

## 7.1.4 User and Group Facts


This lesson covers the following topics:

- User groups and types
- User and group databases
- Commands for managing password file entries

### User Groups and Types

User accounts control the ability to log on to a system, access resources, and perform certain actions. Groups provide a way to group users for administrative purposes, such as assigning permissions to files.

Be aware of the following types of users and groups:

Type	Description
Standard user	<p>Standard user accounts can log into the system. Standard user accounts:</p> <ul style="list-style-type: none"><li>• Have friendly usernames (such as Mary or bkaun). An administrator must create the usernames.</li><li>• Have an ID of 500 or more (on some distributions) or 1000 or more (on other distributions). The ID is automatically assigned by the system when the account is created.</li></ul>
System or service accounts	<p>System user accounts (also called service user accounts) are created by default during the Linux installation and are used by the system for specific roles.</p> <p>System user accounts:</p> <ul style="list-style-type: none"><li>• Have names that correspond with their roles, such as ftp and mail.</li><li>• Cannot be used to log into the system.</li><li>• Have an ID of 500 or less (on some distributions) or 1000 or less (on other distributions). The ID is automatically assigned by the system when the account is created.</li></ul> <div> The root user account is created by default and has a UID of 0; however, it can be used to log into a system and perform tasks.</div>
Primary group	<p>Primary groups (also called the private group) are created by default on most Linux distributions when a standard user is created and are used to manage access to files and directories. Primary groups:</p> <ul style="list-style-type: none"><li>• Have the corresponding user as the only member.</li></ul>

	<ul style="list-style-type: none"> <li>• Are automatically assigned as the owner of files and directories when they are created in the file system.</li> <li>• Are similar to any other group. The only difference is that the group is identified as the primary group in the user account's configuration.</li> </ul>
Secondary group	<p>Secondary groups are also used to manage access to files and directories. Secondary groups:</p> <ul style="list-style-type: none"> <li>• Are not automatically assigned user accounts as members.</li> <li>• Receive their membership as assigned by the system administrator.</li> </ul>

The following table explains the files where user and group databases are stored.

File	Description
<b>/etc/passwd</b>	<p>The <code>/etc/passwd</code> file holds user account information. Be aware of the following details:</p> <ul style="list-style-type: none"> <li>• Each entry identifies a user account.</li> <li>• Each entry contains multiple fields, with each field separated by a colon.</li> </ul> <p>The following line is a sample entry in the <code>/etc/passwd</code> file:</p> <pre>pclark:x:501:501:Petunia Clark:/home/pclark:/bin/bash</pre> <p>The fields within this line are as follows:</p> <ul style="list-style-type: none"> <li>• User account name.</li> <li>• Password. An x in the field indicates passwords are stored in the <code>/etc/shadow</code> file.</li> <li>• User ID number.</li> <li>• Primary group ID number (also known as the GID).</li> <li>• Description field. This field is typically used for the user's full name.</li> <li>• Path to the home directory.</li> <li>• Path to the default shell.</li> </ul>
<b>/etc/shadow</b>	<p>The <code>/etc/shadow</code> file holds passwords and password expiration information for user accounts. Be aware of the following details:</p> <ul style="list-style-type: none"> <li>• Using the <code>/etc/shadow</code> file to separate usernames from passwords increases the security of the user passwords.</li> <li>• Like the <code>/etc/passwd</code> file, each entry corresponds to a user account and each entry contains multiple fields, with each field separated by a colon.</li> </ul> <p>The following line is a sample entry in the <code>/etc/shadow</code> file:</p> <pre>pclark:\$ab7Y56gu9bs:12567:0:99999:7:::</pre> <p>The fields within this line are as follows:</p> <ul style="list-style-type: none"> <li>• User account name.</li> <li>• Password. <ul style="list-style-type: none"> <li>◦ \$ preceding the password identifies the password as an encrypted entry.</li> <li>◦ ! or !! indicates that the account is locked and cannot be used to log in.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>◦ * indicates a system account entry and cannot be used to log in.</li> <li>• Last change. The date of the most recent password change measured in the number of days since 1 January 1970.</li> <li>• Minimum password age. The minimum number of days the user must wait before changing the password.</li> <li>• Maximum password age. The maximum number of days between password changes.</li> <li>• Password change warning. The number of days a user is warned before the password must be changed.</li> <li>• Grace logins. The number of days the user can log in without changing the password.</li> <li>• Disable time. The number of days since 1 January 1970, after which the account will be disabled.</li> </ul>
<b>/etc/group</b>	<p>The /etc/group file holds group information including the group name, GID, and group membership information. Be aware of the following details:</p> <ul style="list-style-type: none"> <li>• Each entry identifies a group.</li> <li>• Each entry contains multiple fields, with each field separated by a colon.</li> </ul> <p>The following line is a sample entry in the /etc/group file:</p> <pre>sales:x:510:pclark,mmckay,hsamson</pre> <p>The fields within this line are as follows:</p> <ul style="list-style-type: none"> <li>• Group name.</li> <li>• Group password. An x indicates the group passwords are contained in the /etc/gshadow file.</li> <li>• Group ID.</li> <li>• Group members (contains a comma-separated list of user accounts that are members of the group).</li> </ul>
<b>/etc/gshadow</b>	<p>The /etc/gshadow file holds passwords for groups. Be aware of the following details:</p> <ul style="list-style-type: none"> <li>• Like the /etc/group file, each line corresponds to a group.</li> <li>• Each line consists of fields separated by colons.</li> </ul> <p>The following line is a sample entry in the /etc/gshadow file:</p> <pre>sales!:pclark:pclark,mmckay,hsamson</pre> <p>The fields within this line are as follows:</p> <ul style="list-style-type: none"> <li>• Group name.</li> <li>• Group password. The group password allows users to add themselves as members of the account. <ul style="list-style-type: none"> <li>◦ If the field contains a single exclamation point (!), the group account cannot be accessed using the password.</li> <li>◦ If the field contains a double exclamation point (!!), no password has been assigned to the group account (and it cannot be accessed using the password).</li> </ul> </li> </ul>

- If there is no value, only group members can log in to the group account.
- Administrators. Contains a comma-separated list of users who have authorization to administer the account.
- Group members. Contains a comma-separated list of user accounts that are members of the group.

## Commands for Managing Password File Entries

Additional commands for managing file entries include the following:

Command	Description
<b>pwck</b>	<p>Verifies the entries in the <code>/etc/passwd</code> and <code>/etc/shadow</code> files to ensure that they have the proper format and contain valid data. Errors are displayed on the screen, and entries may be deleted to solve the errors.</p> <p>For example, checks are made to verify that each entry has:</p> <ul style="list-style-type: none"> <li>• The correct number of fields</li> <li>• A unique and valid user name</li> <li>• A valid user and group identifier</li> <li>• A valid primary group</li> <li>• A valid home directory</li> <li>• A valid login shell</li> </ul>
<b>pwconv</b>	<p>The <b>pwconv</b> command is used to move passwords from the less-secure <code>/etc/passwd</code> file to the more secure <code>/etc/shadow</code> file. The opposite of this action can be done with the <b>pwunconv</b> command and will also remove the shadow file. Today, however, virtually all Linux distributions ship with shadow files enabled by default.</p> <p>The synchronization process is as follows:</p> <ul style="list-style-type: none"> <li>• The entries in the shadowed file that do not exist in the <code>passwd</code> file are removed.</li> <li>• The shadowed entries that don't have <code>x</code> as the password in the <code>passwd</code> file are updated.</li> <li>• Any missing shadowed entries are added.</li> <li>• Passwords found in the <code>passwd</code> file are replaced with <code>x</code>.</li> </ul>

Copyright © 2022 TestOut Corporation All rights reserved.