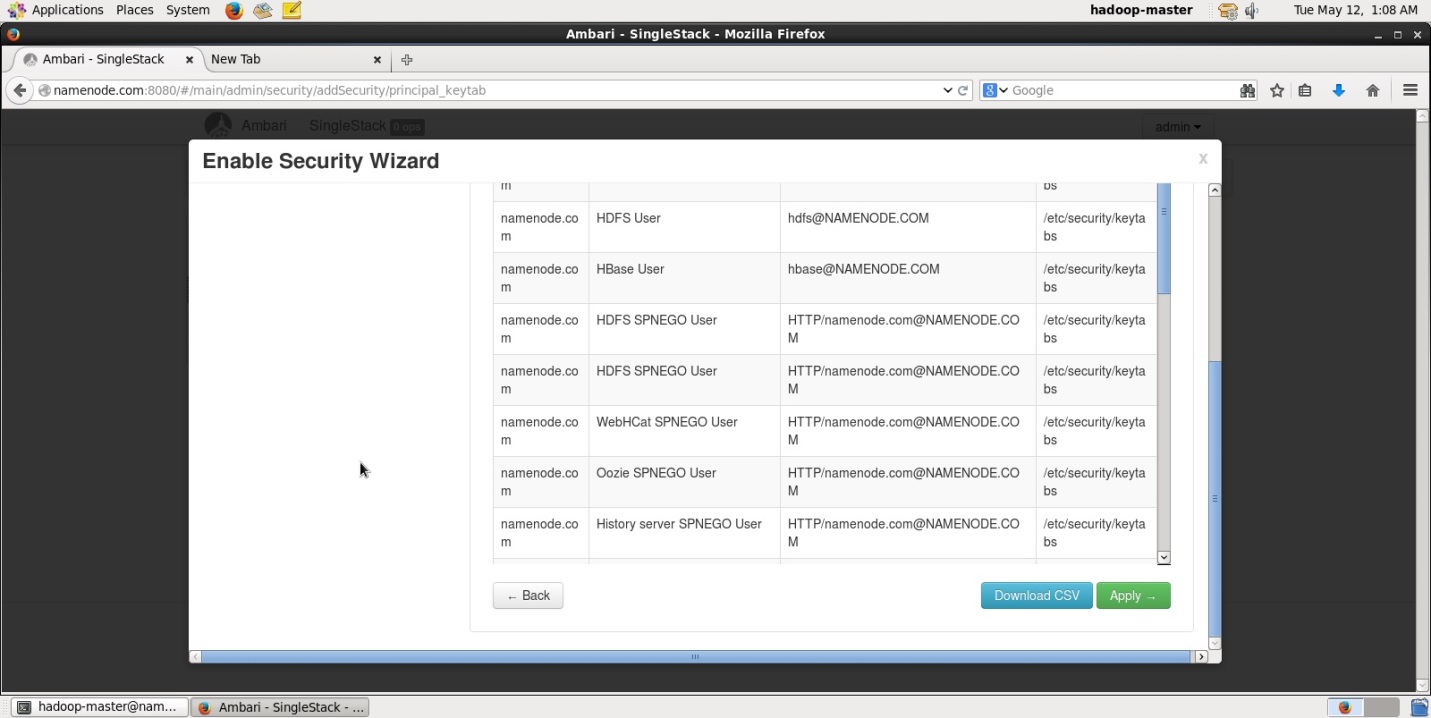
1. Enable security from Ambari
   1. Open Ambari from <http://namenode.com:8080/>
   2. Username admin, Password admin.
   3. Go to Admin 🡪 Security 🡪 Enable security

(If security is enabled by default then disable and again enable it)

* 1. In Ambari Security Wizard edit your cluster realm name, in our case, it is NAMENODE.COM



* 1. Click next to create principals and Keytabs page, which at the bottom has an option to Download CSV containing all the required information of principals and keytabs you’ll need in order to run the Kerberos script.



/var/lib/ambari-server/resources/scripts/kerberos-setup.sh /home/hadoop-master/Downloads/host-principal-keytab-list.csv ~/.ssh/id\_rsa

* 1. Note: The kerberos-setup.sh script contains some unnecessary / repeated steps that may need to comment out as shown below:



* 1. Ensure that /etc/security/keytabs/contains updated keytabs files for the Hadoop services installed on that host.
  2. Note: if the Enable security fails at step “Check HBase” with error massages “Insufficient access on 'ambarismoketest' ”, then you need to drop and create the HBase table with valid access and retry running.

#sudo -u hbase hbase shell

>scan 'ambarismoketest'

>disable 'ambarismoketest'

>drop 'ambarismoketest'

>create 'ambarismoketest', {NAME => 'family'}

>put 'ambarismoketest', 'row01', 'family:col01', '<copy\_this value\_from\_scan\_output>'

>grant 'ambari-qa', 'RWCXA' , 'ambarismoketest', 'family'

* 1. Note: If at any step, it fails with massage “time out error”, then click on **Retry** button.

1. Create a Kerberos administrator
   1. Run the command below and provide a strong password.

/usr/sbin/kadmin.local -q "addprinc root/admin”

(If principle already exists delete it with delprinc option)

* 1. Make sure the ACL file (/var/kerberos/krb5kdc/kadm5.acl) have correct realm name as shown below.

\*/admin@NAMENODE.COM \*

* 1. Add the Kerberos key distribution center account called **krbtgt**

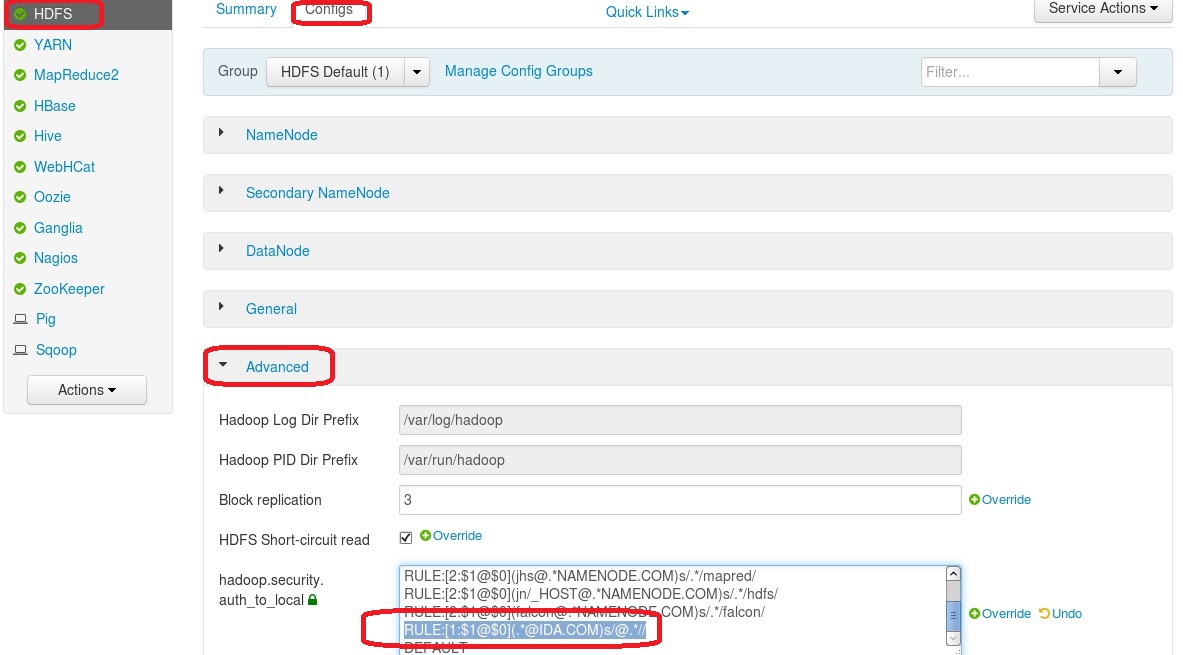
kadmin.local

addprinc -e "aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal" krbtgt/NAMENODE.COM@IDA.COM

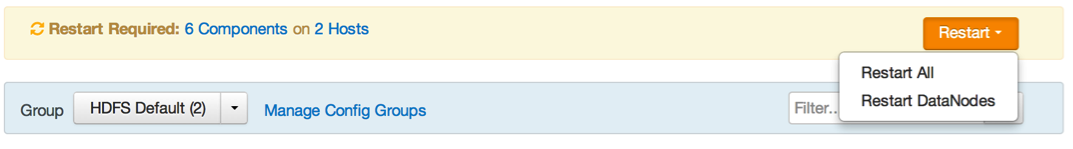
* 1. Obtain a Kerberos ticket with admin user.

kinit root/admin@NAMENODE.COM

1. restart Kerberos services:  
   /sbin/service krb5kdc restart  
   /sbin/service kadmin restart
2. Add rule with variable *hadoop.security.auth\_to\_local* by adding *RULE:[1:$1@$0](.\*@IDA.COM)s/@.\*//*



1. Restart the Hadoop services from Ambari.



1. Authenticate users from the AD and get tickets. Initialize user by running the command below and assign the AD user password.

kinit [IC009965@IDA.COM](mailto:IC009965@IDA.COM)

1. Check the creation of Kerberos TGT by running klist command. Output should like this:

<image>

1. Test by accessing the Hadoop services from kerberised user. E.g.

Sudo –u IC009965 hadoop fs –ls /