PAM Kerberos Release Notes for HP-UX 11.0

HP 9000 Systems

Manufacturing Part Number: J5849-90015
E0905

U.S.A.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Trademark Notices

Copyright Notices

1 PAM Kerberos Release Notes for HP-UX 11.0

Information in this document applies to the Web release of PAM Kerberos v 1.12 for HP-UX 11.0.

Announcement

PAM-Kerberos is based on Kerberos Authentication System V5, developed by Massachusetts Institute of Technology (MIT). The PAM Kerberos module is compliant with IETF RFC 1510 and Open Group RFC 86.HP-UX PAM Kerberos is implemented under the PAM (Pluggable Authentication Module) framework. PAM Kerberos works with Microsoft Windows 2000 and MIT Kerberos V5 KDC. However, it is not intended to work with the HP-UX DCE KDC.

Obsolescence of PAM Kerberos Versions on HP-UX 11.0 and HP-UX 11i v1.6

Table 1-1 lists the obsolescence dates for HP-UX 11.0 and HP-UX 11i v1.6.

Table 1-1 Product Discontinuance and Obsolescence Dates

HP-UX Version	Introduction	Discontinuance	Obsolescence
HP-UX 11.0	November 1997	31st January 2005	31st December 2006
HP-UX 11i v1.6	June 2002	30th April 2004	31st October 2005

What's in This Version

The HP-UX 11.0 PAM-Kerberos bundle contains Kerberos Client and Generic Security Services Application Programming Interface (GSSAPI) products.

The PAM service modules are implemented as a shared library listed below:

- The Kerberos PAM library
- The `/usr/lib/security/libpam_krb5.1` library, which uses Krb5 APIs, and the `pam_krb5` manpage.

Table 1-2 lists the filesets that are included in PAM Kerberos v 1.12.

Table 1-2 Filesets Included in PAM Kerberos v 1.12

Fileset	Path Name
PAM-KRB-SHLIB	/usr/lib/security/libpam_krb5.1
PAM-KRB-MAN	• /usr/share/doc/PAMKerberosRelNotes.pdf • /usr/share/man/man5.Z/pam_krb5.5

New in This Version

This version of PAM Kerberos contains a defect fix in Kerberos Client. For more information on the defect fix, see “Patches and Fixes in This Version” on page 12.

Benefits and Features

Following are the benefits and features of PAM Kerberos:

- Supports HP-UX login, which works with any Kerberos 5 Server. Passwords are effectively unified within a heterogeneous environment such as Microsoft Windows 2000.
- Supports the password change protocol, which automates propagation of password changes.

These two features can significantly reduce user administration complexity in heterogeneous environments.

For detailed product information, installing and configuring instructions, troubleshooting and sample configuration files, refer to *Configuration Guide for Kerberos Client Products on HP-UX* (# T1417-90006).

Known Problems and Workarounds

- The Kerberos system `ftp` service may list the `/etc/issue` file before the expected output. Refer to *SIS (5)* manpage for more details on Secure Internet Services (SIS).
- If the password has expired on a Microsoft Windows 2000 KDC, the user is not prompted for a new password and cannot log in. This is a known problem in Microsoft Windows 2000.

Compatibility Information and Installation Requirements

This section details the prerequisites for installing PAM Kerberos v1.12 on HP-UX 11.0.

Hardware Requirements

HP 9000 servers with a minimum of 32 MB of memory and sufficient swap space (a minimum of 50 MB is recommended).

Operating System Requirements

HP-UX 11.0

Disk Space Requirements

Minimum disk space required to install the product is 1 MB. Additional disk space of 1 KB per user is required to store initial *Ticket Granting Ticket (TGT)* in credential cache files.

The size of each cache file grows in proportion with additional *Service Tickets* obtained. Provision must be made in the `/tmp` folder to accommodate the credential cache files.

Notes, Cautions and Warnings

- For each user, make sure that the UNIX `uid`, home directory, and shell information exist in the UNIX repository, `/etc/passwd`.
- The Kerberos PAM module sets and uses an environment variable, `KRB5CCNAME`, during authentication. Concurrent execution in the same shell environment of any PAM modules may result in unexpected behavior.
- If the superuser `root` changes a user's password, the `passwd` program under the HP-UX environment does not prompt for the old password. However, when Kerberos PAM module, `libpam_krb5.1`, is stacked with UNIX PAM, `libpam_unix.1` in the `pam.conf` file, the behavior is different.

  For example, under this `pam.conf` configuration:

  ```
  passwd password required /usr/lib/security/libpam_unix.1
  passwd password required /usr/lib/security/libpam_krb5.1
  use_first_pass
  ```

  When the superuser `root` changes a user's Kerberos password, the old password is required. However, when UNIX PAM is the first module in the stack, it does not store the old password, so a special situation arises in which the Kerberos password change fails. This failure is caused by the fact that the password is changed for the UNIX account, but is *not* changed for the Kerberos account. You can avoid this situation by *not* using the `use_first_pass` option.
- To take advantage of the user policy definition service module `libpam_updbe.1` (pam_updbe(5)), this module must be the first module in the stack, as shown in the example below:

  ```
  # pam.conf:
  #
  login   auth   required    /usr/lib/security/libpam_updbe.1
  login   auth   sufficient  /usr/lib/security/libpam_krb5.1
  login   auth   required    /usr/lib/security/libpam_unix.1
  try_first_pass
  ```

Patches and Fixes in This Version

All patches have been incorporated into this release.

Defect Fix in This Version

The following defect has been fixed in this version of PAM Kerberos:

JAGaf64805	KRB5-Client was unable to receive packets properly under certain conditions.

Known Limitations

- Do not stack PAM Kerberos module (`libpam_krb5.1`) and DCE plug-in module (`libpam_dce.1`) in the `pam.conf` file. This kind of stacking produces unpredictable results.

  The PAM Kerberos (`libpam_krb5.1`) module and the DCE (`libpam_dce.1`) module use a different principal style and a different credential file path. For the principal style, the DCE Kerberos module uses cell name, whereas PAM Kerberos uses realm name. For the credential cache file, DCE Kerberos stores its credentials in the `/var/opt/dce/creds` path, while PAM Kerberos stores them in the `/tmp/pam_krb5/creds` path.

- When you change passwords on a MIT KDC with a version prior to 1.1, up to 45 seconds may elapse before the password is actually changed. This occurs due to the protocol selection mechanism of the change password protocol.

Related Documentation

The list below contains documentation related to the PAM Kerberos product:

- *Configuration Guide for Kerberos Client Products on HP-UX* (J5849-90006)
- The *krb5.conf (4)*, *kerberos (9)*, *pam.conf (4)*, *pam_user.conf (4),* and `pam (3)`manpages.