

Successful login

Location: /var/log/ secure

```
encryptos@localhost:~$ tail /var/log/secure
tail: cannot open '/var/log/secure' for reading: Permission denied
[encryptos@localhost ~]$ sudo tail /var/log/secure
[sudo] password for encryptos:
Nov 14 00:02:26 localhost gdm-launch-environment[1481]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Nov 14 00:02:45 localhost polkitd[900]: Registered Authentication Agent for unix-session:cl (system bus name :1.25 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:08:27 localhost gdm-password[2586]: gkr-pam: unable to locate daemon control file
Nov 14 00:08:27 localhost gdm-password[2586]: gkr-pam: stashed password to try later in open session
Nov 14 00:08:27 localhost systemd[2606]: pam_unix(systemd-user:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:08:27 localhost gdm-password[2586]: pam_unix(gdm-password:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:08:27 localhost gdm-password[2586]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Nov 14 00:08:29 localhost polkitd[900]: Registered Authentication Agent for unix-session:2 (system bus name :1.69 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:08:34 localhost gdm-launch-environment[1481]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Nov 14 00:08:34 localhost polkitd[900]: Unregistered Authentication Agent for unix-session:cl (system bus name :1.25, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
[encryptos@localhost ~]$
```

Failed Login

Location: /var/log/ secure

```
Nov 14 00:26
encryptos@localhost:~$
Nov 14 00:16:58 localhost polkitd[917]: Loading rules from directory /etc/polkit-1/rules.d
Nov 14 00:16:58 localhost polkitd[917]: Loading rules from directory /usr/share/polkit-1/rules.d
Nov 14 00:16:58 localhost polkitd[917]: Finished loading, compiling and executing 13 rules
Nov 14 00:16:58 localhost polkitd[917]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Nov 14 00:16:59 localhost sshd[1111]: Server listening on 0.0.0.0 port 22.
Nov 14 00:16:59 localhost sshd[1111]: Server listening on :: port 22.
Nov 14 00:16:59 localhost systemd[1404]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by (uid=0)
Nov 14 00:16:59 localhost gdm-launch-environment[1236]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Nov 14 00:17:01 localhost polkitd[917]: Registered Authentication Agent for unix-session:cl (system bus name :1.25 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:17:11 localhost unix_chkpwd[2554]: password check failed for user (encryptos)
Nov 14 00:17:11 localhost gdm-password[2545]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/ttyl ruser= rhost= user=encryptos
Nov 14 00:17:11 localhost gdm-password[2545]: gkr-pam: unable to locate daemon control file
Nov 14 00:17:11 localhost gdm-password[2545]: gkr-pam: stashed password to try later in open session
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: unable to locate daemon control file
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: stashed password to try later in open session
Nov 14 00:17:17 localhost systemd[2564]: pam_unix(systemd-user:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:17:17 localhost gdm-password[2555]: pam_unix(gdm-password:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Nov 14 00:17:19 localhost polkitd[917]: Registered Authentication Agent for unix-session:2 (system bus name :1.70 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:17:22 localhost gdm-launch-environment[1236]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Nov 14 00:17:22 localhost polkitd[917]: Unregistered Authentication Agent for unix-session:cl (system bus name :1.25, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Nov 14 00:17:52 localhost sudo[3446]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail /var/log/secure
Nov 14 00:17:52 localhost sudo[3446]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:17:52 localhost sudo[3446]: pam_unix(sudo:session): session closed for user root
Nov 14 00:18:22 localhost sudo[3469]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -20 /var/log/secure
Nov 14 00:18:22 localhost sudo[3469]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:18:22 localhost sudo[3469]: pam_unix(sudo:session): session closed for user root
Nov 14 00:18:55 localhost sudo[3479]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:18:55 localhost sudo[3479]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:18:55 localhost sudo[3479]: pam_unix(sudo:session): session closed for user root
Nov 14 00:21:16 localhost unix_chkpwd[3495]: password check failed for user (root)
Nov 14 00:21:16 localhost su[3488]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=encryptos rhost= user=root
Nov 14 00:21:33 localhost sudo[3500]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:21:33 localhost sudo[3500]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:21:33 localhost sudo[3500]: pam_unix(sudo:session): session closed for user root
Nov 14 00:23:12 localhost sudo[3511]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:23:12 localhost sudo[3511]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:23:12 localhost sudo[3511]: pam_unix(sudo:session): session closed for user root
[encryptos@localhost ~]$
```

Session opened for user root

```
Nov 14 00:26
encryptos@localhost:~

Nov 14 00:16:58 localhost polkitd[917]: Loading rules from directory /etc/polkit-1/rules.d
Nov 14 00:16:58 localhost polkitd[917]: Loading rules from directory /usr/share/polkit-1/rules.d
Nov 14 00:16:58 localhost polkitd[917]: Finished loading, compiling and executing 13 rules
Nov 14 00:16:58 localhost polkitd[917]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Nov 14 00:16:59 localhost sshd[1111]: Server listening on 0.0.0.0 port 22.
Nov 14 00:16:59 localhost sshd[1111]: Server listening on :: port 22.
Nov 14 00:16:59 localhost systemd[1404]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by (uid=0)
Nov 14 00:16:59 localhost gdm-launch-environment[1236]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Nov 14 00:17:01 localhost polkitd[917]: Registered Authentication Agent for unix-session:cl (system bus name :1.25 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:17:11 localhost unix_chkpwd[2554]: password check failed for user (encryptos)
Nov 14 00:17:11 localhost gdm-password[2545]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/ttyl ruser= rhost= user=encryptos
Nov 14 00:17:11 localhost gdm-password[2545]: gkr-pam: unable to locate daemon control file
Nov 14 00:17:11 localhost gdm-password[2545]: gkr-pam: stashed password to try later in open session
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: unable to locate daemon control file
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: stashed password to try later in open session
Nov 14 00:17:17 localhost systemd[2564]: pam_unix(systemd-user:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:17:17 localhost gdm-password[2555]: pam_unix(gdm-password:session): session opened for user encryptos(uid=1000) by (uid=0)
Nov 14 00:17:17 localhost gdm-password[2555]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Nov 14 00:17:19 localhost polkitd[917]: Registered Authentication Agent for unix-session:2 (system bus name :1.70 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 14 00:17:22 localhost gdm-launch-environment[1236]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Nov 14 00:17:22 localhost polkitd[917]: Unregistered Authentication Agent for unix-session:cl (system bus name :1.25, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Nov 14 00:17:52 localhost sudo[3446]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -v /var/log/secure
Nov 14 00:17:52 localhost sudo[3446]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:17:52 localhost sudo[3446]: pam_unix(sudo:session): session closed for user root
Nov 14 00:18:22 localhost sudo[3469]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -20 /var/log/secure
Nov 14 00:18:22 localhost sudo[3469]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:18:22 localhost sudo[3469]: pam_unix(sudo:session): session closed for user root
Nov 14 00:18:55 localhost sudo[3479]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:18:55 localhost sudo[3479]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:18:55 localhost sudo[3479]: pam_unix(sudo:session): session closed for user root
Nov 14 00:21:16 localhost unix_chkpwd[3495]: password check failed for user (root)
Nov 14 00:21:16 localhost su[3488]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=encryptos rhost= user=root
Nov 14 00:21:33 localhost sudo[3500]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:21:33 localhost sudo[3500]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:21:33 localhost sudo[3500]: pam_unix(sudo:session): session closed for user root
Nov 14 00:23:12 localhost sudo[3511]: encryptos : TTY=pts/0 ; PWD=/home/encryptos ; USER=root ; COMMAND=/bin/tail -50 /var/log/secure
Nov 14 00:23:12 localhost sudo[3511]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 14 00:23:12 localhost sudo[3511]: pam_unix(sudo:session): session closed for user root
[encryptos@localhost ~]$
```

Software Install Log
Location : /var/log dnf.log

```
encryptos@localhost:~ -- sudo tail -f /var/log/dnf.log

return _main(base, args, cli_class, option_parser_class)
File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 106, in _main
    return cli_run(cli, base)
File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 122, in cli_run
    cli.run()
File "/usr/lib/python3.9/site-packages/dnf/cli/cli.py", line 1057, in run
    return self.command.run()
File "/usr/lib/python3.9/site-packages/dnf/cli/commands/install.py", line 118, in run
    raise dnf.exceptions.PackagesNotAvailableError(_("Unable to find a match"))
dnf.exceptions.PackagesNotAvailableError: Unable to find a match: nginx
2023-11-14T01:34:26+0600 CRITICAL Error: Unable to find a match: nginx
2023-11-14T01:35:03+0600 INFO --- logging initialized ---
2023-11-14T01:35:03+0600 DEBUG timer: config: 2 ms
2023-11-14T01:35:03+0600 DEBUG Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install, download, generate_completion_cache, groups-manager, kpatch, needs-restart
ing, playground, product-id, repoclosure, repodiff, repograph, repomanage, reposync, subscription-manager, system-upgrade, uploadprofile, upgrade
2023-11-14T01:35:03+0600 INFO Updating Subscription Management repositories.
2023-11-14T01:35:09+0600 DEBUG DNF version: 4.14.0
2023-11-14T01:35:09+0600 DEBUG Command: dnf install -y nginx
2023-11-14T01:35:09+0600 DEBUG Installroot: /
2023-11-14T01:35:09+0600 DEBUG Releasever: 9
2023-11-14T01:35:09+0600 DEBUG cachedir: /var/cache/dnf
2023-11-14T01:35:09+0600 DEBUG Base command: install
2023-11-14T01:35:09+0600 DEBUG Extra commands: ['install', '-y', 'nginx']
2023-11-14T01:35:09+0600 DEBUG User-Agent: constructed: 'libdnf (Red Hat Enterprise Linux 9.3; generic; Linux.x86_64)'
2023-11-14T01:35:09+0600 DEBUG repo: using cache for: rhel-9-for-x86_64-supplementary-rpms
2023-11-14T01:35:09+0600 DEBUG rhel-9-for-x86_64-supplementary-rpms: using metadata from Fri 03 Nov 2023 06:00:21 PM +06.
2023-11-14T01:35:09+0600 DEBUG repo: using cache for: rhel-9-for-x86_64-baseos-debug-rpms
2023-11-14T01:35:09+0600 DEBUG rhel-9-for-x86_64-baseos-debug-rpms: using metadata from Tue 07 Nov 2023 05:11:09 PM +06.
2023-11-14T01:35:09+0600 DEBUG repo: using cache for: rhel-9-for-x86_64-baseos-rpms
2023-11-14T01:35:09+0600 DEBUG rhel-9-for-x86_64-baseos-rpms: using metadata from Wed 18 Oct 2023 06:16:17 AM +06.
2023-11-14T01:35:09+0600 DEBUG rhel-9-for-x86_64-appstream-rpms: using metadata from Fri 10 Nov 2023 01:36:16 AM +06.
2023-11-14T01:35:09+0600 INFO Last metadata expiration check: 0:27:53 ago on Tue 14 Nov 2023 01:07:16 AM +06.
2023-11-14T01:35:09+0600 DEBUG timer: sack setup: 632 ms
2023-11-14T01:35:09+0600 DEBUG --> Starting dependency resolution
2023-11-14T01:35:10+0600 DEBUG --> Package nginx.x86_64 1:1.20.1-14.el9_2.1 will be installed
2023-11-14T01:35:10+0600 DEBUG --> Package nginx-core.x86_64 1:1.20.1-14.el9_2.1 will be installed
2023-11-14T01:35:10+0600 DEBUG --> Package nginx-filestream.noarch 1:1.20.1-14.el9_2.1 will be installed
2023-11-14T01:35:10+0600 DEBUG --> Finished dependency resolution
2023-11-14T01:35:10+0600 DEBUG timer: depsolve: 82 ms

Install 3 Packages
Total download size: 825 k
Installed size: 1.7 M
Downloading Packages:
(1/3): nginx-1.20.1-14.el9_2.1.x86_64.rpm 9.8 kB/s | 49 kB
(2/3): nginx-filestream-1.20.1-14.el9_2.1.noarch.rpm 2.7 kB/s | 11 kB
(3/3): nginx-core-1.20.1-14.el9_2.1.x86_64.rpm 89 kB/s | 574 kB
Total 100 kB/s | 825 kB

Running transaction test:
Transaction test succeeded.
Running transaction:
Preparing...
Running scriptlet: nginx-filestream-1:1.20.1-14.el9_2.1.noarch
Installing...: nginx-filestream-1:1.20.1-14.el9_2.1.noarch
Installing...: nginx-core-1:1.20.1-14.el9_2.1.x86_64
Installing...: nginx-x86_64-1:1.20.1-14.el9_2.1.x86_64
Running scriptlet: nginx-1:1.20.1-14.el9_2.1.x86_64
Verifying...: nginx-1:1.20.1-14.el9_2.1.x86_64
Verifying...: nginx-core-1:1.20.1-14.el9_2.1.x86_64
Verifying...: nginx-filestream-1:1.20.1-14.el9_2.1.noarch
Installed products updated:
Installed:
  nginx-1:1.20.1-14.el9_2.1.x86_64
  nginx-core-1:1.20.1-14.el9_2.1.x86_64
  nginx-filestream-1:1.20.1-14.el9_2.1.noarch
```

```
Nov 14 01:42
encryptos@localhost:~$ sudo tail -f /var/log/dnf.log

2023-11-14T01:35:10+0600 INFO Dependencies resolved.
2023-11-14T01:35:10+0600 INFO =====
Package Arch Version Repository Size
-----
Installing:
  nginx x86_64 1:1.20.1-14.el9_2.1 rhel-9-for-x86_64-appstream-rpms 40 k
Installing dependencies:
  nginx-core x86_64 1:1.20.1-14.el9_2.1 rhel-9-for-x86_64-appstream-rpms 574 k
  nginxfilesystem noarch 1:1.20.1-14.el9_2.1 rhel-9-for-x86_64-appstream-rpms 11 k
Transaction Summary
-----
Install 3 Packages

2023-11-14T01:35:10+0600 INFO Total download size: 625 k
2023-11-14T01:35:10+0600 INFO Installed size: 1.7 M
2023-11-14T01:35:10+0600 INFO Downloading Packages:
2023-11-14T01:35:15+0600 INFO -----
2023-11-14T01:35:15+0600 INFO Total 188 kB/s | 625 kB 00:05
2023-11-14T01:35:15+0600 DEBUG Using rpmkeys executable at /bin/rpmkeys to verify signatures
2023-11-14T01:35:16+0600 INFO Running transaction check
2023-11-14T01:35:16+0600 INFO Transaction check succeeded.
2023-11-14T01:35:16+0600 INFO Running transaction test
2023-11-14T01:35:18+0600 INFO Transaction test succeeded.
2023-11-14T01:35:18+0600 DDEBUG timer: transaction test: 2078 ms
2023-11-14T01:35:18+0600 INFO Running transaction
2023-11-14T01:35:18+0600 DDEBUG RPM transaction start.
2023-11-14T01:35:21+0600 DDEBUG RPM transaction over.
2023-11-14T01:35:21+0600 DDEBUG timer: verify transaction: 257 ms
2023-11-14T01:35:21+0600 DDEBUG timer: transaction: 2085 ms
2023-11-14T01:35:21+0600 DDEBUG Completion plugin: Generating completion cache...
2023-11-14T01:35:22+0600 INFO Installed products updated.
2023-11-14T01:35:22+0600 DEBUG Installed: nginx-1:1.20.1-14.el9_2.1.x86_64
2023-11-14T01:35:22+0600 DEBUG Installed: nginx-core-1:1.20.1-14.el9_2.1.x86_64
2023-11-14T01:35:22+0600 DEBUG Installed: nginxfilesystem-1:1.20.1-14.el9_2.1.noarch
2023-11-14T01:35:22+0600 INFO Complete!
2023-11-14T01:35:22+0600 DDEBUG Cleaning up.
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginxfilesystem-1.20.1-14.el9_2.1.noarch.rpm removed
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginx-1.20.1-14.el9_2.1.x86_64.rpm removed
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginx-core-1.20.1-14.el9_2.1.x86_64.rpm removed
2023-11-14T01:35:22+0600 DDEBUG Plugins were unloaded.
2023-11-14T01:35:22+0600 DDEBUG Plugins were unloaded.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Software uninstall Log
Location : /var/log dnf.log

```
Nov 14 02:24
encryptos@localhost:~$ sudo tail -f /var/log/dnf.log

2023-11-14T01:35:22+0600 DDEBUG Cleaning up.
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginxfilesystem-1.20.1-14.el9_2.1.noarch.rpm removed
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginx-1.20.1-14.el9_2.1.x86_64.rpm removed
2023-11-14T01:35:22+0600 DDEBUG /var/cache/dnf/rhel-9-for-x86_64-appstream-rpms-3dc6dc0880df5476/packages/nginx-core-1.20.1-14.el9_2.1.x86_64.rpm removed
2023-11-14T01:35:22+0600 DDEBUG Plugins were unloaded.
2023-11-14T02:23:05+0600 INFO --- logging initialized ---
2023-11-14T02:23:05+0600 DDEBUG Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install, download, generate_completion_cache, groups-manager, kpatch, needs-restart
ing, playground, product-id, repoclosure, repodiff, repograph, repomanage, reposync, subscription-manager, system-upgrade, updateassistant
2023-11-14T02:23:05+0600 INFO Updating Subscription Management repositories.
2023-11-14T02:23:07+0600 DDEBUG DNF version: 4.14.0
2023-11-14T02:23:07+0600 DDEBUG Command: dnf remove nginx
2023-11-14T02:23:07+0600 DDEBUG Installroot: /
2023-11-14T02:23:07+0600 DDEBUG Releasever: 9
2023-11-14T02:23:07+0600 DDEBUG cachedir: /var/cache/dnf
2023-11-14T02:23:07+0600 DDEBUG Base command: remove
2023-11-14T02:23:07+0600 DDEBUG Extra commands: ['remove', 'nginx']
2023-11-14T02:23:07+0600 DDEBUG User-Agent: constructed: 'libdnf (Red Hat Enterprise Linux 9.3; generic; Linux.x86_64)'
2023-11-14T02:23:07+0600 DDEBUG timer: sack setup: 275 ms
2023-11-14T02:23:07+0600 DDEBUG --> Starting dependency resolution
2023-11-14T02:23:07+0600 DDEBUG --> Finding unneeded leftover dependencies
2023-11-14T02:23:07+0600 DDEBUG --> Package nginx.x86_64 1:1.20.1-14.el9_2.1 will be erased
2023-11-14T02:23:07+0600 DDEBUG --> Package nginx-core.x86_64 1:1.20.1-14.el9_2.1 will be erased
2023-11-14T02:23:07+0600 DDEBUG --> Package nginxfilesystem.noarch 1:1.20.1-14.el9_2.1 will be erased
2023-11-14T02:23:07+0600 DDEBUG --> Finished dependency resolution
2023-11-14T02:23:07+0600 DDEBUG timer: depolve: 61 ms
2023-11-14T02:23:07+0600 INFO Dependencies resolved.
2023-11-14T02:23:07+0600 INFO =====
Package Arch Version Repository Size
-----
Removing:
  nginx x86_64 1:1.20.1-14.el9_2.1 [rhel-9-for-x86_64-appstream-rpms] 148 k
Removing unused dependencies:
  nginx-core x86_64 1:1.20.1-14.el9_2.1 [rhel-9-for-x86_64-appstream-rpms] 1.6 M
  nginxfilesystem noarch 1:1.20.1-14.el9_2.1 [rhel-9-for-x86_64-appstream-rpms] 0
Transaction Summary
-----
Remove 3 Packages

2023-11-14T02:23:07+0600 INFO Freed space: 1.7 M

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
Activities Terminal Nov 14 02:26
encryptos@localhost:~$ sudo tail -f /var/log/dnf.log

noarch 1:1.20.1-14.el9_2.1 @rhel-9-for-x86_64-appstream-rpms 0

Transaction Summary
=====
Remove 3 Packages

2023-11-14T02:23:07+0600 INFO Freed space: 1.7 M
2023-11-14T02:23:11+0600 INFO Running transaction check
2023-11-14T02:23:11+0600 INFO Transaction check succeeded.
2023-11-14T02:23:11+0600 INFO Running transaction test
2023-11-14T02:23:11+0600 INFO Transaction test succeeded.
2023-11-14T02:23:11+0600 DDEBUG timer: transaction test: 97 ms
2023-11-14T02:23:11+0600 INFO Running transaction
2023-11-14T02:23:11+0600 DDEBUG RPM transaction start.
2023-11-14T02:23:12+0600 DDEBUG RPM transaction over.
2023-11-14T02:23:12+0600 INFO --- logging initialized ---
2023-11-14T02:23:12+0600 DDEBUG timer: config: 3 ms
2023-11-14T02:23:13+0600 DDEBUG timer: verify transaction: 311 ms
2023-11-14T02:23:13+0600 DDEBUG timer: transaction: 1038 ms
2023-11-14T02:23:13+0600 DEBUG Completion plugin: Generating completion cache...
2023-11-14T02:23:13+0600 DEBUG Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install, download, generate_completion_cache, groups-manager, kpatch, needs-restart
ing, playground, product-id, repoclosure, repodiff, repograph, repomanage, reposync, subscription-manager, system-upgrade, uploadprofile
2023-11-14T02:23:13+0600 INFO Updating Subscription Management repositories.
2023-11-14T02:23:13+0600 INFO Installed products updated.
2023-11-14T02:23:13+0600 DEBUG Removed: nginx-1:1.20.1-14.el9_2.1.x86_64
2023-11-14T02:23:13+0600 DEBUG Removed: nginx-core-1:1.20.1-14.el9_2.1.x86_64
2023-11-14T02:23:13+0600 DEBUG Removed: nginxfilesystem-1:1.20.1-14.el9_2.1.noarch
2023-11-14T02:23:13+0600 INFO Complete!
2023-11-14T02:23:13+0600 DDEBUG Cleaning up.
2023-11-14T02:23:13+0600 DDEBUG Plugins were unloaded.
2023-11-14T02:23:15+0600 DEBUG DNF version: 4.14.0
2023-11-14T02:23:15+0600 DDEBUG Command: dnf makecache --timer
2023-11-14T02:23:15+0600 DDEBUG Installroot: /
2023-11-14T02:23:15+0600 DDEBUG Releasever: 9
2023-11-14T02:23:15+0600 DEBUG cachedir: /var/cache/dnf
2023-11-14T02:23:15+0600 DEBUG Base command: makecache
2023-11-14T02:23:15+0600 DDEBUG Extra commands: ['makecache', '--timer']
2023-11-14T02:23:15+0600 DEBUG Making cache files for all metadata files.
2023-11-14T02:23:15+0600 INFO Metadata cache refreshed recently.
2023-11-14T02:23:15+0600 DDEBUG Cleaning up.
2023-11-14T02:23:15+0600 DDEBUG Plugins were unloaded.

Package Arch Version Repository Size
-----
Removing:
  nginx-1:1.20.1-14.el9_2.1.x86_64 @rhel-9-for-x86_64-appstream-rpms 148 K
Removing unused dependencies:
  nginx-core-1:1.20.1-14.el9_2.1.x86_64 @rhel-9-for-x86_64-appstream-rpms 1.5 M
  nginxfilesystem-1:1.20.1-14.el9_2.1.noarch @rhel-9-for-x86_64-appstream-rpms 8 K

Transaction Summary
=====
Remove 3 Packages

Freed space: 1.7 M
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running scripts: nginx-1:1.20.1-14.el9_2.1.x86_64 1/1
                  nginx-core-1:1.20.1-14.el9_2.1.x86_64 1/1
                  nginxfilesystem-1:1.20.1-14.el9_2.1.noarch 1/1
Installed products updated.

Removed:
  nginx-1:1.20.1-14.el9_2.1.x86_64
  nginx-core-1:1.20.1-14.el9_2.1.x86_64
  nginxfilesystem-1:1.20.1-14.el9_2.1.noarch

Complete!
encryptos@localhost ~$
```

System time changed
Location: /var/log message

```
Activities Terminal Nov 14 8:05 PM
root@localhost:/var/log

Nov 14 20:50:00 localhost systemd-journald[762]: Time jumped backwards, rotating.
Nov 14 20:50:00 localhost rsyslogd[1149]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Nov 14 20:48:00 localhost systemd-timedated[3970]: Changed local time to Tue 2023-11-14 20:48:00 +06
Nov 14 20:48:00 localhost systemd-journald[762]: Time jumped backwards, rotating.
Nov 14 20:48:00 localhost rsyslogd[1149]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Nov 14 20:46:00 localhost systemd-timedated[3970]: Changed local time to Tue 2023-11-14 20:46:00 +06
Nov 14 20:46:00 localhost systemd-journald[762]: Time jumped backwards, rotating.
Nov 14 20:46:00 localhost rsyslogd[1149]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Nov 14 20:44:00 localhost systemd-timedated[3970]: Changed local time to Tue 2023-11-14 20:44:00 +06
Nov 14 20:44:00 localhost systemd-journald[762]: Time jumped backwards, rotating.
Nov 14 20:44:00 localhost rsyslogd[1149]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Nov 14 20:44:01 localhost systemd[1]: Starting SSSD Kerberos Cache Manager...
Nov 14 20:44:01 localhost systemd[1]: Started SSSD Kerberos Cache Manager.
Nov 14 20:44:01 localhost sssd_kcm[4141]: Starting up
Nov 14 20:44:30 localhost systemd[1]: systemd-timedated.service: Deactivated successfully.
Nov 14 20:44:30 localhost systemd[1]: Starting Time & Date Service...
Nov 14 20:44:30 localhost systemd[1]: Started Time & Date Service.
Nov 14 20:44:41 localhost systemd-timedated[4144]: chronyd.service: Enabling unit.
Nov 14 20:44:41 localhost systemd[1]: Reloading.
Nov 14 20:44:41 localhost systemd-rc-local-generator[4166]: /etc/rc.d/rc.local is not marked executable, skipping.
Nov 14 20:44:41 localhost systemd-timedated[4144]: Set NTP to enabled (chronyd.service).
Nov 14 20:44:41 localhost systemd[1]: Starting NTP client/server...
Nov 14 20:44:41 localhost chronyd[4179]: chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Nov 14 20:44:41 localhost chronyd[4179]: Frequency 13.093 +/- 0.360 ppm read from /var/lib/chrony/drift
Nov 14 20:44:41 localhost chronyd[4179]: Using right/UTC timezone to obtain leap second data
Nov 14 20:44:41 localhost chronyd[4179]: Loaded seccomp filter (level 2)
Nov 14 20:44:41 localhost systemd[1]: Started NTP client/server.
Nov 14 20:02:52 localhost chronyd[4179]: Selected source 182.16.156.5 (2.rhel.pool.ntp.org)
Nov 14 20:02:52 localhost systemd-journald[762]: Time jumped backwards, rotating.
Nov 14 20:02:52 localhost chronyd[4179]: System clock wrong by -2512.533802 seconds
Nov 14 20:02:52 localhost chronyd[4179]: System clock was stopped by -2512.533802 seconds
Nov 14 20:02:52 localhost chronyd[4179]: System clock TAI offset set to 37 seconds
Nov 14 20:02:52 localhost rsyslogd[1149]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Nov 14 20:02:52 localhost systemd-timedated[4144]: chronyd.service: Disabling unit.
Nov 14 20:02:52 localhost systemd[1]: Reloading.
Nov 14 20:02:52 localhost systemd-rc-local-generator[4199]: /etc/rc.d/rc.local is not marked executable, skipping.
Nov 14 20:02:52 localhost chronyd[4179]: chronyd exiting
Nov 14 20:02:52 localhost systemd-timedated[4144]: Set NTP to disabled.
Nov 14 20:02:52 localhost systemd[1]: Stopping NTP client/server...
Nov 14 20:02:52 localhost systemd[1]: chronyd.service: Deactivated successfully.
Nov 14 20:02:52 localhost systemd[1]: Stopped NTP client/server.
[root@localhost log]#
```

User creation

Location : /var/log/ secure

```
Nov 14 8:42 PM
root@localhost:/var/log

[root@localhost log]# ls
anaconda      boot.log-20231113  cups           hawkey.log-20231109  messages      rhsm           spooler-20231109  vmware-network.5.log  vmware-vmtoolsd-root.log
audit         boot.log-20231114  dnf.librepo.log  insights-client      messages-20231025  samba         ssd            vmware-network.6.log  wtmp
boot.log      btmp              dnf.log         kdump.log           messages-20231109  secure        tallylog        vmware-network.7.log
boot.log-20230819  btmp-20231109    dnf.rpm.log     lastlog             mount_dir        secure-20231025  tuned          vmware-network.8.log
boot.log-20231025  chrony           firewallld      lastlog             mysql            secure-20231109  vmware-network.1.log  vmware-network.9.log
boot.log-20231026  cron            gdm             maillog             private          speech-dispatcher  vmware-network.2.log  vmware-network.log
boot.log-20231109  cron-20231025    hawkey.log      maillog-20231025    qemu-ga         spooler         vmware-network.3.log  vmware-vgauthsvc.log.0
boot.log-20231111  cron-20231109    hawkey.log-20231025  maillog-20231109  README          spooler-20231025  vmware-network.4.log  vmware-vmtoolsd-root.log

[root@localhost log]# tail secure
Nov 14 20:00:56 localhost unix_chkpwd[3899]: password check failed for user (encryptos)
Nov 14 20:00:56 localhost gdm-password[3894]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=encryptos
Nov 14 20:00:56 localhost gdm-password[3894]: gkr-pam: the password for the login keyring was invalid.
Nov 14 20:01:05 localhost gdm-password[3902]: gkr-pam: unlocked login keyring
Nov 14 20:28:50 localhost gdm-password[4322]: gkr-pam: unlocked login keyring
Nov 14 20:37:35 localhost useradd[4377]: new group: name=rafi, GID=1001
Nov 14 20:37:35 localhost useradd[4377]: new user: name=rafi, UID=1001, GID=1001, home=/home/rafi, shell=/bin/bash, from=/dev/pts/0
Nov 14 20:39:40 localhost passwd[4388]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:39:59 localhost passwd[4391]: pam_unix(passwd:chauthtok): password changed for rafi
Nov 14 20:39:59 localhost passwd[4391]: gkr-pam: couldn't update the login keyring password: no old password was entered
[root@localhost log]#
```

User deletion

Location : /var/log/ secure

```
Nov 14 8:46 PM
root@localhost:/var/log

[root@localhost log]# ls
anaconda      boot.log-20231113  cups           hawkey.log-20231109  messages      rhsm           spooler-20231109  vmware-network.5.log  vmware-vmtoolsd-root.log
audit         boot.log-20231114  dnf.librepo.log  insights-client      messages-20231025  samba         ssd            vmware-network.6.log  wtmp
boot.log      btmp              dnf.log         kdump.log           messages-20231109  secure        tallylog        vmware-network.7.log
boot.log-20230819  btmp-20231109    dnf.rpm.log     lastlog             mount_dir        secure-20231025  tuned          vmware-network.8.log
boot.log-20231025  chrony           firewallld      lastlog             mysql            secure-20231109  vmware-network.1.log  vmware-network.9.log
boot.log-20231026  cron            gdm             maillog             private          speech-dispatcher  vmware-network.2.log  vmware-network.log
boot.log-20231109  cron-20231025    hawkey.log      maillog-20231025    qemu-ga         spooler         vmware-network.3.log  vmware-vgauthsvc.log.0
boot.log-20231111  cron-20231109    hawkey.log-20231025  maillog-20231109  README          spooler-20231025  vmware-network.4.log  vmware-vmtoolsd-root.log

[root@localhost log]# tail secure
Nov 14 20:00:56 localhost unix_chkpwd[3899]: password check failed for user (encryptos)
Nov 14 20:00:56 localhost gdm-password[3894]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=encryptos
Nov 14 20:00:56 localhost gdm-password[3894]: gkr-pam: the password for the login keyring was invalid.
Nov 14 20:01:05 localhost gdm-password[3902]: gkr-pam: unlocked login keyring
Nov 14 20:28:50 localhost gdm-password[4322]: gkr-pam: unlocked login keyring
Nov 14 20:37:35 localhost useradd[4377]: new group: name=rafi, GID=1001
Nov 14 20:37:35 localhost useradd[4377]: new user: name=rafi, UID=1001, GID=1001, home=/home/rafi, shell=/bin/bash, from=/dev/pts/0
Nov 14 20:39:40 localhost passwd[4388]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:39:59 localhost passwd[4391]: pam_unix(passwd:chauthtok): password changed for rafi
Nov 14 20:39:59 localhost passwd[4391]: gkr-pam: couldn't update the login keyring password: no old password was entered
[root@localhost log]# remove user rafi
bash: remove: command not found...
[root@localhost log]# userdel rafi
[root@localhost log]# tail secure
Nov 14 20:01:05 localhost gdm-password[3902]: gkr-pam: unlocked login keyring
Nov 14 20:28:50 localhost gdm-password[4322]: gkr-pam: unlocked login keyring
Nov 14 20:37:35 localhost useradd[4377]: new group: name=rafi, GID=1001
Nov 14 20:37:35 localhost useradd[4377]: new user: name=rafi, UID=1001, GID=1001, home=/home/rafi, shell=/bin/bash, from=/dev/pts/0
Nov 14 20:39:40 localhost passwd[4388]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:39:59 localhost passwd[4391]: pam_unix(passwd:chauthtok): password changed for rafi
Nov 14 20:39:59 localhost passwd[4391]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:46:05 localhost userdel[4421]: delete user 'rafi'
Nov 14 20:46:05 localhost userdel[4421]: removed group 'rafi' owned by 'rafi'
Nov 14 20:46:05 localhost userdel[4421]: removed shadow group 'rafi' owned by 'rafi'
[root@localhost log]#
```

Change user

Location : /var/log/ secure

```
Activities Terminal Nov 14 8:51 PM
root@localhost:/var/log

[demo@localhost log]$ uname -a
bash: uname: command not found...
[demo@localhost log]$ uname -a
Linux localhost.localdomain 5.14.0-362.8.1.el9_3.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Oct 3 11:12:36 EDT 2023 x86_64 x86_64 x86_64 GNU/Linux
[demo@localhost log]$ su encreptos
su: user encreptos does not exist or the user entry does not contain all the required fields
[demo@localhost log]$ exit
exit
[root@localhost log]# tail secure
Nov 14 20:39:59 localhost passwd[4391]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:46:05 localhost userdel[4421]: delete user 'rafi'
Nov 14 20:46:05 localhost userdel[4421]: removed group 'rafi' owned by 'rafi'
Nov 14 20:46:05 localhost userdel[4421]: removed shadow group 'rafi' owned by 'rafi'
Nov 14 20:48:35 localhost useradd[4431]: new group: name=demo, GID=1001
Nov 14 20:48:35 localhost useradd[4431]: new user: name=demo, UID=1001, GID=1001, home=/home/demo, shell=/bin/bash, from=/dev/pts/0
Nov 14 20:49:04 localhost passwd[4442]: pam_unix(passwd:chauthtok): password changed for demo
Nov 14 20:49:04 localhost passwd[4442]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:49:56 localhost su[4451]: pam_unix(su:session): session opened for user demo(uid=1001) by (uid=0)
Nov 14 20:50:45 localhost su[4451]: pam_unix(su:session): session closed for user demo
[root@localhost log]#
```

#User Password Change

Location : /var/log/ secure

```
Activities Terminal Nov 14 8:55 PM
root@localhost:/var/log

[root@localhost log]# passwd demo
Changing password for user demo.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost log]# tail secure
Nov 14 20:46:05 localhost userdel[4421]: removed group 'rafi' owned by 'rafi'
Nov 14 20:46:05 localhost userdel[4421]: removed shadow group 'rafi' owned by 'rafi'
Nov 14 20:48:35 localhost useradd[4431]: new group: name=demo, GID=1001
Nov 14 20:48:35 localhost useradd[4431]: new user: name=demo, UID=1001, GID=1001, home=/home/demo, shell=/bin/bash, from=/dev/pts/0
Nov 14 20:49:04 localhost passwd[4442]: pam_unix(passwd:chauthtok): password changed for demo
Nov 14 20:49:04 localhost passwd[4442]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov 14 20:49:56 localhost su[4451]: pam_unix(su:session): session opened for user demo(uid=1001) by (uid=0)
Nov 14 20:50:45 localhost su[4451]: pam_unix(su:session): session closed for user demo
Nov 14 20:55:04 localhost passwd[4518]: pam_unix(passwd:chauthtok): password changed for demo
Nov 14 20:55:04 localhost passwd[4518]: gkr-pam: couldn't update the login keyring password: no old password was entered
[root@localhost log]#
```