

Kerberos Client Version D.1.6.2.04 Release Notes

HP Part Number: 5969-7021
Published: October 2009
Edition: HP-UX 11i v2



© Copyright 2009 Hewlett-Packard Development Company, L.P

Legal Notices

Copyright 2009 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

UNIX is a registered trademark of The Open Group.

Table of Contents

1 Kerberos Client D.1.6.2.04 Release Notes.....	5
Announcement.....	5
Encryption Types Supported by Kerberos Client.....	6
What Is New in This Version.....	7
Features Supported From Kerberos Client Version 1.3.5.....	7
Known Problems and Workarounds.....	8
Installation Requirements for Kerberos Client D.1.6.2.04 on HP-UX 11i v2.....	8
System Requirements.....	8
Patch Requirements.....	8
Installing Kerberos Client D.1.6.2.04.....	9
Defect Fixes in This Version.....	9
Related Documentation.....	10

List of Tables

1-1	Kerberos Client Libraries on PA-RISC (PA) and Itanium (IA) Architecture.....	5
1-2	Kerberos Client Utilities.....	6
1-3	Encryption Types supported by Kerberos Client D.1.6.2.04.....	6
1-4	System Requirements for Installing Kerberos Client D.1.6.2.04.....	8

1 Kerberos Client D.1.6.2.04 Release Notes

Information in this document applies to the Web release of Kerberos Client D.1.6.2.04 for HP-UX 11i v2.

Announcement

Kerberos Client (`krb5client`) is a Web upgrade for KRB5-Client. KRB5-Client is a part of the core HP-UX 11i v1 and HP-UX 11i v2 operating systems. The previous version of Kerberos Client, KRB5-Client, was released as part of the core HP-UX 11i v2 operating system.

HP-UX provides Kerberos Client software including libraries, header files, and utilities for implementing secured client/server applications in either 32-bit or 64-bit development environments. These libraries, header files, and utilities are linked to the corresponding libraries, header files, and utilities in the core product.

Table 1-1 lists the libraries that Kerberos Client supports on HP-UX 11i v2.

Table 1-1 Kerberos Client Libraries on PA-RISC (PA) and Itanium (IA) Architecture

Architecture	32-bit	64-bit	Functionality
PA-RISC	<code>/usr/lib/libkrb5.sl -> /opt/krb5client/lib/libkrb5.1</code>	<code>/usr/lib/pa20_64/libkrb5.sl -> /opt/krb5client/lib/pa20_64/libkrb5.1</code>	Authenticate users, verify tickets, create authenticator, and manage the context.
	<code>/usr/lib/libcom_err.sl -> /opt/krb5client/lib/libcom_err.1</code>	<code>/usr/lib/pa20_64/libcom_err.sl -> /opt/krb5client/lib/pa20_64/libcom_err.1</code>	Print appropriate error messages to <code>stderr</code> based on the error code returned by the Kerberos APIs.
	<code>/usr/lib/libk5crypto.sl -> /opt/krb5client/lib/libk5crypto.1</code>	<code>/usr/lib/pa20_64/libk5crypto.sl -> /opt/krb5client/lib/pa20_64/libk5crypto.1</code>	Encrypt (DES, 3DES, AES, and RC4) and decrypt all communication between users to ensure privacy and data integrity.
	<code>/usr/lib/gss/libgssapi_krb5.sl -> /opt/krb5client/lib/gss/libgssapi_krb5.1</code>	<code>/usr/lib/pa20_64/gss/libgssapi_krb5.sl -> /opt/krb5client/lib/pa20_64/gss/libgssapi_krb5.1</code>	Kerberos-mechanism specific library used by GSSAPI (<code>/usr/lib/libgss.sl</code>)
Itanium	<code>/usr/lib/hpux32/libkrb5.so -> /opt/krb5client/lib/hpux32/libkrb5.so.1</code>	<code>/usr/lib/hpux64/libkrb5.so -> /opt/krb5client/lib/hpux64/libkrb5.so.1</code>	Authenticate users, verify tickets, create authenticator, and manage the context.
	<code>/usr/lib/hpux32/libcom_err.so -> /opt/krb5client/lib/hpux32/libcom_err.so.1</code>	<code>/usr/lib/hpux64/libcom_err.so -> /opt/krb5client/lib/hpux64/libcom_err.so.1</code>	Print appropriate error messages to <code>stderr</code> based on the error code returned by the Kerberos APIs.
	<code>/usr/lib/hpux32/libk5crypto.so -> /opt/krb5client/lib/hpux32/libk5crypto.so.1</code>	<code>/usr/lib/hpux64/libk5crypto.so -> /opt/krb5client/lib/hpux64/libk5crypto.so.1</code>	Encrypt (DES, 3DES, AES, and RC4) and decrypt all communication between users to ensure privacy and data integrity.
	<code>/usr/lib/hpux32/gss/libgssapi_krb5.so -> /opt/krb5client/lib/hpux32/gss/libgssapi_krb5.so.1</code>	<code>/usr/lib/hpux64/gss/libgssapi_krb5.so -> /opt/krb5client/lib/hpux64/gss/libgssapi_krb5.so.1</code>	Kerberos-mechanism specific library used by GSSAPI (<code>/usr/lib/libgss.sl</code>)

The client libraries are based on MIT Kerberos V5 1.6.2 release. The KRB5-Client libraries support DES, 3DES, RC4, and AES, as specified in RFC 1510 of the IETF. This release of Kerberos Client is interoperable with Microsoft Windows® 2000 and 2003.

Table 1-2 lists and describes the utilities that Kerberos Client includes.

Table 1-2 Kerberos Client Utilities

Utility	Function
/usr/bin/kinit ->/opt/krb5client/bin/kinit ¹	Obtains and caches the Kerberos ticket-granting ticket
/usr/bin/klist -> /opt/krb5client/bin/klist	Lists cached Kerberos tickets
/usr/bin/kvno -> /opt/krb5client/bin/kvno	Prints key version numbers of Kerberos principals
/usr/bin/kpasswd -> /opt/krb5client/bin/kpasswd	Changes a user's Kerberos password
/usr/sbin/ktutil -> /opt/krb5client/sbin/ktutil	Maintains the Kerberos keytab file
/usr/bin/kdestroy -> /opt/krb5client/bin/kdestroy	Destroys the user's active Kerberos tickets

¹ The -> symbol indicates that the core file links to the corresponding file in the krb5client product.

Kerberos Client includes the following header files:

- /usr/include/profile.h -> /opt/krb5client/include/profile.h
- /usr/include/krb5.h -> /opt/krb5client/include/krb5.h
- /usr/include/com_err.h -> /opt/krb5client/include/com_err.h
- /usr/include/krb5/gssapi.h -> /opt/krb5client/include/krb5/gssapi.h

Encryption Types Supported by Kerberos Client

Table 1-3 lists the encryption types supported by Kerberos Client D.1.6.2.04.

Table 1-3 Encryption Types supported by Kerberos Client D.1.6.2.04

Encryption Type	Description
des-cbc-crc	DES cbc mode with CRC-32
des-cbc-md4	DES cbc mode with RSA-MD4
des-cbc-md5	DES cbc mode with RSA-MD5
des	DES cbc mode with RSA-MD5 This encryption type is an alias to the des-cbc-md5 encryption type. If you specify des in the configuration file, then its behavior is the same as des-cbc-md5.
des-cbc-raw	DES cbc mode raw
des3-cbc-raw	Triple DES cbc mode raw
des3-cbc-sha1	Triple DES cbc mode with HMAC/sha1
des3-hmac-sha1	Triple DES cbc mode with HMAC/sha1 This encryption type is an alias to the des3-cbc-sha1 encryption type. If you specify des3-hmac-sha1 in the configuration file, then its behavior is the same as des3-cbc-sha1.
des3-cbc-sha1-kd	Triple DES cbc mode with HMAC/sha1 This encryption type is an alias to the des3-cbc-sha1 encryption type. If you specify des3-cbc-sha1-kd in the configuration file, then its behavior is the same as des3-cbc-sha1.

Table 1-3 Encryption Types supported by Kerberos Client D.1.6.2.04 (continued)

Encryption Type	Description
des-hmac-sha1	DES with HMAC/sha1
arcfour-hmac	ArcFour with HMAC/md5
rc4-hmac	ArcFour with HMAC/md5 This encryption type is an alias to the arcfour-hmac encryption type. If you specify rc4-hmac in the configuration file, then it's behavior is the same as arcfour-hmac.
arcfour-hmac-md5	ArcFour with HMAC/md5 This encryption type is an alias to the arcfour-hmac encryption type. If you specify arcfour-hmac-md5 in the configuration file, then it's behavior is the same as arcfour-hmac.
arcfour-hmac-exp	Exportable ArcFour with HMAC/md5
rc4-hmac-exp	Exportable ArcFour with HMAC/md5 This encryption type is an alias to the arcfour-hmac-exp encryption type. If you specify rc4-hmac-exp in the configuration file, then it's behavior is the same as arcfour-hmac-exp.
arcfour-hmac-md5-exp	Exportable ArcFour with HMAC/md5 This encryption type is an alias to the arcfour-hmac-exp encryption type. If you specify arcfour-hmac-md5-exp in the configuration file, then it's behavior is the same as arcfour-hmac-exp.
aes128-cts-hmac-sha1-96	AES-128 CTS mode with 96-bit SHA-1 HMAC
aes128-cts	AES-128 CTS mode with 96-bit SHA-1 HMAC This encryption type is an alias to the aes128-cts-hmac-sha1-96 encryption type. If you specify aes128-cts in the configuration file, then it's behavior is the same as aes128-cts-hmac-sha1-96.
aes256-cts-hmac-sha1-96	AES-256 CTS mode with 96-bit SHA-1 HMAC
aes256-cts	AES-256 CTS mode with 96-bit SHA-1 HMAC This encryption type is an alias to the aes256-cts-hmac-sha1-96 encryption type. If you specify aes256-cts in the configuration file, then it's behavior is the same as aes256-cts-hmac-sha1-96.

What Is New in This Version

Kerberos Client D.1.6.2.04 is a defect-fix release and does not contain any new features. For more information on the defects fixed in this release, see “Defect Fixes in This Version” (page 9).

Features Supported From Kerberos Client Version 1.3.5

Kerberos Client version D.1.6.2.04 also supports the following features from Kerberos Client version 1.3.5:

- SASL/GSS-API bind to Netscape Directory Server used to fail when SSL was enabled
- Support for powerful cryptographic algorithms
This version of Kerberos Client software supports 3DES, AES, and RC4
- Support for IPv6
IPv6 support is enabled on this version of Kerberos Client software

- Support for TCP
Kerberos Client libraries can now use TCP to connect to the Key Distribution Center (KDC). Libraries can use TCP to communicate with Microsoft KDCs (domain controllers) if they issue tickets with excess PAC data.
- Security fixes up to version 1.6.2 made by MIT in the open source version of Kerberos Client.
- Administrators can now control the behavior of Kerberized login applications that call the `krb5_kuserok` API provided by the `libkrb5.s1` library. In earlier versions of Kerberos Client, `krb5_kuserok` checked the `.k5login` file in the user's home directory for access permissions. This enabled users to modify the `.k5login` file and allow access to other users. Administrators can now create files with the name `.k5login.<username>` in the `/etc/krb5/` directory. Administrators can also create symbolic links pointing to the `.k5login` file in the user's home directory. If the `/etc/krb5` directory does not exist `krb5_kuserok` continues to check the `.k5login` file in the user's home directory. If the `/etc/krb5/` directory exists, the `krb5_kuserok` API ignores any corresponding `.k5login` files in the user's home directory while making authorization decisions. The format of the entries in the new files in `/etc/krb5` continues to be the same as that of the `.k5login` file in the user's home directory.

For detailed product information, installing and configuring instructions, troubleshooting and sample configuration files, see *Configuration Guide for Kerberos Client Products on HP-UX* (5991-7718), at: <http://docs.hp.com/en/internet.html#Kerberos>.

Known Problems and Workarounds

Following are the known problems and workarounds:

- To use files to resolve host entries, you must add the following line to the `/etc/nsswitch.conf` file:
`ipnodes : dns files`

Installation Requirements for Kerberos Client D.1.6.2.04 on HP-UX 11i v2

This section discusses the prerequisites for installing Kerberos Client version D.1.6.2.04 on HP-UX 11i v2.

System Requirements

Table 1-4 specifies the minimum system requirements for installing Kerberos Client D.1.6.2.04.

Table 1-4 System Requirements for Installing Kerberos Client D.1.6.2.04

Component	Requirement
Operating system	HP-UX 11i v2
Hardware requirement	HP 9000 workstations and servers with a minimum of 32 MB of memory and sufficient swap space. HP recommends that your servers or workstations have a minimum of 50 MB of memory.
Disk space requirement for the <code>krb5client</code> product	5 MB
Disk space requirement for the complete <code>KRB5CLIENT</code> bundle	36 MB
Software availability in native languages	English only

Patch Requirements

You must install patch PHSS_39765 before installing Kerberos Client D.1.6.2.04.

Installing Kerberos Client D.1.6.2.04

To install Kerberos Client D.1.6.2.04, complete the following steps:

1. Log in as superuser.
2. Download the depot from the Software Depot at: <http://h20293.www2.hp.com/>.
3. Fill out the registration form, and ensure that you select HP-UX 11i v2 as the operating system.
4. Download the Kerberos Client Software Depot and move it to the /tmp directory.
5. Verify if the file downloaded correctly by entering the following command:

```
# swlist -d @ /tmp/<KRB5CLIENT.depot>
```

The following output is displayed if the file is downloaded correctly:

```
# Initializing...
# Contacting target "localhost"...
#
# Target: localhost:/tmp/KRB5CLIENT.depot
#
#
# Bundle(s) :
```

```
KRB5CLIENT D.1.6.2.04 Kerberos V5 Client Version 1.6.2.04
```



NOTE: When using the `swlist` and `swinstall` commands, you must specify the absolute path of the source depot.

6. On a standalone system, enter the following command to install the Kerberos Client software bundle:

```
# swinstall -s /tmp/KRB5CLIENT.depot
```

The `swinstall` window is displayed.
7. Select **Mark for Install** in the **Action** menu to select the bundle and the patches that you want to install.
8. Select **Install** in the **Action** menu.
The Install Analysis window is displayed.
9. Select **OK** when the Status Field displays a Ready message.
The Install window is displayed and the Kerberos Client installation starts.
10. Select **Done** when the Status field displays a Completed message.
11. Select **File->Exit** to exit from the `swinstall` window.

Defect Fixes in This Version

The following defects are fixed in Kerberos Client D.1.6.2.04:

QXCR1000961607 Symptom: HP-UX Kerberos Client does not support the DES-CBC-RAW or DES3-CBC-RAW encryption standards.

Defect Description: HP-UX Kerberos Client does not support the DES-CBC-RAW or DES3-CBC-RAW encryption standards.

Resolution: The Kerberos Client now supports the DES-CBC-RAW and DES3-CBC-RAW encryption standards.

QXCR1000953090 Symptom: HP CIFS Server is not compatible with Kerberos Client version 1.6.2.01 on HP-UX 11i v2.
Defect Description: HP CIFS Server is not compatible with Kerberos Client version 1.6.2.01 on HP-UX 11i v2.
Resolution: This problem is fixed. HP CIFS Server is compatible with Kerberos Client version 1.6.2.04 on HP-UX 11i v2.

Related Documentation

For more information about Kerberos Client, see *Configuration Guide for Kerberos Client Products on HP-UX* (5991-7718), at: <http://docs.hp.com/en/internet.html#Kerberos>.