Upgrading to Kerberos V5 from Kerberos V4

Release: 1.1
Document Edition: 1.0
Last updated: October 8, 1996

MIT

Copyright © 1985-1999 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.

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.

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. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.
4. 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.

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 is 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.

2.2 kdc.conf

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

```
supported_enctypes = 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 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
  ```

- In the file `/etc/inetd.conf`, for a *secure* server, instead of making the changes described in the Kerberos V5 Installation Guide, do the following:

  Find and comment out any lines for the services `ftp`, `telnet`, `shell`, `login`, and `exec`.
  Add the following lines. (Note: each line beginning with ⇒ is a continuation of the previous line.)

  ```
  klogin  stream  tcp  nowait  root
  ⇒    /usr/local/sbin/klogind  klogind -k -c
  eklogin stream  tcp  nowait  root
  n⇒   /usr/local/sbin/klogind  klogind -k -c -e
  kshell  stream  tcp  nowait  root
  ⇒    /usr/local/sbin/kshd  kshd -k -c -A
  ftp     stream  tcp  nowait  root
  ⇒    /usr/local/sbin/ftpd  ftpd -a
  telnet  stream  tcp  nowait  root
  ⇒    /usr/local/sbin/telnetd  telnetd -a valid
  ```

  N.B.: As noted in the Kerberos V5 Installation Guide, if you have some clients running older versions of Kerberos V5 (beta 6 or earlier), checksums were done differently in those versions, which will cause authentication to fail. To get around this problem, have the `klogind` and `kshd` daemons ignore checksums, by replacing each `-c` flag above with `-i`.

  For an *insecure* server, make the changes described in the Kerberos V5 Installation Guide.

  When you make changes to `inetd.conf`, remember to `kill -HUP` the `inetd` process to cause the changes to take effect.

- 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