Configuring Kerberos for Sybase

Author: Joshua Meckler

technology

WHITE PAPER

Introduction

When using Kerberos security with Sybase products such as Adaptive Server Enterprise, Open Client/Open Server, or jConnect, you must perform a series of setup tasks before a successful client-server connection can be made. These setup tasks may differ among Kerberos providers such as CyberSafe, MIT Kerberos and MicroSoft Active Directory.

A complete discussion of the individual Kerberos providers is beyond the scope of the Sybase documentation, and Sybase urges you to refer to the documentation provided by the Kerberos vendors. However, this document will provide a high-level road map for creating a Kerberos setup between client and server. Additionally, this document will include setup information specific to CyberSafe, MIT Kerberos and MicroSoft Active Directory.

Setting Up Kerberos to Work with Sybase

To install and configure Kerberos security software to work with your Sybase product, you need to perform the following general steps:

- Purchase or download software for Kerberos libraries and for a Kerberos Key Distribution Center (KDC).
- Get the KDC and Kerberos admin daemon up and running
- Set up your Kerberos configuration files (such as krb5.conf).
- Create Kerberos users (user principals) and server principals (service principals) in your KDC.
- Use the KDC to extract a keytab for your server.
- Configure your ASE or Open Server to accept Kerberos connections.
- On your client machine, authenticate yourself to the KDC.
- Connect to your server.

Purchase or Download Software for Kerberos Libraries and Kerberos Key Distribution Center (KDC)

Sybase clients and servers do not come equipped "out of the box" with Kerberos software. You need to purchase or download the software. This software consists of:

- Kerberos libraries. These are referred to as the GSS (Generic Security Services) library, or libgss. These libraries implement the well-defined GSS API. The vendor CyberSafe Limited supplies a version of the GSS libraries. The MIT open-source Kerberos libraries can be freely downloaded, but these are unsupported, except through public newsgroups. Also, it may be necessary to compile the MIT source code for your platform. The libraries are needed on each client and server machine that intends to use Kerberos.
- A Kerberos Key Distribution Center (KDC) server. The KDC functions as a storehouse for users and servers. It also verifies the identification of users and servers. The KDC is typically installed on an isolated machine not intended for applications or user logins.
- The KDC typically runs in conjunction with two other server daemons, the admin daemon and the kpasswd daemon. The admin daemon is used for administering the KDC database. You use this server to perform functions such as adding users and service principals, changing passwords and extracting keytab files. The kpasswd daemon allows users to change their own passwords.

> **Note:** When you use MicroSoft Active Directory as your Kerberos provider, you do not have to install a separate KDC or admin daemon. Active Directory serves as both a KDC and admin daemon. More information on Active Directory is found later in this section.

Get the KDC and Kerberos *admin daemon* Up and Running

This step varies according to vendor. Sybase strongly recommends that you read the vendor-supplied documentation and follow vendor-supplied advice for installation requirements.

Set up Your Kerberos Configuration Files

Some Kerberos clients, among them MIT, require that you use a Kerberos configuration file. The file is typically named krb5.conf. The configuration file allows you to set values for, among other things, the default realm, the hostname of the machine on which your KDC is running, and the default encryption key requested during Kerberos authentication. The default location of this file is vendor dependent.

> **Note:** End-users on MIT-based Kerberos software can set up their own configuration files, and set environment variables to point to them. See the vendor documentation for more information.

Unlike the MIT version of Kerberos, the CyberSafe version does not use a krb5.conf configuration file. Instead, by default, CyberSafe uses DNS records to find KDC address mapping and realm information in the same way that MicroSoft Active Directory uses DNS for Kerberos name mapping. CyberSafe products can also find KDC and realm mapping information in two files – krb.conf and krb.realms. Consult your CyberSafe documentation for more information.

The structure for a krb5.conf file is defined in the MIT Kerberos documentation online at http://web.mit.edu/kerberos/www/.

> **Note:** You need a krb5.conf file if you are going to use MIT Kerberos clients to authenticate against any vendor's KDC. You also need a krb5.conf file if you are going to use Java clients.

The following is a sample krb5.conf:

```
#
# This is a sample krb5.conf file. It might be used, for example, by a
# client that is using the MIT Kerberos libraries, or a client that is
# using Sun's Java Kerberos implementation.
#
# Please note that customer must alter the default_realm, [realms] and
# [domain_realm] information to reflect their Kerberos environment. Also
# note that the default encoding types here are set to des-cbc-crc
# (i.e. single DES). Other encoding types (such as triple DES) may be
# possible depending on the Kerberos implementations you are using at
# the client and server.
#
# Please do not attempt to use this file as is.
#

 [libdefaults]
        # set your own default realm here
        default_realm = MYREALM
        default_tgs_enctypes = des-cbc-crc
        default_tkt_enctypes = des-cbc-crc
        kdc_req_checksum_type = 2
        ccache_type = 2

[realms]

        MYREALM = {
           # You'll need to enter your KDC's host name
           kdc = kdchost
           admin_server = kdchost
       }

[domain_realm]

        # Alter these values based on your company's DNS mappings and
        # your default realm.
        .sybase.com = MYREALM
        sybase.com = MYREALM

[logging]

        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log
      kdc_rotate = {

# How often to rotate kdc.log. Logs will get rotated no more
# often than the period, and less often if the KDC is not used
# frequently.
            period = 1d
# how many versions of kdc.log to keep around (kdc.log.0,
# kdc.log.1, ...)
            versions = 10
      }
```

```
   [appdefaults]
      kinit = {
         renewable = true
         forwardable= true
   }

#
# eof
#
```

Create Kerberos Users (User Principals) and Server Principals (Service Principals) in Your KDC

The process for adding Kerberos users and service principals differs depending on which KDC (CyberSafe, MIT, Active Directory or other) you use. You may also need to set your execution path, library search path and other vendor-specific environment variables before creating user and service principals. The examples that follow often refer to using the single-DES encryption type for your keys. This is because single-DES allows the greatest degree of interoperability between various Kerberos implementations at the client, server and KDC. It is possible to use other types such as 3DES (triple-DES) and RC4-HMAC (the default for Active Directory), but successful use of other encryption types is dependent on the particular Kerberos implementations you are using. Please see your Kerberos provider documentation for more information.

CyberSafe

The following example demonstrates how to use the CyberSafe kadmin utility to connect to the admin daemon to add users and service principals. In this example, the Kerberos administrator is called “krb5” or “krb5@MYREALM”, and the realm is called MYREALM.
This example shows kadmin being run from a Unix command line. The command-line version of kadmin for Windows uses the same commands. GUI versions of kadmin also exist.

```
      mymachine% /krb5/bin/kadmin krb5
      Principal - krb5@MYREALM
      Enter password:
      Connected to csfA5v01 in realm MYREALM.
```

Now, add a user, “sybuser1”. This user name must be identical to a login on your server. (The login may be created on the server later.) For maximum compatibility with Java Kerberos applications, you should use a DES encoding for your key. See the CyberSafe documentation for more details. If you do not set a specific encoding when you add a user, the encoding default will be determined by your KDC settings.

```
      Command: add sybuser1
      Enter password:
      Re-enter password for verification:
      Principal added.
```

Next, add an entry for your server. The name entered here must be identical to the name of the Sybase server the client will connect to**.** In this example, the server is named ase1252srv. The command sequence is identical to that used in adding a user.

```
      Command: add ase1252srv
      Enter password:
      Re-enter password for verification:
      Principal added.
```

Note: As an alternative to kadmin, you can use csfadm, a GUI tool provided with your CyberSafe software, to perform these tasks. See the vendor documentation.

MIT

The following example demonstrates how to use the MIT kadmin utility to connect to the MIT admin daemon to add users and service principals. In this example, the Kerberos administrator is called “krb”' or “krb5@MITKDC”, and the realm is called MITKDC.
This example shows kadmin being run from the Unix command line:

```
      mymachine% /work3/mitkrb5/sbin/kadmin -p krb5
      Authenticating as principal krb5 with password.
      Enter password:
        kadmin:
```

Now add a user, “sybuser1”. This user name must be identical to a login on your server. (The login may be created on the server later.) In this example, the user specifies an encoding of “des-cbc-crc:normal” for the principal's key.

```
        kadmin: addprinc -e des-cbc-crc:normal sybuser1
        WARNING: no policy specified for sybuser1@MITKDC; defaulting to no
        policy
        Enter password for principal "sybuser1@MITKDC":
        Re-enter password for principal "sybuser1@MITKDC":
        Principal "sybuser1@MITKDC" created:
```

Next, add a service principal entry for your data server. The name needs to be identical to the name of the server the client will connect to. In example, the server name is ase1252srv. The command sequence is the same as that for adding a user.

```
        kadmin: addprinc -e des-cbc-crc:normal ase1252srv
        WARNING: no policy specified for ase1252srv@MITKDC; defaulting to no
        policy
        Enter password for principal "ase1252srv@MITKDC":
        Re-enter password for principal "ase1252srv@MITKDC":
        Principal "ase1252srv@MITKDC" created:
```

ACTIVE DIRECTORY

To add users and service principals in Active Directory, use the GUI tools on the Active Directory Server machine.

Click on “Manage user accounts and group settings” to bring up the “Active Directory Users and Computers” menu screen. Then, right-click on the “Users” folder and create a new user named “sybuser1”.

Next, create another user, “ase1252srv”, for the service principal.

When creating users and service principals in Active Directory, you may wish to specify that single-DES keys be used. Do this by right clicking on the user or service principal name, then clicking on “Properties”. This brings up a screen with the properties for the user. Click on the “Account” tab, then in the list of Account options, find the item that says “Use DES encryption types for this account”. Selecting that option will force Active Directory to use single-DES keys for that user.

MicroSoft has released several tools that can be used to manage Active Directory accounts from Unix platforms. More information can be found at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnactdir/html/kerberossamp.asp

Use the KDC to Extract a Keytab for Your Server

Servers, like users, must authenticate themselves to the KDC. This is why you must create a server service principal within the KDC. Unlike users, however, servers do not go through the process of signing on to a network. Instead, a server authenticates itself through the use of a keytab file. This keytab is a protected, encrypted file that the server uses to identify itself to the KDC. When a server is started with Kerberos enabled, an environment variable must be set so that the GSS libraries can locate the keytab file. Even before this happens, however, you must get the keytab file from the KDC and place this file on the server machine. This process is called “extracting a keytab”.

If your server is to run on a Unix machine, make sure that the keytab file is readable by the Unix user that will start the server. In a production environment, you need to control access to this file. If a user can read the keytab file, they can create a server that impersonates your server.

CyberSafe Keytab Extraction

When using a CyberSafe KDC, you can use the kadmin utility to log into the admin daemon. Run kadmin as explained in the earlier section, Create Kerberos Users (User Principals) and Server Principals (Service Principals) in Your KDC. Then use the ext command to extract the keytab in to a file. (You extract a keytab for the service principal.)

```
        Command: ext -n ase1252srv
        Service Key Table File Name (/krb5/v5srvtab):
        Key extracted.
        Command: quit
        Disconnected.
```

This extracts the key to the file /krb5/v5srvtab. Place this file in the location configured on your Sybase server for the keytab file. The location of the keytab file on the Sybase server is described in the following section of this document, Configure Your ASE or Open Server to Accept Kerberos Connections.

> **Note**: As an alternative to kadmin, you can use csfadm, a GUI tool provided with your CyberSafe software, to extract a keytab. See the vendor documentation.

MIT Keytab Extraction

When using an MIT KDC, run kadmin as explained in the earlier section, Create Kerberos Users (User Principals) and Server Principals (Service Principals) in Your KDC. Then, use the ktadd command to extract the keytab into a file. (You extract a keytab for the service principal.)

```
kadmin: ktadd -k /tmp/v5srvtab ase1252srv
Entry for principal ase1252srv with kvno 2, encryption type Triple
DES mode with HMAC/sha1 added to keytab WRFILE:/tmp/v5srvtab
Entry for principal ase1252srv with kvno 2, encryption type DES cbc
mode with CRC-32 added to keytab WRFILE:/tmp/v5srvtab
kadmin:
```

> **Note:** In this case, the MIT KDC extracted two keytabs. One is in Triple DES encoding, while the other is in DES encoding. Both keys are placed in the file /tmp/v5srvtab. Depending on your Kerberos client, you may wish to extract only one key type; you do this using the -e option of the ktadd command. Please read the MIT documentation for further details.

You should take your keytab file and place it in the location at which the server has been set up to read the file. The location of the keytab file on the Sybase server is described in the following section of this document, Configure Your ASE or Open Server to Accept Kerberos Connections.

Active Directory Keytab Extraction

MicroSoft provides an executable called ktpass.exe. You use this program to extract a keytab from an Active Directory Server, as well as to make a mapping between a Kerberos service principal name and the service principal account in Active Directory.

For example, if your Active Directory Realm was named “ADREALM”, you might issue a command like the following:

```
ktpass –princ ase1252srv@ADREALM –mapuser ase1252srv -pass
my_password –out ase1252srv.keytab
```

This outputs the keytab to a file called ase1252srv.keytab. You then move that keytab file to the machine on which your Sybase server is running.

For more information on the ktpass.exe utility, including command syntax, see the MicroSoft documentation at http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B324144&Product=win2000

Configure Your Sybase ASE or Open Server to Accept Kerberos Connections

To complete this step, you need to consult the appropriate Sybase manual. Most importantly, you must configure the server to properly locate the keytab file generated in Use the KDC to Extract a Keytab for Your Server. The keytab file can either be kept in the (vendor-specific) default location or it can be indicated by environment variables. For CyberSafe GSS, set the CSFC5KTNAME variable to point to the keytab file. For MIT GSS, set the KRB5_KTNAME environment variable.

Additionally, you need to create a login and user in your server with the same name as the user principal you created in the KDC. To do this, use the **sp_addlogin** and **sp_adduser** stored procedures.

> **Note:** While the username you create in ASE must match the user principal name in the KDC, the password that you specify when creating the user need not match the password you used when you created the user in your KDC. This is because Kerberos logins depend only on the password for the user in the KDC. The password you create for the ASE or Open Server user will never be used, unless you wish log into the server without using Kerberos.

Be sure to start your server with the proper GSS libraries in its library search path. Finally, Sybase servers have a configuration file called libtcl.cfg. This file contains various configuration options, including one, which specifies which GSS library to use. The name of this option is “csfkrb5”. This is the correct option name even if you use MIT GSS libraries for your server. The “csfkrb5” name is a legacy issue left over from the time when Sybase servers could only use CyberSafe GSS libraries.

On the Client Machine, Authenticate Yourself to the KDC.

Log into the KDC and verify your identity. In Kerberos terminology, you need to obtain a Kerberos Ticket Granting Ticket (TGT), which verifies your identity and gives you privileges to do such things as logging into a server.

Some system administrators configure their work environments so that users get a TGT simply by logging into their machine.

If you are using a UNIX machine and you are not set up to automatically receive a TGT at login, you need to run your Kerberos client's kinit binary. The kinit binary authenticates the user to the KDC and places the TGT in a file in a well-defined location (known as a credential cache) on the client machine. This location is commonly a file located at /tmp/krb5cc_ {user_id}.

If you are using a Windows machine and you are not set up to automatically receive a TGT at login, you can use the CyberSafe Authentication Tool from the Start menu to create your TGT. Other vendors also provide kinit executables. For example, Sun provides a version of kinit with its JDK that can be used from a Windows client machine.

Using kinit on Unix

To authenticate your UNIX client, run kinit from the command line as follows:

```
mycomputer% kinit sybuser1@MYREALM
Password for sybuser1@MYREALM:
mycomputer%
```

Note: A common problem that can cause a failure to authenticate to a KDC is a discrepancy in the time settings of the client and KDC machines. Generally, the time settings on the client and KDC machines must be set within a certain number of seconds of each other for a successful authentication to take place. See your KDC documentation for details.

Connect to Your Server

Once you have your TGT, you can make a Kerberos connection to your server. See your Sybase client documentation for more information on connecting with Kerberos.

Sybase, Inc.
Worldwide Headquarters
One Sybase Drive
Dublin, CA 94568-7902 USA
Tel: +800 8 SYBASE
www.sybase.com