z/OS

IBM
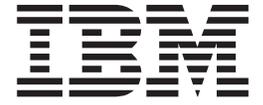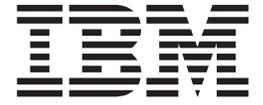
Security Server
Network Authentication Service
Administration

z/OS

Security Server
Network Authentication Service
Administration

Fourth Edition, February 2003

This edition applies to Version 1 Release 4 of z/OS (5694-A01), to Version 1, Release 4 of z/OS.e (5655-G52), and to all subsequent releases of this product until otherwise indicated in new editions.

IBM® welcomes your comments. A form for readers' comments may be provided at the back of this document, or you may address your comments to the following address:

    International Business Machines Corporation
    Department 55JA, Mail Station P384
    2455 South Road
    Poughkeepsie, NY 12601-5400
    United States of America

    FAX (United States & Canada): 1+845+432-9405
    FAX (Other Countries):
        Your International Access Code +1+845+432-9405

    IBMLink™ (United States customers only): IBMUSM10(MHVRCFS)
    Internet e-mail: mhvrcfs@us.ibm.com
    World Wide Web: http://www.ibm.com/servers/eserver/zseries/zos/webqs.html

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:
- Title and order number of this document
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Tables

Figures

ix

About this document

This publication describes how to configure and administer z/OS™ Security Server Network Authentication Service. It supports both z/OS (5694-A01) and z/OS.e (5655-G52).

Who should use this document

This document is for someone installing the product who has system programmer skills and for system administrators.

How this document is organized

This document is divided into two parts. Part 1 is the Guide; it provides overview and how-to information. Part 2 is the Reference; it contains information that you might need to look up.

The chapters in Part 1 are:
- Chapter 1, "Introducing Network Authentication Service", on page 3 - this chapter gives an overview for z/OS Security Server Network Authentication Service.
- Chapter 2, "Configuring Network Authentication Service", on page 9 - this chapter tells how to perform the tasks you do after installing the product but before using it.
- Chapter 3, "Administering Network Authentication Service", on page 31 - this chapter provides background information for the administrator plus the few operator commands you need.

The chapters in Part 2 are:
- Chapter 4, "Commands", on page 47
- Chapter 5, "Status codes", on page 69
- Chapter 6, "Messages", on page 99.

Where to find more information

Where necessary, this document refers to information in other documents. For complete titles and order numbers for all elements of z/OS, see *z/OS: Information Roadmap*, SA22-7500.

The companion publication for this document is *z/OS: Security Server Network Authentication Service Programming*, which describes application programming interfaces for the product. The "Bibliography" on page 149 lists selected publications of z/OS Security Server.

Softcopy publications

The z/OS Security Server Network Authentication Service library is available on a CD-ROM, *z/OS Collection*, SK3T-4269. The CD-ROM online library collection is a set of unlicensed documents for z/OS and related products that includes the IBM Library Reader™. This is a program that enables you to view the BookManager® files. This CD-ROM also contains the Portable Document Format (PDF) files. You can view or print these files with the Adobe Acrobat Reader.

Internet sources

z/OS online library

> The softcopy z/OS publications are also available for web browsing, and PDF versions for viewing or printing using the following URL:
>
> `http://www.ibm.com/servers/eserver/zseries/zos/bkserv/`

You can also provide comments about this document and any other z/OS documentation by visiting that URL. Your feedback is important in helping to provide the most accurate and high-quality information.

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most of the z/OS, z/VM, and VSE messages you encounter, as well as system abends, and some codes. Using LookAt to find information is faster than a conventional search, because, in most cases, LookAt goes directly to the message explanation.

You can use LookAt from the Internet at:

```
http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookat.html
```

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX Systems Services running OMVS).

You can also download code from the *z/OS Collection*, SK3T-4269, or from the LookAt Web site so you can access LookAt from a PalmPilot (Palm VIIx suggested).

To use LookAt on the Internet to find a message explanation, go to the LookAt Web site and simply enter the message identifier (for example, **$HASP701** or **$HASP***). You can select a specific release to narrow your search.

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection*, SK3T-4269, or from the LookAt Web site. To obtain the code from the LookAt Web site, do the following:

1. Go to http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookat.html.
2. Click **News**.
3. Scroll to **Download LookAt Code for TSO/E and z/VM**.
4. Click the **ftp** link, which takes you to a list of operating systems. Click the appropriate operating system. Then click the appropriate release.
5. Open the **lookat.me** file and follow its detailed instructions.

After you have LookAt installed, you can access a message explanation from a TSO/E command line by entering: **lookat** *message-id*. LookAt displays the message explanation for the message requested.To find a message explanation from a TSO command line, simply enter: **lookat** *message-id*. LookAt displays the message explanation for the message requested.

Note: Some messages have information in more than one document. For example, IEC192I has routing and descriptor codes listed in *z/OS MVS System Messages, Vol 7 (IEB-IEE)* and *z/OS: MVS Routing and Descriptor Codes*. For such messages, LookAt displays a list of documents in which the message appears. You can then click the message identifier under each document title to view information about the message.

Accessing licensed documents on the Internet

z/OS licensed documentation is available on the Internet in BookManager and PDF format at the IBM Resource Link™ Web site at:

```
http://www.ibm.com/servers/resourcelink
```

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID, and password, and akey code. With your z/OS order you received a Memo to Licensees, GI10-0671, that includes this key code.

To obtain your IBM Resource Link user ID and password, log on to:

`http://www.ibm.com/servers/resourcelink`

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password
2. Select **User Profiles** located on the left-hand navigation bar
3. Click **Request Access to z/OS Licensed Books**
4. Supply the key code where requested and click **Submit**.

If you supplied the correct key code, you will receive confirmation that your request is being processed. After your request is processed, you will receive an e-mail confirmation.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

To access the licensed documents:

1. Sig in to Resource Link using your Resource Link user ID and password
2. Select **Library** located on the left-hand navigation bar.
3. Click **zSeries**.
4. Click **Software**.
5. Click the release of **z/OS**.
6. Click **Licensed publications**.

Printed licensed documents are not available from IBM.

You can use the PDF format on either *z/OS Licensed Product Library CD-ROM* or IBM Resource Link to print licensed documents.

Conventions used in this document

This document uses the following typographic conventions:

Table 1. Typographic conventions

Boldface	Indicates the name of: • The item you need to select • A field, option, parameter, or command • A new term
Italic	Indicates document titles or variable information that must be replaced by an actual value.
Monofont	Indicates: • Names of directories, files, and user IDs • Information displayed by the system • An example • A portion of a file or sample code • A previously entered value.
Bold Monofont	Indicates information that you type into the system exactly as it appears in this document.
[ ]	Brackets enclose optional items in format and syntax descriptions.
{ }	Braces enclose a list of required items, in format and syntax descriptions, from which you must select one.
		A vertical bar separates items in a list of choices.

Table 1. Typographic conventions (continued)

< >	Angle brackets enclose the name of a key on the keyboard.
. . .	Horizontal ellipsis points indicate that you can repeat the preceding item one or more times.
\	A backslash is used as a continuation character when entering commands from the shell that exceed one line (255 characters). If the command exceeds one line, use the backslash character as the last nonblank character on the line to be continued, and continue the command on the next line.

Sending your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this document, send your comments by using Resource Link at http://www.ibm.com/servers/resourcelink. Select **Feedback** on the Navigation bar on the left. Besure to include the name of the document, the form number of the document, the version of the document, if applicable, and the specific location of the text you are commenting on (for example, a page number or table number).

Summary of Changes

Summary of changes
for SC24-5926-03
z/OS Version 1 Release 4

The document contains information previously presented in SC24-5926-02, which supports z/OS Version 1 Release 4.

Summary of changes
for SC24-5926-02
z/OS Version 1 Release 4

The document contains information previously presented in SC24-5926-01, which supports z/OS Version 1 Release 2.

New information
These items are new for this release:

- Support for IPv6, a new addressing format for the Internet.
- Support for MIT Kerberos's New Database Manager (NDBM), for use with the Hierarchical File System (HFS):
  - The **kadmin** command has been modified for use with NDBM.
  - NDBM allows other platform KDCs to act as part of the z/OS realm. Database propagation to these other platforms is supported for Kerberos V5R1.2.2 and later, and a compatibility mode is provided for Kerberos V5R1.2.1 and earlier.
  - There are new messages and codes to support the NDBM implementation.
- Information has been added to indicate that this document supports z/OS.e.
- An appendix with z/OS product accessibility information has been added.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Starting with z/OS V1R2, you may notice changes in the style and structure of some content in this document--for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of changes
for SC24-5926-01
z/OS Version 1 Release 2

The document contains information previously presented in SC24-5926-00, which supports z/OS Version 1 Release 1.

New information
These items are new for this release:

- Three new commands:
  - **kadmin** - This command allows you to manage the Kerberos database on platforms other than z/OS.
  - **kpasswd** - This command allows you to change the password for a Kerberos principal.
  - **kvno** - This command displays the current key version number for a principal.
- Support for message logging through the **syslog** daemon.

- Hardware cryptographic support for Data Encryption Standard (DES) and Triple DES (DES3).
- A new Function Modification Identifier (FMID) that controls DES3 encryption for customer data (required by the US Government to comply with export regulations).
- New status codes and messages.

Changed information

- Modifications throughout the documentation in support of the new function listed above.

Deleted information

- Messages EUVF04022 through EUVF04027 were deleted.

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Part 1. Guide

This part of the document contains information on:

- Introducing Network Authentication Service for z/OS
- Configuring Network Authentication for Service z/OS
- Administering Network Authentication for Service z/OS

Chapter 1. Introducing Network Authentication Service

This chapter provides an introduction to z/OS Security Server Network Authentication Service.

Overview

Security Server Network Authentication Service for z/OS is the IBM z/OS program based on Kerberos™ Version 5. This component of the Security Server for z/OS will be referred to hereafter as "Network Authentication Service for z/OS," "z/OS Network Authentication Service," or "Network Authentication Service."

Network Authentication Service for z/OS provides Kerberos security services without requiring that you purchase or use a middleware product such as Distributed Computing Environment (DCE). These services include native Kerberos application programming interface (API) functions, as well as the Generic Security Service Application Programming Interface (GSS-API) functions defined in Internet RFC 2078, *Generic Security Service Application Program Interface, Version 2* and Internet RFC 2744, *Generic Security Service API Version 2: C-bindings*.

There is a glossary of terms for Network Authentication Service in the "Glossary" on page 147.

Authentication

Network Authentication Service for z/OS performs authentication as a trusted third-party authentication service by using conventional shared secret-key cryptography. Network Authentication Service provides a means of verifying the identities of principals, without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will.

The two methods for obtaining credentials, the initial-ticket exchange and the ticket-granting-ticket exchange, use slightly different protocols and require different API routines.

The basic difference an application programmer sees is that the initial-ticket exchange does not require a ticket-granting-ticket (TGT) but does require the client's secret key. Usually, the initial-ticket exchange is for a TGT, and TGT exchanges are used from then on. In a TGT exchange, the TGT is sent as part of the request for a ticket and the reply is encrypted in the session key obtained from the TGT. Thus, once a user's password is used to obtain the initial TGT, it is not required for subsequent TGT exchanges to obtain additional tickets.

A *ticket-granting ticket* contains the Kerberos server (**krbtgt/realm**) as the server name. A *service ticket* contains the application server as the server name. A ticket-granting ticket is used to obtain service tickets. In order to obtain a service ticket for a server in another realm, the application must first obtain a ticket-granting ticket to the Kerberos server for that realm.

The Kerberos server reply consists of a ticket and a session key, encrypted either in the user's secret key or the TGT session key. The combination of a ticket and a session key is known as a set of *credentials*. An application client can use these credentials to authenticate to the application server by sending the ticket and an *authenticator* to the server. The authenticator is encrypted in the session key of the ticket and contains the name of the client, the name of the server, and the time the authenticator was created.

In order to verify the authentication, the application server decrypts the ticket using its service key, which is known only by the application server and the Kerberos server. Inside the ticket, the Kerberos server has placed the name of the client, the name of the server, a session key associated with the ticket, and some additional information.

Introducing

The application server then uses the ticket session key to decrypt the authenticator and verifies that the information in the authenticator matches the information in the ticket. The server also verifies that the authenticator timestamp is recent to prevent replay attacks (the default is 5 minutes). Since the session key was generated randomly by the Kerberos server and delivered encrypted in the service key and a key known only by the user, the application server can be confident that users really are who they claim to be, by virtue of the fact that the user was able to encrypt the authenticator in the correct key.

To provide detection of both replay attacks and message stream modification attacks, the integrity of all the messages exchanged between principals can also be guaranteed by generating and transmitting a collision-proof checksum of the client's message, keyed with the session key. The privacy and integrity of the messages exchanged between principals can be secured by encrypting the data to be passed using the session key.

Realms

The Kerberos protocol is designed to operate across organizational boundaries. Each organization wishing to run a Kerberos server establishes its own *realm*. The name of the realm in which a client is registered is part of the client's name and can be used by the application server to decide whether to honor a request.

By establishing *inter-realm keys*, the administrators of two realms can allow a client authenticated in one realm to use its credentials in the other realm. The exchange of inter-realm keys registers the ticket-granting service of each realm as a principal in the other realm. A client is then able to obtain a ticket-granting ticket for the remote realm's ticket-granting service from its local ticket-granting service. Tickets issued to a service in the remote realm indicate that the client was authenticated from another realm.

This method can be repeated to authenticate throughout an organization across multiple realms. To build a valid authentication path to a distant realm, the local realm must share an inter-realm key with the target realm or with an intermediate realm that communicates with either the target realm or with another intermediate realm.

Realms are typically organized hierarchically. Each realm shares a key with its parent and a different key with each child. If an inter-realm key is not directly shared by two realms, the hierarchical organization allows an authentication path to be easily constructed. If a hierarchical organization is not used, it may be necessary to consult some database in order to construct an authentication path between realms.

Although realms are typically hierarchical, intermediate realms may be bypassed to achieve cross-realm authentication through alternate authentication paths. It is important for the end-service to know which realms were transited when deciding how much faith to place in the authentication process. To facilitate this decision, a field in each ticket contains the names of the realms that were involved in authenticating the client.

For more information on realms, and specifically realm trust relationships, see Chapter 3, "Administering Network Authentication Service", on page 31.

Registry database types: SAF or NDBM

The Kerberos security server supports two registry database types: SAF (Kerberos principals stored in the System Authorization Facility database) and NDBM (Kerberos principals stored in a Unix System Services database using HFS files). IBM recommends that the SAF registry be used unless it is necessary to share the Kerberos registry with one or more KDC instances running on another operating system.
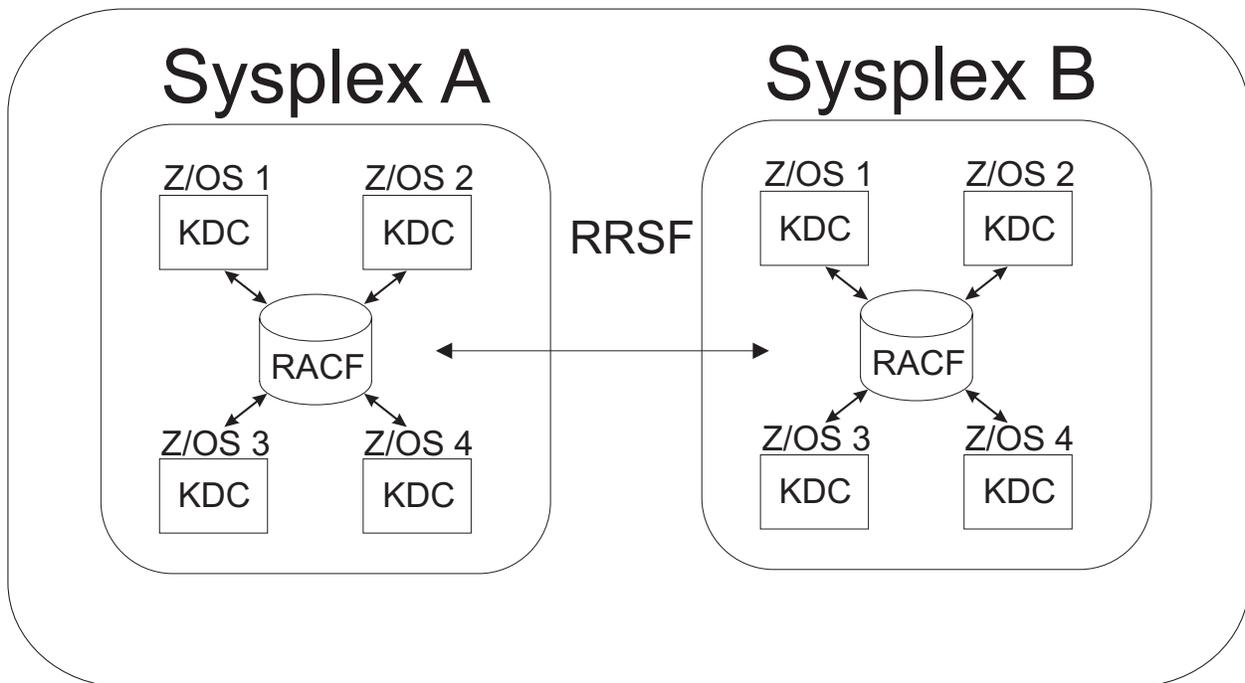
Figure 1. Cross-Sysplex Environment Using SAF Databases

The SAF registry database has these capabilities and requirements:

- Kerberos information is integrated with the z/OS system authorization profiles. All information is managed by SAF and stored in the SAF database. The KDC does not maintain its own registry database.
- The SAF database is shared within the sysplex and can be shared with other z/OS systems by using RACF Remote Sharing Facility (RRSF). Figure 1 shows an example of this environment.
- SAF callable services are provided to map Kerberos principals to system user IDs and to map system user IDs to Kerberos principals.
- Support is provided for using system-authenticated user IDs to eliminate the use of Kerberos passwords and key tables when obtaining and decrypting tickets.
- No Kerberos administration support is provided due to semantic differences between the SAF database and the Kerberos administration wire protocols.
- All KDC instances in the realm must share the same SAF database (homogeneous environment).
- The SAF registry scales to support a large number of principals.

Introducing
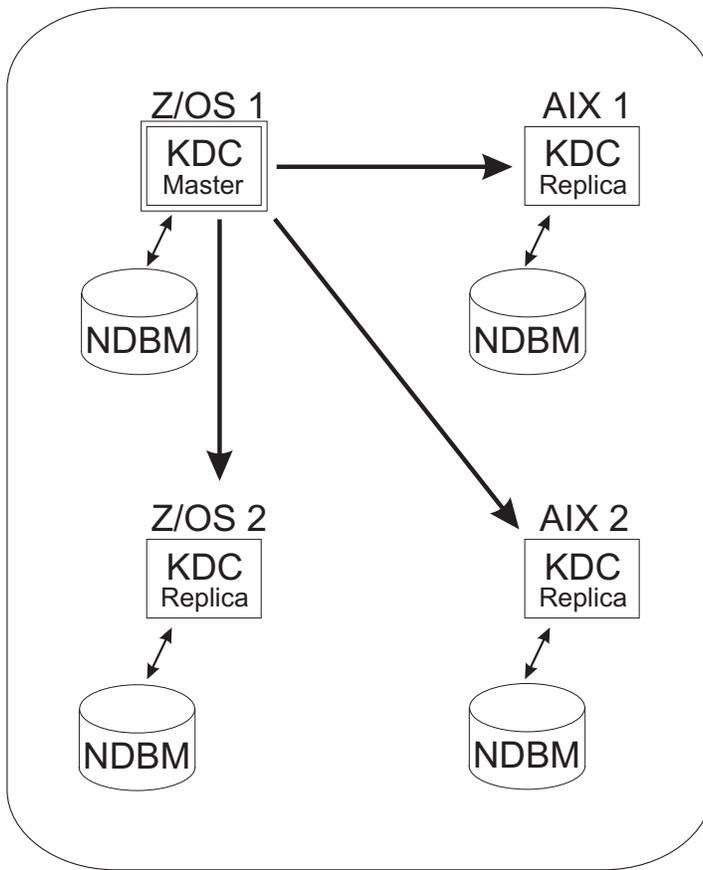
Figure 2. Cross-Platform Environment Using NDBM Databases

The NDBM registry database has these capabilities and requirements:

- The KDC maintains its own registry database using the Unix System Services NDBM support. The database files are located in the **/var/skrb/krb5kdc** directory and must be protected and backed up appropriately.

- The NDBM database is not shared within the sysplex. Each KDC instance must have its own NDBM database files. Database propagation is used to synchronize the database files for each KDC. An example of this environment is shown in Figure 2.

- SAF callable services can be used to map Kerberos principals to system user IDs and to map system user IDs to Kerberos principals. In order to use these services, the Kerberos administrator must define the Kerberos principals in the SAF database as well as in the NDBM database. However, there is no need to synchronize the SAF password for the principal with the NDBM password for the principal since Kerberos always uses the password obtained from the NDBM database.

- System authentication can be used to eliminate the use of Kerberos passwords and key tables when obtaining and decrypting tickets. In order to use these services, the Kerberos administrator must define the Kerberos principals in the SAF database as well as in the NDBM database. However, there is no need to synchronize the SAF password for the principal with the NDBM password for the principal since Kerberos always uses the password obtained from the NDBM database.

- Full Kerberos administration support is provided.

- The realm can contain both z/OS KDC and non-z/OS KDC instances (heterogeneous environment).

- The NDBM registry is limited by the maximum size of an HFS database. In addition, the database propagation protocol is inefficient for a large number of principals unless the update propagation protocol is used.

Encryption types and strong encryption

In Network Authentication Service for z/OS, 56-bit DES encryption is always supported. 168-bit DES3 encryption is available for authentication purposes. However, due to US government export regulations, it may not be available for user data encryption. This means that tickets can be obtained using 168-bit DES3 encryption but the session keys in service tickets may need to be restricted to 56-bit DES encryption (the session key is often used for user data encryption).

The Kerberos security server uses the strongest encryption algorithm available when encrypting a ticket. The SKDC_TKT_ENCTYPES environment variable for the SKRBKDC started task specifies the encryption types to be used for ticket-granting tickets and for service tickets. This is a list of one or more encryption types specified from most-preferred to least-preferred. When generating a ticket, the KDC selects the first entry in this list that has a key available for the server specified in the ticket. Thus, the use of 168-bit DES3 encryption can be controlled on an individual server basis when necessary. For example, if a foreign realm does not support 168-bit DES3 encryption, the **krbtgt/***foreign-realm***@***local-realm* principal entry in the KDC registry database contains just a 56-bit DES key and not a 168-bit DES3 key.

Application programming interfaces

An entire document, *z/OS: Security Server Network Authentication Service Programming*, is devoted to the APIs for Network Authentication Service for z/OS. This document explains how to use the APIs, as well as providing a reference section that describes each API individually.

Chapter 2. Configuring Network Authentication Service

This chapter provides configuration information for Network Authentication Service for z/OS.

Making the program operational

After you have installed z/OS, you must take certain steps to make Network Authentication Service operational. Here are those steps:

1. These steps assume that Resource Access Control Facility (RACF®) is your external security manager. If you have a different but equivalent external security manager, consult the documentation for that product for the corresponding instructions and commands.

   a. Copy the SKRBKDC sample configuration file from **/usr/lpp/skrb/examples/krb5.conf** to **/etc/skrb/krb5.conf**.

      The file permissions should allow everyone to read the file and only the administrator to update it.

   b. Copy the SKRBKDC environment variable definitions from **/usr/lpp/skrb/examples/skrbkdc.envar** to **/etc/skrb/home/kdc/envar**. Modify the SKDC_DATABASE environment variable to select either the SAF or NDBM registry. The SAF registry is used if this environment variable is not set. IBM recommends that the SAF registry be used unless it is necessary to share the Kerberos registry with one or more KDC instances running on another operating system.

      The file permissions should allow only the administrator to read and update the file. Set the TZ and RESOLVER_CONFIG values for your installation, and determine which type of database, NDBM or SAF, your site will use.

   c. If your installation uses the SERVAUTH RACF class profiles to control access to TCP/IP ports and stacks, also use the RACF publications as a guide to update the TCP/IP resource permissions needed for Network Authentication Service users and KDCs.

   d. The IRR.RUSERMAP resource in the FACILITY class must be defined if you are are going to obtain service keys from a local instance of the KDC instead of from a key table. The application server system IDs must have RACF READ access to IRR.RUSERMAP resource to use the KRB5_SERVER_KEYTAB variable set to 1. To define IRR.RUSERMAP and grant READ authority to all system users:

      ```
      RDEFINE FACILITY IRR.RUSERMAP UACC(READ)
      SETROPTS RACLIST(FACILITY) REFRESH
      ```

      See "Security runtime environment variables" on page 19 for more on the KRB5_SERVER_KEYTAB environment variable.

   e. The following steps are to be used only if you are implementing the SAF database. Skip these steps if you are using NDBM.

      1) Before starting the SKRBKDC started task, when using the SAF database implementation, be sure that the REALM definitions and other configuration and RACF items are completed for your installation. See Chapter 3, "Administering Network Authentication Service", on page 31 for more information. Refer also to the appropriate sections of *z/OS: Security Server RACF Security Administrator's Guide* and supporting publications for updating the RACF Database template and the Dynamic Parsing task before using Network Authentication Service for z/OS.

      2) Define the RACF Remote Sharing Facility (RRSF) for the local system, even if you do not plan to set up an RRSF network. An RRSF local node must be defined in order to generate the corresponding Kerberos secret key whenever users change their password. Refer to *z/OS: Security Server RACF Security Administrator's Guide* for information on defining the local RRSF node.

         a) Create the SKRBKDC user ID. This user ID must have UID(0).

            ```
            ADDUSER SKRBKDC DFLTGRP(SYS1) NOPASSWORD OMVS(UID(0) PROGRAM('/bin/sh')
                     HOME('/etc/skrb/home/kdc'))
            ```

Configuring

      b) Activate the APPL class if it is not already active.

```
SETROPTS CLASSACT(APPL) RACLIST(APPL)
```

3) Define the SKRBKDC application and set the universal access to READ. Alternately, you can set the universal access to NONE and define individual groups or users to the SKRBKDC application. Users must have access to the SKRBKDC application to use the **kpasswd** Kerberos command to change their passwords.

```
RDEFINE APPL SKRBKDC UACC(READ)
```

4) Activate the PTKTDATA class if it is not already active.

```
SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
```

5) Define the PassTicket data for the SKRBKDC application. PassTickets are used internally by the Kerberos security server when the user password is changed. A PassTicket is never given to a user by the Kerberos security server. The secured signon key can be any valid DES key as described in *z/OS: Security Server RACF Security Administrator's Guide*.

```
RDEFINE PTKTDATA SKRBKDC UACC(NONE) SSIGNON(KEYMASKED(3734343237343131))
```

6) Refresh the APPL and PTKTDATA classes.

```
SETROPTS RACLIST(APPL PTKTDATA) REFRESH
```

f. Define the SKRBKDC started task and associate it with the SKRBKDC user ID. Define the SKRBWTR started task and associate it with the SKRBKDC user ID if you plan to perform component tracing with the SKRBWTR procedure.

```
RDEFINE STARTED SKRBKDC.** STDATA(USER(SKRBKDC))
```
```
RDEFINE STARTED SKRBWTR.** STDATA(USER(SKRBKDC))
```

g. Refresh the STARTED Class.

```
SETROPTS RACLIST(STARTED) REFRESH
```

2. If you wish, customize the **/etc/services** file to assign ports to the Kerberos services. Add the following service names and change the default entries for port/protocol to reflect how you operate the network at your installation. Each line represents a line in the **/etc/services** file showing the service name and the default values for the port/protocol. Kerberos uses the default port assignments if **/etc/services** does not contain the Kerberos entries, so customizing **/etc/services** is an optional step and only needs to be done if the default port assignments are not acceptable.

```
kerberos       88/udp
kerberos       88/tcp
kpasswd       464/udp
kpasswd       464/tcp
kerberos-adm  749/tcp
krb5_prop     754/tcp
```

3. Because the master KDC function in the DCE Security Server uses port 749, and the primary KDC administration function in Network Authentication Service defaults to port 749, you must take the following action to avoid a conflict. There are these possible situations:

- If you are not running a master DCE Security Server on your system, you will not have a conflict. Skip to Step 4 on page 11.

  Note: The administration service is started only on the DCE *master* security server. DCE security server replicas do not use port 749.

- If you are not planning to use an NDBM database, you will not have a conflict. Skip to Step 4 on page 11.

- If you *are* planning to use an NDBM database, but the primary KDC is not on this system, you will not have a conflict. Skip to Step 4 on page 11.

- If you are planning to use an NDBM database, and if you are running a master DCE Security Server on your system, your primary NDBM KDC **envar** file must specify the environment variable SKDC_KADMIN_PORT with a value other than 749 that complies with how you operate the network at your installation.

4. Because the KDC function in the DCE Security Server uses port 88, and the KDC function in Network Authentication Service defaults to port 88, you must take the following action to avoid a conflict. There are these possible situations:

   • If you are not running a DCE Security Server on your system, you will not have a conflict. Skip to Step 5.

   • If you *are* running a DCE Security Server on your system, but are *not* using the KDC portion of it, add the line SECD_ENABLE_KDC=0 to the DCE Security Server **envar** file to disable DCE use of port 88. (You must stop and start the DCE Security Server to bring changes to its **envar** file online.)

   • If you are running a DCE Security Server on your system, and you *are* using the KDC portion of it, the Network Authentication Service KDC **envar** file in **/etc/skrb/home/kdc** must specify the environment variable SKDC_PORT with a value other than 88 that complies with how you operate the network at your installation. Corresponding changes to the **/etc/skrb/krb5.conf** file, LDAP KDC port specification, or DNS SRV records will be necessary to inform users of this KDC port change.

5. Customize the Communications Server PROFILE DD name member to ensure that the selected ports for the KDC (usually Port 88, unless it was changed above), the KPASSWD port (usually Port 464), and the KADMIN port (usually Port 749 unless it was changed above) are reserved for OMVS.

6. Because DCE uses the same commands and environment variables as Network Authentication Service, you must perform these steps:

   a. Determine which user IDs will be using Network Authentication Service. These user IDs must not use DCE.

   b. Customize the LOGON procedures for the Network Authentication Service users:

      • Remove the DCE REXX exec dataset if it is present in the SYSEXEC DD name concatenation.

      • Add the Network Authentication Service REXX exec dataset, EUVF.SEUVFEXC, to the SYSEXEC DD name concatenation.

      • Update the users' UNIX System Services **.profile** by customizing the PATH environment variable to place **/usr/lpp/skrb/bin** ahead of any **/bin** or DCE subdirectory reference.

Note:

The z/OS SecureWay Security Server for Distributed Computing Environment (DCE) provides Kerberos Key Distribution Center (KDC) services configured on TCP/IP Port 88, which is *not* used by the Remote Procedure Call protocols of DCE security. For this reason, you must do the following:

1. If the z/OS SecureWay Security Server for DCE (DCE Security Server, for short) is part of the DCE configuration for your installation, update the DCE Security Server **envar** file to ensure operation of the server without conflict with the Network Authentication Service Key Distribution Center (KDC), which usually operates on TCP/IP Port 88 . Add the line SECD_ENABLE_KDC=0 to disable the DCE Security Server use of TCP/IP Port 88 for Kerberos services. This has no effect on other services of DCE Security Server.

2. Customize the Network Authentication Service KDC **envar** file in **/etc/skrb/home/kdc** to comply with the operation of the network at your installation. The defaults set Kerberos services on Port 88 and the KPASSWD Port on 464.

3. Customize the Communications Server PROFILE DD name member to ensure that the ports you choose for the KDC (usually Port 88) and for KPASSWD (usually Port 464) are reserved for OMVS.

Configuration of encryption types

The **default_tkt_enctypes** value in the Kerberos configuration profile specifies the encryption types to be used for session keys in initial ticket-granting tickets. This is a list of one or more encryption types specified from most-preferred to least-preferred. The KDC selects the first supported encryption type in the list when it generates the session key for an initial ticket-granting ticket. This encryption type is also used for preauthentication information.

Configuring

The **default_tgs_enctypes** value in the Kerberos configuration profile specifies the encryption types to be used for session keys in service tickets. This is a list of one or more encryption types specified from most-preferred to least-preferred. The KDC selects the first supported encryption type in the list when it generates the session key for a service ticket.

To enable 168-bit DES3 support for tickets, specify the following in the SKRBKDC environment file (**/etc/skrb/home/kdc/envar**):

```
SKDC_TKT_ENCTYPES=des3-cbc-sha1,des-cbc-crc
```

To enable 168-bit DES3 support for authentication information, specify the following in the Kerberos configuration profile (**/etc/skrb/krb5.conf**):

```
default_tkt_enctypes = des3-cbc-sha1,des-cbc-crc
```

To enable 168-bit DES3 support for user data, specify the following in the Kerberos configuration profile (/**etc/skrb/krb5.conf**):

```
default_tgs_enctypes = des3-cbc-sha1,des-cbc-crc
```

To enable DES3 key generation with the SAF database implementation, if your external security manager is RACF, use the following RACF command:

```
SETROPTS KERBLVL(1)
```

Do not enable 168-bit DES3 ticket support until the Kerberos runtimes for all systems in the realm support DES3 encryption. Otherwise, you can obtain tickets that cannot be processed on a given system. In addition, do not enable DES3 encryption support for user data unless all systems in the realm support DES3 encryption for user data. Otherwise, you can obtain session keys that are unuseable for exchanging encrypted data. This means that all systems sharing the database must be running z/OS Version 1 Release 2 or later.

When granting a service ticket, the KDC attempts to use the same encryption algorithm for the service ticket that was used for the ticket-granting ticket. This enables cross-realm encryption compatibility with realms that do not support the same encryption algorithms as the local realm. If the server principal does not have a key for that encryption type, then the KDC selects a key from the list specified by the SKDC_TKT_ENCTYPES environment variable.

GSS-API supports 56-bit DES and 168-bit DES3 encryption. To enable 168-bit DES3 encryption, update the **default_tgs_enctypes** value in the Kerberos configuration profile to specify both **des3-cbc-sha1** and **des-cbc-crc**. The actual encryption type selected for a particular GSS-API security context is the intersection of the **default_tgs_enctypes** list and the available encryption keys for the target principal. For example, if the **default_tgs_enctypes** value is **des3-cbc-sha1,des-cbc-crc**, and the target principal has just a 56-bit DES key, the encryption type for the GSS-API security context is **des-cbc-crc**.

Security runtime configuration with LDAP and DNS considerations

1. Perform the following steps to customize **/etc/skrb/krb5.conf** for your installation:
   - Update the default_realm value with the name of your Kerberos realm.
   - If you want to use LDAP to locate servers and to resolve host names, set the **use_ldap_lookup** value to 1
   - If you want to use DNS SRV and TXT records to locate servers and to resolve host names, set the **use_dns_lookup** value to 1
   - If you will not be using LDAP or DNS lookup, update the [realms] section to identify your Kerberos realm, and then update each realm that can be reached from your realm. The [realms] section is also used when a directory lookup request is unsuccessful.

     For example, if the default realm is KRB390.IBM.COM with two KDC servers using the SAF database, and a peer realm is KRB2000.IBM.COM with one KDC server, the [realms] section is

defined as follows. Since the z/OS implementation combines the KDC and the password change server when the SAF database is implemented, each instance of the Kerberos security server provides both the **kdc** and the **kpasswd_server** services.

```
[realms]
KRB390.IBM.COM = {
        kdc = kdcsrvr1.krb390.ibm.com:88
        kdc = kdcsrvr2.krb390.ibm.com:88
        kpasswd_server = kdcsrv1.krb390.ibm.com:464
        kpasswd_server = kdcsrv2.krb390.ibm.com:464
}
KRB2000.IBM.COM = {
        kdc = winsrvr1.krb2000.ibm.com:88
}
```

- If you will not be using LDAP or DNS lookup, update the [domain_realm] section to identify the host-to-realm mappings for your Kerberos realm and each realm that can be reached from your realm. The [domain_realm] section is also used when a directory lookup request is unsuccessful.

  Using the same example, the [domain_realm] section is defined as follows:

```
[domain_realm]
.krb390.ibm.com = KRB390.IBM.COM
.krb2000.ibm.com = KRB2000.IBM.COM
```

  If no matching entry is found, the default action is to remove the first label from the host name, put what is left in upper case, and use that for the realm name. In this case, the definitions given in the preceding examples are not really needed since they match the default.

2. If you are using DNS lookup, define the Kerberos hosts and servers in the DNS database:

   - SRV records are added for each KDC server in the realm. The Kerberos runtime searches for an SRV record using the realm name as the DNS search name. Note that DNS searches are not case-sensitive, so you cannot have two different realms whose names differ only in their case.

     The general form of the Kerberos SRV record is:

```
service.protocol.realm ttl class SRV priority weight port target
```

     The **_kerberos** service entries define KDC instances, while the **_kerberos-adm** service entries define administration service instances, and **_kpasswd** entries define the password change service instances. Since the z/OS implementation combines the KDC and the password change server when the SAF database is implemented, each instance of the Kerberos security server provides both the KDC and the password change services. Administration service support on z/OS is available *only* when the NDBM database is implemented.

     The server entries are tried in priority order (0 is the highest priority). Server entries with the same priority are tried in a random order. **_udp** protocol records are required for the **_kerberos** and **_kpasswd** services while **_tcp** protocol records are required for the **_kerberos-adm** service. **_tcp** protocol records should be present if the server supports TCP as well as UDP requests (the z/OS Kerberos security server supports both UDP and TCP requests) for **_kerberos** and **_kpasswd**.

     For example, to define z/OS Kerberos security servers **krbsrv1** and **krbsrv2** for the KRB390.IBM.COM realm, add the following SRV records:

```
_kerberos._udp.krb390.ibm.com IN SRV 0 0 88  krbsrv1.krb390.ibm.com
_kerberos._tcp.krb390.ibm.com IN SRV 0 0 88   krbsrv1.krb390.ibm.com

_kpasswd._udp.krb390.ibm.com  IN SRV 0 0 464 krbsrv1.krb390.ibm.com
_kpasswd._tcp.krb390.ibm.com  IN SRV 0 0 464  krbsrv1.krb390.ibm.com

_kerberos._udp.krb390.ibm.com IN SRV 0 0 88  krbsrv2.krb390.ibm.com
_kerberos._tcp.krb390.ibm.com IN SRV 0 0 88  krbsrv2.krb390.ibm.com
_kpasswd._udp.krb390.ibm.com  IN SRV 0 0 464 krbsrv2.krb390.ibm.com
_kpasswd._tcp.krb390.ibm.com  IN SRV 0 0 464  krbsrv2.krb390.ibm.com
```

Configuring

An example of an _**kerberos-adm** SRV record for a z/OS primary KDC implementing the NDBM database is:

```
_kerberos-adm._tcp.krb390.ibm.com IN SRV 0 0 749  krbsrv1.krb390.ibm.com
```

- TXT records are added to associate host names with realm names. The Kerberos runtime searches for a TXT record starting with the host name. If no TXT record is found, the first label is removed and the search is retried with the new name. This process continues until a TXT record is found or the root is reached.

  The general form of the Kerberos TXT record is:

```
service.name ttl class TXT realm
```

  For example, to associate the endicott.ibm.com domain with the KRB390.IBM.COM realm, add the following TXT record:

```
_kerberos.endicott.ibm.com IN TXT KRB390.IBM.COM
```

  Note that the realm name is case-sensitive in the TXT record.

3. If you are using LDAP lookup, define the Kerberos objects and attributes for the LDAP server:

- Add a suffix definition to the LDAP server configuration file for the root domain name. For example, if your Kerberos realm names end in .COM, add the following statement to the LDAP configuration file:

```
suffix "dc=COM"
```

- Use the **ldapadd** command to define the default realm in the LDAP directory. Use the **/usr/lpp/skrb/examples/slapd.ldif** file as an example. Each component of the Kerberos realm name is represented by a domain component entry in the LDAP directory.

  For example, to define the KRB2000.IBM.COM realm in LDAP, use the following **ldif** definitions:

```
dn: dc=COM
dc: COM
objectClass: domain

dn: dc=IBM, dc=COM
dc: IBM
objectClass: domain

dn: dc=KRB2000, dc=IBM, dc=COM
dc: KRB2000
objectClass: domain
```

- Use the **ksetup** command to define the host systems in your Kerberos realm as well as the location of each security server. If you do not want to define each host system in LDAP, you can use the [domain_realm] section of the Kerberos configuration file to supply default rules to map host names to a Kerberos realm.

  Using the example above, define the security servers with the SAF database implementation as follows:

```
addkdc kdcsrvr1.krb390.ibm.com  KRB390.IBM.COM
addkdc kdcsrvr2.krb390.ibm.com  KRB390.IBM.COM
addpwd kdcsrvr1.krb390.ibm.com  KRB390.IBM.COM
addpwd kdcsrvr2.krb390.ibm.com  KRB390.IBM.COM
addkdc winsrvr1.krb2000.ibm.com KRB2000.IBM.COM
```

  For the NDBM database implementation, the **addpwd** command is issued for the Primary KDC only. The **addadmin** command is also issued for the Primary KDC only. Here is an example:

```
addadmin kdcsrvr1.krb390.ibm.com:749  KRB390.IBM.COM
```

- Refer to *z/OS: Security Server LDAP Server Administration and Use* for more information on setting up the LDAP server.

LDAP schema definitions

If you are planning to use LDAP directory lookup functions, the Kerberos runtime requires the following LDAP schema definitions. These definitions are supplied with IBM LDAP servers as part of the IBM schema. You should also create the appropriate schema definitions for other LDAP servers.

- Integer values are represented as a signed-numeric character string with a maximum length of 11 characters
- Boolean values are represented by the character strings ″TRUE″ and ″FALSE″
- Time values are represented as 15-byte character strings encoded in the format ″YYYYMMDDhhmmssZ.″ All times are represented as UTC values.

Table 2. LDAP object classes

Object	Requires	Allows
domain	dc objectClass	description seeAlso
eSAP	objectClass	labeledURI sapName serviceHint
eService	objectClass	startMode startupParameters sapPtr serviceName
ibmCom1986-Krb-KerberosService	objectClass serviceName ibmCom1986-Krb-KerberosRealm	ipServicePort description seeAlso

Table 3. LDAP attributes

Attribute	Table Name	Type	Size	Access	Value
dc	dc	caseIgnoreString	64	normal	single
description	description	caseIgnoreString	1024	normal	multiple
ibmCom1986-Krb-KerberosRealm	krbRealm	caseExactString	256	normal	single
ipServicePort	ipServicePort	integer	11	normal	single
labeledURI	labeledURI	caseExactString	100	normal	multiple
sapName	sapName	caseIgnoreString	256	normal	single
sapPtr	sapPtr	DN	1000	normal	multiple
seeAlso	seeAlso	DN	1000	normal	multiple
serviceHint	serviceHint	DN	1000	normal	single
serviceName	serviceName	caseIgnoreString	256	normal	single
startMode	startMode	caseExactString	10	normal	single
startupParameters	startupParameters	caseExactString	256	normal	single

Security server configuration

Configuring the primary security server for the realm

1. Create the Kerberos definitions:

Configuring

- If you plan to use SAF for the registry database, do these steps to create the Kerberos definitions in the z/OS security registry:

  a. Define the local realm and the default policy.

  For example, to define the KRB2000.IBM.COM realm with a minimum ticket lifetime of 15 seconds, a maximum ticket lifetime of 24 hours, and a default ticket lifetime of 10 hours:

  ```
  RDEFINE REALM KERBDFLT KERB(KERBNAME(KRB2000.IBM.COM)
  PASSWORD(password)
          MINTKTLFE(15) DEFTKTLFE(36000) MAXTKTLFE(86400))
  ```

  b. Create peer trust definitions.

  There will be two definitions for each trust relationship. For example, to define a trust relationship between the KRB2000.IBM.COM and WIN2000.IBM.COM realms:

  ```
  RDEFINE REALM /.../KRB2000.IBM.COM/krbtgt/WIN2000.IBM.COM
                      KERB(PASSWORD(password))
  RDEFINE REALM /.../WIN2000.IBM.COM/krbtgt/KRB2000.IBM.COM
                      KERB(PASSWORD(password))
  ```

  Note: The RDEFINE command converts the realm name to upper case.

  c. Define the administration service. The user ID can be any acceptable name but the Kerberos principal must be **kadmin/admin**.

  ```
  ADDUSER KADMIN DFLTGRP(SYS1) PASSWORD(temporary password)
  ALTUSER KADMIN PASSWORD(password) NOEXPIRED
  KERB(KERBNAME(kadmin/admin))
  ```

  d. Define the password change server. The user ID can be any acceptable name but the Kerberos principal must be **kadmin/changepw**.

  ```
  ADDUSER CHANGEPW DFLTGRP(SYS1) PASSWORD(temporary_password)
  ALTUSER CHANGEPW PASSWORD(password) NOEXPIRED KERB(KERBNAME(kadmin/changepw))
  ```

  e. Add Kerberos segments to existing user definitions.

  For example, to associate the principal **test_server@KRB2000.IBM.COM** with the **krbsrv** user:

  ```
  ALTUSER KRBSRV PASSWORD(password) NOEXPIRED KERB(KERBNAME(test_server))
  ```

  Note: The ALTUSER command converts the password to upper case. You must ensure that the uppercase value is used when you request an initial ticket. The principal name is not converted to upper case and the realm name is not included. You must change the password for the user in order to create the Kerberos secret key.

  f. See *z/OS: Security Server RACF Command Language Reference* for more information.

- If you plan to use NDBM for the registry database instead of SAF, do these steps to create the Kerberos definitions for the NDBM database. Refer to Chapter 4, "Commands", on page 47 for details on the Kerberos commands used in this section.

  a. Use the **kdb5_ndbm** command to create the initial registry database files. This command creates the architected principals for the Kerberos realm. It also creates two user principals, **IBMUSER** and **IBMUSER/admin**, with an initial password of IBMUSER. IBM recommends that you use the **kadmin** command and authenticate with the **IBMUSER/admin** principal to create your own administration principal after the security server is running. The passwords for the **IBMUSER** and **IBMUSER/admin** principals should then be changed or the principals should be deleted.

  b. Copy the example KDC configuration file from **/usr/lpp/skrb/examples/kdc.conf** to **/etc/skrb/home/kdc/kdc.conf**.

  c. Set the **min_life**, **max_life**, **max_renewable_life**, and **default_life** values in **kdc.conf** to the appropriate minimum ticket life, maximum ticket life, maximum renewable ticket life, and default ticket life values. The following relationship must be observed: **min_life** <= **default_life** <= **max_life** <= **max_renewable_life**. The maximum ticket life and maximum renewable ticket life values for a specific principal are the smaller of the values specified in the principal entry and the values specified in the KDC configuration profile.

d. Set the **check_client_address** value in **kdc.conf** to 1 if you want the KDC to validate the address list contained in tickets presented by clients. Note that client address validation fails if requests pass through a firewall or a Network Address Translation (NAT) router because the client address in the ticket does not match the client address as seen by the server.

e. Add Kerberos segments to existing user definitions if you want to use SAF mapping services to map a Kerberos principal to a system user ID. These mappings are required if you plan to use Kerberos system-authentication services to eliminate the need to provide a key when requesting an initial ticket or decrypting a service ticket.

For example, to associate the principal **test_server@KRB2000.IBM.COM** with the **krbsrv** user:

```
ALTUSER KRBSRV KERB(KERBNAME(test_server))
```

2. Copy the example administration access control file from **/usr/lpp/skrb/examples/kadm5.acl** to **/etc/skrb/home/kdc/kadm5.acl** and customize it for your installation if you will be using Kerberos administration services. This file controls the Kerberos administration privileges granted to a user. Each line represents a single administration access definition, has a maximum length of 255 characters, and is assumed to be in the code page specified by the LANG environment variable. Comment lines start with a semi-colon and blank lines are ignored. Each line consists of 2 fields: the client principal name and the privileges granted. The order of the lines in the file is important because the search stops as soon as a match is found for the principal making an administration request.

The following privileges are defined. Use lowercase letters to define the granted privileges (any privilege not listed is denied) and use uppercase letters to define the denied privileges (any privilege not listed is granted). Do not mix uppercase and lowercase letters in the same definition.

a	ADD is granted
A	ADD is denied
c	CHANGEPW is granted
C	CHANGEPW is denied
d	DELETE is granted
D	DELETE is denied
g	GET is granted (this may also be specified as i)
G	GET is denied (this may also be specified as I)
l	LIST is granted
L	LIST is denied
m	MODIFY is granted
M	MODIFY is denied
s	SETKEY is granted
S	SETKEY is denied
*	All privileges are granted

The client principal name can contain the following wildcards:
- ? represents a single character
- * represents zero or more characters
- Paired [ ] represent any one of the characters between the brackets.

3. Copy the example propagation control file from **/usr/lpp/skrb/examples/kpropd.acl** to **/etc/skrb/home/kdc/kpropd.acl** and customize it for your installation if you will be using Kerberos database propagation. The propagation control file contains an entry for each Kerberos security server in the realm and specifies the role assigned to each of the servers. The role should be specified as MANUAL until the secondary security server has been configured and the initial database propagation has been performed. Refer to "Kerberos database propagation" on page 41 for more information.

Configuring

4. Start the SKRBKDC started task.

5. Change the passwords for **IBMUSER** and **IBMUSER/admin** if you are using the NDBM database. These principals are automatically created when the database is created and have an initial password of IBMUSER. You can use the **kpasswd** command or the **kadmin** command to change the passwords. You can also create your own administration user IDs and then delete **IBMUSER** and **IBMUSER/admin** if desired.

Configuring a secondary security server for the realm

Using a SAF registry database

The same SAF registry database must be shared by all of the security servers in the realm. This means you do not need to repeat the RACF (or other external security manager) commands described above when you configure a secondary security server. Database propagation is not used by the Kerberos security server for a SAF registry database since the external security manager is responsible for any required propagation.

If the **/etc/skrb** file system is not shared between systems, copy the **/etc/skrb/krb5.conf** and **/etc/skrb/home/kdc/envar** files from the primary system to the secondary system. You do not need the **/etc/skrb/home/kdc/kadm5.acl** configuration file because Kerberos administration services are not available for the SAF registry database.

Finally, copy the SKRBKDC JCL procedure and, optionally, the message exit used to start the SKRBKDC started task. Once this has been done, you can start the SKRBKDC started task on the secondary system.

Using an NDBM registry database

The NDBM registry database is not shared by each security server in the realm (the file system containing the **/var/skrb/krb5kdc** directory must not be shared between systems). Instead, each security server maintains its own NDBM database and receives updates from the primary security server through the database propagation protocol.

If the **/etc/skrb** file system is not shared between systems, copy the **/etc/skrb/krb5.conf** and **/etc/skrb/home/kdc/envar** files from the primary system to the secondary system. Also copy the **/etc/skrb/home/kdc/kpropd.acl** configuration file. You do not need to copy the **/etc/skrb/home/kdc/kadm5.acl** configuration file since a secondary KDC does not provide Kerberos administration services for the NDBM registry database.

Use the **kdb5_ndbm** command to create the database master key stash file on the secondary system. The master key is used to decrypt Kerberos database entries. This key is not sent over the network as part of the database propagation protocol. For example:

```
kdb5_ndbm stash
```

Use the **kadmin** command to create the host key table used during database propagation. This key table is used to authenticate the secondary security server to the primary security server. The principal is **host/**_system-name_ where _system-name_ is the host name for the secondary system. The host name must be the primary host name for the system as returned by the DNS name server. For example, to create a host principal and key table for the **dcesec4.krb390.ibm.com** system:

```
kadmin> addprinc host/dcesec4.krb390.ibm.com
kadmin> ktadd host/dcesec4.krb390.ibm.com -k /var/skrb/krb5kdc/kpropd.ktf
```

Use the **kpropd** command to receive the initial database propagation from the primary KDC for the realm. Refer to the section on database propagation for more information.

Finally, copy the SKRBKDC JCL procedure and, optionally, the message exit used to start the SKRBKDC started task. Once this has been done, you can start the SKRBKDC started task on the secondary system.

Security runtime environment variables

Environment variables can be defined in the current command shell using the **export** command. They can also be defined in an environment variable (**envar**) file, which is processed during security runtime initialization. Any variables defined through the shell override the same variables in the envar file. The _EUV_ENVAR_FILE environment variable can be used to specify the location of the envar file. By default, the **$HOME/envar** file is used.

z/OS generally sets environment variables in either **/etc/profile** (system-wide settings) or in **$HOME/.profile** (user-specific settings). Environment variables defined in either place override the same variables in the envar file.

The following environment variables are supported:

Table 4. Environment variables for security runtime

Environment Variable	Explanation
_EUV_SVC_DUMP	Specifies whether or not a dump is taken by the security runtime if a serious error is detected. This environment variable applies only to errors that are caught and processed by the security runtime. Error processing for errors handled by the Language Environment® (LE) runtime are controlled by the LE runtime options that are in effect at the time of the error. The following values may be specified for this value: • 0 = No dump is taken. This suppresses dumps generated as a result of an exception as well as dumps requested by the security runtime. A dump may still be taken by the operating system depending upon the nature of the error. • 1 = A dump is taken (this is the default)
_EUV_ENVAR_FILE	Specifies the name of the file that contains environment variable definitions. If this variable is not set, the default is to use the envar file located in the home directory (as specified by the _EUV_HOME or HOME environment variable). A dataset name can be specified by preceding the dataset name with ′″//″, and a DD name can be specified by preceding the DD name with″//DD:.″ Each line of the file consists of the variable name followed by ″=″ followed by the variable value with no intervening blanks or other punctuation. The variable value consists of everything following the ″=″ up to the end of the line (including any trailing blanks). Any line beginning with ″#″ is treated as a comment line. A line can be continued by ending the line with ″\″. Note that the environment variables are not set until the first time that a function in the security runtime is called. Thus, it is mainly useful for setting environment variables that are used by functions within the security runtime, although it can be used to set environment variables that are used by the application as well. In this case, the application should not rely on the environment variable values until after the security runtime has been initialized. The application can access these environment variables using the **getenv()** function. The environment variables are maintained by the C runtime library, so they are not available to operating system functions.

Configuring

Table 4. Environment variables for security runtime (continued)

Environment Variable	Explanation
_EUV_EXC_ABEND_DUMPS	Specifies whether a dump is to be generated when an abnormal termination occurs within the security runtime. This environment variable applies only to errors that are caught and processed by the security runtime. The default is to not take a dump if an abnormal termination occurs (the system may still take a dump if the exception percolates to the top of the condition handler stack without being handled). No dump is taken if _EUV_DUMP is set to 0 even if _EUV_EXC_ABEND_DUMPS is set to enable a dump. The following values may be specified for dump control: • 0 = No dump (this is the default) • 1 = Dump only if no CATCH/CATCH_ALL was found to handle the exception • 2 = Dump only if no explicit catch clause was found to handle the exception (that is, the exception was caught by a CATCH_ALL clause)
_EUV_HOME	The security runtime home directory is set to the value of this environment variable. If this variable is not specified, the HOME variable is used to determine the security runtime home directory. If the HOME variable is not set, the current directory is used.
_EUV_HW_CRYPTO	Specifies whether the hardware cryptographic support is used. A value of **0** disables the use of the hardware support, and a value of **65535** enables the use of the hardware support. The hardware support is used if this environment variable is not defined. Note that Integrated Cryptographic Service Facility (ICSF) must be configured and running in order to use the hardware cryptographic support. Selected hardware cryptographic functions can be disabled by setting the appropriate bits to zero in the _EUV_HW_CRYPTO value. The corresponding software algorithms are used when a hardware function is disabled. For example, 56-bit DES can be enabled and 168-bit DES can be disabled by setting _EUV_HW_CRYPTO to 2. The following bit assignments are defined: • 2 = 56-bit DES encryption/decryption • 4 = 168-bit Triple DES encryption/decryption
_EUV_SEC_KRB5CCNAME_FILE	Specifies the name of the file used to locate the default Kerberos credentials cache. If this variable is not set, the default is to use the **krb5ccname** file located in the security runtime home directory (the home directory is specified by _EUV_HOME or HOME). Precede the dataset name with″//″ to specify an MVS™ dataset name and precede the DD name with ″//DD:″ to specify an MVS DD name.

Table 4. Environment variables for security runtime (continued)

Environment Variable	Explanation
_EUV_SVC_DBG	Specifies subcomponents and levels for the debug messages. Debug messages for a particular subcomponent are not logged unless the subcomponent is included in the _EUV_SVC_DBG list and the debug message level is greater than or equal to the specified level. An asterisk (*) may be used to specify all subcomponents. Debug level 1 generates the minimum amount of debug output, debug level 8 generates the maximum amount of debug output, and debug level 9 generates data dumps in addition to the debug messages. The subcomponent list consists of a subcomponent name and a debug level separated by a period. Multiple subcomponents may be specified by separating the entries with commas. For example, `_EUV_SVC_DBG=*.1,KRB_CCACHE.8` enables debug level 1 for all subcomponents and debug level 8 for the KRB_CCACHE subcomponent.
_EUV_SVC_DBG_FILENAME	Specifies the fully-qualified name of the file to receive debug messages. Debug messages are written to the file specified by the _EUV_SVC_STDOUT_FILENAME if this environment variable is not defined. If _EUV_SVC_STDOUT_FILENAME is not specified, debug messages are written to **stdout**.
_EUV_SVC_DBG_MSG_LOGGING	Specifies whether debug messages are generated. The default is to suppress debug messages. The following values may be specified: • 0 = Suppress debug messages • 1 = Write debug messages
_EUV_SVC_DBG_TRACE	Specifies whether trace records are generated. These trace records are stored in an internal wrap table. The following values may be specified: • 0 = Do not generate trace records (this is the default) • 1 = Generate trace records.
_EUV_SVC_MSG_FACILITY	Specifies the facility class for messages written to the system logging facility. The valid facility classes are: KERN, USER, MAIL, NEWS, UUCP, DAEMON, AUTH, CRON, LPR, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. The default is USER.
_EUV_SVC_MSG_IDENTITY	Specifies the identity string prefixed to messages written to the system logging facility. The default is SKRB.
_EUV_SVC_MSG_LEVEL	Specifies the message level when logging messages. Messages that do not meet this criterion are suppressed. The default is to log all messages. The following values may be specified: • FATAL - Only fatal messages are logged • ERROR - Only fatal and error message are logged. • USER - Only fatal, error, and user messages are logged • WARNING - Only fatal, error, user, and warning messages are logged • NOTICE - Only fatal, error, user, warning, and notice messages are logged • VERBOSE - All messages are logged.

Configuring

Table 4. Environment variables for security runtime (continued)

Environment Variable	Explanation
_EUV_SVC_MSG_LOGGING	Specifies the target where messages are logged. The default is to write informational messages to **stdout** and error messages to **stderr**. The following values may be specified: • NO_LOGGING = Suppress all messages • STDOUT_LOGGING = Write all messages (informational and error) to **stdout** and also write error messages to **stderr** • STDERR_LOGGING = Write informational messages to **stdout** and error messages to **stderr**. • SYSTEM_LOGGING = Write all messages to the system logging facility (**syslogd** daemon).
_EUV_SVC_STDERR_FILENAME	Specifies the fully-qualified name of the file to receive standard error messages. Messages are written to **stderr** if this environment variable is not defined.
_EUV_SVC_STDOUT_FILENAME	Specifies the fully-qualified name of the file to receive standard output messages. Messages are written to **stdout** if this environment variable is not defined.
KRB5CCNAME	Specifies the default name for the credentials cache and is specified as *"type:name."* The supported types are FILE and MEMORY. The default credentials cache name is obtained from the credentials cache pointer file identified by the _EUV_SEC_KRB5CCNAME_FILE environment variable if the KRB5CCNAME environment variable is not set.
KRB5RCACHEDIR	Specifies the default replay cache directory and defaults to **/tmp**.
KRB5RCACHENAME	Specifies the default replay cache name. The Kerberos runtime generates a replay cache name if the KRB5RCACHENAME environment variable is not defined.
KRB5RCACHETYPE	Specifies the default replay cache type and defaults to **dfl**.
KRB5_CONFIG	Specifies one or more configuration file names separated by colons. The default configuration file is **/etc/skrb/krb5.conf**.
KRB5_KTNAME	Specifies the default key table name. The default key table name is obtained from the **default_keytab_name** configuration file entry if the KRB5_KTNAME environment variable is not defined. The default key table is **/etc/skrb/krb5.keytab** if no configuration file entry is found.
KRB5_SERVER_KEYTAB	If this environment variable is set to 1, the **gss_accept_sec_context()** and **krb5_rd_req()** routines use a local instance of the Kerberos security server to decrypt service tickets instead of obtaining the key from a key table. The application must have at least READ access to the IRR.RUSERMAP facility in order to use this capability. The Kerberos principal associated with the current system identity must be the same as the Kerberos principal in the service ticket. The key table is used if the Kerberos principal for the system identity is not the same as the Kerberos principal for the service ticket.

Table 4. Environment variables for security runtime (continued)

Environment Variable	Explanation

RESOLVER_CONFIG	Specifies the name of the DNS resolver configuration file and defaults to **/etc/resolv.conf**. This can be either the name of an HFS file (**/***hfs-path***/***hfs-file*) or the name of a sequential MVS dataset (**//***'dataset-name'*). The configuration file is assumed to be in code page 1047, each line has a maximum length of 255 characters, lines beginning with an asterisk or a semi-colon are comment lines, and blank lines are ignored. Each control statement consists of a keyword and a value separated by a blank. Any additional tokens following the keyword value are ignored. The keyword names are not case-sensitive and lines containing unrecognized keywords are skipped. The following control statements are recognized by the Kerberos runtime:
	
	• ResolveVIA *method*
	  Specifies whether UDP or TCP connections are to be used when communicating with the DNS name server, and defaults to UDP.
	• ResolverTimeout *number*
	  Specifies the number of seconds to wait for a response from the DNS name server and defaults to 5.
	• ResolverUDPRetries *number*
	  Specifies the number of retries for UDP connections and defaults to 1.
	• NSPortAddr *number*
	  Specifies the DNS name server port number and defaults to 53.
	• NSInterAddr *network-address*
	  Specifies the network address of the DNS name server. This statement can be specified more than once if there are multiple name servers. In this case, a request is sent to each server in the order listed until a successful response is received.
	• NameServer *network-address*
	  Same as NSInterAddr.

Security server environment variables

The following environment variables are supported for the SKRBKDC started task. These variables are specified in **/etc/skrb/home/kdc/envar**.

Table 5. Environment variables for security server

Environment Variable	Explanation
SKDC_CREDS_SIZE	Specifies the credentials data space size in kilobytes, with a minimum value of 1024, a maximum value of 2097148, and a default value of 20480. The Kerberos security server stores cross-memory credentials in this data space.

Configuring

Table 5. Environment variables for security server (continued)

Environment Variable	Explanation
SKDC_DATABASE	Specifies the type of registry database used by the security server: • SAF - Indicates the security registry is maintained in the system security database available through the System Authorization Facility (SAF). The database is administered using commands provided by the external security manager. The external security manager is responsible for propagating any database changes to other systems in the realm where an instance of the KDC is running. Kerberos database propagation is not used with the SAF database. • NDBM - Indicates the security registry is maintained in HFS files located in the **/var/skrb/krb5kdc** directory. The database is administered using Kerberos administration commands. The KDC is responsible for propagating any database changes to other systems in the realm where an instance of the KDC is running.
SKDC_KADMIN_PORT	Specifies the administration service port number. If this environment variable is not defined, the administration service port is obtained from the *kerberos-adm* entry in the TCP/IP services files. If this entry is not defined, the administration service port defaults to 749. The administration service uses just the TCP protocol.
SKDC_KPASSWD_PORT	Specifies the password change service port number. If this environment variable is not defined, the password change service port is obtained from the *kpasswd* entry in the TCP/IP services file. If this entry is not defined, the password change service port defauts to 464. The password change service uses both the UDP and TCP protocols.
SKDC_KPROP_INTERVAL	Specifies the database propagation interval in minutes and defaults to 15. The security server sends the current registry database to each secondary security server that is using the full replacement protocol. This propagation occurs at the end of each propagation interval. No propagation is done if the database has not been changed since the last propagation. Secondary security servers that are using the update protocol receive database updates immediately and do not wait for the end of a propagation interval.
SKDC_KPROP_PORT	Specifies the database propagation port number. If this environment variable is not defined, the database propagation port is obtained from the *krb5_prop* entry in the TCP/IP services file. If this entry is not defined, the database propagation service port defaults to 754. Database propagation uses just the TCP protocol.
SKDC_LOCAL_THREADS	Specifies the number of threads to be used for local requests that use the S/390® Program Call instruction to communicate with the security server. The default value is 10 and the minimum value is 2.
SKDC_LOGIN_AUDIT	Specifies the desired auditing level for login attempts (that is, granting a Kerberos initial ticket). The allowed values are: • NONE = no auditing is done • FAILURE = only login attempts that fail due to an invalid password are audited • ALL = both success and failure login attempts are audited. The audit level is set to FAILURE if the SKDC_LOGIN_AUDIT environment variable is not specified or is set to an incorrect value. SMF type 80 records with event code 68 are written for an audit event. See *z/OS: Security Server RACF Macros and Interfaces* for more information about the format of the SMF records.

Table 5. Environment variables for security server (continued)

Environment Variable	Explanation
SKDC_NETWORK_POLL	Specifies the network interface poll interval in minutes and defaults to 5. The security server queries the network configuration at the end of each poll interval to detect new network interfaces or the activation of a failed network interface.
SKDC_NETWORK_THREADS	Specifies the number of threads to be used for remote requests that use TCP/IP to communicate with the security server. The default value is 10 and the minimum value is 2.
SKDC_PORT	Specifies the KDC port number. If this environment variable is not defined, the KDC port is obtained from the *kerberos* entry in the TCP/IP services file. If this entry is not defined, the KDC port defaults to 88. The KDC uses both the UDP and the TCP protocols.
SKDC_TKT_ENCTYPES	Specifies the encryption types to be used for ticket-granting tickets and for service tickets. This is a list of one or more encryption types separated by commas, specified from most-preferred to least-preferred. When generating a ticket, the KDC selects the first entry in the list that is available for the server specified in the ticket. The KDC uses **des-cbc-crc** if this environment variable is not defined. The encryption types specified by the SKDC_TKT_ENCTYPES environment variable are also used by the Kerberos administration server when it generates new keys for a principal and no encryption types are specified by the administration request.

Security runtime configuration profile

The default security runtime configuration profile is **/etc/skrb/krb5.conf**. You can change this by defining the KRB5_CONFIG environment variable. You can specify multiple configuration files for the KRB5_CONFIG variable by separating the names with colons.

If a named entry can have just one value, then the first occurrence of the name is used. Otherwise, all of the entries for the same name are grouped together in the order they are encountered.

The file is divided into sections. Each section contains one or more name/value pairs with one pair per line. The name and value are separated by an equal sign. The value may be either a character string or a group of name/value pairs. If a character string is specified, it consists of all characters starting with the first non-blank character following the equal sign and continuing until the last non-blank character on the line. The maximum length of a single line in the configuration file is 2046 bytes. Comment lines are denoted by a semi-colon in the first position of the line. Blank lines are ignored.

A section name is enclosed in brackets and must appear on a line by itself. Group values are enclosed in braces with one group per line. The opening brace for a group may follow the equal sign or may be on a line by itself. The closing brace must be on a line by itself so that it won't be treated as part of the value string.

The configuration file must be in code page 1047. To support other code pages, you can use the following trigraphs:

Characters	Meaning
??(	left bracket
??)	right bracket
??<	left brace

Configuring

Characters	Meaning
??>	right brace

Numeric values can be specified as follows:

Format	Meaning
dddddd	decimal number
0dddddd	octal number
0xddddd	hexadecimal number

Supported checksum types are (see RFC 1510 for more information about the checksum algorithms):

* crc32
* rsa-md4
* rsa-md4-des
* descbc
* rsa-md5
* rsa-md5-des
* nist-sha
* hmac-sha1-des3

Supported encryption types are (see RFC 1510 for more information about the encryption types):

* des-cbc-crc
* des-cbc-md4
* des-cbc-md5
* des-hmac-sha1
* des3-cbc-sha1

Configuration profile file sections

The following sections of the configuration profile file are supported:

Table 6. Sections of the configuration profile file

Section	Usage
[libdefaults]	This section provides defaults for the Kerberos runtime routines.
[realms]	This section defines each of the realms that can be reached from the local realm. For each realm, one or more key distribution center (KDC) hosts must be defined. The [realms] section is used if no DNS or LDAP server is available or if the desired Kerberos service is not found using the DNS or LDAP server.
[domain_realm]	This section defines the mapping between DNS names and Kerberos realm names. The [domain_realm] section is used if no DNS or LDAP server is available or if the desired mapping is not found using the DNS or LDAP server.
[]	This section defines connection paths between realms. This section is not required if the Kerberos realms are arranged in a hierarchical configuration or if each realm has a peer connection to every other realm. Even in a hierarchical configuration, this section should be defined if there are direct connections between realms.

The information that follows provides details about these sections.

[libdefaults] section

ap_req_checksum_type
Specifies the default checksum type for an application request. The default is rsa-md5.

ccache_type
Specifies the format of the credentials cache file as an integer value between 1 and 4. The default is 3.

check_delegate
Specifies whether the runtime should check the OK-AS-DELEGATE flag in service tickets. Specify 1 to check the flag and 0 to ignore the flag. If checking is enabled and the service ticket returned by the key distribution center (KDC) does not have the OK-AS-DELEGATE flag set, the **gss_init_sec_context()** function does not enable delegation for the target principal. The default is to enable checking.

clockskew
Specifies the maximum clock difference in seconds. The default is 300 (5 minutes). A Kerberos request is rejected if the difference between the server time and the request timestamp exceeds the clock skew value.

default_keytab_name
Specifies the default key table type and name. The KRB5_KTNAME environment variable overrides this specification. The default is **/etc/skrb/krb5.keytab**.

default_realm
Specifies the default realm.

default_tgs_enctypes
Specifies one or more session key encryption types separated by commas. The default is des-cbc-crc,des-cbc-md5. The des-cbc-crc encryption type must be included in the list if you are using GSS-API. The KDC uses the first supported encryption type when generating the session key for a service ticket.

default_tkt_enctypes
Specifies one or more ticket encryption types separated by commas. The default is des-cbc-crc,des-cbc-md5. The KDC uses the first supported encryption type when generating the session key for an initial ticket-granting ticket.

kdc_default_options
Specifies the default options used when requesting an initial ticket from the KDC as follows:
- 0x00000010 = KDC_OPT_RENEWABLE_OK
- 0x10000000 = KDC_OPT_PROXIABLE
- 0x40000000 = KDC_OPT_FORWARDABLE

Mutliple options may be specified by ORing the values together. The default is 0x00000010.

kdc_req_checksum_type
Specifies the default checksum type for a KDC request. The default is rsa-md5.

kdc_timesync
Specifies whether or not to synchronize the local time is with the KDC time. Specify 1 to synchronize the time and 0 not to synchronize the time. Do not specify 1 if the local system is running a time daemon that synchronizes the clock. The default is 0.

kdc_use_tcp
Set this value to 1 to use TCP stream connections instead of UDP datagrams when sending a request to the KDC. If a TCP connection cannot be established with the KDC, the runtime retries by sending a UDP datagram to the KDC. Set this value to 0 to always use UDP datagrams. The default is 0.

kpasswd_use_tcp
Set this value to 1 to use TCP stream connections instead of UDP datagrams when sending a request

Configuring

to the password change server. If a TCP connection cannot be established with the server, the runtime tries again by sending a UDP datagram to the password change server. Set this value to 0 to always use UDP datagrams. The default is 1.

ldap_server
Specifies the location of the LDAP server. The value consists of the host name and the port, separated by a colon. If the port is omitted, it defaults to 389.

rsa_md4_des_compat
Beta versions of Kerberos Version 5 computed the checksum incorrectly for the rsa-md4-des checksum type. Specify 1 to use the old algorithm for compatibility with these beta versions of Kerberos Version 5. The default is to use the new algorithm.

rsa_md5_des_compat
Beta versions of Kerberos Version 5 computed the checksum incorrectly for the rsa-md5-des checksum type. Specify 1 to use the old algorithm for compatibility with these beta versions of Kerberos Version 5. The default is to use the new algorithm.

safe_checksum_type
Specifies the default checksum type for a safe request. The default is **rsa-md5-des**. The specified checksum type must be compatible with the session key encryption type if the checksum uses an encrypted hash. For example, the **rsa-md5-des** checksum type requires a DES session key (such as **des-cbc-crc**) while the **hmac-sha1-des3** checksum type requires a DES3 session key (such as **des3-cbc-sha1**).

use_dns_lookup
Set this value to 1 to use the domain name service (DNS) name server to locate the KDC and to resolve host names. The KDC is located using SRV records, and host names are resolved to realm names using TXT records. The [realms] and [domain_realm] sections are used if the resolution is unsuccessful using the DNS name server. Set this value to 0 to bypass the DNS lookup step. The default is 0. The priority value for SRV records is used to order the service records. Entries with the same priority are randomly selected each time the client needs to contact a Kerberos server.

use_ldap_lookup
Set this value to 1 to use the Lightweight Directory Access Protocol (LDAP) directory to locate the KDC and to resolve host names. The [realms] and [domain_realm] sections are used if the resolution is unsuccessful. Set this value to 0 to bypass the LDAP lookup step. The default is 0. If both LDAP and DNS are used, LDAP is checked first, followed by DNS. The *ldap_server* value must also be specified to use LDAP lookup. LDAP directory entries are randomly selected each time the client needs to contact a Kerberos server.

[realms] section

realm
The *realm* value is a Kerberos realm name. The value is a group definition that defines the Kerberos servers for the realm. Each realm that can be contacted by applications on the local system must have an entry in the [realms] section of the configuration file unless DNS or LDAP lookup is enabled. The group entry consists of one or more occurrences of *kdc*, *admin_server*, and *kpasswd_server* names. Entries are randomly selected each time the client needs to contact a Kerberos server.

The value for each kdc name entry is the host name, the port assigned to the KDC on that system, and the protocol (UDP or TCP), separated by colons. If the port is omitted, it defaults to 88. If the protocol is omitted, the entry can be used with both protocols.

The value for each *admin_server* entry is the host name and the port assigned to the administration service on that system, separated by a colon. If the port is omitted, it defaults to 749. The protocol is always TCP for the administration service.

The value for each *kpasswd_server* entry is the host name, the port assigned to the password service on that system, and the protocol (UDP or TCP), separated by colons. If the port is omitted, it defaults to 464. If the protocol is omitted, the entry can be used with both protocols.

[domain realm] section

hostname

The *hostname* value is a DNS host name. The value is the name of the Kerberos realm that contains the specified host system.

.suffix

The *.suffix* value is the domain portion of a DNS host name. The value is the name of the Kerberos realm that contains host systems in the specified domain. A specific host name definition takes precedence over the domain specification.

If a matching entry is not found for a particular host name, the default is to remove the first label, put what is left in upper case, and use that for the realm name. For example, if no match is found for **host25.krb390.ibm.com**, the realm name is set to KRB390.IBM.COM.

[capath] section

realm

Each *realm* value is a Kerberos realm name and represents the starting point for a request. If the configuration file is not shared between systems, then the only realm that needs to be specified is the local realm. Otherwise, there needs to be a realm definition for each system sharing the configuration file. The value is a group definition that defines the target realms. If multiple trust hops are required to reach the target realm, there are multiple entries defining each of the trust relationships from the local realm to the target realm. If there is a trust relationship between the local realm and the target realm, specify the hop as a period.

Sample /etc/skrb/krb5.conf configuration file

```
[libdefaults]

default_realm=KRB390.IBM.COM
kdc_req_checksum_type = rsa-md5
ap_req_checksum_type = rsa-md5
safe_checksum_type = rsa-md5-des
default_tkt_enctypes = des-cbc-crc,des-cbc-md5
default_tgs_enctypes = des-cbc-crc,des-cbc-md5
kdc_default_options = 0x40000010


[realms]

KRB390.IBM.COM = {
    kdc = dcesec4.krb390.ibm.com:88
    kdc = dcesec7.krb390.ibm.com:88
    admin_server = dcesec4.krb390.ibm.com:749
    kpasswd_server = dcesec4.krb390.ibm.com:464
}

KRB2000.IBM.COM = {
    kdc = sstone1.krb2000.ibm.com:88
    kpasswd_server = sstone1.krb2000.ibm.com:464
}

[domain_realm]

.krb390.ibm.com = KRB390.IBM.COM
.endicott.ibm.com = KRB390.IBM.COM
.krb2000.ibm.com = KRB2000.IBM.COM

[capaths]

KRB390.IBM.COM = {
   KRB2000.IBM.COM = .

}
```

Configuring

Chapter 3. Administering Network Authentication Service

This chapter provides information on administering Network Authentication Service for z/OS.

Realm trust relationships

Network Authentication Service for z/OS supports two types of trust relationships: peer and transitive.

Peer trust

In a peer trust relationship, two realms exchange secret keys so that one realm can create a ticket-granting ticket (TGT) that will be accepted by the other realm. The trust relationship is established by defining a pair of principals in each realm. For example, if a peer trust relationship is to be established between KRB390.IBM.COM and KRB2000.IBM.COM, the following principals must be defined in each realm:

```
krbtgt/KRB390.IBM.COM@KRB2000.IBM.COM
krbtgt/KRB2000.IBM.COM@KRB390.IBM.COM
```

Principal names beginning with **krbtgt/** are reserved for this purpose and must not be used for other purposes.

Transitive trust

In a transitive trust relationship, two realms trust each other if they trust the intermediate realms involved in granting a ticket. Kerberos transitive trust is based upon a hierarchical trust path between the ticket client and the ticket server. The components in the trust path are formed by using periods to separate the realm name into its constituent parts. The common portion between the two realm names forms the top ancestor in the trust path.

For example, if the client is in realm SSTONE1.KRB2000.IBM.COM and the server is in realm DCESEC4.KRB390.IBM.COM, the trust path consists of the following entries:

* SSTONE1.KRB2000.IBM.COM
* KRB2000.IBM.COM
* IBM.COM
* KRB390.IBM.COM
* DCESEC4.KRB390.IBM.COM

If each realm involved in granting the service ticket is present in the trust path, then the ticket is trusted.

When attempting to obtain a service ticket, the Kerberos runtime starts with the client realm and attempts to obtain a TGT for the server realm. If the KDC for the client realm is unable to satisfy the request because there is no peer trust relationship between the client and server realms, the Kerberos runtime attempts to obtain a TGT to a realm that is in the trust path between the client and the server realms. As soon as it obtains a TGT to an intermediate realm, it tries to obtain a TGT to the server realm from the intermediate KDC. This process is repeated until either a server realm TGT is obtained or all of the intermediate realms have been tried.

When setting up transitive trust, a peer trust relationship should be defined between each realm and a common ancestor realm in the hierarchy. For example, consider the following realm tree:

* IBM.COM (Top node)
* KRB390.IBM.COM (First level node)
* DCESEC4.KRB390.IBM.COM (Second level node)
* DCESEC7.KRB390.IBM.COM (Second level node)

Administering

- KRB2000.IBM.COM (First level node)
- SSTONE1.KRB2000.IBM.COM (Second level node)
- SSTONE2.KRB2000.IBM.COM (Second level node)

A fully-connected hierarchy has, at a minimum, the following peer trust relationships:

- DCESEC4.KRB390.IBM.COM <--> KRB390.IBM.COM
- DCESEC7.KRB390.IBM.COM <--> KRB390.IBM.COM
- KRB390.IBM.COM <--> IBM.COM
- KRB2000.IBM.COM <--> IBM.COM
- SSTONE1.KRB2000.IBM.COM <--> KRB2000.IBM.COM
- SSTONE2.KRB2000.IBM.COM <--> KRB2000.IBM.COM

An additional peer trust relationship can be defined to shorten the transited path between the lower layer of realms:

- KRB390.IBM.COM <--> KRB2000.IBM.COM

Do not include the top node in the trust hierarchy if there is no need to obtain tickets for that realm. In the above example, IBM.COM could be omitted and the peer trust relationships would then be the following:

- DCESEC4.KRB390.IBM.COM <--> KRB390.IBM.COM
- DCESEC7.KRB390.IBM.COM <--> KRB390.IBM.COM
- KRB390.IBM.COM <--> KRB2000.IBM.COM
- SSTONE1.KRB2000.IBM.COM <--> KRB2000.IBM.COM
- SSTONE2.KRB2000.IBM.COM <--> KRB2000.IBM.COM

Similarly, a lopsided trust hierarchy can be defined. Suppose there is no need to obtain tickets to the IBM.COM or KRB2000.IBM.COM realms. The peer trust relationships would then be the following:

- DCESEC4.KRB390.IBM.COM <--> KRB390.IBM.COM
- DCESEC7.KRB390.IBM.COM <--> KRB390.IBM.COM
- SSTONE1.KRB2000.IBM.COM <--> KRB390.IBM.COM
- SSTONE2.KRB2000.IBM.COM <--> KRB390.IBM.COM

When defining the transitive trust hierarchy, it is important to remember that the peer trust relationships must be symmetric (tickets can be obtained when traversing the trust path in either direction) and each realm in a peer trust relationship must be capable of either providing a TGT for the destination realm or for an intermediate realm which is further along the trust path between the client and the server realms.

Passwords

The **krbtgt** principals are used for ticket-granting tickets. When using the SAF database, KERBDFLT is used for your local realm (**krbtgt**/*local-realm@local-realm*) and the RDEFINE global name (*/.../realm-name/principal-name*) is used for peer-to-peer connections. In this respect, each pair of peer-to-peer principals is repeated in the foreign registries and must have the same passwords.

For example, if you are connecting REALMA and REALMB using the SAF database implementation, you would have the following RDEFINE statements in *both* REALMA and REALMB:

```
RDEFINE REALM /.../REALMA/KRBTGT/REALMB KERB(PASSWORD(PSWD1))
RDEFINE REALM /.../REALMB/KRBTGT/REALMA KERB(PASSWORD(PSWD2))
```

For the NDBM database, the **krbtgt**/REALMB@REALMA principal is used by the REALMA KDC to grant a ticket to REALMB. Similarly, the **krbtgt**/REALMA@REALMB principal is used by the REALMB KDC to grant a ticket to REALMA. These principals must be added to the NDBM database by the **kadmin** command to establish peer trust.

A password can be any value as long as you specify the same password each time you define the principal.

Cache files

The Kerberos runtime stores network credentials in cache files located in **/var/skrb/creds**. These files should be erased periodically. There are several ways to do this:

- Use a temporary file system mounted at **/var/skrb/creds**. This results in all the credentials cache files being deleted each time the system is restarted.
- Erase all of the files in **/var/skrb/creds** when the **/etc/rc** initialization script is run. This results in all of the credentials cache files being deleted each time the system is restarted.
- Set up a **cron** job to run the **kdestroy** command with the **-e** option. This results in the deletion of only expired credentials cache files. This is the preferred method for managing the credentials cache files. The **cron** job should run with UID 0 so that it can delete the cache files.

Audit

SMF Type 80 records are created for login requests (Kerberos initial ticket requests). Both success and failure events can be logged as determined by the SKDC_LOGIN_AUDIT environment variable. The event code is 68 and the record includes relocate sections 333 (Kerberos principal name), 334 (request source), and 335 (KDC error code).

The Kerberos principal is stored as a global name (**/.../realm-name/principal-name**) and not as a Kerberos name (**principal-name@realm-name**). This is done to avoid code page problems caused by the at-sign variant character. If the request is received through TCP/IP, the request source is the network address (*nnn.nnn.nnn.nnn:ppppp*). If the request is received through Program Call, the request source is the system user ID of the requester The KDC error code is a value between 0 and 127.

KDC error codes

The possible KDC error codes are:

0   No error

1   Client entry is expired

2   Server entry is expired

3   Protocol version is not supported

4   Client key is encrypted in an old master key

5   Server key is encrypted in an old master key

6   Client is not defined in the security registry

7   Server is not defined in the security registry

8   Principal is not unique in the security registry

9   No key is available for the principal

10   Ticket is not eligible for postdating

11   Ticket is never valid

12   Request rejected due to KDC policy

13   Request option is not supported

14   Encryption type is not supported

15   Checksum type is not supported

Administering

16	Preauthentication type is not supported
17	Transited data type is not supported
18	Client account is revoked
19	Server account is revoked
20	TGT is revoked
21	Client account is not valid yet
22	Server account is not valid yet
23	Password is expired
24	Preauthentication failed
25	Preauthentication required
26	Supplied authentication ticket is not for the requested server
27	Server requires user-to-user protocol
31	Decryption integrity check failed
32	Ticket is expired
33	Ticket is not valid yet
34	Request is a replay of a previous request
35	Supplied authentication ticket is not for the current realm
36	Ticket and authenticator do not match
37	Clock skew is too great
38	Incorrect network address
39	Protocol version mismatch
40	Invalid message type
41	Message stream has been modified
42	Message is out of order
44	Key version is not available
45	Service key is not available
46	Mutual authentication failed
47	Incorrect message direction
48	Alternative authentication method required
49	Incorrect message sequence number
50	Inappropriate checksum type
60	Generic error detected
61	Field is too long

Security server operator commands

The operator commands in this section are supported by the Network Authentication Service for z/OS security server (SKRBKDC started task).

All principal names and passwords should consist only of characters from the POSIX portable character set, but should not include any variant characters, such as brace, bracket, or currency symbols. (See *z/OS: Security Server Network Authentication Service Programming* for a table of the POSIX characters.) In addition, principal names should not contain blanks or the commercial ″at″ sign (@).

If for some reason you need to use blanks in a principal name as part of a command-line argument, enclose the whole name in quotation marks.

If you have a need to use principal names or passwords that contain characters not in the POSIX portable character set (in other words, for national language reasons), be sure that the LANG value for the SKRBKDC started task is set to a code page that translates the national language characters to those that Resource Access Control Facility (RACF) can use. This applies to z/OS clients as well.

F SKRBKDC,parameters

Format
Causes a command to be executed by the security server. This command is the same as MODIFY SKRBKDC.

```
F SKRBKDC,parameters
```

Options

DISABLE ADMIN
 Disables the Kerberos administration service. No changes can be made to the Kerberos database while the administration service is disabled.

DISPLAY ADMIN
 Displays the current status of the Kerberos administration service. This option may be abbreviated D ADMIN.

DISPLAY CREDS,_owner_**,**_date_
 Displays all credentials data space allocations for a user that were created before the specified date. All data space allocations for a user are displayed if the date is omitted. All data space allocations are displayed if no owner is specified. A date can be specified without specifying an owner by using two successive commas. A maximum of 252 allocations can be displayed. The date is specified as *yyyy.ddd*.

 This command can be abbreviated as D CREDS,*owner,date*.

DISPLAY CRYPTO
 Displays the available encryption types, whether hardware cryptographic support is available, and whether the encryption type can be used for application data. This option may be abbreviated D CRYPTO.

DISPLAY LEVEL
 Displays the current service level of the Kerberos security server. This option may be abbreviated D LEVEL.

DISPLAY NETWORK
 Displays the status of the network interfaces. The SKDC_NETWORK_POLL environment variable determines how often the Kerberos security server updates the network interface status. This option may be abbreviated D NETWORK.

DISPLAY PROP
 Displays the status of database propagation. The current update sequence number is displayed for each Kerberos security server in the realm that participates in database propagation. This information is available only on the primary security server for the realm. This option may be abbreviated D PROP.

DISPLAY XCF
 Displays the status of all instances of the SKRBKDC started task in the sysplex.

Administering

This command can be abbreviated as D XCF.

DEBUG ON

Enables debug mode.

DEBUG OFF

Disables debug mode.

DEBUG *subcomponent.level*,*subcomponent.level*,**...**

Sets the debug level for one or more subcomponents. All subcomponents can be changed by specifying an asterisk for the subcomponent. The debug level must be an integer between 0 and 9. All debug messages are suppressed for a subcomponent when its debug level is 0. The initial debug settings are obtained from the SKRBKDC environment variable file (**/etc/skrb/home/kdc/envar**).

For example, `F SKRBKDC,DEBUG *.1,KRB_KDC.8`

This sets debug level to 1 for all subcomponents and then sets the debug level to 8 for the KRB_KDC subcomponent.

ENABLE ADMIN

Enables the Kerberos administration service. The administration service can be enabled only if the Kerberos database supports the administration function.

PROP *secondary-name*

Initiates a full database propagation to the specified secondary Kerberos security server. This command can be issued only on the primary Kerberos security server. The secondary security server must be defined in the **/etc/skrb/home/kdc/kpropd.acl** configuration file.

Usage

For the option *subcomponent.level,subcomponent.level,...*, all subcomponents can be changed by specifying an asterisk for the subcomponent. The debug level must be an integer between 0 and 9. All debug messages are suppressed for a subcomponent when its debug level is 0. The initial debug settings are obtained from the SKRBKDC environment variable file,**/etc/skrb/home/kdc/envar**.

Examples

To enable debug mode:

`F SKRBKDC,DEBUG ON`

To disable debug mode:

`F SKRBKDC,DEBUG OFF`

To set the debug level for one or more subcomponents:

`F SKRBKDC,DEBUG *.1,KRB_KDC.8`

This sets the debug level to 1 for all subcomponents and then sets the debug level to 8 for the KRB_KDC subcomponent.

MODIFY SKRBKDC,parameters

Format

MODIFY SKRBKDC,*parameters*

Options

Same as the F SKRBKDC,*parameters* command.

Usage

Same as F SKRBKDC,*parameters*.

Examples

Same as F SKRBKDC, *parameters*.

| **CTRACE debugging utility**
| Component trace records can be captured using either in-storage wrap buffers or an external writer. The
| component trace records contain the same information as the debug messages. The component trace
| options parameter can be used to set or modify the initial subcomponent debug levels. The MODIFY
| SKRBKDC,DEBUG command can then be used to change the subcomponent levels once the trace has
| been started.

| The following commands start the component trace (CTIKDC00 is a sample parmlib member):
| ```
| TRACE CT,WTRSTART=SKRBWTR
| TRACE CT,ON,COMP=SKRBKDC,PARM=CTIKDC00
| ```

| The following commands stop the component trace:
| ```
| TRACE CT,OFF,COMP=SKRBKDC
| TRACE CT,WTRSTOP=SKRBWTR
| ```

| IPCS can be used to format and display the component trace records that were written to the trace
| datasets or contained in a dump dataset. The trace entry type codes are the same as the subcomponent
| names.

P SKRBKDC

Format
```
P SKRBKDC
```

Causes an orderly shutdown of the security server. This command is the same as STOP SKRBKDC.

There are no parameters (options).

STOP SKRBKDC

Format
```
STOP SKRBKDC
```

| # Kerberos administration server

| The Kerberos administration server is provided as part of the SKRBKDC started task. The administration
| capabilities are dependent upon the Kerberos database selected by the SKDC_DATABASE environment
| variable. Communication between the administration client and the administration server uses a variant of
| Sun RPC with GSS-API authentication. The **kadmin** command is provided to perform Kerberos
| administration functions. In addition, the **kadm5_*** API is provided for use by application programs.

| z/OS Network Authentication Service now provides an administration server for the NDBM database.
| Administration for the SAF database is performed using the native system commands. The **kadmin**
| command and the **kadm5_*** API can be used with any Kerberos administration server that is compatible
| with Version 2 of the MIT Kerberos administration protocol.

| ## Administration privileges

| Authorization controls are provided through the **/etc/skrb/home/kdc/kadm5.acl** file. This file controls the
| Kerberos administration privileges. Each line represents a single administration access definition, has a
| maximum length of 255 characters, and is assumed to be in the code page specified by the LANG
| environment variable. Comment lines start with a semi-colon and blank lines are ignored. Each line
| consists of 2 fields: the client principal name and the privileges granted. The order of the lines in the file is
| important because the search stops as soon as a match is found for the principal making an administration
| request.

Administering

The client principal name can contain the following wildcards:

- ? represents a single character
- * represents zero or more characters
- Paired [ ] represent any one of the characters between the brackets.

The following administration privileges are defined. Use lowercase letters to define the granted privileges (any privilege not listed is denied) and use uppercase letters to define the denied privileges (any privilege not listed is granted). Do not mix uppercase and lowercase letters in the same definition.

a	ADD is granted
A	ADD is denied
c	CHANGEPW is granted
C	CHANGEPW is denied
d	DELETE is granted
D	DELETE is denied
g	GET is granted (this may also be specified as i)
G	GET is denied (this may also be specified as I)
l	LIST is granted
L	LIST is denied
m	MODIFY is granted
M	MODIFY is denied
s	SETKEY is granted
S	SETKEY is denied
*	All privileges are granted

Administration RPC functions

- CHPASS_PRINCIPAL - Change the password for a principal.

  This function requires CHANGEPW authority or the principal entry must be the authenticated client entry. The new password is subject to the minimum password lifetime, minimum password classes, and minimum password length rules in effect for the Kerberos database. Depending upon the database implementation, existing keys are deleted when the password is changed.

- CHPASS_PRINCIPAL3 - Change the password for a principal.

  This function is the same as the CHPASS_PRINCIPAL function with the addition that the key types and salt types can be specified. Depending upon the database implementation, existing keys can either be retained or deleted when the password is changed.

- CHRAND_PRINCIPAL - Generate random keys for a principal.

  This function requires CHANGEPW authority or the principal entry must be the authenticated client entry. The password change is subject to the minimum password lifetime rule in effect for the Kerberos database. Depending upon the database implementation, existing keys are deleted when the random keys are generated.

- CHRAND_PRINCIPAL3 - Generate random keys for a principal.

  This function is the same as the CHRAND_PRINCIPAL function with the addition that the key types and salt types can be specified. Depending upon the database implementation, existing keys can either be retained or deleted when the random keys are generated.

- CREATE_POLICY - Create an administration policy.

This function requires ADD authority. The maximum length of a policy name is 128 characters. The name must consist of displayable graphic characters as determined by the locale in effect for the administration server. The name may not contain the backslash character.

The following mask flags are supported:
- KADM5_POLICY - Policy name supplied (required)
- KADM5_PW_MIN_LIFE - Minimum password lifetime supplied
- KADM5_PW_MAX_LIFE - Maximum password lifetime supplied
- KADM5_PW_MIN_LENGTH - Minimum password length supplied
- KADM5_PW_MIN_CLASSES - Minimum number of password classes supplied
- KADM5_PW_HISTORY_NUM - Number of password history entries supplied

- CREATE_PRINCIPAL - Create a principal.

  This function requires ADD authority. The maximum length of a principal name is 235 characters, including the realm name and separator. The name must consist of displayable graphic characters as determined by the locale in effect for the administration server. The name may not contain the backslash or commercial at-sign characters.

  The following principal attributes are supported:
  - KRB5_KDB_DISALLOW_POSTDATED - Disallow post-dated tickets
  - KRB5_KDB_DISALLOW_FORWARDABLE - Disallow forwardable tickets
  - KRB5_KDB_DISALLOW_TGT_BASED - Disallow TGT-based tickets
  - KRB5_KDB_DISALLOW_RENEWABLE - Disallow renewable tickets
  - KRB5_KDB_DISALLOW_PROXIABLE - Disallow proxiable tickets
  - KRB5_KDB_DISALLOW_DUP_SKEY - Disallow duplicate session keys
  - KRB5_KDB_DISALLOW_ALL_TIX - Disallow all tickets
  - KRB5_KDB_REQUIRES_PRE_AUTH - Requires preauthentication
  - KRB5_KDB_REQUIRES_HW_AUTH - Requires hardware authentication
  - KRB5_KDB_REQUIRES_PWCHANGE - Requires password change
  - KRB5_KDB_DISALLOW_SVR - Disallow service tickets
  - KRB5_KDB_PWCHANGE_SERVICE - This is a password change service

  The following mask flags are supported:
  - KADM5_ATTRIBUTES - Principal attributes supplied
  - KADM5_KVNO - Initial key version number supplied
  - KADM5_MAX_LIFE - Maximum ticket lifetime supplied
  - KADM5_MAX_RLIFE - Maximum renewable ticket lifetime supplied
  - KADM5_POLICY - Policy name supplied
  - KADM5_PRINC_EXPIRE_TIME - Account expiration time supplied
  - KADM5_PRINCIPAL - Principal name supplied (required)
  - KADM5_PW_EXPIRATION - Password expiration time supplied
  - KADM5_TL_DATA - Tagged data supplied (the tagged data type must be greater than 255)

- CREATE_PRINCIPAL3 - Create a principal.

  This function is the same as the CREATE_PRINCIPAL function with the addition that the key types and salt types can be specified.

- DELETE_POLICY - Delete an administration policy.

  This function requires DELETE authority. An error is returned if the policy is still refered to by Kerberos principals.

- DELETE_PRINCIPAL - Delete a principal.

  This function requires DELETE authority.

Administering

- GET_POLICY - Get an administration policy.

  This function requires GET authority.
- GET_POLS - List the administration policy names.

  This function requires LIST authority. An error is returned if there are more than 1000 matches for the search expression.
- GET_PRINCIPAL - Get a principal.

  This function requires GET authority.
- GET_PRINCS - List the principal names.

  This function requires LIST authority. An error is returned if there are more than 1000 matches for the search expression.
- GET_PRIVS - Get administration privileges for the authenticated client.

  This function can be issued by any client. The privileges are obtained by matching the authenticated client name to entries in the **/etc/skrb/home/kdc/kadm5.acl** control file.
- MODIFY_POLICY - Modify an administration policy.

  This function requires MODIFY authority.

  The following mask flags are supported:
  – KADM5_PW_MIN_LIFE - Minimum password lifetime supplied
  – KADM5_PW_MAX_LIFE - Maximum password lifetime supplied
  – KADM5_PW_MIN_LENGTH - Minimum password length supplied
  – KADM5_PW_MIN_CLASSES - Minimum number of password classes supplied
  – KADM5_PW_HISTORY_NUM - Number of password history entries supplied
- MODIFY_PRINCIPAL - Modify a principal.

  This function requires MODIFY authority. Only the maximum ticket lifetime and the maximum renewable ticket lifetime values can be modified for protected principals (the architected Kerberos principals for the realm).

  The following principal attributes are supported:
  – KRB5_KDB_DISALLOW_POSTDATED - Disallow post-dated tickets
  – KRB5_KDB_DISALLOW_FORWARDABLE - Disallow forwardable tickets
  – KRB5_KDB_DISALLOW_TGT_BASED - Disallow TGT-based tickets
  – KRB5_KDB_DISALLOW_RENEWABLE - Disallow renewable tickets
  – KRB5_KDB_DISALLOW_PROXIABLE - Disallow proxiable tickets
  – KRB5_KDB_DISALLOW_DUP_SKEY - Disallow duplicate session keys
  – KRB5_KDB_DISALLOW_ALL_TIX - Disallow all tickets
  – KRB5_KDB_REQUIRES_PRE_AUTH - Requires preauthentication
  – KRB5_KDB_REQUIRES_HW_AUTH - Requires hardware authentication
  – KRB5_KDB_REQUIRES_PWCHANGE - Requires password change
  – KRB5_KDB_DISALLOW_SVR - Disallow service tickets
  – KRB5_KDB_PWCHANGE_SERVICE - This is a password change service

  The following mask flags are supported:
  – KADM5_ATTRIBUTES - Principal attributes supplied
  – KADM5_FAIL_AUTH_COUNT - Failed authentication count supplied
  – KADM5_KVNO - Key version number supplied
  – KADM5_MAX_LIFE - Maximum ticket lifetime supplied
  – KADM5_MAX_RLIFE - Maximum renewable ticket lifetime supplied
  – KADM5_POLICY - Policy name supplied

| – KADM5_POLICY_CLR - No policy is associated with the principal
| – KADM5_PRINC_EXPIRE_TIME - Account expiration time supplied
| – KADM5_PW_EXPIRATION - Password expiration time supplied
| – KADM5_TL_DATA - Tagged data supplied (the tagged data type must be greater than 255)
| • RENAME_PRINCIPAL - Rename a principal.

This function requires ADD and DELETE authority.

| • SETKEY_PRINCIPAL - Set the encryption keys for a principal.

This function requires SETKEY authority. The password change is subject to the minimum password lifetime rule in effect for the Kerberos database. Depending upon the database implementation, existing keys are deleted when the new keys are set.

| • SETKEY_PRINCIPAL3 - Set the encryption keys for a principal.

This function is the same as the SETKEY_PRINCIPAL function with the addition that the salt types can be specified. Depending upon the database implementation, existing keys can either be retained or deleted when the new keys are set.

Kerberos database propagation

The Kerberos security server supports two types of security registries: SAF and NDBM. The SAF registry stores Kerberos information in the z/OS system security database and uses SAF services to interface with the external security manager. The external security manager is responsible for database propagation between systems in the same sysplex and between systems in different sysplexes. Kerberos database propagation is not used in this environment and does not need to be configured.

The NDBM registry uses the POSIX database support provided by Unix System Services. The database files are located in the **/var/skrb/krb5kdc** directory. Kerberos database propagation is used to synchronize these files between systems in the same sysplex and between systems in different sysplexes. The file system containing the **/var/skrb/krb5kdc** directory must be large enough to contain two copies of the registry database files plus a complete database dump file.

The Kerberos security server supports two database propagation protocols: full replacement and individual updates. The full replacement protocol sends the entire Kerberos database to each secondary Kerberos security server. This is the only propagation protocol supported by MIT Kerberos. The propagation occurs at timed intervals specified by the SKDC_KPROP_INTERVAL environment variable. A propagation does not occur if there have been no changes to the database since the last database propagation.

The individual update protocol sends just the database updates to each secondary Kerberos security server. The propagation occurs as each change is made to the database. The primary security server keeps track of the update level of each secondary security server and holds pending updates for an unavailable secondary server until the server becomes available. The individual update protocol should be used if it is supported by the primary KDC and the secondary KDC, since it performs much better than the full replacement protocol for large databases.

The **/etc/skrb/home/kdc/kpropd.acl** configuration file contains an entry for each Kerberos security server in the realm, and it specifies the role assigned to each of the servers. Each line consists of three fields, blank lines are ignored,comment lines are indicated by a semi-colon in the first position, and the file is assumed to be in the code page specified by the LANG environment variable. The maximum line length is 255 characters. The first field specifies the host name and optional port, separated by a colon, of a Kerberos security server. Port 754 is used for database propagation if a port is not specified either in **kpropd.acl** or for the **krb5_prop** service. The host name is used as the name of the Kerberos security server in the propagation status database and is converted to lowercase. The second field specifies the role assigned to that security server. The third field specifies the encryption type for the session key in the service ticket. The encryption type field is optional and the default encryption type list obtained from the Kerberos configuration file is used if the field is omitted.

Administering

The roles are:

- Primary - This is the primary security server for the realm. It owns the Kerberos registry database and sends updates to the other security servers in the realm.

- Replace - This is a secondary security server that receives updates by replacing the entire registry database as part of each propagation cycle. The database propagation contains principal policy and password history information. The secondary KDC must be at the MIT Kerberos 1.2.2 level or later.

- Compat - This is a secondary security server that receives updates by replacing the entire registry database as part of each propagation cycle. The database propagation does not contain principal policy or password history information. This propagation format is supported by MIT Kerberos 1.2.1 and earlier. Note that the principal policy and password history information is lost if a database created using this propagation method is later used by the primary KDC for the realm.

- Update - This is a secondary security server that receives individual database updates.

- Manual - This is a secondary security server that receives updates manually when the security server PROP command is issued.

The **/etc/skrb/home/kdc/kpropd.acl** configuration file must exist on the primary system and on each secondary system if database propagation is going to be used. The KDC assumes it is the only KDC in the realm if this file is not found. The host names specified in the **kpropd.acl** file must be valid DNS names and each must be the primary name assigned to its host system. The KDC locates its own entry by using DNS services to translate the host name returned by the **gethostname()** function and then by searching for the translated name in the configuration file.

The **kpropd.acl** file on the primary system must contain an entry for each KDC in the realm, including the primary KDC. These entries define the secondary servers to receive database propagations from the primary KDC.

The **kpropd.acl** file on the secondary systems requires only the entry for the primary KDC, although other entries can be specified. A secondary KDC accepts updates only from servers identified in its **kpropd.acl** configuration file. The secondary KDC checks for an authorized server by using DNS services to translate the remote IP address for a connection to a host name and then searching for the host name in the configuration file.

The KDC identified as the primary KDC provides Kerberos administration services by listening for requests on the administration and password change ports. The primary KDC does not listen for requests on the propagation port.

A KDC identified as a secondary KDC doesl not provide Kerberos administration services. It does not listen for requests on the administration or password change ports. A secondary KDC listens for propagation requests on the propagation port.

The Kerberos registry must contain a service principal for each system with a KDC, including the primary KDC. The principal name is **host/**_primary-host-name_ where _primary-host-name_ is the primary DNS name for the system. For example, if a KDC is running on system **dcesec4.krb390.ibm.com**, the Kerberos registry must contain the principal **host/dcesec4.krb390.ibm.com**.

Each system running a secondary KDC must have a **/var/skrb/krb5kdc/kpropd.ktf** key table file. This key table contains the host key for that system and is created using the **kadmin ktadd** subcommand. For example, if a secondary KDC is running on system **dcesec7.krb390.ibm.com**, the following **kadmin** commands should be issued on the **dcesec7.krb390.ibm.com** system:

```
addprinc host/dcesec7.krb390.ibm.com
ktadd -k /var/skrb/krb5kdc/kpropd.ktf host/dcesec7.krb390.ibm.com
```

The following is a sample **kpropd.acl** for a Kerberos realm containing three Kerberos security servers. Systems **dcesec4.krb390.ibm.com** and **dcesec7.krb390.ibm.com** are z/OS systems in the same

sysplex, while system **dcecpt.mitkrb.ibm.com** is an AIX® system running MIT Kerberos. The KDC on
dcesec4.krb390.ibm.com is the primary KDC for the realm. This sample configuration file can be found in
/usr/lpp/skrb/examples/kpropd.acl:

```
; Sample kpropd.acl configuration file
;
; Host                        Role        Encryption type
; ----                        ----        ---------------
  dcesec4.krb390.ibm.com:754  Primary
  dcesec7.krb390.ibm.com:754  Update
  dcecpt.mitkrb.ibm.com:754   Replace     des-cbc-crc
```

The **kpropd.acl** file may be changed while the Kerberos security server is running and the changes will be
picked up at the next propagation interval. However, the role of a security server may not be changed from
primary to secondary or from secondary to primary while the security server is running.

Setting up a secondary KDC

A new secondary KDC is added to the realm by performing the following steps:

1. Use the **kdb5_ndbm stash** command to create the database master key stash file on the secondary
   system.
2. Create the **/var/skrb/krb5kdc/kpropd.ktf** key table on the secondary system. Use the **kadmin ktadd**
   subcommand to add an entry for the secondary system host principal. The **kadmin** command must
   either be issued on the secondary system or the **kpropd.ktf** file must be copied to the secondary
   system.
3. Create the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the secondary system. The primary
   KDC system for the realm must be listed. The secondary KDC systems can also be included to make
   it easier to move the primary KDC in the future.
4. Start the **kpropd** command on the secondary system. The command waits to receive a database
   propagation from the primary KDC.
5. Edit the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the primary system. Add the new
   secondary system and specify **Manual** for the role.
6. Use the security server PROP command to send the database to the waiting **kpropd** command.
7. Start the SKRBKDC started task on the new secondary system after the **kpropd** command has
   completed.
8. Edit the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the primary system. Change the role of
   the secondary system to **Update**, **Replace**, or **Compat**. You should always specify **Update** if the
   secondary security server supports the update propagation protocol.

Moving the primary KDC to another system

The roles of the primary KDC and a secondary KDC can be swapped by performing the following steps:

1. Use the **kadmin ktadd** command to create the **/var/skrb/krb5kdc/kpropd.ktf** key table on the primary
   system if it does not already exist. This key table is used by a secondary KDC when it receives a
   database propagation from the primary KDC. Since the primary KDC is going to become a secondary
   KDC, it now needs this key table.
2. Use the security server DISABLE ADMIN command to freeze the database on the primary system.
3. Use the security server PROP command to send the current database to the secondary KDC.
4. Shut down the old and the new primary security servers.
5. Update the **/etc/skrb/home/kdc/kpropd.acl** control files and change the role of the old primary KDC to
   Compat, **Replace** or **Update** and change the role of the new primary KDC to **Primary**.
6. Restart both security servers.

Interoperability with MIT Kerberos

A z/OS security server can be a primary KDC or a secondary KDC in the same realm with MIT Kerberos (and compatible) security servers. The MIT Kerberos server must be at release 1.2.2 or later, if the z/OS security server is the primary KDC and the **Replace** role is used. The MIT Kerberos server must be at release 1.0 or later if the z/OS security server is the primary KDC and the **Compat** role is used. The MIT Kerberos server must be at release 1.0 or later if the z/OS security server is a secondary KDC.

If the z/OS security server is the primary KDC for the realm, then each MIT Kerberos security server must be listed in the **kpropd.acl** configuration file with the **Replace** or **Compat** propagation protocol. The **/etc/inetd.conf** configuration file on the secondary system must be updated to start the **kpropd** command when a propagation request is received from the primary KDC.

If the z/OS security server is a secondary KDC for the realm with an MIT Kerberos security server as the primary KDC, then the **Replace** protocol is always used. There is no need to update **/etc/inetd.conf** on the z/OS system since the SKRBKDC started task listens for database propagation requests. The **kpropd** command is used on the z/OS system to receive the initial database propagation before starting the SKRBKDC started task for the first time.

Refer to the MIT documentation for more information on setting up MIT Kerberos.

Part 2. Reference

This Reference section contains:

- Commands for Network Authentication Service for z/OS
- Status Codes for Network AuthenticationService for z/OS
- Messages for Network Authentication Service for z/OS

Chapter 4. Commands

This chapter presents Network Authentication Service for z/OS commands in alphabetical order. It provides the format, options, usage, and examples for each command.

The commands are installed in **/usr/lpp/skrb/bin**. In order to use these commands, you must update the PATH environment variable to place **/usr/lpp/skrb/bin** before **/bin** in the search order or else you must use the fully-qualified command name.

kadmin

Administers the Kerberos database.

Format

```
kadmin [-r realm] [-p principal] [-k keytab] [-w password] [-A] [-e]
```

Options

-r *realm*
> Specifies the Kerberos administration realm. If this option is not specified, the realm is obtained from the principal name. This option is meaningful only if the administration server supports multiple realms.

-p *principal*
> Specifies the administrator principal. If this option is not specified, the string **/admin** is appended to the principal name obtained from the default credentials cache. If there is no credentials cache, the string **/admin** is appended to the name obtained from the USER environment variable, or, if the USER environment variable is not defined, it is appended to the name obtained from the **getpwuid()** function. The local realm is used if an explicit realm is not part of the principal name.

-k *keytab*
> Specifies the key table containing the password for the administrator principal. The user is prompted to enter the password if neither the **-k** nor the **-w** option is specified. When using **-k**, the principal name is *host/host-name* unless the **-p** option is specified. The *host-name* is the primary host name for the local system.

-w *password*
> Specifies the password for the administrator principal. The user is prompted to enter the password if neither the **-k** nor the **-w** option is specified.

-A Specifies that the initial ticket used by the **kadmin** command does not contain a list of client addresses. If this option is not specified, the ticket contains the local host address list. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

-e Echoes each command line to **stdout**. This is useful when **stdout** is redirected to a file.

Usage

The **kadmin** command is used to manage entries in the Kerberos database. You are prompted to enter one or more subcommands. Each subcommand has a maximum length of 1023 characters. To enter a subcommand using multiple input lines, end each line to be continued with a backslash (\) character.

The **kadmin** command can be used with any Kerberos administration server supporting Version 2 of the Kerberos administration protocol. The z/OS Kerberos security server provides Kerberos administration server support for the NDBM database but not the SAF database (the normal system security commands are used to administer the SAF database).

Commands

Subcommand options start with a minus (-) character and principal attributes start with a plus (+) character or a minus (-) character. This means that principal and policy names must not start with these characters. In addition, since the backslash (\) character is used to indicate continuation and the single quote (') and double quote (") characters are used as delimiters, a name or password must not contain any of these characters. The **kadmin** command imposes no other restrictions on the characters used in names or passwords, although it is recommended that you do not use any of the EBCDIC variant characters. The Kerberos administration server may impose additional restrictions.

The following encryption types are supported by the **kadmin** command. An error is returned if an encryption type is specified that is not supported by the administration server.
- des-cbc-crc - DES encryption with 32-bit CRC checksum
- des-cbc-md4 - DES encryption with MD4 checksum
- des-cbc-md5 - DES encryption with MD5 checksum
- des-hmac-sha1 - DES encryption using key derivation and SHA1 checksum
- des3-cbc-sha1 - DES3 encryption using key derivation and SHA1 checksum

The following salt types are supported by the **kadmin command**. An error is returned if a salt type is specified that is not supported by the administration server.
- normal - Kerberos V5 salt using both the principal and realm names
- norealm - Kerberos V5 salt using just the principal name
- onlyrealm - Kerberos V5 salt using just the realm name
- afs3 - AFS® V3 salt
- v4 - Kerberos V4 salt

Time units

Dates are displayed as *day-of-week month day-of-month hour:minute:second timezone year* using the local timezone as specified by the TZ environment variable. Durations are displayed as *days-hours:minutes:seconds*.

The **kadmin** command supports a number of date and duration formats, such as:

```
"15 minutes"
"7 days"
"1 month"
"2 hours"
"400000 seconds"
"next year"
"this Monday"
"next Monday"
yesterday
tomorrow
now
fortnight
"3/31/1992 10:00:07 PST"
"January 23, 2007 10:05pm"
"22:00 GMT"
2000-1-28
17-Jun.-2001
"28 Feb 2002"
```

The date specification must be enclosed in double quotes if it contains spaces. You cannot use a number without a unit (for example, "60 seconds" is correct but "60" is incorrect). If an explicit timezone is not given as part of the date specification, the local timezone is used. The date specification is not case sensitive; it may be entered using uppercase or lowercase characters. The year must be between 1970 and 2037. Two-digit years may be used with 0-37 representing 2000-2037 and 70-99 representing 1970-1999. The unit specification can be either singular or plural (for example, "month" and "months" are both allowed).

A date may be specified as an absolute or a relative value. If a relative value is given, the current date is added to form the date. An interval may also be specified as an absolute or a relative value. If an absolute value is given, the current date is subtracted to form the interval.

Here are the values that are acceptable for various ways of expressing time:

Units of time

year, month, fortnight, week, day, hour, minute, min, second, sec

Relative time

tomorrow, yesterday, today, now, last, this, next, ago

12-hour time delimiters

am, pm

Months

january, jan, february, feb, march, mar, april, apr, may, june, jun, july, jul, august, aug, september, sept, sep, october, oct, november, nov, december, dec

Days sunday, sun, monday, mon, tuesday, tues, tue, wednesday, wednes, wed, thursday, thurs, thur, thu, friday, fri, saturday, sat

In addition, these time zones are acceptable:

Table 7. Time zones recognized by the **kadmin** *command*

Name	Description	Offset in Minutes	Daylight Savings Time Adjustment
GMT	Greenwich Mean	0	No
UT	Universal (Coordinated)	0	No
UTC	Universal (Coordinated)	0	No
WET	Western European	0	No
BST	British Summer	0	Yes
WAT	West Africa	60 West	No
AT	Azores	120 West	No
NFT	Newfoundland	210 West	No
NST	Newfoundland Standard	210 West	No
NDT	Newfoundland Daylight	210 West	Yes
AST	Atlantic Standard	240 West	No
ADT	Atlantic Daylight	240 West	Yes
EST	Eastern Standard	300 West	No
EDT	Eastern Daylight	300 West	Yes
CST	Central Standard	360 West	No
CDT	Central Daylight	360 West	Yes
MST	Mountain Standard	420 West	No
MDT	Mountain Daylight	420 West	Yes
PST	Pacific Standard	480 West	No
PDT	Pacific Daylight	480 West	Yes
YST	Yukon Standard	540 West	No
YDT	Yukon Daylight	540 West	Yes
HST	Hawaii Standard	600 West	No

Commands

Table 7. Time zones recognized by the **kadmin** *command (continued)*

Name	Description	Offset in Minutes	Daylight Savings Time Adjustment
HDT	Hawaii Daylight	600 West	Yes
CAT	Central Alaska	600 West	No
AHST	Alaska-Hawaii Standard	600 West	No
NT	Nome	660 West	No
IDLW	International Date Line West	720 West	No
CET	Central European	60 East	No
MET	Middle European	60 East	No
MEWT	Middle European Winter	60 East	No
MEST	Middle European Summer	60 East	Yes
SWT	Swedish Winter	60 East	No
SST	Swedish Summer	60 East	Yes
FWT	French Winter	60 East	No
FST	French Summer	60 East	Yes
EET	Eastern Europe	120 East	No
BT	Baghdad	180 East	No
IT	Iran	210 East	No
ZP4	Eastern Europe Zone 4	240 East	No
ZP5	Eastern Europe Zone 5	300 East	No
IST	Indian Standard	330 East	No
ZP6	Eastern Europe Zone 6	360 East	No
WAST	West Australian Standard	420 East	No
WADT	West Australian Daylight	420 East	Yes
JT	Java	450 East	No
CCT	China Coast	480 East	No
JST	Japan Standard	540 East	No
KST	Korean Standard	540 East	No
CAST	Central Australian Standard	570 East	No
CADT	Central Australian Daylight	570 East	Yes
EAST	Eastern Australian Standard	600 East	No
EADT	Eastern Australian Daylight	600 East	Yes
GST	Guam Standard	600 East	No
KDT	Korean Daylight	600 East	No
NZT	New Zealand	720 East	No
NZST	New Zealand Standard	720 East	No
NZDT	New Zealand Daylight	720 East	Yes
IDLE	International Date Line East	720 East	No

Subcommands

The following subcommand descriptions assume the administration server is using the standard MIT Kerberos database for the registry. Other database implementations may not support all of the subcommand options and attributes.

The following subcommands are supported:

help [*subcommand***]**
> The **help** subcommand displays the command syntax for the specified subcommand. If no subcommand name is specified, the available subcommands are displayed.

get_privs
> The **get_privs** (also known as **getprivs**) subcommand lists the administrative privileges for the authenticated client. Additional authorization checking may be performed for a specific administration function depending upon the function and the database implementation.

list_principals [*expression***]**
> The **list_principals** (also known as **listprincs**) subcommand lists all of the principals in the Kerberos database that match the specified search expression. If no search expression is provided, all principals are listed. You must have LIST authority.

> The search expression can include the "*" and "?" wild cards where "*" represents zero or more characters and "?" represents a single character. For example, the expression ***/admin@*** returns all principal names that end with **/admin**, the expression **rwh*** returns all principal names that begin with **rwh**, and the expression **test_client?@*** returns principal names such as **test_client1**, **test_client2**, and so forth.

> The search string can also contain paired "[" and "]" characters with one or more characters between the brackets. A match occurs if a name contains one of the characters between the brackets. For example, the expression ***/[ad]*** returns all names containing **/a** and **/d**, while the expression **[ckr]*** returns all names beginning with **c**, **k**, or **r**.

get_principal *name*
> The **get_principal** (also known as **getprinc**) subcommand displays information for a single principal entry. You must have GET authority, or the principal entry must be your own entry.

> The following principal attributes can be displayed by the **get_principal** subcommand. The attributes that are supported by the administration server are dependent upon the Kerberos database implementation.

> **DISALLOW_DUP_SKEY**
> > Specifies that a service ticket cannot be encrypted using the session key of an existing ticket.

> **DISALLOW_FORWARDABLE**
> > Specifies that forwardable tickets are not allowed.

> **DISALLOW_POSTDATED**
> > Specifies that postdated tickets are not allowed.

> **DISALLOW_PROXIABLE**
> > Specifies that proxiable tickets are not allowed.

> **DISALLOW_RENEWABLE**
> > Specifies that renewable tickets are not allowed.

> **DISALLOW_SVR**
> > Specifies that service tickets cannot be obtained for this principal.

> **DISALLOW_TGT_BASED**
> > Specifies that service tickets cannot be obtained using a ticket-granting ticket.

> **DISALLOW_ALL_TIX**
> > Specifies that tickets cannot be obtained for this principal.

Commands

REQUIRES_PWCHANGE
Specifies that the password must be changed.

PWCHANGE_SERVICE
Specifies that this is a password-changing service. The KDC grants an initial ticket to a password-changing service even if the current password is expired.

REQUIRES_HW_AUTH
Specifies that hardware authentication must be used when requesting a ticket. When requesting an initial ticket, hardware authentication must be used, and when requesting a service ticket, the ticket-granting ticket must indicate hardware authentication.

REQUIRES_PRE_AUTH
Specifies that preauthentication must be used when requesting a ticket. When requesting an initial ticket, preauthentication data must be provided, and when requesting a service ticket, the ticket-granting ticket must indicate preauthentication.

SUPPORT_DESMD5
Specifies that ENCTYPE_DES_CBC_MD5 keys are supported for this principal.

add_principal [options**] [**attributes**]** name
The **add_principal** (also known as **addprinc**) subcommand adds a new principal entry to the Kerberos database. The options and attributes may be specified before or after the principal name and may be entered in any order. You must have ADD authority.

The following options are supported for the **add_principal** subcommand:

-clearpolicy
Specifies that no policy is to be associated with the principal entry. The default policy is used if neither **-policy** nor **-clearpolicy** is specified and a policy named **default** exists. This option is mutually exclusive with the **-policy** option.

-e key types
Specifies the key types to be generated. All available key types are generated if this option is not specified. Entries in the list are separated by commas. Each entry consists of an encryption type and a salt type, separated by a colon. The salt type can be omitted and defaults to **normal**. Similar encryption types are ignored when processing the list. For example, encryption types **des-cbc-crc** and **des-cbc-md5** use the same 56-bit DES key, so only one of these encryption types needs to be specified to cause a 56-bit DES key to be generated.

-expire date
Specifies the expiration date for the principal entry. If this option is not specified, the entry does not expire.

-kvno version
Specifies the key version number for the encryption keys generated by this command. If this option is not specified, the initial key version number is set to 1. A key version of 0 is not allowed.

-maxlife interval
Specifies the maximum ticket lifetime. If this option is not specified, the maximum ticket lifetime is obtained from the KDC policy.

-maxrenewlife interval
Specifies the maximum renewable ticket lifetime. If this option is not specified, the maximum renewable ticket lifetime is obtained from the KDC policy.

-policy name
Specifies the policy associated with the principal. The default policy is used if neither **-policy** nor **-clearpolicy** is specified and a policy named **default** exists. This option is mutually exclusive with the **-clearpolicy** option.

-pw *password*
> Specifies the password for the principal entry. The user is prompted to enter the password in non-display mode if neither **-pw** nor **-randkey** is specified. This option is mutually exclusive with the **-randkey** option.

-pwexpire *date*
> Specifies the expiration date for the password. If this option is not specified, the password lifetime from the effective policy is used to set the password expiration date.

-randkey
> Specifies that a random key is to be generated for this principal. This option is mutually exclusive with the **-pw** option. If neither **-pw** nor **-randkey** is specified, the user is prompted to enter the password in non-display mode.

The following attributes are supported for the **add_principal** subcommand. The attributes that are supported by the administration server are dependent upon the Kerberos database implementation.

+allow_dup_skey
> Specifies that a service ticket can be encrypted using the session key of an existing ticket. This is the default.

-allow_dup_skey
> Specifies that a service ticket cannot be encrypted using the session key of an existing ticket.

+allow_forwardable
> Specifies that forwardable tickets are allowed. This is the default.

-allow_forwardable
> Specifies that forwardable tickets are not allowed.

+allow_postdated
> Specifies that postdated tickets are allowed. This is the default.

-allow_postdated
> Specifies that postdated tickets are not allowed.

+allow_proxiable
> Specifies that proxiable tickets are allowed. This is the default.

-allow_proxiable
> Specifies that proxiable tickets are not allowed.

+allow_renewable
> Specifies that renewable tickets are allowed. This is the default.

-allow_renewable
> Specifies that renewable tickets are not allowed.

+allow_svr
> Specifies that service tickets can be obtained for this principal. This is the default.

-allow_svr
> Specifies that service tickets cannot be obtained for this principal.

+allow_tgs_req
> Specifies that service tickets can be obtained using a ticket-granting ticket. This is the default.

-allow_tgs_req
> Specifies that service tickets cannot be obtained using a ticket-granting ticket.

+allow_tix
> Specifies that tickets can be obtained for this principal. This is the default.

-allow_tix
> Specifies that tickets cannot be obtained for this principal.

Commands

+needchange
Specifies that the password must be changed.

-needchange
Specifies that the password does not need to be changed. This is the default.

+password_changing_service
Specifies that this is a password changing service. The KDC grants an initial ticket to a password changing service even if the current password is expired.

-password_changing_service
Specifies that this is not a password changing service. This is the default.

+requires_hwauth
Specifies that hardware authentication must be used when requesting a ticket. Hardware authentication must be used when requesting an initial ticket, and the ticket-granting ticket must indicate hardware authentication when requesting a service ticket.

-requires_hwauth
Specifies that hardware authentication is not required. This is the default.

+requires_preauth
Specifies that preauthentication must be used when requesting a ticket. Preauthentication data must be provided when requesting an initial ticket, and the ticket-granting ticket must indicate preauthentication when requesting a service ticket.

Note that a z/OS KDC always requires preauthentication when requesting an initial ticket, even if this attribute is not set. This is done to improve the security of the Kerberos secret keys.

-requires_preauth
Specifies that preauthentication is not required. This is the default.

+support_desmd5
Specifies that ENCTYPE_DES_CBC_MD5 keys are supported for this principal.

-support_desmd5
Specifies that ENCTYPE_DES_CBC_MD5 keys are not supported for this principal. This is the default.

delete_principal *name*
The **delete_principal** (also known as **delprinc**) subcommand deletes a principal entry from the Kerberos database. You must have DELETE authority.

modify_principal [*options***] [***attributes***] *name*
The **modify_principal** (also known as **modprinc**) subcommand modifies an existing principal entry in the Kerberos database. The options and attributes may be specified before or after the principal name and may be entered in any order. You must have MODIFY authority.

The following options are supported for the **modify_principal** subcommand. The attributes that are supported by the administration server are dependent upon the Kerberos database implementation.

-clearpolicy
Specifies that no policy is to be associated with the principal entry. This option is mutually exclusive with the **-policy** option.

-expire *date*
Specifies the expiration date for the principal entry.

-kvno *version*
Specifies the key version number for the principal.

-maxlife *interval*
Specifies the maximum ticket lifetime.

-maxrenewlife *interval*
Specifies the maximum renewable ticket lifetime.

-policy *name*
Specifies the policy associated with the principal. This option is mutually exclusive with the **-clearpolicy** option.

-pwexpire *date*
Specifies the expiration date for the password.

The following attributes are supported for the **modify_principal** subcommand:

+allow_dup_skey
Specifies that a service ticket can be encrypted using the session key of an existing ticket. Resets the DISALLOW_DUP_SKEY attribute.

-allow_dup_skey
Specifies that a service ticket cannot be encrypted using the session key of an existing ticket. Sets the DISALLOW_DUP_SKEY attribute.

+allow_forwardable
Specifies that forwardable tickets are allowed. Resets the DISALLOW_FORWARDABLE attribute.

-allow_forwardable
Specifies that forwardable tickets are not allowed. Sets the DISALLOW_FORWARDABLE attribute.

+allow_postdated
Specifies that postdated tickets are allowed. Resets the DISALLOW_POSTDATED attribute.

-allow_postdated
Specifies that postdated tickets are not allowed. Sets the DISALLOW_POSTDATED attribute.

+allow_proxiable
Specifies that proxiable tickets are allowed. Resets the DISALLOW_PROXIABLE attribute.

-allow_proxiable
Specifies that proxiable tickets are not allowed. Sets the DISALLOW_PROXIABLE attribute.

+allow_renewable
Specifies that renewable tickets are allowed. Resets the DISALLOW_RENEWABLE attribute.

-allow_renewable
Specifies that renewable tickets are not allowed. Sets the DISALLOW_RENEWABLE attribute.

+allow_svr
Specifies that service tickets can be obtained for this principal. Resets the DISALLOW_SVR attribute.

-allow_svr
Specifies that service tickets cannot be obtained for this principal. Sets the DISALLOW_SVR attribute.

+allow_tgs_req
Specifies that service tickets can be obtained using a ticket-granting ticket. Resets the DISALLOW_TGT_BASED attribute.

-allow_tgs_req
Specifies that service tickets cannot be obtained using a ticket-granting ticket. Sets the DISALLOW_TGT_BASED attribute.

+allow_tix
Specifies that tickets can be obtained for this principal. Resets the DISALLOW_TIX attribute.

-allow_tix
Specifies that tickets cannot be obtained for this principal. Sets the DISALLOW_TIX attribute.

Commands

+needchange
Specifies that the password must be changed. Sets the REQUIRES_PWCHANGE attribute.

-needchange
Specifies that the password does not need to be changed. Resets the REQUIRES_PWCHANGE attribute.

+password_changing_service
Specifies that this is a password changing service. The KDC grants an initial ticket to a password changing service even if the current password is expired. Sets the PWCHANGE_SERVICE attribute.

-password_changing_service
Specifies that this is not a password changing service. Resets the PWCHANGE_SERVICE attribute.

+requires_hwauth
Specifies that hardware authentication must be used when requesting a ticket. Hardware authentication must be used when requesting an initial ticket, and the ticket-granting ticket must indicate hardware authentication when requesting a service ticket. Sets the REQUIRES_HW_AUTH attribute.

-requires_hwauth
Specifies that hardware authentication is not required. Resets the REQUIRES_HW_AUTH attribute.

+requires_preauth
Specifies that preauthentication must be used when requesting a ticket. Preauthentication data must be provided when requesting an initial ticket, and the ticket-granting ticket must indicate preauthentication when requesting a service ticket. Sets the REQUIRES_PRE_AUTH attribute.

-requires_preauth
Specifies that preauthentication is not required. Resets the REQUIRES_PRE_AUTH attribute.

Note that a z/OS KDC always requires preauthentication when requesting an initial ticket, even if this attribute is not set. This is done to improve the security of the Kerberos secret keys.

+support_desmd5
Specifies that ENCTYPE_DES_CBC_MD5 keys are supported for this principal. Sets the SUPPORT_DESMD5 attribute.

-support_desmd5
Specifies that ENCTYPE_DES_CBC_MD5 keys are not supported for this principal. Resets the SUPPORT_DESMD5 attribute.

change_password [-randkey | -pw *password*] **[-keepold] [-e keytypes]** *name*
The **change_password** (also known as **cpw**) subcommand changes the password for a principal. You must have CHANGEPW authority, or the principal entry must be your own entry.

A random key is generated if the **-randkey** option is specified. Otherwise, you are prompted to enter the new password unless the **-pw** option is specified.

Any existing encryption keys are discarded unless the **-keepold** option is specified. The number of retained keys is dependent upon the Kerberos database implementation.

All available key types are generated unless the **-e** option is specified. Entries in the key types list are separated by commas. Each entry consists of an encryption type and a salt type, separated by a colon. The salt type can be omitted and defaults to **normal**. Similar encryption types are ignored when processing the list. For example, encryption types **des-cbc-crc** and **des-cbc-md5** use the same 56-bit DES key, so only one of these encryption types needs to be specified to cause a 56-bit DES key to be generated.

rename_principal *oldname newname*

> The **rename_principal** (also known as **renprinc**) subcommand changes the name of a principal entry in the Kerberos database. You must have both ADD and DELETE authority.
>
> Since the principal name is often used as part of the password salt, you should change the password for the principal after the entry is renamed. Some implementations of the Kerberos administration server do not allow a principal to be renamed if the principal name is used in the password salt. In this case, you must delete the existing principal entry using the **delete_principal** subcommand and then add the new principal entry using the **add_principal** subcommand.

list_policies [*expression***]**

> The **list_policies** (also known as **listpols**) subcommand lists all of the policies in the Kerberos database that match the specified search expression. All policies are listed if no search expression is provided. You must have LIST authority.
>
> The search expression can include the "*" and "?" wild cards where "*" represents zero or more characters and "?" represents a single character. For example, the expression ***_local** returns all policy names that end with **_local**, the expression **def*** returns all policy names that begin with **def**, and the expression **test_policy?** returns policy names such as **test_policy1**, **test_policy2**, and so forth.
>
> The search string can also contain paired "[" and "]" characters with one or more characters between the brackets. A match occurs if a name contains one of the characters between the brackets. For example, the expression **[adh]*** returns all names beginning with **a**,**d**, or **h**.

get_policy *name*

> The **get_policy** (also known as **getpol**) subcommand displays information for a single policy entry. You must have GET authority or the policy must be associated with your own principal entry.

add_policy [*options***]** *name*

> The **add_policy** (also known as **addpol**) subcommand adds a new policy to the Kerberos database. The options may be specified before or after the policy name and may be specified in any order. You must have ADD authority.
>
> The following options are supported for the **add_policy** subcommand:
>
> **-maxlife** *interval*
>> Specifies the maximum password lifetime. The password must be changed after this interval has elapsed.
>
> **-minlife** *interval*
>> Specifies the minimum password lifetime. A new password cannot be changed until this interval has elapsed.
>
> **-minlength** *number*
>> Specifies the minimum password length.
>
> **-minclasses** *number*
>> Specifies the minimum number of character classes in the password.
>
> **-history** *number*
>> Specifies the number of passwords in the password history. A new password cannot match any of the remembered passwords.

modify_policy [*options***]** *name*

> The **modify_policy** (also known as **modpol**) subcommand modifies an existing policy in the Kerberos database. The options may be specified before or after the policy name and may be specified in any order. You must have MODIFY authority.
>
> The following options are supported for the **modify_policy** subcommand:
>
> **-maxlife** *interval*
>> Specifies the maximum password lifetime. The password must be changed after this interval has elapsed.

Commands

-minlife *interval*
Specifies the minimum password lifetime. A new password cannot be changed until this interval has elapsed.

-minlength *number*
Specifies the minimum password length.

-minclasses *number*
Specifies the minimum number of character classes in the password.

-history *number*
Specifies the number of passwords in the password history. A new password cannot match any of the remembered passwords.

delete_policy *name*
The **delete_policy** (also known as **delpol**) subcommand deletes a policy entry from the Kerberos database. You must have DELETE authority.

add_key [[-keytab | -k] *keytab_name***] [-keepold] [-e keytypes]** *principal_name*
The **add_key** (also known as **ktadd**) subcommand generates a set of random encryption keys for the named principal and then adds the generated keys to the specified key table. You must have CHANGEPW authority or the principal entry must be your own entry.

The default key table is used if the **-keytab** option is not specified. A key table name prefix of "FILE:" is changed to "WRFILE:" because the **add_key** subcommand must update the key table.

Any existing encryption keys are discarded unless the **-keepold** option is specified. The number of retained keys is dependent upon the Kerberos database implementation.

All available key types are generated unless the **-e** option is specified. Entries in the key types list are separated by commas. Each entry consists of an encryption type and a salt type, separated by a colon. The salt type can be omitted and defaults to **normal**. Similar encryption types are ignored when processing the list. For example, encryption types **des-cbc-crc** and **des-cbc-md5** use the same 56-bit DES key, so only one of these encryption types needs to be specified to cause a 56-bit DES key to be generated.

---

kdb5_ndbm

This is the Kerberos NDBM database maintenance utility.

Format

```
kdb5_ndbm create [-k keytype] [-e keytypes]
kdb5_ndbm destroy
kdb5_ndbm dump [-k keytype] [-mkey_convert] [-compat}[-v] filename
kdb5_ndbm load [-k keytype] [-mkey_convert] [-v] filename
kdb5_ndbm stash [-k keytype]
```

Options

-e keytypes
Specifies the encryption types to be used when generating the initial principal keys. Keys are generated for all supported encryption types if this option is not specified. Entries in the list are separated by commas. Similar encryption types are ignored when processing the list. For example, encryption types **des-cbc-crc** and **des-cbc-md5** use the same 56-bit DES key, so only one of these encryption types needs to be specified to cause a 56-bit DES key to be generated.

-k keytype
Specifies the encryption type for the database master key. The **des3-cbc-sha1** encryption type is used if this option is not specified. The encryption type specified for the **-k** option is added to the encryption types specified for the **-e** option if it is not already in the list, because the **K/M** and **kadmin/history** architected principals must have a key available for the database master key encryption type.

-mkey_convert
    Indicates that the master key is to be changed.

-compat
    Creates the database dump using the version 4 format instead of the version 5 format.

-v The principal and policy names should be displayed as they are processed.

Usage

The **kdb5_ndbm** command is used to maintain a Kerberos NDBM registry database. It is not used with a Kerberos SAF registry database. The **kdb5_ndbm** command must be run by a user with write access to the **/var/skrb/krb5kdc** directory and to all of the files in this directory. The **/var/skrb/krb5kdc** directory path is created if it does not already exist.

The following functions are provided:

- **kdb5_ndbm create [-k keytype] [-e keytypes]**

  This command creates a new Kerberos NDBM database. An error is reported if an NDBM database already exists. The architected KDC principals are created in the new database. In addition, user principals **IBMUSER** and **IBMUSER/admin** are created with an initial password of IBMUSER. Finally, the master key stash file is created.

  The **kdb5_ndbm create** command is used to create a new database for the primary KDC for a realm. It is not used to create a database for a secondary KDC since a secondary KDC receives its database by propagation from the primary KDC.

  You are prompted to enter the master key for the new database. This key is used to encrypt the database entries and should not be an obvious password string. Do not forget this password since you need it when you create a secondary KDC or when you attempt to reload the database from a backup copy created by the **kdb5_ndbm dump** command.

- **kdb5_ndbm destroy**

  This command destroys an existing Kerberos NDBM database. The database files are removed along with the master key stash file.

- **kdb5_ndbm dump [-k keytype] [-mkey_convert] [-compat] [-v] filename**

  This command creates a portable copy of the Kerberos NDBM database. The dump file is a printable text file created in the local code page as defined by the LANG environment variable. You should convert it to the code page of the target system when moving it to another system.

  The **kdb5_ndbm dump** command is used to create a backup copy of the Kerberos database. The database can be recreated from the backup copy using the **kdb5_ndbm load** command. The backup copy can also be used to create a copy of the Kerberos database on another system. The NDBM database files themselves cannot be moved to another system since the internal database formats are not portable.

  The database dump includes principal and policy information. The dump key is the same as the database master key unless the **-mkey_convert** option is specified.

  The dump file created by the z/OS Network Authentication Service **kdb5_ndbm** command uses the version 5 dump format and is compatible with the dump file created by the MIT Kerberos 1.2.2 **kdb5_util** command. The version 5 dump format includes principal policy and password history information. Earlier releases of the MIT Kerberos **kdb5_util** command do not support this dump format. You can specify the **-compat** option to create a dump in the version 4 format, which can be processed by earlier releases of MIT Kerberos. A version 4 dump does not include principal policy or password history information. This information is lost if a database created from a version 4 dump is used by the primary KDC for the realm.

- **kdb5_ndbm load [-k keytype] [-mkey_convert] [-v] filename**

  This command creates a Kerberos NDBM database using the portable copy created by the **kdb5_ndbm dump** command. An error is returned if an NDBM database already exists.

Commands

You are prompted for the dump key. The master key for the new database is the same as the dump key unless the **-mkey_convert** option is specified.

The z/OS Network Authentication Service **kdb5_ndbm** command processes dump files created by MIT Kerberos 1.2 (version 4 dump format) and MIT Kerberos 1.2.2 (version 5 dump format). Per-principal policy information is lost if the version 4 dump format is used, because that dump format does not contain this information.

- **kdb5_ndbm stash [-k keytype]**

This command creates the database master key stash file. An error is returned if the stash file already exists since the master key cannot be changed after the database is created. Use the **kdb5_ndbm destroy** command to remove an existing database before attempting to create a new database.

The **kdb5_ndbm stash** command is used to create the master key stash file for a secondary KDC. An error occurs during database propagation if the stash file is created using the wrong database master key.

---

kdestroy

Destroys a Kerberos credentials cache.

Format

```
kdestroy [-c cache_name] [-e time_delta]
```

Options

-c *cache_name*
Specifies the name of the credentials cache to destroy. The default credentials cache is destroyed if no command options are specified. This option and the **-e** option are mutually exclusive.

-e *time_delta*
Specifies that all credentials cache files containing expired tickets are deleted if the tickets have been expired at least as long as the *time_delta* value.

Usage

The kdestroy command deletes a Kerberos credentials cache file.

The **-e** option causes the **kdestroy** command to check all of the credentials cache files in the default cache directory (**/var/skrb/creds**). Any file that contains only expired tickets that have expired for the time delta are deleted. The time delta is expressed as n**w**n**d**n**h**n**m**n**s** where n represents a number, **w** indicates weeks, **d** indicates days, **h** indicates hours, **m** indicates minutes, and **s** indicates seconds. The components must be specified in this order but any component may be omitted (for example, 4h5m represents four hours and 5 minutes and 1w2h represents 1 week and 2 hours). If only a number is specified, the default is hours.

To delete a credentials cache, the user must be the owner of the file or must be a root (uid 0) user.

Examples

To delete the default credentials cache for the user:
```
kdestroy
```

To delete all credentials caches with expired tickets older than 1 day:
```
kdestroy -e 1d
```

---

keytab

Manages a key table.

Format

```
keytab add principal [-p password] [-v version] [-k keytab]
keytab delete principal [-v version] [-k keytab]
keytab list [principal] [-k keytab]
```

Options

-k *keytab*
  Specifies the key table name. The default key table is used if this option is not specified.

-p *password*
  Specifies the password. The user is prompted to enter the password if this option is not specified when adding an entry to the key table.

-v *version*
  Specifies the key version number. When adding a key, the next version number is assigned if this option is not specified. When deleting a key, all keys for the principal are deleted if this option is not specified.

principal
  Specifies the principal name. When listing the key table, all principals are displayed if this option is not specified.

Usage

The keytab command is used to add or delete a key from a key table or to display the entries in a key table.

The **keytab** command creates key table entries for each unique key type when adding a key version to the key table. Key table entries are not created for all supported encryption types because some of the encryption types share the same key type. When retrieving a key from the key table, the Kerberos runtime selects the appropriate key based upon the requested encryption type.

The following key types and associated encryption types are supported:

Table 8. Key types and their associated encryption types

56-bit DES	des-cbc-crc (ENCTYPE_DES_CBC_CRC) des-cbc-md4 (ENCTYPE_DES_CBC_MD4) des-cbc-md5 (ENCTYPE_DES_CBC_MD5) des-cbc-raw (ENCTYPE_DES_CBC_RAW)
56-bit DES with key derivation	des-hmac-sha1 (ENCTYPE_DES_HMAC_SHA1)
168-bit DES with key derivation	des3-cbc-sha1 (ENCTYPE_DES3_CBC_SHA1) des3-cbc-raw (ENCTYPE_DES3_CBC_RAW)

Examples

To add a key for principal **rwh** in the **/home/rwh/my_keytab** key table:

```
keytab add rwh -k /home/rwh/my_keytab
```

To list all of the entries in the **/home/rwh/my_keytab** key table:

```
keytab list -k /home/rwh/my_keytab
```

kinit

Obtains or renews the Kerberos ticket-granting ticket.

Format

```
kinit [-s] [-r time] [-R] [-p] [-f] [-A] [-l time] [-c cache]
      [-k] [-t keytab] [principal]
```

Options

-s   Specifies that an initial ticket is to be obtained using the Kerberos principal associated with the current system identity. No password is used since the system has already verified the identity. The Kerberos security server must be running on the local system in order to use the -s option.

-r *time*
Specifies the renew time interval for a renewable ticket. The ticket may no longer be renewed after the expiration of this interval. The renew time must be greater than the end time. The ticket is not renewable if this option is not specified (a renewable ticket may still be generated if the requested ticket lifetime exceeds the maximum ticket lifetime).

-R   Specifies that an existing ticket is to be renewed. No other ticket options may be specified when renewing an existing ticket.

-p   Specifies that the ticket is to be proxiable. The ticket is not proxiable if this option is not specified.

-f   Specifies that the ticket is to be forwardable. The ticket is not forwardable if this option is not specified.

-A   Specifies that the ticket should not contain a list of client addresses. The ticket contains the local host address list if this option is not specified. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

-l *time*
Specifies the ticket end time interval. The ticket may not be used after this interval has expired unless it has been renewed. The interval is set to 10 hours if this option is not specified.

-c *cache*
Specifies the name of the credentials cache that the kinit command uses. The default credentials cache is used if this option is not specified.

-k   Specifies obtaining the key for the ticket principal from a key table. The user is prompted to enter the password for the ticket principal if this option, the **-R** option, or the **-s** option, is not specified.

-t *keytab*
Specifies the key table name. The default key table is used if this option is not specified and the **-k** option is specified. The **-t** option implies the **-k** option.

principal
Specifies the ticket principal. The principal is obtained from the credentials cache if the principal is not specified on the command line.

Usage

The **kinit** command obtains or renews a Kerberos ticket-granting ticket. The KDC options specified by **kdc_default_options** in the Kerberos configuration file are used if no ticket options are specified on the **kinit** command.

If an existing ticket is not being renewed, the credentials cache is re-initialized and contains the new ticket-granting ticket received from the KDC. If the principal name is not specified on the command line and the **-s** option is not specified, the principal name is obtained from the credentials cache. The new credentials cache become the default credentials cache unless the cache name is specified using the **-c** option.

Ticket time values are expressed as *n***w***n***d***n***h***n***m***n***s** where *n* represents a number, **w** indicates weeks, **d** indicates days, **h** indicates hours, **m** indicates minutes, and **s** indicates seconds. The components must be

specified in this order but any component may be omitted (for example, 4h5m represents four hours and 5 minutes and 1w2h represents 1 week and 2 hours). If only a number is specified, the default is hours.

Examples

To obtain a ticket-granting ticket with a lifetime of ten hours that is renewable for one week:

```
kinit -l 10h -r 1w my_principal
```

To obtain an initial ticket based upon the current system identity:

```
kinit -s
```

To renew an existing ticket:

```
kinit -R
```

klist

Displays the contents of a Kerberos credentials cache or key table.

Format

```
klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [filename]
```

Options

-a Shows all tickets in the credentials cache, including expired tickets. Expired tickets are not listed if this option is not specified. This option is valid only when listing a credentials cache.

-e Displays the encryption type for the session key and the ticket. This option is valid only when listing a credentials cache.

-c Lists the tickets in a credentials cache. This is the default if neither the **-c** nor the **-k** option is specified. This option and the **-k** option are mutually exclusive.

-f Shows the ticket flags using the following abbreviations. This option is valid only when listing a credentials cache.

- A - Preauthentication used
- C - Transited list checked by KDC
- D - Postdateable ticket
- d - Postdated ticket
- F - Forwardable ticket
- f - Forwarded ticket
- H - Hardware preauthentication used
- I - Initial ticket
- i - Invalid ticket
- P - Proxiable ticket
- p - Proxy ticket
- R - Renewable ticket
- O - Server can be a delegate

-s Suppresses command output but sets the exit status to 0 if a valid ticket-granting ticket is found in the credentials cache. This option is valid only when listing a credentials cache.

-k Lists the entries in a key table. This option and the **-c** option are mutually exclusive.

-t Displays timestamps for key table entries. This option is valid only when listing a key table.

Commands

-K Displays the encryption key value for each key table entry. This option is valid only when listing a key table.

filename
Specifies the name of the credentials cache or key table. The default credentials cache or key table is used if no filename is specified.

Usage

The **klist** command displays the contents of a Kerberos credentials cache or key table.

Examples

To list all of the entries in the default credentials cache:

```
klist
```

To list all of the entries in the **/krb5/my_keytab** key table with timestamps:

```
klist -k -t /krb5/my_keytab
```

kpasswd

Changes the password for a Kerberos principal.

Format

kpasswd [*principal*]

Options

principal
Specifies the principal whose password is to be changed. The principal is obtained from the default credentials cache if the principal is not specified on the command line.

Usage

The **kpasswd** command changes the password for the specified Kerberos principal using the password change service. You must supply the current password for the principal as well as the new password. The password change server applies any applicable password policy rules to the new password before changing the password.

You may not change the password for a ticket-granting service principal (**krbtgt/***realm*) using the **kpasswd** command.

kpropd

This is the Kerberos stand-alone database propagation catcher.

Format

kpropd [-r realm] [-P port] [-v]

Options

-P *port*
Specifies the port to use for the database propagation. The port assigned to the **krb5_prop** service is used if this option is omitted. Port 754 is used if the **krb5_prop** service is not defined.

| **-r** *realm*

| Specifies the database realm. The default realm obtained from the Kerberos configuration file is used if this option is omitted.

| **-v**   The principal and policy names should be displayed as they are processed.

| ## Usage

| The **kpropd** command is used to receive a stand-alone database propagation from the primary KDC for the realm. The **kpropd** command is used when creating a secondary KDC or when recovering from a catastrophic database error.

| To use the **kpropd** command for a secondary KDC, perform the following steps:

| 1. Stop the SKRBKDC started task if it is running on the secondary system.

| 2. Add the secondary system to the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the primary system if it is not already defined. The propagation protocol should be set to **Manual** to prevent automatic propagation of database updates.

| 3. Use the **kdb5_ndbm destroy** command to remove an existing Kerberos database.

| 4. Use the **kdb5_ndbm stash** command to create the database master key stash file.

| 5. Create the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the secondary system if it does not exist. The primary KDC for the realm must be listed in this file.

| 6. Use the **kadmin ktadd** command to create the **/var/skrb/krb5kdc/kpropd.ktf** key table if it does not exist. The principal name is **host/**_host-name_ where *host-name* is the primary host name for the local system. The primary host name is determined by doing a DNS lookup on the host name to get the IP address and then doing a DNS lookup on the IP address to get the host name.

| 7. Start the **kpropd** command on the secondary system.

| 8. Issue the **PROP** *host-name* command on the primary KDC to initiate the database propagation.

| 9. Wait until the propagation is complete and the **kpropd** command ends.

| 10. Start the SKRBKDC started task on the secondary system.

| 11. Change the propagation protocol to **Update** in the **/etc/skrb/home/kdc/kpropd.acl** configuration file on the primary system.

ksetup

Manages Kerberos service entries in the LDAP directory for a Kerberos realm.

Format

```
ksetup [-h host-name] [-n bind-name] [-p bind-password] [-e]
```

Options

-h *host-name*
    Specifies the host name for the LDAP server. The LDAP server specified in the Kerberos configuration file is used if this option is not specified.

-n *bind-name*
    Specifies the distinguished name to use when binding to the LDAP server. The LDAP_BINDDN environment variable is used to obtain the name if this option is not specified.

-p *bind-password*
    Specifies the password to use when binding to the LDAP server. The LDAP_BINDPW environment variable is used to obtain the password if this option is not specified.

-e   Echo each command line to **stdout**. This is useful when **stdout** is redirected to a file.

Commands

Usage

The **ksetup** command manages Kerberos service entries in the LDAP directory. The following subcommands are supported.

- **addadmin** *host-name:port-number realm-name*

  This subcommand adds an administration service entry for the specified realm. The port number is set to 749 if it is not specified. The fully-qualified host name should be used, so that it is resolved correctly no matter what default DNS name is in effect on the Kerberos clients. The default realm name is used if no realm name is specified.

- **addhost** *host-name realm-name*

  This subcommand adds a host entry for the specified realm. The fully-qualified host name should be used so that it is resolved correctly no matter what default DNS domain is in effect on the Kerberos clients. The default realm name is used if no realm name is specified. An error is displayed if the host entry already exists.

- **addkdc** *host-name:port-number realm-name*

  This subcommand adds a KDC entry for the specified realm. A host entry is created if one does not already exist. The port number is set to 88 if it is not specified. The fully-qualified host name should be used so that it is resolved correctly no matter what default DNS domain is in effect on the Kerberos clients. The default realm name is used if no realm name is specified. An existing KDC entry will be modified.

- **addpwd** *host-name:port-number real-name*

  This subcommand adds a password change service entry for the specified realm. The port number is set to 464 if it is not specified. The fully-qualified host name should be used so that it is resolved correctly no matter what default DNS domain is in effect on the Kerberos clients. The default realm name is used if no realm name is specified. An existing password service entry will be modified.

- **deladmin** *host-name real-name*

  This subcommand deletes an administration service entry for the specified host. The default realm name is used if no realm name is specified.

- **delhost** *host-name realm-name*

  This subcommand deletes a host entry and any associated KDC specification from the specified realm. The default realm name is used if no realm name is specified.

- **delkdc** *host-name realm-name*

  This subcommand deletes a KDC entry for the specified host. The host entry itself is not deleted. The default realm name is used if no realm name is specified.

- **delpwd** *host-name realm-name*

  This subcommand deletes a password change service entry for the specified host. The default realm name is used if no realm name is specified.

- **listadmin** *realm-name*

  This subcommand lists the administration service entries for a realm. The default realm name is used if no realm name is specified.

- **listhost** *realm-name*

  This subcommand lists the host entries for a realm. The default realm name is used if no realm name is specified.

- **listkdc** *realm-name*

  This subcommand lists the KDC entries for a realm. The default realm name is used if no realm name is specified.

- **listpwd** *realm-name*

  This subcommand lists the password change service entries for a realm. The default realm name is used if no realm name is specified.

- **exit**

This subcommand ends the **ksetup** command.

kvno

Displays the current key version number for a principal.

Format

kvno [*principal*]

Options

principal

Specifies the principal whose current key version number is to be displayed. The principal is obtained from the default credentials cache if the principal is not specified on the command line.

Commands

Chapter 5. Status codes

This chapter lists the status codes for z/OS Network Authentication Service. The status codes are listed in numerical order.

Major status values

GSS-API routines return GSS status codes as their function value. These codes indicate generic API errors and are common across GSS-API implementations. A GSS status code indicates a single API error from the routine and a single calling error. Additional status information can be contained in the GSS status code as supplementary information. The errors are encoded into a 32-bit GSS status code as follows:

MSB		LSB
Calling Error	Routine Error	Supplementary Information
Bit 31 24	23 16	15 0

Figure 3. GSS status code bit locations

If a GSS-API routine returns a GSS status code whose upper 16 bits contain a nonzero value, the call failed. If the calling error field is nonzero, the application's call of the routine was in error. In addition, the routine can indicate additional information by setting one or more bits in the supplementary information field of the status code.

The following table lists the GSS-API calling errors and their meanings:

Table 9. GSS-API calling errors

Error Number (Hexidecimal)	Meaning
01	Unable to read an input parameter
02	Unable to write an output parameter
03	Incorrect parameter structure

The following table lists the GSS-API routine errors and their meanings:

Table 10. GSS-API routine errors

Error Number (Hexidecimal)	Meaning
01	Mechanism is not supported
02	Name is not valid
03	Name type is not valid
04	Channel bindings are not correct
05	Status value is not valid
06	Token signature is not correct
07	No credentials supplied
08	No context established
09	Token is not valid
0A	Credential is not valid
0B	Credentials have expired

Table 10. GSS-API routine errors (continued)

Error Number (Hexidecimal)	Meaning
0C	Context has expired
0D	Routine failed (check minor status)
0E	Bad quality-of-protection value
0F	Operation not authorized by local security policy
10	Operation or option not available
11	Credential element already exists
12	Not a mechanism name

The following table lists the GSS-API supplementary status bits and their meanings:

Table 11. GSS-API supplementary status bits

Status Bit Number (Hexidecimal)	Meaning
0001	Call routine again to complete request
0002	Token is duplicate of earlier token
0004	Token validity period has expired
0008	Later token has already been processed
0010	Skipped predecessor token detected

Kerberos administration database (numbers 01B79C00 - 01B79CFF)

01B79C01   Principal or policy already exists.

Explanation: The principal or policy entry already exists in the Kerberos database.

User Response: Specify a name that does not already exist.

01B79C02   Principal or policy does not exist.

Explanation: The principal or policy entry does not exist in the Kerberos database.

User Response: Specify a name that does exist.

01B79C03   Database is not initialized.

Explanation: The Kerberos database is not initialized.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C04   Policy name is not valid.

Explanation: The policy name is not valid.

User Response: Contact the owner of the Kerberos administration server to obtain the policy name guidelines for that server.

01B79C05   Principal name is not valid.

Explanation: The principal name is not valid.

User Response: Contact the owner of the Kerberos administration server to obtain the principal name guidelines for that server.

01B79C06   Database inconsistency detected.

Explanation: A database inconsistency has been detected by the Kerberos administration server.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C07   XDR encoding error.

Explanation: The Kerberos administration server detected an error while decoding the administration request or while encoding the administration response.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C08   Database operation failed.

Explanation: The Kerberos administration server is unable to complete a database operation.

User Response: Report the problem to the owner of

the Kerberos administration server.

01B79C09   **Database lock mode is not valid.**

Explanation: The Kerberos administration server is unable to lock the database.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C0A   **Unable to lock database.**

Explanation: The Kerberos administration server is unable to lock the database.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C0B   **Database is not locked.**

Explanation: The Kerberos administration server is unable to perform a database operation.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C0C   **Administration database lock file is missing.**

Explanation: The Kerberos administration server is unable to perform a database operation.

User Response: Report the problem to the owner of the Kerberos administration server.

01B79C0D   **Insufficient permission to lock file.**

Explanation: The Kerberos administration server is unable to perform a database operation.

User Response: Report the problem to the owner of the Kerberos administration server.

GSS_API Kerberos mechanism codes (numbers 025EA100 - 025EA1FF)

025EA100   **Principal is not found in credentials cache.**

Explanation: The principal name in the default credentials cache is not the same as the principal name on the GSS-API request.

User Response: Either specify the correct principal or specify GSS_C_NO_NAME to use the default principal.

025EA101   **Principal is not found in key table.**

Explanation: The principal specified on a GSS-API request is not found in the key table.

User Response: Specify a principal that is defined in the key table or use the KRB5_KTNAME environment variable to specify a different key table.

025EA102   **Ticket-granting ticket is not found in credentials cache.**

Explanation: GSS-API is creating a credential that can be used to initiate a security context. The credentials cache does not contain a ticket-granting ticket that can be used to obtain service tickets.

User Response: Obtain a valid ticket-granting ticket for the principal to be used to initiate the security context. Then retry the request.

025EA104   **Context already established.**

Explanation: The **gss_init_sec_context()** function is called to continue setting up the security context. However, the security context has already been established. The application should not call **gss_init_sec_context()** again unless the previous call

returned a major status of GSS_C_CONTINUE_NEEDED.

User Response: Verify that the previous call to **gss_init_sec_context()** returned a major status of GSS_C_CONTINUE_NEEDED.

025EA105   **Signature algorithm is not supported.**

Explanation: The signature algorithm is not supported by the local system or is not compatible with the current security context.

User Response: Ensure that the selected signature algorithm is supported by both the local and the remote system and is compatible with the encryption key associated with the current security context. Contact your service representative if the error persists.

025EA106   **Length value is not correct.**

Explanation: The length of a field in an input token is not correct.

User Response: Ensure that the input token is not modified. Contact your service representative if the error persists.

025EA107   **Context is not established.**

Explanation: A GSS-API function was called that requires an established security context. The supplied context has been initiated but the response from the context acceptor has not been received.

User Response: Process the response token before attempting to use the security context.

Status codes

025EA108   Context identifier is not valid.

Explanation: An unassigned context identifier is specified on a GSS-API function call.

User Response: Specify a valid context identifier and then retry the request.

025EA109   Credential identifier is not valid.

Explanation: An unassigned credential identifier is specified on a GSS-API function call.

User Response: Specify a valid credential identifier and then retry the request.

025EA10B   Token sequence number is not valid.

Explanation: The token sequence number is not correctly formed. This error can occur if the token is modified or if the session key in the security context is not correct.

User Response: Ensure that the token is not modified and that the correct security context is used to process the token.

025EA140   Token pad characters are not valid.

Explanation: The token does not contain the correct pad characters.

User Response: Verify that the token is not modified. Contact your service representative if the error persists.

025EA141   Data privacy service is not available.

Explanation: The **gss_unwrap_()** function was called to process a message that was encrypted by the sender. However, data encryption support is not available on the local system.

User Response: Do not request message confidentiality protection unless both systems provide data encryption services.

025EA142   Seal algorithm is not supported.

Explanation: The seal algorithm is not supported by the local system or is not compatible with the current security context.

User Response: Ensure that both systems are at compatible software levels. Contact your service representative if the error persists.

025EA143   Token length is not correct.

Explanation: The length of the buffer containing the input token is not correct.

User Response: Verify that the correct length is specified for the token buffer. Contact your service representative if the error persists.

025EA144   Encryption type is not supported.

Explanation: The encryption type specified in the input token is not valid or is not supported by the current software level.

User Response: Ensure that both systems are at compatible software levels. Contact your service representative if the error persists.

025EA145   No key is available to accept a security context.

Explanation: The **gss_accept_sec_context()** function failed because it is unable to obtain the session key for the security context.

User Response: Contact your service representative if the error persists.

025EA146   Bindings in token do not match supplied bindings.

Explanation: The channel bindings specified on the **gss_accept_sec_context()** call do not match the channel bindings contained in the input token.

User Response: Ensure that the input token is not modified and that the context initiator is specifying the correct channel bindings on the **gss_init_sec_context()** call.

025EA147   Checksum in token is not valid.

Explanation: The checksum in the input token does not have the correct type and length values.

User Response: Ensure that both systems are at compatible software levels. Contact your service representative if the error persists.

025EA148   Context is not in the correct state.

Explanation: The context state is not valid for the requested operation. This error can occur if an operation is attempted while the context is still in the initialization state. This error can also occur if **gss_init_sec_context()** or **gss_accept_sec_context()** is called after the context has been established.

User Response: Ensure that the context is in the correct state for the requested operation.

025EA149   Locking error is detected.

Explanation: An internal locking error is detected.

User Response: Contact your service representative if the error persists.

025EA14A   No mechanism credentials available.

Explanation: The credential context supplied on the **gss_init_sec_context**or the **gss_inquire_cred_by_mech** API function does not contain credentials for the requested mechanism.

User Response: Specify a credential context that contains the necessary mechanism credentials. The **gss_acquire_cred** API function can be used to create the credential context.

025EA14B   No internal name provided for requested mechanism.

Explanation: A *gss_name_t* parameter does not contain an internal representation that is valid for the

requested mechanism. Names returned by one mechanism may not be used with a different mechanism. The **gss_import_name** API function can be used to generate a *gss_name_t* that contains internal representations for all of the supported mechanisms.

User Response: Provide a *gss_name_t* that is valid for the requested mechanism.

Kerberos administration codes (numbers 029C2500 - 029C25FF)

029C2500   Operation failed.

Explanation: A Kerberos administration request has failed. There may be additional information on the cause of the failure in the administration server log.

User Response: Correct the cause of the failure and retry the request. Contact your service representative if the error persists.

029C2501   Operation requires 'get' privilege.

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to retrieve an entry from the security registry.

User Response: Repeat the request using a client with the proper authorization.

029C2502   Operation requires 'add' privilege.

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to add an entry to the security registry.

User Response: Repeat the request using a client with the proper authorization.

029C2503   Operation requires 'modify' privilege.

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to modify an entry in the security registry.

User Response: Repeat the request using a client with the proper authorization.

029C2504   Operation requires 'delete' privilege.

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to delete an entry from the security registry.

User Response: Repeat the request using a client with the proper authorization.

029C2505   Insufficient authorization for operation.

Explanation: A Kerberos administration request cannot be processed because the client does not have the necessary authorization.

User Response: Repeat the request using a client with the proper authorization.

029C2506   Database inconsistency detected.

Explanation: The Kerberos administration server detects an error in the security registry.

User Response: Contact your service representative.

029C2507   Principal or policy already exists.

Explanation: A Kerberos administration request cannot be processed because the principal or policy already exists in the security registry.

User Response: Choose a different name for the new registry object or delete the existing registry object.

029C2508   Communication failure with administration server.

Explanation: A Kerberos administration request cannot be processed due to an RPC communication failure.

User Response: Verify that the administration server is running and there are no network problems. Contact your service representative if the error persists.

029C2509   No administration server available.

Explanation: No Kerberos administration server is available for the requested realm. This error can occur if

Status codes

no administrator server is defined or a session cannot be established with the administration server.

User Response: Verify that an administration server is defined for the realm and the server is running.

029C250A **Key version mismatch for password history principal.**

Explanation: The key version number for the password history principal is incorrect.

User Response: Verify that the key table contains the correct key for the principal. Contact your service representative if the error persists.

029C250B **Administration server connection is not initialized.**

Explanation: A connection to the Kerberos administration server has not been initialized. Use the **kadm5_init_with_password()**, **kadm5_init_with_skey()**, or **kadm5_init_with_creds()** routine to initialize a connection.

User Response: Correct the application to initialize the connection before calling any administration routines.

029C250C **Principal does not exist.**

Explanation: The requested principal does not exist in the security registry.

User Response: None

029C250D **Policy does not exist.**

Explanation: The requested policy does not exist in the security registry.

User Response: None

029C250E **Field mask is not valid for operation.**

Explanation: The configuration parameters field mask is not valid for the requested administration operation. Refer to the API documentation to determine which field mask settings are valid.

User Response: Correct the application to specify a valid field mask.

029C250F **Character class count is not valid.**

Explanation: The number of character classes is not valid for the requested administration operation.

User Response: Contact the owner of the Kerberos administration server to determine the allowable range for the number of character classes.

029C2510 **Password length is not valid.**

Explanation: The password length is not valid. Contact your security administration to get the password requirements for your installation.

User Response: Contact the owner of the Kerberos administration server to determine the allowable range for the password length.

029C2511 **Policy name is not valid.**

Explanation: The policy name is not valid.

User Response: Specify a valid policy name.

029C2512 **Principal name is not valid.**

Explanation: The principal name is not valid.

User Response: Specify a valid principal name.

029C2513 **Auxillary attributes are not valid.**

Explanation: Auxillary attributes are not valid.

User Response: Specify a valid set of auxillary attributes.

029C2514 **Password history count is not valid.**

Explanation: The password history count is not valid.

User Response: Contact the owner of the Kerberos administration server to determine the allowable range for the password history count.

029C2515 **Minimum password lifetime is not valid.**

Explanation: The minimum password lifetime is not valid. The minimum lifetime must not be greater than the maximum lifetime.

User Response: Specify a valid password lifetime.

029C2516 **Password is too short.**

Explanation: The password is too short. Contact your security administrator to get the password requirements for your installation.

User Response: Specify a valid password.

029C2517 **Password does not contain enough character classes.**

Explanation: The password does not contain characters from enough different character classes. Contact your security administrator to get the password requirements for your installation.

User Response: Specify a valid password.

029C2518   Password is in the password dictionary.

Explanation: The password is in the password dictionary. Contact your security administrator to get the password requirements for your installation.

User Response: Specify a valid password.

029C2519   Password cannot be reused.

Explanation: The password has already been used and cannot be used again. Contact your security administrator to get the password requirements for your installation.

User Response: Specify a valid password.

029C251A   Password minimum lifetime has not expired.

Explanation: The password cannot be changed until the minimum lifetime has expired. Contact your security administrator to get the password requirements for your installation.

User Response: Wait until the minimum lifetime has elapsed before attempting to change the password.

029C251B   Policy is in use.

Explanation: The policy cannot be deleted because it is referenced by one or more principals.

User Response: Delete the principals that reference the policy before deleting the policy.

029C251C   Connection to server is already initialized.

Explanation: The connection to the administration server is already initialized.

User Response: None

029C251D   Password is not correct.

Explanation: The password entered is not the correct one for the current client.

User Response: Specify the correct password.

029C251E   Protected principal cannot be modified.

Explanation: The principal is protected and cannot be modified.

User Response: None

029C251F   Administration server handle is not valid.

Explanation: The server handle passed to an administration function is not valid.

User Response: Correct the application to pass the correct service handle to the administration function.

029C2520   Structure version is not valid.

Explanation: The structure version number is not valid.

User Response: Change the application to specify a valid version number.

029C2521   Old structure version is not supported.

Explanation: An obsolete structure version number was specified by the application.

User Response: Change the application to use the current structure version.

029C2522   New structure version is not supported.

Explanation: The structure version is not supported by the current level of the administration support.

User Response: Change the application to use a supported structure version.

029C2523   API version is not valid.

Explanation: The API version is not valid.

User Response: Change the application to specify a valid version number.

029C2524   Old API version is not supprted by the administration library.

Explanation: An obsolete API version is specified by the application.

User Response: Change the application to use the current API version.

029C2525   Old API version is not supprted by the administration server.

Explanation: An obsolete API version is specified by the application.

User Response: Change the application to use the current API version.

Status codes

029C2526   **New API version is not supprted by the administration library.**

Explanation: The API version is not supported by the current level of the administration support.

User Response: Change the application to use a supported API version.

029C2527   **New API version is not supported by the administration server.**

Explanation: The API version is not supported by the current level of the administration support.

User Response: Change the application to use a supported API version.

029C2528   **Required administration principal is not found.**

Explanation: A required administration principal was not found in the security registry.

User Response: Contact your service representative.

029C2529   **Principal cannot be renamed.**

Explanation: The salt type for the principal does not allow the principal to be renamed.

User Response: None

029C252A   **Administration client configuration parameters are not valid.**

Explanation: The client configuration parameters are not valid.

User Response: Verify that the application parameters are valid and that valid parameters are specified in the Kerberos profile. Contact your service represertative if the error persists.

029C252B   **Administration server configuration parameters are not valid.**

Explanation: The server configuration parameters are not valid.

User Response: Verify that valid parameters are specified in the server configuration profile. Contact your service representative if the errror persists.

029C252C   **Operation requires 'list' privilege.**

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to list the contents of the security registry.

User Response: Repeat the rquest using a client with the proper authorization.

029C252D   **Operation requires 'change-password' privilege.**

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to change the password for a principal.

User Response: Repeat the rquest using a client with the proper authorization.

029C252E   **GSS-API error.**

Explanation: A Kerberos administration request cannot be processed due to an error reported by GSS-API function.

User Response: Contact your service representative if the error persists.

029C252F   **Tagged data list type is not valid.**

Explanation: A tagged data list type contains a type code that is not valid.

User Response: Contact your service representative if the error persists.

029C2530   **Required configuration parameter is missing.**

Explanation: A required configuration parameter is not specified in the Kerberos configuration profile.

User Response: Verify that all administration server configuration parameters are specified. Contact your service representative if the error persists.

029C2531   **Administration server host name is not valid.**

Explanation: The administration server host name is not valid.

User Response: Specify a valid host name.

029C2532   **Operation requires 'set-key' privilege.**

Explanation: A Kerberos administration request cannot be processed because the client is not authorized to set the encryption key for a principal.

User Response: Repeat the request using a client with the proper authorization.

029C2533   **Duplicate encryption types specified.**

Explanation: Duplicate encryption types specified when setting the encryption key for a principal. This error can also occur if two encryption types are specified that use the same encryption key (for example, ENCTYPE_DES_CBC_CRC and ENCTYPE_DES_CBC_MD5 use the same 56-bit DES encryption key).

User Response: Do not specify duplicate encryption types.

| **029C2535   Encryption type mismatch.**

| **Explanation:** The key-salt entries do not match the corresponding key entries on a call to the **kadm5_setkey_principal_3()** routine.

| **User Response:** Specify a matching key-salt entry for each key entry.

| **029C25F0   Too many matching database records.**

| **Explanation:** A database search request resulted in more than 1000 matching records.

| **User Response:** Repeat the request using a more restrictive search expression.

| **029C25F1   Database record is too big.**

| **Explanation:** An attempt to create a Kerberos database entry failed because the record is too big. The Kerberos database has a maximum record size of 1024 bytes. This size includes the record key and any database overhead.

| **User Response:** Reduce the amount of data stored for the failing principal or policy.

| **029C25F2   Password change rejected.**

| **Explanation:** The password change was rejected by the system authorization facility. This error occurs if the password is too long or violates the password policy defined for the system.

| **User Response:** Select a different password. Contact your system administrator if the error persists.

| **029C25F3   Unsupported encryption type.**

| **Explanation:** The encryption type is not supported by the current software level.

| **User Response:** Upgrade to a software level that supports the encryption type.

| **029C25F4   Unsupported salt type.**

| **Explanation:** The password salt type is not supported by the current software level.

| **User Response:** Upgrade to a software level that supports the salt type.

| **029C25F5   Function not supported.**

| **Explanation:** The requested function is not supported by the Kerberos administration server.

| **User Response:** Refer to the documentation for the Kerberos administration server to determine which administration functions are supported.

| **029C25F6   Function disabled.**

| **Explanation:** The requested function is currently disabled by the Kerberos administration server.

| **User Response:** Retry the request when Kerberos administration services are enabled. Contact your Kerberos administrator if the error persists.

| **029C25F7   Target is not a Kerberos object.**

| **Explanation:** A request to rename or delete a registry object cannot be performed because the object was not created by the Kerberos administration service.

| **User Response:** The registry object must be renamed or deleted with the same service that was used to create it.

ASN.1 operations codes (numbers 6EDA3600 - 6EDA36FF)

6EDA3600   ASN.1 is unable to obtain the system time.

Explanation: An ASN.1 encode/decode function is unable to obtain the current system time. This error can occur if the time provider is not running.

User Response: Verify that the time provider is running and is configured properly. Then retry the request. Contact your service representative if the error persists.

6EDA3601   An ASN.1 structure is missing a required field.

Explanation: An ASN.1 encode function was unable to process a request because an input structure is missing a required field. This error can also occur on a decode request if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that all input structures contain all required fields and then retry the request. Contact your service representative if the error persists.

Status codes

6EDA3602   ASN.1 encounters an unexpected field number.

Explanation: An ASN.1 decode function is unable to process a request because the input byte stream contains a misplaced field. This error can occur if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that the input byte stream has not been modified and then retry the request. Contact your service representative if the error persisits.

6EDA3603   ASN.1 type number is not correct.

Explanation: An ASN.1 decode function is unable to process a request because the input byte stream contains an invalid type specification. This error can occur if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that the input byte stream has not been modified and then retry the request. Contact your service representative if the error persists.

6EDA3604   ASN.1 value is too large.

Explanation: An ASN.1 encode/decode function is unable to process a request because a data value is too large.

User Response: Verify that all data values are within the defined limits for that data type. Contact your service representative if the error persists.

6EDA3605   ASN.1 endecoding operation fails at end of data.

Explanation: An ASN.1 encoding function was unable to process a request because the end of the encoded stream was reached prematurely.

User Response: Verify that the encoded stream has not been modified and then retry the request. Contact your service representative if the error persists.

6EDA3606   ASN.1 identifier does not match expected value.

Explanation: An ASN.1 decode function was unable to process a request because an internal identifier does not match the expected value for the identifier. This error can occur if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that the input byte stream has not been modified and then retry the request. Contact your service representative if the error persists.

6EDA3607   ASN.1 length is not correct.

Explanation: An ASN.1 encode/decode function was unable to process a request because the length of a field does not match the expected value.

User Response: Verify that all field lengths are correct and then retry the request. Contact your service representative if the error persists.

6EDA3608   ASN.1 encoded byte stream is not valid.

Explanation: An ASN.1 decode function was unable to process a request because the input byte stream is formatted incorrectly. This error can occur if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that the input byte stream has not been modified and then retry the request. Contact your service representative if the error persists.

6EDA3609   ASN.1 is unable to parse the request.

Explanation: An ASN.1 decode function was unable to process a request because the input byte stream cannot be parsed. This error can occur if the byte stream was created by a different level of the ASN.1 software.

User Response: Verify that the input byte stream has not been modified and then retry the request. Contact your service representative if the error persists.

GSS-API codes (numbers 861B6D00 - 861B6DFF)

861B6D00   Service name is not valid.

Explanation: The supplied name is not a valid Kerberos service name.

User Response: Specify a valid service name.

861B6D01   UID string is not valid.

Explanation: The supplied UID string is not valid

User Response: Specify a valid UID string

861B6D02   UID does not resolve to a user.

Explanation: The specified UID does not resolve to a valid user on the local system.

User Response: Specify a UID that is valid on the local system and then retry the request.

861B6D03   Control block validation fails.

Explanation: A GSS-API control block or token is not correct. This error can occur if an exported context or credential is imported by an earlier version of the Kerberos runtime.

User Response: Upgrade the Kerberos runtime to the same level on all systems.

861B6D04   Unable to allocate memory.

Explanation: A GSS-API operation is unable to allocate memory.

User Response: Increase the memory available to the application and then retry the request. Contact your service representative if the error persists.

861B6D05   Message context is not valid.

Explanation: The **gss_display_status()** routine was called with an incorrect message context.

User Response: Initialize the message context to zero before the first call to the **gss_display_status()** routine.

861B6D06   Buffer length is not correct.

Explanation: The length of the supplied buffer is not correct for the operation being attempted.

User Response: Provide a buffer of the proper length and then retry the request.

861B6D07   Credential usage type is not valid.

Explanation: The credential usage must be GSS_C_INITIATE, GSS_C_ACCEPT, or GSS_C_BOTH when acquiring a credential. The credential usage must be GSS_C_INITIATE or GSS_C_BOTH when initiating a security context. The credential usage must be GSS_C_ACCEPT or GSS_C_BOTH when accepting a security context.

User Response: Specify a credential usage that is valid for the operation being attempted.

861B6D08   Quality of protection is not valid.

Explanation: The quality of protection (QOP) value specified for the GSS-API operation is not valid or is not supported by the current software level.

User Response: Specify a valid quality of protection value and then retry the request.

861B6D0A   Security mechanism is not correct.

Explanation: The security mechanism specified in the token header is not correct.

User Response: Verify that the token was created using a security mechanism that is supported by the current software level and that this security mechanism is the same security mechanism that was used to create the security context.

861B6D0B   Token header is not correct.

Explanation: The GSS-API token header is malformed or is corrupted.

User Response: Verify that the token was not modified and then retry the request. Contact your service representative if the error persists.

861B6D0C   Packet replayed in the wrong direction.

Explanation: The security mechanism specified in the token header is not correct.

User Response: A GSS-API token was processed by the wrong partner. Tokens generated by the context initiator must be processed by the context acceptor. Tokens generated by the context acceptor must be processed by the context initiator.

861B6D51   Message is not within the current window.

Explanation: The message is not within the current receive window. This indicates that multiple messages are missing or an old message is being replayed. GSS-API is unable to determine whether the message has been processed previously.

User Response: Verify that messages are being processed in the correct order and that no messages are being lost. Contact your service representative if the error persists.

Status codes

861B6D52   Message is after the next message in the sequence.

Explanation: The message is within the current receive window but is later than the next message in the sequence. This indicates that one or more messages are missing.

User Response: Verify that messages are being processed in the correct order and that no messages are being lost. Contact your service representative if the error persists.

861B6D53   Message has already been received.

Explanation: The message is within the current receive window but has already been received. This indicates that an old message is being replayed.

User Response: Verify that messages are being processed in the correct order and that no messages are being lost. Contact your service representative if the error persists.

861B6D54   Message is before the next message in the sequence.

Explanation: The message is within the current receive window but is earlier than the next message in the sequence. The message has not been received previously.

User Response: Verify that messages are being processed in the correct order and that no messages are being lost. Contact your service representative if the error persists.

861B6D55   Token signature is not correct.

Explanation: The checksum computed using the token data does not match the checksum contained in the token.

User Response: Verify that the token was not modified and then retry the request. Contact your service representative if the error persists.

861B6D56   Credential already contains a mechanism element.

Explanation: The **gss_add_cred_()** function was called to add a mechanism element to a credential. The credential already contains an element for the requested mechanism.

User Response: Do not add an existing mechanism to a credential.

861B6D57   Context is expired.

Explanation: The GSS-API context has expired. This indicates that either the context lifetime has expired or the associated Kerberos ticket is no longer valid.

User Response: Create a new GSS-API security context.

861B6D58   Token type is not correct.

Explanation: An attempt to decode a token failed due to incorrect API usage.

User Response: If the token was created using the **gss_get_mic()** function, use the **gss_verify_mic()** function to process it. If the token was created using the **gss_wrap()** function, use the **gss_unwrp()** function to process it. If the token was created using the **gss_delete_sec_context()** function, use the **gss_process_context_token()** function to process it. If the token was created using the **gss_accept_sec_context()** function, use the **gss_init_sec_context()** function to process it.

861B6D59   Credential is expired.

Explanation: The GSS-API credential has expired. This indicates that either the credential lifetime has expired or the associated Kerberos ticket is no longer valid.

User Response: Create a new GSS-API credential.

861B6D5A   Required parameter is missing.

Explanation: A required parameter is not specified on a GSS-API function call.

User Response: Specify the required parameter and then retry the request.

861B6D5B   Name is not a valid GSS-API name.

Explanation: A *gss_name_t* parameter does not refer to a valid GSS-API name.

User Response: Verify that the name parameter is correct. Names created by an application must be converted to the internal representation by calling the **gss_import_name()** function.

861B6D5C   No name is specified.

Explanation: GSS_C_NO_NAME is specified on an API that requires that a name be provided.

User Response: Specify a valid name and then retry the request.

861B6D5D   No mechanism is specified.

Explanation: GSS_C_NO_OID is specified for the mechanism on an API that requires that a mechanism be specified.

User Response: Specify a mechanism and then retry the request.

861B6D5E   Name type is not valid.

Explanation: The name type specified on the **gss_import_name()** function call is not valid or is not supported by the current software level.

User Response: Specify a valid name type and then retry the request.

861B6D5F   Name is not valid.

Explanation: An attempt to convert a name to its internal representation was not successful, or, a different name was specified when **gss_init_sec_context()** was called to finish establishing the security context.

User Response: Specify a valid name and then retry the request.

861B6D60   Security mechanism is not valid.

Explanation: The security mechanism is not valid or is not supported by the current software level.

User Response: Specify a supported security mechanism.

861B6D61   Status type is not valid.

Explanation: The status type specified on the **gss_display_status()** function call is not valid.

User Response: Specify a valid status type and then retry the request.

861B6D62   Status value is not valid.

Explanation: The status value specified on the **gss_display_status()** function call cannot be translated to an error message.

User Response: Verify that the message catalog is installed and is available to the application.

861B6D63   Object identifier encoding is not valid.

Explanation: An object identifier does not have a valid encoding. Object identifiers are encoded using ASN.1 encoding rules. The string encoding consists of a series of blank-delimited or period-delimited numbers. The entire string is enclosed in braces.

User Response: Specify a valid object identifier.

Kerberos database (numbers 95E73A00 - 95E73AFF)

95E73A01   Entry already exists in database.

Explanation: A request to add an entry to the Kerberos database failed because the entry already exists.

User Response: Specify a name that does not already exist in the database.

95E73A02   Unable to store entry in database.

Explanation: An attempt to update the Kerberos database failed.

User Response: Contact your service representative if the error persists.

95E73A03   Unable to read entry from database.

Explanation: An attempt to read an entry from the Kerberos database failed.

User Response: Contact your service representative if the error persists.

95E73A04   Not authorized to perform requested operation.

Explanation: The requested operation cannot be performed because the client principal is not authorized.

User Response: Ask your Kerberos administrator to grant the necessary authority to your Kerberos account.

95E73A05   Entry not found in database.

Explanation: The requested entry is not found in the Kerberos database.

User Response: None

95E73A06   Incorrect use of wildcard character.

Explanation: A wildcard character is used incorrectly as part of a database search request.

User Response: Specify a valid database search argument.

Status codes

95E73A07   Database is in use by another process.

Explanation: The Kerberos database is locked by another process.

User Response: Wait for the other process to release the Kerberos database and then retry the command.

95E73A08   Database modified during read operation.

Explanation: The Kerberos database was modified while a read request was being processed.

User Response: Retry the failing request. Contact your service representative if the error persists.

95E73A09   Database record incomplete or corrupted.

Explanation: A record in the Kerberos database is incomplete or has been corrupted.

User Response: Contact your service representative.

95E73A0A   Recursive database lock request.

Explanation: The database support detected an attempt to lock the Kerberos database by a process that already holds the database lock.

User Response: Contact your service representative.

95E73A0B   Database is not locked.

Explanation: The database support detected an attempt to access the Kerberos database without holding the database lock.

User Response: Contact your service representative.

95E73A0C   Incorrect database lock mode.

Explanation: The database support detected an incorrect lock mode for a request to lock the Kerberos database.

User Response: Contact your service representative.

95E73A0D   Database is not initialized.

Explanation: An attempt to access the Kerberos database failed because the database has not been initialized.

User Response: Contact your service representative.

95E73A0E   Database is already initialized.

Explanation: An attempt to initialize the Kerberos database failed because the database has already been initialized.

User Response: Contact your service representative.

95E73A0F   Incorrect direction for key conversion.

Explanation: An incorrect direction flag was specified for an attempt to convert a Kerberos key.

User Response: Contact your service representative.

95E73A10   No master key for database.

Explanation: The master key for the Kerberos database cannot be found.

User Response: Contact your service representative.

95E73A11   Incorrect master key for database.

Explanation: The master key is not the correct database master key.

User Response: Contact your service representative.

95E73A12   Key size is not valid.

Explanation: The key size for a database entry is not valid.

User Response: Contact your service representative.

95E73A13   Unable to read stored master key.

Explanation: The database support is unable to read the stored master key for the Kerberos database.

User Response: Contact your service representative.

95E73A14   Stored master key is corrupted.

Explanation: The stored master key for the Kerberos database has been corrupted.

User Response: Contact your service representative.

95E73A15   Unable to lock database.

Explanation: The database support is unable to lock the Kerberos database.

User Response: Contact your service representative.

95E73A16   Database corrupted.

Explanation: The Kerberos database is corrupted.

User Response: Contact your service representative.

95E73A17   Unsupported database version.

Explanation: The Kerberos database version is not supported by the current software level.

User Response: Upgrade to a software level that supports the database version.

95E73A18   Unsupported salt type.

Explanation: The password salt type is not supported by the current software level.

User Response: Upgrade to a software level that supports the salt type.

95E73A19   Unsupported encryption type.

Explanation: The encryption type is not supported by the current software level.

User Response: Upgrade to a software level that supports the encryption type.

95E73A1A   Incorrect database creation flags.

Explanation: An attempt to create the Kerberos database failed because the creation request is not correct.

User Response: Contact your service representative.

95E73AF0   Database record is too big.

Explanation: An attempt to create a Kerberos database entry failed because the record is too big. The Kerberos database has a maximum record size of 1024 bytes.

User Response: Contact your service representative.

95E73AF1   Too many matching database records.

Explanation: A database search request resulted in more than 1000 matching records.

User Response: Reduce the amount of data stored for the failing principal or policy.

95E73AF2   Duplicate database entry.

Explanation: A database entry cannot be created because an entry with the same name already exists.

User Response: Use a different name for the new database entry.

95E73AF3   Database entry is still referenced.

Explanation: A database entry cannot be deleted because it is still refered to by other database entries.

User Response: Modify the other database entries to remove the reference to the database entry that is to be deleted. Then retry the delete request.

95E73AF4   Database function is not supported.

Explanation: A database function was requested that is not supported by the current database.

User Response: Do not request unsupported database functions.

95E73AF5   Unknown security server.

Explanation: The requested Kerberos security server is not defined.

User Response: Either define the Kerberos security server or specify an existing security server.

Kerberos runtime codes (numbers 96C73A00 - 96C73CFF)

96C73A01   Client entry in security registry has expired.

Explanation: The client's entry in the registry database has expired.

User Response: Restore the client's access and then retry the request.

96C73A02   Server entry in security registry has expired.

Explanation: The server's entry in the registry database has expired.

User Response: Restore the server's access and then retry the request.

96C73A03   Requested protocol version is not supported.

Explanation: Kerberos request has been encoded using an unsupported protocol version.

User Response: Ensure that the client and the server are at compatible software levels.

96C73A04   Client key is encrypted using an old master key.

Explanation: The client's key was encrypted using an old master key that is no longer contained in the registry database.

User Response: Authenticate the client again in order to obtain a new ticket that is encrypted with the current master key.

96C73A05   Server key is encrypted using an old master key.

Explanation: The server's key was encrypted using an old master key that is no longer contained in the registry database.

User Response: Obtain a new service ticket for the desired server.

Status codes

96C73A06 Client principal is not found in security registry.

Explanation: The client principal in a Kerberos request was not found in the registry database.

User Response: Add the client principal to the registry database and then retry the request.

96C73A07 Server principal is not found in security registry.

Explanation: The server principal in a Kerberos request was not found in the registry database. This error can occur if server principal is not defined in the security registry or if the Kerberos runtime is unable to obtain a TGT for the realm containing the server principal.

User Response: Add the server principal to the registry database for the server realm. Ensure that a trust relationship exists between the client realm and the server realm. Then retry the request.

96C73A08 Server principal is not unique.

Explanation: The server principal in a Kerberos request has multiple entries in the registry database.

User Response: This error should never be reported by the z/OS security server. Contact your service representative.

96C73A09 Key in security registry is not valid.

Explanation: A principal does not have an associated key in the registry database.

User Response: Create a key for the principal and then retry the request.

96C73A0A Ticket is ineligible for postdating.

Explanation: A Kerberos request contains a ″good-since″ date that is in the future. The current security policy does not allowed postdated tickets.

User Response: Retry the request without requesting a postdated ticket.

96C73A0B Effective ticket lifetime is too short.

Explanation: A Kerberos request specifies a lifetime that is less than the minimum lifetime allowed for a ticket.

User Response: Retry the request specifying a longer lifetime.

96C73A0C Ticket request violates account administrative policy.

Explanation: A Kerberos request cannot be processed, for one of the following reasons:

- The client principal in the request is forbidden to have tickets by the administrative policy of the principal account.
- The server principal in the request is forbidden to be a server by the administrative policy of the principal account..
- The request asks for a ticket-granting ticket that allows postdating of tickets, which is not allowed by the client principal account.
- The request indicates that it is from a local client, but the contents of the request indicate that the request originates from a client in a foreign cell.
- The ticket-granting ticket in a request to the ticket-granting service has options that are not valid.

User Response: Change the appropriate administrative policy to permit the request.

96C73A0D Ticket cannot be granted with requested properties.

Explanation: A Kerberos request cannot be processed because one or more of the ticket options are either not supported or are not allowed by the account policy.

User Response: Change the account policy if desired and then retry the request.

96C73A0E Encryption type is not supported.

Explanation: A Kerberos request contains an encryption type that is not supported by the security server.

User Response: Specify a supported encryption type and then retry the request. Ensure that the client and server software levels are compatible.

96C73A0F Checksum type is not supported.

Explanation: A Kerberos request contains a checksum type that is not supported by the security server.

User Response: Specify a supported checksum type and then retry the request. Ensure that the client and server software levels are compatible.

96C73A10 Preauthentication type is not supported.

Explanation: A Kerberos request contains a preauthentication type that is not supported by the security server. This error can occur if a request for a service ticket does not contain the ticket-granting ticket for the client.

User Response: Provide the ticket-granting ticket

when making a request to the ticket-granting service. Ensure that the client and server software levels are compatible.

96C73A11   Transited ticket not supported.

Explanation: A Kerberos request for a foreign principal contains a ticket-granting ticket granted by a foreign realm. The foreign realm is not a trust peer of the security server receiving the request.

User Response: Use a ticket-granting ticket granted by the security server that will process the request or establish a trusted peer relationship between the two realms.

96C73A12   Client account is revoked.

Explanation: The ″account valid″ indicator is not set for the client account.

User Response: Set the ″account valid″ indicator for the client account. Then retry the request.

96C73A13   Server account is revoked.

Explanation: The ″account valid″ indicator is not set for the server account.

User Response: Set the ″account valid″ indicator for the server account. Then retry the request.

96C73A14   Ticket-granting ticket is expired.

Explanation: The expiration time for a ticket has been reached.

User Response: Obtain a new ticket-granting ticket and then retry the request.

96C73A15   Client account is not yet valid.

Explanation: The ″good-since″ time for a client account is in the future.

User Response: Wait until the client account becomes valid or change the ″good-since″ time for the account. Then retry the request.

96C73A16   Server account is not yet valid.

Explanation: The ″good-since″ time for a server account is in the future.

User Response: Wait until the server account becomes valid or change the ″good-since″ time for the account. Then retry the request.

96C73A17   Password is expired.

Explanation: The principal's password has expired.

User Response: Change the password for the principal and then retry the request.

96C73A18   Preauthentication failed.

Explanation: Preauthentication failed for a Kerberos request.

User Response: Retry the failing request. Contact your service representative if the error persists.

96C73A19   Preauthentication required.

Explanation: An initial ticket request does not contain preauthentication data. The account policy for the principal requires preauthentication.

User Response: Retry the request and provide preauthentication data.

96C73A1A   Ticket is not for the requested server.

Explanation: The ticket supplied with a Kerberos request is not for the server specified in the request.

User Response: Retry the request and provide the proper ticket.

96C73A1B   Server requires ticket encrypted with session key.

Explanation: A request for a service ticket does not contain a session key. The account policy for the requested server requires that tickets be encrypted with a session key and not with the server key.

User Response: Retry the request and provide the session key.

96C73A1C   Transited path rejected.

Explanation: The KDC rejected the transited path encoded in the ticket-granting ticket provided with the request. This indicates that one of the realms involved in granting the ticket is not trusted by the KDC.

User Response: Contact your administrator to update the trust relationships between the realms.

96C73A1D   Service is not available.

Explanation: The requested service is not available.

User Response: Retry the request. Contact your administrator if the problem persists.

Status codes

96C73A1F   Integrity check fails.

Explanation: The checksum computed using the decrypted message is not the same as the checksum contained within the message. This error can occur if the message has been modified or the wrong key was used to decrypt the message. This error can also occur if the checksum contained in the authenticator does not match the checksum computed using the supplied application data.

User Response: Verify that the message was not modified. Retry the request if an incorrect key was used.Contact your service representative if the error persists.

96C73A20   Ticket is expired.

Explanation: A Kerberos request cannot be completed because the associated ticket has expired.

User Response: Obtain a new ticket and then retry the request.

96C73A21   Ticket is not yet valid.

Explanation: A Kerberos request cannot be completed because the start time for the associated ticket is in the future.

User Response: Obtain a new ticket or wait until the current ticket is valid. Then retry the request.

96C73A22   Replay attempt detected.

Explanation: The Kerberos replay detection mechanism indicates that the received request is a replay of a prior request.

User Response: Try the request again. Contact your service representative if the error persists.

96C73A23   Server name is not correct.

Explanation: A Kerberos request contains a ticket-granting ticket for another ticket-granting service.

User Response: Obtain a ticket to the desired ticket-granting service and then retry the request. Contact your service representative if the error persists.

96C73A24   Client name is not correct.

Explanation: The client principal stored in the authenticator part of the Kerberos request does not match the client principal stored in the accompanying ticket.

User Response: Ensure that the proper authenticator is used and then retry the request. Contact your service representative if the error persists.

96C73A25   Time differential exceeds maximum clock skew.

Explanation: The absolute difference between the timestamp in the message and the current system time is greater than the maximum clock skew value (normally 5 minutes). This problem can occur if the time on the client system is not the same as the time on the server system.

User Response: Ensure that the time on both systems is synchronized properly.

96C73A26   Network address is not correct.

Explanation: The address of the message sender does not match any of the possible client addresses stored in the associated ticket.

User Response: Obtain a new ticket containing the correct client addresses. Then retry the request. Contact your service representative if the error persists.

96C73A27   Message protocol version is not correct.

Explanation: The protocol version in a Kerberos message is not correct or is not supported by the security server.

User Response: Ensure that the client and server software levels are compatible. Then retry the request. Contact your service representative if the error persists.

96C73A28   Message type is not correct.

Explanation: The message type in Kerberos message is not correct or is not supported by the security server.

User Response: Ensure that the client and server software levels are compatible. Then retry the request. Contact your service representative if the error persists.

96C73A29   Message stream is modified.

Explanation: The messge packet sent to or received from the security server has been modified.

User Response: Ensure that there are no communication problems between the client and the server. Then retry the request. Contact your service representative if the error persists.

96C73A2A   Security message received in incorrect order.

Explanation: A security message was received that is not in the correct sequence.

User Response: Ensure that there are no communication problems between the client and the server. Then retry the request. Contact your service representative if the error persists.

96C73A2B   Illegal cross-realm ticket.

Explanation: An illegal cross-realm ticket was found when parsing an authorization service message.

User Response: Obtain a ticket to the server that the request is attempting to access. Then retry the request. Contact your service representative if the error persists.

96C73A2C   Service key version is not correct.

Explanation: The ticket associated with a Kerberos request specifies a server key type that is not correct or a server key version that is no longer contained in the registry database.

User Response: Obtain a new ticket to the server that the request is attempting to access. Then retry the request. Contact your service representative if the error persists.

96C73A2D   Service key is not available.

Explanation: The server key is not available for the server principal specified in a ticket. This error can occur if the server account was deleted after the ticket was granted.

User Response: Recreate the server account and then retry the request.

96C73A2E   Mutual authentication fails.

Explanation: A mutual authentication attempt failed.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A2F   Message direction is incorrect.

Explanation: The message direction in a Kerberos message stream is incorrect. This error can occur if Kerberos peer services are being used and one of the messages is received out of order.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A30   Alternative authentication method required.

Explanation: A Kerberos request specifies an authentication method that is not supported by the security server. An alternative authentication method is required.

User Response: Ensure that the client and server software levels are compatible. Then retry the request using an authentication method that is supported by the server.

96C73A31   Message sequence number is incorrect.

Explanation: A message was received containing an incorrect sequence number. This error can occur if one or more messages have been dropped by the communications network.

User Response: Ensure that no communication errors are causing messages to be lost. Then retry the request. Contact your service representative if the error persists.

96C73A32   Checksum type is not appropriate.

Explanation: A checksum type has been selected that does not have the required properties for use with a security message. For example, generated checksums may not be unique using the selected checksum algorithm.

User Response: Retry the request using an appropriate checksum type.

96C73A33   Transited path rejected.

Explanation: The application server rejected the transited path encoded in the service ticket provided with the request. This indicates that one of the realms involved in granting the ticket is not trusted by the server.

User Response: Contact the application administrator to update the trust relationships between the realms.

96C73A34   Response too large for datagram.

Explanation: The response cannot be returned because it is too large for a UDP datagram.

User Response: Increase the maximum datagram size or change the application to use TCP instead of UDP for its communications.

96C73A3C   Generic error occurs.

Explanation: An error has occurred that is not covered by any of the specific status codes defined for the Kerberos Key Distribution Center (KDC) component. Check the security server message log for more information about the cause of this error.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A3D   Message field is too long.

Explanation: A Kerberos message contains a field that is longer than the maximum length supported by the security server.

User Response: Ensure that the client and server software levels are compatible. Then retry the request.

Status codes

Contact your service representative if the error persists.

96C73A81   **Lock request is not valid.**

Explanation: A request to lock a file does not specify a valid lock type.

User Response: Specify a valid lock type and retry the request.

96C73A82   **Unable to read password.**

Explanation: An attempt to read a password from the terminal failed due to an input/output error. This error can also occur if no password is entered.

User Response: Ensure that a valid input device is available to the application. Then retry the request. Contact your service representative if the error persists.

96C73A83   **Password does not match expected value.**

Explanation: The supplied password does not match the expected value. This error can occur if the same password is not specified for both the password prompt and the password validation prompt.

User Response: Specify the same password for both the password prompt and the password validation prompt.

96C73A84   **Password read is interrupted.**

Explanation: An interrupt signal was received while reading the password from the terminal.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A85   **Illegal character in component name.**

Explanation: A component of a Kerberos name contains an illegal character.

User Response: Ensure that a valid input device is available to the application. Then retry the request. Contact your service representative if the error persists.

96C73A86   **Principal name is not valid.**

Explanation: An error was detected while parsing the string representation of a principal name. The string representation consists of the name followed by an optional realm separated by ″@″ (the @ must be omitted if no realm is specified).

User Response: Ensure that the principal name is properly formed.

96C73A87   **Unable to open Kerberos configuration file.**

Explanation: The Kerberos configuration file cannot be opened.

User Response: Ensure that the configuration file exists and that the file permissions allow read access. Contact your service representative if the error persists.

96C73A88   **Kerberos configuration file format is not valid.**

Explanation: The Kerberos configuration file format is not valid. Refer to the administration guide for more information about the proper format of the file.

User Response: Correct the file format errors and then retry the request.

96C73A89   **Buffer is too small.**

Explanation: The buffer specified on a Kerberos function call is too small to hold all of the return information.

User Response: Specify a larger buffer and then retry the request. Contact your service representative if the error persists.

96C73A8A   **Message type is not valid.**

Explanation: A Kerberos message cannot be encoded because the message type is not correct or is not supported by the current software level.

User Response: Ensure that the software is at the correct level and then retry the request. Contact your service representative if the error persists.

96C73A8B   **Credentials cache name is not valid.**

Explanation: The credentials cache name is not valid. A credentials cache name consists of an optional cache type followed by the name separated by a colon (:). The colon must be omitted if no cache type is specified.

User Response: Specify a valid credentials cache name and then retry the request.

96C73A8C   **Credentials cache type is not valid.**

Explanation: The credentials cache type is not valid or is not supported by the current software level. This error can occur if an application-specific cache type is specified and the cache type has not been registered with the Kerberos runtime.

User Response: Specify a valid credentials cache type and then retry the request.

96C73A8D   Matching credential is not found.

Explanation: A search of the credentials cache does not find a credential with the requested attributes.

User Response: Change the search criteria and then retry the request.

96C73A8E   End of credentials cache is reached.

Explanation: A read request has reached the end of the credentials cache.

User Response: No action is required.

96C73A8F   Required ticket is not supplied.

Explanation: A Kerberos request does not have a required ticket or the ticket is not complete.

User Response: Refresh the credentials cache and then retry the request. Contact your service representative if the error persists.

96C73A90   Application server principal is not correct.

Explanation: The server principal in an application message does not match the principal name of the server receiving the request.

User Response: Ensure that the application message is sent to the proper server. Contact your service representative if the error persists.

96C73A91   Application ticket is not valid.

Explanation: The ticket in an application message is not valid.

User Response: Obtain a new service ticket and then retry the request. Contact your service representative if the error persists.

96C73A92   Principals do not match.

Explanation: An attempt to obtain credentials failed because the principal in the ticket-granting ticket does not match the target principal.

User Response: Obtain a ticket-granting ticket for the correct principal and then retry the request.

96C73A93   Security server reply is modified.

Explanation: The values in the security server reply are not consistent with the request that was sent to the security server.

User Response: Ensure that the security server reply was not modified. Contact your service representative if the error persists.

96C73A94   Clock skew in reply exceeds maximum value.

Explanation: The absolute difference between the timestamp in the security server reply and the local system time exceeds the maximum clock skew (normally 5 minutes).

User Response: Ensure that the client and server system times are synchronized properly.

96C73A95   Realm mismatch in initial ticket request.

Explanation: The client realm is not the same as the principal realm in an initial ticket request.

User Response: Ensure that the initial ticket request is sent to the security server for the client realm.

96C73A96   Encryption type is not valid.

Explanation: A Kerberos message specifies an encryption type that is not valid or is not supported by the current software level.

User Response: Specify a valid encryption type and then retry the request. Contact your service representative if the error persists.

96C73A97   Key type is not valid.

Explanation: A Kerberos message specifies a key type that is not valid or is not supported by the current software level.

User Response: Specify a valid key type and then retry the request. Contact your service representtive if the error persists.

96C73A98   Encryption type is not correct.

Explanation: A Kerberos message is encrypted with the incorrect encryption type.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A99   Checksum type is not valid.

Explanation: A Kerberos message specifies a checksum type that is not valid or is not supported by the current software level.

User Response: Specify a valid checksum type and then retry the request. Contact your service representative if the error persists.

Status codes

96C73A9A   **Unable to locate security server.**

Explanation: The Kerberos runtime is unable to locate the security server for the requested realm.

User Response: Ensure that the requested realm is defined in the LDAP directory, the DNS name server, or the Kerberos configuration file. Ensure that the appropriate lookup mode is enabled in the Kerberos configuration file. Then retry the request.

96C73A9B   **Kerberos service is not defined.**

Explanation: The requested Kerberos service is not defined or is not supported by the current software level.

User Response: For an undefined service, define the desired service and then retry the request. For an unsupported service, upgrade to a software level that supports the service.

96C73A9C   **Unable to contact security server.**

Explanation: The Kerberos runtime was unable to contact the security server for the requested realm.

User Response: Ensure that the security server is running and is defined correctly in the LDAP directory, the DNS name server, or the Kerberos configuration file. Ensure that the appropriate lookup mode is enabled in the Kerberos configuration file. Then retry the request.

96C73A9D   **No local name found for principal.**

Explanation: The Kerberos runtime was unable to translate a foreign principal to a local name.

User Response: Ensure that a local name is defined for the foreign principal. Then try the request again.

96C73A9E   **Mutual authentication fails.**

Explanation: A mutual authentication request was not successful.

User Response: Retry the request. Contact your service representative if the error persists.

96C73A9F   **Replay cache type is already registered.**

Explanation: The replay cache type is already registered with the Kerberos runtime.

User Response: No action is required.

96C73AA0   **Replay cache operation is unable to allocate memory.**

Explanation: A memory allocation request failed for a replay cache control block.

User Response: Increase the amount of memory

available to the application and then retry the request.

96C73AA1   **Replay cache type is not valid.**

Explanation: The requested replay cache type is not valid or is not supported by the current software level. This error can occur if an application-specific cache type is requested and the cache type has not been registered with the Kerberos runtime.

User Response: Register the cache type with the Kerberos runtime and then retry the request.

96C73AA2   **Replay cache operation detects an unexpected error.**

Explanation: An internal error was detected during a replay cache operation.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AA3   **Message is a replay.**

Explanation: The current message is a replay of a previous message.

User Response: Ensure that your network has not been compromised and communication errors are not causing messages to be retransmitted. Contact your service representative if the error persists.

96C73AA4   **Replay cache operation fails.**

Explanation: A replay cache operation failed due to a file system error.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AA7   **Replay cache file is truncated.**

Explanation: An attempt to read from the replay cache file failed due to a premature end-of-file.

User Response: Ensure that the replay cache file has not been modified. Contact your service representative if the error persists.

96C73AA8   **Replay cache file operation is unable to allocate memory.**

Explanation: A memory allocation request failed for a replay cache file request.

User Response: Increase the amount of memory available to the application and then retry the request.

96C73AA9   Replay cache operation is unable to access file.

Explanation: An attempt to read from or write to the replay cache file failed.

User Response: Ensure that the replay cache file is not damaged and that the file permissions allow the desired file access. Contact your service representative if the error persists.

96C73AAA   Replay cache file system request fails.

Explanation: A file system request failed for the replay cache file.

User Response: Ensure that the replay cache file is not damaged. Contact your service representative if the error persists.

96C73AAB   Replay cache operation fails.

Explanation: A replay cache operation failed due to an internal error.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AAC   Replay cache operation fails due to insufficient space.

Explanation: A replay cache operation failed due to insufficient space in the file system.

User Response: Increase the available space in the file system and then retry the request.

96C73AB2   Cryptographic system detects an unexpected error.

Explanation: An unexpected error was detected by the Kerberos cryptographic system.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AB3   Key table name is not valid.

Explanation: The key table name is not valid. A key table name consists of an optional key table type followed by the name separated by a colon (:). The colon must be omitted if the key table type is not specified.

User Response: Specify a valid key table name and then retry the request.

96C73AB4   Key table type is not valid.

Explanation: The key table type is not valid or is not supported by the current software level. This error can occur if an application-specific key table type is specified, and the key table type has not been

registered with the Kerberos runtime.

User Response: Register the key table type with the Kerberos runtime and then retry the request.

96C73AB5   Key table entry is not found.

Explanation: The requested key table entry was not found in the key table.

User Response: No action is required.

96C73AB6   End of key table is reached.

Explanation: A key table read operation failed because the end of the key table was reached.

User Response: No action is required.

96C73AB7   Key table does not support write operations.

Explanation: An attempt to add or delete a key table entry failed because the key table does not support write operations. This error can occur if the key table is opened using the FILE key table type instead of the WRFILE key table type.

User Response: Change the key table type to WRFILE and then retry the request.

96C73AB8   Key table operation fails due to file system error.

Explanation: An attempt to read from or write to a key table failed due to a file system error.

User Response: Ensure that the key table file was not damaged and then retry the request. Contact your service representative if the error persists.

96C73AB9   No ticket is found for ticket-granting service.

Explanation: An attempt to obtain a service or privilege ticket failed because no ticket was found for the ticket-granting service. This error can occur if the ticket-granting ticket (TGT) has expired and the application has not renewed it.

User Response: Obtain a ticket-granting ticket for the desired ticket-granting service and then retry the request.

96C73ABA   Key parity is not correct.

Explanation: A Data Encryption Standard (DES) key was supplied to the Kerberos cryptographic system. The DES key has incorrect parity. This error can occur if the DES key has been modified.

User Response: Supply a valid DES key and then retry the request. Contact your service representative if the error persists.

Status codes

96C73ABB   Key does not provide adequate security.

Explanation: A Data Encryption Standard (DES) key was supplied to the Kerberos cryptographic system. The DES key is weak and does not provide adequate security for use by Kerberos.

User Response: Supply a valid DES key and then retry the request. Contact your service representative if the error persists.

96C73ABC   Encryption or checksum type is not supported.

Explanation: A cryptographic request failed because the requested encryption or checksum type is not supported.

User Response: Specify a supported encryption or checksum type and then retry the request.

96C73ABD   Key size is not valid.

Explanation: A key was supplied to the Kerberos cryptographic system. The key size is not valid.

User Response: Specify a valid cryptographic key and then retry the request.

96C73ABE   Encrypted message is too small.

Explanation: A request to decrypt a message failed because the message length is less than the minimum length for an encrypted message or the result buffer is smaller than the source buffer. A request to encrypt a message failed because the result buffer is too small. This error can also occur if the length of the initial vector is not correct for the requested encryption algorithm.

User Response: For an error during decryption,ensure that the message has not been modified, and then retry the request. For an error during encryption, call the **krb5_c_encrypt_length()** routine to determine the required length for the result buffer. Contact your service representative if the error persists.

96C73ABF   Credentials cache type is already registered.

Explanation: A request to register a credentials cache type failed because the credentials cache type is already registered with the Kerberos runtime.

User Response: No action is required.

96C73AC0   Key table type is already registered.

Explanation: A request to register a key table type failed because the key table type is already registered with the Kerberos runtime.

User Response: No action is required.

96C73AC1   Credentials cache file operation fails.

Explanation: A file system request failed for the credentials cache file.

User Response: Ensure that the credentials cache file was not damaged and then retry the request. Contact your service representative if the error persists.

96C73AC2   Credentials cache file cannot be accessed.

Explanation: The credentials cache file cannot be accessed due to a file system error.

User Response: Ensure that the credentials cache file exists and the file permissions permit the application to access the file. Then retry the request. Contact your service representative if the error persists.

96C73AC3   Credentials cache file does not exist.

Explanation: The credentials cache file does not exist.

User Response: Specify an existing credentials cache file and then retry the request.

96C73AC4   Credentials cache operation detects an unexpected error.

Explanation: A credentials cache operations failed due to an internal error.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AC5   Credentials cache write operation fails.

Explanation: A credentials cache write request failed due to a file system error.

User Response: Retry the request. Contact your service representative if the error persists.

96C73AC6   Credentials cache operation is unable to allocate memory.

Explanation: A credentials cache request was unable to allocate memory.

User Response: Increase the amount of memory available to the application and then retry the request. Contact your service representative if the error persists.

96C73AC7   Credentials cache format is not valid.

Explanation: Credentials cache format is not valid.

User Response: Specify a credentials cache format that is supported and then retry the request. Contact your service representative if the error persists.

96C73AC8   Credentials request specifies incorrect options.

Explanation: A security credentials request specifies options that are not correct or are not supported by the current software level.

User Response: Specify valid options and then retry the request. Contact your service representative if the error persists.

96C73AC9   Credentials request does not contain second ticket.

Explanation: A credentials request cannot be processed because two tickets are required, and the request does not contain the second ticket.

User Response: Provide the second ticket and then retry the request. Contact your service representative if the error persists.

96C73ACA   No credentials are available.

Explanation: A Kerberos function was called, but no credentials are provided by the caller.

User Response: Provide the required credentials and then retry the request. Contact your service representative if the error persists.

96C73ACB   Incorrect authentication protocol version.

Explanation: The authentication protocol version in the message stream is not supported by the **krb5_recvauth()** routine.

User Response: Ensure that compatible levels of the Kerberos runtime are installed on the local and remote systems. Contact your service representative if the error persists.

96C73ACC   Incorrect application version identifier.

Explanation: The application version identifier specified for the **krb5_recvauth()** routine does not match the application version identifier specified for the **krb5_sendauth()** routine.

User Response: Specify the same application version identifier string.

96C73ACD   Unrecognized response received from remote application

Explanation: The remote application returned an unrecognized response.

User Response: Ensure that compatible levels of the Kerberos runtime are installed on the local and remote systems. Contact your service representative if the error persists.

96C73ACE   Authentication rejected by application server.

Explanation: The remote application server has rejected the client authentication.

User Response: Contact the application support programmer.

96C73ACF   Preauthentication type is not valid.

Explanation: The preauthentication type is not valid or is not supported by the current software level.

User Response: Specify a valid preauthentication type and then retry the request. Contact your service representative if the error persists.

96C73AD0   No preauthentication key is provided.

Explanation: The Kerberos runtime is unable to encrypt the preauthentication data because the encryption key is not provided by the application.

User Response: Provide the required encryption key and then retry the request. Contact your service representative if the error presists.

96C73AD1   Preauthentication fails.

Explanation: A preauthentication request failed. This error can occur if the incorrect principal key is specified. It can also occur if the system clocks on the client and server systems are not within 5 minutes of each other.

User Response: Ensure that the system clocks are synchronized and the correct principal key is specified. Then retry the request. Contact your service representative if the error persists.

96C73AD2   Replay cache version number is not valid.

Explanation: The replay cache version number is not valid or is not supported by the current software level.

User Response: Ensure that the replay cache file has not been modified and then retry the request. Contact your service representative if the error persists.

96C73AD3   Credentials cache version number is not valid.

Explanation: The credentials cache version number is not valid or is not supported by the current software level.

User Response: Ensure that the credentials cache file has not been modified and then retry the request. Contact your service representative if the error persists.

Status codes

96C73AD4   Key table version number is not valid.

Explanation: The key table version number is not valid or is not supported by the current software level.

User Response: Ensure that the key table file has not been modified and then retry the request. Contact your service representative if the error persists.

96C73AD5   Address type is not valid.

Explanation: The network address type is not valid or is not supported by the current software level.

User Response: Provide a valid network address type and then retry the request. Contact your service representative if the error persists.

96C73AD6   Replay detection requires a replay cache.

Explanation: Replay detection was requested but no replay cache is available.

User Response: Set up a replay cache and then retry the request. Contact your service representative if the error persists.

96C73AD7   Host name is not defined.

Explanation: An attempt to obtain the network host entry using the **gethostbyname()** or **gethostbyaddr()** function failed. The most likely cause of this error is that the host name or network address is not defined to the domain name service.

User Response: Ensure that the host name is defined to the domain name service and that name resolution is working. Then retry the request. Contact your service representative if the error persists.

96C73AD8   Host realm is not defined.

Explanation: The realm corresponding to a host name cannot be determined.

User Response: Ensure the host realm is defined in the Kerberos configuration file and then retry the request. Contact your service representative if the error persists.

96C73AD9   Name cannot be converted to service principal.

Explanation: A name was provided that cannot be converted to a service principal because no conversion exists for the name type.

User Response: Provide a name that can be converted to a service principal and then retry the request. Contact your service representative if the error persists.

96C73ADA   Initial ticket response generated by Kerberos Version 4.

Explanation: The response to an initial ticket response is in Kerberos Version 4 format. The Kerberos runtime supports only Kerberos Version 5 formats.

User Response: Send the initial ticket request to a Kerberos Version 5 security server. Contact your service representative if the error persists.

96C73ADB   Security server is not defined for requested realm.

Explanation: The Kerberos runtime is unable to locate the security server for the requested realm. This error can occur if the requested realm is not defined or if the security server host name cannot be resolved to a network address.

User Response: Ensure the security server is defined in either the LDAP directory or the Kerberos configuration file and then retry the request. Contact your service representative if the error persists.

96C73ADC   Ticket-granting ticket does not allow ticket forwarding.

Explanation: An attempt to obtain a forwarded ticket failed because the ticket-granting ticket (TGT) provided with the request does not allow ticket forwarding.

User Response: Provide a ticket that allows ticket forwarding and then retry the request. Contact your service representative if the error persists.

96C73ADD   Principal name is not correct for forwarding credentials.

Explanation: The principal name is not correct for forwarding credentials. The principal name type must be KRB5_NT_SRV_HST. When creating forwarded credentials for use with GSS-API delegation, the target name must have been imported by specifying GSS_C_OID_KRBV5_SERVICE as the name type on the **gss_import_name()** function call.

User Response: Create the principal name in the proper format and then retry the request. Contact your service representative if the error persists.

96C73ADE   Request loop is detected while obtaining initial ticket.

Explanation: The **krb5_get_in_tkt()** function detects a request loop while obtaining the intermediate ticket-granting tickets necessary to process the request. This error can occur if the peer trust relationships are not correct between the security servers in the intermediate realms.

User Response: Retry the request. Contact your service representative if the error persists.

96C73ADF No default realm is specified in the configuration file.

Explanation: The Kerberos configuration file does not define a default realm.

User Response: Define a default realm in the configuration file. Then retry the request.

96C73AE1 Key table name is too long.

Explanation: The key table name is too long.

User Response: Specify a valid key table name and then retry the request.

96C73C00 Unable to load code page table.

Explanation: The Kerberos runtime is unable to load the tables that are used to convert text strings between the network code page and the local code page.

User Response: Contact your service representative if the error persists.

96C73C01 Unable to convert text string.

Explanation: The Kerberos runtime is unable to convert a text string to/from the network code page.

User Response: Contact your service representative if the error persists.

96C73C02 Unable to allocate memory.

Explanation: The Kerberos runtime was unable to allocate memory for a control block.

User Response: Increment the memory available to the application and then retry the request. Contact your service representative if the error persists.

96C73C03 Unable to obtain the current time.

Explanation: The Kerberos runtime is unable to obtain the current time of day.

User Response: Verify that the system time provider is running and is configured properly. Contact your service representative if the error persists.

96C73C04 Key table file specification is not valid.

Explanation: The key table file specification is not valid. Either the file name is not correct or the file cannot be accessed.

User Response: Verify that the file name is correct and that the file permissions allow access by the application. Then retry the request. Contact your service representative if the error persists.

96C73C05 Key table operation encounters unexpected error.

Explanation: An unexpected error was detected during a key table operation.

User Response: Contact your service representative if the error persists.

96C73C06 Unable to create socket.

Explanation: The Kerberos runtime was unable to create a socket because the **socket()** function failed.

User Response: Contact your service representative if the error persists.

96C73C07 Unable to obtain local address information.

Explanation: The Kerberos runtime was unable to obtain local address information for a socket because the **ioctl()** function failed.

User Response: Contact your service representative if the error persists.

96C73C08 Control block validation fails.

Explanation: A Kerberos control block does not contain the proper identifier value.

User Response: Verify that the control block was not modified. Contact your service representative if the error persists.

96C73C09 Invalid parameter specified on function call.

Explanation: A parameter specified on a Kerberos function call is not correct.

User Response: Verify that the proper parameters are specified and then retry the request. Contact your service representative if the error persists.

96C73C13 Unable to send data to remote application.

Explanation: The Kerberos runtime is unable to send data to the remote application.

User Response: Ensure that there are no network problems and that the remote application is running. Contact your service representative if the error persists.

96C73C14 Unable to receive data from remote application.

Explanation: The Kerberos runtime is unable to receive data from the remote application.

User Response: Ensure there are no network problems and the remote application is running. Contact

Status codes

your service representative if the error persists.

96C73C15   Connection closed by remote application.

Explanation: The Kerberos runtime is unable to receive data from the remote application because the connection has been closed. This error can occur if the local system is not authorized to establish a connection with the remote system.

User Response: Ensure that there are no network problems, that the remote application is running, and that the local system is authorized to establish the connection. Contact your service representative if the error persists.

96C73C0A   Unsupported Kerberos function requested.

Explanation: A Kerberos function was requested that is not implemented in the current software configuration.

User Response: Change the application to request a supported function.

96C73C0B   Replay cache file does not exist.

Explanation: The replay cache file does not exist.

User Response: Verify that the replay cache file exists and that the file permissions allow access by the application.

96C73C0C   Not authorized to access credentials cache.

Explanation: The application is not authorized to access the credentials cache.

User Response: Verify that the credentials cache access permissions allow access by the application.

96C73C0D   Not authorized to access replay cache.

Explanation: The application is not authorized to access the replay cache.

User Response: Verify that the file permissions allow access by the application.

96C73C0E   Not authorized to access key table.

Explanation: The application is not authorized to access the key table.

User Response: Verify that the file permissions allow access by the application.

96C73C0F   Data privacy service is not available.

Explanation: The requested cryptographic algorithm is not available. This error can occur if the software algorithm is not installed or if a cryptographic algorithm requires the use of a hardware cryptographic processor that is not available on the current system.

User Response: Ensure that the proper hardware and software is installed for the cryptographic algorithm.

96C73C10   Unable to retrieve message *msg-identifier* **from the message catalog.**

Explanation: The security runtime is unable to retrieve message text from the message catalog.

User Response: Ensure the NLSPATH environment variable is set properly and then retry the request. Contact your service representative if the error persists.

96C73C11   Unable to contact server.

Explanation: The Kerberos runtime is unable to contact the server providing the requested service.

User Response: Ensure that the server is running and is defined correctly in the LDAP directory, the DNS name server, or the Kerberos configuration file. Ensure that the appropriate lookup mode is enabled in the Kerberos configuration file. Then retry the request.

96C73C12   Key version value is not supported by the key table format.

Explanation: The key version value is not within the range supported by the key table format. The current key table implementations store the key version as a 1-byte value. This means the key version must be between 1 and 255 when stored in a key table.

User Response: Use a key version between 1 and 255. If the Kerberos database does not allow the key version to be reset for a principal, you must delete the principal from the database and then add it again in order to reset the key version to 1.

Profile operations codes (numbers AACA6000 - AACA60FF)

AACA6002   Profile section is not found.

Explanation: A profile read request failed because the requested profile section was not found.

User Response: No action is required.

AACA6003   Profile relation is not found.

Explanation: A profile read request failed because the requested profile relation was not found.

User Response: No action is required.

AACA6004   Profile node is not a section node.

Explanation: A profile add was requested, but the supplied node is not a section node.

User Response: Provide a section node and retry the request.

AACA6005   Profile section node has a value.

Explanation: A profile section node is not allowed to have a value.

User Response: Verify that the configuration file is formatted properly. Contact your service representative if the error persists.

AACA6009   Profile section does not have a parent.

Explanation: The parent pointer in a profile section node is not valid.

User Response: Verify that the profile entries in memory are not corrupted. Contact your service representative if the error persists.

AACA600A   Profile section is not correct.

Explanation: A profile section is not formatted correctly.

User Response: Verify that the configuration file is formatted properly. Contact your service representative if the error persists.

AACA600B   Profile relation is not correct.

Explanation: A profile relation is not formatted correctly.

User Response: Verify that the configuration file is formatted properly. Contact your service representative if the error persists.

AACA600C   Extra closing brace is specified.

Explanation: An extra closing brace was found in a list of relations while processing a profile definition.

User Response: Verify that the configuration file is formatted properly. Contact your service representative if the error persists.

AACA600D   Opening brace is missing.

Explanation: An opening brace is missing for a list of relations while processing a profile definition.

User Response: Verify that the configuration file is formatted properly. Contact your service representative if the error persists.

AACA6013   Profile name set is not correct.

Explanation: The set of names specified for a profile lookup operation is not correct. The name set must include at least the section name and the relation name.

User Response: Specify a valid name set and retry the request.

AACA6014   No profile is available.

Explanation: No Kerberos profile was found.

User Response: Create a Kerberos configuration file if needed.

Status codes

Chapter 6. Messages

This chapter contains three sets of messages:

- Messages from the Kerberos runtime (EUVF02000 through EUVF03999)
- Messages from the security server (EUVF04000 through EUVF05999)
- Messages from Kerberos commands (EUVF06000 through EUVF06999).

Messages are listed in numerical order.

Kerberos runtime messages (numbers EUVF02000 - EUVF03999)

EUVF02001E   Unable to read a required input parameter.

Explanation: An attempt to read a required input parameter failed.

User Response: Verify that all required parameters are specified and then retry the request. Contact your service representative if the error persists.

EUVF02002E   Unable to modify a required output parameter.

Explanation: An attempt to modify a required output parameter fails.

User Response: Verify that all required parameters are specified and then retry the request. Contact your service representative if the error persists.

EUVF02003E   Parameter is incorrectly structured.

Explanation: A parameter is incorrectly structured.

User Response: Verify that all parameters are correct and then retry the request. Contact your service representative if the error persists.

EUVF02004E   Security mechanism is not supported.

Explanation: The security mechanism is not valid or is not supported by the current software level.

User Response: Specify a security mechanism that is supported by the current software level. Contact your service representative if the error persists.

EUVF02005E   Name value is not valid.

Explanation: The specified name value is not valid.

User Response: Specify a valid name value and then retry the request. Contact your service representative if the error persists.

EUVF02006E   Name type is not valid.

Explanation: The specified name type is not valid.

User Response: Specify a valid name type and then retry the request. Contact your service representative if the error persists.

EUVF02007E   Channel bindings do not match token bindings.

Explanation: The channel bindings specified on the function call do not match the channel bindings contained in the input token.

User Response: Ensure that the security context initiator is specifying the correct channel bindings. Contact your service representative if the error persists.

EUVF02008E   Status value is not valid.

Explanation: The status value passed to the **gss_display_status()** function is not a valid GSSAPI status.

User Response: Verify that the status value is not modified. Contact your service representative if the error persists.

EUVF02009E   Token signature is not correct.

Explanation: The checksum computed from the token data does not match the signature contained in the token.

User Response: Verify that the token is not modified. Contact your service representative if the error persists.

EUVF02010E   No security credential supplied.

Explanation: Either the supplied security credential is not valid for context acceptance or the credential handle is not valid.

User Response: Provide a valid security credential that can be used to accept a security context.

Messages

EUVF02011E   No security context established.

Explanation: The requested function requires a security context but no security context is supplied.

User Response: Provide a security context and then retry the request.

EUVF02012E   Token is not valid.

Explanation: The token contents are not valid.

User Response: Verify that the token is not modified and then retry the request. Contact your service representative if the error persists.

EUVF02013E   Security credential is not valid.

Explanation: The security credential is not valid because internal consistency checks fail.

User Response: Verify that no storage overlay has occurred and then retry the request. Contact your service representative if the error persists.

EUVF02014E   Security credential is expired.

Explanation: Either the security credential lifetime is expired or the associated ticket is no longer valid.

User Response: Create a new security credential and then retry the request. Contact your service representative if the error persists.

EUVF02015E   Security context is expired.

Explanation: Either the security context lifetime is expired or the associated security credential is no longer valid.

User Response: Create a new security context and then retry the request. Contact your service representative if the error persists.

EUVF02016E   Security mechanism detects error.

Explanation: The security mechanism detects an error. The minor status code provides additional information concerning the error. The minor status code is zero if the error cannot be isolated to a single security mechanism.

User Response: Refer to the minor status code to determine the action to be taken. Contact your service representative if the error persists.

EUVF02017E   Quality of protection value is not valid.

Explanation: The quality of protection value is not valid or is not supported by the current software level.

User Response: Specify a valid quality of protection value and then retry the request. Contact your service

representative if the error persists.

EUVF02018E   Requested operation is not authorized.

Explanation: The requested operation is not authorized by the associated security credential.

User Response: Obtain the necessary authorization and then retry the request. Contact your service representative if the error persists.

EUVF02019E   Requested operation is not available.

Explanation: The requested operation is not provided by the current software level.

User Response: Upgrade the software to a level that supports the requested operation.

EUVF02020E   Duplicate credential element requested.

Explanation: The requested credential element is already present in the security credential.

User Response: None required.

EUVF02021E   Name contains multiple mechanism elements.

Explanation: The supplied name contains elements for multiple mechanisms. The requested operation requires a name with a single mechanism element.

User Response: Provide a valid name and then retry the request.

EUVF02022I   Response token required from peer application.

Explanation: To complete the security context, the current function must be called again with the response token obtained from the peer application.

User Response: None required.

EUVF02023W   Message is a duplicate of one already received.

Explanation: The message is valid and is a duplicate of one that was already received.

User Response: Application specific.

EUVF02024W   A more recent message was already received.

Explanation: The current message is old. A more recent message has already been received. The message validity period has expired, so the routine cannot determine whether the message is a duplicate of one that was already received.

User Response: Application specific.

EUVF02025W   Message received out of sequence.

Explanation: The message is valid but an earlier message in the sequence has not been received.

User Response: Application specific.

EUVF02026W   Skipped predecessor message detected.

Explanation: The message is valid but a later message in the sequence has already been received.

User Response: Application specific.

EUVF02027E   Kerberos control block validation fails: Expected *exp-value***, Actual** *act-value***.**

Explanation: Kerberos internal control blocks have a unique identifier for each type of control block. The Kerberos runtime detects a mismatch between the expected identifier and the actual identifier. This error can occur if storage has been overlaid or modified.

User Response: Contact your service representative.

EUVF02028E   The *name* **system function detects an error.** *error-text***.**

Explanation: A system function detects an error. Refer to the documentation for the failing system function to obtain more information about the cause of the failure.

User Response: Contact your service representative if the error persists.

EUVF02029E   The *name* **system function detects an error on** *filename***.** *error-text***.**

Explanation: A system function detected an error while processing the indicated file.

User Response: Contact your service representative if the error persists.

EUVF02030E   Syntax error on line *number* **of** *filename***. Error** *number***:** *error-text***.**

Explanation: A syntax error was detected while processing the Kerberos profile.

User Response: Correct the line in error and restart the application.

EUVF02031E   The *name* **cryptographic function detects an error: Return code** *rtn-code***, Reason code** *rsn_code***.**

Explanation: A cryptographic function detected an error. Refer to *ICSF Application Programmer's Guide* for

a description of the failing function and an explanation of the return code and reason code.

User Response: Contact your service representative if the error persists.

| **EUVF02032E   The** *name* **network function detects**
| **an error,** *error-text***.**

| **Explanation:** A network function detected an error.
| Refer to the documentation for the failing function to
| obtain more information about the cause of the failure.

User Response: Contact your service representative if the error persists.

EUVF02033R   Enter password:

Explanation: The security runtime needs the user password to complete a request.

User Response: Enter your password.

EUVF02034E   Unable to initialize Kerberos GSS-API mechanism: Error *code***.**

Explanation: An error occurred during the initialization of the Kerberos GSS-API mechanism.

User Response: Contact your service representative if the error persists.

EUVF02035E   Mutex operation fails. *error-text***.**

Explanation: A mutex operation failed. error-text is the message text associated with the error code.

User Response: Contact your service representative if the error persists.

EUVF02036I Call stack traceback called from *filename* **at line** *linenumber***.**

Explanation: A call stack trace was requested by the security runtime. This message identifies the source module name and source line number that made the request.

User Response: No action is required.

EUVF02037I Called from *function* **at offset** *displacement***.**

Explanation: A call stack trace was requested by the security runtime. This message is issued for each entry in the call stack and identifies the offset within the function that issued the call.

User Response: No action is required.

Messages

EUVF02038I IBM Kerberos dump created.

Explanation: A dump has been created by the security runtime. The dump was created in the directory specified by the _CEEDUMP_DIR environment variable.

User Response: Contact your service representative and provide the dump file.

EUVF02039E Incorrect request format.

Explanation: The password change protocol packet is not formatted correctly. The result string returned by the password server contains additional information about the error.

User Response: Contact your service representative if the error persists.

EUVF02040E Password server error.

Explanation: The password server detected an error. The result string returned by the password server contains additional information about the error.

User Response: Contact your service representative if the error persists.

EUVF02041E Authentication error.

Explanation: The authentication information supplied with a password change request is not correct. The

result string returned by the password server contains additional information about the error.

User Response: Contact your service representative if the error persists.

EUVF02042E Password change rejected.

Explanation: The password change request is rejected by the password server. The result string returned by the password server contains additional information about the error.

User Response: Choose a new password that meets the password policy. Contact your service representative if the error persists.

EUVF02043E Password change failed.

Explanation: The password change request was not successful.

User Response: Contact your service representative if the error persists.

EUVF02044I Password changed.

Explanation: The password change request was successful.

User Response: None

Security server messages (numbers EUVF04000 - EUVF05999)

EUVF04001I Security server version *version.release* Service level *level*.

Explanation: The security server is starting. This message displays the version, release, and service level of the security server.

User Response: None

EUVF04002I Security runtime version *version.release* Service level *level*.

Explanation: The security server is starting. This message displays the version, release, and service level of the runtime DLL.

User Response: None

EUVF04003A Unable to make address space non-swappable: Error *error-code*.

Explanation: The security server is unable to make its address space non-swappable. The error code is the value returned by the SYSEVENT system service. An error code of 1 indicates the security server job step is not APF-authorized. Refer to the description of the SYSEVENT macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services*

Reference, for more information on the error.

User Response: Verify that the SKRBKDC started task is APF-authorized. Contact your service representative if the error persists.

EUVF04004E The *function-name* system function detects an error: *error-message*.

Explanation: A system function detected an error. The error message text is returned by the **strerror()** function. Refer to the description of the failing system function in *z/OS C/C++ Run-Time Library Reference*, SA22-7821-03, for more information on the error.

User Response: Contact your service representative if the error persists.

EUVF04005E Insufficient storage available.

Explanation: The security server is unable to obtain storage for an internal control block.

User Response: Increase the storage available to the program and then retry the request.

EUVF04006I Security server shutdown requested.

Explanation: The system operator has entered a STOP command for the security server.

User Response: None

EUVF04007E   Unrecognized security server command: Specify DISABLE, DISPLAY, ENABLE, PROP, DEBUG, or STOP.

Explanation: An unrecognized command name is specified on a MODIFY operator command. The only valid security server commands are DISABLE, DISPLAY, ENABLE, PROP, DEBUG, and STOP.

User Response: Specify a valid security server command.

EUVF04008I Debug option processed: *debug-option***.**

Explanation: The indicated debug request has been processed by the security server.

User Response: None

EUVF04009E   Incorrect command option specified.

Explanation: An incorrect security server command option was specified. The valid DISPLAY command options are:

- ADMIN - Display the current status of the Kerberos administration service
- CREDS - Display credentials data space allocations
- CRYPTO - Display the available encryption types.
- LEVEL - Display the security server version, release, and service level.
- NETWORK - Display the network interface status.
- PROP - Display the database propagation status.
- XCF - Display security server sysplex status

The valid DEBUG command options are:

- OFF - Turn off debug messages.
- ON - Turn on debug messages.
- *subcomp.level,subcomp.level,...* - Set the debug level for one or more subcomponents.

User Response: Specify a valid command option.

EUVF04010A Database type *type* **is not supported.**

Explanation: The SKDC_DATABASE environment variable specifies an unsupported database type.

User Response: Specify a supported database type. The security server supports the SAF and NDBM databases.

EUVF04011E   Unable to receive datagram. *error_text***.**

Explanation: The security server is unable to receive a datagram from the network. The error text is returned by the **strerror()** routine.

User Response: Contact your network support group.

EUVF04012E Unable to send response to *network-address***.** *error-text***.**

Explanation: The security server is unable to send data to the specified network address. The error text is returned by the **strerror()** routine.

User Response: Contact your network support group.

EUVF04013E   Unable to initialize local services: Error *error-code***, Reason** *reason-code***.**

Explanation: The security server is unable to initialize the local services support. This support is used by applications running on the same system as the security server. The error code indicates the failing system function and the reason code is the error code returned by the system function.

The following error codes are defined:

- 1 = The job step is not APF-authorized.
- 2 = The security server is already running.
- 3 = ESTAEX failed. See the ESTAEX macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information on the error.
- 5 = LXRES failed. See the LXRES macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.
- 6 = ETCRE failed. See the ETCRE macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.
- 7 = ETCON failed. See the ETCON macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.
- 8 = IEANTCR failed. See the IEANTCR macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.
- 9 = CTRACE DEFINE failed. See the CTRACE macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.

User Response: Contact your service representative, if you are unableto correct the error.

Messages

EUVF04014E   Unable to end local services: Error *error-code***, Reason** *reason-code***.**

Explanation: The security server is unable to end the local services support. The error code indicates the failing system function and the reason code is the error code returned by the system function.

The following error codes are defined:

- 102 = Unable to cancel ESTAEX. See the ESTAEX macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information on the error.
- 110 = IEANTDL failed. See the IEANTDL macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.
- 111 = Unable to obtain control lock.
- 112 = CTRACE DELETE failed. See the CTRACE macro description in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services* for more information.

User Response: Contact your service representative.

EUVF04015E   Local program call request failed: Error *error-code***.**

Explanation: The security server is unable to process a local program call request.

The following error codes are defined:

- 8 = Parameter buffer overflow
- 12 = Unable to allocate storage
- 16 = Local service support not enabled
- 20 = Program call task abended
- 24 = Unable to obtain control lock
- 28 = SRB mode is not supported.

User Response: Contact your service representative.

EUVF04016E   Login audit mode *mode* **is not supported.**

Explanation: The SKDC_LOGIN_AUDIT environment variable specified an unsupported audit mode. The supported audit modes are NONE, FAILURE, and ALL.

User Response: Specify a supported login audit mode.

EUVF04017A   Unable to initialize the KDC.

Explanation: The security server is unable to initialize the KDC (Key Distribution Center). A previous error message contains more information about the failure.

User Response: Correct the problem and then restart the security server. Contact your service representative if the error persists

EUVF04018I Security server initialization complete.

Explanation: The security server initialization is complete.

User Response: None

EUVF04019A   Realm name *name* **contains separator characters.**

Explanation: The realm name contains the '/' or '@' characters. These characters are used as component separators and may not be used in the realm name.

User Response: Use a valid realm name.

EUVF04020A   Security server is already running.

Explanation: Security server is already running.

User Response: None

EUVF04021A   Unable to initialize registry database support.

Explanation: The security server is unable to initialize the registry database support. A previous message provides more information on the cause of the failure.

User Response: Correct the problem and restart the security server. Contact your service representative if the error persists.

EUVF04028E   Unable to retrieve information from the System Authorization Facility registry. SAF error *error-code***, Return code** *return-code***, Reason code** *reason-code***.**

Explanation: The call to the IRRSIM00 system function fails with the indicated error code. Refer to *z/OS: Security Server RACF Callable Services* for more information on the IRRSIM00 callable service and its error return values.

User Response: Contact your service representative if the error persists.

EUVF04029E   Kerberos segment field *field-name* **for user** *user-name* **is not valid.**

Explanation: The Kerberos segment for the specified user is not valid. The data is either too long or is not formatted correctly.

User Response: Use the ALTUSER (or equivalent) command to correct the Kerberos segment data.

EUVF04030A   Registry realm *name* **does not match configured realm** *name***.**

Explanation: The realm name in the security registry is not the same as the default realm specified in the krb5.conf configuration file.

User Response: Change the default realm name or create a new registry for the realm.

EUVF04031E   Limit of *number* **sockets exceeded.**

Explanation: The maximum number of open sockets has been exceeded.

User Response: Run additional instances of the security server on other systems within the Kerberos realm.

EUVF04032E   Unable to receive data from *network-address***.** *error-text***.**

| **Explanation:**   The security server is unable to receive
| data from a client at the specified network address. The
| error text is returned by the **strerror()** routine.

| **User Response:**   Contact your network support group.

EUVF04033E   Message received from *network-address* **with length** *size* **exceeds the maximum size.**

Explanation: The security server received a request that is too large to be processed. The maximum request message size is 32768.

User Response: Verify that the client is sending a valid Kerberos request to the security server. Contact your service representative if the problem persists.

EUVF04034E   R_kerbinfo request fails: Function *code***, Error** *error-code***, RC** *return-code***, Reason** *reason-code***. Kerberos name:** *name*

Explanation: The **R_kerbinfo** (IRRSMK00) function call failed. Refer to *z/OS: Security Server RACF Callable Services* for more information. In addition to the return codes documented in the callable services publication, you can also receive error code 8, return code 8, reason code 16, if the SKRBKDC started task is not APF-authorized.

User Response: Contact your service representative if you are unable to correct the problem.

EUVF04035E   Local Kerberos realm is not defined.

Explanation: The local Kerberos realm has not been defined in the system security database. Refer to *z/OS: Security Server RACF Command Language Reference* for more information.

User Response: Define the local realm and then restart the security server.

EUVF04036E   Unable to generate PassTicket for *userid***.**

Explanation: The security server is unable to generate a PassTicket for the indicated user.

User Response: Verify that the PTKTDATA class is active and that the SKRBKDC application has been defined in the PTKTDATA class with a valid secured signon key.

EUVF04037E   Unable to change password for *userid***. SAF error** *code***, Return code** *code***, Reason code** *code***.**

Explanation: The security server is unable to change the password for the indicated user. Refer to *z/OS: Security Server RACROUTE Macro Reference* for more information about the error codes returned by the RACROUTE REQUEST=VERIFY function.

User Response: Contact your service representative if the error persists.

EUVF04038I   Kerberos login successful for *principal* **at** *address***.**

Explanation: A request for an initial ticket was successful. This message is controlled by the SKDC_LOGIN_AUDIT environment variable.

User Response: None

EUVF04039W   Kerberos login failed for *principal* **at** *address***. KDC status code:** *error-text***.**

Explanation: A request for an initial ticket failed. This message is controlled by the SKDC_LOGIN_AUDIT environment variable.

User Response: Contact the user attempting to get the initial ticket if the problem persists.

| **EUVF04040E   Unable to encode database entry for**
| *name***: Status** *status-code* -
| *status-message*

Explanation: The Kerberos security server was unable to encode a database entry.

User Response: Contact your service representative.

| **EUVF04041E   Unable to read database master key:**
| *error-text*.

| **Explanation:**   The Kerberos security server was unable
| to read the database master key from the stash file.
| This key is used to encrypt entries in the principal
| database. The error text is returned by the **strerror()**
| routine.

Messages

User Response: Verify that the stash file **/var/skrb/krb5kdc/.k5** exists and is accessible. Contact your service representative if the error persists.

EUVF04042E   Unable to write database master key: *error-text.*

Explanation: The Kerberos security server was unable to write the database master key to the stash file. This key is used to encrypt entries in the principal database. The error text is returned by the **strerror()** routine.

User Response: Verify that the stash file **/var/skrb/krb5kdc/.k5** exists and is accessible. Contact your service representative if the error persists.

EUVF04043E   Unable to store database entry for *name. Error-text.*

Explanation: The Kerberos security server was unable to store the indicated entry in its database. The database files are stored in the **/var/skrb/krb5kdc** directory. The error text is returned by the **strerror()** routine.

User Response: Verify that the **/var/skrb/krb5kdc** directory exists and is mounted in read/write mode. Contact your service representative if the error persists.

EUVF04044E   Unable to fetch database entry for *name. Error-text.*

Explanation: The Kerberos security server was unable to retrieve the indicated entry in its database. The database files are stored in the **/var/skrb/krb5kdc** directory. The error text is returned by the **strerror()** routine.

User Response: Verify that the **/var/skrb/krb5kdc** directory exists and is mounted in read/write mode. Contact your service representative if the error persists.

EUVF04045A   The security server must have UID 0.

Explanation: The Kerberos security server requires UID 0 authority.

User Response: Ensure that the security server is started with UID 0.

EUVF04046E   Unable to decode RPC message received from *network-address.*

Explanation: The Kerberos administration server was unable to decode an RPC message received from a client.

User Response: Contact your service representative if the error persists.

EUVF04047E   Unable to create directory *name.*

Explanation: The Kerberos security server was unable to create the indicated directory.

User Response: Verify that all path components exist and that the security server is running with UID 0. Contact your service representative if the error persists.

EUVF04048E   Unable to open database *name. Error-text.*

Explanation: The Kerberos security server was unable to open the indicated registry database. The error text is returned by the **strerror()** routine.

User Response: Verify that all path components exist and that the security server is running with UID 0. Contact your service representative if the error persists.

EUVF04049E   Unable to open administration key table *name. Status status-code - status-message.*

Explanation: The Kerberos security server was unable to open the administration key table.

User Response: Verify that all path components exist and that the security server is running with UID 0. Contact your service representative if the error persists.

EUVF04050E   Unable to add entry to administration key table *name. Status status-code - status-message.*

Explanation: The Kerberos security server was unable to add an entry to the administration key table.

User Response: Verify that all path components exist and that the security server is running with UID 0. Contact your service representative if the error persists.

EUVF04051E   Unable to read entry for principal *name. Status status-code - status-message.*

Explanation: The Kerberos security server was unable to read a principal entry from the database.

User Response: Verify that the principal entry exists in the database. Contact your service representative if the error persists.

EUVF04052E   GSS-API function *name* **detects error.** *major-status minor-status*

Explanation: The Kerberos security server was unable to process an administration request due to a GSS-API error. The z/OS Security Server supports the Kerberos Administration Version 2 protocol as implemented in MIT Kerberos 1.2.2. Refer to the description for the failing GSS-API function in *z/OS: Security Server*

Network Authentication Service Programming for more information on the error.

User Response: Contact your service representative if the error persists.

EUVF04053E **Unable to create credentials data space: Error** *error-code***, Reason** *reason-code***.**

Explanation: The Kerberos security server was unable to create the credentials data space.

The error codes have the following values:

- 1 = DSPSERV CREATE failed. The reason code contains the DSPSERV return code in the upper halfword and bits 8-23 of the DSPSERV reason code in the lower halfword. See the description of the DSPSERV macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services Reference* for more information on the error.
- 2 = ALESERV ADD failed. The reason code is the ALESERV return code. See the description of the ALESERV macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services Reference* for more information on the error.

User Response: Security server initialization continues but data space services are not available. Contact your service representative if the error persists.

EUVF04054E **Unable to delete credentials data space: Error** *error-code***, Reason** *reason-code***.**

Explanation: The Kerberos security server was unable to delete the credentials data space.

The error codes have the following values:

- 1 = DSPSERV DELETE failed. The reason code contains the DSPSERV return code in the upper halfword and bits 8-23 of the DSPSERV reason code in the lower halfword. See the description of the DSPSERV macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services Reference* for more information on the error.
- 2 = ALESERV DELETE failed. The reason code is the ALESERV return code. See the description of the ALESERV macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services Reference* for more information on the error.

User Response: Security server termination continues. Contact your service representative if the error persists.

EUVF04055E **Unable to extend the credentials data space: Error** *error-code***, Reason** *reason-code***.**

Explanation: The Kerberos security server is unable to increase the size of the credentials data space.

The error codes have the following values:

- 1 = DSPSERV EXTEND failed. The reason code contains the DSPSERV return code in the upper halfword and bits 8-23 of the DSPSERV reason code in the lower halfword. See the description of the DSPSERV macro in the appropriate volume of *z/OS MVS Programming: Authorized Assembler Services Reference* for more information on the error.

User Response: The new credentials are not stored in the credentials data space. The SKDC_CREDS_SIZE environment variable specifies the maximum allowable size for the credentials data space.

EUVF04056E **Unable to initialize cross-system services: Error** *error-code***, Reason** *reason-code***.**

Explanation: The Kerberos security server is unable to initialize cross-system services.

The error codes have the following values:

- 1 = The job step is not APF-authorized.
- 3 = IXCJOIN failed. The reason code contains the IXCJOIN return code in the upper halfword and the IXCJOIN reason code in the lower halfword. See the description of the IXCJOIN macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.
- 4 = IXCQUERY failed. The reason code contains the IXCQUERY return code in the upper halfword and the IXCQUERY reason code in the lower halfword. See the description of the IXCQUERY macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.

User Response: Security server initialization continues but cross-system services are not available. Contact your service representative if the error persists.

EUVF04057E **Unable to end cross-system services: Error** *error-code***,** *reason-code***.**

Explanation: The Kerberos security server is unable to end cross-system services.

The error codes have the following values:

- 5 = IXCLEAVE failed. The reason code contains the IXCLEAVE return code in the upper halfword and the IXCLEAVE reason code in the lower halfword. See the description of the IXCLEAVE macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.

User Response: Security server processing continues. Contact your service representative if the error persists.

Messages

EUVF04058I System *name* **has joined the Kerberos security server group.**

Explanation: The SKRBKDC started task has completed initialization on the indicated system and is now a member of the EUVFSKRB cross-system group.

User Response: None

EUVF04059I System *name* **has left the Kerberos security server group.**

Explanation: The SKRBKDC started task is stopping on the indicated system.

User Response: None

EUVF04060I Cross-system services ended due to sysplex partitioning.

Explanation: The local system is leaving the sysplex. As a result, Kerberos security server cross-system services are no longer available.

User Response: Security server processing continues.

EUVF04061E Unable to send cross-system message: Error *error-code***, Reason** *reason-code***.**

Explanation: The Kerberos security server is unable to send a message to another member of the Kerberos security server group.

The error codes have the following values:

* 1 = Unable to obtain XCF control lock on target system.
* 2 = Cross-system services are not available.
* 3 = Requested token not found on target system.
* 4 = User not authorized to access token data.
* 5 = Unable to allocate storage on the target system.
* 6 = Target replica is not a member of the security server group.
* 7 = Target replica is not active.
* 8 = IXCMSGO failed. The reason code contains the IXCMSGO return code in the upper halfword and the IXCMSGO reason code in the lower halfword. See the description of the IXCMSGO macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.
* 9 = IXCMSGI failed on the target system. The reason code contains the IXCMSGI return code in the upper halfword and the IXCMSGI reason code in the lower halfword. See the description of the IXCMSGI macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.
* 10 = Request function code is not supported.
* 11 = Request canceled.
* 12 = Unknown notification message.

* 13 = No response received from target system.
* 14 = Unable to allocate storage on the local system.
* 15 = IXCMSGI failed on the local system. The reason code contains the IXCMSGI return code in the upper halfword and the IXCMSGI reason code in the lower halfword. See the description of the IXCMSGI macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.

User Response: The request was not processed. Contact your service representative if the error persists.

EUVF04062A The security server is not APF-authorized.

Explanation: The Kerberos security server must be APF-authorized.

User Response: Verify that the dataset containing the EUVFSKDC load module is APF-authorized. If you are using a STEPLIB or JOBLIB for the SKRBKDC started task, verify that all datasets in the concatenation are APF-authorized.

EUVF04063E Unable to allocate *size* **bytes in the credentials data space.**

Explanation: The credentials data space is full. The SKDC_CREDS_SIZE environment variable can be used to increase the size of the credentials data space. SKDC_CREDS_SIZE specifies the credentials data space size in kilobytes, with a minimum value of 1024, a maximum value of 2097148, and a default value of 20480.

User Response: Increase the size of the credentials data space and then restart the Kerberos security server.

EUVF04064I Sysplex status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY XCF command. The remaining lines in this multi-line message display the status of each Kerberos security server in the sysplex. A security server is ACTIVE if the SKRBKDC started task is running. A security server is INACTIVE if the SKRBKDC started task has been stopped. No entry is displayed for a system where the SKRBKDC started task has not been active at any time since the local security server was started.

User Response: None

EUVF04065I No active security servers.

Explanation: There are no active security servers in the sysplex. This message can occur if there was an error in setting up the cross-system coupling facility support.

User Response: None

EUVF04066I Data space status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY CREDS command. The remaining lines in this multi-line message display the data space allocations.

User Response: None

EUVF04067I No data space allocations.

Explanation: There are no data space allocations.

User Response: None

EUVF04068I Maximum number of lines displayed.

Explanation: A maximum of 253 status lines can be displayed in response to a single command.

User Response: None

EUVF04069I Listening for requests on network interface *address***.**

Explanation: The security server is listening for requests on the indicated network interface.

User Response: None

EUVF04070I No longer listening for requests on network interface *address***.**

Explanation: The security server is no longer listening for requests on the indicated network interface.

User Response: None

EUVF04071E Unable to bind socket to *network-address: error-text***.**

Explanation: The security server is unable to bind a socket to listen for client requests on the indicated network interface. The error text is returned by the **strerror()** routine.

User Response: Ensure that the TCP/IP configuration profile does not reserve the network port for use by another application. The SKDC_PORT, SKDC_KPASSWD_PORT, and SKDC_KADMIN_PORT environment variables can be used to change the ports used by the security server.

EUVF04072I Security server restart registration complete on *system***.**

Explanation: The security server has successfully registered with ARM (Automatic Restart Management) on the indicated system. The security server is automatically restarted if it fails unexpectedly (the security server is not restarted if it detects an error and stops). The ARM element type is SYSKERB and the ARM element name is EUVFKDC_system-name. The

ARM policy can be used to override the default registration values if needed. Refer to *z/OS MVS Programming: Sysplex Services Guide* for more information on automatic restart management.

User Response: None

EUVF04073I Security server restarting on *system***.**

Explanation: The security server is being restarted following an unexpected failure. The RESTART_ATTEMPTS value in the ARM policy determines the number of restarts attempted. Refer to *z/OS MVS Programming: Sysplex Services Guide* for more information on automatic restart management.

User Response: None

EUVF04074I Unable to register for restart: Error *error-code***, Reason** *reason-code***.**

Explanation: The security server is unable to register with ARM (Automatic Restart Management). The IXCARM request failed with the indicated error and reason codes. See the description of the IXCARM macro in *z/OS MVS Programming: Sysplex Services Reference* for more information on the error.

User Response: Contact your service representative if you are unable to correct the error.

EUVF04075E Cryptographic status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY CRYPTO command. The remaining lines in this multi-line message display the available encryption types and whether encryption and decryption operations are performed using the Integrated Cryptographic Service Facility (ICSF).

User Response: None

EUVF04076E Unable to open access control file *filename: error-text*

Explanation: The Kerberos security server was unable to open an access control file. The security server uses this file to control access to the Kerberos functions. The error text is returned by the **strerror()** routine.

User Response: Verify that all path components exist, the security server is running with UID 0, and the access control file exists. Contact your service representative if the error persists.

EUVF04077E Unable to read access control file *filename: error-text*

Explanation: The Kerberos security server is unable to read an access control file. The error text is returned by the **strerror()** routine.

Messages

User Response: Contact your service representative if the error persists.

EUVF04078E Unable to convert *expression* **to a regular expression:** *error-text*

Explanation: The Kerberos security server is unable to parse a line in the administration access control file. The expression cannot be converted to a regular expression for the indicated reason. The error text is returned by the **strerror()** routine.

User Response: Correct the expression in the administration access control file. Contact your service representative if the error persists.

EUVF04079E Unable to decode database entry for *name***: Status** *status-code - status-message*

Explanation: The Kerberos security server is unable to decode a database entry.

User Response: Contact your service representative.

EUVF04080E Unable to delete database entry for *name***:** *error-message*

Explanation: The Kerberos security server is unable to delete an entry from the registry database.

User Response: Contact your service representative if the error persists.

EUVF04081E Unable to validate database master key: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to validate the database master key. This error can occur if the master key stash file is generated using the wrong database password. This error also can occur when loading a new database if the wrong master key is entered in response to the database password prompt.

User Response: For an existing database, create a master key stash file containing the correct database master key. For a new database, enter the correct database master key when prompted. Contact your service representative if the error persists.

EUVF04082E The *option-name* **option requires a value.**

Explanation: A command option is specified without a corresponding value.

User Response: Specify a value for the indicated option.

EUVF04083E *option-name* **is not a valid command option.**

Explanation: An unrecognized command option is specified.

User Response: Specify a valid command option.

EUVF04084E The *option-name* **option is not valid for the '***function-name***' function.**

Explanation: A valid option is specified but the option is not valid for the requested function.

User Response: Specify a valid command option.

EUVF04085I kdb5_ndbm function [-e keytypes] [-k keytype] [-mkey_convert] [-compat] [-v] filename

Explanation: This message displays the command syntax for the **kdb5_ndbm** command.

User Response: None

EUVF04086E No database utility function specified.

Explanation: A database utility command is entered without specifying a function to be performed.

User Response: Specify a database utility function.

EUVF04087E *function-name* **is not a valid database utility function.**

Explanation: An unrecognized function is specified for a database utility command.

User Response: An unrecognized function is specified for a database utility command.

EUVF04088E Unable to create KDC database: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to create the registry database.

User Response: Ensure that the failing command is being run under a user ID with write access to the **/var/skrb/krb5kdc** directory and to all of the files in that directory. Contact your service representative if the error persists.

EUVF04089E Unable to obtain the default realm: Status *status-code - status-message*

Explanation: The **krb5_get_default_realm()** function failed.

User Response: Verify that the **/etc/skrb/krb5.conf** configuration file exists and contains an entry for the default realm. Contact your service representative if the error persists.

EUVF04090E Encryption type *name* **is not supported.**

Explanation: An unsupported encryption type was specified.

User Response: Specify a supported encryption type.

EUVF04091R Enter the KDC database master password:

Explanation: Enter the master password for the KDC database. The password should not be obvious or easily guessed since it will be used to generate the master key for the database. The master key is used to encrypt the database entries.

User Response: Enter the password string for the database master key.

EUVF04092R Re-enter the KDC database master password:

Explanation: Re-enter the master password for the KDC database to verify the password was entered correctly.

User Response: Enter the same password string as you entered for the initial prompt.

EUVF04093E Unable to read the KDC database master password: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to prompt for the database master password.

User Response: Contact your service representative if the error persists.

EUVF04094E Unable to generate the KDC database master key: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to convert the password string into an encryption key.

User Response: Contact your service representative.

EUVF04095I KDC database master key created.

Explanation: The KDC database master key has been created.

User Response: None

EUVF04096E A KDC database already exists.

Explanation: A request to create a new KDC database cannot be completed because a database already exists.

User Response: Use the **kdb5_ndbm** command to remove the existing database and then retry the failing command.

EUVF04097E Unable to delete database file *filename***:** *error-text*

Explanation: The Kerberos security server is unable to delete a database file. The error text is returned by the **strerror()** routine.

User Response: Verify that the command is being run by a user ID with UID 0. Contact your service representative if the error persists.

EUVF04098I KDC database files deleted.

Explanation: The KDC database files have been deleted.

User Response: None

EUVF04099I KDC database created.

Explanation: The KDC database has been created.

User Response: None

EUVF04100E The dump filename must be specified.

Explanation: A database dump or load function was requested but no dump filename is provided.

User Response: Specify the dump filename.

EUVF04101E Unable to dump the KDC database: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to dump the KDC database.

User Response: Contact your service representative if the error persists.

EUVF04102I KDC database dump file *filename* **created.**

Explanation: The KDC database has been dumped to the indicated file.

User Response: None

EUVF04103E Unable to load the KDC database: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to load the KDC database.

User Response: Contact your service representative.

Messages

EUVF04104I KDC database loaded from file *filename***.**

Explanation: The KDC database has been loaded from the indicated file.

User Response: None

EUVF04105E   The KDC database does not exist.

Explanation: An attempt to read from the KDC database failed because the database does not exist.

User Response: Verify that the database files exist. The files are located in the **/var/skrb/krb5kdc** directory. Contact your service representative if the error persists.

EUVF04106R   Enter the database dump password:

Explanation: Enter the password for the database dump. The password should not be obvious or easily guessed since it will be used to encrypt the database entries in the dump.

User Response: Enter the password string for the database dump key.

EUVF04107R   Re-enter the database dump password:

Explanation: Re-enter the password for the database dump to verify the password was entered correctly.

User Response: Enter the same password string as you entered for the initial prompt.

EUVF04108E   Unable to read the database dump password: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to prompt for the database dump password.

User Response: Contact your service representative if the error persists.

EUVF04109E   Unable to generate the database dump key: Status *status-code - status-message*

Explanation: The Kerberos security server is unable to convert the password string into an encryption key.

User Response: Contact your service representative.

EUVF04110E   Unable to write to dump file filename: *error-text*

Explanation: The Kerberos security server is unable to write to the indicated database dump file.The error text is returned by the **strerror()** routine.

User Response: Verify that the user has write access to the directory and the file. Contact your service

---

representative if the error persists.

EUVF04111E   Unable to read from dump file filename: *error-text*

Explanation: The Kerberos security server is unable to read from the indicated database dump file. The error text is returned by the **strerror()** routine.

User Response: Verify that the user has read access to the directory and the file. Contact your service representative if the error persists.

EUVF04112E   Principal *name* **references unknown policy** *name***.**

Explanation: A principal entry in the Kerberos database contains a reference to an unknown policy. This indicates the database has become corrupted.

User Response: Either restore the database from a backup or remove the policy reference from the principal entry. Contact your service representative if the error persists.

EUVF04113E   Database entry *name* **with size** *number* **exceeds maximum size** *number***.**

Explanation: A database entry is larger than the maximum supported size. This indicates the database has become corrupted.

User Response: Restore the database from a backup. Contact your service representative if the error persists.

EUVF04114E   Architected principal *name* **is not found in the KDC database.**

Explanation: The Kerberos security server is unable to locate a required principal in the database. This indicates the database has become corrupted.

User Response: Restore the database from a backup. Contact your service representative if the error persists.

EUVF04115W   Password history for *principal* **with** *number* **entries is too large.**

Explanation: The password history for the indicated principal has become too large to be stored in the Kerberos database. The oldest entries will be removed until the resulting history is small enough to fit in a database record.

User Response: Reduce the history count for the policy associated with the principal.

EUVF04116E   File *filename* **does not contain a valid database dump.**

Explanation: The indicated file does not contain a valid Kerberos database dump. This problem can occur if the dump is created using the database utility

provided with an older Kerberos implementation.

User Response: Recreate the dump using the current level of the Kerberos database utility command.

EUVF04117E   Dump record type *name* **is not valid.**

Explanation: A record in the database dump file was not recognized.

User Response: Contact your support representative.

EUVF04118E   Unable to rename database file from *oldname* **to** *newname***:** *error-text*

Explanation: The Kerberos security server is unable to rename a database file. The error text is returned by the **strerror()** routine.

User Response: Contact your service representative.

EUVF04119E   No history key is available for master key type *encryption-type***.**

Explanation: The history principal (**kadmin/history**) does not have a key for the encryption type defined by the database master key.

User Response: Change the keys for the history principal and generate a new key with the same encryption type as the database master key.

EUVF04120E   Unable to encrypt database entry for *name***: Status** *status-code - status-message*

Explanation: The Kerberos security server was unable to encrypt an entry in the KDC database.

User Response: Contact your service representative.

EUVF04121E   Unable to decrypt database entry for *name***: Status** *status-code - status-message*

Explanation: The Kerberos security server is unable to decrypt an entry in the KDC database. This error can be caused by an incorrect database master key.

User Response: For a secondary KDC, destroy the existing Kerberos database and then recreate it from the primary KDC database. Ensure that the correct database master key is entered when you are prompted for the master password. Contact your service representative if the error persists.

EUVF04122E   Principal name *name* **is not valid.**

Explanation: A principal name is not composed of valid graphical characters as determined by the current locale. In addition, the backslash and commercial at-sign characters are not allowed in a principal name.

User Response: Use only valid graphical characters in principal names.

EUVF04123E   Policy name *name* **is not valid.**

Explanation: A policy name is not composed of valid graphical characters as determined by the current locale. In addition, the backslash character is not allowed in a policy name.

User Response: Use only valid graphical characters in principal names.

EUVF04124E   Unrecognized propagation role specified for *name***.**

Explanation: The **kpropd.acl** access control file contains an unrecognized role specified for the indicated server entry. The valid roles are Primary, Replace, Compat, and Update.

User Response: Specify a valid propagation role.

EUVF04125E   Unable to resolve host principal for *name***: Status** *status-code - status-message*

Explanation: The Kerberos security server is unable to convert a host name to a Kerberos principal. This error can occur if the host name is not defined in the DNS name server or the DNS name server cannot be reached.

User Response: Ensure the host name is defined and the DNS name server can be reached.

EUVF04126E   Unable to log *type* **request from** *name***: Status** *status-code - status-message*

Explanation: The Kerberos security server is unable to log an administration request from the indicated user. This means that the database update will not be propagated to secondary security servers that are using the update protocol. The change has been made to the database on the primary security server.

User Response: Use the Kerberos security server PROP command to force a full database replication for each secondary security server. Contact your service representative if the error persists.

EUVF04127E   Database propagation failed to *host***: Status** *status-code - status-message*

Explanation: The Kerberos security server is unable to send a database update to the indicated secondary server.

User Response: Verify that the secondary server is running and that there are no network problems. The update will be retried at the next propagation interval or the PROP command can be used to initiate a manual

Messages

replication. Contact your service representative if the error persists.

EUVF04128E   Unable to fetch update *number*: *error-text*

Explanation: The Kerberos security server is unable to retrieve the indicated update from its database. The database files are stored in the **/var/skrb/krb5kdc** directory. The error text is returned by the **strerror()** routine.

User Response: Verify that the **/var/skrb/krb5kdc** directory exists and is mounted in read/write mode. Contact your service representative if the error persists.

EUVF04129E   Unable to store update *number*: *error-text*

Explanation: The Kerberos security server is unable to store the indicated update in its database. The database files are stored in the **/var/skrb/krb5kdc** directory. The error text is returned by the **strerror()** routine.

User Response: Verify that the **/var/skrb/krb5kdc** directory exists and is mounted in read/write mode. Contact your service representative if the error persists.

EUVF04130E   Update to delete update *number* : *error-text*

Explanation: The Kerberos security server is unable to delete the indicated update from its database. The database files are stored in the **/var/skrb/krb5kdc** directory.The error text is returned by the **strerror()** routine.

User Response: Verify that the **/var/skrb/krb5kdc** directory exists and is mounted in read/write mode. Contact your service representative if the error persists.

EUVF04131I Propagation status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY PROP command. The remaining lines in this multi-line message display the propagation status for each security server in the realm.

User Response: None

EUVF04132I Propagation complete.

Explanation: The Kerberos security server has successfully completed a database propagation request.

User Response: None

EUVF04133E   Propagation failed: Status *status-code* - *status-message*

Explanation: The Kerberos security server is unable to process a PROP command for the indicated reason. The status of the secondary KDC involved in the propagation remains unchanged.

User Response: Ensure that the secondary KDC is running and that there are no network problems. Contact your service representative if the error persists.

EUVF04134E   Missing command option.

Explanation: A Kerberos security server command was entered that requires a command option but no command option was entered.

User Response: Enter a complete Kerberos security server command.

EUVF04135I No propagation status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY PROP command when database propagation is not enabled or the security server is a secondary security server.

User Response: Enter the DISPLAY PROP command at the primary security server for the realm.

EUVF04136E   The PROP command is not available.

Explanation: The Kerberos security server PROP command was entered on a system that does not support database propagation. This can occur if the Kerberos database does not support propagation, propagation is not enabled, or the Kerberos security server is not the primary security server for the realm.

User Response: None

EUVF04137E   The primary security server cannot be changed.

Explanation: The propagation control file has been updated to change the role of the local Kerberos security server from primary to secondary or from secondary to primary while the security server is running. The security server must be stopped and then restarted in order to change its role.

User Response: Stop both security servers involved in the role change, propagate the latest version of the Kerberos database from the old primary system to the new primary system, and then restart both security servers.

EUVF04138E Unable to receive propagation from
host **- Status** *status-code -*
status-message

Explanation: The Kerberos security server was unable to receive a database propagation from the indicated host.

User Response: Verify that the primary security server is correctly identified in the **kpropd.acl** configuration file and that there are no network errors. The primary security server must have a DNS entry and the entry must be associated with the IP address used for the database propagation. Contact your service representative if the error persists.

EUVF04139E Administration services are not available.

Explanation: The Kerberos security server database does not support the administration functions. Database administration must be performed using the system security commands.

User Response: None

EUVF04140I Administration services are enabled.

Explanation: Kerberos administration services are enabled.

User Response: None

EUVF04141I Administration services are disabled.

Explanation: Kerberos administration services are disabled. Either the Kerberos database does not support the administration functions or the DISABLE ADMIN command has been issued.

User Response: Use the Kerberos security server ENABLE ADMIN command to enable administration services if the Kerberos database supports the administration functions.

EUVF04142I kpropd [-r realm] [-P port] [-v]

Explanation: This message lists the command syntax for the kpropd command.

User Response: None

EUVF04143E *port* **is not a valid port specification.**

Explanation: The port specification is not a decimal number between 1 and 65535.

User Response: Specify a valid port.

EUVF04144E No propagation servers are defined.

Explanation: No propagation servers are defined in the **/etc/skrb/home/kdc/kpropd.acl** configuration file. A database propagation is accepted only from servers listed in this configuration file.

User Response: Add the name of the primary KDC for the realm to the propagation configuration file.

EUVF04145I Listening for database propagation on port *number***.**

Explanation: The **kpropd** command is ready to receive a database propagation.

User Response: Initiate the database propagation from the primary KDC for the realm.

EUVF04146I Receiving database propagation from *server***.**

Explanation: The **kpropd** command is receiving a database propagation.

User Response: None

EUVF04147I Network interface status.

Explanation: This message is displayed in response to the Kerberos security server DISPLAY NETWORK command. The remaining lines in this multi-line message display the status of each network interface. A network interface is ACTIVE if the Kerberos security server is listening for requests on that interface. A network interface is INACTIVE if the interface has been stopped and has not been restarted yet. No entry is displayed for network interfaces that have never been active since the security server was started. The Kerberos security server checks for network interface changes based on the value of the SKDC_NETWORK_POLL environment variable, which has a default value of 5 minutes.

User Response: None

EUVF04148I No active network interfaces.

Explanation: There are no active network interfaces.

User Response: None

EUVF04149R Enter 1 to delete the database or 0 to cancel the request.

Explanation: The **kdb5_ndbm destroy** command has been issued and the user is being prompted to confirm the request to delete the KDC database.

User Response: Enter 1 to continue with the delete request or 0 to cancel the delete request.

Messages for Kerberos commands (numbers EUVF06000 - EUVF06999)

EUVF06001E **The** *option* **option requires value.**

Explanation: A command line parameter is specified
that requires a value. No value is found.

User Response: Specify a value for the command line
parameter.

EUVF06002E *option* **is not a valid command option.**

Explanation: An unrecognized command line
parameter is specified.

User Response: Specify a valid command line
parameter.

EUVF06003E **Time delta value** *value* **is not valid.**

Explanation: The time delta specified is not correct.
Time deltas are specified as a string of time values with
no intervening blanks. Each time value consists of a
decimal number followed by **w, d, h, m,** or **s**
corresponding to weeks, days, hours, minutes, and
seconds. If a number is specified without a letter, it
defaults to hours. For example, **1d6h30m** specifies a
time delta of 1 day, 6 hours, 30 minutes.

User Response: Specify a valid time delta value.

EUVF06004I **Usage: kinit [-s] [-c cache_name] [-k [-t**
keytab]] [-A] [-f] [-p] [-R] [-l end] [-r till]
[principal]

Explanation: This message displays the valid
command line options for the **kinit** command.

-s Use the Kerberos principal associated with the
current system identity. No password is used
since the system has already verified the
identity.

-c Specify the credentials cache name. The
default credentials cache is used if this option
is not specified.

-k Obtain the password from a key table. The
user is prompted for the password if this option
is not specified.

-t Specify the name of the key table. The default
key table is used if this option is not specified.

-A Request a ticket that does not contain a client
address list.

-f Request a ticket that can be forwarded.

-p Request a ticket that a proxy can use.

-R Renew an existing ticket.

-l Renew an existing ticket.

-r Request a ticket that can be renewed for the
specified time period.

Delta times are specified as a string of time values with
no intervening blanks. Each time value consists of a
decimal number followed by **w, d, h, m,** or **s**,
corresponding to weeks, days, hours, minutes, and
seconds. If a number is specified without a letter, it
defaults to hours. For example, **1d6h30m** specifies a
time delta of 1 day, 6 hours, 30 minutes.

If no client principal is specified, the default principal for
the credentials cache is used.

User Response: None

EUVF06005E **Unable to parse principal name.**
Status *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to parse
the principal name.

User Response: Specify a valid principal name on the
kinit command line.

EUVF06006E **No options allowed when renewing**
or validating ticket.

Explanation: No options may be specified when the
-R option is specified for the **kinit** command.

User Response: Do not specify any other options
when the -R option is specified.

EUVF06007E **Unable to obtain name of default**
credentials cache.

Explanation: The **kinit** command is unable to obtain
the default credentials cache name.

User Response: Verify that the KRB5CCNAME
environment variable, if set, specifies a valid credentials
cache name. Contact your service representative if the
error persists.

EUVF06008E **Unable to resolve credentials cache**
*name***. Status** *status-code* **-**
*status-message***.**

Explanation: The **kinit** command is unable to resolve
the credentials cache name.

User Response: Enter a valid credentials cache
name. Contact your service representative if the error
persists.

EUVF06009E **No initial ticket available.**

Explanation: The **kinit** command is unable to renew
the initial ticket because no ticket is available in the

credentials cache or because the ticket principal does not match the principal specified on the **kinit** command line.

User Response: Ensure the credentials cache contains a renewable initial ticket.

EUVF06010E   Principal name must be specified.

Explanation: No principal name is specified on the **kinit** command line but the credentials cache does not contain a default principal.

User Response: Specify the principal name.

EUVF06011E   Unable to retrieve principal from credentials cache *name***. Status** *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to get the default principal name from the credentials cache.

User Response: Verify that the credentials cache is not modified. Contact your service representative if the error persists.

EUVF06012E   Unable to retrieve ticket from credentials cache name. Status *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to retrieve the ticket-granting ticket from the credentials cache. The most likely cause is that the ticket-granting ticket has expired.

User Response: Use the **kinit** command to obtain a new initial ticket.

EUVF06013E   Initial ticket is not renewable.

Explanation: The **kinit** command is invoked with the -R option but the initial ticket in the credentials cache is not renewable.

User Response: Use the **kinit** command with the **-r** option to obtain a renewable initial ticket.

EUVF06014E   Unable to obtain initial credentials. Status *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to obtain initial credentials from the Kerberos security server.

User Response: Ensure the security server is operational and the correct password is entered. Contact your service representative if the error persists.

EUVF06015E   Unable to resolve key table *name***. Status** *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to resolve the key table name.

User Response: Ensure the key table exists and can

be accessed. Contact your service representative if the error persists.

EUVF06016E   Password is not correct for *name***.**

Explanation: The supplied password is not correct.

User Response: Provide the correct password for the principal.

EUVF06017R   Enter password:

Explanation: The **kinit** command is waiting for the user to enter the password.

User Response: Enter your password.

EUVF06018E   Unable to read password. Status *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to read the password.

User Response: Contact your service representative if the error persists.

EUVF06019E   Unable to store initial credentials in credentials cache *name***. Status** *status-code* **-** *status-message***.**

Explanation: The **kinit** command is unable to store the new credentials in the credentials cache.

User Response: Ensure the credentials cache is available to the user. Contact your service representative if the error persists.

EUVF06020I   Usage: klist [[-c] [-f] [-e] [-s] [-a]] [-k [-e] [-t] [-K]] [name]

Explanation: This message displays the valid command line options for the **klist** command.

-c   List the contents of a credentials cache. This option is mutually exclusive with the **-k** option. This option is the default if neither **-c** nor **-k** is specified.

-k   List the contents of a key table. This option is mutually exclusive with the **-c** option.

-a   Display expired tickets.

-e   Display ticket encryption types.

-f   Display ticket flag values.

-s   Set exit status based on valid TGT existence.

-t   Show key table timestamps.

-K   Show key table keys.

If no name is specified, the default credentials cache or key table is used.

Messages

User Response: None

EUVF06021E *option-1* **and** *option-2* **may not be specified together**

Explanation: Mutually exclusive options are specified.

User Response: Specify just one of the options.

EUVF06022E **No default credentials cache found.**

Explanation: No credentials cache name is specified on the **klist** command line and a default credentials cache was not found.

User Response: Use the **kinit** command to create a default credentials cache or specify the name of the credentials cache on the **klist** command line.

EUVF06023E **Unable to resolve credentials cache** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **klist** command is unable to resolve the credentials cache name.

User Response: Enter a valid credentials cache name. Contact your service representative if the error persists.

EUVF06024E **Unable to retrieve principal from credentials cache** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **klist** command is unable to get the default principal name from the credentials cache.

User Response: Verify that the credentials cache is not modified. Contact your service representative if the error persists.

EUVF06025E **Unable to retrieve ticket from credentials cache** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **klist** command is unable to retrieve a ticket from the credentials cache.

User Response: Use the **kinit** command to create a new credentials cache.

EUVF06026E **Unable to decode ticket. Status** *status-code* **-** *status-message*

Explanation: The **klist** command is unable to decode a ticket retrieved from the credentials cache.

User Response: Verify that the credentials cache is not modified. Contact your service representative if the error persists.

EUVF06027E **No default key table found.**

Explanation: No key table name is entered on the **klist** command line and a default key table is not found.

User Response: Specify the key table name.

EUVF06028E **Unable to resolve key table** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **klist** command is unable to resolve the key table name.

User Response: Enter a valid key table name. Contact your service representative if the error persists.

EUVF06029E **Unable to read entry key table** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **klist** command is unable to read an entry from the key table.

User Response: Verify that the key table is not modified. Contact your service representative if the error persists.

EUVF06030I **Usage: kdestroy [-c cache_name] [-e exp_delta]**

Explanation: This message displays the valid command line options for the **kdestroy** command.

-c Specify the credentials cache name. This option is mutually exclusive with the -e option. The default credentials cache is used if this option is not specified.

-e Specify the credentials expiration time delta value. This option is mutually exclusive with the -c option. The expiration time is computed by subtracting this delta from the current time. A credentials cache is deleted if all of the credentials in the cache have an expiration time earlier than the computed expiration time.

User Response: None

EUVF06031E **No default credentials cache found.**

Explanation: No credentials cache name is specified on the **kdestroy** command line and a default credentials cache was not found.

User Response: Use the **kinit** command to create a default credentials cache or specify the name of the credentials cache on the **kdestroy** command line.

EUVF06032E **Unable to resolve credentials cache** *name*. **Status** *status-code* **-** *status-message*.

Explanation: The **kdestroy** command is unable to resolve the credentials cache name.

User Response: Enter a valid credentials cache name. Contact your service representative if the error persists.

EUVF06033E Unable to destroy credentials cache *name*. **Status** *status-code* **-** *status-message***.**

Explanation: The **kdestroy** command is unable to delete the credentials cache.

User Response: Verify that the credentials cache exists and is accessible. Contact your service representative if the error persists.

EUVF06034I Credentials cache *name* **destroyed.**

Explanation: The **kdestroy** command has successfully deleted the credentials cache.

User Response: None

EUVF06035E Unable to read credentials cache directory. *error-message*

Explanation: The **kdestroy** command is unable to read the credentials cache directory.

User Response: Ensure the credentials cache directory exists and is accessible. Contact your service representative if the error persists.

EUVF06036E Unable to retrieve ticket from credentials cache *name*. **Status** *status-code* **-** *status-message***.**

Explanation: The **kdestroy** command is unable to retrieve a ticket from the credentials cache.

User Response: Use the **kinit** command to create a new credentials cache.

EUVF06037E The name function detects an error. *error-text***.**

Explanation: A system function detected an error. Refer to the documentation for the failing system function to obtain more information about the cause of the failure.

User Response: Contact your service representative if the error persists.

EUVF06038E Usage: keytab add | delete | list principal [-p password] [-v version] [-k keytab]

Explanation: This message displays the valid command line options for the **keytab** command.

-k Specify the key table name. The default key table is used if this option is not specified.

-p Specify the password when adding an entry to

the key table. The user is prompted for the password if this option is not specified.

-v Specify the key version number. When adding a key, the next version number is assigned if this option is not specified. When deleting a key, all keys for the principal are deleted if this option is not specified.

User Response: None

EUVF06039E *value* **is not a valid number.**

Explanation: A non-numeric value was entered for a numeric field.

User Response: Specify a valid number.

EUVF06040E The key version must not be zero.

Explanation: The key version starts at 1 and increments for each new key.

User Response: Specify a valid key version number.

EUVF06041E You must specify add, delete, or list.

Explanation: No operation is specified on the **keytab** command line.

User Response: Specify add, delete, or list.

EUVF06042E No default key table found.

Explanation: No key table name is entered on the **keytab** command line and a default key table was not found.

User Response: Specify the key table name.

EUVF06043E Unable to resolve key table *name*. **Status** *status-code* **-** *status-message***.**

Explanation: The **keytab** command is unable to resolve the key table name.

User Response: Enter a valid key table name. Contact your service representative if the error persists.

EUVF06044E Unable to read entry key table *name*. **Status** *status-code* **-** *status-message***.**

Explanation: The **keytab** command is unable to read an entry from the key table.

User Response: Verify that the key table was not modified. Contact your service representative if the error persists.

Messages

EUVF06045E You must specify the principal name.

Explanation: The principal name is not specified for a key table add or delete operation.

User Response: Specify the principal name.

EUVF06046E Unable to parse principal name. Status *status-code* **-** *status-message***.**

Explanation: The **keytab** command was unable to parse the principal name.

User Response: Specify a valid principal name on the **keytab** command line.

EUVF06047E The *option* **is not valid for** *operation* **request.**

Explanation: An option was specified on the **keytab** command line that is not valid for the requested operation.

User Response: Specify options that are supported by the requested operation.

EUVF06048R Enter password:

Explanation: The **keytab** command needs the user password to complete a request.

User Response: Enter your password.

EUVF06049R Re-enter password:

Explanation: The **keytab** command needs the user password to complete a request.

User Response: Enter your password.

EUVF06050E Unable to read password. Status *status-code* **-** *status-message***.**

Explanation: The **keytab** command is unable to obtain the password from the user.

User Response: Contact your service representative if the error persists.

EUVF06051E Unable to add entry to key table *name***.**

Explanation: The **keytab** command is unable to add an entry to the key table.

User Response: Ensure that the key table is accessible. Contact your service representative if the error persists.

EUVF06052E Unable to remove entry from key table *name***.**

Explanation: The **keytab** command was unable to remove an entry from the key table.

User Response: Ensure that the key table is accessible. Contact your service representative if the error persists.

EUVF06053E Key version *version* **not found for** *principal***.**

Explanation: The **keytab** command was unable to delete the requested key version because the key table entry does not exist.

User Response: None

EUVF06054E No entries found for *principal***.**

Explanation: The **keytab** command was not able to find any key table entries for the specified principal.

User Response: None

EUVF06055I Usage: ksetup [-h host] [-n name] [-p password] [-e]

Explanation: This message displays the valid command line options for the **ksetup** command.

-h　　　Specify the host for the LDAP server. The host is specified as *host-name:port-number*. The default LDAP port of 389 is used if the port number is omitted. The LDAP server specification in the Kerberos configuration file is used if this option is omitted.

-n　　　Specify the distinguished name to use when binding to the LDAP server. The LDAP_BINDDN environment variables used if this option is omitted.

-p　　　Specify the password to use when binding to the LDAP server. The LDAP_BINDPW environment variable is used if this option is omitted.

-e　　　Echo each command to **stdout.**

User Response: None

EUVF06056E *command* **is not a valid subcommand.**

Explanation: The indicated subcommand is not valid for the **ksetup** command.

User Response: Enter a valid subcommand.

EUVF06057I Valid subcommands are addhost, addkdc, addpwd, addadmin, delhost, delkdc, delpwd, deladmin, listhost, listkdc, listpwd, listadmin, exit.

Explanation: This message lists the valid subcommands for the **ksetup** command.

User Response: None

EUVF06058E Unable to initialize LDAP client. *error-text***.**

Explanation: The **ksetup** command was unable to initialize the LDAP client runtime. The error text provides additional information on the cause of the failure.

User Response: Contact your service representative.

EUVF06059E Unable to bind to LDAP server. *error-text***.**

Explanation: The **ksetup** command was unable to bind to the LDAP server. The error text provides additional information on the cause of the failure.

User Response: Ensure that the LDAP server is operational and that the bind name and password are correct. Contact your service representative if the error persists.

EUVF06060E Realm name must be specified.

Explanation: The realm name must be specified on the **ksetup** subcommand.

User Response: Specify a realm name.

EUVF06061E Host name must be specified.

Explanation: The host name must be specified on the **ksetup** subcommand.

User Response: Specify a host name.

EUVF06062E Too many positional parameters.

Explanation: Too many positional parameters are specified.

User Response: Specify a valid subcommand.

EUVF06063E Host *name* **already exists.**

Explanation: The host cannot be added to the LDAP directory because it already exists.

User Response: None

EUVF06064E Root domain *name* **is not defined.**

Explanation: The root domain is not defined in the LDAP directory.

User Response: Add the root domain to the LDAP directory by adding the appropriate naming suffix entry to the LDAP server configuration file.

EUVF06065E Realm name *name* **is not valid.**

Explanation: A realm name consists of one or more domain components separated by periods.

User Response: Enter a valid realm name.

EUVF06066E The *name* **function detects an error. DN:** *distinguished-name error-text*

Explanation: An LDAP function detected an error for the specified distinguished name.

User Response: Ensure that the LDAP server is operational. Contact your service representative if the error persists.

EUVF06067E Insufficient storage available.

Explanation: There is not enough storage available to process the request.

User Response: Increase the amount of storage available to the command.

EUVF06068E Host name *name* **is not valid.**

Explanation: A host name may not contain a colon.

User Response: Enter a valid host name.

EUVF06069E Port number *value* **is not valid.**

Explanation: The port value is not a valid number.

User Response: Enter a valid number.

EUVF06070E Host *name* **is not defined.**

Explanation: The **ksetup** command was unable to delete the indicated host because it is not defined in the LDAP directory.

User Response: None.

EUVF06071E No KDC defined for host *name***.**

Explanation: The **ksetup** command was unable to delete the KDC definition because no KDC is defined for the indicated host.

User Response: None.

Messages

EUVF06072E   Unable to obtain default realm name. Status *status-code* **-** *status-message***.**

Explanation: The **ksetup** command is unable to obtain the default realm name.

User Response: Ensure the default realm name is set in the Kerberos configuration file. Contact your service representative if the error persists.

EUVF06073E   Principal name not allowed with -s option.

Explanation: The principal name may not be specified on the **kinit** command when the **-s** option is specified.

User Response: Do not specify a principal name when using the system identity.

EUVF06074E   Principal *name* **is not valid. Status** *status-code* **-** *status-message***.**

Explanation: The principal name specified on the **kvno** command line is not valid.

User Response: Enter a valid principal name.

EUVF06075E   Network credentials are not available. Status *status-code* **-** *status-message***.**

Explanation: No default network credentials are available.

User Response: Use the **kinit** command to create a default credentials cache and then retry the **kvno** command.

EUVF06076E   Unable to obtain temporary credentials cache. Status *status-code* **-** *status-message***.**

Explanation: The **kvno** command is unable to create a temporary credentials cache.

User Response: Contact your service representative if the error persists.

EUVF06077E   Unable to obtain service ticket. Status *status-code* **-** *status-message***.**

Explanation: The **kvno** command is unable to obtain a service ticket for the specified principal.

User Response: Verify that the Kerberos security server is started and that the principal is enabled for service tickets. Then retry the **kvno** command. Contact your service representative if the error persists.

EUVF06078E   Principal *name* **is not valid. Status** *status-code* **-** *status-message***.**

Explanation: The principal name specified on the **kpasswd** command line is not valid.

User Response: Enter a valid principal name.

EUVF06079E   Unable to read default credentials cache *name***. Status** *status-code* **-** *status-message***.**

Explanation: The **kpasswd** command is unable to obtain the principal name from the default credentials cache.

User Response: Create a new default credentials cache using the **kinit** command and then retry the **kpasswd** command.

EUVF06080E   No default credentials cache.

Explanation: There is no default credentials cache for the current user.

User Response: Either create a default credentials cache using the **kinit** command or specify the principal name on the **kpasswd** command line.

EUVF06081E   Unable to parse *name***. Status** *status-code* **-** *status-message***.**

Explanation: The **kpasswd** command is unable to parse the principal name.

User Response: Enter a valid principal name and retry the command. Contact your support representative if the error persists.

EUVF06082E   Unable to map user *name* **to a Kerberos principal. SAF error** *code***, Return code** *code***, Reason code** *code***.**

Explanation: The **kpasswd** command is unable to map the user ID to a Kerberos principal. Refer to the description of the IRRSIM00 function in the *z/OS: Security Server RACF Callable Services* document for more information on the error codes.

User Response: Verify that the user ID is defined in the security database with an associated Kerberos principal.

EUVF06083I Changing password for *principal***.**

Explanation: The **kpasswd** command is changing the password for the indicated principal.

User Response: None

EUVF06084R   Enter current password:

Explanation: The **kpasswd** command needs the current password for the principal.

User Response: Enter the current password.

EUVF06085R   Enter new password:

Explanation: The **kpasswd** command needs the new password for the principal.

User Response: Enter the new password.

EUVF06086R   Re-enter new password:

Explanation: The **kpasswd** command compares both new password values to check for typing errors.

User Response: Enter the new password again.

EUVF06087E   Unable to read password. Status
*status-code - status-message***.**

Explanation: The **kpasswd** command is unable to obtain a password from the user.

User Response: Contact your service representative.

EUVF06088E   Unable to obtain initial ticket. Status
*status-code - status-message***.**

Explanation: The **kpasswd** command is unable to obtain an initial ticket to the **kadmin/changepw** service.

User Response: Verify that the **kadmin/changepw** principal is defined in the security database. Contact your service representative if the error persists.

EUVF06089E   Password is not correct for *principal***.**

Explanation: The entered password is not correct.

User Response: Enter the correct password for the principal. Contact your service representative if the error persists.

EUVF06090E   Unable to issue password change
request. Status *status-code -*
*status-message***.**

Explanation: The **kpasswd** command was unable to send the password change request to the password server.

User Response: Verify that the password server is defined properly and is operational. Contact your service representative if the error persists.

EUVF06091E   Password change request failed.
Error code *error-code - error-message***.**

Explanation: The password change request was rejected by the password server.

User Response: Verify that the new password is valid for the user and that the user is authorized to change his password. Contact your service representative if the error persists.

EUVF06092E   Password change request failed.
Error code *error-code - error-message***.**
Server status:*status-message***.**

Explanation: The password change request was rejected by the password server.

User Response: Verify that the new password is valid for the user and that the user is authorized to change his password. Contact your service representative if the error persists.

EUVF06093I Password changed.

Explanation: The password has been changed.

User Response: None

EUVF06094I Password change canceled.

Explanation: The password change request was canceled because no password was entered in response to the prompt.

User Response: None

EUVF06095E   No password server defined for host
*name***.**

Explanation: The **ksetup** command is unable to delete a password server definition because no password server is associated with the indicated host.

User Response: None

EUVF06096I Key table add canceled.

Explanation: The key table add request was canceled because no password was entered in response to the prompt.

User Response: None

EUVF06097E   No administration server defined for
host *name***.**

Explanation: The **ksetup** command was unable to delete an administration server definition because no administration server is associated with the indicated host.

User Response: None

Messages

EUVF06098I Usage: kpasswd [-A] principal

Explanation: This message displays the valid command line options for the **kpasswd** command.

-A Specifies that an address list will not be included in the initial ticket used by the **kpasswd** command.

principal
Specifies the principal whose password is to be changed.

User Response: None

EUVF06099I Usage: kadmin [-r realm] [-p principal] [-k keytab] [-w password] [-A] [-e]

Explanation: This message displays the valid command line options for the **kadmin** command.

-r realm
Specifies the Kerberos administration realm. The local realm is used if this option is not specified.

-p principal
Specifies the administrator principal. The string **/admin** is appended to the principal obtained from the credentials cache if this option is not specified.

-k keytab
Specifies the key table containing the password for the administrator principal. The user is prompted to enter the password if neither the **-k** nor the **-w** option is specified.

-w password
Specifies the password for the administrator principal. The user is prompted to enter the password if neither the **-k** nor the **-w** option is specified.

-A Specifies that an address list will not be included in the initial ticket used by the kadmin command.

-e Echo each command to **stdout**.

User Response: None

EUVF06100E *subcommand* **is not a valid subcommand.**

Explanation: The specified subcommand is not valid for the **kadmin** command.

User Response: Enter a valid subcommand.

EUVF06101I Valid subcommands:

```
list_principals  (listprincs)
get_principal  (getprinc)
add_principal  (addprinc)
delete_principal  (delprinc)
modify_principal  (modprinc)
rename_principal  (renprinc)
change_password  (cpw)
```

```
list_policies  (listpols)
get_policy  (getpol)
add_policy  (addpol)
modify_policy  (modpol)
delete_policy  (delpol)
get_privs  (getprivs)
add_key  (ktadd)
exit  (quit)
```

Explanation: This message lists the valid subcommands for the **kadmin** command.

User Response: None

EUVF06102E Unable to obtain principal from default credentials cache. *Status-code - Error-text.*

Explanation: The **kadmin** command was unable to obtain the principal from the default credentials cache.

User Response: Verify that the credentials cache can be accessed and has not been modified.

EUVF06103E Unable to determine the administration principal.

Explanation: The **kadmin** is unable to determine the administration principal.

User Response: Either specify the **-p** command line option for the **kadmin** command or use the **kinit** command to set up a default credentials cache.

EUVF06104E Unable to initialize connection with administration server.

Explanation: The **kadmin** command is unable to establish a connection with the Kerberos administration server.

User Response: Verify that the administration server is running and then retry the request.

EUVF06105E Unable to perform *request-type* administration request.

Explanation: The **kadmin** command is unable to perform the requested administration function.

User Response: Verify that the administration server is running and then retry the request. Contact your service representative if the error persists.

EUVF06106E Too many positional parameters.

Explanation: Too many positional parameters are specified.

User Response: Specify a valid subcommand.

EUVF06107I list_principals [expression]

Explanation: This message displays the syntax for the **list_principals** subcommand.

User Response: None

EUVF06108E Unable to obtain default realm.
Status-code - Error-text.

Explanation: The **kadmin** command is unable to get the default realm from the Kerberos configuration file.

User Response: Verify that the default realm is defined in the Kerberos configuration file.

EUVF06109E No name specified.

Explanation: No object name is specified on a **kadmin** subcommand.

User Response: Specify an object name.

EUVF06110I get_principal name

Explanation: This message displays the syntax for the **get_principal** subcommand.

User Response: None

EUVF06111E Unable to parse principal name *name***.**

Explanation: The **kadmin** command is unable to parse the indicated principal name.

User Response: Specify a valid principal name.

EUVF06112I add_principal [options] [attributes] name

Explanation: This message displays the syntax for the **add_principal** subcommand.

User Response: None

EUVF06113E The *name* **option requires a value.**

Explanation: The indicated **kadmin** subcommand option requires a value but no value was specified.

User Response: Specify a value for the option.

EUVF06114E The date specified for the *option* **option is not valid.**

Explanation: The date is not valid. Refer to the *z/OS: Security Server Network Authentication Service Programming* for a description of the valid date formats. This error can also occur if the specified date is in the past.

User Response: Specify a valid date.

EUVF06115E Key version *version* **is not valid.**

Explanation: The key version is not valid. The key version is an unsigned number between 1 and 2147483647.

User Response: Specify a valid key version.

EUVF06116R Enter password:

Explanation: The **kadmin** command is waiting for the user to enter the password.

User Response: Enter the password for the principal.

EUVF06117R Re-enter password:

Explanation: The **kadmin** command is waiting for the user to re-enter the password. The re-entered password must match the password that was entered previously.

User Response: Enter the password for the principal.

EUVF06118E Password is too long.

Explanation: The password is longer than 128 characters.

User Response: Enter a shorter password.

EUVF06119E Unable to read password. Status
*status-code - status-message***.**

Explanation: The **kadmin** command is unable to read the password.

User Response: Contact your service representative if the error persists.

EUVF06120I list_policies [expression]

Explanation: This message displays the syntax for the **list_policies** subcommand.

User Response: None

EUVF06121I get_policy name

Explanation: This message displays the syntax for the **get_policy** subcommand.

User Response: None

EUVF06122I Principal *name* **added.**

Explanation: The indicated principal has been added to the Kerberos database.

User Response: None

Messages

EUVF06123I delete_principal name

Explanation: This message displays the syntax for the **delete_principal** subcommand.

User Response: None

EUVF06124I Principal *name* **deleted.**

Explanation: The indicated principal has been deleted from the Kerberos database.

User Response: None

EUVF06125I modify_principal [options] [attributes] name

Explanation: This message displays the syntax for the **modify_principal** subcommand.

User Response: None

EUVF06126I Principal *name* **modified.**

Explanation: The indicated principal has been modified in the Kerberos database.

User Response: None

EUVF06127I rename_principal oldname newname

Explanation: This message displays the syntax for the **rename_principal** subcommand.

User Response: None

EUVF06128I Principal *oldname* **renamed to** *newname***.**

Explanation: The indicated principal has been renamed in the Kerberos database.

User Response: None

EUVF06129E Subcommand is too long.

Explanation: The maximum length of a **kadmin** subcommand is 1023 characters.

User Response: Enter a shorter subcommand string.

EUVF06130I change_password [-randkey | -pw password] [-keepold] [-e keytypes] name

Explanation: This message displays the syntax for the **change_password** subcommand.

User Response: None

EUVF06131I Random keys generated for *name***.**

Explanation: Random keys have been generated for the indicated principal.

User Response: None

EUVF06132I Administration request cancelled.

Explanation: The user canceled the current **kadmin** request by entering a zero-length password when prompted.

User Response: None

EUVF06133I Password changed for *name*

Explanation: The password has been changed for the indicated principal.

User Response: None

EUVF06134E *value* **is not a valid numeric value.**

Explanation: A positive number is required.

User Response: Enter a valid number.

EUVF06135I add_policy [options] name

Explanation: This message displays the syntax for the **add_policy** subcommand.

User Response: None

EUVF06136I Policy *name* **added.**

Explanation: The indicated policy has been added to the Kerberos database.

User Response: None

EUVF06137I modify_policy [options] name

Explanation: This message displays the syntax for the **modify_policy** subcommand.

User Response: None

EUVF06138I Policy *name* **modified.**

Explanation: The indicated policy has been modified in the Kerberos database.

User Response: None

EUVF06139I delete_policy name

Explanation: This message displays the syntax for the **delete_policy** subcommand.

User Response: None

EUVF06140I Policy *name* **deleted.**

Explanation: The indicated policy has been deleted from the Kerberos database.

User Response: None

EUVF06141I help [subcommand]

Explanation: This message displays the syntax for the help subcommand.

User Response: None

EUVF06142I exit

Explanation: This message displays the syntax for the exit subcommand.

User Response: None

**EUVF06143I add_key [[-keytab | -k] keytab_name]
[-keepold] [-e keytypes] principal_name**

Explanation: This message displays the syntax for the **add_key** subcommand.

User Response: None

EUVF06144I Keys generated for *principal* **and added
to** *keytab***.**

Explanation: Random keys have been generated for the indicated principal.

User Response: None

EUVF06145E Unable to open key table *name***.
Status** *status-code - status-message***.**

Explanation: The **kadmin** command is unable to open the indicated key table.

User Response: Verify that the key table exists and can be accessed. Contact your service representative if the error persists.

EUVF06146E Unable to add entry to key table
*name***. Status** *status-code -
status-message*

Explanation: The **kadmin** command is unable to add an entry to the indicated key table.

User Response: Verify that the key table can be accessed. Contact your service representative if the error persists.

EUVF06147I Authenticating as *name***.**

Explanation: The **kadmin** command is obtaining an initial ticket for the indicated principal. The administration privileges associated with this principal are used for subsequent administration requests.

User Response: None

EUVF06148I get_privs

Explanation: This message displays the syntax for the **get_privs** subcommand.

User Response: None

EUVF06149E Encryption type *name* **is not valid.**

Explanation: An unrecognized encryption type was specified.

User Response: Specify a valid encryption type.

EUVF06150E Salt type *name* **is not valid.**

Explanation: An unrecognized salt type was specified.

User Response: Specify a valid salt type.

**EUVF06151E Connection broken with the
administration server.**

Explanation: The connection with the administration server has been broken. This indicates either a network problem or a server failure.

User Response: Verify the network connectivity with the administration server. Contact your service representative if the error persists.

Appendix A. Sample Kerberos configurations

In this appendix, IBM provides sample configurations for three Kerberos realms:

- The KRB390.IBM.COM realm with the KDC on z/OS using z/OS Kerberos. The DNS domain is **krb390.ibm.com**. The sysplex contains two systems with host names **dcesec4.krb390.ibm.com** and **dcesec7.krb390.ibm.com**.

- The KRB2000.IBM.COM realm with the KDC on the Microsoft Windows 2000 operating system using Windows 2000 Server. The DNS domain is **krb2000.ibm.com** and the domain controller is **sstone1.krb2000.ibm.com**.

- The MITKRB.IBM.COM realm with the KDC on AIX using MIT Kerberos 1.2.1. The DNS domain is **mitkrb.ibm.com** and the KDC is located on the **dcecpt.mitkrb.ibm.com** system.

  The DNS server for this example is located on Windows 2000.

The z/OS commands used in these examples assume that the external security manager is RACF.

KRB390.IBM.COM configuration

For this configuration, do these steps:

1. Network Authentication Service for z/OS supports three encryption types: 56-bit DES (DES), 56-bit DES with key derivation (DESD), and 168-bit triple DES (DES3). By default, only DES is enabled. If you want to enable the additional encryption types, use the RACF SETROPTS command to change KERBLVL from 0 to 1. After this is done, RACF creates keys for all three encryption types when a user changes his password. The use of the additional encryption keys can be controlled on an individual user basis through the ENCRYPT option of the KERB keyword on the ALTUSER and RALTER commands.

2. By default, the z/OS KDC uses 56-bit DES to encrypt tickets. If you want to enable the use of the additional encryption algorithms when encrypting tickets, add the following line to **/etc/skrb/home/kdc/envar**:

   ```
   SKDC_TKT_ENCTYPES=des3-cbc-sha1,des-hmac-sha1,des-cbc-crc
   ```

3. Edit **/etc/skrb/krb5.conf** and define the local realm. Copy the initial configuration file from **/usr/lpp/skrb/examples/krb5.conf**. In this file, the **default_realm** value is set to the local realm, the **kdc_default_options** value is set to request forwardable tickets, and the **use_dns_lookup** value is set to use the DNS name server instead of the [realms] and [domain_realm] sections of the configuration file. For completeness, the [realms] and [domain_realm] sections are set but aren't needed since the DNS name server is used to locate Kerberos services (SRV records) and to resolve host names to realm names (TXT records).

   ```
   [libdefaults]
   default_realm = KRB390.IBM.COM
   kdc_default_options = 0x40000010
   use_dns_lookup = 1
   [realms]
   KRB390.IBM.COM = {
       kdc = dcesec4.krb390.ibm.com:88
       kdc = dcesec7.krb390.ibm.com:88
       kpasswd_server = dcesec4.krb390.ibm.com:464
       kpasswd_server = dcesec7.krb390.ibm.com:464
   }
   [domain_realm]
   .krb390.ibm.com = KRB390.IBM.COM
   ```

4. Define the default realm attributes in the RACF database. The password can be any value, but the resource name must be KERBDFLT. The KERBNAME value specifies the name of the local Kerberos realm. For this example, the minimum ticket life is 15 seconds, the default ticket life is 10 hours, and the maximum ticket life is 24 hours. Note that the realm name is converted to upper case by the RDEFINE command but the password is unchanged.

```
RDEFINE REALM KERBDFLT KERB(KERBNAME(KRB390.IBM.COM)
    PASSWORD(74427532) MINTKTLFE(15) DEFTKTLFE(36000)
    MAXTKTLFE(86400))
```

5. Define the password change service. The user name and password can be any value but the Kerberos principal must be **kadmin/changepw**. Note that the password is converted to upper case by the ALTUSER command but the principal is unchanged.

```
ADDUSER CHANGEPW DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER CHANGEPW PASSWORD(74427533) NOEXPIRED
    KERB(KERBNAME(kadmin/changepw))
```

6. Create Kerberos principals for the samples shipped in **/usr/lpp/skrb/examples/gssapi_test** and **/usr/lpp/skrb/examples/krbmsg_test**. The user name and password can be any value but the Kerberos principal names must match the values coded in the examples. Note that the password is converted to upper case by the ALTUSER command but the principal is unchanged.

```
ADDUSER KRBSRV4 DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER KRBSRV4 PASSWORD(TEST4SRV) NOEXPIRED
    KERB(KERBNAME(test_server/dcesec4.krb390.ibm.com))
ADDUSER KRBSRV7 DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER KRBSRV7 PASSWORD(TEST7SRV) NOEXPIRED
    KERB(KERBNAME(test_server/dcesec7.krb390.ibm.com))
ADDUSER KRBDLG4 DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER KRBDLG4 PASSWORD(TEST4DLG) NOEXPIRED
    KERB(KERBNAME(test_delegate/dcesec4.krb390.ibm.com))
ADDUSER KRBDLG7 DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER KRBDLG7 PASSWORD(TEST7DLG) NOEXPIRED
    KERB(KERBNAME(test_delegate/dcesec7.krb390.ibm.com))
ADDUSER KRBCLNT DFLTGRP(SYS1) PASSWORD(TEMPPASS)
ALTUSER KRBCLNT PASSWORD(TESTPSWD) NOEXPIRED
    KERB(KERBNAME(test_client))
```

7. Because the SKRBKDC started task is running on each system in the sysplex, there is no need to set up key tables for use by applications. Instead, the KRB5_SERVER_KEYTAB environment variable is set to 1.

With RACF as the external security manager, the IRR.RUSERMAP resource in the FACILITY class must be defined. The **test_server** and **test_delegate** system IDs (for example, KRBSRV4 and KRBDLG4) must have RACF READ access to IRR.RUSERMAP resource to use the KRB5_SERVER_KEYTAB variable set to 1. To define IRR.RUSERMAP and grant READ authority to all system users:

```
REDEFINE FACILITY IRR.RUSERMAP UACC(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

See "Security runtime environment variables" on page 19 for more on the KRB5_SERVER_KEYTAB environment variable.

8. Create SRV records for the **_kerberos** and **_kpasswd** services using the UDP and TCP protocols. The example that follows uses the Microsoft® Windows® 2000 DNS management console to create the SRV entries for the **krb390.ibm.com** domain. The SKRBKDC started task is running on both the **dcesec4** and **dcesec7** systems, so there are **_kerberos** and **_kpasswd** entries for both systems. The Kerberos runtime randomly selects entries with the same priority when attempting to contact a service provider, so this example uses the same priority for all entries to provide rudimentary load balancing.
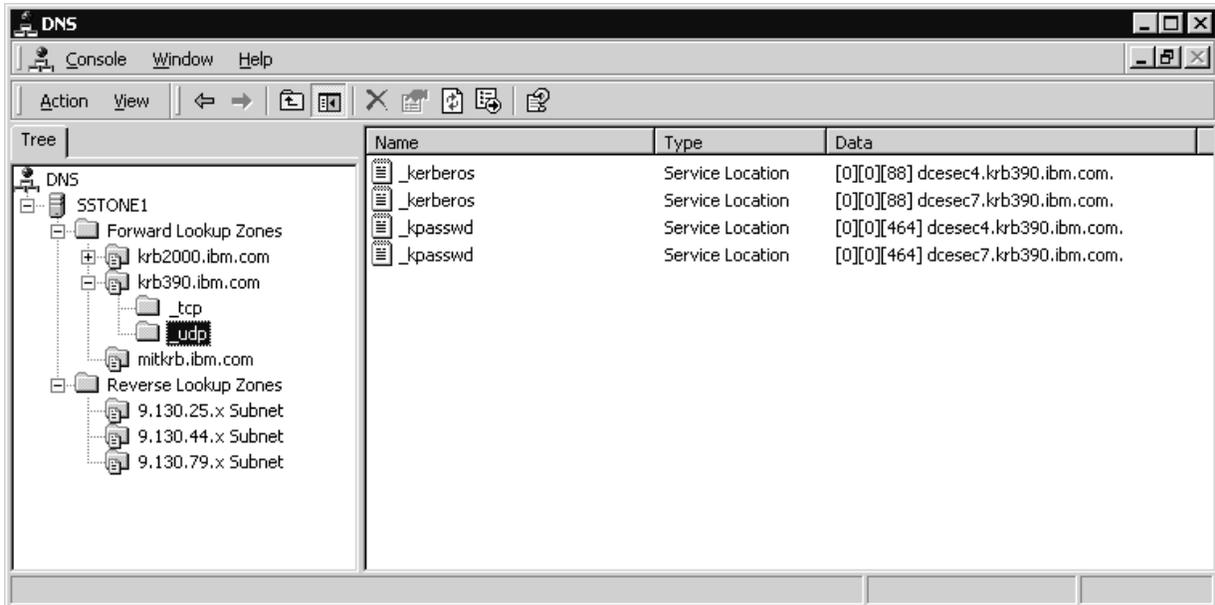
Figure 4. KRB390.IBM.COM configuration - creating SRV entries

9. Create a TXT record to map host names in the **krb390.ibm.com** DNS domain to the KRB390.IBM.COM Kerberos realm. This example uses the Windows 2000 DNS management console to create the TXT record.
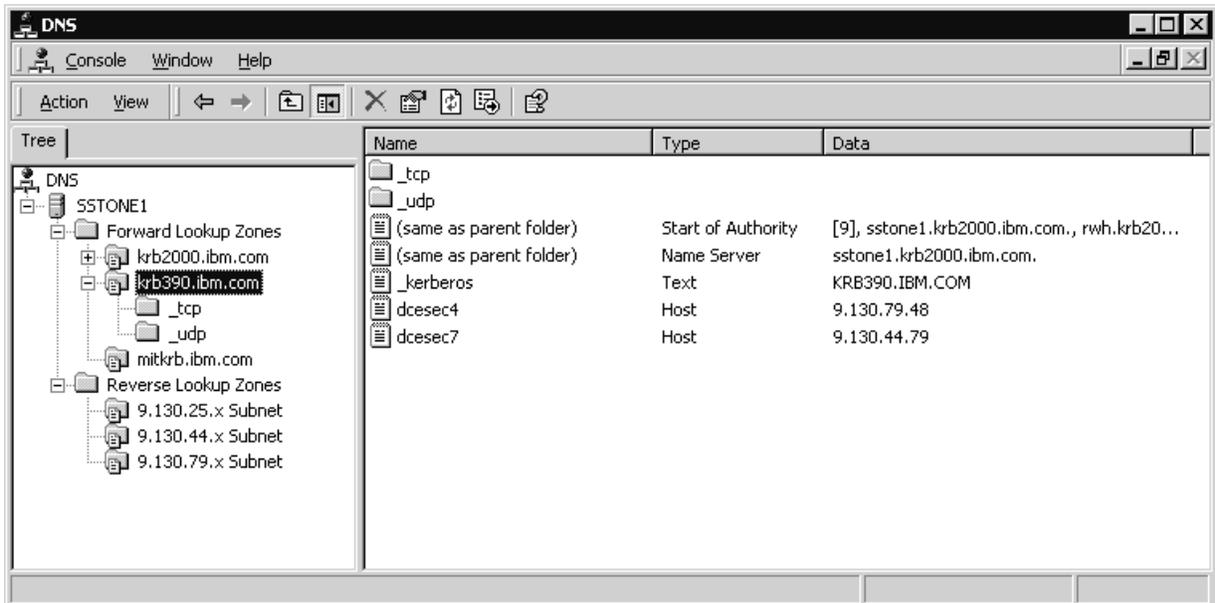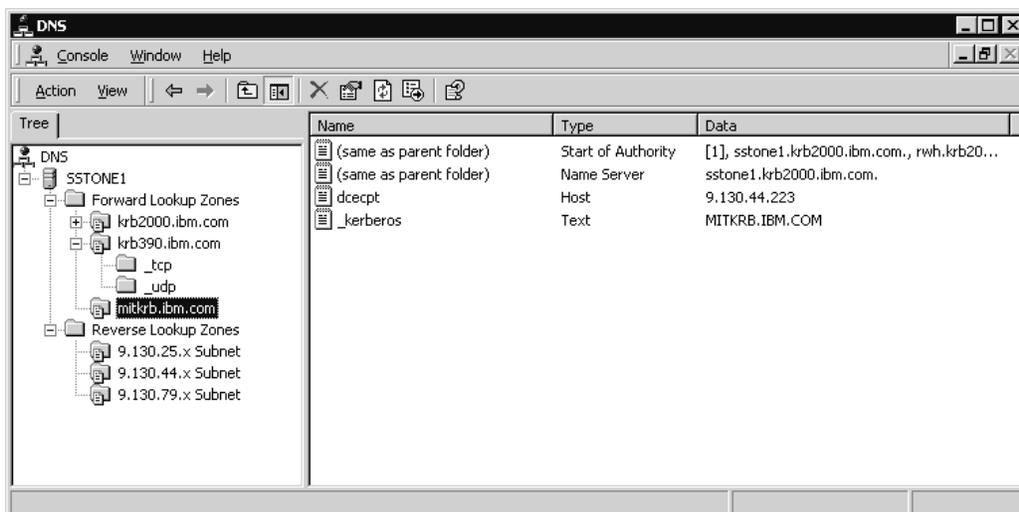

Figure 5. KRB390.IBM.COM configuration - creating a TXT record

KRB2000.IBM.COM configuration

For this configuration, do these steps:

1. The usual Windows® 2000 server installation sets up the active directory and creates SRV records for the **_kerberos** and **_kpasswd** services provided by the Windows 2000 domain controller. However, the server installation does not create a TXT record to map host names in the Windows 2000 domain, so you have to create one yourself.
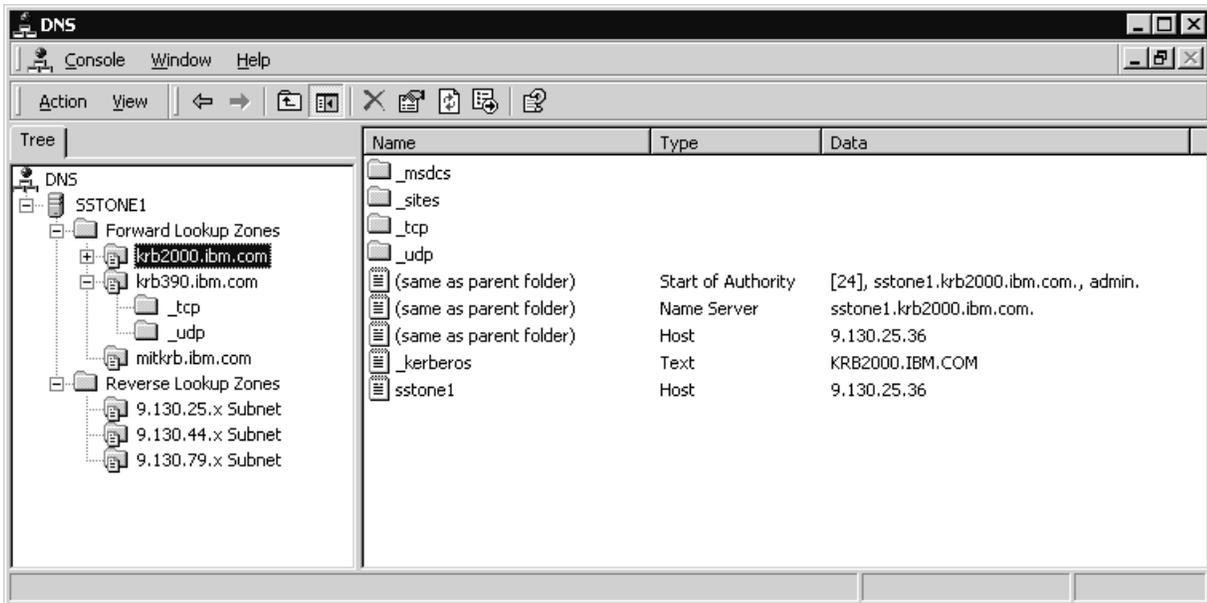
Figure 6. KRB2000.IBM.COM configuration - creating a TXT record to map host names

2. Set up a peer-to-peer trust relationship between the KRB390.IBM.COM realm and the KRB2000.IBM.COM. This allows clients in the KRB2000.IBM.COM realm to access services in the KRB390.IBM.COM realm, and vice versa.

3. The following RACF commands set up the z/OS side of the peer-to-peer trust relationship. Note that the password is case-sensitive on the RDEFINE REALM command but the realm name is converted to upper case.

```
RDEFINE REALM
    /.../KRB390.IBM.COM/krbtgt/KRB2000.IBM.COM
    KERB(PASSWORD(peerw2kp))
RDEFINE REALM
    /.../KRB2000.IBM.COM/krbtgt/KRB390.IBM.COM
    KERB(PASSWORD(peer390p))
```

4. Windows 2000 does not support the DES3 and DESD encryption types. If these encryption types have been enabled for the z/OS KDC, they should be disabled for cross-realm ticket-granting tickets issued for the Windows 2000 realm.

```
RALTER REALM
    /.../KRB390.IBM.COM/krbtgt/KRB2000.IBM.COM
    KERB(ENCRYPT(NODESD NODES3))
```

5. Use the Active Directory Domains and Trusts management console to set up the Windows 2000 side of the peer-to-peer trust relationships. Open the Properties dialog for the **krb2000.ibm.com** domain. The password specified for the "Domains trusted by this domain" entry must be the same as the password specified on the /.../KRB390.IBM.COM/krbtgt/KRB2000.IBM.COM RDEFINE command. The password specified for the "Domains that trust this domain" entry must be the same as the password specified on the /.../KRB2000.IBM.COM/krbtgt/KRB390.IBM.COM RDEFINE command.
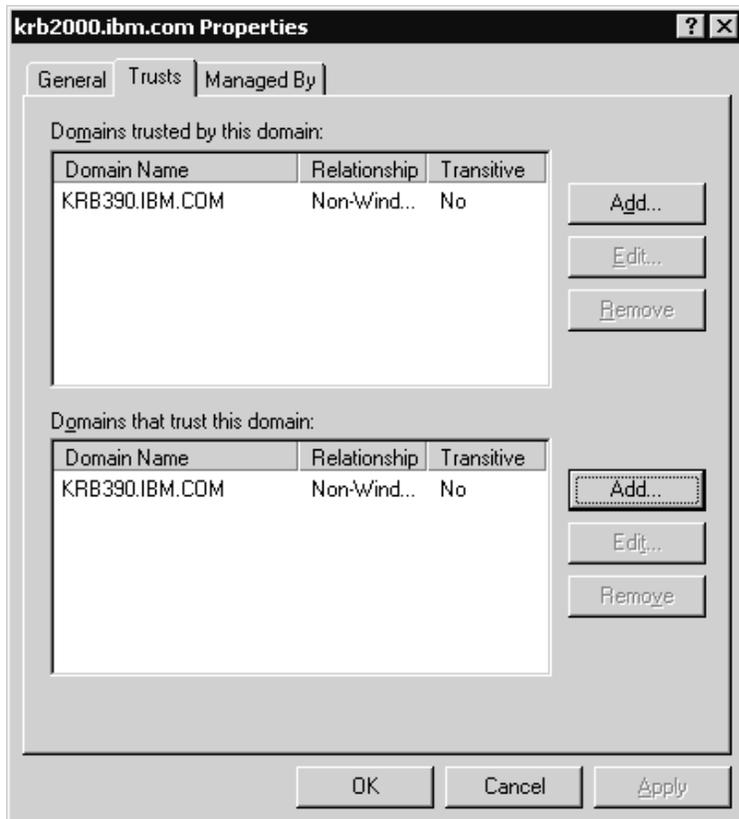
Figure 7. KRB390.IBM.COM configuration - setting up the Windows 2000 side of the peer-to-peer trust relationships

6. Define the location of the KRB390.IBM.COM KDC on each Windows 2000 client using the **ksetup** command. This command is shipped as part of the Windows 2000 Support Tools on the Windows 2000 CD.

```
ksetup /addkdc KRB390.IBM.COM dcesec4.krb390.ibm.com
ksetup /addkdc KRB390.IBM.COM dcesec7.krb390.ibm.com
```

MITKRB.IBM.COM configuration

For this configuration, do these steps:

1. Edit **/etc/krb5.conf** and add definitions for the KRB390.IBM.COM and KRB2000.IBM.COM realms.

```
[libdefaults]
    ticket_lifetime = 600
    default_realm = MITKRB.IBM.COM
    default_tkt_enctypes = des-cbc-crc
    default_tgs_enctypes = des-cbc-crc
    default_keytab_name = /etc/krb5.keytab

[realms]
    MITKRB.IBM.COM = {
        kdc = dcecpt.mitkrb.ibm.com:88
        kpasswd_server = dcecpt.mitkrb.ibm.com:464
        admin_server = dcecpt.mitkrb.ibm.com:749
        default_domain = mitkrb.ibm.com
    }

    KRB390.IBM.COM = {
        kdc = dcesec7.krb390.ibm.com:88
        kpasswd_server = dcesec7.krb390.ibm.com:464
        default_domain = krb390.ibm.com
```

```
        }

        KRB2000.IBM.COM = {
            kdc = sstone1.krb2000.ibm.com:88
            kpasswd_server = sstone1.krb2000.ibm.com:464
            default_domain = krb2000.ibm.com
        }

    [domain_realm]
        .mitkrb.ibm.com = MITKRB.IBM.COM
        .krb390.ibm.com = KRB390.IBM.COM

    [capaths]
    MITKRB.IBM.COM = {
        KRB390.IBM.COM = .
        KRB2000.IBM.COM = .
    }
```

2. Create SRV records for the **_kerberos** and **_kpasswd** services using the UDP protocol (MIT Kerberos does not support the TCP protocol for the **_kerberos** and **_kpasswd** services). Create an SRV record for the **_kerberos-adm** service using the TCP protocol. This example uses the Windows 2000 DNS management console to create the SRV entries for the **mitkrb.ibm.com** domain.
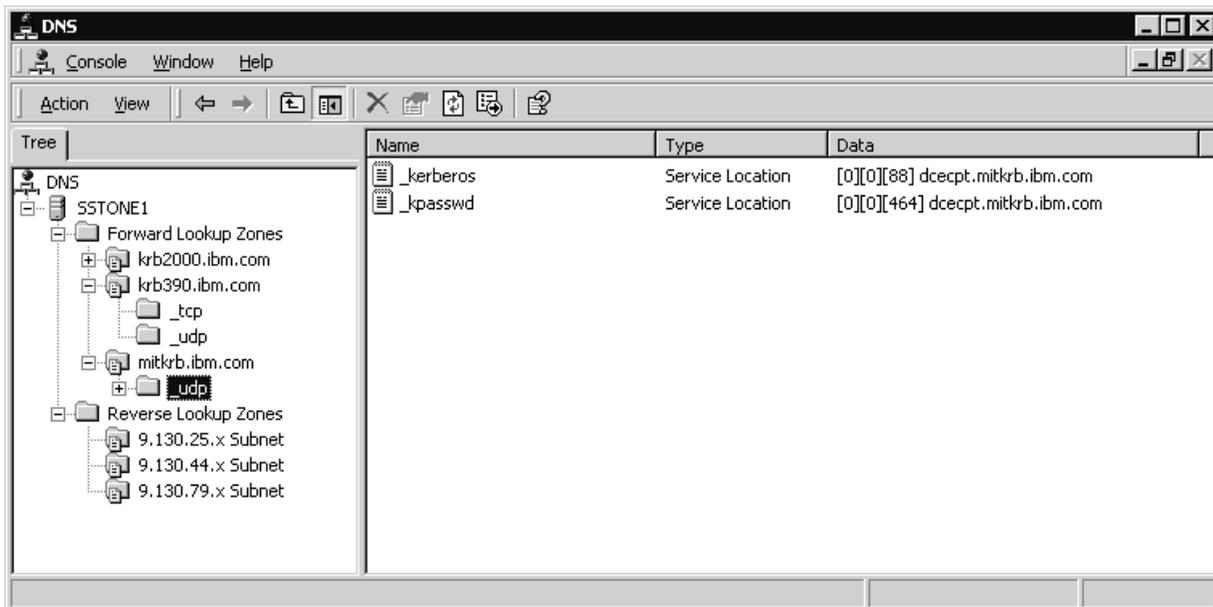
Figure 8. MITKRB.IBM.COM configuration - creating an SRV record using the UDP protocol
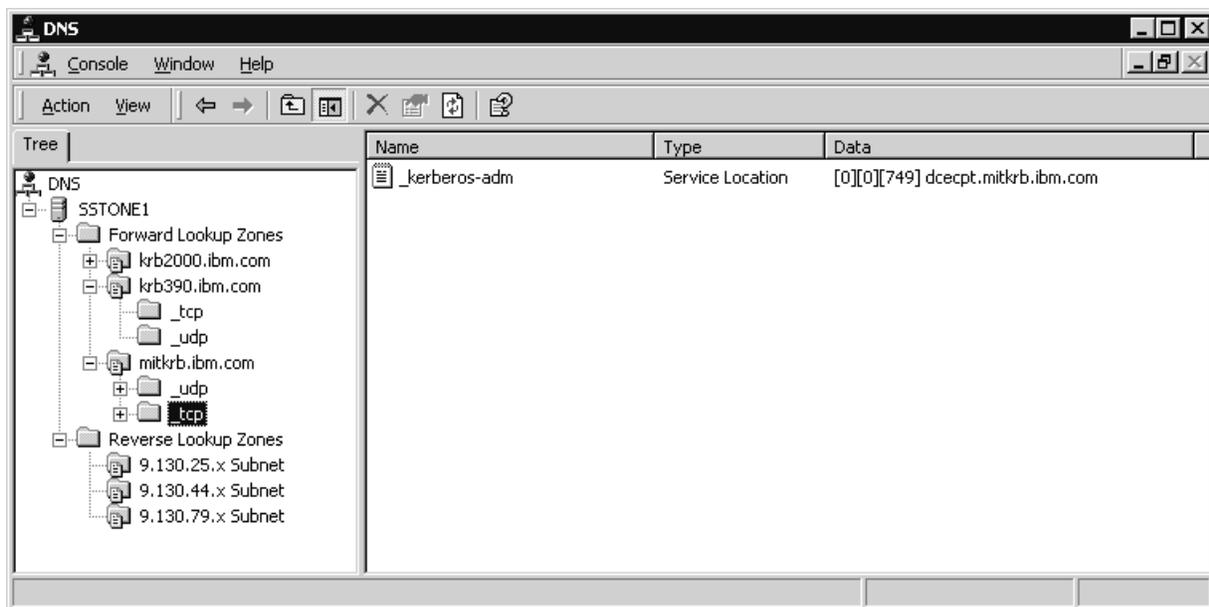
Figure 9. MITKRB.IBM.COM configuration - creating an SRV record using the TCP protocol

3. Create a TXT record to map host names in the **mitkrb.ibm.com** DNS domain to the MITKRB.IBM.COM Kerberos realm. This example uses the Windows 2000 DNS management console to create the TXT record.

Figure 10. MITKRB.IBM.COM configuration - creating a TXT record to map host names

4. Set up peer-to-peer trust relationships between the KRB390.IBM.COM realm and the MITKRB.IBM.COM and between the KRB2000.IBM.COM realm and the MITKRB.IBM.COM realm. This allows clients in one realm to access services in another realm.

5. The following RACF commands set up the z/OS side of the peer-to-peer trust relationship. Note that the password is case-sensitive on the RDEFINE REALM command but the realm name is converted to upper case.

```
RDEFINE REALM
    /.../KRB390.IBM.COM/krbtgt/MITKRB.IBM.COM
    KERB(PASSWORD(s3902mit))
RDEFINE REALM
    /.../MITKRB.IBM.COM/krbtgt/KRB390.IBM.COM
    KERB(PASSWORD(mit2s390))
```

6. Use the **kadmin** command to create the peer-to-peer trust relations on the MIT Kerberos side. This example uses the z/OS **kadmin** command to create the **krbtgt** principals in the MITKRB.IBM.COM Kerberos database.

```
DCESEC4:/home/susec4/> kadmin -p rwh/admin@MITKRB.IBM.COM
EUVF06147I Authenticating as rwh/admin@MITKRB.IBM.COM.
EUVF02033R Enter password:

kadmin>
addprinc -pw s3902mit krbtgt/MITKRB.IBM.COM@KRB390.IBM.COM
EUVF06122I Principal krbtgt/MITKRB.IBM.COM@KRB390.IBM.COM added.
kadmin>
addprinc -pw mit2s390 krbtgt/KRB390.IBM.COM@MITKRB.IBM.COM
EUVF06122I Principal krbtgt/KRB390.IBM.COM@MITKRB.IBM.COM added.
kadmin>
addprinc -pw w2k2mit krbtgt/MITKRB.IBM.COM@KRB2000.IBM.COM
EUVF06122I Principal krbtgt/MITKRB.IBM.COM@KRB2000.IBM.COM added.
kadmin>
addprinc -pw mit2w2k krbtgt/KRB2000.IBM.COM@MITKRB.IBM.COM
EUVF06122I Principal krbtgt/KRB2000.IBM.COM@MITKRB.IBM.COM added.
```

7. If you have not enabled DES3 encryption for the MIT KDC but you have enabled DES3 encryption for the z/OS KDC, you must disable DES3 encryption for cross-realm ticket-granting tickets issued for the MIT Kerberos realm.

```
RALTER REALM
    /.../KRB390.IBM.COM/krbtgt/MITKRB.IBM.COM
    KERB(ENCRYPT(NODESD NODES3))
```

8. Use the Windows 2000 Active Directory Domains and Trusts management console to set up the Windows 2000 side of the peer-to-peer trust relationships. Open the Properties dialog for the **krb2000.ibm.com** domain. The password specified for the "Domains trusted by this domain" entry must be the same as the password specified for the /.../MITKRB.IBM.COM/krbtgt/KRB2000.IBM.COM principal. The password specified for the "Domains that trust this domain" entry must be the same as the password specified for the /.../KRB2000.IBM.COM/krbtgt/MITKRB.IBM.COM principal.
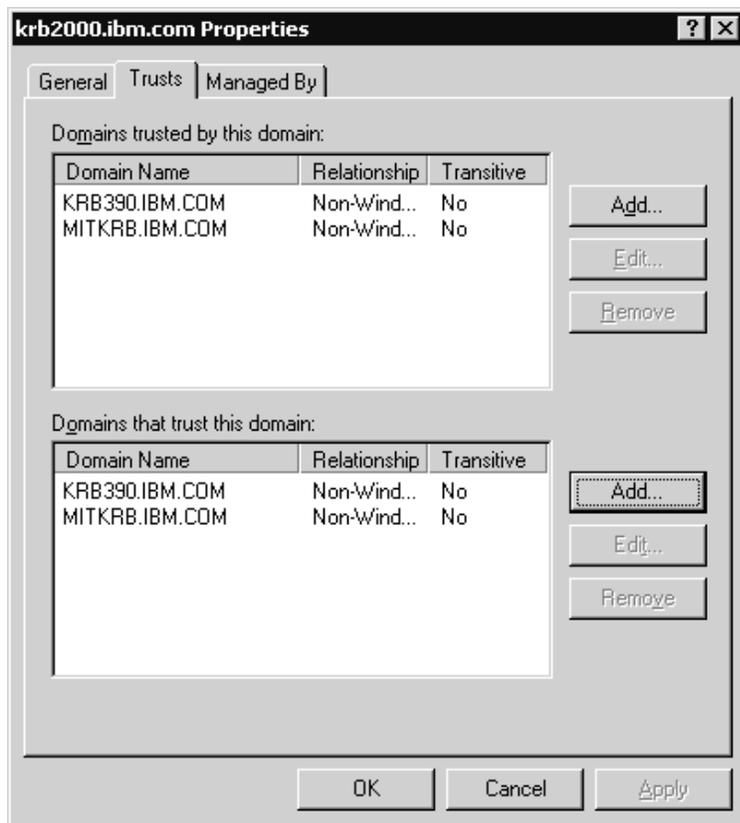
Figure 11. MITKRB.IBM.COM configuration - setting up the Windows 2000 side of the peer-to-peer trust relationships

9. Define the location of the MITKRB.IBM.COM KDC on each Windows 2000 client using the ksetup command. This command is shipped as part of the Windows 2000 Support Tools on the Windows 2000 CD.

   ```
   ksetup /addkdc MITKRB.IBM.COM dcecpt.mitkrb.ibm.com
   ```

Appendix B. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen-readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen-readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS: TSO/E Primer*, SA22-7787, *z/OS: TSO/E User's Guide*, SA22-7787, and *z/OS: ISPF User's Guide Volume I*, SC34-4822, for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

141

The following copyright and permission notice applies to portions of this information that were obtained
from the Massachusetts Institute of Technology.

```
/* Copyright 1985,1986,1987,1988,1990 by the Massachusetts Institute    */
/* of Technology.                                                        */
/* All Rights Reserved.                                                  */
/*                                                                       */
/* Copyright 1987,1995 by the Massachusetts Institute of Technology.     */
/* All Rights Reserved.                                                  */
/*                                                                       */
/* Copyright 1994 by the Massachusetts Institute of Technology.          */
/* Copyright (c)1994 CyberSAFE Corporation                               */
/* Copyright (c)1993 Open Computing Security Group                       */
/* Copyright (c)1990,1991 by the Massachusetts Institute of              */
/* Technology.                                                           */
/* All Rights Reserved.                                                  */
/*                                                                       */
/* Under U.S. law, this software may not be exported outside the US      */
/* without license from the U.S.Commerce department.                     */
/*                                                                       */
/* These routines form the library interface to the DES facilities.      */
/*                                                                       */
/* 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 M..I.T. not be used in advertising or publicity pertaining */
/* to distribution of the software without specific, written prior       */
/* permission.  Neither M.I.T., the Open Computing Security Group, nor    */
/* CyberSAFE Corporation make any representations about the suitability of*/
/* this software for any purpose.  It is provided "as is" without express */
/* or implied warranty.                                                  */
/*                                                                       */
* Copyright ((c)1990,1993,1994
*      The Regents of the University of California.  All rights reserved.
* This code is derived from software contributed to Berkeley by
* Margo Seltzer.
* 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.
*
* 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
```

```
/* 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.  Neither M.I.T., the Open Computing     */
/* Security Group, nor CyberSAFE Corporation make any representations*/
/* about the suitability of this software for any purpose.  It is    */
/* provided "as is" without express or implied warranty.             */

/*
 * Copyright 1990,1991 by the Massachusetts Institute of Technology.
 * Copyright 1996 by Lehman Brothers, 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 M.I.T.or Lehman Brothers not be used in advertising or
 * publicity pertaining to distribution of the software without
 * specific, written prior permission M.I.T.and Lehman Brothers
 * make no representations about the suitability of this software for
 * any purpose.  It is provided "as is" without express or implied
 * warranty.
 */
/* Copyright 1995 by Richard P. Basch.  All Rights Reserved.          */
/* Copyright 1995 by Lehman Brothers, 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 Richard P. Basch, Lehman Brothers and M.I.T.not be used */
/* in advertising or publicity pertaining to distribution of the software */
/* without specific, written prior permission.  Richard P. Basch,    */
/* Lehman Brothers and M.I.T. make no representations about the suitability*/
/* of this software for any purpose.  It is provided "as is" without  */
/* express or implied warranty.                                       */
```

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- BookManager
- IBM
- IBMLink
- Language Environment
- Library Reader
- MVS
- RACF

- Resource Link
- S/390
- z/OS
- z/OS.e

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

This glossary defines technical terms and abbreviations used in the documentation for z/OS Security Server Network Authentication Service. If you do not find the term you are looking for, refer to the index of the appropriate z/OS Security Server Network Authentication Service manual or view *IBM Glossary of Computing Terms*, available from:

`http://www.ibm.com/ibm/terminology`

A

Authentication.   Verifying the claimed identity of a principal.

Authentication header.   A record containing a ticket and an authenticator to be presented to a server as part of the authentication process.

Authentication path.   A sequence of intermediate realms transited in the authentication process when communicating from one realm to another.

Authenticator.   A record containing information that can be shown to have been recently generated using the session key known only by the client and the server.

Authorization.   The process of determining whether a client may use a service, which objects the client is allowed to access, and the type of access allowed for each.

C

Ciphertext.   The output of an encryption function. Encryption transforms plaintext into ciphertext.

Client.   A process that makes use of a network service on behalf of a user. Note that in many cases a server may itself be a client of some other server (for example, a print server may be a client of a file server).

Credentials.   A ticket plus the secret session key necessary to successfully use that ticket in an authentication exchange.

K

KDC.   Key Distribution Center, a network service that supplies tickets and temporary session keys; or an instance of that service or the host on which it runs. The KDC processes both initial ticket and ticket-granting ticket requests. The initial ticket portion is sometimes referred to as the Authentication Service (AS) while the ticket-granting portion is sometimes referred to as the Ticket Granting Service (TGS).

Kerberos.   This is the name given to the Massachusetts Institute of Technology (MIT) computing system authentication service, the protocol used by that service, and the programs used to implement the authentication service. The name comes from Greek mythology: Kerberos was the 3-headed dog guarding Hades.

P

Plaintext.   The input to an encryption function or the output of a decryption function. Decryption transforms ciphertext into plaintext.

Principal.   A uniquely named client or server instance that participates in a network communication.

Principal identifier.   The name used to uniquely identify each different principal.

S

Seal.   To encipher a record containing several fields in such a way that the fields cannot be individually replaced without either knowledge of the encryption key or leaving evidence of tampering.

Secret key.   An encryption key shared by a principal and the KDC, distributed outside the bounds of the system, with a long lifetime. In the case of a human user's principal, the secret key is derived from a password.

Server.   A particular principal that provides a resource to network clients.

Service.   A resource provided to network clients, often provided by more than one server.

Session key.   A temporary encryption key used between two principals, with a lifetime limited to the duration of a single login session.

Sub-session key.   A temporary encryption key used between two principals, selected and exchanged by the principals using the session key, and with a lifetime limited to the duration of a single association.

T

Ticket.   A record that helps a client authenticate itself to a server; it contains the client's identity, a session key, a timestamp, and other information, all sealed

using the server's secret key. It serves to authenticate a
client only when presented along with a fresh
authenticator.

Bibliography

This is the same bibliography that appears in *z/OS: Security Server Network Authentication Service Programming*. Not every document listed here is cited in both publications.

z/OS documents for Network Authentication Service

- *z/OS: Security Server Network Authentication Service Administration*, SC24-5926
- *z/OS: Security Server Network Authentication Service Programming*, SC24-5927

Other Security Server publications

Lightweight Directory Access Protocol (LDAP)

- *z/OS: Security Server LDAP Server Administration and Use*, SC24-5923
- *z/OS: Security Server LDAP Client Programming*, SC24-5924

Resource Access Control Facility (RACF)

- *z/OS: Security Server RACF Macros and Interfaces*, SA22-7682
- *z/OS: Security Server RACF Callable Services*, SA22-7691
- *z/OS: Security Server RACF Command Language Reference*, SA22-7687
- *z/OS: Security Server RACROUTE Macro Reference*, SA22-7692

MVS programming documents

- *z/OS: MVS Programming: Authorized Assembler Services, Volume 1 (ALESERV-DYNALLO)*, SA22-7609
- *z/OS: MVS Programming: Authorized Assembler Services, Volume 2 (ENFREQ-IXGWRITE)*, SA22-7610
- *z/OS: MVS Programming: Authorized Assembler Services, Volume 3 (LLACOPY-SDUMPX)*, SA22-7611
- *z/OS: MVS Programming: Authorized Assembler Services, Volume 4 (SETFRR-WTOR)*, SA22-7612

- *z/OS: MVS Programming: Sysplex Services Guide*, SA22-7617
- *z/OS: MVS Programming: Sysplex Services Reference*, SA22-7618

Other documents

- *z/OS: System Secure Sockets Layer Programming*, SC24-5901
- *z/OS: C/C++ Run-Time Library Reference*, SA22-7821

Bibliography

Index

A
about this book   xi
accessibility   139
administering Network Authentication Service   31
application programming interfaces   7
ASN.1 operations status codes   77
audit   33
authentication   3

B
bibliography   149

C
cache files   33
capath section of configuration profile   29
checksum types   26
code page 1047   25
commands   47
   kdestroy   60
   keytab   60
   kinit   61
   klist   63
   ksetup   65
configuration profile   25
   checksum types   26
   encryption types   26
   numeric values   26
   sections   26
      capath   29
      domain realm   29
      libdefaults   27
      realms   28
configuring the Network Authentication Service   9
conventions used in this book   xiii
crc32   26
creating SRV entries   131

D
database propagation, Kerberos   41
des-cbc-crc   26
des-cbc-md4   26
des-cbc-md5   26
des-hmac-sha1   26
des3-cbc-sha1   26
descbc   26
destroy a Kerberos credentials cache   60
disability   139
display contents of credentials cache or key table   63
domain realm section of configuration profile   29

E
encryption types   26
environment variables for the security runtime   19
environment variables for the security server   23

F
F SKRBKDC command   35

G
glossary   147
GSS_API Kerberos mechanism status codes   71
GSS-API status codes   79

H
hmac-sha1-des3   26

I
introduction to Network Authentication   3

K
KDC error codes   33
kdestroy command   60
Kerberos
   database propagation   41
Kerberos commands
   kdestroy   60
   keytab   60
   kinit   61
   klist   63
   ksetup   65
Kerberos commands messages   116
Kerberos runtime messages   99
Kerberos runtime status codes   83
keyboard   139
keytab command   60
kinit command   61
klist command   63
ksetup command   65

L
LDAP schema definitions   15
libdefaults section of configuration profile   27

M
manage a key table   60
manage service entries in LDAP directory for a
  realm   65
messages   99
   for Kerberos commands   116

Readers' Comments — We'd Like to Hear from You

z/OS
Security Server
Network Authentication Service
Administration

Publication No. SC24-5926-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you?   ☐ Yes   ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____   Address _____

Company or Organization _____

Phone No. _____

IBM ®
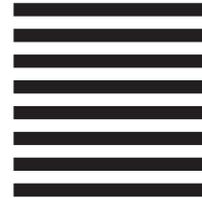
Program Number: 5694-A01, 5655-G52

Printed in U.S.A.