8.11.3 Linux User Security and Restriction Facts

When considering user security, keep in mind the following:

- Users should be trained to use secure passwords. Secure passwords use numbers and letters, and are more than 7 characters in length.
- Passwords should expire periodically, but not too often.
- Administrators can limit the resources that user can access.

The following table describes commands used to promote user security and restrictions:

Use	To	Examples
chage	Set user passwords to expire. Be aware of the following options: - **-M** sets the maximum number of days before the password expires. - **-W** sets the number of days before the password expires that a warning message displays. - **-m** sets the minimum number of days that must pass after a password has been changed before a user can change the password again. Look in the **/etc/shadow** file to see current limits for users.	**chage -M 60 -W 10 jsmith** sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires.
ulimit	Limit computer resources used for applications launched from the shell. Limits can be hard or soft limits. Soft limits can be temporarily exceeded up to the hard limit setting. Users can modify soft limits, but only root can modify hard limits. Options include: - **-c** limits the size of a core dump file. The value is in blocks. - **-f** limits the file size of files created using the shell session. The value is in blocks. - **-n** limits the maximum number of open files. - **-t** limits the amount of CPU time a process can use. This is set in seconds. - **-u** limits the number of concurrent processes a user can run. - **-d** limits the maximum amount of memory a process can use. The value is in kilobytes. - **-H** sets a hard resource limit. - **-S** sets a soft resource limit. - **-a** displays current limits. The default shows soft limits.	**ulimit -H -f 1024** uses a hard limit to limit the size of files to 1020 KB. **ulimit -H -a** shows current hard limits. **ulimit -a** shows the current soft limits. **ulimit -S -u 10** sets a soft limit that limits the number of processes that a single user can use to 10. **ulimit -t 600** limits CPU time for a process to 10 minutes. This sets both hard and soft limits. **ulimit -d unlimited** removes all restrictions for process memory usage.

Use the **/etc/security/limits.conf** file to limit resource use for all applications. This file is from the pam_limits module of the Pluggable Authentication Modules (PAM) module set. Entries in **/etc/security/limits.conf** use the following syntax:

```
Entity   Type   Limit   Value
```

The following table describes the entry options in the **/etc/security/limits.conf** file:

Entity	Type	Limits	Value
When specifying the Entity: - Specify a single user with a username. - Use an at sign (@) to specify a group. - Use an asterisk (*) as a wildcard.	For the Type: - Use **hard** to set a limit that cannot be exceeded. - Use **soft** to set a limit that can be exceeded temporarily.	The following are some types of limits: - **core** limits the size of core dump files. The value uses kilobytes. - **data** limits the amount of RAM an application can use. The value uses kilobytes. - **fsize** limits maximum file size. The value uses kilobytes. - **nofile** limits the number of concurrently open data files. - **cpu** limits the amount of CPU time a process can use. The value uses minutes. - **nproc** limits the number of concurrent processes a user can have. - **maxlogins** limits the number of concurrent logins. - **priority** sets process priority limits. The value range is from -20 (highest priority) to 19 (lowest priority), with 0 being the default. - **rss** limits the total amount of memory a user can use. The value uses kilobytes.	Values include integers, such as 1, 5, or 3000.

The following are examples of entries in the **/etc/security/limits.conf** file:

Example	Description
jsmith hard fsize 1024	Limits the maximum file size that jsmith can create to 1024 KB.
@guests hard maxlogins 3	Limits the number of concurrent logins from the guest group to three.
*** hard maxlogins 1**	Limits concurrent logins from the same user to one.
*** soft cpu 10**	Sets a soft limit of 10 minutes on the amount of CPU time any single process for any user can take.
rss hard rss 5000	Limits the total amount of memory available to a single user to 5 MB