Configuring Kerberos master-slave KDC with LDAP master-replica topology on AIX

Step-by-step guide

Vipin Rathor

April 21, 2009

Learn how to configure and manage the Kerberos master-slave KDC with an LDAP master-replica setup. This article gives a step-by-step example of how to achieve one such complex Kerberos setup.

Introduction

In a Kerberos production environment, it is a best practice to use an LDAP (Lightweight Directory Access Protocol) directory to store the Kerberos principal and policy information. This allows the Kerberos administrator to centrally manage and monitor the Kerberos data.

In the Kerberos setup, along with the master KDC (Key Distribution Center), it is always advisable to have more than one slave KDC, which will support the master KDC to render round-the-clock availability and constant support for the authentication service and other kerberized services (for example, AIX® NFS v4, SSH, telnet, and more).

When using the LDAP directory, it is very common to have one master LDAP server and a few other LDAP replica servers, so as to achieve the load-balancing and high availability of the directory data.

A typical Kerberos production environment usually has both of the above configurations together, which means it may have a Kerberos master-slave KDC setup along with the LDAP master-replica setup. And it takes an expert Kerberos administrator to set up this type of configuration. This article deals with configuring one such environment.

Example setup

This article will use IBM® Network Authentication Service (IBM NAS) for the Kerberos and IBM Tivoli® Directory Server 6.1 (ITDS) for the LDAP directory server on the AIX platform.

The configuration of LDAP master and replica servers is out of the scope of this article. Please refer to your LDAP documentation for that specific information. This article references the following LDAP setup:
The following information pertains to the Kerberos setup.

Kerberos Administrator Name:
admin/admin

Kerberos Realm Name:
TEST

IBM NAS 1.4.0.7 Master KDC:
Hostname: master.in.ibm.com Port: 88

IBM NAS 1.4.0.7 Administration Server:
Hostname: master.in.ibm.com Port: 749

IBM NAS 1.4.0.7 Slave KDC:
Hostname: slave.in.ibm.com Port: 88

IBM NAS 1.4.0.7 client configured to the Master KDC:
Hostname: client.in.ibm.com

IBM Tivoli Directory Server v6.1 (LDAP master servers):
Hostname: lmaster1.in.ibm.com Port: 389
Hostname: lmaster2.in.ibm.com Port: 389

IBM Tivoli Directory Server v6.1 (LDAP replica servers):
Hostname: replica1.in.ibm.com Port: 389
Hostname: replica2.in.ibm.com Port: 389
Hostname: replica3.in.ibm.com Port: 389

All of these machines use IBM NAS version 1.4.0.7. You can get it either from the AIX Expansion Pack CDs or from the IBM AIX Web Download Pack Programs. (see Related topics).

Figure 2 shows the Kerberos setup that will be achieved at the end of this article.
Figure 2. Example setup for Kerberos master-slave KDC configuration

**Configuration steps**

This section covers the necessary steps that an administrator needs to carry out to set up the above Kerberos configuration.

Since the master KDC and administration servers need the read-write copy of the principal database to make the required changes, you are going to configure the master KDC with the LDAP masters. If one LDAP master server is down, there needs to be a backup LDAP master server (with the latest updated copy of the principal database), which will take charge immediately. For this reason, you will use two LDAP master servers with peer-to-peer replication configuration, so that the changes made to one master server will be immediately reflected to the other.

On the other hand, the slave KDCs can work with the read-write and read-only copies of the Kerberos principal database. Since the slave KDC is meant for backing up the master KDC in an emergency, the slave KDC might need to use the read-write copy. That is the reason that you will configure the slave KDC primarily with the master LDAP servers and with the LDAP replica as a fallback mechanism. So even if both the LDAP master servers are down, the slave KDC should continue its service by using the LDAP replicas.

**Preparing the LDAP servers for Kerberos**

In order to make use of any LDAP server to store Kerberos data, there are few preparations that need to be done on the LDAP server.

1. **Adding the proper suffix.** In the LDAP directory, a suffix is a top-level entry in LDAP directory hierarchy, under which all the logically related information is stored. So, even for the Kerberos information, you will use a suffix. For example, "ou=india, o=ibm, c=in" is the suffix that is used in this article. The LDAP server can have multiple suffixes, with each suffix denoting a specific directory hierarchy.
2. **Loading Kerberos schema.** In order to store the Kerberos data in any LDAP server (master or replica), the adequate Kerberos schema definitions should be loaded first in the LDAP directory. Only after doing this will the Kerberos data be understood and properly stored by the LDAP server. IBM NAS 1.4 ships the Kerberos schema definitions as LDIF (LDAP Data Interchange Format) file. These files are:

```
/usr/krb5/ldif/IBM.KRB.schema.ldif for IBM Directory Server 5.1 and 5.2
/usr/krb5/ldif/NS5.KRB.schema.ldif for SunONE Directory Server 5.1 and 5.2
```

You can use the ldappadd or ldapmodify commands to load the schema definition in the LDAP server. Please consult your LDAP documentation for more options and a detailed description of these commands.

3. **Loading realm entry.** The IBM NAS principal database is represented by a realm entry. This realm entry acts as the base for storing the Kerberos principal and policy information. This realm entry is comprised of the realm name and the suffix. In the example setup, you will add the realm entry `krbrealmName-V2=TEST,ou=india,o=ibm,c=in`. IBM NAS ships a template realm entry LDIF file, which can be edited to reflect the actual realm information. This file is installed by the name `/usr/krb5/ldif/realm_add.ldif`.

Since this article emphasizes the Kerberos configuration, it assumes that the LDAP setup is already present as shown in the example setup. For now, the article will concentrate on the Kerberos configuration steps.

The whole Kerberos configuration process can be logically divided into the following major steps:

- Configuration of master KDC with the LDAP master servers
- Configuration of slave KDC with the LDAP master and replica servers

**Configuration of master KDC with the LDAP master servers**

As stated earlier, you will configure the master KDC with two LDAP master servers and with no LDAP replica servers.

1. To configure the master KDC, you can use either the IBM NAS command `/usr/krb5/sbin/config.krb5` or the AIX command wrapper `mkkrb5srv`. Use the `mkkrb5srv` command to configure the master KDC with the master LDAP server. On the master KDC machine, run the `mkkrb5ksrv`, as shown below:

```bash
bash-2.05b# mkkrb5srv -r TEST -d in.ibm.com -a admin/admin -l lmaster1.in.ibm.com -u cn=admin -p adminpwd
```

```
Fileset                      Level  State      Description
----------------------------------------------------------------------------
Path: /usr/lib/objrepos
krb5.server.rte            1.4.0.7  COMMITTED  Network Authentication Service Server
Path: /etc/objrepos
krb5.server.rte            1.4.0.7  COMMITTED  Network Authentication Service Server
```

The `-s` option is not supported.
The administration server will be the local host.
Initializing configuration... Creating `/etc/krb5/krb5_crg_type`... Creating `/etc/krb5/krb5.conf`... Creating `/var/krb5/krb5Kdc/kdc.conf`... Creating database files...

```
Initializing database 'LDAP' for realm 'TEST'
master key name 'K/M@TEST'
Attempting to bind to one or more LDAP servers. This may take a while...
You are prompted for the database Master Password.
It is important that you DO NOT FORGET this password.
Enter database Master Password:
Re-enter database Master Password to verify:
Attempting to bind to one or more LDAP servers. This may take a while...
WARNING: no policy specified for admin/admin@TEST;
   defaulting to no policy. Note that policy may be overridden by
   ACL restrictions.
Enter password for principal "admin/admin@TEST":
Re-enter password for principal "admin/admin@TEST":
Principal "admin/admin@TEST" created.
Creating keytable...
Attempting to bind to one or more LDAP servers. This may take a while...
Creating /var/krb5/krb5kdc/kadm5.acl...
Starting krb5kdc...
Attempting to bind to one or more LDAP servers. This may take a while...
krb5kdc was started successfully.
Starting kadmind...
Attempting to bind to one or more LDAP servers. This may take a while...
kadmind was started successfully.
The command completed successfully.
Restarting kadmind and krb5kdc

Now the master KDC is up and running, but only this master KDC to one LDAP master server. 
In order to configure with another LDAP master server, you need to manually edit the KDC 
2. To add another LDAP master server, edit the /var/krb5/krb5kdc/.kdc_ldap_data file as 
shown below (the highlighted text is being added now).

```bash
bash-2.05b# cat /var/krb5/krb5kdc/.kdc_ldap_data
[ldapdefaults]
    realm = TEST
    bind_dn = cn=admin
    bind_dn_pw = adminpwd
    ldapserver = lmaster1.in.ibm.com
    ldapserver = lmaster2.in.ibm.com
    bind_type = simple
    #LDAP_OPT_REFERRALS = 1
    #LDAP_OPT_DEBUG = 0
    #LDAP_OPT_DEREF = 0
    #LDAP_OPT_TIMELIMIT = 300
    #LDAP_OPT_SIZELIMIT = 0
    #LDAP_OPT_SSL_TIMEOUT = 43200
    #LDAP_OPT_REFOPLIMIT = 10

[servers]
lmaster1.in.ibm.com = {
    port = 389
    replica_type = readwrite
    preference = 9
}

lmaster2.in.ibm.com = {
    port = 389
    replica_type = readwrite
    preference = 4
}
```
The preference relation in the above box shows the priority number while connecting to any LDAP server. The higher the value, the higher the priority. If the preference value is same for two servers, then the load balancing is used to determine which server to read and search from.

3. Once you have finished editing the file, you must restart both the Kerberos daemons:

```
bash-2.05b# /usr/krb5/sbin/stop.krb5; /usr/krb5/sbin/start.krb5
Stopping /usr/krb5/sbin/krb5kdc...
/usr/krb5/sbin/krb5kdc was stopped successfully.
Stopping /usr/krb5/sbin/kadmind...
/usr/krb5/sbin/kadmind was stopped successfully.
The command completed successfully.
Starting krb5kdc...
krb5kdc was started successfully.
Starting kadmind...
kadmind was started successfully.
The command completed successfully.
bash-2.05b#
```

4. The master KDC is now configured with the two LDAP master servers. To test this configuration, stop one master LDAP server and try performing some Kerberos requests (like kinit, klist, or kadmin). The master KDC should never panic in this case and transmission from one LDAP server to another should be seamless from the end-users' point of view.

**Configuration of slave KDC with the LDAP master and replica servers**

Now configure the slave KDC with the two LDAP master servers and three LDAP replica servers.

1. Use the `/usr/krb5/sbin/config.krb5` command to configure the slave KDC.

```
bash-2.05b# /usr/krb5/sbin/config.krb5 -E -d in.ibm.com -r TEST -s master.in.ibm.com -l lmaster1.in.ibm.com -u admin -p admin_pswd -R replica1.in.ibm.com replica2.in.ibm.com replica3.in.ibm.com
Initializing configuration...
Creating /etc/krb5/krb5_cfg_type...
Creating /etc/krb5/krb5.conf...
Creating /var/krb5/krb5kdc/kdc.conf...
Password for admin/admin@TEST:
Starting krb5kdc...
Attempting to bind to one or more LDAP servers. This may take a while...
krb5kdc was started successfully.
The command completed successfully.
bash-2.05b#
```

A few things to note in the command are:

- Only a krb5kdc daemon will be running at the slave machine, because a slave KDC never runs an administration server (kadmind).
- There is no database propagation. Since you are storing the Kerberos data in the LDAP directory, there is no need to propagate data from the master KDC to the slave KDC.

2. Please note that right now the slave KDC is configured to one LDAP master server and three replicas with the default preference values. You need to add another LDAP master server manually. For this, edit the `/var/krb5/krb5kdc/.kdc_ldap_data` file and insert the highlighted entries below.

```
bash-2.05b# cat /var/krb5/krb5kdc/.kdc_ldap_data
```
3. Restart the Kerberos daemon by using `stop.krb5` and `start.krb5`:

```
bash-2.05b# /usr/krb5/sbin/stop.krb5 krb5kdc; /usr/krb5/sbin/start.krb5 krb5kdc
Stopping /usr/krb5/sbin/krb5kdc... 
/kusr/krb5/sbin/krb5kdc was stopped successfully. 
The command completed successfully. 
Starting krb5kdc... 
krb5kdc was started successfully. 
The command completed successfully. 
bash-2.05b#```

4. The slave KDC is all set to assist the master KDC to handle the client requests. Check the configuration by configuring a client to this slave KDC and running the IBM NAS commands like `kinit`, `klist`, and `kadmin`.

Configure and use IBM NAS client to test the setup

Now you are going to set up a Kerberos client to the above master-slave KDC setup that you have successfully configured. To configure a client, you can use either `config.krb5` (an IBM

```
[ldapdefaults]
realm = TEST
bind_dn = cn=admin
bind_dn_pw = adminpwd
ldapserver = replica1.in.ibm.com
ldapserver = replica2.in.ibm.com
ldapserver = replica2.in.ibm.com
ldapserver = lmaster1.in.ibm.com
ldapserver = lmaster2.in.ibm.com
bind_type = simple
#LDAP_OPT_REFERRALS = 1
#LDAP_OPT_DEBUG = 0
#LDAP_OPT_DEREF = 0
#LDAP_OPT_TIMELIMIT = 300
#LDAP_OPT_SIZELIMIT = 0
#LDAP_OPT_SSL_TIMEOUT = 43200
#LDAP_OPT_REFHOPLIMIT = 10

[servers]
replica1.in.ibm.com = {
    port = 389
    replica_type = readonly
    preference = 5
}
replica2.in.ibm.com = {
    port = 389
    replica_type = readonly
    preference = 5
}
replica3.in.ibm.com = {
    port = 389
    replica_type = readonly
    preference = 5
}
lmaster1.in.ibm.com = {
    port = 389
    replica_type = readwrite
    preference = 4
}
lmaster2.in.ibm.com = {
    port = 389
    replica_type = readwrite
    preference = 4
}
```
NAS command) or mkkrb5clnt (an AIX wrapper). By using mkkrb5clnt, you can also configure an integrated Kerberized login for the AIX machine along with the IBM NAS client in a single command. But, executing mkkrb5clnt requires more understanding of a few things. For now, use config.krb5 to configure a simple IBM NAS client to the above configuration of master-slave KDCs.

1. Run `/usr/krb5/sbin/config.krb5` as shown below to configure the client:

```
bash-2.05b# /usr/krb5/sbin/config.krb5 -c -d in.ibm.com -r TEST -c master.in.ibm.com
   -s master.in.ibm.com
Initializing configuration...
Creating /etc/krb5/krb5_cfg_type...
Creating /etc/krb5/krb5.conf...
The command completed successfully.
bash-2.05b#
```

2. You only have one KDC (master.in.ibm.com) listed in the `/etc/krb5/krb5.conf` file. Edit this file and make another KDC entry for the slave KDC (slave.in.ibm.com) as shown below:

```
-bash-2.05b# cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = TEST
    default_keytab_name = FILE:/etc/krb5/krb5.keytab
    default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-md5
des-cbc-crc
    default_tgs_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-md5
des-cbc-crc

[realms]
    TEST = {
        kdc = master.in.ibm.com:88
        kdc = slave.in.ibm.com:88
        admin_server = master.in.ibm.com:749
        default_domain = in.ibm.com
    }

[domain_realm]
    .in.ibm.com = TEST
    master.in.ibm.com = TEST

[logging]
    kdc = FILE:/var/krb5/log/krb5kdc.log
    admin_server = FILE:/var/krb5/log/kadmin.log
    default = FILE:/var/krb5/log/krb5lib.log

-bash-2.05b#
```

3. Now you are all set to test the configuration. Use the `/usr/krb5/bin/kinit` and `/usr/krb5/bin/klist` commands to test whether the client can contact KDC or not.

```
bash-2.05b# /usr/krb5/bin/kinit admin/admin
Password for admin/admin@TEST:

bash-2.05b# /usr/krb5/bin/klist
Ticket cache:  FILE:/var/krb5/security/creds/krb5cc_0
Default principal:  admin/admin@TEST
Valid starting     Expires            Service principal
05/09/08 07:08:53  05/10/08 07:08:51  krbtgt/TEST@TEST

bash-2.05b#
```

4. You can also test the connection to kadmind by running the `/usr/krb5/sbin/kadmin` command.
bash-2.05b# /usr/krb5/sbin/kadmin -p admin/admin
Authenticating as principal admin/admin with password.
Password for admin/admin@TEST:
kadmin: getprincs
K/M@TEST
admin/admin@TEST
kadmin/admin@TEST
kadmin/changepw@TEST
kadmin/history@TEST
krbtgt/TEST@TEST
kadmin: q
bash-2.05b#

To test the fail-safe mechanism, you can try shutting down either the slave / master KDC or LDAP servers. The above configured client can follow these fail-over paths in case of failure of any server:

**Figure 3. Possible fail-over paths for IBM NAS client**

Finally, you are able to successfully configure IBM NAS master-slave KDC with LDAP master-replica topology.

**Conclusion**

This article shows you the configuration of the Kerberos master-slave KDC duo with the LDAP master-replica setup. Though not an easy task, this article provides a step-by-step guide along with the adequate examples to make ensure that everything runs smoothly.
Related topics

- **A Kerberos Primer** (developerWorks, Nov 2001): This article introduces Kerberos technology and Distributed Computing Environment-based applications.
- **IBM Network Authentication Service for AIX**: Download the IBM Network Authentication Service for AIX from IBM AIX Web Download Pack Programs.
- **IBM Network Authentication Service for Linux, Solaris**: Download the IBM Network Authentication Service for Linux, Solaris from here.
- **IBM GUI-based Administration Tool for Network Authentication Service**: Experience the GUI to perform the IBM NAS related administration tasks. Download from the IBM alphaWorks today.

© Copyright IBM Corporation 2009
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)