AIX security commands, Part 1: General, LDAP, and Kerbos commands

Uma Chandolu
Puneet Mahajan

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 do I create a user on AIX?

To create a user on AIX, type:

```
mkuser &lt;username&gt;
```

or

```
useradd &lt;username&gt;
```

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 &lt;username&gt;
```
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 &lt;username&gt;
```

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 &lt;groupname&gt;
```

How do I remove a user?

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

```
rmuser &lt;username&gt;
```

or

```
userdel &lt;username&gt;
```

How do I remove a group?

Use the rmgroup command to remove a group.

```
rmgroup &lt;groupname&gt;
```

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 &lt;username&gt;
```

How do I list group attributes?

To show the attributes of a group, type:

```
lsgroup &lt;groupname&gt;
```

How do I change user attributes?
The chuser command changes the user information and updates the configuration files.

```
chuser attribute=value &lt;username&gt;
```

**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?**

<table>
<thead>
<tr>
<th>AIX security configuration files</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/passwd</code></td>
</tr>
<tr>
<td><code>/etc/group</code></td>
</tr>
<tr>
<td><code>/etc/security/passwd</code></td>
</tr>
<tr>
<td><code>/etc/security/user</code></td>
</tr>
<tr>
<td><code>/etc/security/group</code></td>
</tr>
<tr>
<td><code>/etc/security/fastlog</code></td>
</tr>
<tr>
<td><code>/etc/security/login.cfg</code></td>
</tr>
<tr>
<td><code>/usr/lib/security/methods.cfg</code></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>usrck</code></td>
<td>This command corrects the user information.</td>
</tr>
<tr>
<td><code>grpck</code></td>
<td>This command corrects the group information.</td>
</tr>
<tr>
<td><code>pwdck</code></td>
<td>This command verifies the correctness of the password information in the user database files.</td>
</tr>
</tbody>
</table>

**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 -&gt; System Environments -&gt; 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 Related topics section for more information.

**How do I stop the LDAP client daemon?**

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

**How do I start the LDAP client daemon?**

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

**How do I restart the secldapclntd daemon?**

Use the /usr/sbin/restart-secldapclntd command to restart the secldapclntd 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 secldapclntd 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
```
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 &lt;KDC server&gt; -s &lt;Kerberos server&gt; -d &lt;domain&gt; -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" &lt;username&gt; OR mkuser -R KRB5LDAP registry=KRB5LDAP SYSTEM="KRB5LDAP" &lt;username&gt;
```

How do I set the password for a Kerberos user?

```
passwd -R KRB5files &lt;username&gt; OR passwd -R KRB5LDAP &lt;username&gt;
```

This command works if the Kerberos client is configured with the kadmin support. If there is no kadmind 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 &lt;realm&gt; -d &lt;domain&gt; -c &lt;KDC server&gt; -s &lt;kerberos server&gt;
```

where

- &lt;realm&gt; is the Windows Active Directory domain name
- &lt;domain&gt; is the domain name of the machine hosting the Active Directory server
- &lt;KDC server&gt; is the host name of the Windows server
- &lt;kerberos server&gt; 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_enctypes = des-cbc-crc des-cbc-md5 default_tgs_enctypes = des-cbc-crc des-cbc-md5
```

AIX security commands, Part 1: General, LDAP, and Kerberos commands
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.
Related topics

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

© Copyright IBM Corporation 2008
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)