To verify that a client host is ready to use the AES-NI instruction set optimization for HDFS encryption, use the following command:

hadoop checknative

ln -s /usr/lib64/libcrypto.so.1.0.1e /usr/lib64/libcrypto.so

yum install openssl-devel

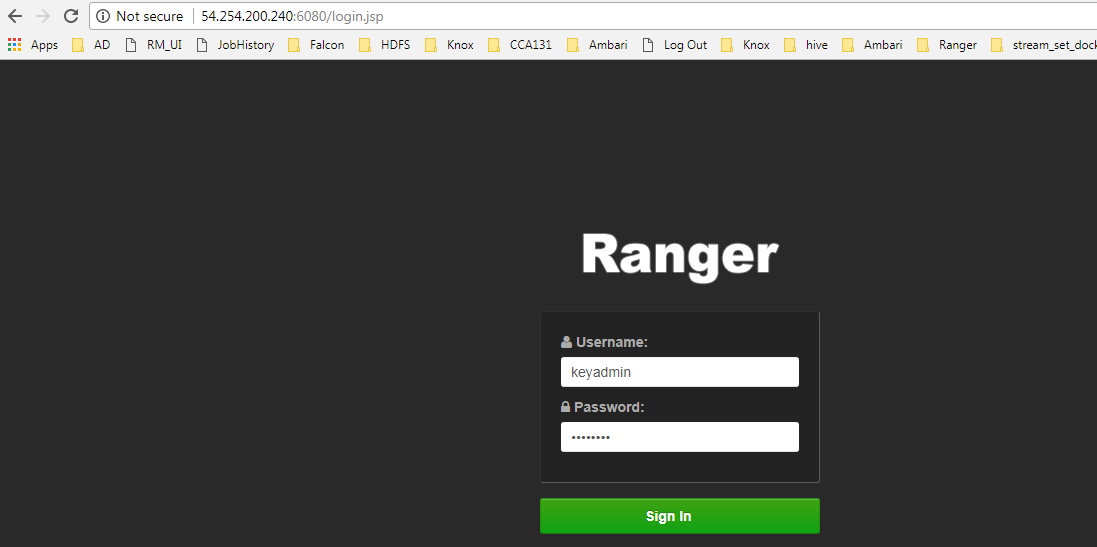
AES-NI optimization requires an extended CPU instruction set for AES hardware acceleration.

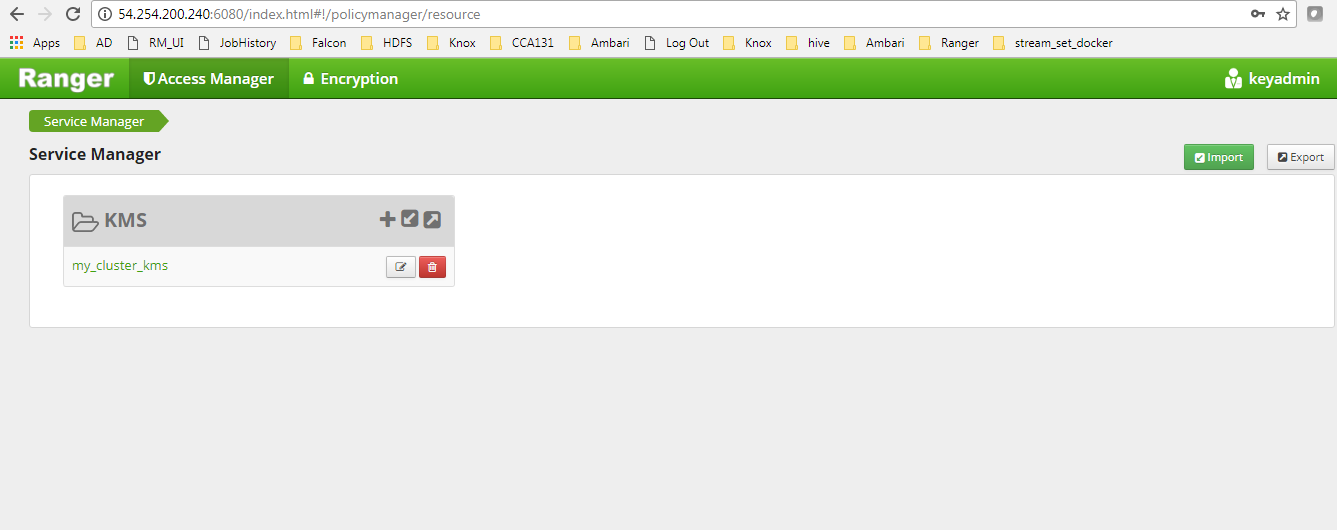
cat /proc/cpuinfo | grep aes

Under Custom core-site.xml, set the value of the hadoop.proxyuser.kms.groups property to \* or service user

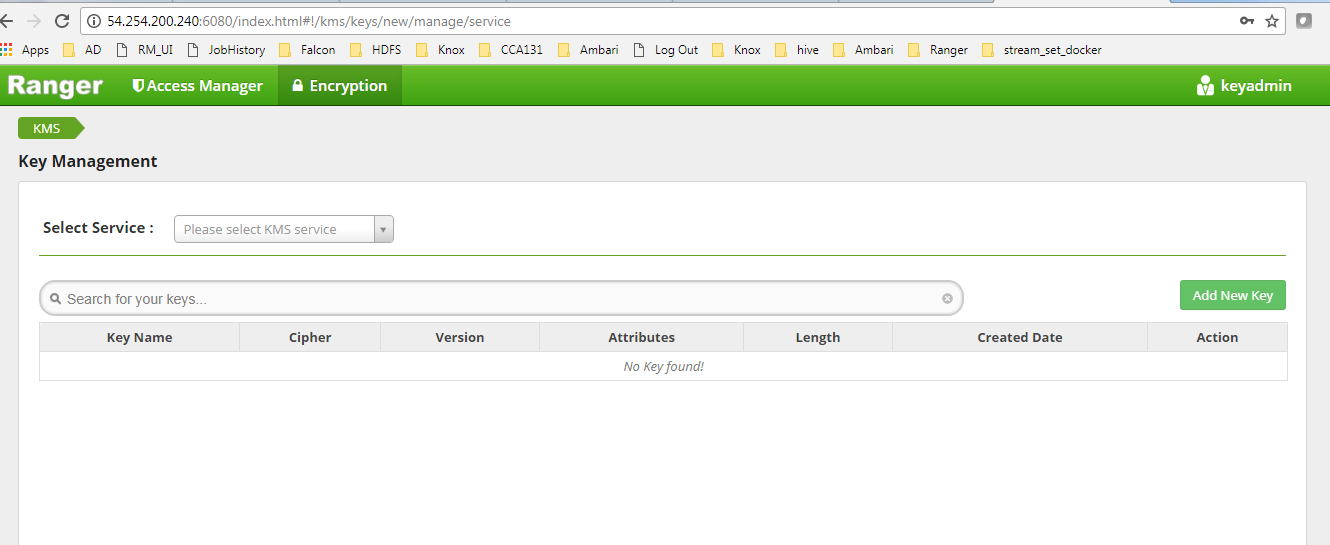
Add service Ranger KMS ( Need to add Ranger service before this )

Login as keyadmin / keyadmin

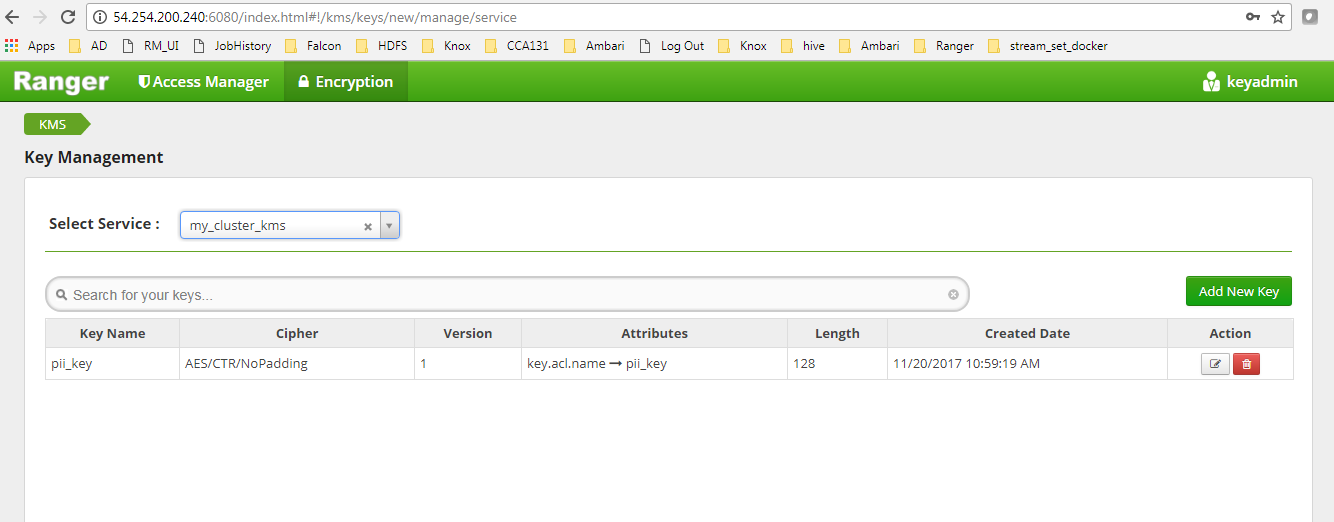




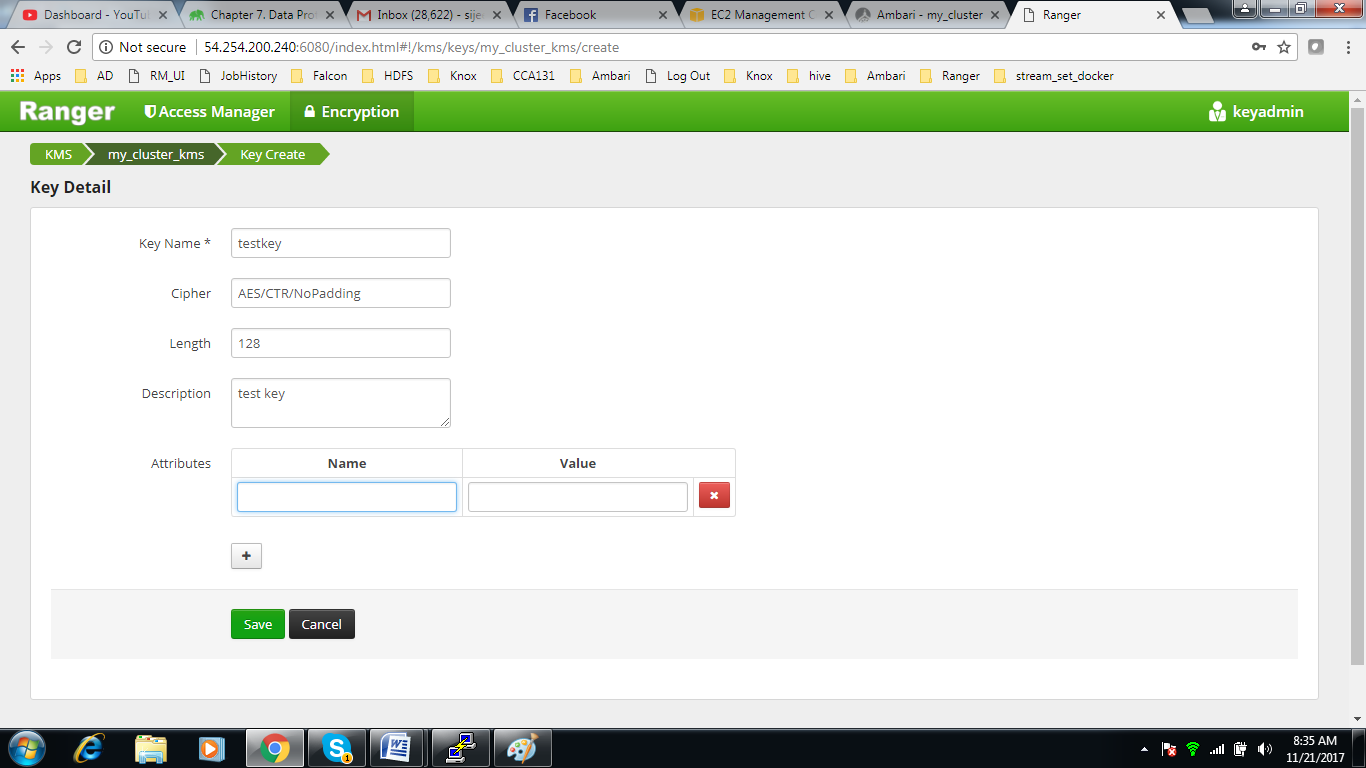
Select Encryption -> Keymanager

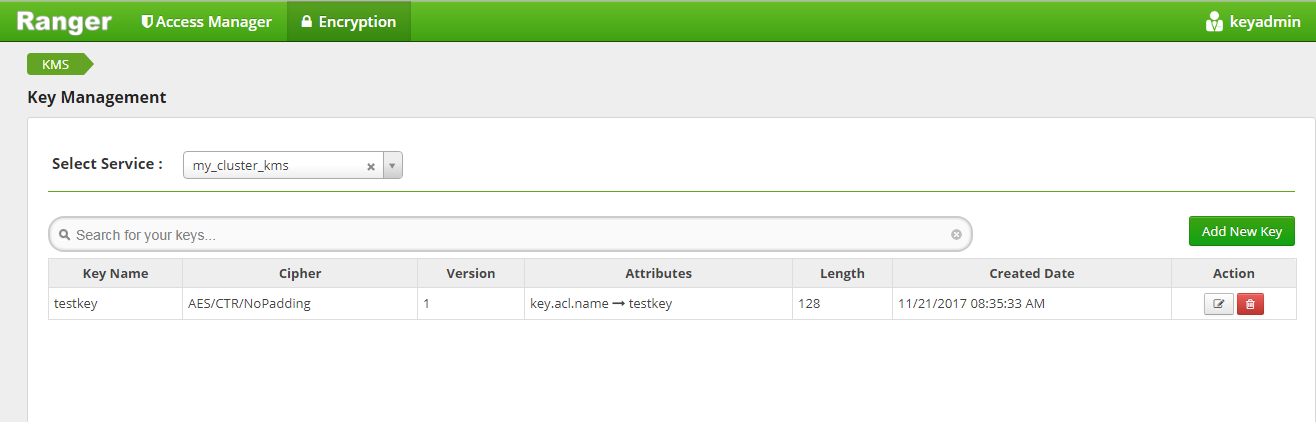


Select Service

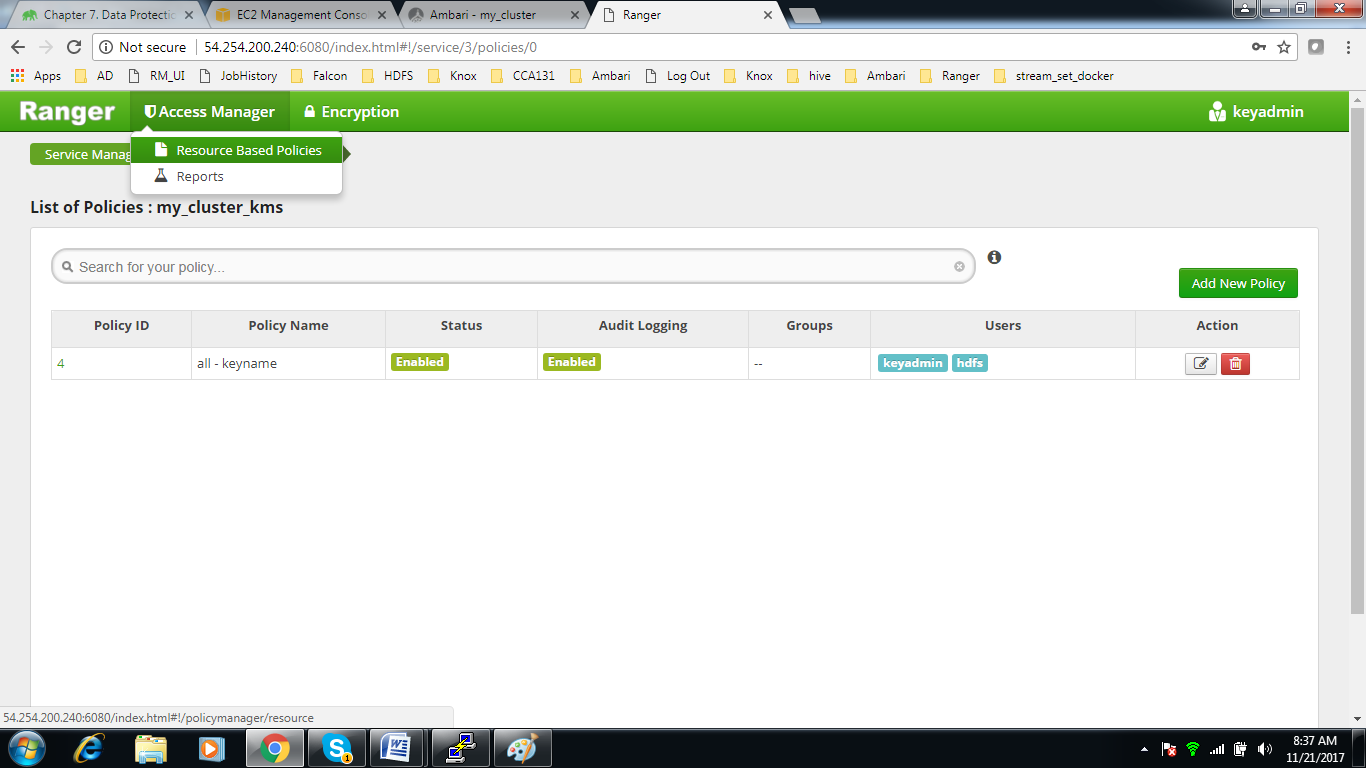


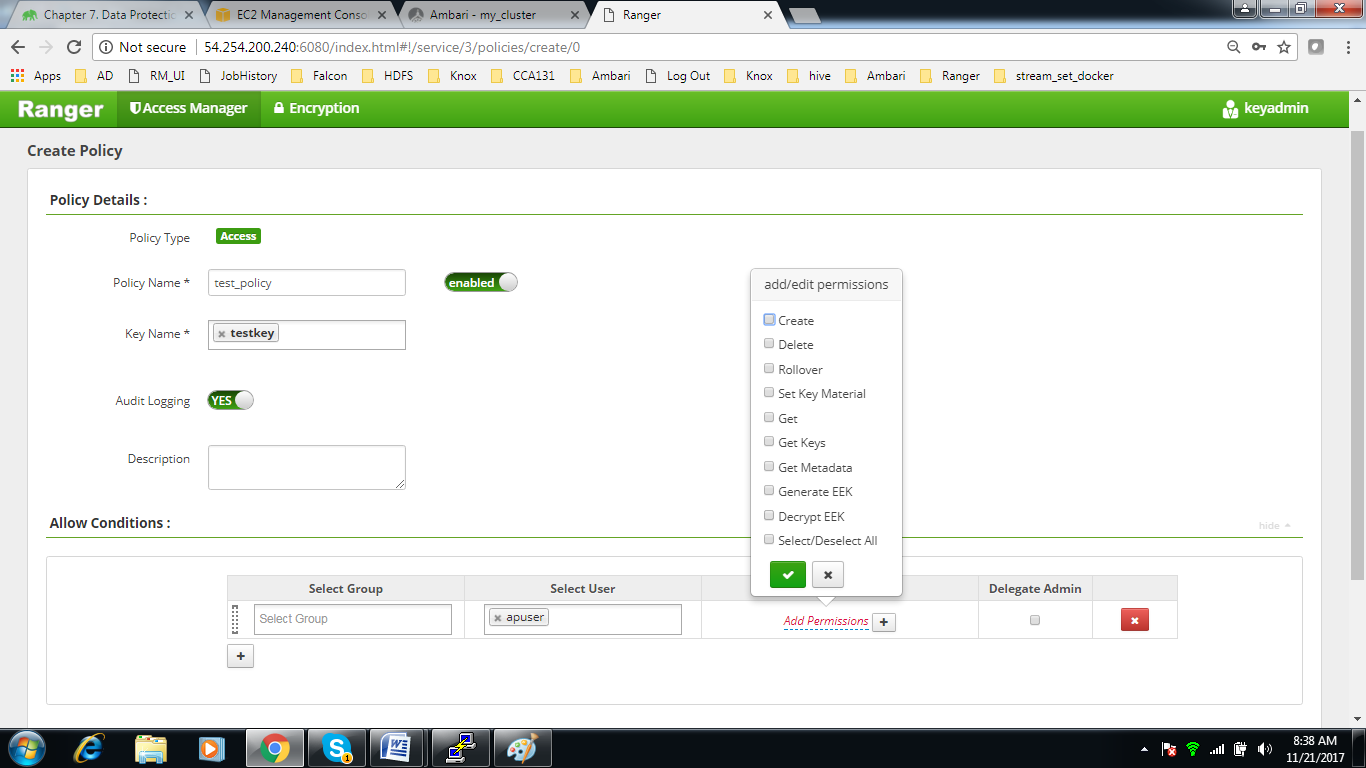
Add New Key





Add new policy Access Manager -> Resource Based Policy





As hdfs user execute the bellow command

[hdfs@domU-12-31-38-04-B4-88 ~]$ hdfs crypto -createZone -keyName testkey -path /user/apuser/ap\_encrypted

Added encryption zone /user/apuser/ap\_encrypted

[hdfs@domU-12-31-38-04-B4-88 ~]$

From Ranger KMS provide Decrypt EEK permission to users apuser and nauser , these two users would be able to access data from encryption zone created by key **testkey**

