UNICOS/mk® Kerberos Enigma Installation Guide

004–5295–002

Record of Revision

Version	*Description*
1.3	December 1996 Original printing. This guide supports the 1.3 release of the UNICOS/mk operating system.
1.5	April 1997 This guide supports the 1.5 release of the UNICOS/mk operating system.
1.5.1	May 1997 This guide supports the 1.5.1 release of the UNICOS/mk operating system.
2.0.2	February 1998 This guide supports the 2.0.2 release of the UNICOS/mk operating system.
2.0.3	May 1998 This guide supports the 2.0.3 release of the UNICOS/mk operating system.
2.0.5	October 1999 This guide supports the 2.0.5 release of the UNICOS/mk operating system.

Contents

Preface

This publication is for analysts who install and maintain system software on Cray Research computer systems. This document contains procedures for installing the UNICOS/mk Kerberos Enigma software using the Common Install Tool (CIT) and the UNICOS/mk configuration tool (ConfigTool).

Related Publications

The following documents contain additional information that may be helpful:

- *Common Installation Tool (CIT) Reference Card*
- *Kerberos Administrator's Guide*
- *Kerberos User's Guide*
- *UNICOS/mk General Administration*
- *UNICOS/mk Resource Administration*
- *UNICOS/mk Configuration Reference Manual*
- *UNICOS/mk Networking Facilities Administration*
- *NQE Administration*
- *UNICOS/mk Tape Subsystem Administration*
- *UNICOS/mk Installation Guide for Cray T3E Series Systems*
- *UNICOS/mk User Commands Reference Manual*

Obtaining Publications

The *User Publications Catalog* describes the availability and content of all Cray hardware and software documents that are available to customers. Customers who subscribe to the Cray Inform (CRInform) program can access this information on the CRInform system.

To order a document, call +1 651 683 5907. SGI employees may send e-mail to `orderdsk@sgi.com`

Customers who subscribe to the CRInform program can order software release packages electronically by using the `Order Cray Software` option.

Customers outside of the United States and Canada should contact their local service organization for ordering and documentation information.

Conventions

The following conventions are used throughout this document:

Convention	Meaning
`command`	This fixed-space font denotes literal items (such as commands, files, routines, pathnames, signals, messages, programming language structures, and e-mail addresses) and items that appear on the screen.
`manpage`(*x*)	Man page section identifiers appear in parentheses after man page names. The following list describes the identifiers: 1 User commands 1B User commands ported from BSD 2 System calls 3 Library routines, macros, and opdefs 4 Devices (special files) 4P Protocols 5 File formats 7 Miscellaneous topics 7D DWB-related information 8 Administrator commands Some internal routines (for example, the `_assign_asgcmd_info`() routine) do not have man pages associated with them.
variable	Italic typeface denotes variable entries and words or concepts being defined.

`user input`	This bold, fixed-space font denotes literal items that the user enters in interactive sessions. Output is shown in nonbold, fixed-space font.
[ ]	Brackets enclose optional portions of a command or directive line.
...	Ellipses indicate that a preceding element can be repeated.

The default shell in the UNICOS and UNICOS/mk operating systems, referred to as the *standard shell*, is a version of the Korn shell that conforms to the following standards:

- Institute of Electrical and Electronics Engineers (IEEE) Portable Operating System Interface (POSIX) Standard 1003.2–1992
- X/Open Portability Guide, Issue 4 (XPG4)

The UNICOS and UNICOS/mk operating systems also support the optional use of the C shell.

Reader Comments

If you have comments about the technical accuracy, content, or organization of this document, please tell us. Be sure to include the title and part number of the document with your comments.

You can contact us in any of the following ways:

- Send e-mail to the following address:

  `techpubs@sgi.com`

- Send a fax to the attention of "Technical Publications" at: +1 650 932 0801.
- Use the Feedback option on the Technical Publications Library World Wide Web page:

  `http://techpubs.sgi.com`

- Call the Technical Publications Group, through the Technical Assistance Center, using one of the following numbers:

  For SGI IRIX based operating systems: 1 800 800 4SGI

For UNICOS or UNICOS/mk based operating systems or Cray Origin 2000 systems: 1 800 950 2729 (toll free from the United States and Canada) or +1 651 683 5600

- Send mail to the following address:

  Technical Publications
  SGI
  1600 Amphitheatre Pkwy.
  Mountain View, California 94043–1351

We value your comments and will respond to them promptly.

Installing UNICOS/mk Kerberos Enigma 2.0.5 [1]

1.1 Introduction

This section contains procedures for installing UNICOS/mk Kerberos Enigma software, release 2.0.5, using the Common Installation Tool (CIT).

The base UNICOS/mk 2.0.5 operating system and the latest revision or update software must be loaded before Kerberos Enigma software can be installed.

Note: UNICOS/mk Kerberos Enigma software must be reinstalled whenever the UNICOS/mk operating system is updated or changed.

1.2 UNICOS/mk Kerberos Enigma CD

The UNICOS/mk Kerberos Enigma CD contains the UNICOS/mk Kerberos Enigma software that can be used for upgrade installations. The path to these packages after the UNICOS/mk Kerberos Enigma CD has been mounted on the SWS is `/cdrom/cdrom0`.

Two types of Kerberos Enigma software are distributed:

`krb_dom`	*Domestic_Kerberos* is the Common Installation Tool (CIT) name for this package. It is a binary-only version of Kerberos for domestic sites.
`krb_for`	*International_Kerberos* is the CIT name for this package, which is a binary-only version of Kerberos for international sites.

Sites should install the UNICOS/mk Kerberos Enigma software after they have successfully installed and configured the UNICOS/mk release. Kerberos Enigma installation should be done as a separate step because it involves loading new software, configuring various system daemons, and possibly restarting a system.

1.3 Preparing for the Upgrade

Before you start the Kerberos Enigma Installation process, you must complete the following tasks:

- Load the corresponding UNICOS/mk release.
- Complete the network system configuration so that it is up and running.
- Make, label, and mount the partitions on which the Kerberos Enigma software will be installed.

Before starting the Kerberos Enigma installation and CIT, you must properly set up two `.rhosts` files by performing the following steps:

- Verify that the `~crayadm/.rhosts` file on the SWS allows `root` to send remote shell commands to the SWS from the mainframe.
- Verify that the `/.rhosts` file on the Cray Research mainframe allows `crayadm` to send remote shell commands to the mainframe from the SWS.

  Note: For more information on the communications path between the SWS and the Cray Research mainframe, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the */cdrom_mountpoint*`/CYRIinstall/2218.ps`.

1.4 Starting the Kerberos Enigma Software Installation

Now that you prepared the workstation or console, you can load the Kerberos Enigma software onto the Cray Research mainframe. To load the software, follow these steps:

1. Insert the UNICOS/mk Kerberos Enigma CD into the SWS.
2. Log in to the SWS as `crayadm`.
3. Use CIT to install Kerberos Enigma by loading it from the SWS to the Cray Research mainframe with the following command:

   ```
   sws% /cdrom_mountpoint/setup -c CrayNetworkNodeName -l root
   ```

   The installation log files are located on the workstation as `/tmp/cit.`*username*`/*.log`.

   For more information about using CIT, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the

/cdrom_mountpoint/CYRIinstall/2218.ps. You may also select the Help button from the GUI, or enter **help all** at the interactive interface prompt.

a. Select the Kerberos Enigma release.

b. Install the Kerberos Enigma release.

c. Verify that the Cray Research mainframe information is correct. If it is not, correct the information in CIT.

d. Quit CIT when you have finished loading the UNICOS/mk release.

4. Remove the root entry from the ~crayadm/.rhosts file on the SWS and the crayadm entry from the /.rhosts file on the Cray system. This will undo the .rhosts file changes made in Section 1.3, page 2.

1.5 Configuring the Kerberos Enigma Software

Follow the steps in this section to configure the UNICOS/mk Kerberos Enigma software using the ConfigTool (CT) configuration tool.

For more information on the use of the CT, see the *UNICOS/mk Installation Guide for Cray T3E Series Systems.*

1.5.1 Configuring /etc/krb.conf

The Kerberos configuration file is usually named /etc/krb.conf in UNICOS/mk applications. This file contains information about the local Kerberos configuration.

Create the /etc/krb.conf file by using vi or another editor. This file should have permissions set to 644 and be owned by root.

The following is a sample /etc/krb.conf file:

```
CRAY.COM
CRAY.COM   krb_server_1
CRAY.COM   krb_server_2
CRAY.COM   krb_server_1            admin server
```

Line 1 of this file specifies the name of the local realm. In the example file, this is CRAY.COM. (You are free to name your realm whatever you choose; however, the realm name in the /etc/krb.conf file must match the realm name used to create the Kerberos database on the Kerberos server.) Lines 2 and 3 list the

host names for two Kerberos servers, krb_server_1 and krb_server_2. These are the servers from which the Kerberos software will request tickets. The software searches the /etc/krb.conf file from the top and tries each listed server until it obtains a response.

The last line indicates the location at which the Kerberos administrative server process is running. It is recommended that only one administrative server process be configured, because no mechanism is in place to propagate changes to the Kerberos principal database from a slave to the primary server.

1.5.2 Configuring /etc/services

The network services configuration file, /etc/services, should be modified to support Kerberos utilities and kerberized clients and servers on the Cray Research system.

In the following example, each row represents information in the /etc/services file that needs to be entered into a new record using the configuration tool's (CT) Form Viewer. Each record in the Form Viewer corresponds to a row in /etc/services.

If the following records already exist in your /etc/services file, you can skip steps 1–11.

```
klogin            543/tcp         # Kerberos authenticated rlogin
kshell            544/tcp         # Kerberos authenticated rshell
kerberos          750/udp         # Kerberos server
kerberos_master   751/tcp         # Kerberos administrator
eklogin           2105/tcp        # Kerberos encrypted login
```

To configure the/etc/services file with the CT, complete the following steps:

1. In the /etc/ct directory, start the CT by entering the following command:

   ./configtool

2. If there is an existing /etc/services file, create a backup copy. Select Preferences->Backup Old Configuration.
3. Select the /etc/services subsystem (Services).
4. Load the existing /etc/services file, or create a new file.
5. Select New Record to create a new record.
6. Select the new record in the Form Viewer window.

7. Edit the new record.

   The following example shows how the `klogin` information in the example `/etc/services` file is entered in the CT. Each record in the `Form Viewer` corresponds to a row in `/etc/services`.

```
Networking Services Configuration

 S-> Transport Protocol                          tcp
     Service name                                klogin
     TCP Port number                             543
     Comment                                     Kerberos
     Alias
     Alias
     Alias
     Alias
```

8. Repeat steps 5–7 until you have made new records for `klogin`, `kshell`, `kerberos`, `kerberos_master`, and `eklogin` (if they don't already exist in `/etc/services`).
9. In the `Menu Viewer` window, select `File->Save`.
10. In the `ConfigTool Save` window, select the path and file name and `Save`.
11. In the `Menu Viewer` window, select `File->Exit`.

1.5.3 Configuring `/etc/inetd.conf`

In the following example, each row represents information in the `/etc/inetd.conf` file that needs to be entered into a new record using the CT's `Form Viewer`. Each record in the `Form Viewer` corresponds to a row in the `/etc/inetd.conf` file.

If the following records already exist in your `/etc/inetd.conf` file, you can skip steps 1–12.

```
kshell  stream  tcp  nowait  root  /etc/kshd      kshd
klogin  stream  tcp  nowait  root  /etc/klogind   klogind
eklogin stream  tcp  nowait  root  /etc/klogind   eklogind
```

To configure `/etc/inetd.conf` with the CT, complete the following steps:

1. In the `/etc/ct` directory, start the CT by entering the following command:

   `./configtool`

2. If there is an existing `/etc/inetd.conf` file, create a backup copy. Select `Preferences menu->Backup Old Configuration`.
3. Select the `/etc/inetd.conf` subsystem (`Inetd`).
4. Load the existing `/etc/inetd.conf` file, or create a new file.
5. Select `New Record` to create a new record.
6. Edit the new record.
7. In the `Menu Viewer` window, select the new record, as shown:

```
Generic Internet Daemon Configuration

 S-> Enable this daemon?                          YES
     Port name or number                          kshell
     Connection type                              stream
     Transport protocol                           tcp
     Wait for the daemon to return?               NO
     User name to run daemon as                   root
     Internal to inetd?                           NO
     Pathname of daemon                           /etc/kshd
     Arguments                                    kshd
```

   The example below shows how the `kshell` information from the example `/etc/inetd.conf` file is entered in the CT. Each record in the `Form Viewer` corresponds to a row in the example `/etc/inetd.conf` file.

```
Port name or number    Pathname of daemon    Arguments
-------------------    ------------------    ---------
klogin                 /etc/klogind          klogind
eklogin                /etc/klogind          eklogind
```

8. Repeat steps 5–7 until you have made new records for `kshell`, `klogin`, and `eklogin` (if they do not already exist in `/etc/inetd.conf` on the Cray Research mainframe).

   Note: If this is an international site (excluding the United States and Canada) do not add `eklogin` to the `inetd.conf` file.

9. After you add the daemons, press `e` to escape and respond **`y`** to the question `Do you want to update form file? (y/n):`
10. In the `Menu Viewer` window, select `File->Save`.
11. In the `ConfigTool Save` window, select the path and file name and `Save`.

12. In the Menu Viewer window, select File->Exit.

1.5.4 Configuring /etc/srvtab

The /etc/srvtab binary file is generated on your site's Kerberos server by the Kerberos administrator on the Kerberos master server machine. This file must be securely transferred to the Cray Research system, installed in /etc/srvtab with a permission of 600, and owned by root.

1.5.5 Signaling inetd

If your site has configured inetd.conf for Kerberos on a running system, use the kill(1) command to send a signal to the inetd daemon so that it will reread the configuration file (inetd.conf) and start using Kerberos.

The following is an example of using the kill command:

```
# ps -e | grep inetd
  1719 ?     0:27 inetd
# kill -1 1719
```

1.5.6 Configuring krbipd into the /etc/config/daemons File

If your site decides to run krbipd, which is the Kerberos remote procedure call (RPC) daemon for multihomed machines (more than one network interface), use the CT to configure krbipd to be started at boot time. Specifically, you will add the following line to the /etc/config/daemons file:

```
TCP   Krbipd  YES  *  /etc/krbipd
```

1. In the /etc/ct directory, start the CT by entering the following command:

   ```
   ./configtool
   ```

2. If there is an existing /etc/config/daemons file, create a backup copy. Select Preferences menu->Backup Old Configuration.
3. Select the /etc/config/daemons subsystem (Daemons).
4. Load the existing /etc/config/daemons file, or create a new file.
5. Select New Record to create a new record.
6. Edit the new record.

7. In the Menu Viewer window, select the new record.
8. Enter the new krbipd daemon.

   The following example shows how the krbipd information from the example /etc/config/daemons file is entered in the CT. The new record represents a new row in the configuration file after it is saved.

```
System Daemons Table

 S-> Group                                          TCP
     Name                                           krbipd
     Start up at boot time?                         YES
     Kill action                                    *
     Executable path name                           /etc/krbipd
     Command-line arguments
     Additional command-line arguments
     Additional command-line arguments
```

9. In the ConfigTool Save window, select the path and file name and Save.
10. In the Menu Viewer window, select File->Exit.
11. In the ConfigTool Save window, select the path and file name and Save.
12. In the Menu Viewer window, select File->Exit.

1.5.7 Restarting /etc/krbipd daemon

To start krbipd on a running system, without rebooting the system, enter the following command:

```
# /etc/krbipd
```

1.5.8 Configuring kerbd into the /etc/config/daemons File

If your site has decided to run kerberized network file system (NFS) (NFSKRB), you must add kerbd to the daemons to be started at boot time. Specifically, you will add the following line to the file:

```
NFS  kerbd  YES  *  /etc/kerbd
```

1. In the /etc/ct directory, start the CT by entering ./configtool.

2. If there is an existing /etc/config/daemons file, create a backup copy. Select Preferences menu->Backup Old Configuration.
3. Select the /etc/config/daemons subsystem (Daemons).
4. Load the existing /etc/config/daemons file, or create a new file.
5. Select New Record to create a new record.
6. In the Menu Viewer window, select the new record.
7. Edit the new record.
8. Enter the new kerbd daemon.

   The following example shows how the kerbd information in the example /etc/config/daemons file is entered in the CT. The new record represents a new row in the configuration file after it is saved.

```
System Daemons Table

 S-> Group                                   NFS
     Name                                    kerbd
     Start up at boot time?                  YES
     Kill action                             *
     Executable path name                    /etc/kerbd
     Command-line arguments
     Additional command-line arguments
     Additional command-line arguments
```

9. In the ConfigTool Save window, select the path and file name and Save.
10. In the Menu Viewer window, select File->Exit.
11. In the ConfigTool Save window, select the path and file name and Save.
12. In the Menu Viewer window, select File->Exit.

1.5.9 Restarting /etc/kerbd Daemon

To start kerbd on a running system without rebooting the system, enter the following command:

```
# sdaemon -s kerbd
```