

AIX security commands

Skill Level: Intermediate

[Uma M. Chandolu \(uchandol@in.ibm.com\)](mailto:uchandol@in.ibm.com)
Software Engineer
IBM

[Puneet Mahajan \(pmahajan@us.ibm.com\)](mailto:pmahajan@us.ibm.com)
Software Engineer
IBM

22 Jul 2008

Security is an important aspect of the IBM® AIX® operating system. Follow along with this quick reference guide on AIX security commands to learn more.

Introduction

AIX provides a vast array of commands to handle user and group management. This article discusses some of these core security commands and provides a list that you can use as a ready reference. The behavior of these commands should be identical in all releases of AIX.

Commands

General commands

How to do I create a user on AIX?

To create a user on AIX, type:

```
mkuser <username>
```

or

```
useradd <username>
```

Both of these commands create the user on AIX and update the user information in the `/etc/passwd` file.

How do I set a user password?

The `passwd` command sets the password for user and updates the user's password information to `/etc/security/passwd` file. When the password is set for user using the `passwd` command, it sets the `ADMCHK` flag so that the user is prompted to change the password during their next login.

To set the password, type:

```
passwd <username>
```

How do I clear the ADMCHK flag for a user?

To clear the `ADMCHK` flag and all password flags for a user, type:

```
pwdadm -c <username>
```

The `-c` flag clears the `ADMCHK` flag for user and modifies the user's password stanza in `/etc/security/passwd` file.

How do I create a group on AIX?

Use the `mkgroup` command to create groups on AIX and update group information in the `/etc/group` and `/etc/security/group` files.

```
mkgroup <groupname>
```

How do I remove a user?

Two commands are available to remove a user. To remove users, type:

```
rmuser <username>
```

or

```
userdel <username>
```

How do I remove a group?

Use the `rmgroup` command to remove a group.

```
rmgroup <groupname>
```

How do I list the user attributes?

The `lsuser` command displays all of the user attributes from the `/etc/passwd` and `/etc/security/user` files.

```
lsuser <username>
```

How do I list group attributes?

To show the attributes of a group, type:

```
lsgroup <groupname>
```

How do I change user attributes?

The `chuser` command changes the user information and updates the configuration files.

```
chuser attribute=value <username>
```

How do I disable remote logins on the system?

User attributes are stored in the `/etc/security/user` configuration file. To disable users from logging in remotely, set the "rlogin" attribute as "false."

What's the difference between "registry" and "SYSTEM" attributes of a user?

The registry attribute specifies where the user or group identification information is administrated and the SYSTEM attribute controls which methods are used and how the methods affect the overall authentication. Every user on AIX must have a value for the registry and SYSTEM attribute. Groups only have registry values.

What are the AIX Security configuration files?

/etc/passwd
/etc/group
/etc/security/passwd
/etc/security/user
/etc/security/group
/etc/security/lastlog

```
/etc/security/login.cfg
```

```
/usr/lib/security/methods.cfg
```

How do I check for inconsistencies in the security configuration files?

```
usrck
```

```
grpck
```

```
pwdck
```

How do I get the user and group name length limits from kernel?

The getconf command with the LOGIN_NAME_MAX parameter retrieves the user and group name length limits in the kernel.

```
getconf LOGIN_NAME_MAX
```

What is the maximum name length for user and group?

For AIX 5.2 and below, the maximum name length for user and group is 8 characters. AIX 5.3 and above allows the administrator to increase the name length for users and groups up to 255 characters.

How do I increase the name length for users and groups?

Using the smit , the smit -> System Environments -> Change / Show Characteristics of Operation System panel can be used to change the value (in "Maximum login name length at boot time" field) in the ODM database. The value specified in the smit panel takes effect after the next reboot.

Using the command line, the chdev command can be used to change the sys0 device's v_max_logname parameter in the ODM database through the max_logname attribute. The changed value in the ODM database takes effect after the next reboot.

```
# chdev -l sys0 -a max_logname=30
sys0 changed
```

LDAP commands

How do I configure the ITDS LDAP server/client on AIX?

The mksecldap command configures the ITDS LDAP server/client. Please refer to the [Resources](#) section for more information.

How do I stop the LDAP client daemon?

Use the `/usr/sbin/stop-secdapclntd` command to stop the LDAP client daemon.

How do I start the LDAP client daemon?

Use the `/usr/sbin/start-secdapclntd` command to start the ldap client daemon..

How do I restart the secdapclntd daemon?

Use the `/usr/sbin/restart-secdapclntd` command to restart the secdapclntd daemon.

How do I get the LDAP user information from the LDAP server?

The `lsldap` command gets the information from the LDAP server through the LDAP client and `secdapclntd` daemon.

```
lsldap -a passwd username OR lsuser -R LDAP username
```

How do I get LDAP group information from the LDAP server?

```
lsldap -a group groupname OR lsgroup -R LDAP groupname
```

For more information about the LDAP commands, please refer to this [whitepaper](#).

Kerberos commands

How do I configure a NAS Kerberos server on AIX?

```
mkkrb5srv -r <realm> -s <servername> -d <domain>
```

This command configures the Kerberos server on AIX and creates the `/etc/krb5/krb5.conf`, `/var/krb5/krb5kdc/kdc.conf`, and `kdm5.acl` files.

How do I configure a NAS Kerberos client on AIX?

```
mkkrb5clnt -r <realm name> -c <KDC server> -s  
<Kerberos server> -d <domain> -a admin/admin -A i files -K - T
```

This command configures a Kerberos client on AIX and uses "files" as the database for the Kerberos. If you want to use "LDAP" as the database, specify **LDAP** in place of "files" in the above command. This command also updates the KRB5files and KRB5 modules information to `/usr/lib/security/methods.cfg` files.

How do I create a Kerberos user?

```
mkuser -R registry=KRB5files SYSTEM="KRB5files" <username>  
OR  
mkuser -R KRB5LDAP registry=KRB5LDAP SYSTEM="KRBLDAP" <username>
```

How do I set the password for a Kerberos user?

```
passwd -R KRB5files <username>  
OR  
passwd -R KRB5LDAP <username>
```

This command works if the Kerberos client is configured with the kadmin support. If there is no kadmin support, users can't change their passwords from the Kerberos client.

How do I configure the AIX Kerberos client with a Microsoft® Windows® Active Directory server?

```
config.krb5 -C -r <realm> -d <domain> -c <KDC server> -s <kerberos server>
```

where

- <realm> is the Windows Active Directory domain name
- <domain> is the domain name of the machine hosting the Active Directory server
- <KDC server> is the host name of the Windows server
- <kerberos server> is the host name of the Windows server

What are the encryption mechanisms supported by Microsoft Windows?

Microsoft Windows supports DES-CBC-MD5 and DES-CBC-CRC encryption types. Change the AIX Kerberos client /etc/krb5/krb5.conf files as follows.

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

How do I unconfigure the Kerberos client/server?

```
unconfig.krb5
```

This command removes the Network Authentication Service configuration information and files from clients and servers.

How do I verify which authentication method was used during the login?

```
echo $AUTHSTATE
```

This command provides the authentication method that was used during the login.

Resources

Learn

- The [AIX Security Guide](#) provides system administrators with complete information on file, system, and network security.
- [LDAP configuration management and troubleshooting on AIX](#). This article provides an overview of the LDAP configuration and management.
- [AIX 5L LDAP user management](#). This article provides an overview of the LDAP-related enhancements in the AIX 5L operating system V5.3 TL5 update.
- Browse the [technology bookstore](#) for books on these and other technical topics.

Get products and technologies

- Download [IBM product evaluation versions](#) and get your hands on application development tools and middleware products from DB2®, Lotus®, Rational®, Tivoli®, and WebSphere®.

Discuss

- - [AIX Forum](#)
 - [AIX Forum for Developers](#)
 - [Cluster Systems Management](#)
 - [IBM Support Assistant Forum](#)
 - [Performance Tools Forum](#)
 - [Virtualization Forum](#)
 - [More AIX and UNIX forums](#)
- Check out [developerWorks blogs](#) and get involved in the [developerWorks community](#).

About the authors

Uma M. Chandolu

Uma M. Chandolu works as a Development Support Specialist on AIX. He is currently the team lead of AIX Security Development Support team at IBM Bangalore. He has three years of extensive hands-on experience in AIX environments, and demonstrated expertise in AIX system administration and other subsystems. He has experience interfacing with customers and handling customer

critical situations. You can reach him at uchandol@in.ibm.com.

Puneet Mahajan

Puneet Mahajan is an Advanced AIX technical support specialist with over 7 years of experience in AIX System Administration. He is currently the team lead of AIX remote support for Independent Software Vendors (ISV) at IBM Austin. You can reach him at pmahajan@us.ibm.com .