1. Set host name

|  |
| --- |
| [root@mac127 ~]# hostnamectl set-hostname mac127.cybage.com  [root@mac127 ~]# hostname  mac127.cybage.com |

Add new user to filesystem

|  |
| --- |
| [root@mac127 ~]# **useradd shalaj**  [root@mac127 ~]# |

|  |
| --- |
| #yum install krb5-server krb5-workstation pam-krb5 |

|  |
| --- |
| [root@mac127 ~]# yum install krb5-server krb5-workstation pam-krb5  Loaded plugins: fastestmirror, langpacks  Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast  base | 3.6 kB 00:00:00  cloudera-manager | 951 B 00:00:00  extras | 3.4 kB 00:00:00  mysql-connectors-community | 2.5 kB 00:00:00  mysql-tools-community | 2.5 kB 00:00:00  mysql56-community | 2.5 kB 00:00:00  updates | 3.4 kB 00:00:00  (1/5): mysql-connectors-community/x86\_64/primary\_db | 13 kB 00:00:00  (2/5): extras/7/x86\_64/primary\_db | 151 kB 00:00:00  (3/5): mysql-tools-community/x86\_64/primary\_db | 33 kB 00:00:02  (4/5): updates/7/x86\_64/primary\_db | 4.8 MB 00:00:03  (5/5): mysql56-community/x86\_64/primary\_db | 168 kB 00:00:05  Loading mirror speeds from cached hostfile  \* base: mirror.fibergrid.in  \* extras: mirror.fibergrid.in  \* updates: mirror.fibergrid.in  Package krb5-workstation-1.14.1-27.el7\_3.x86\_64 already installed and latest version  No package pam-krb5 available.  Resolving Dependencies  --> Running transaction check  ---> Package krb5-server.x86\_64 0:1.14.1-27.el7\_3 will be installed  extras/7/x86\_64/filelists\_db | 770 kB 00:00:00  mysql-connectors-community/x86\_64/filelists\_db | 15 kB 00:00:00  mysql-tools-community/x86\_64/filelists\_db | 99 kB 00:00:00  mysql56-community/x86\_64/filelists\_db | 547 kB 00:00:00  updates/7/x86\_64/filelists\_db | 2.9 MB 00:00:00  --> Finished Dependency Resolution  Dependencies Resolved  ==========================================================================================================================  Package Arch Version Repository Size  ==========================================================================================================================  Installing:  krb5-server x86\_64 1.14.1-27.el7\_3 updates 977 k  Transaction Summary  ==========================================================================================================================  Install 1 Package  Total download size: 977 k  Installed size: 1.3 M  Is this ok [y/d/N]: y  Downloading packages:  krb5-server-1.14.1-27.el7\_3.x86\_64.rpm | 977 kB 00:00:00  Running transaction check  Running transaction test  Transaction test succeeded  Running transaction  Installing : krb5-server-1.14.1-27.el7\_3.x86\_64 1/1  Verifying : krb5-server-1.14.1-27.el7\_3.x86\_64 1/1  Installed:  krb5-server.x86\_64 0:1.14.1-27.el7\_3  Complete! |

|  |
| --- |
| [root@mac127 ~]# **cd /var/kerberos/krb5kdc/**  [root@mac127 krb5kdc]# ls  kadm5.acl kdc.conf  [root@mac127 krb5kdc]# **vi kadm5.acl** |

Replace EXAMPLE.COM to CYBAGE.COM

|  |  |
| --- | --- |
| **Original file** | **Update file** |
| \*/admin@EXAMPLE.COM \* | \*/admin@CYBAGE.COM \* |

|  |
| --- |
| **vi kdc.conf**  -- Replace EXAMPLE.COM to CYBAGE.COM  [kdcdefaults]  kdc\_ports = 88  kdc\_tcp\_ports = 88  [realms]  CYBAGE.COM = {  #master\_key\_type = aes256-cts  acl\_file = /var/kerberos/krb5kdc/kadm5.acl  dict\_file = /usr/share/dict/words  supported\_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal camellia256-cts:normal camellia128-cts:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal  } |

---- Need to check <start> ignore this---------------------

|  |
| --- |
| [kdcdefaults]  kdc\_ports = 88  kdc\_tcp\_ports = 88  [realms]  CYBAGE.COM = {  #master\_key\_type = aes256-cts  acl\_file = /var/kerberos/krb5kdc/kadm5.acl  dict\_file = /usr/share/dict/words  max\_renewable\_life = 7d  max\_life = 1d  admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab  supported\_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal camellia256-cts:normal camellia128-cts:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal  default\_principal\_flags = +renewable, +forwardable  } |

---- Need to check <end> ---------------------

|  |
| --- |
| **vi /etc/krb5.conf** |

|  |  |
| --- | --- |
| **Default file** | **Updated file** |
| # Configuration snippets may be placed in this directory as well  includedir /etc/krb5.conf.d/  [logging]  default = FILE:/var/log/krb5libs.log  kdc = FILE:/var/log/krb5kdc.log  admin\_server = FILE:/var/log/kadmind.log  [libdefaults]  dns\_lookup\_realm = false  ticket\_lifetime = 24h  renew\_lifetime = 7d  forwardable = true  rdns = false  # default\_realm = EXAMPLE.COM  default\_ccache\_name = KEYRING:persistent:%{uid}  [realms]  # EXAMPLE.COM = {  # kdc = kerberos.example.com  # admin\_server = kerberos.example.com  # }  [domain\_realm]  # .example.com = EXAMPLE.COM  # example.com = EXAMPLE.COM | # Configuration snippets may be placed in this directory as well  includedir /etc/krb5.conf.d/  [logging]  default = FILE:/var/log/krb5libs.log  kdc = FILE:/var/log/krb5kdc.log  admin\_server = FILE:/var/log/kadmind.log  [libdefaults]  dns\_lookup\_realm = false  ticket\_lifetime = 24h  renew\_lifetime = 7d  forwardable = true  rdns = false  default\_realm = CYBAGE.COM  default\_ccache\_name = KEYRING:persistent:%{uid}  [realms]  CYBAGE.COM = {  kdc = mac127.cybge.com  admin\_server = mac127.cybage.com  }  [domain\_realm]  .cybage.com = CYBAGE.COM  cybagee.com = CYBAGE.COM |

|  |
| --- |
| [root@mac127 krb5kdc]# **kdb5\_util create -s -r CYBAGE.COM**  Loading random data  Initializing database '/var/kerberos/krb5kdc/principal' for realm 'CYBAGE.COM',  master key name 'K/M@CYBAGE.COM'  You will be prompted for the database Master Password.  It is important that you NOT FORGET this password.  Enter KDC database master key:  Re-enter KDC database master key to verify:  [root@mac127 krb5kdc]# |

Password given – master@123

List principal

|  |
| --- |
| [root@mac127 krb5kdc]# pwd  /var/kerberos/krb5kdc  [root@mac127 krb5kdc]# ls  kadm5.acl kdc.conf principal principal.kadm5 principal.kadm5.lock principal.ok |

|  |
| --- |
| [root@mac127 krb5kdc]# **systemctl start krb5kdc kadmin**  [root@mac127 krb5kdc]# **systemctl enable krb5kdc kadmin**  Created symlink from /etc/systemd/system/multi-user.target.wants/krb5kdc.service to /usr/lib/systemd/system/krb5kdc.service.  Created symlink from /etc/systemd/system/multi-user.target.wants/kadmin.service to /usr/lib/systemd/system/kadmin.service. |

|  |
| --- |
| [root@mac127 krb5kdc]# **kadmin.local**  Authenticating as principal root/admin@CYBAGE.COM with password.  kadmin.local: **listprincs**  K/M@CYBAGE.COM  kadmin/admin@CYBAGE.COM  kadmin/changepw@CYBAGE.COM  kadmin/mac127.cybage.com@CYBAGE.COM  kiprop/mac127.cybage.com@CYBAGE.COM  krbtgt/CYBAGE.COM@CYBAGE.COM |

For Cloudera

|  |
| --- |
| kadmin.local: **addprinc cloudera-scm/admin**  WARNING: no policy specified for cloudera-scm/admin@CYBAGE.COM; defaulting to no policy  Enter password for principal "cloudera-scm/admin@CYBAGE.COM":  Re-enter password for principal "cloudera-scm/admin@CYBAGE.COM":  Principal "cloudera-scm/admin@CYBAGE.COM" created.  kadmin.local: |

Password- cloudera

Need to add root in principal list

|  |
| --- |
| kadmin.local: **addprinc root/admin**  WARNING: no policy specified for root/admin@CYBAGE.COM; defaulting to no policy  Enter password for principal "root/admin@CYBAGE.COM":  Re-enter password for principal "root/admin@CYBAGE.COM":  Principal "root/admin@CYBAGE.COM" created. |

Password – root@123

Now again list the principal, now you can see root/admin has been added

|  |
| --- |
| kadmin.local: **listprincs**  K/M@CYBAGE.COM  kadmin/admin@CYBAGE.COM  kadmin/changepw@CYBAGE.COM  kadmin/mac127.cybage.com@CYBAGE.COM  kiprop/mac127.cybage.com@CYBAGE.COM  krbtgt/CYBAGE.COM@CYBAGE.COM  root/admin@CYBAGE.COM |

Add principal for user shalaj

|  |
| --- |
| kadmin.local: **addprinc shalaj**  WARNING: no policy specified for shalaj@CYBAGE.COM; defaulting to no policy  Enter password for principal "shalaj@CYBAGE.COM":  Re-enter password for principal "shalaj@CYBAGE.COM":  Principal "shalaj@CYBAGE.COM" created.  kadmin.local: l**istprincs**  K/M@CYBAGE.COM  kadmin/admin@CYBAGE.COM  kadmin/changepw@CYBAGE.COM  kadmin/mac127.cybage.com@CYBAGE.COM  kiprop/mac127.cybage.com@CYBAGE.COM  krbtgt/CYBAGE.COM@CYBAGE.COM  root/admin@CYBAGE.COM  shalaj@CYBAGE.COM |

|  |
| --- |
| kadmin.local: **addprinc -randkey host/mac127.cybage.com**  WARNING: no policy specified for host/mac127.cybage.com@CYBAGE.COM; defaulting to no policy  Principal "host/mac127.cybage.com@CYBAGE.COM" created.  kadmin.local: **listprincs**  K/M@CYBAGE.COM  host/mac127.cybage.com@CYBAGE.COM  kadmin/admin@CYBAGE.COM  kadmin/changepw@CYBAGE.COM  kadmin/mac127.cybage.com@CYBAGE.COM  kiprop/mac127.cybage.com@CYBAGE.COM  krbtgt/CYBAGE.COM@CYBAGE.COM  root/admin@CYBAGE.COM  shalaj@CYBAGE.COM  kadmin.local: |

When we are creating it for a particular host it can use a random password

|  |
| --- |
| kadmin.local: **ktadd host/mac127.cybage.com**  Entry for principal host/mac127.cybage.com with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type des3-cbc-sha1 added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type arcfour-hmac added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type camellia256-cts-cmac added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type camellia128-cts-cmac added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type des-hmac-sha1 added to keytab FILE:/etc/krb5.keytab.  Entry for principal host/mac127.cybage.com with kvno 2, encryption type des-cbc-md5 added to keytab FILE:/etc/krb5.keytab.  kadmin.local: |

Principals entries have been added to FILE:/etc/krb5.keytab.

Now quit kadmin.local

|  |
| --- |
| kadmin.local: **quit**  [root@mac127 krb5kdc]# |

|  |
| --- |
| vi /etc/ssh/ssh\_config |

|  |  |
| --- | --- |
| **Default file** | **Updated file** |
| # PasswordAuthentication yes  # HostbasedAuthentication no  # GSSAPIAuthentication no  # GSSAPIDelegateCredentials no  # GSSAPIKeyExchange no  # GSSAPITrustDNS no | # PasswordAuthentication yes  # HostbasedAuthentication no  GSSAPIAuthentication yes  GSSAPIDelegateCredentials yes  # GSSAPIKeyExchange no  # GSSAPITrustDNS no |

|  |
| --- |
| [root@mac127 krb5kdc]# |

|  |
| --- |
| [root@mac127 krb5kdc]# **systemctl reload sshd.service**  [root@mac127 krb5kdc]# |

|  |
| --- |
| [root@mac127 krb5kdc]# **su - shalaj**  [shalaj@mac127 ~]$ **kinit**  Password for shalaj@CYBAGE.COM:  [shalaj@mac127 ~]$ **klist**  Ticket cache: KEYRING:persistent:1001:1001  Default principal: shalaj@CYBAGE.COM  Valid starting Expires Service principal  04/26/2017 14:40:49 04/27/2017 14:40:49 krbtgt/CYBAGE.COM@CYBAGE.COM |

Password for shalaj – shalaj@123

Kinit says try to get Ticket from ticket granting ticket from the authentication server or key distribution center

Now ticket is assigned which is valid for 24 hours

Now we can check by using ssh , it will not ask for password

|  |
| --- |
| [shalaj@mac127 ~]$ **ssh mac127.cybage.com**  The authenticity of host 'mac127.cybage.com (fe80::725a:fff:fe3d:dc07%enp4s0)' can't be established.  ECDSA key fingerprint is b1:0f:16:02:43:5b:94:20:62:04:b8:6e:34:a8:53:27.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added 'mac127.cybage.com,fe80::725a:fff:fe3d:dc07%enp4s0' (ECDSA) to the list of known hosts.  Last login: Wed Apr 26 14:40:14 2017 |

If we do the same from root user it will ask password for shalaj which is shalaj@123

|  |
| --- |
| [shalaj@mac127 ~]$ logout  Connection to mac127.cybage.com closed.  [root@mac127 krb5kdc]# **ssh shalaj@mac127.cybage.com**  shalaj@mac127.cybage.com's password:  Last login: Wed Apr 26 14:46:21 2017 from fe80::725a:fff:fe3d:dc07%enp4s0  [shalaj@mac127 ~]$ |

**Login with client machine**

|  |
| --- |
| [root@mac127 krb5kdc]# **scp /etc/krb5.conf root@172.27.155.92:/etc/**  The authenticity of host '172.27.155.92 (172.27.155.92)' can't be established.  ECDSA key fingerprint is bf:90:22:74:9a:72:fa:7d:7c:bf:86:20:00:1c:19:03.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added '172.27.155.92' (ECDSA) to the list of known hosts.  root@172.27.155.92's password:  krb5.conf |

On client machine (mac92)

|  |
| --- |
| [root@a ~]# yum install krb5-workstation pam-krb5 |

|  |
| --- |
| [root@a ~]# useradd shalaj |

Add mac127 in /etc/hosts file

|  |
| --- |
| 172.27.155.127 mac127.cybage.com mac127 |

|  |
| --- |
| [root@a ~]# **su - shalaj**  Last login: Wed Apr 26 05:54:18 EDT 2017 on pts/1  [shalaj@a ~]$ **kinit**  Password for shalaj@CYBAGE.COM:  [shalaj@a ~]$ |

|  |
| --- |
| [shalaj@a ~]$ **klist**  Ticket cache: KEYRING:persistent:1007:1007  Default principal: shalaj@CYBAGE.COM  Valid starting Expires Service principal  04/26/2017 05:55:37 04/27/2017 05:55:37 krbtgt/CYBAGE.COM@CYBAGE.COM |

|  |
| --- |
| [shalaj@a ~]$ **ssh mac127.cybage.com**  The authenticity of host 'mac127.cybage.com (172.27.155.127)' can't be established.  ECDSA key fingerprint is b1:0f:16:02:43:5b:94:20:62:04:b8:6e:34:a8:53:27.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added 'mac127.cybage.com,172.27.155.127' (ECDSA) to the list of known hosts.  Last login: Wed Apr 26 14:46:34 2017 from fe80::725a:fff:fe3d:dc07%enp4s0 |

# Add Cloudera-scm to KDC

|  |
| --- |
| [root@mac127 krb5kdc]# **kadmin.local**  Authenticating as principal root/admin@CYBAGE.COM with password.  kadmin.local: **addprinc cloudera-scm**  WARNING: no policy specified for cloudera-scm@CYBAGE.COM; defaulting to no policy  Enter password for principal "cloudera-scm@CYBAGE.COM":  Re-enter password for principal "cloudera-scm@CYBAGE.COM":  add\_principal: Password mismatch while reading password for "cloudera-scm@CYBAGE.COM".  kadmin.local: |

Password – Cloudera-scm@123