



Configuring AIX 5L for Kerberos Based Authentication Using Windows Kerberos Service

February 1, 2006

Ufuk Çelikkan
IBM Corporation

CONTENTS

CONTENTS	2
1 OVERVIEW	4
1.1 Loadable Authentication/Identification Mechanism	4
1.2 "registry" and "SYSTEM" Attributes	5
1.3 Kerberos	5
2 CONFIGURING KRB5A AGAINST WINDOWS SERVER KERBEROS SERVICE	6
2.1 Windows Server 2000 Kerberos Service	7
2.2 Windows Server 2003 Kerberos Service	13
3 KRB5A QUESTIONS AND TROUBLESHOOTING INFORMATION FOR WINDOWS SERVER	13
3.1 How do I Modify AIX Configuration for Kerberos Integrated Login	13
3.2 How do I Create an AIX User for Kerberos Integrated Login Using KRB5A	14
3.3 How do I Remove a Kerberos Authenticated User	14
3.4 How do I change the Password of a Kerberos Authenticated User	14
3.5 How do I Convert an AIX User to a Kerberos Authenticated User	15
3.6 What do I do if the Password is Forgotten	15
3.7 What is the Purpose of <i>auth_name</i> and <i>auth_domain</i> Attributes	15
3.8 Can a Kerberos-Authenticated User Become Authenticated Using Standard AIX Authentication	16
3.9 Do I Need to Set up Kerberos Server (KDC) on AIX When Using Windows Server 2000 Kerberos Service	16
3.10 AIX Does not Accept My Password	16
3.11 Cannot Log Into the System	17

3.12	How Can I Disable TGT Verification	18
3.13	Cannot Login due to Hostname Resolution and Fully Qualified Host Name Failure	18
3.14	Can I login to Two Different Realms From the Same Client	19
4	SOLARIS AND HP-UX	22
4.1	Solaris SEAM	22
4.2	HP-UX 11i v1 KDC 2.1	25
	REFERENCES	27

Figure 1:	Loadable identification and authentication framework.....	5
Figure 2:	User creation main panel.	8
Figure 3:	Password Panel.	9
Figure 4:	User Creation Confirmation Panel.	9
Figure 5:	Sample Output of Ktpass Command.	10
Figure 6:	Creation of user foo.....	11
Figure 7:	Confirmation panel for user foo.....	11
Figure 8:	Windows Server 2000 KDC Service Status.	17

1 Overview

This document describes the use of Kerberos as an alternative authentication mechanism to AIX® using Windows® 2000/2003 Server Kerberos Service (We shall use the terms AIX and AIX 5L interchangeably.). Authentication applications on AIX do not require any change to alternatively perform Kerberos authentication as it is woven into the fabric of the AIX security subsystem. By utilizing the loadable identification and authentication framework of AIX, the system directs authentication requests to use Kerberos instead of standard UNIX® authentication.

1.1 Loadable Authentication/Identification Mechanism

AIX's loadable identification and authentication framework hides the details related to authentication and identification from other parts of the operating system. The framework defines a common interface and modules that implement this interface can be plugged into the framework to provide support to various technologies used for identification and/or authentication such as Kerberos or LDAP.

Modules created for the framework can support authentication and/or database functionality. Authentication modules are required to implement authentication and include password verification and modification functions. Database modules are required to implement account management interfaces and thereby support storage, retrieval and modification of user/group account information. An authentication module and a database module can be combined together into a compound module. The authentication half of the compound load module provides authentication services and the database side provides AIX identification services. Some modules implement both interfaces and can be used as either the authentication or database side of a compound load module or as stand-alone module.

The following figure gives a simplified view of the loadable identification and authentication framework of AIX. It demonstrates the authentication flow of the su command.

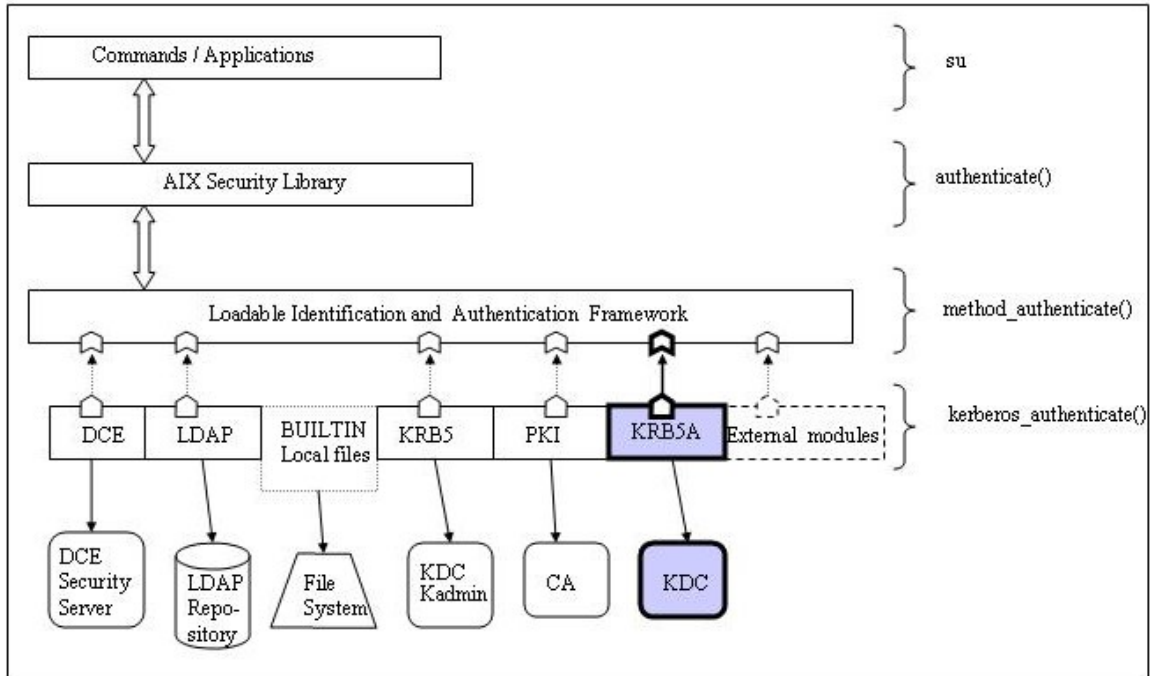


Figure 1: Loadable identification and authentication framework.

1.2 "registry" and "SYSTEM" Attributes

AIX security subsystem directs authentication and identification requests to the proper module by using the “**registry**” and “**SYSTEM**” attributes. The registry attribute specifies where the user or group identification information is administrated and the SYSTEM attribute controls which methods will be used and how the methods result will affect the overall authentication. Every user on AIX must have a value for the registry and SYSTEM attribute. Groups only have registry values.

By default, users and groups are defined in the "files" registry. This means that user and group information is stored in the flat-ASCII files. User and group definitions can also be stored in LDAP and managed through **LDAP** module.

The SYSTEM attribute allows the system administrator to specify to a fine granularity which method (or methods) a user must successfully authenticate to in order to gain access to the system. For instance, when SYSTEM attribute is set to “SYSTEM=KRB5Afiles OR compat”, the AIX host will first try a Kerberos flow for authentication and if it fails then it will try standard AIX authentication. A brief introduction to SYSTEM attribute values can be found in [8].

1.3 Kerberos

Kerberos is a network authentication service that originated at MIT as part of Project Athena [1]. It provides a means of verifying the identities of principals on an open,

unprotected network under the assumption that packets traveling along the network can be read, modified, and inserted at will. A Kerberos principal is a unique identity that uses Kerberos authentication services. Kerberos verifies identities without relying on authentication by the host operating system, without basing trust on host addresses and without requiring physical security of all the hosts on the network. Refer to [1] and [2] for a detailed discussion of subject matter.

Kerberos tickets are credentials that prove your identity. There are two types of tickets, a ticket granting ticket (TGT) and a service ticket. The TGT serves to validate the requested identity and is obtained after some form of authentication. Once you have a TGT you may then use your TGT to request service tickets for specific services. The service ticket grants you the permission to use the services. In summary, your TGT proves to the Kerberos server that you are who you say you are and your service ticket is your secure introduction to the service. This two-ticket method provides the "trusted third-party" security of Kerberos

The trusted "third-party" or intermediary in Kerberos is called a KDC- Key Distribution Center. It issues all the Kerberos tickets to the clients. Each Kerberos administrative domain or realm must have a KDC.

Network Authentication Service is IBM's implementation of MIT Kerberos Version 5. The terms "Kerberos" and "Network Authentication Service" shall be used interchangeably in this paper.

2 Configuring KRB5A Against Windows Server Kerberos Service

Note: The KRB5A Authentication Load Module is only supported in AIX 5L™ V5.2 ML01 and later.

AIX provides the authentication only Kerberos module **KRB5A** for use in the authentication half of a compound load module. The **KRB5A** load module enables Kerberos as an alternative authentication mechanism against Windows 2000/2003 Server Kerberos Service. AIX also provides a pseudo load module called BUILTIN to provide access to the security library's functionality through the loadable module paradigm. The idea behind BUILTIN load module is to combine it with authentication only load modules to provide the database half of the compound load module. BUILTIN module provides legacy user and group storage and access i.e. file system. **LDAP** load module could also be used as the database side, to provide a compound load module.

Unlike the other Kerberos module **KRB5**, **KRB5A** does not provide Kerberos principal management. For more information on Kerberos authentication using KRB5 refer to [8]. The KRB5A load module is tailored to an environment where Kerberos principals are stored on a non-AIX system and cannot be managed from AIX by using the Kerberos database interface kadmin. Kerberos principal management must be performed separately

by using Kerberos principal-management tools. These tools may be part of a Kerberos product developed by software vendors or they may be integrated into the OS such as the case in Windows 2000.

2.1 Windows Server 2000 Kerberos Service

Windows 2000 Kerberos Service and Network Authentication Service client are interoperable at the Kerberos protocol level (RFC1510). AIX clients must use KRB5A since Windows Server 2000 does not support the kadmin interface. Principal management must be done on the Windows system using Windows tools. Perform the following steps to configure AIX client for Kerberos based authentication against Windows Server 2000 Kerberos Service.

1. Setup Windows Server 2000. Please refer to appropriate Microsoft® documentation on how to configure a Microsoft Active Directory Server.
2. If Network Authentication Service client is not installed on the AIX client then install the **krb5.client.rte** file set from the Expansion Pack.
3. Use the **config.krb5** command to configure an AIX Kerberos client. Configuring the client requires Kerberos Server information. Use **config.krb5** command with the following configuration information:

realm : Windows Active Directory Domain name
domain : Domain name of the machine hosting the Active Directory server
KDC : The host name of the Windows server
server : The host name of the Windows server

Note that the realm name is derived from the Windows Active Directory domain name. Server information is not meaningful and will not be used by the Network Authentication Service clients, as Active Directory does not support the kadmin interface. Refer to 3] for details and usage of **config.krb5** command.

Use the **config.krb5** command as shown in the following example:

```
# config.krb5 -C -r MYREALM -d austin.ibm.com -c w2k.austin.ibm.com -s  
w2k.austin.ibm.com
```

4. Windows supports DES-CBC-MD5 and DES-CBC-CRC encryption types. Change the **krb5.conf** file to contain information similar to the following:

```
[libdefaults]  
    default_realm = MYREALM  
    default_keytab_name = FILE:/etc/krb5/krb5.keytab  
    default_tkt_encypes = des-cbc-crc des-cbc-md5  
    default_tgs_encypes = des-cbc-crc des-cbc-md5
```

5. Add the following stanzas in the **methods.cfg** file:

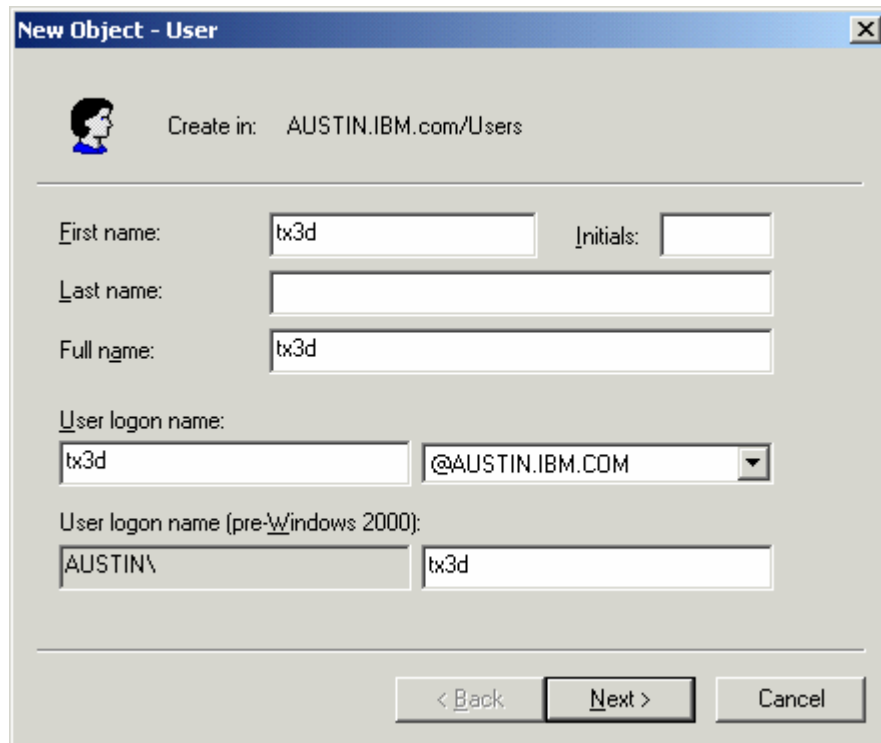
```
KRB5A:
    program = /usr/lib/security/KRB5A
    options = authonly
KRB5Afiles:
    options = db=BUILTIN,auth=KRB5A
```

6. Create a host principal. Unlike Network Authentication Service principal names, Windows account names are not multi part. Because of this it is not possible to directly create an account of the name host/<fully qualified host name>. Such a principal instance is created through service principal name mappings. In this case, an account is created corresponding to the host principal and a principal name mapping is added.

On the Active Directory server, do the following:

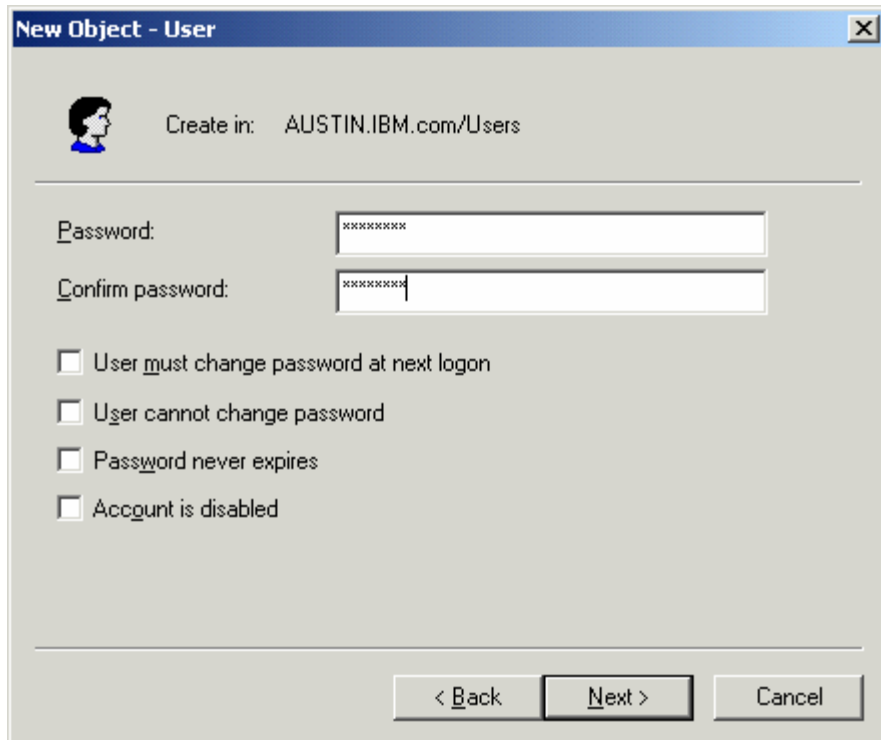
Use the Active Directory Management tool to create a new user account corresponding to the AIX client machine *tx3d.austin.ibm.com*:

- A. Select The Users folder.
- B. Right-click with the mouse and select New.
- C. Choose user.
- D. Type the name *tx3d*.



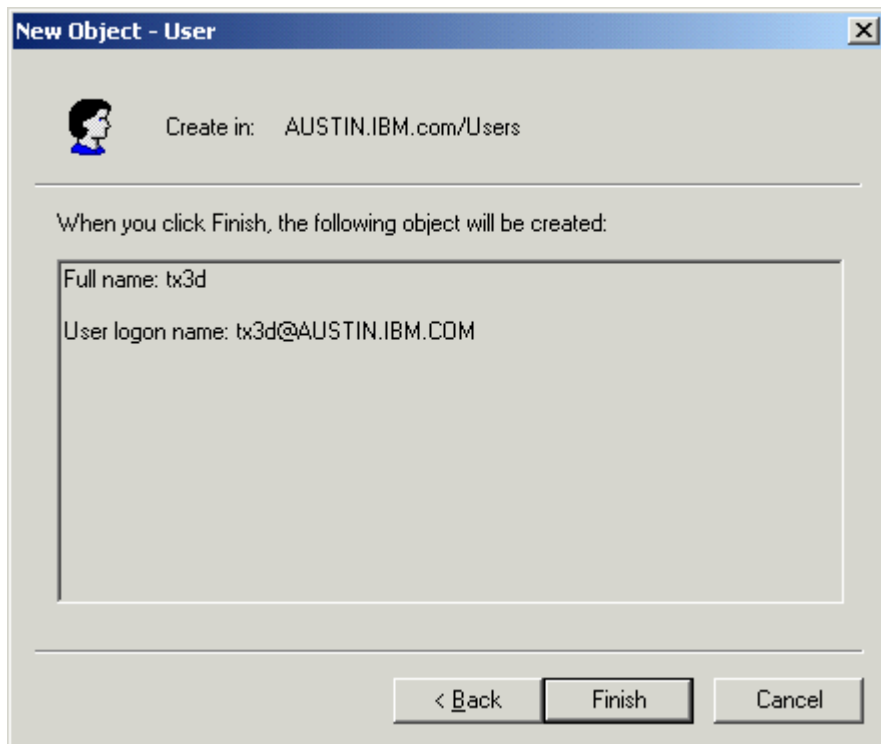
The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: AUSTIN.IBM.com/Users'. Below this, there are several input fields: 'First name' with 'tx3d', 'Initials' (empty), 'Last name' (empty), 'Full name' with 'tx3d', 'User logon name' with 'tx3d' and a dropdown menu showing '@AUSTIN.IBM.COM', and 'User logon name (pre-Windows 2000)' with 'AUSTIN\' and 'tx3d'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 2: User creation main panel.



The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It features a user icon and the text "Create in: AUSTIN.IBM.com/Users". Below this, there are two password input fields: "Password:" and "Confirm password:", both containing masked characters (asterisks). Underneath the password fields are four unchecked checkboxes with the following labels: "User must change password at next logon", "User cannot change password", "Password never expires", and "Account is disabled". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 3: Password Panel.

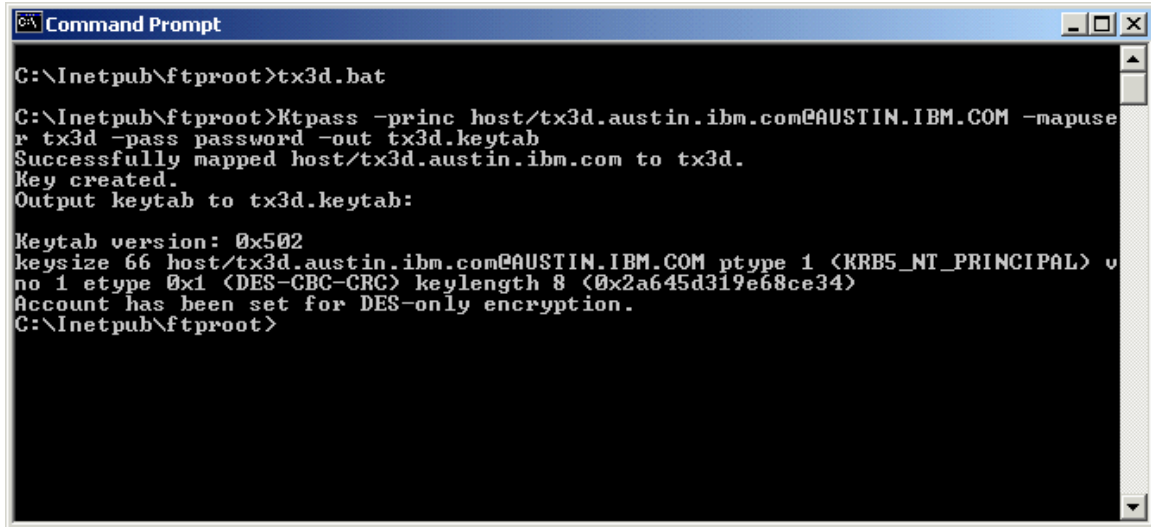


The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It features a user icon and the text "Create in: AUSTIN.IBM.com/Users". Below this, the text "When you click Finish, the following object will be created:" is displayed. A large text box contains the following information: "Full name: tx3d" and "User logon name: tx3d@AUSTIN.IBM.COM". At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

Figure 4: User Creation Confirmation Panel.

7. Use the **Ktpass** command from the command line on the Windows Server 2000 machine to create tx3d.keytab file and set up the account for the AIX host as follows:

```
Ktpass -princ host/tx3d.austin.ibm.com@MYREALM -mapuser tx3d -pass password -out tx3d.keytab
```



```
Command Prompt
C:\Inetpub\ftproot>tx3d.bat
C:\Inetpub\ftproot>Ktpass -princ host/tx3d.austin.ibm.com@AUSTIN.IBM.COM -mapuser tx3d -pass password -out tx3d.keytab
Successfully mapped host/tx3d.austin.ibm.com to tx3d.
Key created.
Output keytab to tx3d.keytab:

Keytab version: 0x502
keysize 66 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM ptype 1 <KRB5_NT_PRINCIPAL> v
no 1 etype 0x1 <DES-CBC-CRC> keylength 8 <0x2a645d319e68ce34>
Account has been set for DES-only encryption.
C:\Inetpub\ftproot>
```

Figure 5: Sample Output of Ktpass Command.

8. Copy tx3d.keytab file to the AIX host system.

Merge tx3d.keytab file into the **/etc/krb5/krb5.keytab** file on the AIX system as follows:

```
$ ktutil
ktutil: rkt tx3d.keytab
ktutil: wkt /etc/krb5/krb5.keytab
ktutil: q
```

9. Create Windows domain accounts using the Active Directory user management tools.

The screenshot shows a dialog box titled "New Object - User" with a close button (X) in the top right corner. Below the title bar is a user icon and the text "Create in: AUSTIN.IBM.com/Users". The main area contains several input fields: "First name:" with the value "foo", "Initials:" (empty), "Last name:" (empty), "Full name:" with the value "foo", "User logon name:" with the value "foo" and a dropdown menu showing "@AUSTIN.IBM.COM", and "User logon name (pre-Windows 2000):" with the value "AUSTIN\" and a sub-field with the value "foo". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Figure 6: Creation of user foo.

The screenshot shows the same dialog box, but now it is in a confirmation state. The text "When you click Finish, the following object will be created:" is displayed above a large text box. The text box contains the following information: "Full name: foo" and "User logon name: foo@AUSTIN.IBM.COM". At the bottom are three buttons: "< Back", "Finish", and "Cancel".

Figure 7: Confirmation panel for user foo.

10. Create AIX accounts corresponding to the Windows domain accounts as follows such that the login process will use Kerberos authentication:

```
mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles foo
```

11. Login to the AIX system through telnet to verify the configuration.

Example: Sample Kerberos integrated login session using KRB5A

```
telnet tx3d
Trying...
Connected to tx3d.austin.ibm.com.
Escape character is '^]'.

telnet (tx3d.austin.ibm.com)
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2004.
login: foo
foo's Password:
*****
*
*
* Welcome to AIX Version 5.3!
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****
[tx3d] $ echo $AUTHSTATE
KRB5Afiles
[tx3d] $ /usr/krb5/bin/klist
Ticket cache: FILE:/var/krb5/security/creds/krb5cc_foo@AUSTIN.IBM.COM_203
Default principal: foo@AUSTIN.IBM.COM

Valid starting Expires Service principal
04/29/05 14:37:28 04/30/05 00:39:22 krbtgt/AUSTIN.IBM.COM@AUSTIN.IBM.COM
Renew until 04/30/05 14:37:28
04/29/05 14:39:22 04/30/05 00:39:22 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
[tx3d] $
```

Example: Sample Kerberos based su using KRB5A

```
$ id
uid=100(guest) gid=100(usr)
$ su - foo
foo's Password:
[tx3d] $ id
uid=203(foo) gid=1(staff)
[tx3d] $ echo $AUTHSTATE
KRB5Afiles
[tx3d] $ /usr/krb5/bin/klist
Ticket cache: FILE:/var/krb5/security/creds/krb5cc_foo@AUSTIN.IBM.COM_203
Default principal: foo@AUSTIN.IBM.COM

Valid starting Expires Service principal
```

```
04/29/05 14:40:07 04/30/05 00:42:01 krbtgt/AUSTIN.IBM.COM@AUSTIN.IBM.COM
Renew until 04/30/05 14:40:07
04/29/05 14:42:01 04/30/05 00:42:01 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
[tx3d] $
```

2.2 Windows Server 2003 Kerberos Service

Configuration of an AIX client against a Windows Server 2003 can use the same steps documented above for Windows Server 2000. Windows Server 2003 with March 2005 security updates was used to verify AIX client authentication against Windows Server 2003 Kerberos Service. One difference between Windows Server 2003 and Windows Server 2000 is that Network Authentication Service **kpasswd** client utility cannot change the password of a Kerberos principal on Windows Server 2003 Active Directory. Consequently after a successful login to AIX machine using Kerberos, the user cannot change the password on the Windows Server 2003.

3 KRB5A Questions and Troubleshooting Information for Windows Server

The following section provides answers to **KRB5A** Authentication Load Module questions and troubleshooting information. Before performing any problem determination and troubleshooting make sure all the servers and daemons are running.

KRB5A load module uses the **syslog** subsystem to write its error and debug information. Turn on **syslog** logging before carrying out any problem determination for KRB5A based logins. Please refer to AIX system reference documentation how to turn on **syslog** debugging.

3.1 How do I Modify AIX Configuration for Kerberos Integrated Login

To enable Kerberos integrated login, modify the **/usr/lib/security/methods.cfg** file. The compound load-module entry must be added to the **methods.cfg** file. The authentication side will be **KRB5A**. The database side can be chosen as either **BUILTIN** or **LDAP**. For example, if you choose local file system as the AIX user account repository, then modify the **/usr/lib/security/methods.cfg** file as follows:

Example: Local file system is chosen as the AIX user account repository.

```
KRB5A:
    program = /usr/lib/security/KRB5A
    options=authonly
```

```
KRB5Afiles:
```

```
options = db=BUILTIN,auth=KRB5A
```

If LDAP is chosen as the AIX user account repository then add the following:

```
KRB5A:  
  program = /usr/lib/security/KRB5A  
  options=authonly
```

```
KRB5ALDAP:  
  options = auth=KRB5A,db=LDAP
```

Make sure **mksecdap** command is invoked before adding KRB5ALDAP into **/usr/lib/security/methods.cfg** file. Refer to [8][9] and [10] for information on how to use **mksecdap** to configuring LDAP. Refer to [7] for more information on **/usr/lib/security/methods.cfg** file.

3.2 How do I Create an AIX User for Kerberos Integrated Login Using KRB5A

To create an AIX user for Kerberos integrated login with the KRB5A load module, use the **mkuser** command as follows:

```
mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles foo
```

This only creates the user on AIX. One must also create an account for the user on Windows Server Active Directory corresponding to the AIX account. On Windows Server Active Directory, creating a user account implicitly creates the principals. For example, if you create a user account named `foo` on Active Directory then the principal `foo@MYREALM` associated with the `foo` user is also created. For information on creating users on Active Directory, see the Active Directory user management documentation.

3.3 How do I Remove a Kerberos Authenticated User

rmuser removes users only from AIX. The user must also be removed from the Windows Server Active Directory using the appropriate user management tools on Windows Server.

```
#rmuser -R KRB5Afiles foo
```

3.4 How do I change the Password of a Kerberos Authenticated User

A user can change the password by invoking `passwd` command.

```
$ passwd -R KRB5Afiles foo
```

This changes the password of the Kerberos principal `foo@MYREALM` on the Kerberos Server if the KDC supports `kpasswd`. Refer to Sections 2.2 and 3 for information on Kerberos server's that do not support password change from an AIX client.

3.5 How do I Convert an AIX User to a Kerberos Authenticated User

The first thing to do is, to check if the client system is configured for authentication against Windows Server Active Directory. If the system is configured then verify that the user has an account on Windows Server Active Directory. If the user has an account, then setting the `SYSTEM` and registry attributes using `chuser` command simply converts the user into a Kerberos authenticated user, as shown in the following example:

```
chuser registry=KRB5Afiles SYSTEM=KRB5Afiles foo
```

If the user does not have an account on Active Directory then create an account on Active Directory and set the `SYSTEM` and registry attributes using `chuser` command. The Active Directory account may or may not have the same AIX user name. If a different name is chosen, then use the `auth_name` attribute to map to the Active Directory name. For example, to map the AIX user name `chris` to user `christopher` on Active Directory, type the following:

```
chuser registry=KRB5Afiles SYSTEM=KRB5Afiles auth_name=Christopher chris
```

3.6 What do I do if the Password is Forgotten

On AIX, the root user cannot set the password of an Active Directory Kerberos principal. For this reason the password must be changed by the Active Directory administrator.

3.7 What is the Purpose of *auth_name* and *auth_domain* Attributes

The `auth_name` and `auth_domain` attributes are used to map AIX user names into Kerberos principal names on the KDC. For example, if the AIX user `chris`, has the attributes `auth_name=christopher` and `auth_domain=SOMEREALEM`, then the Kerberos principal name would be `christopher@SOMEREALEM`. By using `auth_domain`, the requests are sent to `SOMEREALEM` realm name instead of the default realm name. This allows the user `chris` to authenticate to the `SOMEREALEM` realm instead of to the `MYREALM` realm. In this example, the `krb5.conf` file would also need to be modified to include the realm name `SOMEREALEM` in order for this to work.

These attributes are optional. If the AIX system is configured to support user names greater than 8-character long there may not be a need to use `auth_name` attribute.

3.8 Can a Kerberos-Authenticated User Become Authenticated Using Standard AIX Authentication

The answer is yes. Perform the following actions to authenticate the Kerberos-authenticated user using AIX authentication:

1. Set the AIX password (`/etc/security/passwd`) using the `passwd` command, as follows:

```
# passwd -R files foo
```

2. Change the **SYSTEM** and **registry** attribute of the user, as follows:

```
# chuser -R KRB5Afiles registry=files SYSTEM=compat foo.
```

This changes authentication from Kerberos to `compat` which uses `crypt()`. Next time a login is attempted by `foo`, the local password from `/etc/security/passwd` file will be used. If you want to instead use `crypt` authentication as a backup mechanism, the **SYSTEM** attribute could be changed as follows to allow the user to authenticate locally when Kerberos authentication fails:

```
# chuser -R KRB5Afiles SYSTEM="KRB5Afiles or compat" foo.
```

3.9 Do I Need to Set up Kerberos Server (KDC) on AIX When Using Windows Server 2000 Kerberos Service

No, the KDC is not necessary on the AIX client because users are authenticating against an Active Directory KDC. Therefore, there is no need to configure the KDC on AIX. If you plan to use AIX Network Authentication Service KDC as the Kerberos server for some other purpose, then the Kerberos server must be configured.

3.10 AIX Does not Accept My Password

Check that the client is communicating with the Windows 2000 Active Directory Server.

Check that the password meets the requirements of both AIX and Windows Server 2000 Active Directory. AIX enforces password policy independent of Windows Server 2000 Active Directory. The password must comply both. You may change the password rules on AIX by properly modifying the password policy related attributes. By doing this you may effectively bypass AIX password composition rules and rely on the decision made by Windows Server 2000 Active Directory Server. Refer to AIX documentation for how to change password policy rules on AIX.

Password change is not possible for Windows Server 2003 Kerberos Service.

3.11 Cannot Log Into the System

If you cannot log into the system, check the followings:

- Verify that the KDC is up and running. On Windows systems, do the following:
 1. In the Control Panel, double-click the Administrative Tools icon
 2. Double-click the Services icon
 3. Verify that the Kerberos Key Distribution Center is in the started state

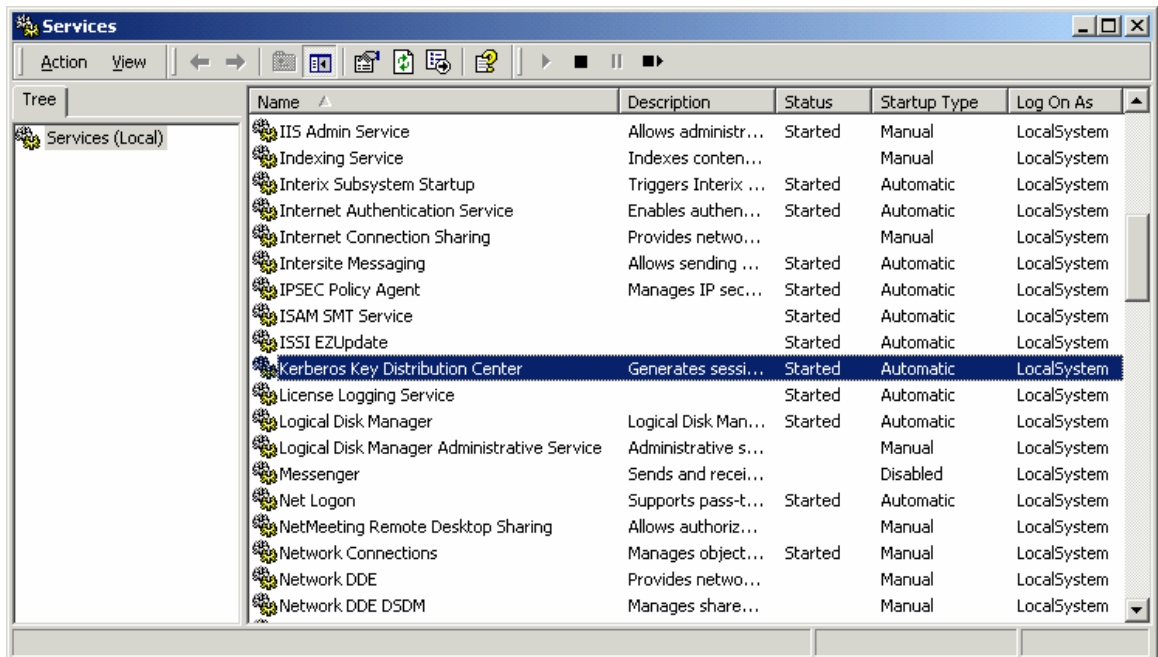


Figure 8: Windows Server 2000 KDC Service Status.

- On AIX systems, verify that the `/etc/krb5/krb5.conf` file points to the correct KDC, and has valid parameters.
- On AIX systems, verify that client `keytab` file contains the host key. For example, assume you have the `/etc/krb5/krb5.keytab` default `keytab` file. Type the following:

```
$ ktutil
ktutil: rkt /etc/krb5/krb5.keytab
ktutil: l

slot    KVNO    Principal
-----
1       4      host/krbtest.xyz.com@MYREALM
```

ktutil: q

- Verify that the kvno in the keytab file matches to the one obtained using **Ktpass**.
- Verify that, if **auth_name** and **auth_domain** attributes are set, they refer to a valid principal name on the AD KDC.
- Verify that the **SYSTEM** attribute is set for Kerberos login (**KRB5Afiles** or **KRB5ALDAP**).
- Verify that password is not expired.

3.12 How Can I Disable TGT Verification

The KRB5A authentication module uses the **host/Host_Name** to verify if a TGT is genuine or not. Network Authentication Service uses the default keytab file specified in **/etc/krb5/krb5.conf** file (unless the keytab location is overwritten) when it needs to access the keys. After securely transferring the keytab file containing the host principal keys from KDC server to the client machine, the keytab files are merged. The TGT verification could be disabled by specifying an option in the **/usr/lib/security/methods.cfg** file under the KRB5A stanza as follows:

```
KRB5A:
    program = /usr/lib/security/KRB5A
    options = tgt_verify=no
KRB5Afiles:
    options = db=BUILTIN,auth=KRB5A
```

The possible values for **tgt_verify** are **no** or **false** for disabling, and **yes** or **true** for enabling. By default, the TGT verification is enabled. When **tgt_verify** is set to **no**, TGT verification will not be done. Consequently, there is no need to transfer the keys of host principal. This only eliminates the need of the **keytab** file for authentication purposes when KRB5A module is used. Many other Kerberized applications may still require the keytab file for host and service principals.

3.13 Cannot Login due to Hostname Resolution and Fully Qualified Host Name Failure

TGT verification requires the creation of principal **host/<host_name>** on the KDC where **host_name** is the fully qualified host name of the client where authentication is performed. The client system requests a service ticket using the host principal name **host/<host_name>**. In certain configurations, the client machine is unable to obtain the fully qualified hostname. Instead of a full name, it gets a short name. This causes a mismatch to occur and TGT verification failure results in login failure. For instance, if **/etc/hosts** has only the short name and **/etc/netsvc.conf** file specifies **hosts=local,bind** then the name resolution returns the shortname.

Perform one of the following actions to correct problems due to name resolution:

1. Modify the name resolution so that fully qualified host name is returned. This can be done by changing the order in `/etc/netsvc.conf`. `netsvc.conf` specifies the sequential order for resolving host names and aliases. In the following example the resolver first uses the BIND service to resolve host name, then `/etc/hosts` file if BIND fails. If both methods fail then it consults to nis.

Example: `hosts=bind,local,nis`

If `local` has to be the first method used in search order then change the short name (i.e. `myhost`) in `/etc/hosts` file into a fully qualified host name (`myhost.austin.ibm.com`).

2. If TGT validation is not needed, disable this option. Refer to the Section “How Can I Disable TGT Verification” for how to do this.

3.14 Can I login to Two Different Realms From the Same Client

Yes. This requires configuration of the two realms and modification of `/etc/krb5/krb5.conf` file on the client. When login name is prompted during the login session, enter the full principal name including the realm name. In the next example we use a Solaris SEAM Kerberos server and a HP-UX 11i Kerberos server to show how to achieve this. Please refer to Section 4.1 and 4.2 for how to configure authentication using Solaris and HP-UX Kerberos servers.

Note: Solaris SEAM and HP-UX KDC are used only for demonstration purposes. Kerberos integrated login against Solaris SEAM and HP-UX KDC are not supported configurations.

The machine and realm information is as follows:

HP-UX 11i:

Machine name: *hpsys.austin.ibm.com*

Realm Name : *HPSYS.AUSTIN.IBM.COM*

Sun Solaris 9:

Machine name: *sunsys.austin.ibm.com*

Realm Name : *AUSTIN.IBM.COM*

1. Set up Solaris SEAM and HP-UX Kerberos servers as described in Sections 4.1 and 4.2. While creating principals choose the same name (i.e. `krbuser`) but different passwords. This makes the example more interesting.
2. Merge the host principals from two realms using the `ktutil` tool. The keytab file should look similar to the following after the merge.

```

[tx3d] # ktutil
ktutil: rkt krb5.keytab
ktutil: l
slot   KVNO   Principal
-----
      1      2 host/tx3d.austin.ibm.com@HPSYS.AUSTIN.IBM.COM
      2      3 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
ktutil:

```

3. On the AIX client machine modify **/etc/krb5/krb5.conf** file such that both realms are defined .

Example: Sample krb5.conf file with two realms.

```

[realms]
  AUSTIN.IBM.COM = {
    kdc = sunsys.austin.ibm.com:88
    admin_server = sunsys.austin.ibm.com:749
    default_domain = austin.ibm.com
  }
  HPSYS.AUSTIN.IBM.COM = {
    kdc = hpsys.austin.ibm.com:88
    admin_server = hpsys.austin.ibm.com:749
    default_domain = austin.ibm.com
  }

[domain_realm]
  .austin.ibm.com = AUSTIN.IBM.COM
  tx3d.austin.ibm.com = AUSTIN.IBM.COM

```

4. Create a user on the AIX client with the same name as the Kerberos principal.

```
mkuser -R KRB5Afiles SYSTEM=KRB5Afiles registry=KRB5Afiles krbuser
```

To login HPSYS.AUSTIN.IBM.COM domain enter krbuser@HPSYS.AUSTIN.IBM.COM as the user name at the login prompt.

Example: Kerberos based login to HPSYS.AUSTIN.IBM.COM realm

```

telnet tx3d
Trying...
Connected to tx3d.austin.ibm.com.
Escape character is '^]'.

telnet (tx3d.austin.ibm.com)

AIX Version 5
(C) Copyrights by IBM and by others 1982, 2004.
login: krbuser@HPSYS.AUSTIN.IBM.COM
krbuser@HPSYS.AUSTIN.IBM.COM's Password:
*****
*
*
* Welcome to AIX Version 5.3!
*

```

```

*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****

```

Last login: Fri Apr 29 18:14:12 CDT 2005 on /dev/pts/0 from localhost

```

[tx3d] $ id
uid=202(krbuser) gid=1(staff)
[tx3d] $ /usr/krb5/bin/klist
Ticket cache:
FILE:/var/krb5/security/creds/krb5cc_krbuser@HPSYS.AUSTIN.IBM.COM_202
Default principal: krbuser@HPSYS.AUSTIN.IBM.COM

Valid starting      Expires            Service principal
04/29/05 18:17:47  04/30/05 18:15:44  krbtgt/HPSYS.AUSTIN.IBM.COM@HPSYS.AUSTIN.IBM.COM
04/29/05 18:17:47  04/30/05 18:15:44  host/tx3d.austin.ibm.com@HPSYS.AUSTIN.IBM.COM
[tx3d] $

```

To login AUSTIN.IBM.COM domain enter `krbuser@AUSTIN.IBM.COM` as the user name.

Example: Kerberos based login to AUSTIN.IBM.COM realm

```

tn tx3d
Trying...
Connected to tx3d.austin.ibm.com.
Escape character is '^T'.

```

```
telnet (tx3d.austin.ibm.com)
```

```

AIX Version 5
(C) Copyrights by IBM and by others 1982, 2004.
login: krbuser@AUSTIN.IBM.COM
krbuser@AUSTIN.IBM.COM's Password:
*****
*
*
* Welcome to AIX Version 5.3!
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****

```

Last login: Fri Apr 29 18:15:44 CDT 2005 on /dev/pts/0

```

[tx3d] $ id
uid=202(krbuser) gid=1(staff)
[tx3d] $ /usr/krb5/bin/klist
Ticket cache: FILE:/var/krb5/security/creds/krb5cc_krbuser@AUSTIN.IBM.COM_202
Default principal: krbuser@AUSTIN.IBM.COM

Valid starting      Expires            Service principal
04/29/05 18:15:35  04/30/05 02:15:35  krbtgt/AUSTIN.IBM.COM@AUSTIN.IBM.COM
Renew until 04/30/05 18:17:18

```

If the user name is entered without realm information then default realm will be used. Default realm is specified in `/etc/krb5/krb5.conf` file.

4 Solaris and HP-UX

The following Sections discuss the configuration and possible issues encountered when attempting to use an AIX Network Authentication Service client against Solaris SEAM and HP-UX KDC's using KRB5A.

Note: The steps given for Solaris SEAM and HP-UX are information purposes only. The configurations that involve AIX Kerberos integrated login against Solaris SEAM and HP-UX are not supported.

4.1 Solaris SEAM

Sun Enterprise Authentication Mechanism (SEAM) is Sun's implementation of MIT Kerberos V5 protocol. Solaris SEAM KDC and AIX Network Authentication Service client are interoperable at the Kerberos protocol level (RFC1510). However, Solaris kadmind daemon interface is incompatible with the Network Authentication Service clients, so one cannot use the kadmin command (or kadm5_*** API's) to administer a Solaris-based Kerberos database. Solaris kadmind daemon interface is also incompatible with MIT-based clients. AIX clients can use KRB5A to authenticate against SEAM. However, principal management must be done on the Solaris system using Solaris tools. The password change protocol between Solaris SEAM Kerberos servers and Network Authentication Service clients is incompatible. Changing the password of a principal will result in failure.

Solaris version 9 is used in the following example.

```
# uname -a
SunOS sunsys 5.9 Generic_118558-05 sun4u sparc SUNW,Ultra-5_10
#
```

1. Setup Solaris SEAM. Refer to appropriate Solaris documentation on how to configure SEAM.
2. If Network Authentication Service client is not installed then install the **krb5.client.rte** fileset on the AIX client machine from the Expansion Pack.
3. Use the **config.krb5** command to configure an AIX Kerberos client. Configuring the client requires Kerberos KDC information. Use **config.krb5** command with the following options:

realm	Solaris Kerberos realm name	: <i>AUSTIN.IBM.COM</i>
domain	domain name of the machine hosting Kerberos servers	: <i>austin.ibm.com</i>
KDC	The host name Solaris system hosting the KDC	: <i>sunsys.austin.ibm.com</i>
server	The host name of Solaris system hosting kadmind daemon. This is usually same as the KDC server.	: <i>sunsys.austin.ibm.com</i>

server information is not meaningful since Solaris kadmind daemon does not interoperate with Network Authentication Service clients.

Use the **config.krb5** command as shown in the following example to configure AIX client:

```
config.krb5 -C -r AUSTIN.IBM.COM -d austin.ibm.com -c sunsys.austin.ibm.com -s sunsys.austin.ibm.com
```

Refer to [3] for more information on **config.krb5**.

4. Add the following stanzas in the **methods.cfg** file:

```
KRB5A:
        program = /usr/lib/security/KRB5A
        options = authonly

KRB5Afiles:
        options = db=BUILTIN,auth=KRB5A
```

5. Use the **kadmin** tool on Solaris to create host principal **host/tx3d.austin.ibm.com@MYREALM** and save it to a file.

```
kadmin: add_principal -randkey host/tx3d.austin.ibm.com
Principal "host/tx3d.austin.ibm.com@AUSTIN.IBM.COM" created.

kadmin:ktadd -k /tmp/tx3d.keytab host/tx3d.austin.ibm.com
Entry for principal host/tx3d.austin.ibm.com with kvno 3, encryption type
DES-CBC-CRC added to keytab WRFILE:/tmp/tx3d.keytab.
kadmin: quit
#
```

6. Copy the keytab file to the AIX host system.

Merge the keytab file into the **/etc/krb5/krb5.keytab** file as follows:

```
ktutil: rkt tx3d.keytab
ktutil: l
slot   KVNO   Principal
-----
      1      3 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
ktutil: wkt /etc/krb5/krb5.keytab
ktutil: q
```

7. Create a Kerberos principal using the kadmin tool on Solaris

```
kadmin: add_principal sunuser
Enter password for principal "sunuser@AUSTIN.IBM.COM":
Re-enter password for principal "sunuser@AUSTIN.IBM.COM":
Principal "sunuser@AUSTIN.IBM.COM" created.
kadmin:
```

8. Create AIX account corresponding to the Kerberos principal on Solaris such that the login process will know to use Kerberos authentication, as follows:

```
mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles sunuser
```

9. Telnet to the AIX system using Kerberos authentication against Solaris KDC to verify the configuration.

```
# telnet tx3d
Trying...
Connected to tx3d.austin.ibm.com.
Escape character is '^]'.

telnet (tx3d.austin.ibm.com)
```

```
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2004.
login: sunuser
sunuser's Password:
*****
*
*
* Welcome to AIX Version 5.3!
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****
```

```
Last login: Fri Apr 22 16:04:51 CDT 2005 on /dev/pts/4 from localhost
```

```
$ echo $AUTHSTATE
KRB5Afiles
$ echo $KRB5CCNAME
FILE:/var/krb5/security/creds/krb5cc_sunuser@AUSTIN.IBM.COM_207
$ /usr/krb5/bin/klist
Ticket cache: FILE:/var/krb5/security/creds/krb5cc_sunuser@AUSTIN.IBM.COM_207
Default principal: sunuser@AUSTIN.IBM.COM
```

```
Valid starting Expires Service principal
04/22/05 16:03:30 04/23/05 00:03:30 krbtgt/AUSTIN.IBM.COM@AUSTIN.IBM.COM
Renew until 04/23/05 16:05:10
04/22/05 16:03:30 04/23/05 00:03:30 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
$
```

Note: Due to interoperability in the password change protocol between Solaris SEAM Kerberos servers and Network Authentication Service clients, password change operations will result in failure.

```
$ passwd
Changing password for "sunuser"
sunuser's Old password:
sunuser's New password:
Enter the new password again:
```

```
3004-321 Please see the system administrator to change your password.
$
```

4.2 HP-UX 11i v1 KDC 2.1

The steps needed to authenticate against HP-UX 11i are very similar to the steps performed in the Solaris case. The interoperability between a Network Authentication Service client and HP **kadmind** daemon fails like Solaris case. However, Network Authentication Service client and HP-UX KDC interoperable at the Kerberos protocol level. Password change protocol is also compatible.

```
# uname -r
B.11.11
```

1. Setup HP-UX 11i Kerberos Version 2.1. Refer to appropriate HP documentation on how to configure Kerberos Server 2.1.
2. If Network Authentication Service client is not installed then install the **krb5.client.rte** fileset on the AIX client machine from the Expansion Pack.
3. Use the **config.krb5** command to configure an AIX Kerberos client. Configuring the client requires Kerberos KDC information. Use **config.krb5** command with the following options:

realm	HP Kerberos realm name	: <i>HPSYS.AUSTIN.IBM.COM</i>
domain	domain name of the machine hosting the HP-UX Kerberos Server	: <i>austin.ibm.com</i>
KDC	The host name HP-UX system hosting the KDC	: <i>hpsys.austin.ibm.com</i>
server	The host name of HP-UX server	: <i>hpsys.austin.ibm.com</i>

server information will not be meaningful, as HP-UX does not interoperate with Network Authentication Service clients.

Use the **config.krb5** command as shown in the following example:

```
config.krb5 -C -r AUSTIN.IBM.COM -d austin.ibm.com -c hpsys.austin.ibm.com -s
hpsys.austin.ibm.com
```

Modify the **krb5.conf** file so that the encryption type matches the value used during the HP-UX Kerberos setup (**krbsetup**). If DES-CRC is chosen then edit the [libdefaults] stanza in krb5.conf on the AIX client as follows:

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

4. Add the following stanzas in the **methods.cfg** file:

```
KRB5A:
    program = /usr/lib/security/KRB5A
    options = authonly
KRB5Afiles:
    options = db=BUILTIN,auth=KRB5A
```

5. Use the **kadmin_ui** tool on HP-UX to create host principal. host/tx3d.austin.ibm.com. Extract the key and save it to a file (From the Edit menu in Principal Information window, select Extract Service Key to extract the keys.)

6. Copy the keytab file to the AIX host system and merge the keytab file into the **/etc/krb5/krb5.keytab** file using the **ktutil** tool.

7. Create a Kerberos principal, **hpuser**, using the **kadmin_ui** tool on HP-UX. Clear the pw_require flag by clicking Edit/Attribute tab,

8. Create AIX account corresponding to the Kerberos principal on HP-UX as follows

```
mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles hpuser
```

9. Telnet to the AIX system using Kerberos authentication against HP-UX Kerberos server to verify the configuration.

Example: Authenticating against HP-UX Ili Kerberos server.

```
tn tx3d
Trying...
Connected to tx3d.austin.ibm.com.
Escape character is '^T'.
```

```
telnet (tx3d.austin.ibm.com)
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2004.
login: hpuser
hpuser's Password:
*****
*
*
* Welcome to AIX Version 5.3!
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
```

```

*
*
*****
1 unsuccessful login attempt since last login.
Last unsuccessful login: Fri Apr 29 17:23:57 CDT 2005 on /dev/pts/0
Last login: Fri Apr 29 17:05:35 CDT 2005 on /dev/pts/0 from localhost

[tx3d] $ echo $AUTHSTATE
KRB5Afiles
[tx3d] $ /usr/krb5/bin/klist
Ticket cache:
FILE:/var/krb5/security/creds/krb5cc_hpuser@HPSYS.AUSTIN.IBM.COM_208
Default principal: hpuser@HPSYS.AUSTIN.IBM.COM

Valid starting      Expires            Service principal
04/29/05 17:26:17  04/30/05 17:24:14  krbtgt/HPSYS.AUSTIN.IBM.COM@HPSYS.AUSTIN.IBM.COM
04/29/05 17:26:17  04/30/05 17:24:14  host/tx3d.austin.ibm.com@HPSYS.AUSTIN.IBM.COM
[tx3d] $ id
uid=208(hpuser) gid=1(staff)
[tx3d] $

```

The user can change the password using `passwd` command.

```

[tx3d] $ passwd
Changing password for "hpuser"
hpuser's Old password:
hpuser's New password:
Enter the new password again:
[tx3d] $

```

Note that HP UNIX's Kerberos password policy is enforced while changing the password. Refer to HP-UX documentation to determine how to set the password policy.

References

1. Steiner, J. G., Neuman, C. and Jeffrey I. Schiller, "Kerberos: An Authentication Service for Open Network Systems." in Usenix Conference Proceedings, Dallas, Texas, February 1998.
2. Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510.
3. IBM Network Authentication Service Administrator's and User's Guide. Network Authentication Service documentation is provided in the **krb5.doc.lang.[pdf/html]** package, where *lang* represents the supported language (i.e. `krb5.doc.en_US.pdf`). After the installation, one can locate the documents in `/usr/lpp/krb5/doc/pdf/en_US`.
4. AIX 5L Version 5.3 Commands Reference, Volume 1
5. AIX 5L Version 5.3 Commands Reference, Volume 2
6. AIX 5L Version 5.3 Commands Reference, Volume 4
7. AIX 5L Version 5.3 Files Reference

8. AIX Kerberos setup white paper for KRB5. “Configuring AIX for Kerberos Based Authentication Using Network Authentication Services”. To be published.
9. AIX client setup white paper for LDAP user/group management. “Configuring an AIX Client System for User Authentication and Management Through LDAP” http://www.ibm.com/servers/aix/whitepapers/ldap_client.html
10. “Configuring an IBM Directory Server for User Authentication and Management in AIX 5L V5.2” http://www.ibm.com/servers/aix/whitepapers/ldap_server.html



© IBM Corporation 2006
IBM Corporation
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
February 2006
All Rights Reserved

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, AIX, AIX 5L, DB2, Tivoli are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at: <http://www.ibm.com/legal/copytrade.shtml>.

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Microsoft and Windows are registered trademarks of the Microsoft Corporation.

Solaris, SEAM and Sun logo are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Kerberos and Project Athena are trademarks of Massachusetts Institute of Technology.

HP-UX is registered trademark of Hewlett-Packard Company.

Other company, product, and service names may be trademarks or service marks of others.

Copying or downloading the images contained in this document is expressly prohibited without the written consent of IBM.

Information concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of the non-IBM products should be addressed with those suppliers.

The IBM home page on the Internet can be found at: <http://www.ibm.com>.

The IBM System p5 and @server p5 home page on the Internet can be found at: <http://www.ibm.com/systems/p5>.