

Kerberos Version 1.0 for OpenVMS Security Client

Installation Guide and Release Notes

Kerberos Version 1.0 for OpenVMS Security Client, based on MIT Kerberos V5 Release 1.0.5

Contents:

Prerequisites
Documentation
Configuration
Sample Configuration
Release Notes

Kerberos Version 1.0 for OpenVMS Security Client, based on MIT Kerberos V5 Release 1.0.5, is now integrated into OpenVMS Alpha Version 7.3-1.

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

Kerberos was created by the Massachusetts Institute of Technology as a solution for network security. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity.

Kerberos is freely available from MIT, under a copyright permission notice. Kerberos for OpenVMS is supplied by Compaq Computer Corporation under the terms of the license from the Massachusetts Institute of Technology. For more information on the Kerberos license, please see <http://web.mit.edu/kerberos/www/>.

Prerequisites

Compaq Computer Corporation supports the following configuration:

TCP/IP Transport

Compaq TCP/IP Services for OpenVMS Version 5.0 or higher.

Compaq supports Compaq TCP/IP Services for OpenVMS, and is actively working with third-party TCP/IP vendors to test Kerberos on other TCP/IP implementations.

Documentation

The Kerberos for OpenVMS Installation Guide and Release Notes (this document) contain OpenVMS-specific information about configuration, release notes, and known problems.

General information about Kerberos is available at <http://web.mit.edu/kerberos/www/>.

The following Kerberos documentation is available from this website. This documentation is included in the MIT distribution and is not specific to OpenVMS.

- *Kerberos V5 Installation Guide*
(HTML PDF)
- *Kerberos V5 User's Guide*
(HTML PDF)
- *Kerberos V5 System Administrator's Gui*
(HTML PDF)
- *Upgrading to Kerberos V5 from Kerberos V4*
(HTML PDF)

Configuration

To configure Kerberos, perform the following steps from a privileged OpenVMS username (for example, SYSTEM).

1. Insert the following line into SYS\$MANAGER:SYSTARTUP_VMS.COM. This line must be entered **after** the startup command for Compaq TCP/IP Services for OpenVMS. (If you start Compaq TCP/IP Services for OpenVMS as a batch job, be sure that TCP/IP has started before you start Kerberos.)

```
$ @SYS$STARTUP:KRB$STARTUP.COM
```

2. Add the following line to your SYLOGIN command procedure, or into the LOGIN.COM of each user who will use Kerberos.

```
$ @SYS$MANAGER:KRB$SYMBOLS
```

3. Run the following command procedure to configure the Kerberos clients and servers.

```
$ @SYS$STARTUP:KRB$CONFIGURE.COM
```

4. Read the *Kerberos V5 Installation Guide* for additional setup and configuration information.

Sample Configuration on an Alpha System

```
$ @SYS$STARTUP:KRB$CONFIGURE.COM

Kerberos V1.0 for OpenVMS Configuration Menu

Configuration options:

    1 - Setup Client configuration
    2 - Edit Client configuration

    3 - Setup Server configuration
    4 - Edit Server configuration

    5 - Shutdown Servers
    6 - Startup Servers

    E - Exit configuration procedure

Enter Option: 1
```

Where will the OpenVMS Kerberos 5 V1.0 KDC be running [<node>]: <CR>
What is the OpenVMS Kerberos 5 V1.0 default domain [<domain>]: <CR>
What is the OpenVMS Kerberos 5 V1.0 Realm name [<realm>]: <CR>

Press Return to continue ...

Kerberos V1.0 for OpenVMS Configuration Menu

Configuration options:

- 1 - Setup Client configuration
- 2 - Edit Client configuration

- 3 - Setup Server configuration
- 4 - Edit Server configuration

- 5 - Shutdown Servers
- 6 - Startup Servers

- E - Exit configuration procedure

Enter Option: 3

Where will the OpenVMS Kerberos 5 V1.0 KDC be running [<node>]: <CR>
What is the OpenVMS Kerberos 5 V1.0 default domain [<realm>]: <CR>
What is the OpenVMS Kerberos 5 V1.0 Realm name [<realm>]: <CR>

The type of roles the KDC can perform are:

- NO_KDC -- where the KDC will not be run
- SINGLE_KDC -- where the KDC is the only one in the realm
- MASTER_KDC -- where the KDC is the master of 1 or more other KDCs
- SLAVE_KDC -- where the KDC is slave to another KDC

What will be the KDC's role on this node [NO_KDC]: MASTER

Create the OpenVMS Kerberos 5 V1.0 database [Y]: <CR>

Creating OpenVMS Kerberos 5 V1.0 database ...

Initializing database 'krb\$root:[krb5kdc]principal' for realm '<realm>',
master key name 'K/M@<realm>'

You will be prompted for the database Master Password.

It is important that you NOT FORGET this password.

Enter KDC database master key: <MASTER_KEY>

Re-enter KDC database master key to verify: <MASTER_KEY>

Priority: info

No dictionary file specified, continuing without one.

Please enter a default OpenVMS Kerberos 5 V1.0 administrator [SYSTEM]: <CR>

Enter password for principal "SYSTEM/admin@<realm>": <PASSWORD>

Re-enter password for principal "SYSTEM/admin@<realm>": <PASSWORD>

Principal "SYSTEM/admin@<realm>" created.

Priority: info

No dictionary file specified, continuing without one.

Create OpenVMS Kerberos 5 V1.0 principals [Y]: NO

Priority: info

No dictionary file specified, continuing without one.

Entry for principal kadmin/admin with kvno 3, encryption type

DES-CBC-CRC added to keytab WRFILE=KRB\$ROOT:[KRB5KDC]KADM5.KEYTAB.

Priority: info

No dictionary file specified, continuing without one.

```
Entry for principal kadmin/changepw with kvno 3, encryption type
DES-CBC-CRC added to keytab WRFILE=KRB$ROOT:[KRB5KDC]KADM5.KEYTAB.
```

```
Press Return to continue ...
```

```
Kerberos V1.0 for OpenVMS Configuration Menu
```

```
Configuration options:
```

- 1 - Setup Client configuration
- 2 - Edit Client configuration

- 3 - Setup Server configuration
- 4 - Edit Server configuration

- 5 - Shutdown Servers
- 6 - Startup Servers

- E - Exit configuration procedure

```
Enter Option: 6
```

```
Starting OpenVMS Kerberos 5 V1.0 Servers (Role: MASTER_KDC)...
```

```
Starting OpenVMS Kerberos 5 V1.0 server KRB$KRB5KDC ...
%RUN-S-PROC_ID, identification of created process is 0000023B
Starting OpenVMS Kerberos 5 V1.0 server KRB$KADMIND ...
%RUN-S-PROC_ID, identification of created process is 0000023D
```

```
Press Return to continue ...
```

```
Kerberos V1.0 for OpenVMS Configuration Menu
```

```
Configuration options:
```

- 1 - Setup Client configuration
- 2 - Edit Client configuration

- 3 - Setup Server configuration
- 4 - Edit Server configuration

- 5 - Shutdown Servers
- 6 - Startup Servers

- E - Exit configuration procedure

```
Enter Option: e
```

```
$
```

Release Notes

- **Remove Kerberos V1.0 layered product before upgrading**

If you have the layered product kit of Kerberos Version 1.0 for OpenVMS Alpha installed, you must use the PCSI utility to remove it before you upgrade the OpenVMS operating system to V7.3-1. Kerberos is integrated into OpenVMS in Version 7.3-1.

To remove Kerberos, select **Remove installed products** at the main menu. During the removal, you are asked if you want to remove the data and directories. (Data refers to the configuration data files along with the principal database, if one was created.) If you want to save this information for use later, respond "No" to the question. Return to the main menu and perform the upgrade of OpenVMS.

After the upgrade, the new Kerberos directories are located under SYSEXE in KERBEROS.DIR. New Kerberos data is either created during configuration or copied from the old Kerberos directories. If you removed a previously installed Kerberos PCSI kit and saved the data and directories, you can copy that data into the new directories. To do this, enter the following commands from the SYSTEM account:

```
$ @sys$manager:krb$logicals.com
$ rename/log sys$common:[sysexec.etc]*.* krb$root:[etc]*.*;
$ rename/log sys$common:[sysexec.bin]*.dat krb$root:[bin]*.*;
$ rename/log sys$common:[sysexec.krb5kdc]*.*
krb$root:[krb5kdc]*.*;
```

To optionally save the log files, enter the following:

```
$ rename/log sys$common:[sysexec.log]*.* krb$root:[log]*.*;
```

Start the Kerberos servers by entering the following command:

```
$ @sys$startup:krb$startup.com
```

- **Kerberos is not cluster-aware**

Kerberos for OpenVMS is not cluster-aware. Kerberos tickets are encoded with the originating node name as a security feature. A ticket-granting ticket (TGT), obtained from one node in a cluster, is valid only on the node from which the request was made. Further requests for tickets must originate from the same node where the ticket-granting-ticket request originated.

Although the ticket cache is visible from other nodes in the cluster, the Kerberos KDC does not allow nodes other than the node encoded in the ticket to use the TGT.

- **Kerberos and lowercase user names**

When Kerberos obtains a user name from the system's user authorization file (UAF), by default it does not modify the case of the user name. OpenVMS user names are in uppercase.

To accommodate the use of lowercase user names (UNIX user names are usually lowercase), you can define the logical `KRB$LOWERCASE_UAF_USERNAME`. This logical causes a user name retrieved from the UAF file to be lowercased. If you do not define this logical, the case of the user name remains unchanged.

- **Kerberos command lines entered are changed to upper case**

When you enter commands at the Kerberos prompt, the commands you enter are changed to uppercase unless they are enclosed in quotation marks. For portions of the

command that contain lowercase letters like principal names and passwords, be sure to use quotation marks. This does not apply to password prompting.

In the following example, foobar was changed to uppercase because it was not enclosed in quotation marks.

```
Kerberos> modify password foobar /password="passfoobar"  
Password for "FOOBAR@REALM" changed.  
Kerberos> modify password foobar  
Enter password for principal "FOOBAR": foobarpass  
Re-enter password for principal "FOOBAR": foobarpass  
change_password: password for "FOOBAR@REALM" changed.  
Kerberos> exit  
$
```

- **Kerberos KDC Propagation Daemon on OpenVMS fails on slave KDC systems on OpenVMS**

The Kerberos KDC Propagation Daemon on OpenVMS unexpectedly fails on slave KDC systems on OpenVMS, causing scheduled KDC propagation to not update the slave's KDC database.

Workaround: Set up the propagation daemon as a TCP/IP service. As such, the daemon will run only when an update request is made to the slave KDC system from the master. The daemon will execute and then exit. To set up the service, the following commands may be used either manually or saved and executed as a .COM file. This setup procedure need only be done once.

```
$!  
$! Sets up Kerberos5 propagation daemon as TCP/IP service  
$!  
$ tcpip set service krb5_prop -  
    /file=krb$root:[bin]krb$krbpropd.com -  
    /port=754 -  
    /user=SYSTEM -  
    /process_name=KRB$KPROP -  
    /log_options=(file=sys$manager:krb$krbprop.log,all)  
$!  
$ tcpip enable service krb5_prop  
$!  
$ tcpip show service/full krb5_prop  
$!  
$ exit
```

- **Problem obtaining a ticket granting ticket**

A problem exists where you cannot obtain a ticket granting ticket from a Tru64 Unix (Digital UNIX V4.0F (Rev. 1229)) system running an MIT Kerberos5 1.1.x KDC. If this problem occurs, you receive the following error:

```
"KINIT: Cannot contact any KDC for requested realm while getting  
initial credentials"
```

The KDC appears to be active and running on the Tru64 system.

Analysis: This is not a problem with the Kerberos Client on OpenVMS, and will appear on any system that attempts to access this particular KDC. If the KDC is installed on the Tru64 Unix system (as outlined in the *Kerberos Installation Guide*) so that it starts at system boot time by making entries in the file `inittab`, this problem results. At system startup, the KDC loops, appearing as though it is active and ready to service requests. The reason for this behavior is unknown.

Workaround: The KDC must be started manually. First, if the KDC process is running and is looping, kill the process. Then issue the command `/usr/local/sbin/krb5kdc` from a terminal window or command line prompt to manually start the KDC. The KDC will then start properly and begin servicing requests.

- **UNIX to OpenVMS file naming differences**

The Kerberos documentation is written for a UNIX audience. When reading the Kerberos documentation, note the following differences between UNIX and OpenVMS:

- File specification format

The following example shows the differences in the file specification format of a lock file. In this example, the UNIX file specification `/usr/local/var/krb5kdc/principal.kadm5.lock` is equivalent to `KRB$ROOT: [KRB5KDC] PRINCIPAL_KADM5_LOCK. ;1` on OpenVMS.

- Configuration file format

The following examples show the differences in format of two configuration files, `krb5.conf` and `kdc.conf`.

The `krb5.conf` file on a UNIX system is as follows:

```
[libdefaults]
    ticket_lifetime = 600
    default_realm = ATHENA.MIT.EDU

default_tkt_enctypes = des-cbc-crc
default_tgs_enctypes = des-cbc-crc

[realms]
    ATHENA.MIT.EDU = {
        kdc = kerberos.mit.edu:88
        kdc = kerberos-1.mit.edu:88
        kdc = kerberos-2.mit.edu:88
        admin_server = kerberos.mit.edu:749
        default_domain = mit.edu
    }

[domain_realm]
    .mit.edu = ATHENA.MIT.EDU
    mit.edu = ATHENA.MIT.EDU

[logging]
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmin.log
    default = FILE:/var/log/krb
5lib.log
```

The `krb5.conf` file on an OpenVMS system is as follows:

```
[libdefaults]
    default_realm = NODE32.DEC.COM
    default_tgs_enctypes = des-cbc-crc
    default_tkt_enctypes = des-cbc-crc

[realms]
    NODE32.DEC.COM = {
        kdc = node32.zko.dec.com:88
        admin_server = node32.zko.dec.com:749
        default_domain = zko.dec.com
    }

[domain_realm]
    .zko.dec.com = NODE32.DEC.COM
    zko.dec.com = NODE32.DEC.COM

[logging]
    kdc = FILE=krb$root:[log]krb$krb5kdc.log
    admin_server = FILE=krb$root:[log]krb$kadmind.log
    default = FILE=krb$root:[log]krb5lib.log
```

The `kdc.conf` file on a UNIX system is as follows:

```
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    ATHENA.MIT.EDU = {
        database_name = /usr/local/var/krb5kdc/principal
        admin_keytab = /usr/local/var/krb5kdc/kadm5.keytab
        acl_file = /usr/local/var/krb5kdc/kadm5.acl
        dict_file = /usr/local/var/krb5kdc/kadm5.dict

        key_stash_file = /usr/local/var/krb5kdc/.k5.ATHENA.MIT.EDU
        kadmind_port = 749
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = des-cbc-crc
        supported_enctypes = des-cbc-crc:normal
    }
}
```

The `krb5.conf` file on an OpenVMS system is as follows:

```
[kdcdefaults]
    kdc_ports = 750,88
    clockskew = 5000

[realms]
    NODE32.DEC.COM = {
        database_name = krb$root:[krb5kdc]principal
        ad
min_keytab = krb$root:[krb5kdc]kadm5.keytab
        acl_file = krb$root:[krb5kdc]kadm5.acl
        key_stash_file = krb$root:[krb5kdc]_k5_NODE32_DEC_COM
        kdc_ports = 750,88
        max_life = 10h 0m 0s
```

```
max_renewable_life = 7d 0h 0m 0s
master_key_type = des-cbc-crc
supported_enctypes = des-cbc-crc:normal des:normal
                    des:v4 des:norealm des:onlyrealm
des:afs3
}
```
