Technical Note

Using the DirectControl Kerberos Tools

Kerberos-enabled services, utilities and development components

Published: October 3, 2005

Introduction

Centrify DirectControl uses Kerberos technology to authenticate UNIX sessions with Active Directory credentials. One of the advantages of using Kerberos is that it enables applications and many common network tools to be used without having to re-enter user and password information. Since Kerberos is built into DirectControl, it is possible to use standard Kerberos tools to leverage secure, authenticated, ticket-based, single sign-on sessions.

Centrify has compiled an optional package that includes Kerberos-based development components as well as Kerberized utilities and services. These are based on the latest Kerberos distribution from MIT and the tools can be used with the standard DirectControl product. This Application Note describes how to install, configure and use the components included with the Centrify DirectControl Kerberos Tools package.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

Contents

1 What's Included 3

2 Installation 4

2.1 Preparation 4

2.2 Installing the DirectControl Kerberos Tools 4

2.2.1 Installing DirectControl Kerberos Tools on Linux 4

2.2.2 Installing DirectControl Kerberos Tools on UNIX 5

2.2.3 Installing DirectControl Kerberos Tools on Mac OS X 5

3 Basic Configuration 5

3.1 Setting up the DirectControl Kerberos Tools Server Applications 5

3.1.1 Adding Kerberos Service Principal Names 6

3.1.2 Kerberos Telnet Server 7

3.1.3 Kerberos FTP Server 8

3.1.4 Kerberos rlogin Server 8

3.1.5 Kerberos rsh Server 9

3.2 Using the DirectControl Kerberos Tools Client Applications 9

3.2.1 Setting up your command execution PATH 9

3.2.2 Setting up a .k5login file 10

3.2.3 Setting up a .netrc file 11

3.2.4 Using the Centrify Kerberos libraries in runtime applications 11

3.2.5 Running Centrify Kerberos user utilities 13

3.3 Using the DirectControl Kerberos Development Components 14

4 Summary 15

4.1 Related Information and Technical Notes 15

4.2 For more information 16

4.3 Legal Notices 16

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

1 What's Included

Centrify has made a number of enhancements to the MIT Kerberos environment that make deployment of Kerberos applications simpler. Some of these enhancements include:

- **Automated setup of Kerberos:** When you join a UNIX, Linux or Mac computer to an Active Directory domain using DirectControl, the set up of all Kerberos-related system configuration files is automatically done for you. For example, the file /etc/krb5.conf will be configured correctly for using the Active Directory domain controller as the Kerberos key distribution center. Having these configuration files automatically set up for you means that Kerberized UNIX applications will "just work" using Active Directory as the Kerberos authority.

- **Removing the need for .k5login:** Normally a Kerberized login-type application such as **ssh**, **telnet** or **rsh** requires a .k5login file on the target system. The creation of these files can become a significant administrative burden. Centrify removes the need for this file in almost all cases. See the related section below for a detailed explanation of when a .k5login file is needed.

- **Remove the need for host-to-realm mapping:** If you have disjoint DNS and Active Directory domain names, then you normally need host-to-realm name mappings in the Kerberos configuration file. The maintenance of these entries can be a significant administrative overhead. Centrify's Kerberos implementation removes the need for these entries.

- **Secure canonicalization:** In many cases Kerberos needs to convert a partial host name to a fully qualified name including its realm name. This process is called canonicalization. For example, the host name in the command:

  ```
  telnet –a system1
  ```

  will actually be interpreted as system1.centrify.com@CENTRIFY.COM if the system is part of the CENTRIFY.COM realm. MIT's Kerberos distribution uses a combination of DNS and host-to-realm mappings to achieve this translation. The use of DNS is inherently insecure, and RFC 1510 (the main Kerberos standard) specifically recommends against using it but does not offer an alternative. DirectControl implements a more secure mechanism that uses Active Directory's knowledge of the domain and does not rely on DNS.

Once the DirectControl Kerberos Tools have been installed, a number of new files are placed under the Centrify directory structure: /usr/share/centrifydc/kerberos. These new files can be summarized as follows:

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

Directory	Components
/usr/share/centrifydc/kerberos/bin	Kerberized client applications such as **ftp**, **rlogin**, **telnet** and **rcp**
/usr/share/centrifydc/kerberos/man	UNIX style MAN pages for the components
/usr/share/centrifydc/kerberos/sbin	Kerberized server and administration applications such as **ftpd**, **krlogind**, **telnetd** and **ktutil**
/usr/share/centrifydc/kerberos/include	Header files for use when compiling Kerberized applications
/usr/share/centrifydc/kerberos/lib	Libraries files for use when linking Kerberized applications
/usr/share/centrifydc/kerberos/share	Configuration and application examples

This remainder of this Technical Note describes how to install, configure and use the components included with the Centrify DirectControl Kerberos Tools package.

2 Installation

2.1 Preparation

It is assumed that DirectControl 2.0 or later has been installed and the UNIX, Linux or Mac system has been joined to an Active Directory domain. These instructions do not work with DirectControl 1.0. Make sure that the correct package file for the DirectControl Kerberos Tools has been downloaded to your UNIX or Linux system. This file uses the standard package system for the UNIX or Linux system that you are using. For example, on a Red Hat Linux system, the file is named centrifydc-krb5-2.*x.x*-rh9-i386.rpm. On a Sun Solaris system, the package is contained in a gzipped tar file that includes a PKG format archive.

2.2 Installing the DirectControl Kerberos Tools

The DirectControl Kerberos Tools are installed using the native package install tools for each UNIX, Linux or Mac system. It is assumed that the user is logged in as root on the UNIX, Linux or Mac system and the appropriate package file for that system is located in the current working directory. The following instructions can be used for each of the supported operating systems.

2.2.1 Installing DirectControl Kerberos Tools on Linux

For Red Hat Linux, use:

```
rpm –Uvh centrifydc-krb5-2.x.x-rh9-i386.rpm
```

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

For SuSE Linux, use:

```
rpm –Uvh centrifydc-krb5-2.x.x-suse8-i386.rpm
```

For VMware ESX, use:

```
rpm –Uvh centrifydc-krb5-2.x.x-esx2-i386.rpm
```

For Debian, use:

```
dpkg –i centrifydc-krb5-2.x.x-deb3-i386.deb
```

2.2.2 Installing DirectControl Kerberos Tools on UNIX

For Solaris, use:

```
gunzip centrifydc-krb5-2.x.x-sol9-local.tgz
tar –xf centrifydc-krb5-2.x.x-sol9-local.tar
pkgadd –d CentrifyDC-krb5
```

For HP-UX, use:

```
gunzip –d ./ centrifydc-krb5-2.x.x-hp11.11-pa.depot.gz
swinstall –s $full_path/ centrifydc-krb5-2.x.x-hp11.11-pa.depot \
–x allow_incompatible=true
```

For IBM AIX, use:

```
gunzip centrifydc-krb5-2.x.x-aix5.2-ppc-bff.gz
inutoc .
installp -aY -d . CentrifyDC-krb5.core
```

2.2.3 Installing DirectControl Kerberos Tools on Mac OS X

To install the package on a computer with Mac OS X, use:

```
sudo tar –C / -zxvf centrifydc-krb5-2.x.x-mac10.3.tgz
```

3 Basic Configuration

The following steps should be used as a guideline for getting Kerberos applications and services running correctly in your environment. This technical note includes the steps for setting up most of the DirectControl Kerberos Tools components on a Red Hat 9 Linux system. These steps can be used as guidelines for setting up other Kerberos applications and services on other platforms.

3.1 Setting up the DirectControl Kerberos Tools Server Applications

If you wish to enable Kerberized services such as **telnetd** or **ftpd**, then you will need to replace the existing services if they are running and set up the services to auto start each time your system boots. These instructions describe how to set up the Kerberos **telnetd, ftpd, klogind** and **kshd** servers. Other servers in the /usr/share/centrifydc/kerberos/sbin directory can be set up in a similar manner.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

The /usr/share/centrifydc/kerberos/sbin directory includes tools for Kerberos system administration as well as the Kerberos server applications. The following table provides a brief description for each of these applications. For detailed information on each utility, see the included MAN page for the program.

Utility	Description
ftpd	DARPA Internet File Transfer Protocol server
k5srvutil	Host key table (keytab) manipulation utility
kadmin	Kerberos V5 database administration program
kadmind	KADM5 administration server
kadmin	Kerberos V5 database administration program
kdb5_util	Kerberos database maintenance utility
klogind	Remote login server
kprop	Propagate a Kerberos V5 principal database to a slave server
kpropd	Kerberos V5 slave KDC update server
krb524d	Version 5 to Version 4 Credentials Conversion Daemon
krb5kdc	Kerberos V5 KDC
kshd	Kerberized remote shell server
ktutil	Kerberos keytab file maintenance utility
login.krb5	Kerberos enhanced login program
sserver	Sample Kerberos version 5 server
telnetd	DARPA TELNET protocol server

3.1.1 Adding Kerberos Service Principal Names

The steps in this section only need to be followed if you are running DirectControl version 2.0.5 or earlier. However, it is suggested that you check these settings to make sure they have not been modified on your system.

Centrify uses the file /etc/centrifydc/centrifydc.conf to control the operation of the DirectControl service on a UNIX or Linux system. One of the settings in this file controls the services that can be used with the DirectControl Kerberos environment. To modify the services, follow these steps:

1. Edit the file /etc/centrifydc/centrifydc.conf

2. Locate the lines

```
# Additional service principals for key table entry
adclient.krb5.service.principals: nfs cifs
```

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

3. Add “ftp” to the end of the line so that it reads
   `adclient.krb5.service.principals: nfs cifs ftp`

4. Note that in recent versions of DirectControl, the entry for “ftp” already exists and therefore no changes are required. You may need to add additional entries to this line if you wish to run other Kerberos services. Note that the telnet, klogin and ksh services do not need an entry as they use the built-in HOST service that is available by default.

5. If you have made changes and the machine is already joined to the domain then leave the domain by using **adleave**.

6. Now join the domain using **adjoin *domain***.

3.1.2 Kerberos Telnet Server

On most Linux systems, many network services are controlled by **xinetd**. The configuration files for each of the **xinetd** controlled services are located in the directory /etc/xinetd.d. There should be a file already created for the telnet service called telnet. Modify this file so that it now has the following lines:

```
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/share/centrifydc/kerberos/sbin/telnetd
        server_args     = -L /bin/login
        log_on_failure  += USERID
}
```

The **xinetd** program now needs to re-read its configuration files. An easy way to do this is to force the xinetd service to re-read its configuration files using:

```
pkill –HUP xinetd
```

To test that the telnet service is working correctly, login as an Active Directory authenticated user on the Linux system. Run the following command:

```
/usr/share/centrifydc/kerberos/bin/telnet –a hostname
```

Where hostname is the host name for machine you are logged into. Do not use “localhost” as the hostname or use the IP address of the machine. The “-a” flag tells telnet to attempt to login automatically. If Kerberized telnet is working correctly, then you should be able to login to the system directly without entering a username or password.

By adding the line “server_args = -L /bin/login” the telnet server will also correctly respond to non-Kerberos based logins. In environments where you want to enforce Kerberos-based credentials, this line should be removed.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

3.1.3 Kerberos FTP Server

Installing the Kerberos enabled FTP server is very similar to installing the Kerberos telnet server. The /etc/xinetd.d directory should have a configuration file called ftp. Modify this file so that is now has the following lines:

```
service ftp
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/share/centrifydc/kerberos/sbin/ftpd
        log_on_failure  += USERID
}
```

Restart the xinetd service using the instructions in the telnet server section.

To test that the FTP service is working correctly, login as an Active Directory authenticated user on the Linux system. Run the following command:

```
/usr/share/centrifydc/kerberos/bin/ftp hostname
```

Where hostname is the host name for machine you are logged into. Do not use “localhost” or the IP address as the hostname. The **ftp** program will attempt to log you in automatically and you should not be prompted for a user name or password.

3.1.4 Kerberos rlogin Server

To run the Kerberos enabled rlogin service (the Kerberized version is called **klogind**), you will need a klogin file in the /etc/xinetd.d directory. Modify this file so that is now has the following lines:

```
service klogin
    {
            flags           = REUSE
            socket_type     = stream
            wait            = no
            user            = root
            server          = /usr/share/centrifydc/kerberos/sbin/klogind
            server_args     = -5
            disable         = no
    }
```

Restart the xinetd service using the instructions in the telnet server section.

To test that the rlogin service is working correctly, login as an Active Directory authenticated user on the Linux system. Run the following command:

```
/usr/share/centrifydc/kerberos/bin/rlogin hostname
```

Where hostname is the host name for machine you are logged into. The **rlogin** program will attempt to log you in automatically and you should not be prompted for a user name or password.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

3.1.5 Kerberos rsh Server

To run the Kerberos enabled rsh, rshell or rcp service, you will need a kshell file in the /etc/xinetd.d directory. Modify this file so that is now has the following lines:

```
service kshell
    {
            flags            = REUSE
            socket_type      = stream
            wait             = no
            user             = root
            log_on_success   += USERID
            log_on_failure   += USERID
            server           = /usr/share/centrifydc/kerberos/sbin/kshd
            server_args      = -5c
            disable          = no
    }
```

Restart the xinetd service using the instructions in the telnet server section.

To test that the rsh service is working correctly, login as an Active Directory authenticated user on the Linux system. Run the following command:

```
/usr/share/centrifydc/kerberos/bin/rsh hostname ls
```

Where hostname is the host name for machine you are logged into. The **rsh** program will attempt to login automatically and you should not be prompted for a user name or password. If the **ls** command was used then you should see a listing of the files in your home directory.

3.2 Using the DirectControl Kerberos Tools Client Applications

This section describes how to set up your Linux or UNIX execution environment to run the Kerberos utilities included with the DirectControl Kerberos Tools.

3.2.1 Setting up your command execution PATH

If you plan to use the Centrify Kerberos-based network utilities such as **telnet** or **ftp** by default, then it makes sense to alter your PATH environment variable to search the Kerberos bin directory before searching other directories. This can be accomplished by executing the following line, either at a shell session or from a startup script such as .profile or .bash_profile:

```
PATH=/usr/share/centrifydc/kerberos/bin:$PATH export PATH
```

Syntax for csh will be slightly different. Putting this directory at the beginning of your command execution path will ensure that the Centrify Kerberos utilities are run instead of existing Kerberos utilities that might already be loaded on your system.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

By setting the PATH variable, not only will the Kerberos utilities be found automatically but the MAN pages for these utilities will be found instead of standard MAN pages for each utility. For example, if you type:

```
man telnet
```

The manual page for the Kerberized **telnet** program will be displayed instead of the default manual page for BSD **telnet**.

With the path set correctly, you can now execute the programs in /usr/share/centrifydc/kerberos/bin directly from the shell.

3.2.2 Setting up a .k5login file

Network tools that use the MIT Kerberos stack use the .k5login file to indicate which users can connect without having to supply a password. A .k5login file indicates the User Principal Name (UPN) of users that are permitted to login silently as a given user. It is used by **ssh**, **telnet**, **ftp**, **rlogin** and **rsh**. This section explains when it is needed and what it must contain.

The file is not required if:

a) The UPN can be simply converted to the local user name by removing the default realm name from the UPN,

b) You are using Centrify's Kerberos libraries and you are logging in as yourself. These libraries can determine that your UPN matches your zone alias.

Otherwise you must create a .k5login file in the home directory of the target user on the target machine. The file must be owned either by root or by the target user.

The following includes some examples of when a .k5login file should be used and when it is not necessary if using the **telnet** utility:

- I am logged on as fred@centrify.com on machine1. My zone alias is "fred". I want to telnet to machine2 where my zone alias is also "fred". Machine2 is in the same zone as machine1. Both machines are in the centrify.com domain. In this case, I do not need a .k5login file. To invoke telnet to directly log into machine2, I would run:

  ```
  telnet –a machine2
  ```

- I am logged on as fred.thomas@centrify.com on machine1. My zone alias is "fred". I want to telnet to machine2 where my zone alias is also "fred". Machine2 is in the same zone. The telnet server on machine2 is using the Centrify libraries. In this case I do not need a .k5login file. To invoke telnet to directly log into machine2, I would run:

  ```
  telnet –a machine2
  ```

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

- I am logged on as fred.thomas@centrify.com on machine1. My zone alias is "fred". I want to telnet to machine2 where my zone alias is also "fred". Machine2 is in the same zone. The telnet server on machine2 is *not* using the Centrify libraries. In this case I do need a .k5login file. I need to create a .k5login file in the ~fred directory on machine2. It must contain (note the case):
  ```
  fred.thomas@CENTRIFY.COM
  ```
  Then I can do ...
  ```
  telnet –a machine2
  ```

- I am logged on as fred.thomas@centrify.com on machine1. My zone alias is "fred". I want to telnet to machine2 as "jane". In this case I do need a .k5login file. I need to create a .k5login file in the ~jane directory on machine2. It must contain:
  ```
  fred.thomas@CENTRIFY.COM
  ```
  Then I can do ...
  ```
  telnet –a –l jane machine2
  ```

Throughout these examples **telnet** was used as the sample application but these rules apply to all the Kerberized applications listed earlier. Note that the case of names in the .k5login file are important. The username is in lowercase. The domain name is in upper case.

3.2.3 Setting up a .netrc file

By default **ftp** will prompt you for the user name that you want to use. It will suggest your currently logged in user name but you will still need to press Enter in order to proceed. You can avoid this by creating a .netrc file in your home directory on the client machine. The .netrc file must contain a line indicating the user name for each target ftp server or you can specify a default.

For example I have logged on as fred.thomas on machine1. My zone alias is fredt. I want to silently connect to machine2. My .netrc file should contain:

```
default login fredt
```

or...

```
machine2 login fredt
```

3.2.4 Using the Centrify Kerberos libraries in runtime applications

The Centrify Kerberos libraries provide several enhancements over the standard MIT libraries. This section explains how to determine which libraries are being called by a program and how to change the libraries being used.

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

How to tell which libraries are being used

On most platforms you can use the **ldd** command to see what libraries a given binary will load. Here is a Linux example of a program that is using Centrify's libraries:

```
$ ldd /usr/share/centrifydc/kerberos/bin/telnet
libkrb4.so.2 => /usr/share/centrifydc/kerberos/lib/libkrb4.so.2
libdes425.so.3 => /usr/share/centrifydc/kerberos/lib/libdes425.so.3
libkrb5.so.3 => /usr/share/centrifydc/kerberos/lib/libkrb5.so.3
libk5crypto.so.3 => /usr/share/centrifydc/kerberos/lib/libk5crypto.so.3
libcom_err.so.3 => /usr/share/centrifydc/kerberos/lib/libcom_err.so.3
```

Here is an example using the original MIT telnet binary:

```
$ ldd /usr/kerberos/bin/telnet
libkrb4.so.2 => /usr/kerberos/lib/libkrb4.so.2
libkrb5.so.3 => /usr/kerberos/lib/libkrb5.so.3
libdes425.so.3 => /usr/kerberos/lib/libdes425.so.3
libk5crypto.so.3 => /usr/kerberos/lib/libk5crypto.so.3
libcom_err.so.3 => /usr/kerberos/lib/libcom_err.so.3
```

As you can see the second binary is not using Centrify's libraries. For MacOS you must use:

```
otool –L <binary
```

Controlling which libraries get used

There are three ways to control which libraries a program will use.

1. **Build time**: All of the tools that Centrify supply are built to explicitly use the Centrify libraries. In general the option of using different libraries is not available to you unless you can rebuild the application.

2. **System wide**: It is possible to tell the OS where to look for libraries to be loaded across the whole system. The mechanism for doing this varies from platform to platform.

   To modify the library search order for all applications on Linux, edit the file /etc/ld.so.conf and add the path to the Centrify libraries at the top of the file:

   ```
   /usr/share/centrifydc/kerberos/lib
   /usr/X11R6/lib
   /usr/lib/qt-3.1/lib
   /usr/lib/sane
   /usr/local/lib
   ```

   Then run the **ldconfig** command. For Solaris use the **crle** command.

   Warning: Before performing any system wide configuration changes of this nature consult your operating system documentation and ensure you have a backup route into your system. It is possible to configure the system in such a way that you cannot log on to it.

3. **For individual sessions**: It is possible to force applications to use a specific set of libraries while executing a script or running in a shell session. The mechanism for doing this varies from platform to platform. On Linux you must set the

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

LD_LIBRARY_PATH variable. Here is an example of running the MIT telnet program with the Centrify Kerberos libraries:

```
$ export LD_LIBRARY_PATH=/usr/share/centrifydc/kerberos/lib
$ ldd /usr/kerberos/bin/telnet
libkrb4.so.2 => /usr/share/centrifydc/kerberos/lib/libkrb4.so.2
libkrb5.so.3 => /usr/share/centrifydc/kerberos/lib/libkrb5.so.3
libdes425.so.3 => /usr/share/centrifydc/kerberos/lib/libdes425.so.3
libk5crypto.so.3 =>/usr/share/centrifydc/kerberos/lib/libk5crypto.so.3
libcom_err.so.3 => /usr/share/centrifydc/kerberos/lib/libcom_err.so.3
```

Note: For HP-UX the variable is called SHLIB_PATH. For AIX the variable is called LIBPATH.

3.2.5 Running Centrify Kerberos user utilities

A number of standard Kerberos utilities can be found the directory: /usr/share/centrifydc/kerberos/bin. These include: **kdestroy**, **kinit**, **klist**, **kpasswd**, **kvno**, **compile_et**, **ftp**, **gss-client**, **krb5-config**, **krb524init**, **ksu**, **rcp**, **rlogin**, **rsh**, **sclient**, **sim_client**, **telnet**, **uuclient**, **v4rcp.**

The following table provides a brief description for each of these utilities. For detailed information on each utility, see the included MAN page for the program.

Utility	Description
compile_et	Error table compiler
ftp	ARPANET file transfer program
kdestroy	Destroy Kerberos tickets
kinit	Obtain and cache Kerberos ticket-granting ticket
klist	List cached Kerberos tickets
kpasswd	Change a user's Kerberos password
krb5-config	Tool for linking against MIT Kerberos libraries
krb5-send-pr	Send problem report (PR) to a central support site
ksu	Kerberized super-user
kvno	Print key version numbers of Kerberos principals
rcp	Remote file copy
rlogin	Remote login
rsh	Remote shell
sclient	Sample Kerberos version 5 client
telnet	User interface to the TELNET protocol
v4rcp	Back end for Kerberos V4 rcp

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

To invoke the **telnet** remote login utility to login as the same user, use:

```
telnet –a machine
```

or if logging in as a different user, use:

```
telnet –a –l user machine
```

I both cases the "-a" flag will instruct the telnet program to attempt to log you in using your Kerberos ticket and if the ticket is valid, proceed directly to the remote terminal session without prompting you for a username or password. If the remote machine rejects your Kerberos ticket or if the telnet server is not Kerberos enabled, then you will be prompted for a password.

The FTP file transfer utility can be run by simply using:

```
ftp machine
```

The rsh and rlogin commands can be run in the usual way using:

```
rsh machine command
```

or…

```
rlogin machine
```

For all these Kerberos utilities, it is necessary to specify the target host by its hostname and not by its IP address or using "localhost" if logging into the same machine. When running **rsh**, the command can be any non-interactive command that could normally be run from your login shell. For example, to show all the processes on a remote machine called "linuxbox", you could run:

```
rsh linuxbox ps -aef
```

The rcp program is also Kerberos enabled and will allow you to copy files from one machine to another without being prompted for your user name or password. For example, to copy the file "localfile", that is in your current working directory to a file called "newfile" in your home directory on a remote machine called "linuxbox", use the following command:

```
rcp localfile linuxbox:newfile
```

The command **klist** can be used to see which tickets have been issued to you and when they are scheduled to expire. The **kinit** utility can be used for renewing your Kerberos tickets on the system. The **kdestroy** command can be used to remove all tickets that have been issued to you. Each of these commands will use the underlying Kerberos service that is automatically setup and maintained by Centrify DirectControl. The Kerberos authority corresponds to the domain controller that is being used for the Active Directory domain that you are joined to.

For specific instructions on usage for each of the included utilities, see the MAN pages that are included with the package.

3.3 Using the DirectControl Kerberos Development Components

With the DirectControl Kerberos Tools package installed, it is possible to use the Centrify Kerberos libraries when building applications. The Kerberos Tools package includes both

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

header files in /usr/share/centrifydc/include as well as standard Kerberos library files in /usr/share/centrifydc/lib. In order to use the headers and libraries, your application development environment needs to be able to locate these files. This is especially important on a system were an earlier version of MIT Kerberos is installed. For example, Red Hat 9 Linux includes version 1.2 of the MIT Kerberos environment. This version has some known issues working correctly with Microsoft's Kerberos implementation. Since the Centrify Kerberos environment is based on the latest MIT Kerberos 1.3 distribution, you will want to make sure your applications are linked with the Centrify Kerberos components.

There are a number of standard methods for ensuring that your build environment knows where to find the Centrify Kerberos components. For example, you might need to define these in a Makefile using something like:

```
CFLAGS= -I/usr/share/centrifydc/kerberos/include
CPPFLAGS= -I/usr/share/centrifydc/kerberos/include
LDFLAGS= -L/usr/share/centrifydc/kerberos/lib
```

Or, you may want to include the Kerberos library directory by defining the library path in the shell. For example:

```
LD_LIBRARY_PATH=/usr/share/centrifydc/kerberos/lib:$LD_LIBRARY_PATH
```

You may also find that if you are using the "configure" tool, it can take arguments which can specify which directory to use for Kerberos. For example, if you were building Samba on your system, you might use something like:

```
./configure --with-krb5=/usr/share/centrifydc/kerberos
```

Since the Centrify Kerberos development components are based on the latest MIT Kerberos distribution, there is no need to change existing application code that is designed to work with Kerberos. Applications that have been previously compiled to use Kerberos dynamically linked libraries do not need to be recompiled. Simply follow the instructions in the section "Using the Centrify Kerberos libraries in runtime applications" to ensure that the Centrify libraries are used when the application is run.

4 Summary

The Centrify DirectControl Kerberos Tools can be used by end users, system administrators and application developers to further leverage the secure connected computing environment that is enabled by DirectControl. This package provides the necessary components to allow single sign-on applications to run on UNIX, Linux and Mac while utilizing the security services provided by Active Directory.

4.1 Related Information and Technical Notes

Numerous books are available for developers that describe how to write Kerberos-enabled client and server applications or that provide more detail on existing applications that support Kerberos. O'Reilly's Kerberos: The Definitive Guide at

© CENTRIFY CORPORATION 2005. ALL RIGHTS RESERVED.

http://www.oreilly.com/catalog/kerberos/index.html is a good reference for further information about Kerberos and Kerberos applications.

4.2 For more information

For the latest product information on DirectControl, check out our web site at http://www.centrify.com/products.asp

4.3 Legal Notices

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Centrify Corporation. All rights reserved.

Centrify and DirectControl are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.