

Step 1: Add User on LDAP server and principles in kerberos

```
[root@ip-172-31-42-187 ~]# rpm -qa | grep openldap*
openldap-clients-2.4.40-13.el7.x86_64
openldap-2.4.40-13.el7.x86_64
openldap-servers-2.4.40-13.el7.x86_64
[root@ip-172-31-42-187 ~]# useradd newman
[root@ip-172-31-42-187 ~]# passwd newman
Changing password for user newman.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-42-187 ~]# kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local: addprinc newman
WARNING: no policy specified for newman@EXAMPLE.COM; defaulting to no policy
Enter password for principal "newman@EXAMPLE.COM":
Re-enter password for principal "newman@EXAMPLE.COM":
Principal "newman@EXAMPLE.COM" created.
```

Step 2: check created Principle

```
kadmin.local: list_principals
HTTP/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
HTTP/ip-172-31-44-158.ec2.internal@EXAMPLE.COM
K/M@EXAMPLE.COM
ambari-ga-testing_rs@EXAMPLE.COM
ambari-server-testing_rs@EXAMPLE.COM
amshbase/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
amszk/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
ashnee@EXAMPLE.COM
demolo@EXAMPLE.COM
dn/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
dn/ip-172-31-44-158.ec2.internal@EXAMPLE.COM
hbase-testing_rs@EXAMPLE.COM
hbase/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
hbase/ip-172-31-44-158.ec2.internal@EXAMPLE.COM
hdfs-testing_rs@EXAMPLE.COM
hitman@EXAMPLE.COM
hive/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
hive/ip-172-31-44-158.ec2.internal@EXAMPLE.COM
host/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
jhs/ip-172-31-44-158.ec2.internal@EXAMPLE.COM
kadmin/admin@EXAMPLE.COM
kadmin/changepw@EXAMPLE.COM
kadmin/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
kiprop/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
knox/ip-172-31-42-187.ec2.internal@EXAMPLE.COM
krbtgt/EXAMPLE.COM@EXAMPLE.COM
newman@EXAMPLE.COM
```

Step 3: add keytab for newuser in kerberos

```
kadmin.local: exit
[root@ip-172-31-42-187 ~]# cd /var/kerberos/mykeytab/
[root@ip-172-31-42-187 mykeytab]# kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local: ktadd -k newman -norandkey newman@EXAMPLE.COM
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type aes256-cts-hmac-sha1-96 added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type des3-cbc-sha1 added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type arcfour-hmac added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type camellia256-cts-cmac added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type camellia128-cts-cmac added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type des-hmac-sha1 added to keytab WRFILE:newman.
Entry for principal newman@EXAMPLE.COM with kvno 1, encryption type des-cbc-md5 added to keytab WRFILE:newman.
kadmin.local: exit
[root@ip-172-31-42-187 mykeytab]# ktutil
ktutil: read_kt /var/kerberos/mykeytab/newman
ktutil: list
slot KVNO Principal
-----
 1      1      newman@EXAMPLE.COM
 2      1      newman@EXAMPLE.COM
 3      1      newman@EXAMPLE.COM
 4      1      newman@EXAMPLE.COM
 5      1      newman@EXAMPLE.COM
 6      1      newman@EXAMPLE.COM
 7      1      newman@EXAMPLE.COM
 8      1      newman@EXAMPLE.COM
ktutil: exit
[root@ip-172-31-42-187 mykeytab]#
```

Step 4: go cd /usr/share/migrationtools for adding entry of newman user in ldap

```
[root@ip-172-31-42-187 migrationtools]# ll
total 144
-rw-r--r-- 1 root root 15 Jun 14 05:39 group
-rw-r--r-- 1 root root 133 Jun 14 05:45 groups.ldif
-rwxr-xr-x 1 root root 2652 Dec 28 2013 migrate_aliases.pl
-rwxr-xr-x 1 root root 2950 Dec 28 2013 migrate_all_netinfo_offline.sh
-rwxr-xr-x 1 root root 2946 Dec 28 2013 migrate_all_netinfo_online.sh
-rwxr-xr-x 1 root root 3011 Dec 28 2013 migrate_all_nis_offline.sh
-rwxr-xr-x 1 root root 3006 Dec 28 2013 migrate_all_nis_online.sh
-rwxr-xr-x 1 root root 3164 Dec 28 2013 migrate_all_nisplus_offline.sh
-rwxr-xr-x 1 root root 3146 Dec 28 2013 migrate_all_nisplus_online.sh
-rwxr-xr-x 1 root root 5267 Dec 28 2013 migrate_all_offline.sh
-rwxr-xr-x 1 root root 7468 Dec 28 2013 migrate_all_online.sh
-rwxr-xr-x 1 root root 3278 Dec 28 2013 migrate_automount.pl
-rwxr-xr-x 1 root root 2608 Dec 28 2013 migrate_base.pl
-rw-r--r-- 1 root root 8886 Jun 9 03:50 migrate_common.ph
-rwxr-xr-x 1 root root 2952 Dec 28 2013 migrate_fstab.pl
-rwxr-xr-x 1 root root 2714 Dec 28 2013 migrate_group.pl
-rwxr-xr-x 1 root root 3087 Dec 28 2013 migrate_hosts.pl
-rwxr-xr-x 1 root root 2856 Dec 28 2013 migrate_netgroup_byhost.pl
-rwxr-xr-x 1 root root 2856 Dec 28 2013 migrate_netgroup_byuser.pl
-rwxr-xr-x 1 root root 3879 Dec 28 2013 migrate_netgroup.pl
-rwxr-xr-x 1 root root 2840 Dec 28 2013 migrate_networks.pl
-rwxr-xr-x 1 root root 5635 Dec 28 2013 migrate_passwd.pl
-rwxr-xr-x 1 root root 2428 Dec 28 2013 migrate_profile.pl
-rwxr-xr-x 1 root root 2873 Dec 28 2013 migrate_protocols.pl
-rwxr-xr-x 1 root root 2854 Dec 28 2013 migrate_rpc.pl
-rwxr-xr-x 1 root root 11465 Dec 28 2013 migrate_services.pl
-rwxr-xr-x 1 root root 3419 Dec 28 2013 migrate_slapd_conf.pl
-rw-r--r-- 1 root root 43 Jun 14 05:38 passwd
-rw-r--r-- 1 root root 527 Jun 14 05:39 users.ldif
[root@ip-172-31-42-187 migrationtools]# rm -rvf passwd group
removed âpasswdâ
removed âgroupâ
[root@ip-172-31-42-187 migrationtools]#
```

Step 5: add entry of user and group in passwd and group

```
[root@ip-172-31-42-187 migrationtools]# tail -n1 /etc/passwd >> passwd
[root@ip-172-31-42-187 migrationtools]# cat passwd
newman:x:1026:1026::/home/newman:/bin/bash
[root@ip-172-31-42-187 migrationtools]# ./migrate_passwd.pl passwd users.ldif
[root@ip-172-31-42-187 migrationtools]# ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f users.ldif
adding new entry "uid=newman,ou=People,dc=example,dc=com"

[root@ip-172-31-42-187 migrationtools]# tail -n1 /etc/group
groff/ group group-
[root@ip-172-31-42-187 migrationtools]# tail -n1 /etc/group >> group
[root@ip-172-31-42-187 migrationtools]# ./migrate_group.pl group groups.ldif
[root@ip-172-31-42-187 migrationtools]# ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f groups.ldif
adding new entry "cn=newman,ou=Group,dc=example,dc=com"

[root@ip-172-31-42-187 migrationtools]#
```

Step 6 : Now try to connect with newman user and check klist and home directory

```
Connection to t1 closed.
[root@ip-172-31-42-187 ~]# ssh newman@t2
newman@t2's password:
Could not chdir to home directory /home/newman: No such file or directory
-bash-4.2$ klist
Ticket cache: FILE:/tmp/krb5cc_1026
Default principal: newman@EXAMPLE.COM

Valid starting      Expires            Service principal
06/14/2017 07:41:11 06/15/2017 07:41:11  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 06/21/2017 07:41:11
-bash-4.2$ exit
logout
Connection to t2 closed.
[root@ip-172-31-42-187 ~]# cd /home
[root@ip-172-31-42-187 home]# ll
total 12
drwx----- 4 ambari-qa  hadoop    103 Jun 12 06:44 ambari-qa
drwx----- 3 ams        hadoop     87 Jun 12 06:39 ams
drw-r--r--  2 ashnee    ashnee     83 Jun  9 08:14 ashnee
drwx----- 2 demolo     demolo     83 Jun 14 05:37 demolo
drwx----- 3 ec2-user   ec2-user   95 Jun  9 02:00 ec2-user
-rw-r--r--  1 root      root      175 Jun  9 08:01 group
-rw-r--r--  1 root      root       15 Jun  9 08:13 groups
drwxr-xr-x  5 root      root       60 Jun  9 07:47 guests
drwx----- 3 hbase     hadoop     87 Jun 12 06:36 hbase
drwx----- 2 hcat      hadoop     62 Jun 12 06:24 hcat
drwx----- 5 hdfs      hadoop    156 Jun 14 02:39 hdfs
drwx----- 2 hitman    hitman     83 Jun 14 03:20 hitman
drwx----- 3 hive      hadoop    145 Jun 13 03:09 hive
drwx----- 3 knox      hadoop     87 Jun 12 06:36 knox
drwx----- 2 mapred    hadoop     62 Jun 12 06:24 mapred
drwx----- 2 newman    newman     83 Jun 14 07:40 newman
-rw-r--r--  1 root      root       43 Jun  9 08:11 passwd
drwx----- 4 rahul     rahul     124 Jun 13 04:17 rahul
drwx----- 2 ranger    hadoop     62 Jun 12 07:37 ranger
drwx----- 2 saif      saif       83 Jun 14 02:40 saif
drwx----- 3 shehbaz   shehbaz   108 Jun 12 09:26 shehbaz
drwx----- 3 spark     hadoop     87 Jun 12 06:37 spark
drwx----- 2 t3        t3        83 Jun 12 05:32 t3
drwx----- 2 tez        hadoop     62 Jun 12 06:24 tez
drwx----- 3 yarn      hadoop    108 Jun 13 03:09 yarn
drwx----- 3 zookeeper hadoop     87 Jun 12 06:36 zookeeper
[root@ip-172-31-42-187 home]#
```

Step 7 : go to ambari ui and check for user and group sink in ranger

Ranger Access Manager Audit Settings admin

Users/Groups

UsersGroups

User List

Add New UserSet Visibility

| | User Name | Email Address | Role | User Source | Groups | Visibility |
|--------------------------|-----------|---------------|------|-------------|--------|------------|
| <input type="checkbox"/> | newman | | User | External | -- | Visible |

Ranger Access Manager Audit Settings admin

Users/Groups

UsersGroups

Group List

Add New GroupSet Visibility

| | Group Name | Group Source | Visibility |
|--------------------------|------------|--------------|------------|
| <input type="checkbox"/> | demolo | External | Visible |
| <input type="checkbox"/> | newman | External | Visible |

```
# rpm -qa | grep openldap*

# useradd newman

# passwd newman

# kadmin.local

    Kadmin.local: Addprinc newman

    Kadmin.local: list_principals

    Kadmin.local: exit

# cd /var/Kerberos/mykeytab

# kadmin.local

    Kadmin.local: ktadd -k newman -norandkey newman@EXAMPLE.COM

    Kadmin.local: read_kt /var/Kerberos/mykeytab/newman

    Kadmin.local: list

    Kadmin.local: exit

# cd /usr/share/migrationtools

# ll

#rm -rvf passwd group

tail -n1 /etc/passwd >> passwd

cat passwd

./migrate_passwd.pl passwd users.ldif

ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f users.ldif

tail -n1 /etc/group >> group

./migrate_group.pl group groups.ldif

ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f groups.ldif

cd
```