Linux Users, Groups, and Permissions

Hunter Kirk

Grand Canyon University College of Engineering and Technology

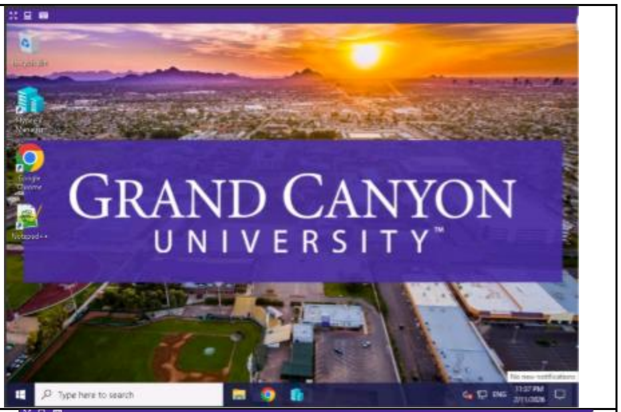
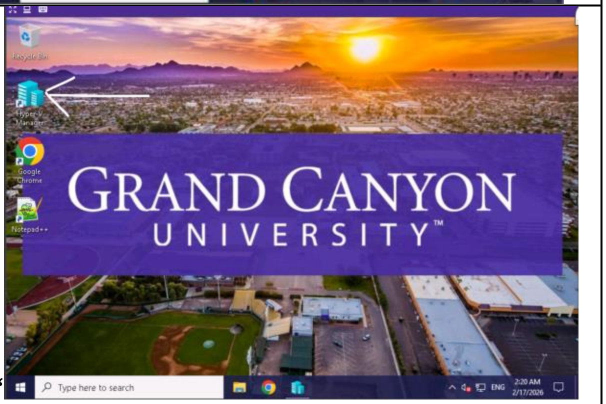
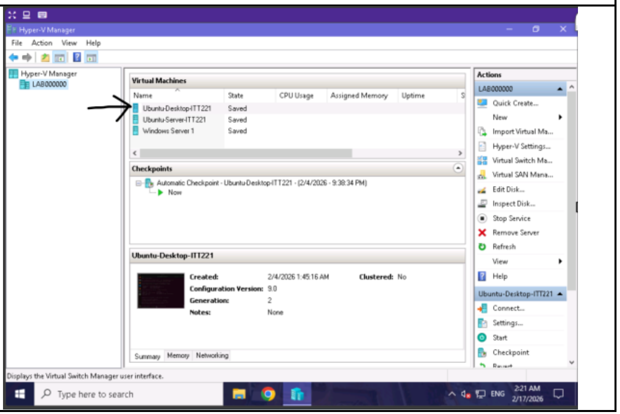
ITT 221: Linux System Administration and Maintenance

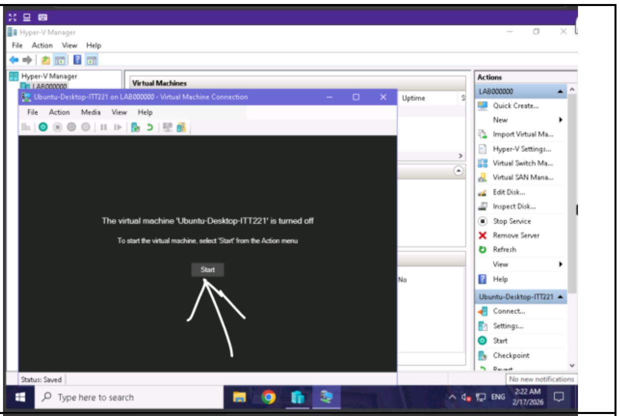
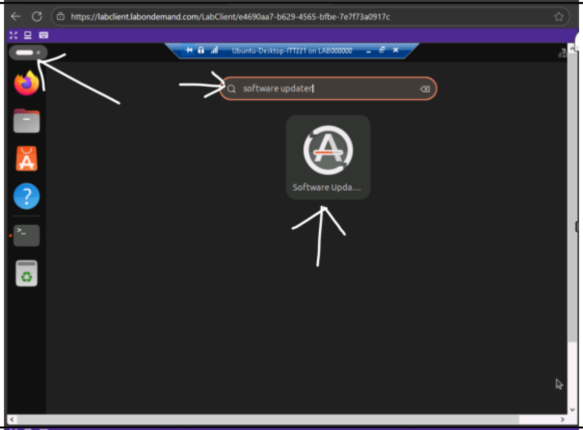
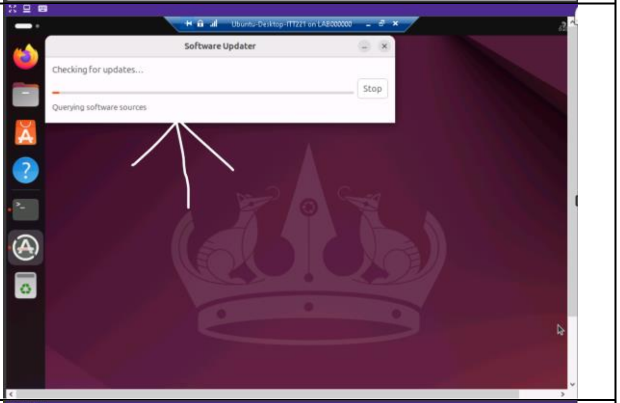
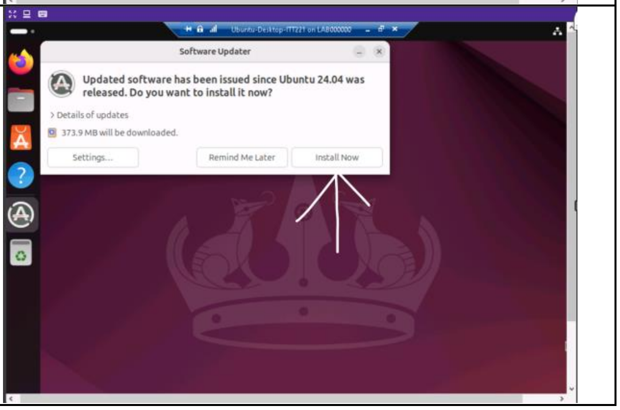
Professor: Aaron Jackson

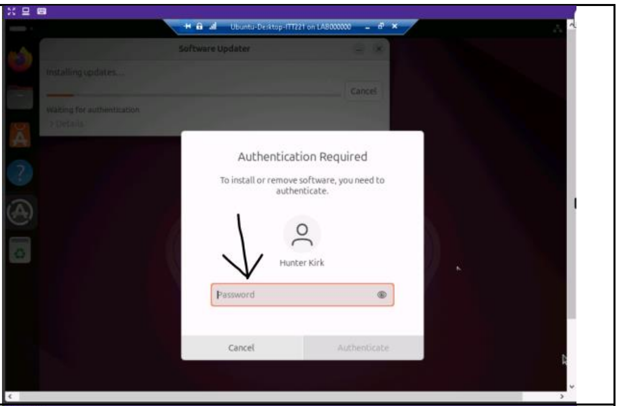
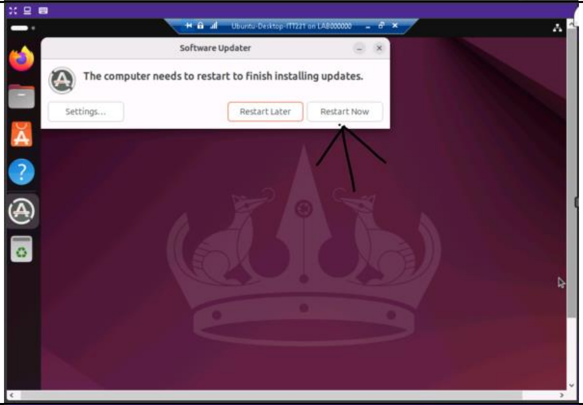
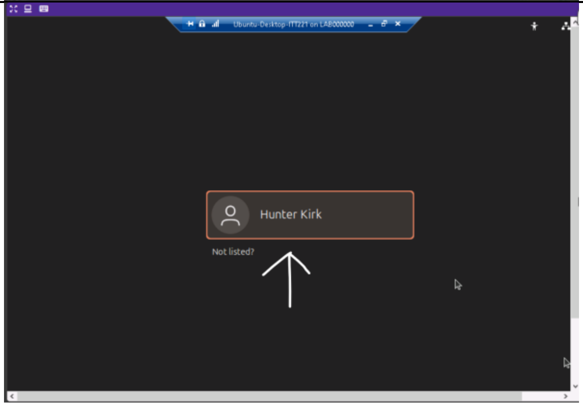
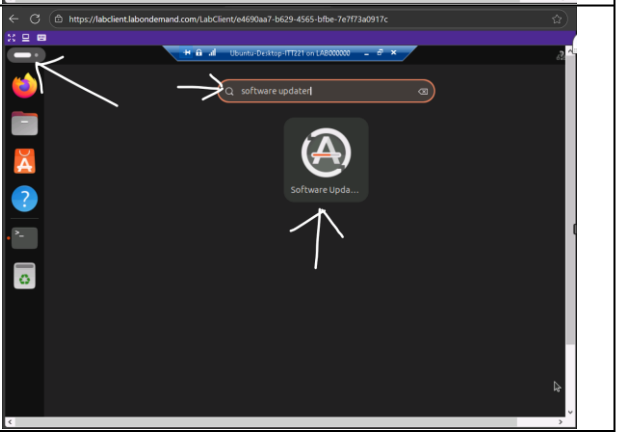
March 1st   2026

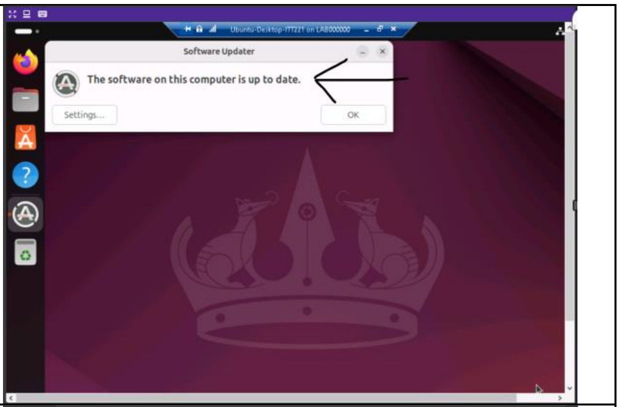
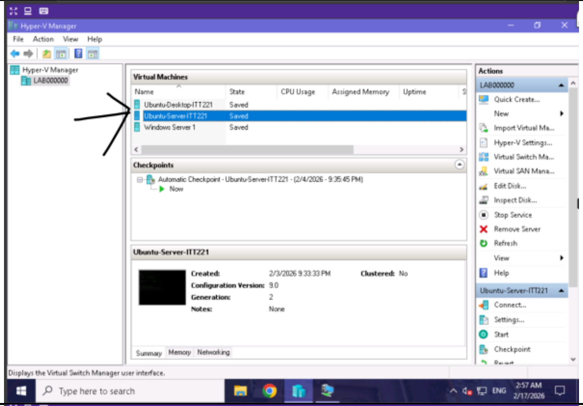
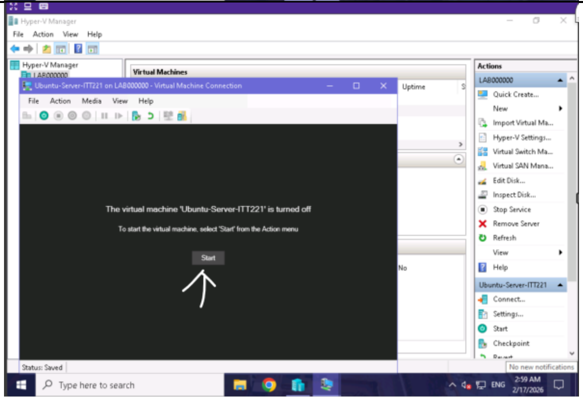
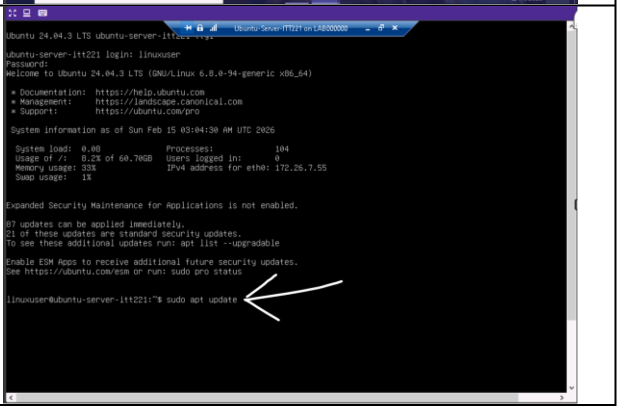
GRAND CANYON UNIVERSITY™

ITT-221 Step by Step Template

First, we will log into our Virtual Service	
Now we will launch Hyper-V Manager	“ 
“Double-Click" on the “Ubuntu Desktop” VM	 Hyper-V Manager Virtual Machines Name State CPU Usage Assigned Memory Uptime Ubuntu-Desktop-ITT221 Saved Ubuntu-Server-ITT221 Saved Windows Server 1 Saved Checkpoints Automatic Checkpoint - Ubuntu-Desktop-ITT221 - (2/4/2026 - 9:38:34 PM) Now Ubuntu-Desktop-ITT221 Created: 2/4/2026 1:45:16 AM Clustered: No Configuration Version: 9.0 Generation: 2 Notes: None Displays the Virtual Switch Manager user interface. File Action View Help Hyper-V Manager LAB000000 Actions LAB000000 Quick Create... New Import Virtual Ma... Hyper-V Settings... Virtual Switch Ma... Virtual SAN Mana... Edit Disk... Inspect Disk... Stop Service Remove Server Refresh View Help Ubuntu-Desktop-ITT221 Connect... Settings... Start Checkpoint Revert Summary Memory Networking Type here to search ENG 2:21 AM 2/17/2026

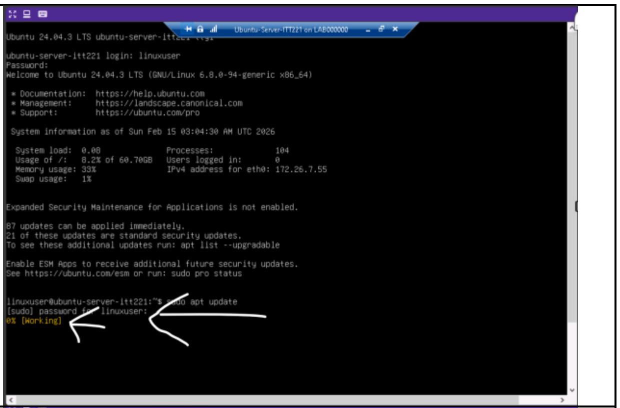
A pop-up menu will appear "click" the "Start" option	 Ubuntu-Desktop-ITT221 on LAB000000 - Virtual Machine Connection The virtual machine 'Ubuntu-Desktop-ITT221' is turned off To start the virtual machine, select 'Start' from the Action menu Start Status: Saved
Once you are logged into the "Ubuntu Desktop" in the top left corner click the "activities" option. A window will pop-up. In the search bar type "Software Updater" and "Launch" the application	 software updater Software Upda...
Once you "Launch" the application, your Ubuntu Desktop will automatically start updating your software.	 Software Updater Checking for updates... Stop Querying software sources
Once the Software Updater has finished checking for updates, you will be asked to install. "Click" the "Install" option	 Software Updater Updated software has been issued since Ubuntu 24.04 was released. Do you want to install it now? > Details of updates 373.9 MB will be downloaded. Settings... Remind Me Later Install Now

You will then be prompted to input your password. Put your password in and press “enter”	 Installing updates… Waiting for authentication Authentication Required To install or remove software, you need to authenticate. Hunter Kirk Ubuntu-Desktop-ITT221 on LAB000000 Software Updater Cancel Details Password Cancel Authenticate
Once the download is completed you will be asked the “restart” your VM. Press “restart”	 The computer needs to restart to finish installing updates. Ubuntu-Desktop-ITT221 on LAB000000 Software Updater Settings… Restart Later Restart Now
You will need to log back into your Ubuntu Desktop	 Ubuntu-Desktop-ITT221 on LAB000000 Hunter Kirk Not listed?
Once you are logged into go to the activities and open the software updater application again	 https://labclient.labondemand.com/LabClient/e4690aa7-b629-4565-bfbe-7e7f73a0917c software updater

The software updater will automatically check for updates. When it finished checking for updates you will get a message saying “Your system is up to date”	 Software Updater The software on this computer is up to date.
Log out of the Ubuntu Desktop. “Double-click" on the “Ubuntu Server” VM	 Virtual Machines Ubuntu-Desktop-ITT221 Saved Ubuntu-Server-ITT221 Saved Windows Server 1 Saved Checkpoints Automatic Checkpoint - Ubuntu-Server-ITT221 - (2/4/2026 - 9:35:45 PM) Now Ubuntu-Server-ITT221 Created: 2/3/2026 9:33:33 PM Configuration Version: 9.0 Generation: 2 Notes: None Clustered: No Displays the Virtual Switch Manager user interface.
A pop-up menu will appear “click” the “Start” option	 Ubuntu-Server-ITT221 on LAB000000 - Virtual Machine Connection The virtual machine 'Ubuntu-Server-ITT221' is turned off To start the virtual machine, select 'Start' from the Action menu Start Status: Saved
In the Command Terminal type “sudo apt update” and press “enter”	

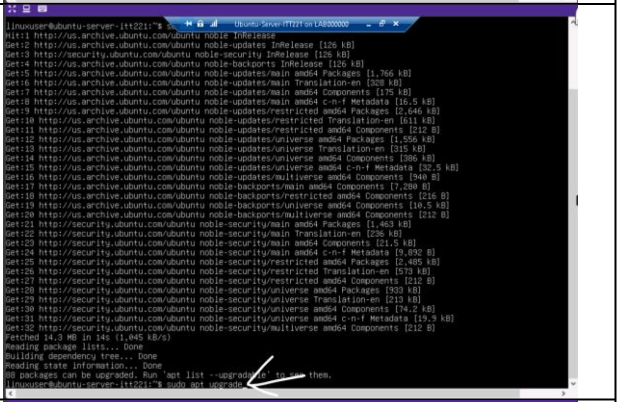
```
Ubuntu 24.04.3 LTS ubuntu-server-itt221 tty1

ubuntu-server-itt221 login: linuxuser
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Feb 15 03:04:30 AM UTC 2026

  System load:  0.08              Processes:             104
  Usage of /:   8.2% of 60.70GB   Users logged in:       0
  Memory usage: 33%               IPv4 address for eth0: 172.26.7.55
  Swap usage:   1%


Expanded Security Maintenance for Applications is not enabled.

87 updates can be applied immediately.
21 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


linuxuser@ubuntu-server-itt221:~$ sudo apt update
```

You will be prompted to input your password and press “enter”. You will then see a loading percentage in the next command line



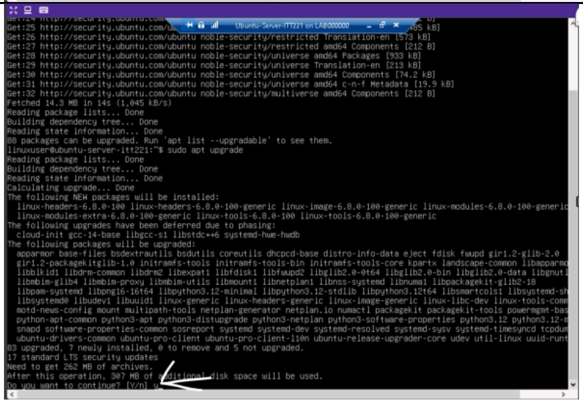
```
Ubuntu 24.04.3 LTS ubuntu-server-itt

ubuntu-server-itt221 login: linuxuser
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Feb 15 03:04:30 AM UTC 2026

  System load:  0.08              Processes:             104
  Usage of /:   8.2% of 60.70GB   Users logged in:       0
  Memory usage: 33%               IPv4 address for eth0: 172.26.7.55
  Swap usage:   1%


Expanded Security Maintenance for Applications is not enabled.

87 updates can be applied immediately.
21 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


linuxuser@ubuntu-server-itt221:~$ sudo apt update
[sudo] password for linuxuser:
0% [Working]
```

After the Ubuntu Server update is fully completed. Type “Sudo apt upgrade”



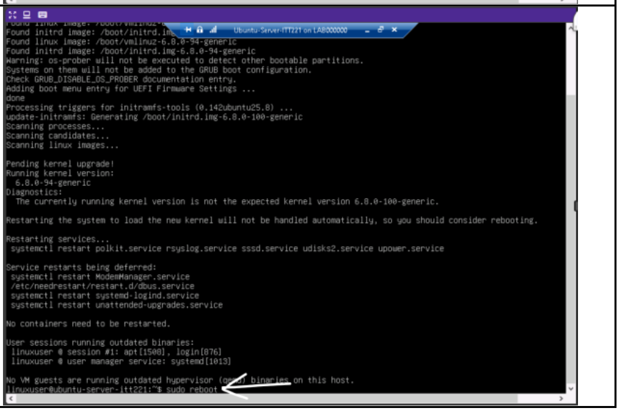
```
linuxuser@ubuntu-server-itt221:~$ s
Hit:1 http://us.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,766 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [328 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [16.5 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2,646 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [611 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:12 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,556 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [315 kB]
Get:14 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [386 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [32.5 kB]
Get:16 http://us.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:17 http://us.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,280 B]
Get:18 http://us.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:19 http://us.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [10.5 kB]
Get:20 http://us.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,463 kB]
Get:22 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [236 kB]
Get:23 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:24 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [9,092 B]
Get:25 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [2,485 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [573 kB]
Get:27 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:28 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [933 kB]
Get:29 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [213 kB]
Get:30 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [74.2 kB]
Get:31 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.9 kB]
Get:32 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 14.3 MB in 14s (1,045 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
88 packages can be upgraded. Run 'apt list --upgradable' to see them.
linuxuser@ubuntu-server-itt221:~$ sudo apt upgrade
```

You will be asked to continue type “Y” and press “enter”



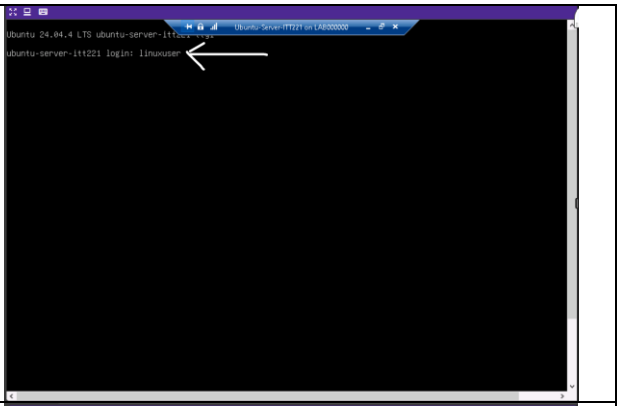
```
Get:24 http://security.ubuntu.com
Get:25 http://security.ubuntu.com/u                                              85 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [573 kB]
Get:27 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:28 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [933 kB]
Get:29 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [213 kB]
Get:30 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [74.2 kB]
Get:31 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.9 kB]
Get:32 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 14.3 MB in 14s (1,045 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
88 packages can be upgraded. Run 'apt list --upgradable' to see them.
linuxuser@ubuntu-server-itt221:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-headers-6.8.0-100 linux-headers-6.8.0-100-generic linux-image-6.8.0-100-generic linux-modules-6.8.0-100-generic
  linux-modules-extra-6.8.0-100-generic linux-tools-6.8.0-100 linux-tools-6.8.0-100-generic
The following upgrades have been deferred due to phasing:
  cloud-init gcc-14-base libgcc-s1 libstdc++6 systemd-hwe-hwdb
The following packages will be upgraded:
  apparmor base-files bsdextrautils bsdutils coreutils dhcpcd-base distro-info-data eject fdisk fwupd gir1.2-glib-2.0
  gir1.2-packagekitglib-1.0 initramfs-tools initramfs-tools-bin initramfs-tools-core kpartx landscape-common libapparmo
  libblkid1 libdrm-common libdrm2 libexpat1 libfdisk1 libfwupd2 libglib2.0-0t64 libglib2.0-bin libglib2.0-data libgnutl
  libmbim-glib4 libmbim-proxy libmbim-utils libmount1 libnetplan1 libnss-systemd libnuma1 libpackagekit-glib2-18
  libpam-systemd libpng16-16t64 libpython3.12-minimal libpython3.12-stdlib libpython3.12t64 libsmartcols1 libsystemd-sh
  libsystemd0 libudev1 libuuid1 linux-generic linux-headers-generic linux-image-generic linux-libc-dev linux-tools-comm
  motd-news-config mount multipath-tools netplan-generator netplan.io numactl packagekit packagekit-tools powermgmt-bas
  python-apt-common python3-apt python3-distupgrade python3-netplan python3-software-properties python3.12 python3.12-m
  snapd software-properties-common sosreport systemd systemd-dev systemd-resolved systemd-sysv systemd-timesyncd tcpdum
  ubuntu-drivers-common ubuntu-pro-client ubuntu-pro-client-l10n ubuntu-release-upgrader-core udev util-linux uuid-runt
83 upgraded, 7 newly installed, 0 to remove and 5 not upgraded.
17 standard LTS security updates
Need to get 262 MB of archives.
After this operation, 307 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Once your Ubuntu Server is fully updated in the command line type “sudo reboot” and press “enter”



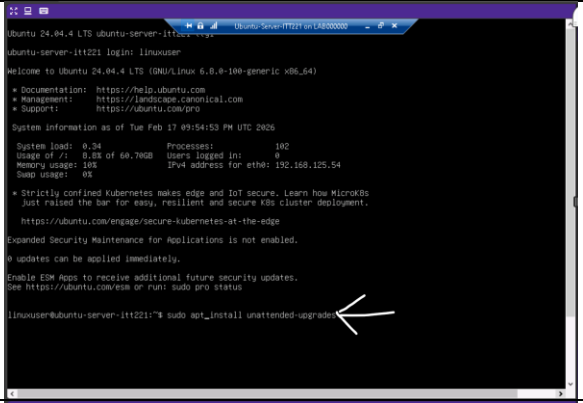
```
Found linux image: /boot/vmlinuz-6
Found initrd image: /boot/initrd.im
Found linux image: /boot/vmlinuz-6.8.0-94-generic
Found initrd image: /boot/initrd.img-6.8.0-94-generic
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
Processing triggers for initramfs-tools (0.142ubuntu25.8) ...
update-initramfs: Generating /boot/initrd.img-6.8.0-100-generic
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
Running kernel version:
  6.8.0-94-generic
Diagnostics:
  The currently running kernel version is not the expected kernel version 6.8.0-100-generic.

Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.

Restarting services...
 systemctl restart polkit.service rsyslog.service sssd.service udisks2.service upower.service

Service restarts being deferred:
 systemctl restart ModemManager.service
 /etc/needrestart/restart.d/dbus.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
 linuxuser @ session #1: apt[1500], login[876]
 linuxuser @ user manager service: systemd[1013]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
linuxuser@ubuntu-server-itt221:~$ sudo reboot
```

After the Ubuntu Server reboots, you will need to log back in. Type your username and password and press “enter”



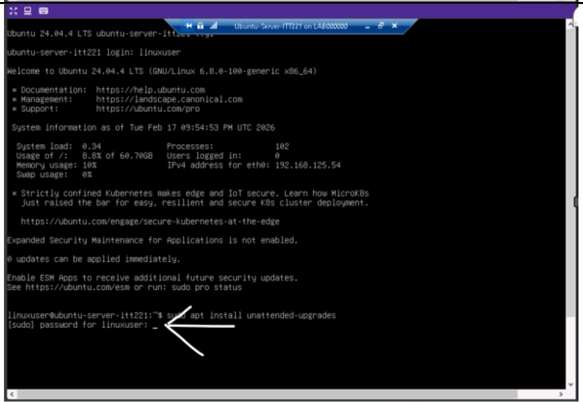
```
Ubuntu 24.04.4 LTS ubuntu-server-itt221 tty1

ubuntu-server-itt221 login: linuxuser
```

After login into the Ubuntu Server in the command line type “sudo apt install unattended-upgrades" and press “enter”



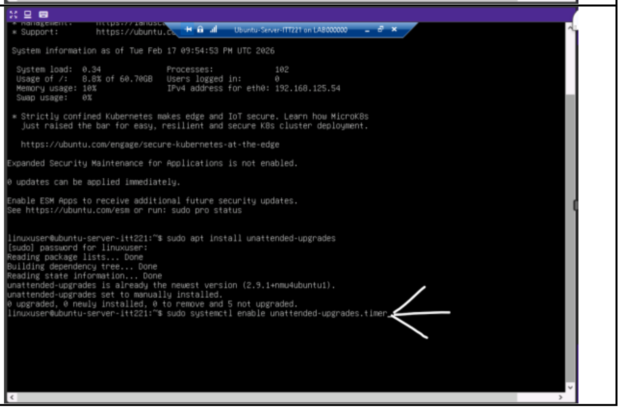
```
Ubuntu 24.04.4 LTS ubuntu-server-itt221 tty1

ubuntu-server-itt221 login: linuxuser

Welcome to Ubuntu 24.04.4 LTS (GNU/Linux 6.8.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb 17 09:54:53 PM UTC 2026

  System load:  0.34              Processes:             102
  Usage of /:   8.8% of 60.70GB   Users logged in:       0
  Memory usage: 10%               IPv4 address for eth0: 192.168.125.54
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


linuxuser@ubuntu-server-itt221:~$ sudo apt_install unattended-upgrades
```

You will be asked to input your password. Type your password and then press “enter”



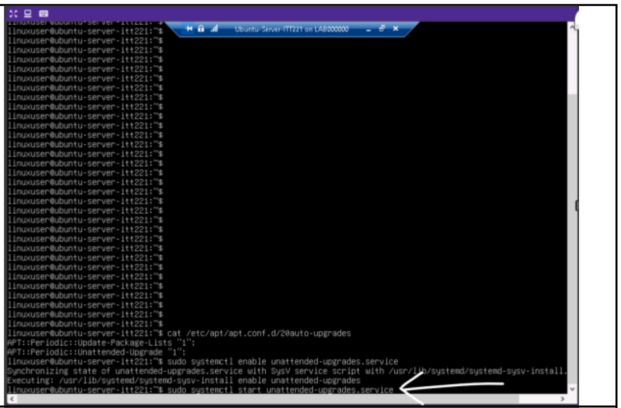
```
Ubuntu 24.04.4 LTS ubuntu-server-itt221 tty1

ubuntu-server-itt221 login: linuxuser

Welcome to Ubuntu 24.04.4 LTS (GNU/Linux 6.8.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb 17 09:54:53 PM UTC 2026

  System load:  0.34              Processes:             102
  Usage of /:   8.8% of 60.70GB   Users logged in:       0
  Memory usage: 10%               IPv4 address for eth0: 192.168.125.54
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


linuxuser@ubuntu-server-itt221:~$ sudo apt install unattended-upgrades
[sudo] password for linuxuser: _
```

Once your Ubuntu Server is finished installing the unattended-upgrades. In the next command line type “sudo systemctl enable unattended-upgrades.timer” and press “enter”



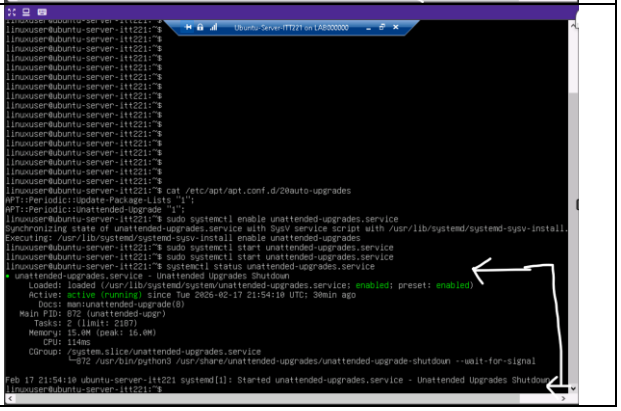
```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb 17 09:54:53 PM UTC 2026

  System load:  0.34              Processes:             102
  Usage of /:   8.8% of 60.70GB   Users logged in:       0
  Memory usage: 10%               IPv4 address for eth0: 192.168.125.54
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


linuxuser@ubuntu-server-itt221:~$ sudo apt install unattended-upgrades
[sudo] password for linuxuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.9.1+nmu4ubuntu1).
unattended-upgrades set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
linuxuser@ubuntu-server-itt221:~$ sudo systemctl enable unattended-upgrades.timer
```

After running the previous command, you will get a message stating that the command is now enabled. Now in the command line type “sudo systemctl start unattended-upgrades.timer” and press “enter”



```
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$ cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
linuxuser@ubuntu-server-itt221:~$ sudo systemctl enable unattended-upgrades.service
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable unattended-upgrades
linuxuser@ubuntu-server-itt221:~$ sudo systemctl start unattended-upgrades.service
```

After inputting both commands to ensure proper function in the next command line type “systemctl status unattedned-upgrades.service” to verify that the command is working properly



```
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$
linuxuser@ubuntu-server-itt221:~$ cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
linuxuser@ubuntu-server-itt221:~$ sudo systemctl enable unattended-upgrades.service
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable unattended-upgrades
linuxuser@ubuntu-server-itt221:~$ sudo systemctl start unattended-upgrades.service
linuxuser@ubuntu-server-itt221:~$ sudo systemctl start unattended-upgrades.service
linuxuser@ubuntu-server-itt221:~$ systemctl status unattended-upgrades.service
● unattended-upgrades.service - Unattended Upgrades Shutdown
     Loaded: loaded (/usr/lib/systemd/system/unattended-upgrades.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-02-17 21:54:10 UTC; 30min ago
       Docs: man:unattended-upgrade(8)
   Main PID: 872 (unattended-upgr)
      Tasks: 2 (limit: 2187)
     Memory: 15.0M (peak: 16.0M)
        CPU: 114ms
     CGroup: /system.slice/unattended-upgrades.service
             └─872 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal

Feb 17 21:54:10 ubuntu-server-itt221 systemd[1]: Started unattended-upgrades.service - Unattended Upgrades Shutdown
linuxuser@ubuntu-server-itt221:~$
```

Questions

1. Why should a system administrator review the list of packages after apt update is run?

System administrators should review the list of packages after running “apt update” in the command line to fully understand what will be changed and the appropriate actions needed to correct any configuration issues. The reason is that when you run the “apt update”, the OS pulls all the latest versions of each component. Once reviewed, an administrator can run the “apt upgrade” to upgrade the OS to the latest version. For example, if an administrator does not review the packages being updated, there may be configuration issues with manually configured software in the system, and the administrator may lose access or misconfigure it. It is an important task for administrators to not only update the packages but also review them to ensure the systems' stability. This not only allows the administrator to know what problems may arise, but also allows the system to stay up to date on security features and any configuration issues (Islam, 2023)

2. As a Linux system administrator managing patching, what is a key risk to evaluate during implementation and a single strategy to mitigate it?

One of the biggest risks for patch management is downtime. In the corporate world, any unnecessary downtime is viewed as a loss of profits. This risk can be avoided by scheduling times when administrators can set up dates and times to update the system without interrupting daily operations (*Linux Security Patches: Best Practices for Risk-Mitigation and Uptime | Ubuntu*, 2026). Not only can the time of day for updates play a major factor, but also whether an administrator reviews what is changing or being implemented during the update, as this can break critical applications used in daily operations. One strategy to mitigate this issue is to test the patch on an internal virtual machine before deploying it to the main network (Souppaya & Scarfone, 2013). This allows administrators the ability to make critical changes before the update. Another strategy to mitigate this risk is to schedule the update for a time when administrators can push it with minimal or no network traffic present. This allows administrators to make these configuration changes and test critical applications for further refinement without worrying about downtime or a flood of work order tickets for certain work-based applications.

References:

Islam, A. (2023, August 21). *A Complete Overview of "sudo apt update" Command in Linux*. LinuxSimply. https://linuxsimply.com/linux-basics/package-management/update-packages/sudo-apt-update/

Linux security patches: best practices for risk-mitigation and uptime | Ubuntu. (2026). Ubuntu. https://ubuntu.com/engage/ensure-security-and-uptime-when-patching-linux-vulnerabilities

Souppaya, M., & Scarfone, K. (2013). Guide to Enterprise Patch Management Technologies. *NIST Special Publication 800-40 Revision 3*. https://doi.org/10.6028/nist.sp.800-40r3