

Upgrading to Kerberos V5 from Kerberos V4

Release: 1.6

Document Edition: 1.0

Last updated: May 22, 2003

Copyright

Copyright © 1985-2007 by the Massachusetts Institute of Technology.

Export of software employing encryption from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Individual source code files are copyright MIT, Cygnus Support, Novell, OpenVision Technologies, Oracle, Red Hat, Sun Microsystems, FundsXpress, and others.

Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

“Commercial use” means use of a name in a product or other for-profit manner. It does NOT prevent a commercial firm from referring to the MIT trademarks in order to convey information (although in doing so, recognition of their trademark status should be given).

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in `kadmin/create`, `kadmin/dbutil`, `kadmin/passwd`, `kadmin/server`, `lib/kadm5`, and portions of `lib/rpc`:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved

WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system.

You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you “AS IS” EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code.

OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

Portions contributed by Matt Crawford <crowdad@fnal.gov> were work performed at Fermi National Accelerator Laboratory, which is operated by Universities Research Association, Inc., under contract DE-AC02-76CHO3000 with the U.S. Department of Energy.

Portions of `src/lib/crypto` have the following copyright:

Copyright © 1998 by the FundsXpress, INC.

All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of FundsXpress. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. FundsXpress makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The implementation of the Yarrow pseudo-random number generator in `src/lib/crypto/yarrow` has the following copyright:

Copyright 2000 by Zero-Knowledge Systems, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Zero-Knowledge Systems, Inc. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Zero-Knowledge Systems, Inc. makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

ZERO-KNOWLEDGE SYSTEMS, INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL ZERO-KNOWLEDGE SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE,

DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTUOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The implementation of the AES encryption algorithm in `src/lib/crypto/aes` has the following copyright:

Copyright © 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK.
All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of any properties, including, but not limited to, correctness and fitness for purpose.

Portions contributed by Red Hat, including the pre-authentication plug-in framework, contain the following copyright:

Copyright © 2006 Red Hat, Inc.
Portions copyright © 2006 Massachusetts Institute of Technology
All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Red Hat, Inc., nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The implementations of GSSAPI mechglue in GSSAPI-SPNEGO in `src/lib/gssapi`, including the following files:

```
lib/gssapi/generic/gssapi_err_generic.et
lib/gssapi/mechglue/g_accept_sec_context.c
lib/gssapi/mechglue/g_acquire_cred.c
lib/gssapi/mechglue/g_canon_name.c
lib/gssapi/mechglue/g_compare_name.c
lib/gssapi/mechglue/g_context_time.c
lib/gssapi/mechglue/g_delete_sec_context.c
lib/gssapi/mechglue/g_dsp_name.c
lib/gssapi/mechglue/g_dsp_status.c
lib/gssapi/mechglue/g_dup_name.c
lib/gssapi/mechglue/g_exp_sec_context.c
lib/gssapi/mechglue/g_export_name.c
lib/gssapi/mechglue/g_glue.c
lib/gssapi/mechglue/g_imp_name.c
lib/gssapi/mechglue/g_imp_sec_context.c
lib/gssapi/mechglue/g_init_sec_context.c
lib/gssapi/mechglue/g_initialize.c
lib/gssapi/mechglue/g_inquire_context.c
lib/gssapi/mechglue/g_inquire_cred.c
lib/gssapi/mechglue/g_inquire_names.c
lib/gssapi/mechglue/g_process_context.c
lib/gssapi/mechglue/g_rel_buffer.c
lib/gssapi/mechglue/g_rel_cred.c
lib/gssapi/mechglue/g_rel_name.c
lib/gssapi/mechglue/g_rel_oid_set.c
lib/gssapi/mechglue/g_seal.c
lib/gssapi/mechglue/g_sign.c
lib/gssapi/mechglue/g_store_cred.c
lib/gssapi/mechglue/g_unseal.c
lib/gssapi/mechglue/g_userok.c
lib/gssapi/mechglue/g_utils.c
lib/gssapi/mechglue/g_verify.c
lib/gssapi/mechglue/gssd_pname_to_uid.c
lib/gssapi/mechglue/mglueP.h
lib/gssapi/mechglue/oid_ops.c
lib/gssapi/spnego/gssapiP_spnego.h
lib/gssapi/spnego/spnego_mech.c
```

are subject to the following license:

Copyright © 2004 Sun Microsystems, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Kerberos V5 includes documentation and software developed at the University of California at Berkeley, which includes this copyright notice:

Copyright © 1983 Regents of the University of California.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions contributed by Novell, Inc., including the LDAP database backend, are subject to the following license:

Copyright (c) 2004-2005, Novell, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The copyright holder's name is not used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Permission is granted to make and distribute verbatim copies of this manual provided the copyright notices and this permission notice are preserved on all copies.

Permission is granted to copy and distribute modified versions of this manual under the conditions for verbatim copying, provided also that the entire resulting derived work is distributed under the terms of a permission notice identical to this one.

Permission is granted to copy and distribute translations of this manual into another language, under the above conditions for modified versions.

1 Introduction

As with most software upgrades, Kerberos V5 is generally backward compatible but not necessarily forward compatible. The Kerberos V5 daemons can interoperate with Kerberos V4 clients, but most of the Kerberos V4 daemons can not interoperate with Kerberos V5 clients. This suggests the following strategy for performing the upgrade:

1. **Upgrade your KDCs.** This must be done first, so that interactions with the Kerberos database, whether by Kerberos V5 clients or by Kerberos V4 clients, will succeed.
2. **Upgrade your servers.** This must be done before upgrading client machines, so that the servers are able to respond to both Kerberos V5 and Kerberos V4 queries.
3. **Upgrade your client machines.** Do this only after your KDCs and application servers are upgraded, so that all of your Kerberos V5 clients will be talking to Kerberos V5 daemons.

2 Configuration Files

The Kerberos `krb5.conf` and KDC `kdc.conf` configuration files allow additional tags for Kerberos V4 compatibility.

2.1 `krb5.conf`

If you used the defaults, both when you installed Kerberos V4 and when you installed Kerberos V5, you should not need to include any of these tags. However, some or all of them may be necessary for nonstandard installations.

2.1.1 [libdefaults]

In the [libdefaults] section, the following additional tags may be used:

krb4_srvtab

Specifies the location of the Kerberos V4 `srvtab` file. Default is `/etc/srvtab`.

krb4_config

Specifies the location of the Kerberos V4 configuration file. Default is `/etc/krb.conf`.

krb4_realms

Specifies the location of the Kerberos V4 domain/realm translation file. Default is `/etc/krb.realms`.

2.1.2 [realms]

In the [realms] section, the following Kerberos V4 tags may be used:

default_domain

Identifies the default domain for hosts in this realm. This is needed for translating V4 principal names (which do not contain a domain name) to V5 principal names. The default is your Kerberos realm name, converted to lower case.

v4_instance_convert

This subsection allows the administrator to configure exceptions to the `default_domain` mapping rule. It contains V4 instances (tag name) which should be translated to some specific hostname (tag value) as the second component in a Kerberos V5 principal name.

v4_realm

This relation allows the administrator to configure a different realm name to be used when converting V5 principals to V4 ones. This should only be used when running separate V4 and V5 realms, with some external means of password synchronization between the realms.

2.1.3 AFS and the Appdefaults Section

Many Kerberos 4 sites also run the Andrew File System (AFS).

Modern AFS servers (OpenAFS > 1.2.8) support the AFS 2b token format. This allows AFS to use Kerberos 5 tickets rather than version 4 tickets, enabling cross-realm authentication. By default, the 'krb524d' service will issue the new AFS 2b tokens. If you are using old

AFS servers, you will need to disable these new tokens. Please see the documentation of the `appdefaults` section of `'krb5.conf'` in the Kerberos Administration guide.

2.2 kdc.conf

Because Kerberos V4 requires a different type of salt for the encryption type, you will need to change the `supported_encytypes` line in the `[realms]` section to:

```
supported_encytypes = des-cbc-crc:normal des-cbc-crc:v4
```

This is the only change needed to the `kdc.conf` file.

3 Upgrading KDCs

To convert your KDCs from Kerberos V4 to Kerberos V5, do the following:

1. Install Kerberos V5 on each KDC, according to the instructions in the Kerberos V5 Installation Guide, up to the point where it tells you to create the database.
2. Find the `kadmind` (V4) daemon process on the master KDC and kill it. This will prevent changes to the Kerberos database while you convert the database to the new Kerberos V5 format.
3. Create a dump of the V4 database in the directory where your V5 database will reside by issuing the command:

```
% kdb_util dump /usr/local/var/krb5kdc/v4-dump
```

4. Load the V4 dump into a Kerberos V5 database, by issuing the command:

```
% kdb5_util load_v4 v4-dump
```

5. Create a Kerberos V5 stash file, if desired, by issuing the command:

```
% kdb5_util stash
```

6. Proceed with the rest of the Kerberos V5 installation as described in the Kerberos V5 Installation Guide. When you get to the section that tells you to start the `krb5kdc` and `kadmind` daemons, first find and kill the Kerberos V4 `kerberos` daemon on each of the KDCs. Then start the `krb5kdc` and `kadmind` daemons as You will need to specify an argument to the `-4` command line option to enable Kerberos 4 compatibility. See the `krb5kdc` man page for details. directed. Finally, start the Kerberos V5 to V4 ticket translator daemon, `krb524d`, by issuing the command:

```
% /usr/local/sbin/krb524d -m > /dev/null &
```

If you have a stash file and you start the `krb5kdc` and `kadmind` daemons at boot time, you should add the above line to your `/etc/rc` (or `/etc/rc.local`) file on each KDC.

4 Upgrading Application Servers

Install Kerberos V5 on each application server, according to the instructions in the Kerberos V5 Installation Guide, with the following exceptions:

- In the file `/etc/services`, add or edit the lines described in the Kerberos V5 Installation Guide, with the following exception:

in place of:

```
kerberos      88/udp      kdc      # Kerberos V5 KDC
kerberos      88/tcp      kdc      # Kerberos V5 KDC
```

add instead:

```
kerberos-sec  88/udp      kdc      # Kerberos V5 KDC
kerberos-sec  88/tcp      kdc      # Kerberos V5 KDC
```

- Convert your Kerberos V4 `srvtab` file to Kerberos V5 `keytab` file as follows:

```
# /usr/local/sbin/ktutil
ktutil: rst /etc/krb-srvtab
ktutil: wkt /etc/krb5.keytab
ktutil: q
#
```

5 Upgrading Client machines

Install Kerberos V5 on each client machine, according to the instructions in the Kerberos V5 Installation Guide.

Tell your users to add the appropriate directory to their paths. On UNIX machines, this will probably be `/usr/local/bin`.

Note that if you upgrade your client machines before all of your application servers are upgraded, your users will need to use the Kerberos V4 programs to connect to application servers that are still running Kerberos V4. (The one exception is the UNIX version of Kerberos V5 telnet, which can connect to a Kerberos V4 and Kerberos V5 application servers.) Users can use either the Kerberos V4 or Kerberos V5 programs to connect to Kerberos V5 servers.

6 Firewall Considerations

Kerberos V5 uses port 88, which is the port assigned by the IETF, for KDC requests. Kerberos V4 used port 750. If your users will need to get to any KDCs outside your firewall, you will need to allow TCP and UDP requests on port 88 for your users to get to off-site Kerberos V5 KDCs, and on port 750 for your users to get to off-site Kerberos V4 KDCs.

Table of Contents

Copyright	1
1 Introduction.....	7
2 Configuration Files	8
2.1 krb5.conf	8
2.1.1 [libdefaults]	8
2.1.2 [realms]	8
2.1.3 AFS and the Appdefaults Section	8
2.2 kdc.conf	9
3 Upgrading KDCs	10
4 Upgrading Application Servers	11
5 Upgrading Client machines	12
6 Firewall Considerations	13