GSS/Kerberos setup guide for Lustre

short URL: http://goo.gl/yWTvzT
Author: Andrew Perepechko
2014-10-29

KDC setup

Assuming we chose LUSTRE as the Kerberos realm name.

1. *yum install krb5-server krb5-libs*
2. edit **/var/kerberos/krb5kdc/kdc.conf**, replace EXAMPLE.COM with the uppercase domain name, e.g. LUSTRE (this is called the realm)
3. edit **/etc/krb5.conf**, replace EXAMPLE.COM with the uppercase domain name, e.g. LUSTRE (the realm), set “kdc” and “admin_server” to the domain name of KDC, e.g. localhost.localdomain, add domain->realm translation to [domain_realm] section, e.g. “.localdomain = LUSTRE”, “localdomain = LUSTRE”.
4. run *kdb5_util create -s* to create the key database
5. edit **/var/kerberos/krb5kdc/kadm5.acl**, add “*/admin@LUSTRE *” to allow admin actions
6. *kadmin.local -q "addprinc root/admin"*
7. */sbin/service krb5kdc start && /sbin/service kadmin start*

It is important that every client and server should be able to translate each other’s addresses to host names. This is usually achieved by using a single domain name system, which can be replaced by filling out /etc/hosts and keeping them synchronous, but the latter solution is error-prone.

Firewall needs to be configured for communication through a few ports:

TCP/UDP Port 88 should be accessible in order to be able to reach KDC from network.
TCP/UDP Ports 464, 749 should be accessible in order to be able to reach kadmin from network.

Generic Kerberos client setup

1. *yum install krb5-libs krb5-workstation*
2. edit /etc/krb5.conf as described for the KDC setup (be sure to use the real domain name for kdc/admin_server, localhost will not work for a host which is not itself KDC!)

Assuming client host name is sdac-1.

1. [on KDC] kadmin.local: *addprinc -randkey host/sdac-1*
2. [on client] kadmin: *ktadd -k /etc/krb5.keytab host/sdac-1*

Testing generic Kerberos setup with ssh

This section is only relevant if you want to test basic (non-Lustre) Kerberos installation and setup.

Choose a client and a server. Assume sdac-1 is the client and sdac-2 is the server, LUSTRE is the realm.

1. add “*GSSAPIKeyExchange yes*” to /etc/ssh/ssh_config on the client
2. add “*GSSAPIAuthentication yes*” to /etc/ssh/sshd_config on the server
3. add “*GSSAPIKeyExchange yes*” to /etc/ssh/sshd_config on the server
4. add “*root/admin@LUSTRE*” to /root/.k5login on the server
5. execute “kinit root/admin@LUSTRE” from the client, enter password
6. ssh sdac-2

You should be able to log in without using a key or entering your password.

Building Lustre

In order to build Lustre, one needs to install libgssglue, libgssglue-devel, krb5-libs, krb5-devel and run *configure --enable-gss* for Lustre itself.

Lustre client Kerberos setup

Assuming client host name is sdac-2.

1. kadmin: addprinc -randkey lustre_root/sdac-2@LUSTRE
2. kadmin: ktadd -k /etc/krb5.keytab lustre_root/sdac-2@LUSTRE
3. echo " nfsd   /proc/fs/nfsd   nfsd   defaults   0 0 " >> /etc/fstab
4. echo "create lgssc * * /usr/sbin/lgss_keyring %o %k %t %d %c %u %g %T %P %S" >> /etc/request-key.conf
5. start /usr/sbin/lsvcgssd

One more step can be useful in order to run sanity-krb5.sh in the future:

1. [on KDC] kadmin.local: *addprinc sanityusr@LUSTRE*

Lustre server Kerberos setup

Assuming the Lustre server host name is sdac-1. “lustre_mds” should be replaced by lustre_oss or lustre_mgs for OSS and MGS servers.

1. kadmin: addprinc -randkey lustre_mds/sdac-1@LUSTRE
2. kadmin: ktadd -k /etc/krb5.keytab lustre_mds/sdac-1@LUSTRE
3. echo " nfsd   /proc/fs/nfsd   nfsd   defaults   0 0 " >> /etc/fstab
4. echo "create lgssc * * /usr/sbin/lgss_keyring %o %k %t %d %c %u %g %T %P %S" >> /etc/request-key.conf
5. start /usr/sbin/lsvcgssd