institute
of mine
seismology

Installation and configuration of the Ubuntu 20.04 operating system for IMS servers

September 25, 2020

Document Number:
IMS-SERVER-INSTALL-UBUNTU-20-04-LTS-202009-RE-v1

Contents

NOTE: All sections marked with * can be skipped when installing on a virtual server

1 Introduction

The purpose of this document is to document the procedure for installing and configuring the operating system of IMS Servers. For the recommended server specifications, please refer to the following document:
http://software.imseismology.org/documents/PC-Specification_IMS-DOC-201201-IL.pdf

For general IT requirements needed by the seismic system, please refer to the following document:
http://software.imseismology.org/documents/IT/IMS_IT_requirements.pdf

If the operating system is not being installed by IMS, this guide should be completed to the end of Section 6: Update Ubuntu, at which point IMS will complete the system configuration.

2 Preparation

2.1 Create Ubuntu Boot Media

The version of Ubuntu to be installed is:

- Latest Ubuntu Server 20.04.x LTS (64-bit) (currently Ubuntu Server 20.04 LTS)
  - 64 bit version (for 64 bit hardware)
  - Ubuntu Server edition does not support 32bit architecture

The boot media can be created using a USB disk or CD:

Download the correct ISO image from one of the following sites:

- http://software.imseismology.org/os/ubuntu-20.04.x-live-server-amd64.iso
- http://www.ubuntu.com/download/server

Create the bootable USB or CD image from the downloaded ISO image file. The recommended method within a Linux OS is to image a USB flash drive using the **dd** command (images created with Ubuntu startup disk creator are known to have some issues) (root privileges required).

```
sudo dd if=<iso_file.iso> of=/dev/<device>
```

Example:

```
$ sudo dd if=ubuntu-20.04-server-amd64.iso of=/dev/sdd
```

Note: Ensure that you specify the correct drive as depending on the PC it may be `/dev/sdb` or `/dev/sdc`

If creating a boot CD/DVD from within a Windows OS, burn the ISO image to the CD/DVD

2.2 Network details

As part of the server configuration process, the operating system and software packages will be updated to their most recent versions by downloading updates from the Internet. You will therefore need to connect the server to the Internet and have the network configuration details available before proceeding.

- Dynamic network configuration via DHCP:
  - Host name
  - Proxy settings if applicable (IP, port, authentication details, etc.)

or

- Static network configuration:
  - hostname
  - IP address and netmask
  - DNS IP address
  - DNS domain
  - Gateway IP address
  - Proxy settings if applicable (IP, port, authentication details, etc.)

3 Hardware Configuration *

3.1 Set PC BIOS

- Boot PC
- Enter BIOS
- Set boot sequence to CD or USB first
- Set **Hardware Clock** to **UTC (GMT) - this can be more accurately set in section 7.11.**
- Set **AC Recovery** to **on**
- Enable **Hyper-Threading** (if option available)
- Ensure that if the PC has an on-board serial port, this is set to **COM1**
- If the system supports **UEFI**, turn it **on**
- Disable **Secure Boot** (if option available) - If enabled it may cause the MOXA driver installation to fail.
- Disable the **Windows Boot Manager** (if option available)

3.2 RAID

If the system is planned for a RAID configuration

- Boot PC
- Enter Boot Menu
- Select Device Configuration
- Use the right arrow key to select “AVAGO Mega RAID...”

Only configure RAID if the PC has a dedicated **hardware** RAID controller. Do **NOT** configure software raid. During virtual disk configuration, the virtual disk should be initialised.

- For a configuration with 2 physical hard drives, create 1 virtual disk using RAID 1
- For a configuration with 4 physical hard drives, create 2 virtual disks using RAID 1

4 Install Ubuntu

Ubuntu Server does not assume that the machine has a graphical interface (i.e. may be installed via a terminal), all the installers user interaction is via keyboard interactive text based menus. Control keys are usually documented on the bottom of screen; usually <TAB> moves between fields, <SPACE> selects and <ENTER> activates fields.

4.1 Boot from Ubuntu Boot Media

- With the boot media (created in step 2.1) inserted into the machine, boot from the the device (you may need to enter the BIOS boot menu to select the correct boot device).
- Select your language and then from the boot menu select "Install Ubuntu Server".

4.2 Select Locale Settings

- language (English)
- location (**not** the end user/customer's timezone, but the local one where the machine is being setup - this is important because Ubuntu uses this setting to select the best software package repository servers to use based on region)
- keyboard (follow the interactive menus to detect your keyboard)

4.3 Configure the Network

Once the keyboard has been configured, the installer will scan and detect the machine's hardware configuration and may load the required drivers from the installation media. As part of this hardware detection process the machine's network interfaces should be detected. It is recommended that at this point, the PC does not have access to the Internet. To speed up Ubuntu installation time and reliability, updates should not be performed until after the OS is fully installed.

- If disconnected from a network the auto-configuration will fail. In this case, select "Do not configure the network at this time"
- Enter the hostname for this system. This is usually set to be the same as the ims user password which is in the format of <customer short name>ims1 e.g. tstims1

4.4 Create IMS User Account

- Full name of user: IMS
- username: ims
- password: <usually same as hostname>
  - You may be prompted with a message telling you that the password chosen is too weak, select **Yes** to bypass the prompt and continue using the entered password.
- encrypt /home partition: No

4.5 Timezone

The timezone should be configured to reflect the **current location** (not the final location) of the PC being installed as this will allow the closest, fastest update repositories to be used. Once the PC is on site, the timezone should be adjusted to reflect the site's location.

4.6 Disk Partitioning

The following subsections show specific partition details for both physical servers and virtual servers. Please be sure to follow the partitioning applicable to the machine type and disk setup being used.

4.6.1 Physical machine partitioning

- select **manual** partitioning
- follow the interactive menus to partition the disks as follows:
  - for a multi-disk system (with or without raid) put /data and /home on a second or third disk
  - delete all existing partitions if the PC has a pre-installed OS
  - if this is an upgrade preserve /data and /home
  - for systems supporting UEFI (recommended), the first partition should be an EFI boot partition of 1 GB
  - for systems NOT supporting UEFI, the first partition should be 1GB mounted to /boot
  - if the disk sizes are below 1TB, the size of the /home partition might need to be adjusted to ensure the /data partition is large enough for long-term data storage

– create partitions according to the following table (example partition sizes based on a minimum disk size of 1TB):

NOTE: Only use one boot option depending on the BIOS configuration.
(EFI boot OR BIOS boot)

Description	Disk		Mount-point	Type	Primary/ Logical	Size
	2 HDDs	1 HDD				
EFI boot **or** BIOS boot	1	1	/boot	EFI boot ext4	Primary	1GB
Root partition	1	1	/	ext4	Primary	50GB
Log files and spool data	1	1	/var	ext4	Logical	50GB
Swap space	1	1	-	swap	Logical	2 x RAM (max 32GB)
IMS spare data area	1	n/a	/data1	ext4	Logical	rest of drive
Home directory	2	1	/home	ext4	Primary	250GB
IMS data area	2	1	/data	ext4	Logical	rest of drive

Table 1: Minimum partition sizes for a 1 or 2 disk system.

Note: Correct disk partition sizes are critical to the long-term stability of the system, please contact IMS Support if unsure of what partition sizes to use.

4.6.2 Virtual machine partitioning

- select **manual** partitioning
- follow the interactive menus to partition the disks as follows:
  - if this is an upgrade preserve /data and /home
  - for systems supporting UEFI (recommended), the first partition should be an EFI boot partition of 1 GB
  - for systems NOT supporting UEFI, the first partition should be 1GB mounted to /boot
  - create partitions according to the following table (example partition sizes based on a minimum disk size of 400GB for disk 1 and 1TB for disk 2):

NOTE: Only use one boot option depending on the BIOS configuration.
(EFI boot OR BIOS boot)

Description	Disk	Mount-point	Type	Primary/Logical	Size
EFI boot **or** BIOS boot	1	 /boot	EFI boot ext4	Primary	1GB
Root partition	1	/	ext4	Primary	50GB
Log files and spool data	1	/var	ext4	Logical	50GB
Swap space	1	-	swap	Logical	2 x RAM (max 32GB)
Home directory	1	/home	ext4	Primary	rest of drive
IMS data area	2	/data	ext4	Logical	entire drive

Table 2: Minimum partition sizes for 2 virtual disk system.

Note: Correct disk partition sizes are critical to the long-term stability of the system, please contact IMS Support if unsure of what partition sizes to use.

4.7 Proxy Settings

When prompted to enter HTTP proxy information, enter the required details or leave blank and continue with the installation if proxy server is not used.

4.8 Updates

When prompted to configure system updates ("Configuring tasksel") ensure that automatic updates are disabled.

- Select **No automatic updates**

4.9 Additional Software Selection

When prompted to select additional software packages for installation, select the **OpenSSH Server** package leave the rest unselected.

- Use the arrow keys and press **spacebar** to select **OpenSSH Server** and then **enter** to continue with the installation.

4.10 Installation Complete

- When prompted, select **Continue** to finish the installation and restart into Ubuntu.
- When inquired, install GRUB boot loader on same drive as operating system.

5 Network Settings

After Ubuntu installation, edit the `/etc/netplan/01-netcfg.yaml` file and configure the network settings for all network interfaces. Use the example network interfaces file as a starting point, available from: http://software.imseismology.org/documents/System/01-netcfg.yaml

Note: The functional lines in this file MUST be indented as per the template otherwise the network interfaces will not function.

After updating or replacing the file, run the following command to apply the new settings.

```
sudo netplan apply
```

6 Update Ubuntu

Update the Ubuntu installation:

```
sudo apt-get update
sudo apt-get dist-upgrade
```

7 Server Preparation

7.1 Create root password

Normally Ubuntu does not have a login for root - all access is via the sudo command using the ims password. For some cases a root login is useful. The following commands will create the root login:

```
sudo passwd
```

- enter the ims root password when prompted
- enter the technical services root password (twice) when prompted

7.2 Additional Packages required by IMS

7.2.1 Ubuntu Extras (compulsory)

A number of additional packages are required by the IMS system. A script named `ubuntu_extras.sh` is available to install these packages; the latest version of the script can be downloaded from:
http://software.imseismology.org/os/ubuntu_extras_2004.sh

Run the script, it will determine the package dependencies and install them.

```
chmod +x ubuntu_extras_2004.sh
./ubuntu_extras_2004.sh
```

Follow the interactive menus, answering Yes if asked to install additional packages.

The postfix installation will ask for some information:

- select **OK**
- select **local only**
- system mail name - leave as default <**hostname**>

After the script has completed, a log file will be written to disk (in the same directory from which the script was run) which summaries the packages installed. Check that all packages were installed correctly. It is recommended that this log file gets copied to the directory:
`/home/ims/Documents/InstallationRecords`

7.2.2 Ubuntu Extras - GUI addon (disable by default for ALL servers)

To install the Ubuntu GUI packages, run the script named `ubuntu_extras_2004_gui_addon.sh` which is available for download from:
http://software.imseismology.org/os/ubuntu_extras_2004_gui_addon.sh

- Run the script:

```
chmod +x ubuntu_extras_2004_gui_addon.sh
./ubuntu_extras_2004_gui_addon.sh
```

- When prompted, select LightDM from the list of display managers (GDM3 may be a second option, do not select this).
- After the script has completed, a log file will be written to disk which summaries the packages installed. Check that all packages were installed correctly. It is recommended that this log file gets copied to the directory: `/home/ims/Documents/InstallationRecords`
- Reboot the system and then proceed to install the required graphics drivers (DSS only).
  - In the "Software and Updates" menu, select "Additional Drivers"; the appropriate graphics drivers should be automatically detected. Apply the changes and restart the system.
    - Note: If no recommended drivers are displayed in this menu, download and install from the manufacturers webpage.
- Once the GUI is fully configured disable it using the following command, this is the state that all servers should be shipped in, both DSS and RMS.

```
systemctl set-default multi-user.target
```

- If the GUI must be re-enabled at any point due to customer specific requirements, use the following command:

```
systemctl set-default graphical.target
```

7.2.3 3D drivers (Desktop PC Synapse server only)

If the GUI is to be enabled on a desktop seismic server the 3D drivers should be installed following the enabling of the GUI. This can be done using the following steps.

1. When logged into Ubuntu using the GUI, select "Activities" from the top left of the screen
2. In the search field type "software & updates" and select the application
3. From the top tabs select "Additional Drivers"
4. Wait for the list to be populated with the available drivers
5. Select and apply the latest "(open source)" driver

7.2.4 Disable Automatic System Updates (compulsory)

After all additional packages have been installed, disable automatic installation of updates. This should only be completed **after** all updates and packages have been installed.

From the command line as root (sudo), edit the file `/etc/apt/apt.conf.d/10periodic` and ensure the contents are the same as the below:

```
APT::Periodic::Unattended-Upgrade "0";
APT::Periodic::Update-Package-Lists "0";
APT::Periodic::Download-Upgradeable-Packages "0";
APT::Periodic::AutocleanInterval "0";
```

7.3 DELL Hardware RAID utility, `megacli` for PERC (if available) *

If the disk controller is a Dell PERC H series hardware RAID controller, then install the `megacli` utility to enable monitoring or changing the disk status.

A version of the package for Ubuntu 20.04 is available at URL:
http://software.imseismology.org/os/

Install with `sudo dpkg -i megacli*.deb`, there should be no problems with dependencies.

To find the device ID's of the installed disks and check their status, run

```
sudo megacli -PDList -a0
```

7.4 Configure smart monitoring tools *

7.4.1 For RAID system

The `smartmontools` package should have been installed in step 7.2 above and running `megacli` creates the device file `/dev/megaraid_sas_ioctl_node` which the smart utilities use. Perform the following steps to check that the error counts for all disks are 0.

Run the following command to list the megaraid IDs, and their corresponding SCSI device.

```
sudo smartctl --scan
```

Note: The output should look similar to the following (megaraid ID in Underline, SCSI device in **Bold**)

```
/dev/sda -d scsi # /dev/sda, SCSI device
/dev/bus/0 -d megaraid,8 # /dev/bus/0 [megaraid_disk_09], SCSI device
/dev/bus/0 -d megaraid,9 # /dev/bus/0 [megaraid_disk_09], SCSI device
```

Run the following command to check for error counts.

```
sudo smartctl -a -d megaraid,<megaraid ID> <SCSI device>
```

The above command should list the S.M.A.R.T. info for the specified disk. Repeat for all disk IDs listed by `smartctl {scan`.

To enable continuous monitoring by `smartd`, add a line like the example below to `/etc/smartd.conf` for each disk.

```
<SCSI device> -d megaraid,<megaraid ID> -a
```

Ensure that smartd will be started at boot by uncommenting or adding the following line in: `/etc/default/smartmontools` (edit as root).

```
start_smartd=yes
```

Also, to ensure that the `smartd` messages are reported by `logwatch`.
Create a file `/etc/logwatch/conf/services/smartd.conf` with the following line.

```
LogFile = syslog
```

Add an entry to root's cron to run the above `megacli` command once a day.

```
su (enter ts root password)
crontab -e
```

At the bottom of the the cron table enter the following.

```
3 3 * * * /usr/sbin/megacli -PDList -aAll >/dev/null 2<&1
```

Optionally, divert root's mail to someone who would like to receive disk error notificaitons, by setting an alias in `/etc/aliases`, and running the command `newaliases`.

7.4.2 For non-RAID system

The `smartmontools` package should have been installed in step 7.2 above. Perform the following steps to check that the error counts for all disks are 0.

Run the following command to list the SCSI devices.

```
sudo smartctl --scan
```

Note: The output should look similar to the following (SCSI device in **Bold**)

```
/dev/sda -d scsi # /dev/sda, SCSI device
```

Run the following command to check for error counts.

```
sudo smartctl -a <SCSI device>
```

The above command should list the S.M.A.R.T. info for the specified disk. Repeat for all disks listed by `smartctl {scan`.

To enable continuous monitoring by `smartd`, add a line like the example below to `/etc/smartd.conf` for each disk.

```
<SCSI device> -a
```

Ensure that smartd will be started at boot by uncommenting or adding the following line in: `/etc/default/smartmontools` (edit as root).

```
start_smartd=yes
```

Also, to ensure that the `smartd` messages are reported by `logwatch`.
Create a file `/etc/logwatch/conf/services/smartd.conf` with the following line.

```
LogFile = syslog
```

7.5 Grub Configuration

- Edit the following file (root privileges required):

```
/etc/default/grub
```

- Add the following lines at the end of the file:

```
# If this option is set, it overrides the default
# recordfail setting. The default setting is -1,
# which causes GRUB to wait for user input.
# This option should be set on headless and appliance
# systems where access to a console is restricted
# or limited.
GRUB_RECORDFAIL_TIMEOUT=30
```

- Run the command (root privileges required):

```
update-grub
```

7.6 Remove IMS database from locate DB

The locate database must not be left to run on the IMS database partitions

- Edit the following file (root privileges required)

```
/etc/updatedb.conf
```

- make sure that the following partitions are added to the PRUNEPATHS entry

```
/data/ims
/data1/ims (if used)
```

7.7 Serial Port UDEV Rules

Usually serial ports appear in the `/dev` directory which is owned by `root` user, and `dialout` group. The `ims` user should have been added to the `dialout` group as part of the ubuntu extras script.

If not, run the following:

```
sudo adduser ims dialout
```

The following UDEV rules should be added. Examples can be found at:
http://software.imseismology.org/documents/System/udev_rules/

The Ubuntu extras script should have already created the udev rules but please confirm content.

7.7.1 USB port *

- Create or edit the following file (root permissions required):

  ```
  /etc/udev/rules.d/ttyUSB.rules
  ```

- Contents of the file should be:

  ```
  # rules for USB ports: change ownership to ims:dialout
  SUBSYSTEM=="tty", KERNEL=="ttyUSB*", OWNER="ims", GROUP="dialout"
  ```

7.7.2 Standard serial ports *

- Create or edit the following file (root permissions required):

  ```
  /etc/udev/rules.d/ttyS.rules
  ```

- The contents of the file should be:

  ```
  # rules for standard serial ports: change ownership to ims:dialout
  SUBSYSTEM=="tty", KERNEL=="ttyS*", OWNER="ims", GROUP="dialout"
  # uncomment the next line for NTP with GPS NMEA messaging on ttyS0
  #SUBSYSTEM=="tty", KERNEL=="ttyS0", SYMLINK+="gps0", RUN+="stty -F /dev/gps0 9600"
  ```

7.7.3 Moxa terminal servers (N-ports)

- Create or edit the following file (root permissions required):

```
/etc/udev/rules.d/ttyr.rules
```

- The contents of the file should be:

```
# rules for moxa serial ports: change ownership to ims:dialout
SUBSYSTEM=="tty", KERNEL=="ttyr*", OWNER="ims", GROUP="dialout"
# uncomment the line below for NTP with GPS on ttyr00
# note that ttyr00 and ttyr0 are the same port,
# the moxa driver creates both and both are linked
# to kernel ttyr0
#SUBSYSTEM=="tty", KERNEL=="ttyr0", SYMLINK+="gps0", RUN+="stty -F /dev/gps0 9600"
```

NB Caveat

Please note that the Moxa driver installer changes the permissions on the `/tmp` directory. This may cause the X-server to fail after the PC is rebooted and cause the IMS software packages to misbehave. After driver installation, change the permissions on `/tmp`.

```
sudo chmod -R 777 /tmp
```

7.8 Change ssh settings

Edit the file `/etc/ssh/sshd_config` as root (sudo) and make sure the following are set correctly

```
PermitRootLogin no
UseDNS no
```

Edit or create the file `~/.ssh/config (as ims user, not root or sudo)`

```
mkdir /home/ims/.ssh
vi /home/ims/.ssh/config
```

Add the following contents to the file

```
Host *
HostKeyAlgorithms +ssh-dss
```

7.9 Time Synchronisation (NTP)

The Synapse server should synchronise to external time servers and will act as the time server for IMS devices in the field.

Most customer sites should have an NTP server accessible to the LAN (IP address supplied by the IT department).

If a locan NTP source is unavailable, a list of Internet NTP servers is provided and maintained by the POOL.NTP.ORG project. Time servers that are relatively close to the network location should be used; so if possible use servers that are specific to the country, or else servers in nearby countries, or servers in the appropriate world region. See `pool.ntp.org` for servers in the appropriate pool. Note that using Internet server's assumes that the port used by NTP (123) is allowed past the firewall etc.

7.9.1 Disable timesyncd

Ubuntu 20.04 comes with a new NTP client named timesyncd. As this is client only and we require our NTP service to be both client and server timesyncd must be disabled using the following command:

```
timedatectl set-ntp false
```

7.9.2 NTP configuration file

- The NTP configuration file should always contain an entry for the local clock (server 127.127.1.0) so that if all external servers are unreachable, the server can still act as a time source to clients (IMS devices).
- ***Never*** *have only 2 servers defined* (not including the local clock) - 1 is better, 4 to 5 are recommended.
- Edit `/etc/ntp.conf`, commenting out all servers defined by default in Ubuntu, and add entries for the local clock, regional servers, local server and GPS. Example sections of the `ntp.conf` file defining the servers (with comments) is available at the following URL.
  `http://software.imseismology.org/documents/System/ntp.conf-config-additions.txt`
- Restart ntp:

  ```
  sudo service ntp restart
  ```

- Check NTP status:

  ```
  ntpq -p
  ```

7.9.3 Synchronising to GPS

Where time synchronisation is via a GPS, the GPS's NMEA port should be connected to a serial port on the server, with the PPS signal on the DCD line of the serial port. Remember to make the correct symbolic link (`/dev/gps0`) to the serial port at boot time - refer to section 7.7.2.

The NTP program is started by the system by `ntp` user which will by default not have permission to read from the serial port. This permission is re-configured by the ubuntu extras script to allow the `ntp` user serial port access. If this script has not been run, the permission can be maually configured using the following command:

```
sudo adduser ntp dialout
```

AppArmor ntpd profile By default Ubuntu will have an AppArmor profile enabled which restricts `ntpd`'s access to the serial port. As a result `ntpd` will not be able to access the GPS NMEA messages via the serial port. The symptoms of this are that the GPS clock (refid: `.GPS.`) will not be visible in the output of the `ntpq -p` program command. There should also be a message in the system logs (`/var/log/syslog` and/or `/var/log/messages`) with fields such as: `apparmor="DENIED"`, `profile="/usr/sbin/ntpd"` and `name="/dev/ttyS0"`.

To disable this behaviour, put AppArmor's `ntpd` profile into complain mode, which will log attempts by `ntpd` to open the serial port, but will not disallow it. An AppArmor profile can be put into complain mode by using the `aa-complain` command. `aa-complain` should have been installed by the Ubuntu extras script, but if it is not installed on the machine, you can do so by typing the following:

```
sudo apt-get install apparmor-utils
```

To put the ntpd program into complain mode, run the following command:

```
sudo aa-complain /usr/sbin/ntpd
```

7.10 Timezone

The timezone of the PC should be set to the correct location. This can be done from the commandline:

```
sudo dpkg-reconfigure tzdata
```

Follow the directions to select the correct timezone.

If the Ubuntu GUI is available, the following can be performed:

1. Open the **System Settings** (available on the power icon in the top right corner of the screen).
2. Open the **Time & Date** application.
3. Use the **Time & Date** panel to set the location and timezone.

7.11 Hardware Clock

It is important that the hardware clock (a.k.a. BIOS clock, RTC, etc.) is kept up to date and synchronised to UTC, so that after a reboot or power cycle the server starts up with reasonably accurate time (accurate enough for NTP to slave the local clock to external time servers, i.e. within a few seconds/couple of minutes of UTC). This is handled automatically by the operating system and NTP, but it is possible that the hardware clock can drift far out of sync (e.g. due to the BIOS battery running flat or other software changing the hardware clock to localtime).

For this reason the Synapse Server software will periodically check the hardware clock, and raise an issue if the hardware clock time is out of sync with UTC.

The system needs to be told to set the hardware clock to UTC time. The following command will achieve this.

```
timedatectl set-local-rtc 0
```

Check that it was correctly configured by typing the following.

```
timedatectl
```

Output should read “RTC in local TZ: no”

Once the time on the PC is correct - preferrably set through NTP, the following can be performed to set the hardware clock based on the current system time:

```
sudo hwclock --systohc --utc
```

Double-check that the time was set correctly by printing out the system time and hardware clock (they should be roughly the same):

```
date; sudo hwclock --utc
```

7.12 SAMBA

Setting up SAMBA shares:

Samba can be set up either graphically or from the commandline. Either way at least one data share must be setup to share the IMS database (`/data/ims`) for remote access by Windows Trace clients:

From a Graphical Login:

- On the server, open Nautilus file browser:
  - Places > Home
- Create the directory you wish to share if necessary
- Right click on the folder and select **Sharing Options**
  - Check the **Share this folder** checkbox (e.g. `/data/ims`)
  - Add a share name and comment (e.g. "`ims_data`" and "`IMS databases share`")
  - Check the **Allow others to create and delete files** option ONLY IF NECESSARY
  - Ensure **Guest access** checkbox is left UN-CHECKED
  - Click **Create share**
    - Click on the **Add permissions automatically** if prompted to do so

OR From the Command-Line:

- Open a terminal
- Type the following command: (Note: the /data/ims directory gets created by the IMS setup software package)

  ```
  net usershare add ims_data /data/ims/ "IMS databases share" ims:F guest_ok=n
  ```

  - If this command fails with an error about you not having permisssions to create a usershare, then you should add the ims user to the "sambashare" group as follows:

    ```
    sudo adduser ims sambashare
    ```

  - Logout and login again for the new group membership changes to take affect: you can check what groups the user belongs to by typing:

    ```
    groups
    ```

- Once you have added the ims user to the sambashare group, run the above "`net usershare...`" command again
- This adds a share called "`ims_data`" with description/comment "`IMS databases share`", which shares the `/data/ims` directory with full permissions for the ims user, guest access is not allowed
- To check the created usershare, type:

  ```
  net usershare info --long
  ```

  - You should see the following output:

    ```
    [ims_data]
    path=/data/ims/
    comment=IMS databases share
    usershare_acl=TSTIMS1\ims:F,
    guest_ok=n
    ```

Final Steps:

- Create a SAMBA password for the ims user (if not already done):

  ```
  sudo smbpasswd -a ims
  ```

  - (use the same password as the system ims user)

- Ensure ims user is enabled in local smbpasswd file:

```
sudo smbpasswd -e ims
sudo service smbd restart
```

- On Windows client:
  - Browse to the share by entering **hostname****share_name** in Windows explorer file browser
  - Map network drive as usual for use with Trace/JDi

7.13 Create hardware summary of system

A unified summary of the system hardware is useful for future technical support, and should be saved to html and xml files using the `lshw` command.

First, create a directory for the Installation Records.

```
mkdir /home/ims/Documents/InstallationRecords
```

Run the following commands to generate the hardware summary files anad save them to the desired directory.

```
sudo lshw -html > "/home/ims/Documents/InstallationRecords/${HOSTNAME}_lshw.html"
sudo lshw -xml > "/home/ims/Documents/InstallationRecords/${HOSTNAME}_lshw.xml"
```

This command will create a summary of the system hardware (including the DELL service tag number).

8 Install IMS Software

Continue with the installation of IMS software (Services pacakges, Synapse server, Database server, etc)

Change Record

Date	Author	Description	Revision
Change Control Record			
2020/09/10	RE	Based on document IMS-SERVER-INSTALL-UBUNTU-18-04-201805-THv16	0
2020/09/25	RE	Fixed broken Ubuntu ISO link	1

Table 4: Change record