2023

DATA HUB REPORT

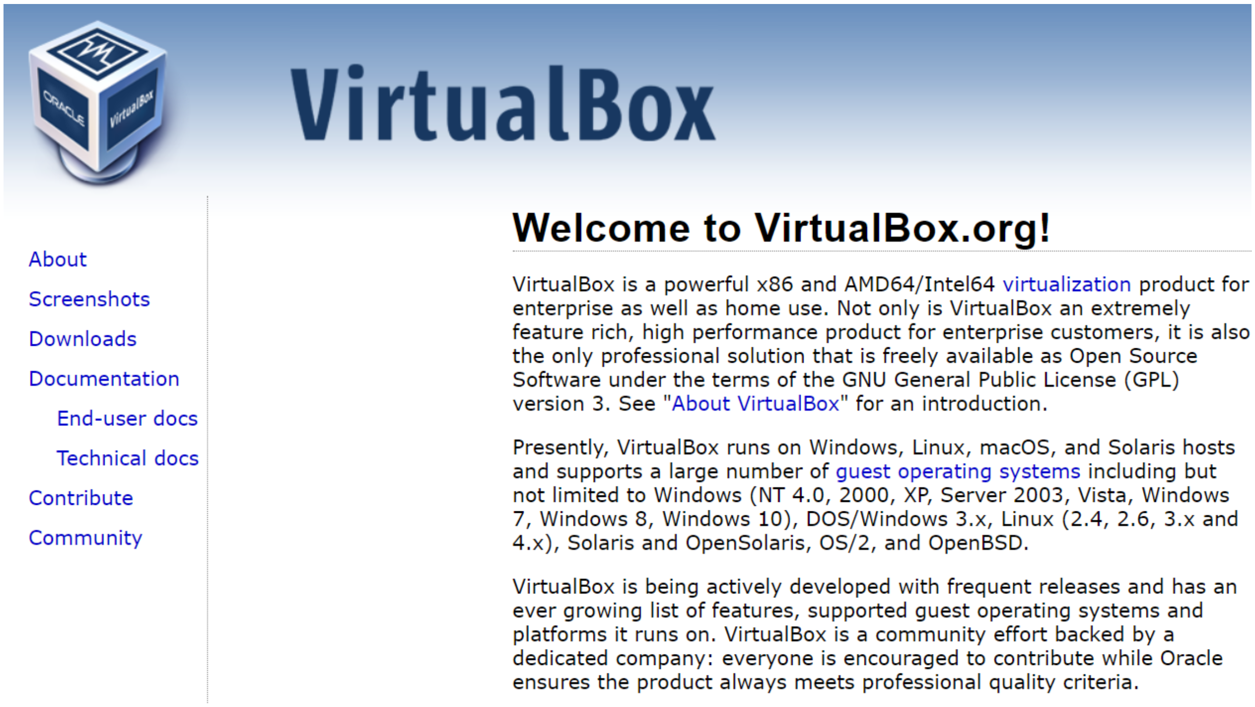
MANOGYA HARSHA BAJRACHARYA

DATA HUB | Sanepa, Lalitpur

Table of Contents

1. Installing virtual box

- Visit the official VirtualBox website: https://www.virtualbox.org/



Welcome to VirtualBox.org!

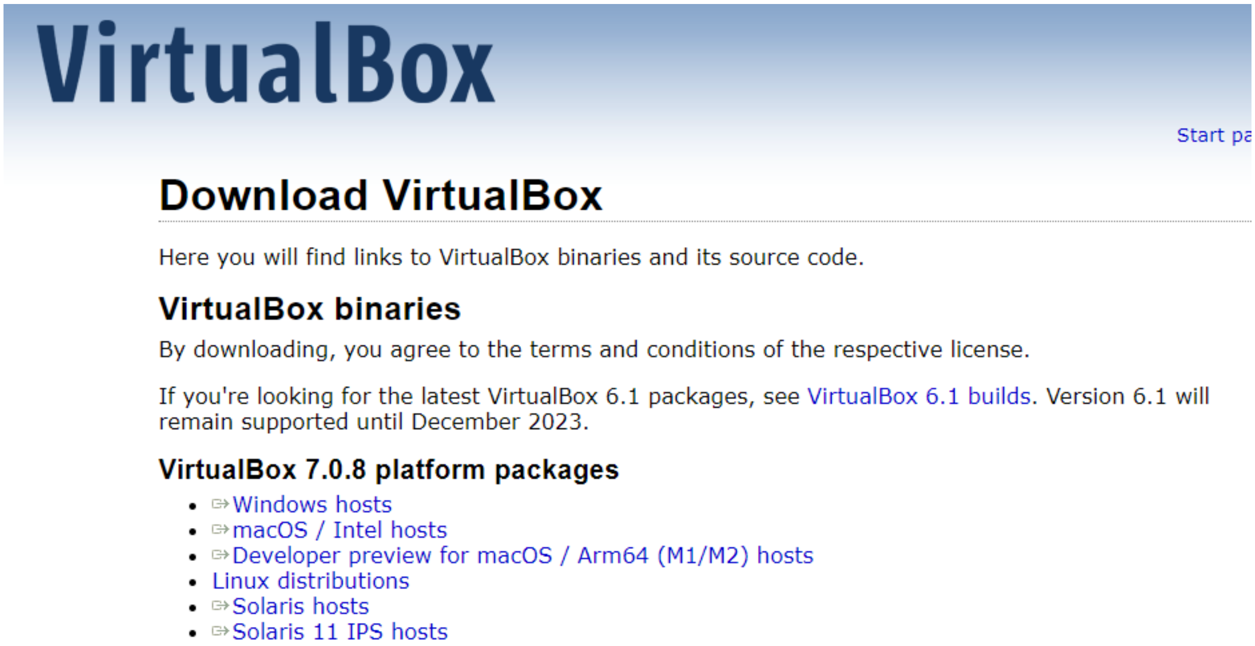
VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Figure 1

- Click on the "Downloads" menu at the top of the page



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

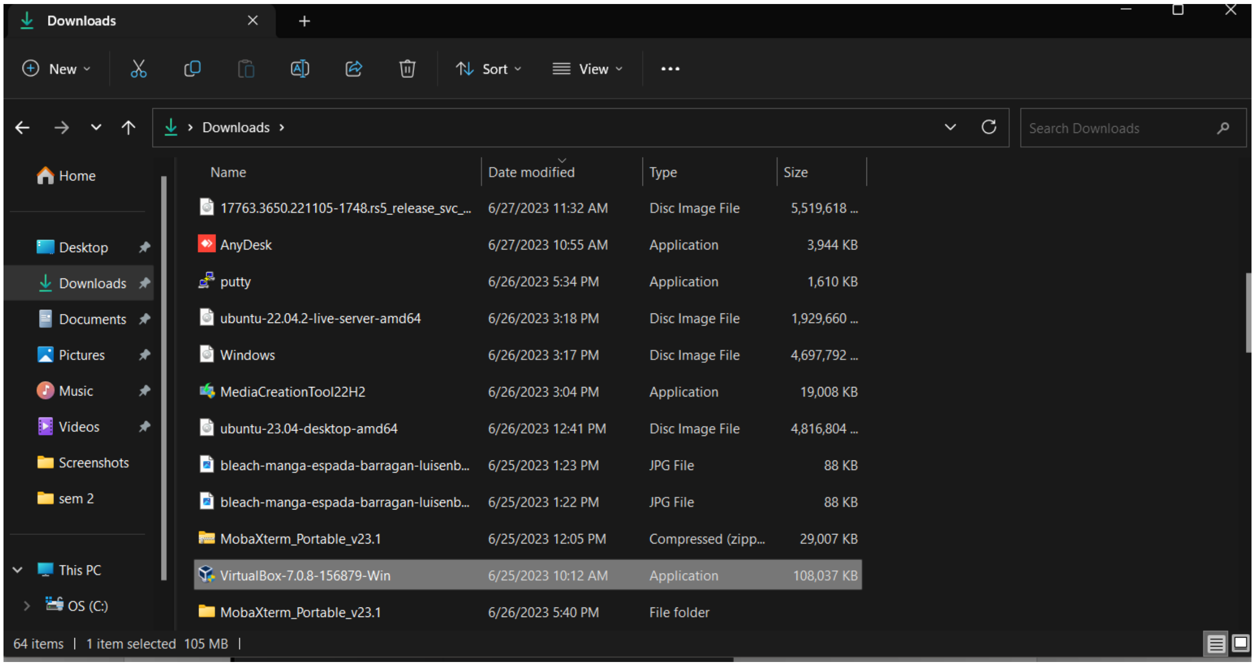
If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.8 platform packages

- ⇨Windows hosts
- ⇨macOS / Intel hosts
- ⇨Developer preview for macOS / Arm64 (M1/M2) hosts
- Linux distributions
- ⇨Solaris hosts
- ⇨Solaris 11 IPS hosts

Figure 2

- Once the installer file is downloaded, locate it on your computer and double-click on it to run the installer.

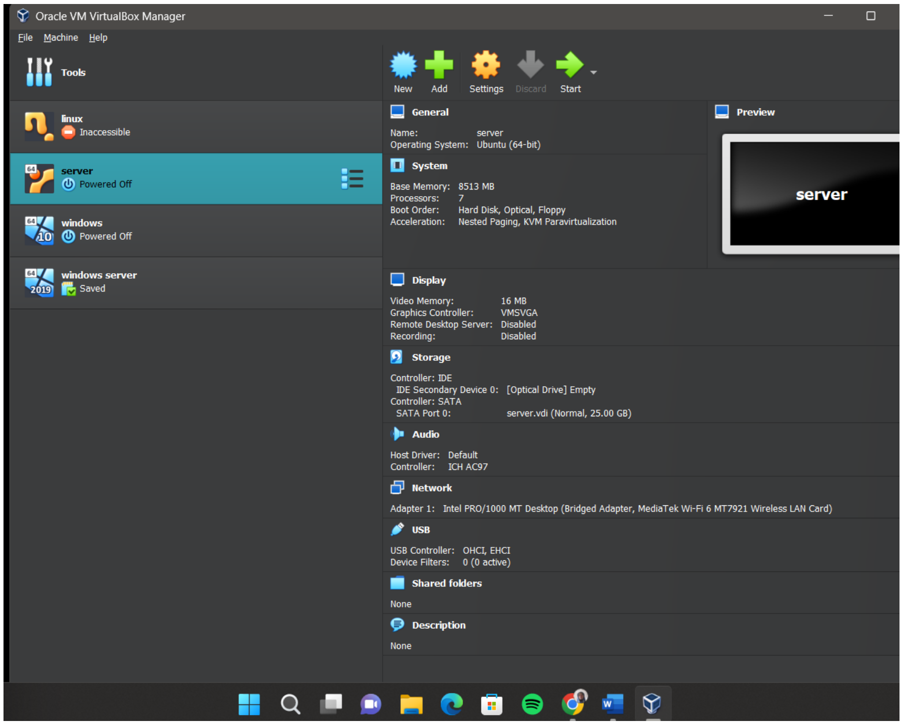


Name	Date modified	Type	Size
17763.3650.221105-1748.rs5_release_svc_...	6/27/2023 11:32 AM	Disc Image File	5,519,618 ...
AnyDesk	6/27/2023 10:55 AM	Application	3,944 KB
putty	6/26/2023 5:34 PM	Application	1,610 KB
ubuntu-22.04.2-live-server-amd64	6/26/2023 3:18 PM	Disc Image File	1,929,660 ...
Windows	6/26/2023 3:17 PM	Disc Image File	4,697,792 ...
MediaCreationTool22H2	6/26/2023 3:04 PM	Application	19,008 KB
ubuntu-23.04-desktop-amd64	6/26/2023 12:41 PM	Disc Image File	4,816,804 ...
bleach-manga-espada-barragan-luisenb...	6/25/2023 1:23 PM	JPG File	88 KB
bleach-manga-espada-barragan-luisenb...	6/25/2023 1:22 PM	JPG File	88 KB
MobaXterm_Portable_v23.1	6/25/2023 12:05 PM	Compressed (zipp...	29,007 KB
VirtualBox-7.0.8-156879-Win	6/25/2023 10:12 AM	Application	108,037 KB
MobaXterm_Portable_v23.1	6/26/2023 5:40 PM	File folder	

64 items | 1 item selected 105 MB |

Figure 3

- Complete the installation process by following the prompts provided by the installer.



General

```
Name:             server
Operating System: Ubuntu (64-bit)
```

System

```
Base Memory:   8513 MB
Processors:    7
Boot Order:    Hard Disk, Optical, Floppy
Acceleration:  Nested Paging, KVM Paravirtualization
```

Display

```
Video Memory:           16 MB
Graphics Controller:    VMSVGA
Remote Desktop Server:  Disabled
Recording:              Disabled
```

Storage

```
Controller: IDE
  IDE Secondary Device 0:  [Optical Drive] Empty
Controller: SATA
  SATA Port 0:             server.vdi (Normal, 25.00 GB)
```

Audio

```
Host Driver:  Default
Controller:   ICH AC97
```

Network

```
Adapter 1:  Intel PRO/1000 MT Desktop (Bridged Adapter, MediaTek Wi-Fi 6 MT7921 Wireless LAN Card)
```

USB

```
USB Controller:  OHCI, EHCI
Device Filters:  0 (0 active)
```

Shared folders

None

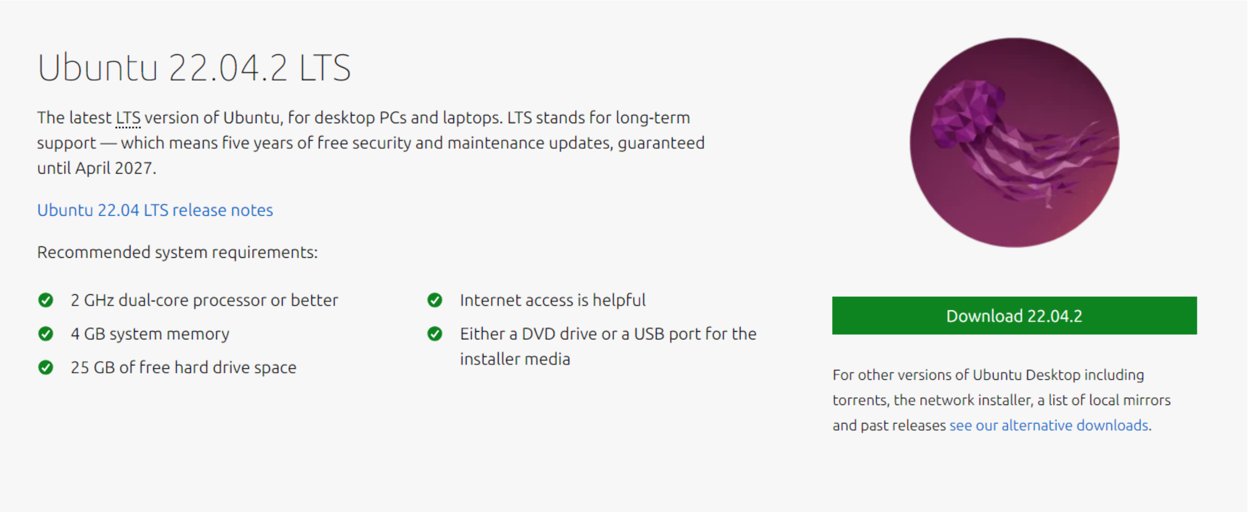
Description

None

Figure 4

2. Downloading the Ubuntu ISO

- Visit the official Ubuntu website: https://ubuntu.com/download
- Select the desired version of Ubuntu and click on the download link to obtain the ISO file.



Ubuntu 22.04.2 LTS

The latest LTS version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years of free security and maintenance updates, guaranteed until April 2027.

Ubuntu 22.04 LTS release notes

Recommended system requirements:

- ✓ 2 GHz dual-core processor or better
- ✓ 4 GB system memory
- ✓ 25 GB of free hard drive space
- ✓ Internet access is helpful
- ✓ Either a DVD drive or a USB port for the installer media

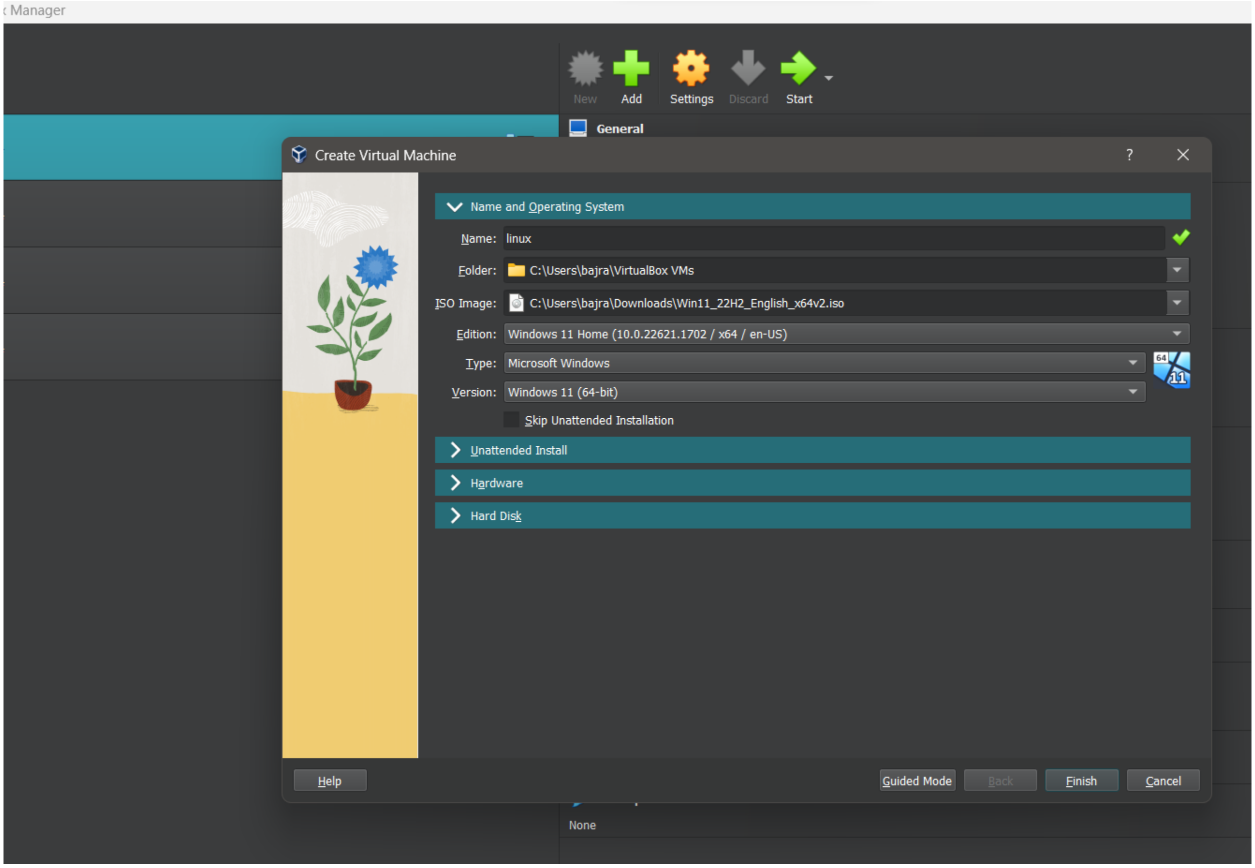
For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors and past releases see our alternative downloads.

Figure 5

3. Creating a new virtual machine in VirtualBox

- Open VirtualBox.
- Click on the "New" button to create a new virtual machine.
- Enter a name for the virtual machine (e.g., "Ubuntu").
- Select the appropriate Type as "Linux" and Version as the Ubuntu version you downloaded (e.g., Ubuntu (64-bit)).
- Allocate memory for the virtual machine. The default value should be fine, but you can adjust it according to your needs.
- In the "Hard disk" section, select "Create a virtual hard disk now" and click "Create".
- Choose the hard disk file type. The default option of "VDI (VirtualBox Disk Image)" is recommended.
- Select the storage on physical hard disk. Again, the default option is usually suitable.
- Set the virtual hard disk size. The default size is typically fine, but you can allocate more if you have sufficient space.

- Click "Create" to create the virtual machine.



Name and Operating System

Name: linux

Folder: C:\Users\bajra\VirtualBox VMs

ISO Image: C:\Users\bajra\Downloads\Win11_22H2_English_x64v2.iso

Edition: Windows 11 Home (10.0.22621.1702 / x64 / en-US)

Type: Microsoft Windows

Version: Windows 11 (64-bit)

□ Skip Unattended Installation

Unattended Install

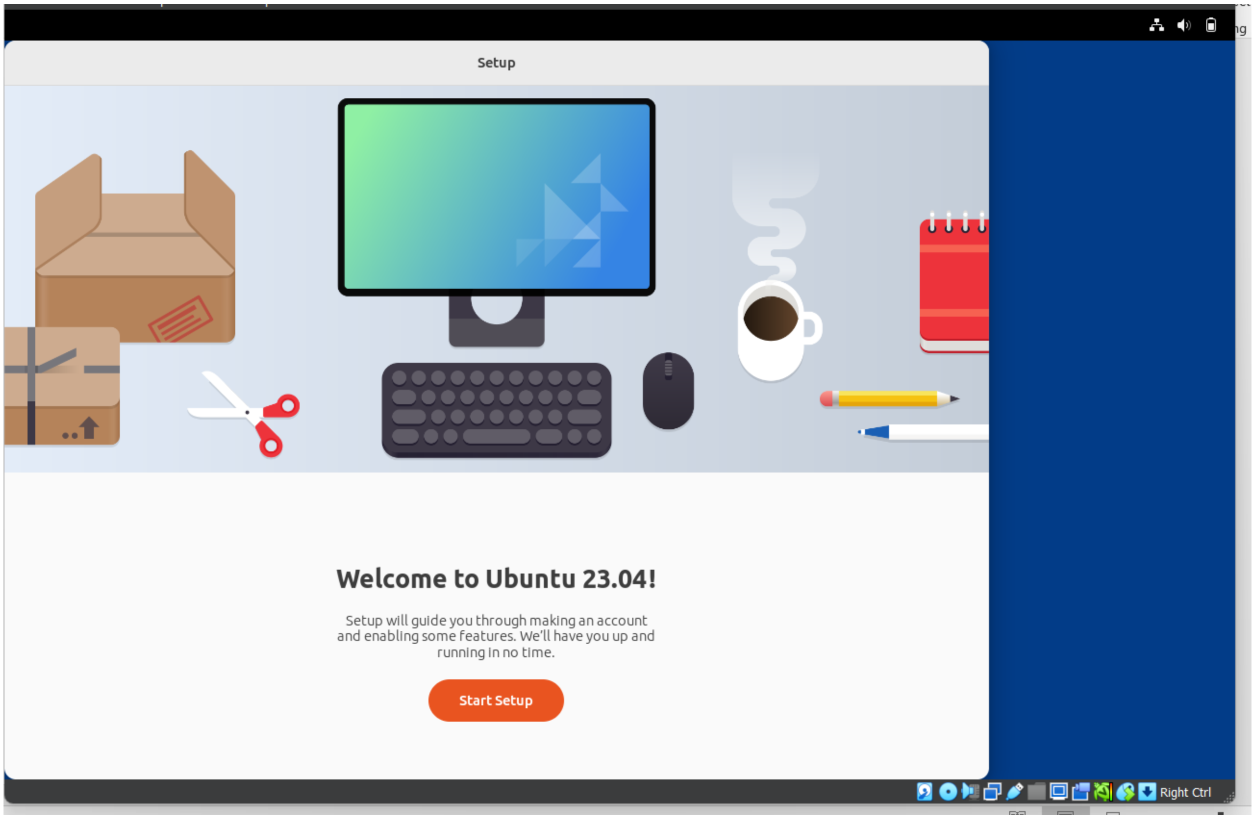
Hardware

Hard Disk

Figure 6

- Start the virtual machine by selecting it in the VirtualBox Manager and clicking on the "Start" button.
- The virtual machine will boot from the Linux ISO you mounted.
- Follow the on-screen instructions to install Linux. The installation process may vary depending on the Linux distribution you chose.
- Make sure to partition the virtual hard disk properly during the installation process.
- Once the installation is complete, restart the virtual machine.
- Run Linux in VirtualBox:
- After the virtual machine restarts, you should see the login screen for your Linux distribution.
- Enter your username and password to log in to the Linux virtual machine.

- Linux should now be running within VirtualBox, allowing you to explore and use it just like a regular Linux installation.



Setup

Welcome to Ubuntu 23.04!

Setup will guide you through making an account and enabling some features. We'll have you up and running in no time.

Figure 7

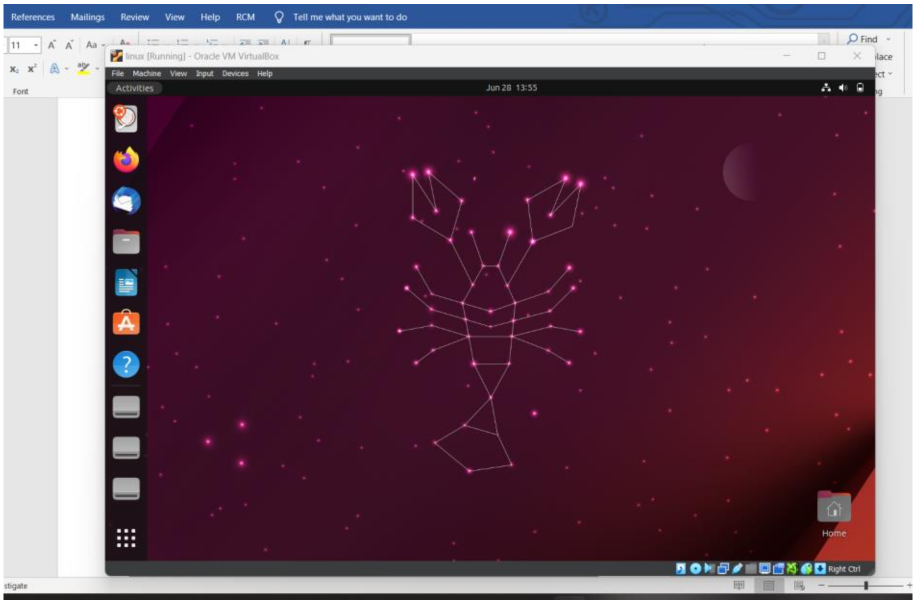
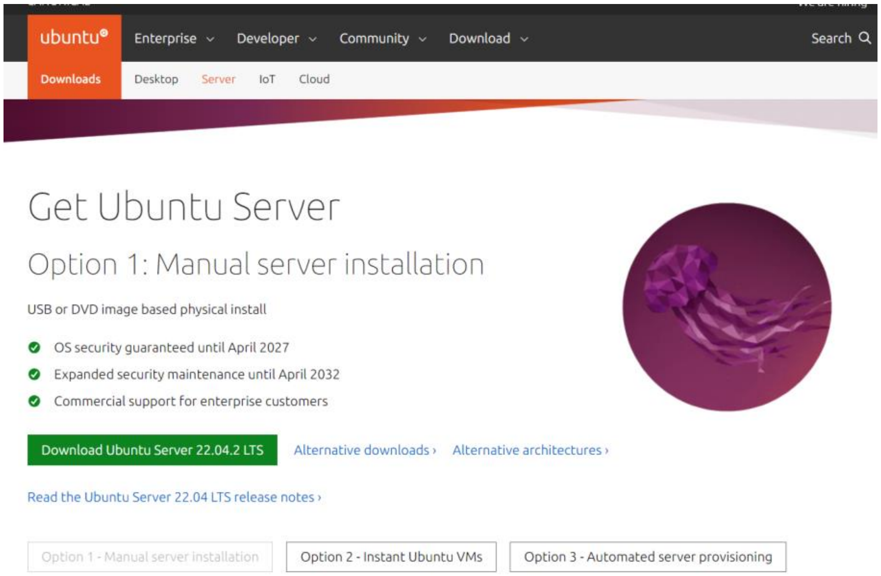


Figure 8

- Choose a Linux distribution:
- Determine which Linux distribution is suitable for your server needs. Popular options for server installations include Ubuntu Server, CentOS, Debian, or Fedora Server. Consider factors such as community support, stability, and specific requirements of your server.
- Download the Linux distribution
- Visit the official website of the Linux distribution you have chosen.
- Look for the server edition or the version specifically designed for server installations.
- Download the ISO file for the desired Linux server distribution.
- Create a new virtual machine in VirtualBox:
- Open VirtualBox.
- Click on the "New" button to create a new virtual machine.
- Enter a name for the virtual machine (e.g., "Ubuntu").
- Select the appropriate Type as "Linux" and Version as the Ubuntu version you downloaded (e.g., Ubuntu (64-bit)).
- Allocate memory for the virtual machine. The default value should be fine, but you can adjust it according to your needs.
- In the "Hard disk" section, select "Create a virtual hard disk now" and click "Create".
- Choose the hard disk file type. The default option of "VDI (VirtualBox Disk Image)" is recommended.
- Select the storage on physical hard disk. Again, the default option is usually suitable.

- Set the virtual hard disk size. The default size is typically fine, but you can allocate more if you have sufficient space.


ubuntu®
Enterprise
Developer
Community
Download
Search
Downloads
Desktop
Server
IoT
Cloud

Get Ubuntu Server

Option 1: Manual server installation

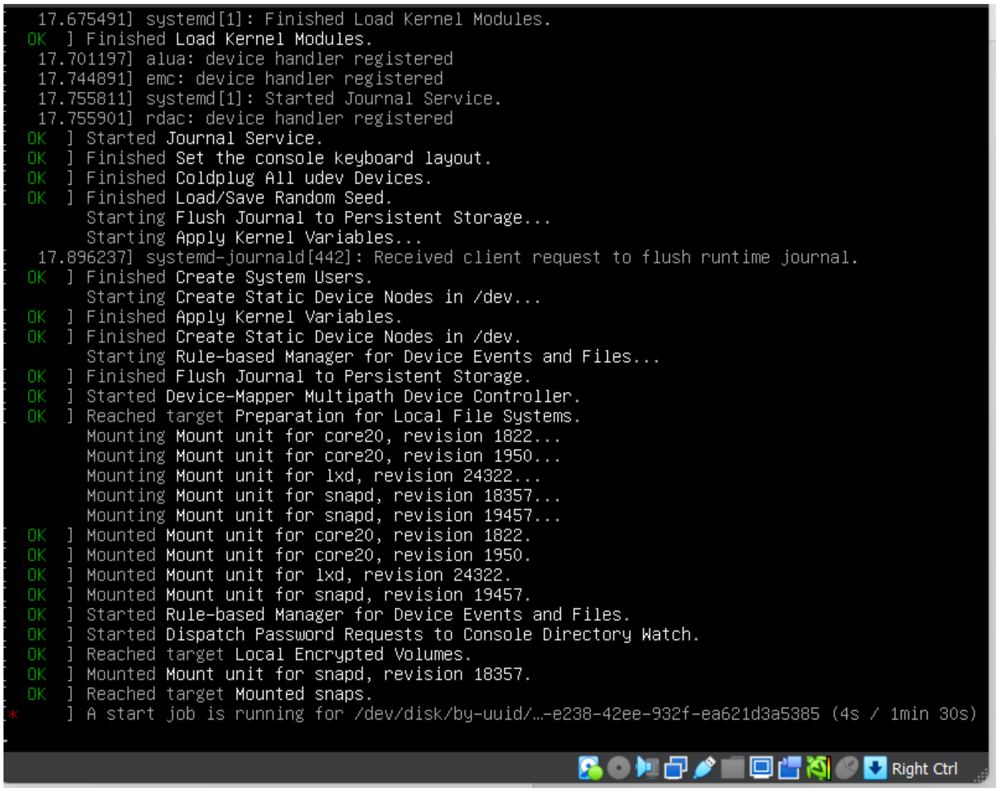
USB or DVD image based physical install

- OS security guaranteed until April 2027
- Expanded security maintenance until April 2032
- Commercial support for enterprise customers

Download Ubuntu Server 22.04.2 LTS
Alternative downloads ›
Alternative architectures ›
Read the Ubuntu Server 22.04 LTS release notes ›
Option 1 - Manual server installation
Option 2 - Instant Ubuntu VMs
Option 3 - Automated server provisioning

Figure 9

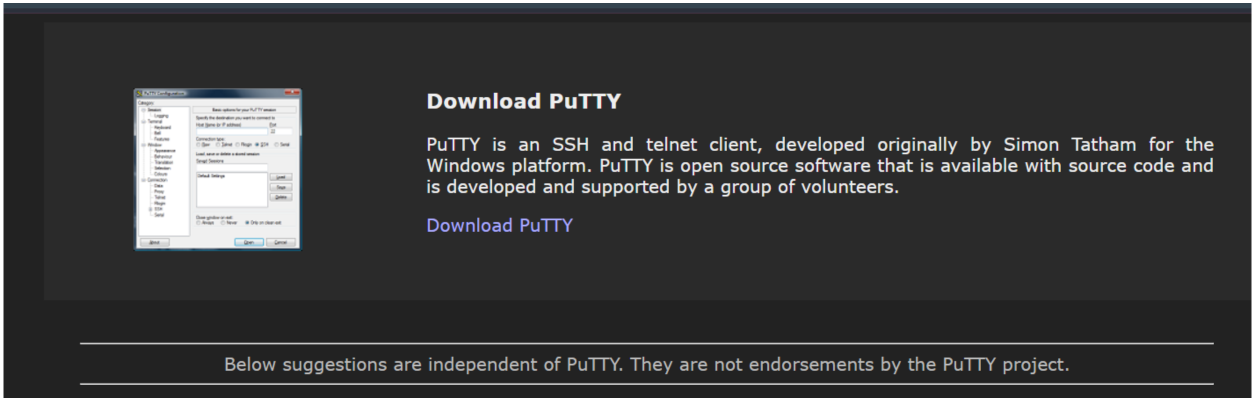
- Access and configure the Linux server:
- After the virtual machine restarts, you should see the login screen for your Linux server.
- Enter the appropriate username and password to log in to the Linux server.
- Now you can configure the Linux server based on your requirements, such as installing additional software, setting up network services, configuring security measures, etc.



```
[   17.675491] systemd[1]: Finished Load Kernel Modules.
[  OK  ] Finished Load Kernel Modules.
[   17.701197] alua: device handler registered
[   17.744891] emc: device handler registered
[   17.755811] systemd[1]: Started Journal Service.
[   17.755901] rdac: device handler registered
[  OK  ] Started Journal Service.
[  OK  ] Finished Set the console keyboard layout.
[  OK  ] Finished Coldplug All udev Devices.
[  OK  ] Finished Load/Save Random Seed.
         Starting Flush Journal to Persistent Storage...
         Starting Apply Kernel Variables...
[   17.896237] systemd-journald[442]: Received client request to flush runtime journal.
[  OK  ] Finished Create System Users.
         Starting Create Static Device Nodes in /dev...
[  OK  ] Finished Apply Kernel Variables.
[  OK  ] Finished Create Static Device Nodes in /dev.
         Starting Rule-based Manager for Device Events and Files...
[  OK  ] Finished Flush Journal to Persistent Storage.
[  OK  ] Started Device-Mapper Multipath Device Controller.
[  OK  ] Reached target Preparation for Local File Systems.
         Mounting Mount unit for core20, revision 1822...
         Mounting Mount unit for core20, revision 1950...
         Mounting Mount unit for lxd, revision 24322...
         Mounting Mount unit for snapd, revision 18357...
         Mounting Mount unit for snapd, revision 19457...
[  OK  ] Mounted Mount unit for core20, revision 1822.
[  OK  ] Mounted Mount unit for core20, revision 1950.
[  OK  ] Mounted Mount unit for lxd, revision 24322.
[  OK  ] Mounted Mount unit for snapd, revision 19457.
[  OK  ] Started Rule-based Manager for Device Events and Files.
[  OK  ] Started Dispatch Password Requests to Console Directory Watch.
[  OK  ] Reached target Local Encrypted Volumes.
[  OK  ] Mounted Mount unit for snapd, revision 18357.
[  OK  ] Reached target Mounted snaps.
[*     ] A start job is running for /dev/disk/by-uuid/…-e238-42ee-932f-ea621d3a5385 (4s / 1min 30s)
```

Figure 10

4. Installing putty.exe



Download PuTTY

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

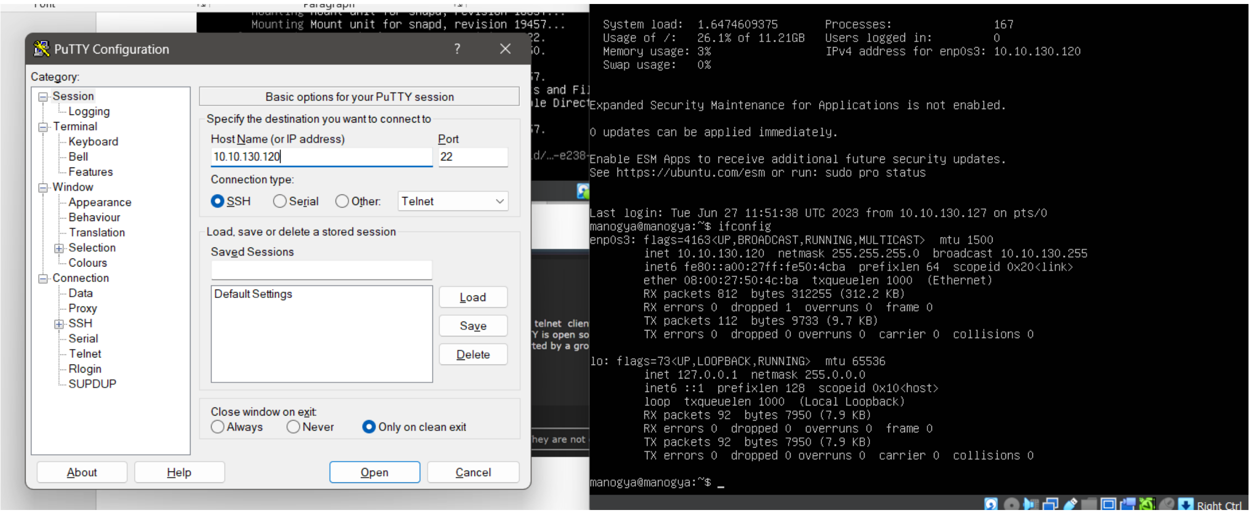
Download PuTTY

Below suggestions are independent of PuTTY. They are not endorsements by the PuTTY project.

Figure 11

- Download and install PuTTY:
- Visit the official PuTTY website: https://www.chiark.greenend.org.uk/~sgtatham/putty/
- Download the appropriate installer for your operating system (e.g., PuTTY for Windows).
- Run the installer and follow the on-screen instructions to install PuTTY.
- You need the following information to connect to an SSH server:
- IP address or hostname
- SSH port: The port number on which the SSH server is listening. The default SSH port is 22, but it may be different depending on the server configuration.
- Username: Your username on the SSH server.
- Password or SSH key: Depending on the server configuration, you will need either a password or an SSH key for authentication.
- Open PuTTY from the Start menu or desktop shortcut (on Windows) or from the Applications folder (on macOS).
- In the PuTTY Configuration window, enter the IP address or hostname of the SSH server in the "Host Name (or IP address)" field.
- Select the connection type as "SSH".
- Enter the SSH port number in the "Port" field. If you're using the default SSH port (22), you can leave this field blank.
- Make sure the "Connection type" is set to "SSH".
- If you have an SSH key for authentication, navigate to the "Connection" -> "SSH" -> "Auth" section and click on the "Browse" button to select your private key file (.ppk).

- If you're using a username and password for authentication, enter your username in the "Auto-login username" field.
- Click "Open" to start the SSH connection.
- Accept SSH server's key fingerprint:
- The first time you connect to an SSH server, PuTTY will display the server's key fingerprint and ask you to verify it. Make sure the fingerprint matches the one provided by the server administrator.
- If the fingerprint is correct, click "Yes" to add the server to PuTTY's cache.
- PuTTY will save the server's key fingerprint for future connections, and subsequent connections will not prompt this message again.
- Enter password or use SSH key passphrase:
- Connect to the SSH server:
- Once you have provided the authentication credentials, PuTTY will establish the SSH connection to the remote server.
- You will see a command prompt indicating that you are connected to the remote server via SSH.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.10.130.120

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

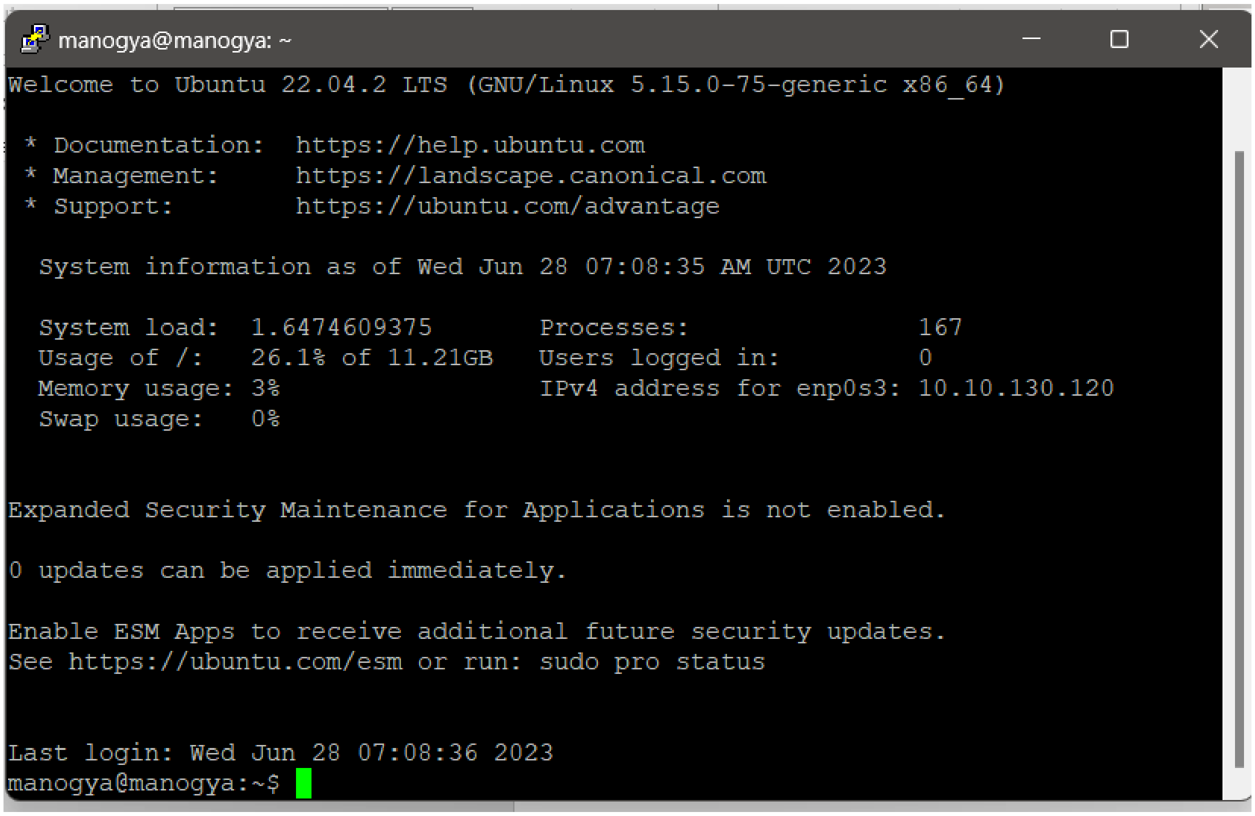
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

```
  System load:  1.6474609375       Processes:               167
  Usage of /:   26.1% of 11.21GB   Users logged in:         0
  Memory usage: 3%                 IPv4 address for enp0s3: 10.10.130.120
  Swap usage:   0%


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


Last login: Tue Jun 27 11:51:38 UTC 2023 from 10.10.130.127 on pts/0
manogya@manogya:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.130.120  netmask 255.255.255.0  broadcast 10.10.130.255
        inet6 fe80::a00:27ff:fe50:4cba  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:50:4c:ba  txqueuelen 1000  (Ethernet)
        RX packets 812  bytes 312255 (312.2 KB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 112  bytes 9733 (9.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 92  bytes 7950 (7.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92  bytes 7950 (7.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

manogya@manogya:~$ _
```

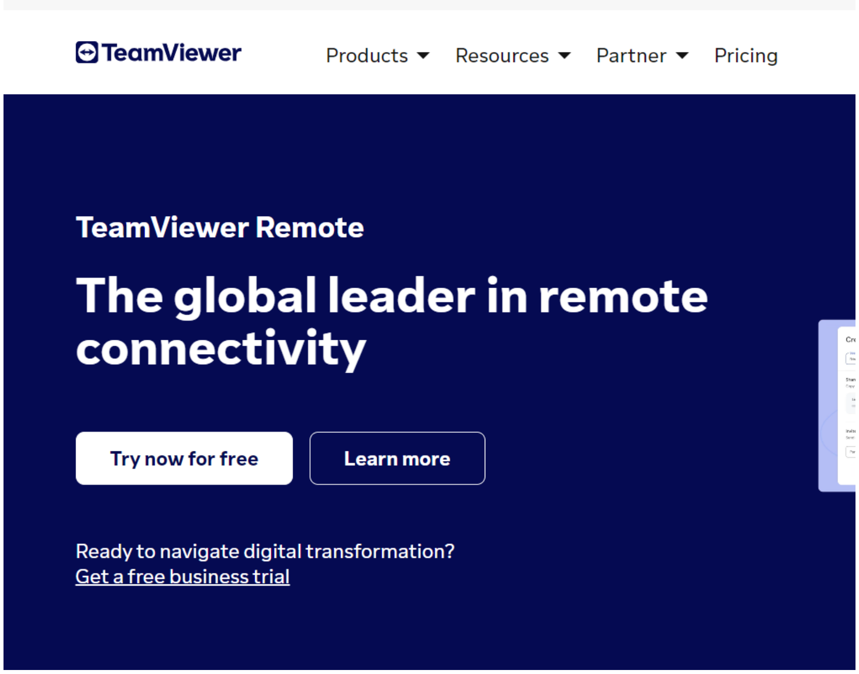
Figure 12



```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-75-generic x86_64)

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

  System information as of Wed Jun 28 07:08:35 AM UTC 2023

  System load:  1.6474609375       Processes:             167
  Usage of /:   26.1% of 11.21GB   Users logged in:       0
  Memory usage: 3%                 IPv4 address for enp0s3: 10.10.130.120
  Swap usage:   0%


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


Last login: Wed Jun 28 07:08:36 2023
manogya@manogya:~$
```

Figure 13

5. Installing and using remote desktop software

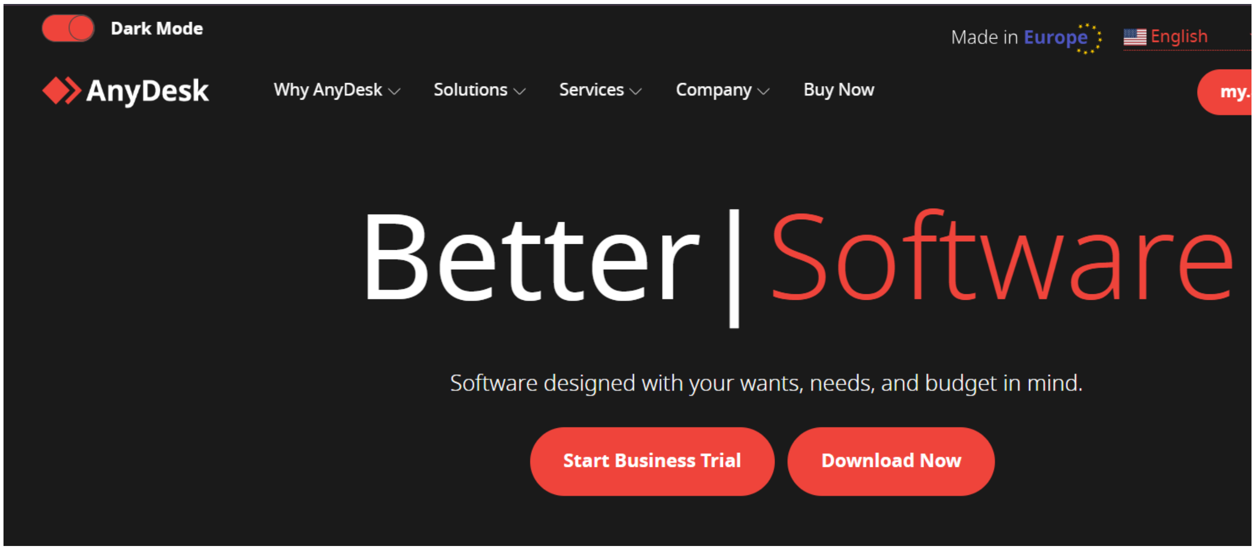


TeamViewer Remote

The global leader in remote connectivity

Ready to navigate digital transformation?
Get a free business trial

Figure 14



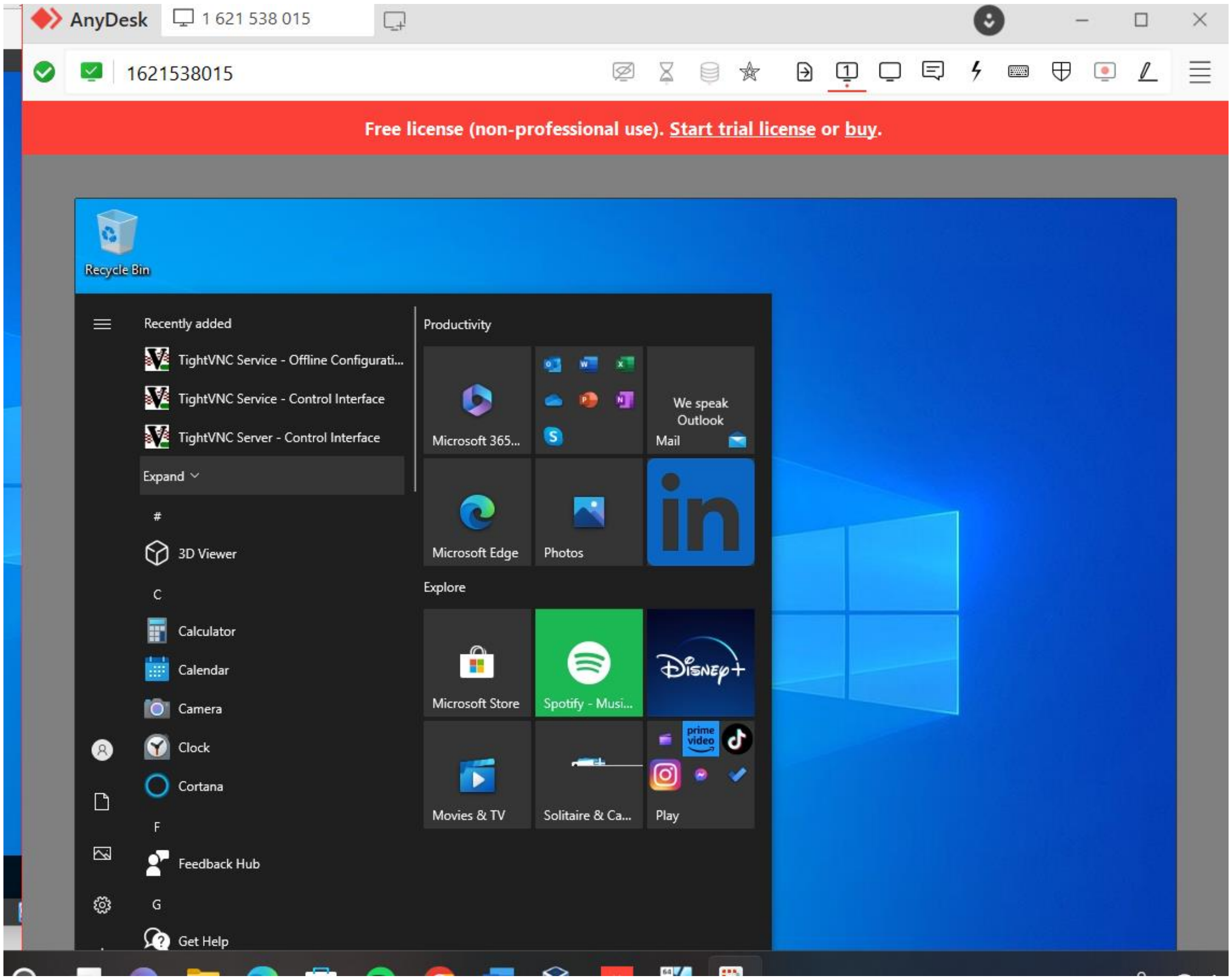
Better | Software

Software designed with your wants, needs, and budget in mind.

Figure 15

- Visit the official AnyDesk website:
- Go to the official AnyDesk website at https://anydesk.com/.
- AnyDesk provides versions for various operating systems, including Windows, macOS, Linux, and mobile platforms. Choose the appropriate version for your operating system.
- Download AnyDesk:

- On the AnyDesk website, locate the "Download" section.
- Click on the download button corresponding to your operating system.
- Run the AnyDesk installer:
- Once the download is complete, locate the downloaded installer file.
- Double-click on the installer file to run it.
- Accept the license agreement
- The installer will present you with a license agreement. Read through the agreement and, if you agree to the terms, select the checkbox indicating your acceptance.
- Choose the installation options:
- The installer may provide some installation options, such as the destination folder or additional components. Review and customize these options as desired.
- Start the installation
- Click on the "Install" or "Next" button to begin the installation process.
- Complete the installation:
- The installer will copy the necessary files and components to your system.
- Once the installation is complete, you may be prompted to create shortcuts or perform other optional configurations. Follow the prompts and make your selections accordingly.



Free license (non-professional use). Start trial license or buy.

Figure 16

- Launch AnyDesk After the installation is finished, AnyDesk should be ready to use.
- Look for the AnyDesk icon on your desktop or in the Start menu (on Windows) or in the Applications folder (on macOS).
- Double-click on the AnyDesk icon to launch the application.
- Obtain AnyDesk ID
- When AnyDesk launches, it will display an "AnyDesk ID" on the main screen. This ID is unique to your device and serves as your identification when connecting with other devices.
- Connect to remote devices or share your AnyDesk ID:
- To connect to a remote device, obtain the AnyDesk ID of the device you want to access.

- Enter the remote device's AnyDesk ID in the "Remote Desk" field on your AnyDesk application and click on the "Connect" button.

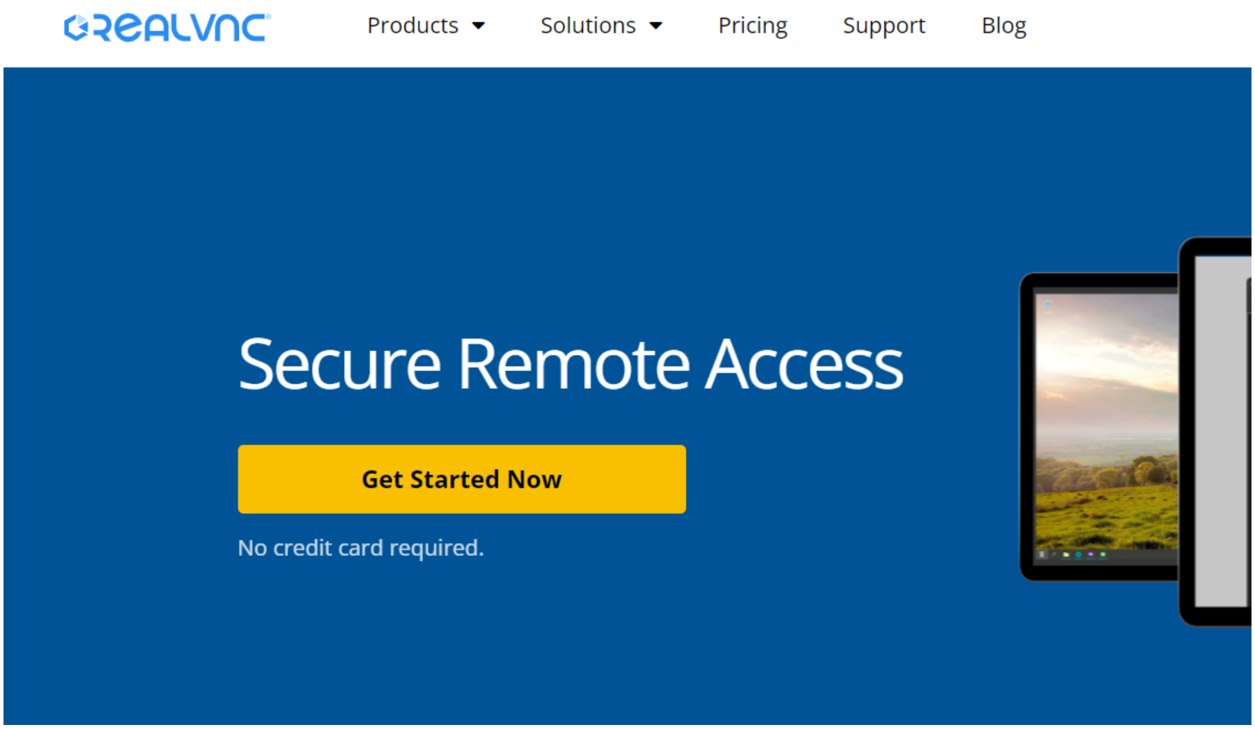
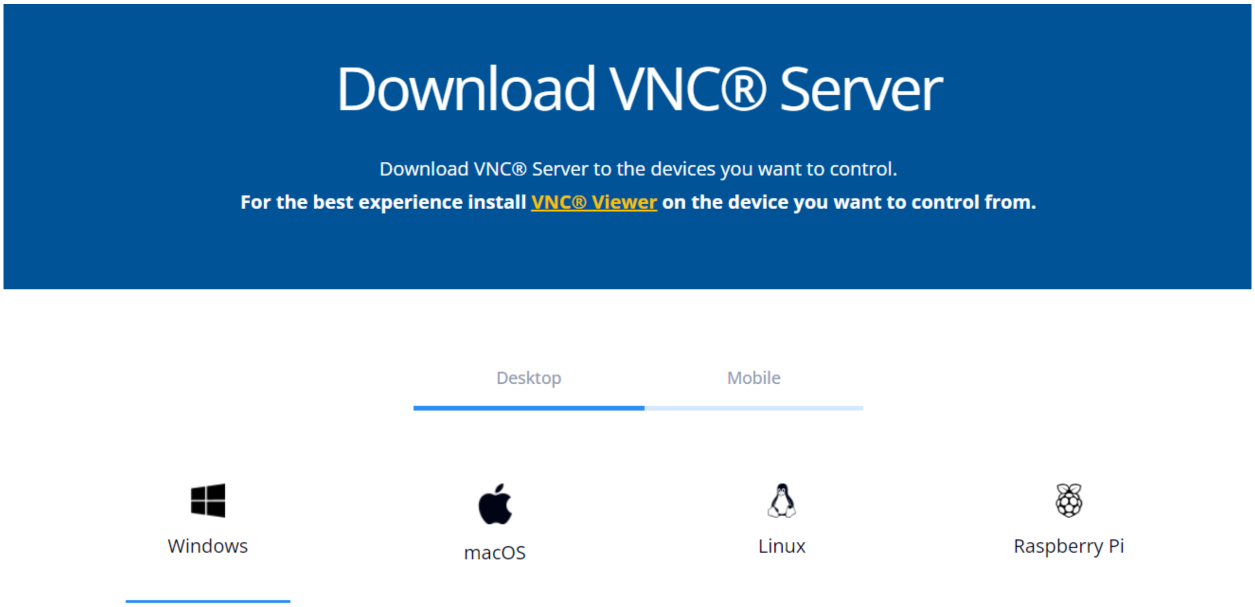


Figure 17

6. Download RealVNC:

- Visit the official RealVNC website at https://www.realvnc.com/.
- Navigate to the "Downloads" section.
- Choose the appropriate version of RealVNC for your Linux distribution and download the installation package.
- Install RealVNC:
- Open a terminal on your Linux system.
- Navigate to the directory where you downloaded the RealVNC installation package
- Installing real vnc server



Download VNC® Server

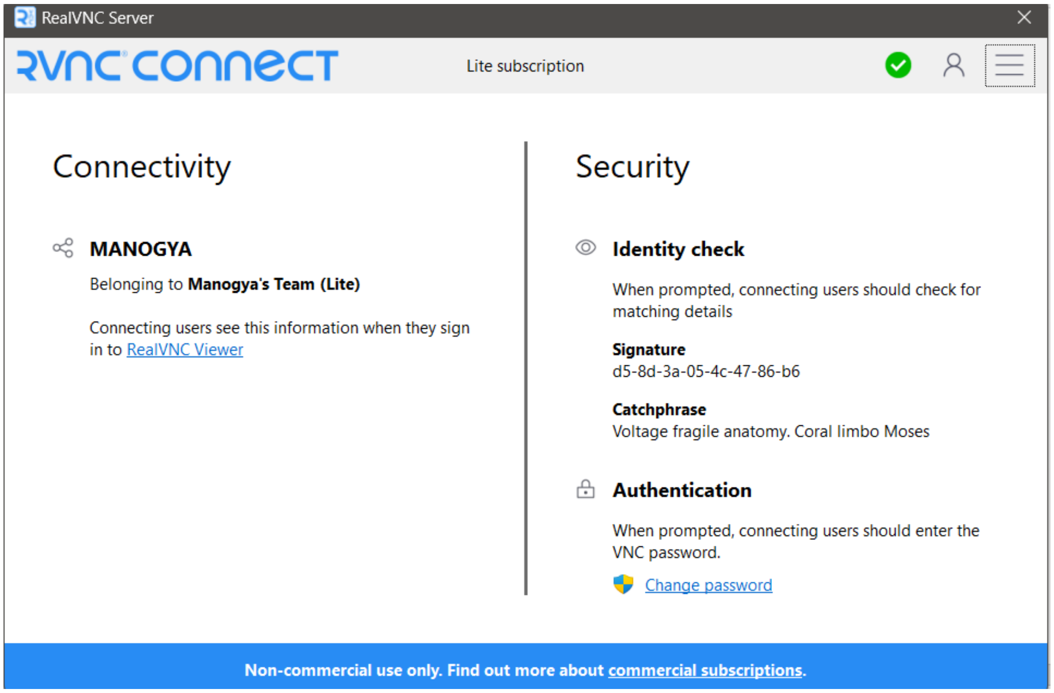
Download VNC® Server to the devices you want to control.

For the best experience install VNC® Viewer on the device you want to control from.

Figure 18

7. Downloading RealVNC Server

- Visit the official RealVNC Server website at https://www.realvnc.com/.
- Navigate to the "Downloads" section.
- Choose the appropriate version of RealVNC for your Linux distribution and download the installation package.



Connectivity

MANOGYA

Belonging to **Manogya's Team (Lite)**

Connecting users see this information when they sign in to RealVNC Viewer

Security

Identity check

When prompted, connecting users should check for matching details

Signature
d5-8d-3a-05-4c-47-86-b6

Catchphrase
Voltage fragile anatomy. Coral limbo Moses

Authentication

When prompted, connecting users should enter the VNC password.

Change password

Non-commercial use only. Find out more about commercial subscriptions.

Figure 19

- Launch the RealVNC Viewer:
- On your computer, open the RealVNC Viewer application. If you haven't installed it yet, you can download it from the RealVNC website.
- Enter the VNC server address:
- In the RealVNC Viewer, enter the IP address or hostname of the computer running the VNC server. The address should be in the format of IP_ADDRESS:PORT_NUMBER, where the default VNC port is 5900. For example, 192.168.1.100:5900.
- If the VNC server is using a different port, specify it accordingly.
- Connect to the VNC server:
- Click on the "Connect" button in the RealVNC Viewer to establish the connection to the VNC server.
- If prompted, enter the password associated with the VNC server. This is the password you set during the RealVNC server setup.

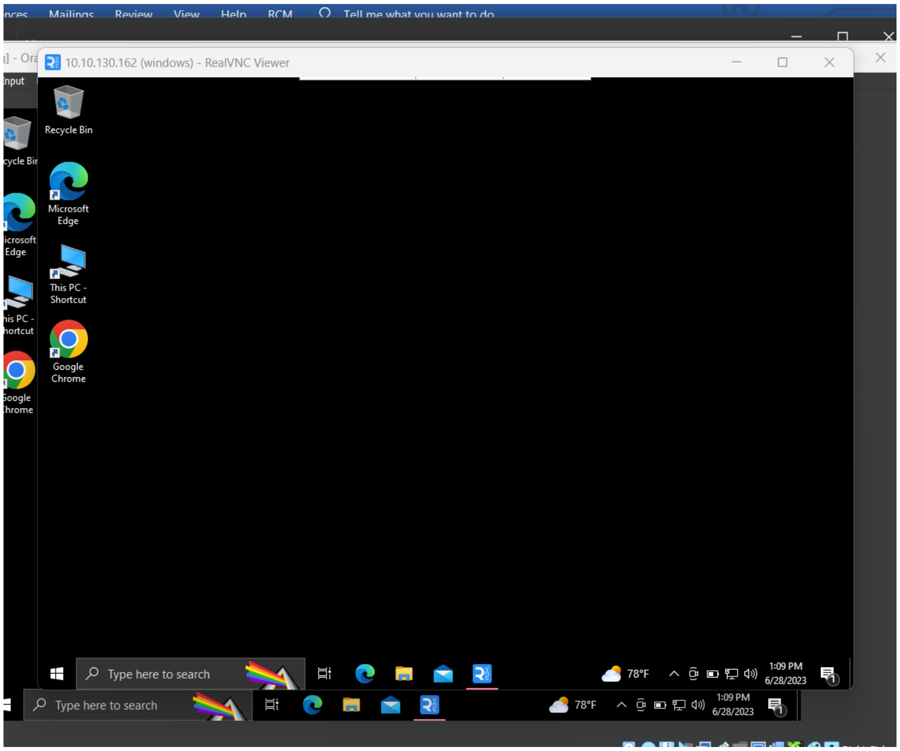
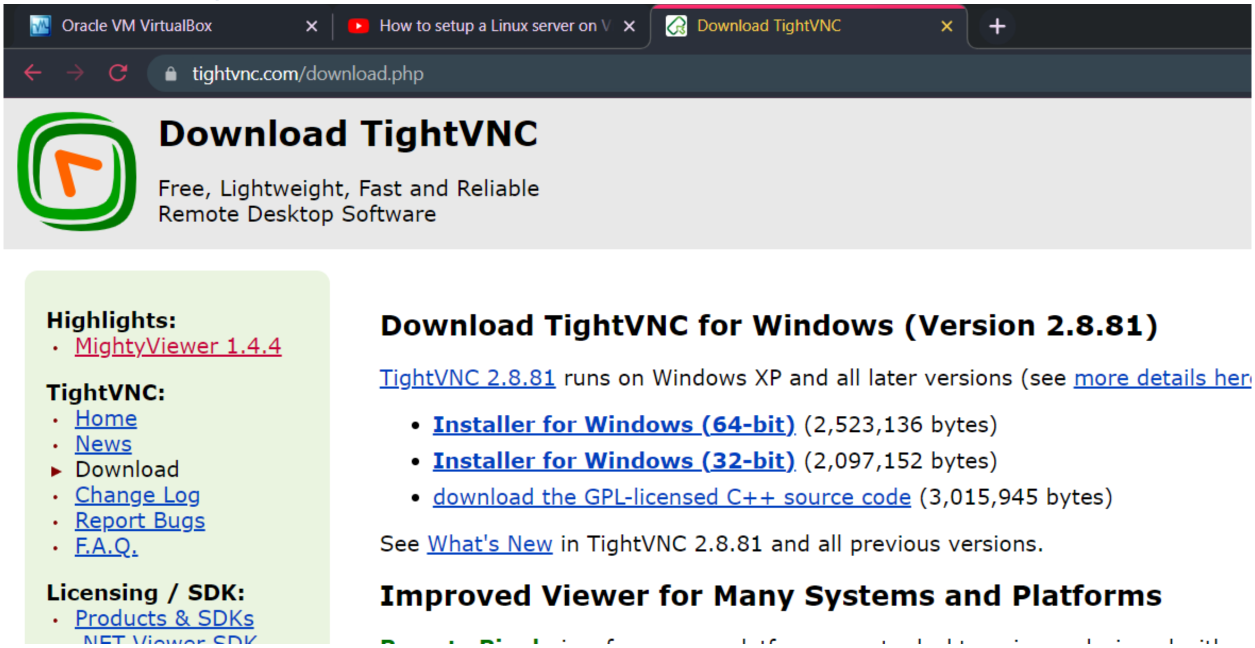


Figure 20

8. Installing different vnc server



Download TightVNC

Free, Lightweight, Fast and Reliable
Remote Desktop Software

Highlights:

- MightyViewer 1.4.4

TightVNC:

- Home
- News
- Download
- Change Log
- Report Bugs
- F.A.Q.

Licensing / SDK:

- Products & SDKs

Download TightVNC for Windows (Version 2.8.81)

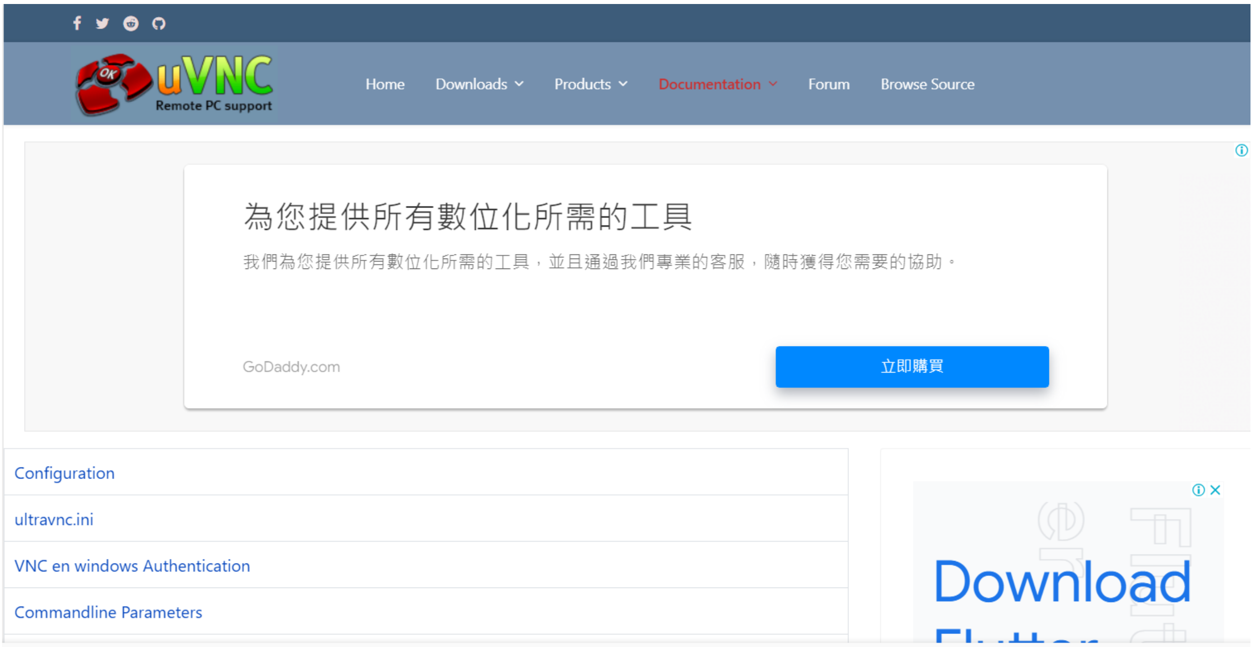
TightVNC 2.8.81 runs on Windows XP and all later versions (see more details her

- **Installer for Windows (64-bit)** (2,523,136 bytes)
- **Installer for Windows (32-bit)** (2,097,152 bytes)
- download the GPL-licensed C++ source code (3,015,945 bytes)

See What's New in TightVNC 2.8.81 and all previous versions.

Improved Viewer for Many Systems and Platforms

Figure 21



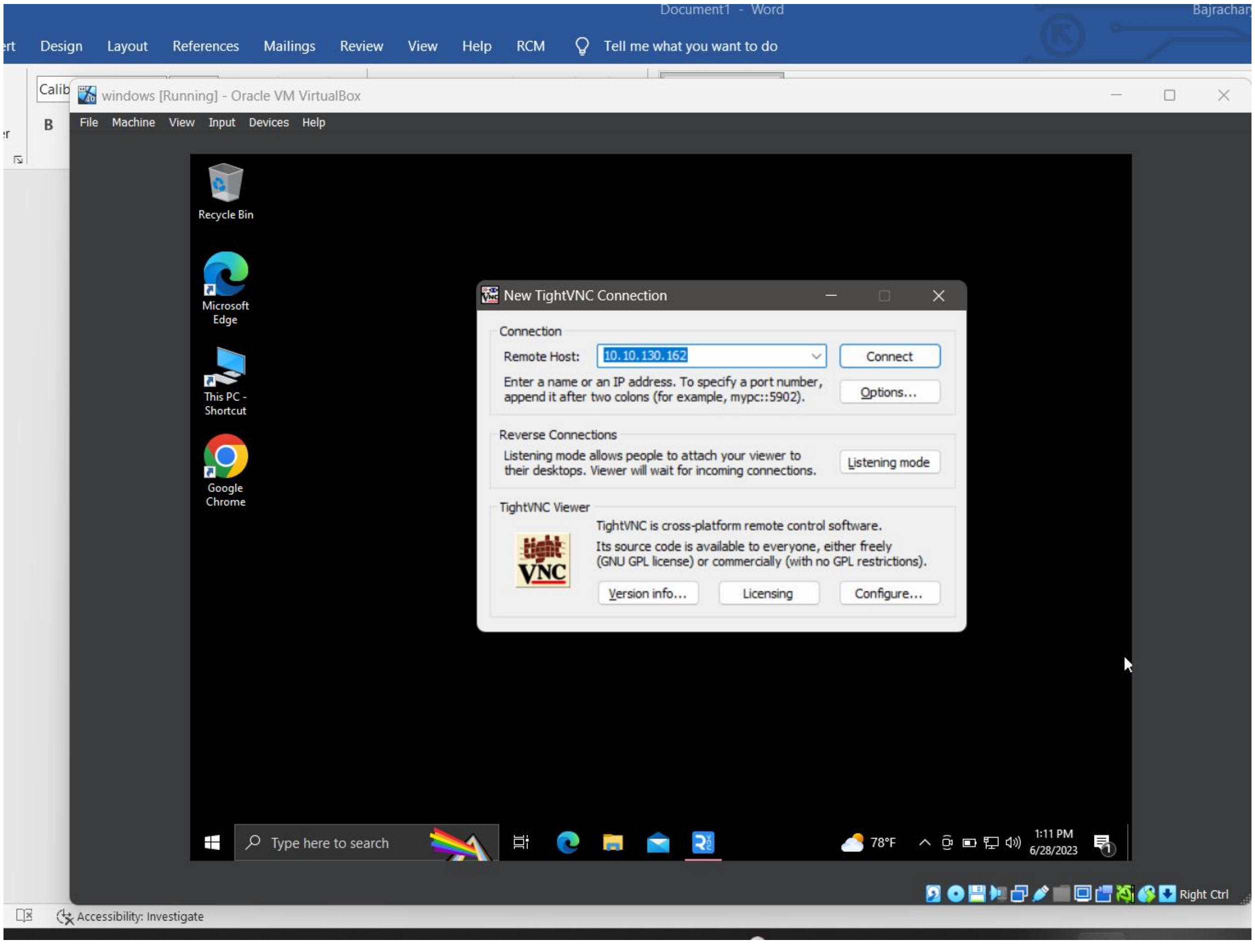
Configuration

ultravnc.ini

VNC en windows Authentication

Commandline Parameters

Figure 22



New TightVNC Connection

Connection

Remote Host: 10.10.130.162

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Reverse Connections

Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC Viewer

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

Figure 23

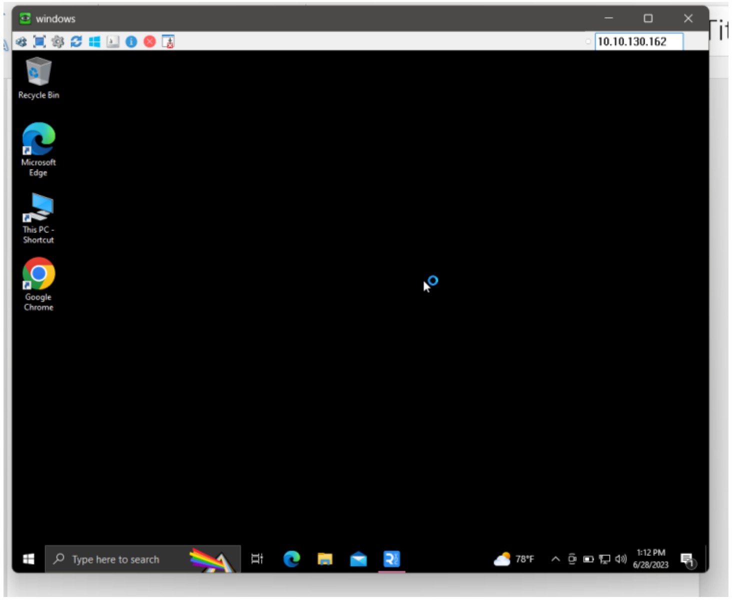
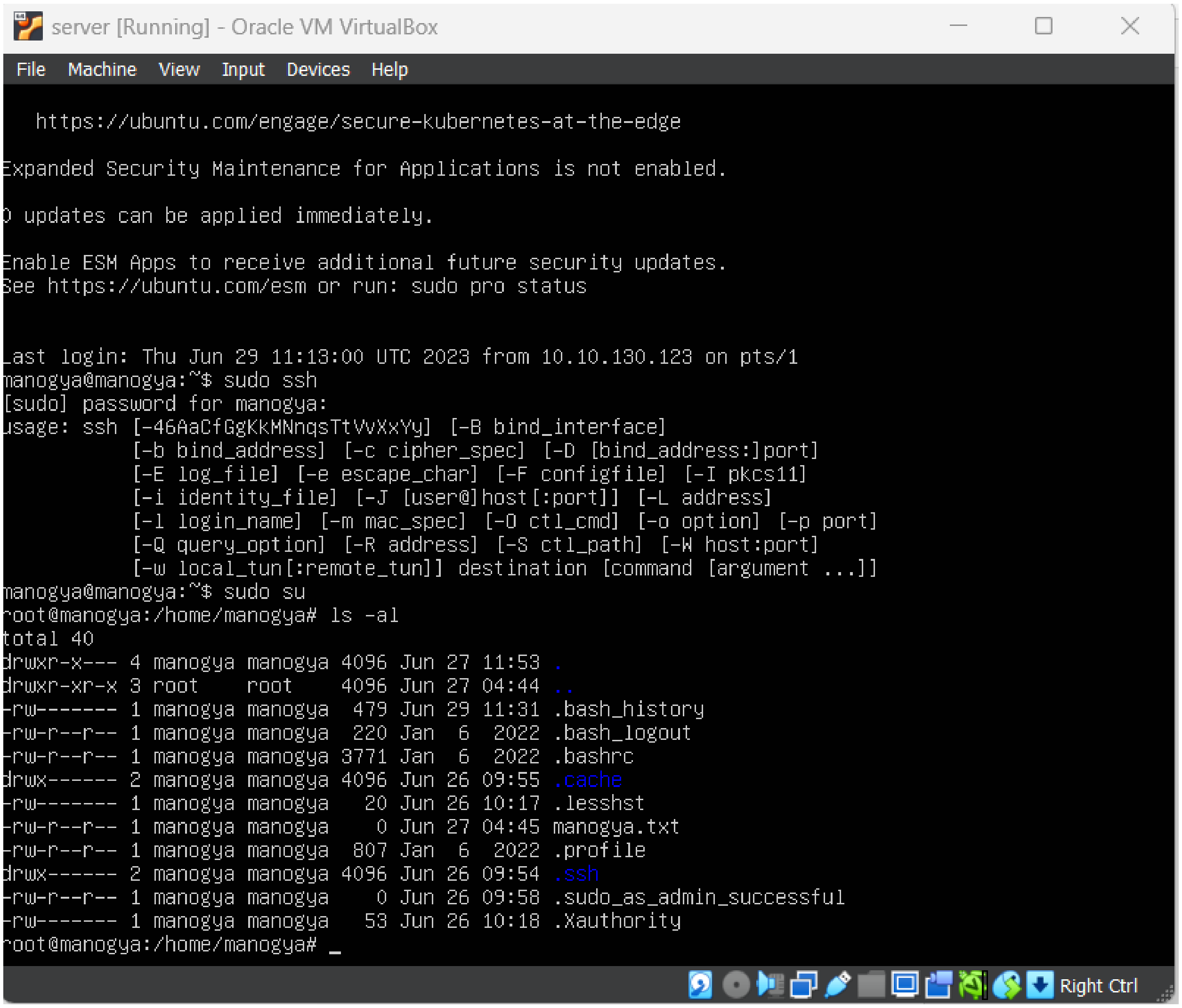


Figure 24

9. Changing host name Linux

- Open a terminal window on your Linux system. The method for opening a terminal varies depending on the Linux distribution you are using. You can usually find the terminal application in the system's application launcher or by pressing a keyboard shortcut like Ctrl+Alt+T.
- Check the current hostname:
- In the terminal, type the following command to check the current hostname:
- hostname
- The current hostname will be displayed in the terminal.
- Edit the hostname configuration file:
- Depending on your Linux distribution, the hostname is usually stored in the /etc/hostname file or the /etc/hosts file. You need to edit one of these files to change the hostname.
- Use a text editor like nano or vim to edit the file. For example, to edit the /etc/hostname file with nano, run the following command:
- sudo nano /etc/hostname
- If you need to edit the /etc/hosts file instead, use the following command:
- sudo nano /etc/hosts
- Change the hostname:
- In the editor, locate the line containing the current hostname.
- Modify the hostname to your desired value. Remove or replace the existing hostname with the new one.
- Save the changes and exit the editor. In nano, you can do this by pressing Ctrl+O to save and Ctrl+X to exit.
- Update the hostname:
- After editing the hostname configuration file, you need to update the hostname in the running system.
- Use the following command to update the hostname:
- sudo hostnamectl set-hostname <new_hostname>
- Replace <new_hostname> with your desired hostname.
- To view the files and groups in linux

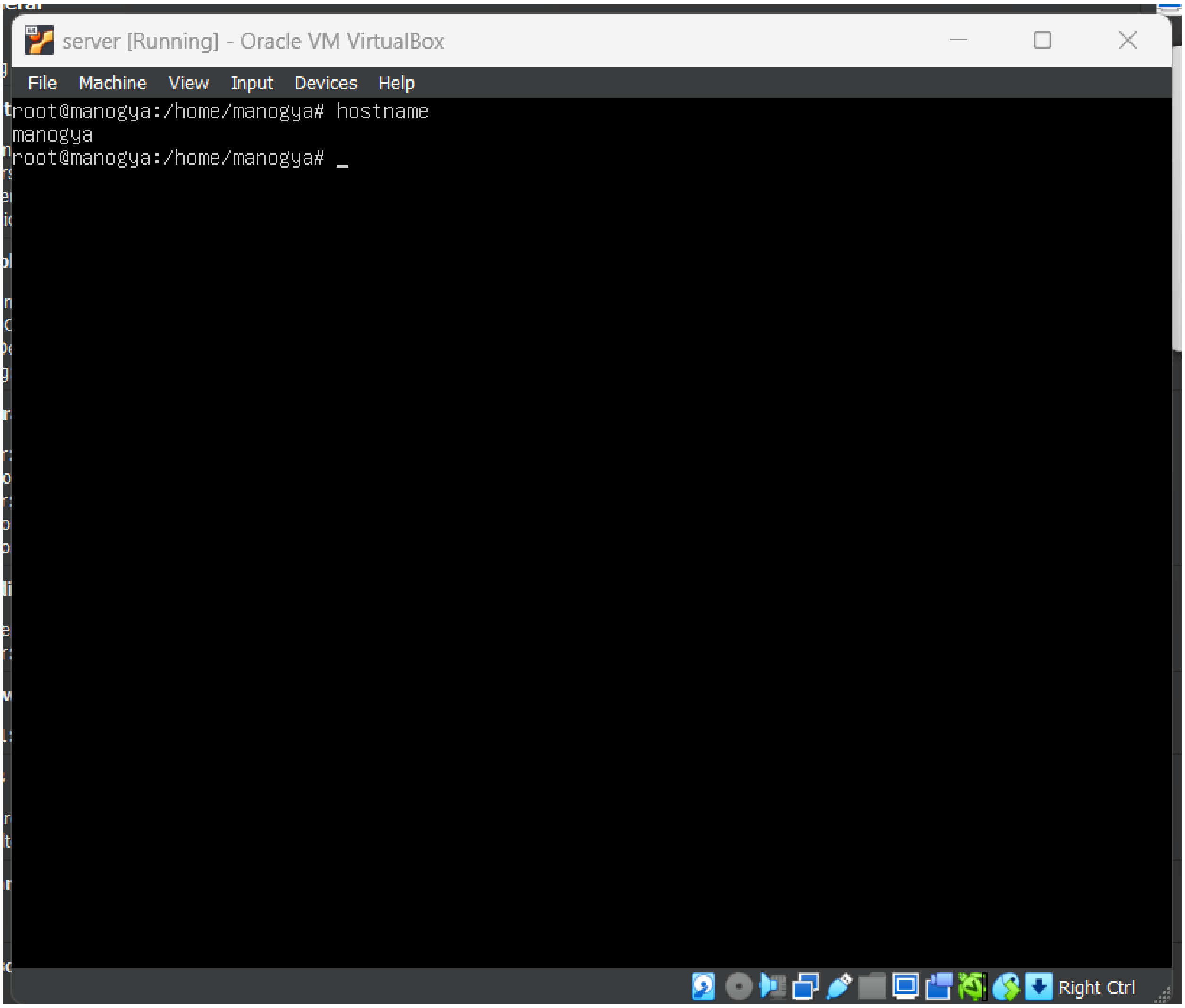


```
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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


Last login: Thu Jun 29 11:13:00 UTC 2023 from 10.10.130.123 on pts/1
manogya@manogya:~$ sudo ssh
[sudo] password for manogya:
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]
manogya@manogya:~$ sudo su
root@manogya:/home/manogya# ls -al
total 40
drwxr-x--- 4 manogya manogya 4096 Jun 27 11:53 .
drwxr-xr-x 3 root    root    4096 Jun 27 04:44 ..
-rw------- 1 manogya manogya  479 Jun 29 11:31 .bash_history
-rw-r--r-- 1 manogya manogya  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 manogya manogya 3771 Jan  6  2022 .bashrc
drwx------ 2 manogya manogya 4096 Jun 26 09:55 .cache
-rw------- 1 manogya manogya   20 Jun 26 10:17 .lesshst
-rw-r--r-- 1 manogya manogya    0 Jun 27 04:45 manogya.txt
-rw-r--r-- 1 manogya manogya  807 Jan  6  2022 .profile
drwx------ 2 manogya manogya 4096 Jun 26 09:54 .ssh
-rw-r--r-- 1 manogya manogya    0 Jun 26 09:58 .sudo_as_admin_successful
-rw------- 1 manogya manogya   53 Jun 26 10:18 .Xauthority
root@manogya:/home/manogya# _
```

Figure 25

10. Changing the hostname of a Linux system

- Open a terminal on your Linux system.
- Check the current hostname by running the hostname command:
- hostname
- To change the hostname, use the hostnamectl command with superuser privileges (sudo):
- sudo hostnamectl set-hostname newhostname
- Replace newhostname with the desired hostname you want to set.
- Open the /etc/hosts file with a text editor:
- sudo nano /etc/hosts
- Replace any occurrences of the old hostname with the new hostname in the file. Look for lines starting with 127.0.0.1 or ::1 and ensure that the new hostname is associated with the loopback address.
- Save the changes and exit the text editor.
- Restart your system or execute the following command to apply the new hostname without a system restart:



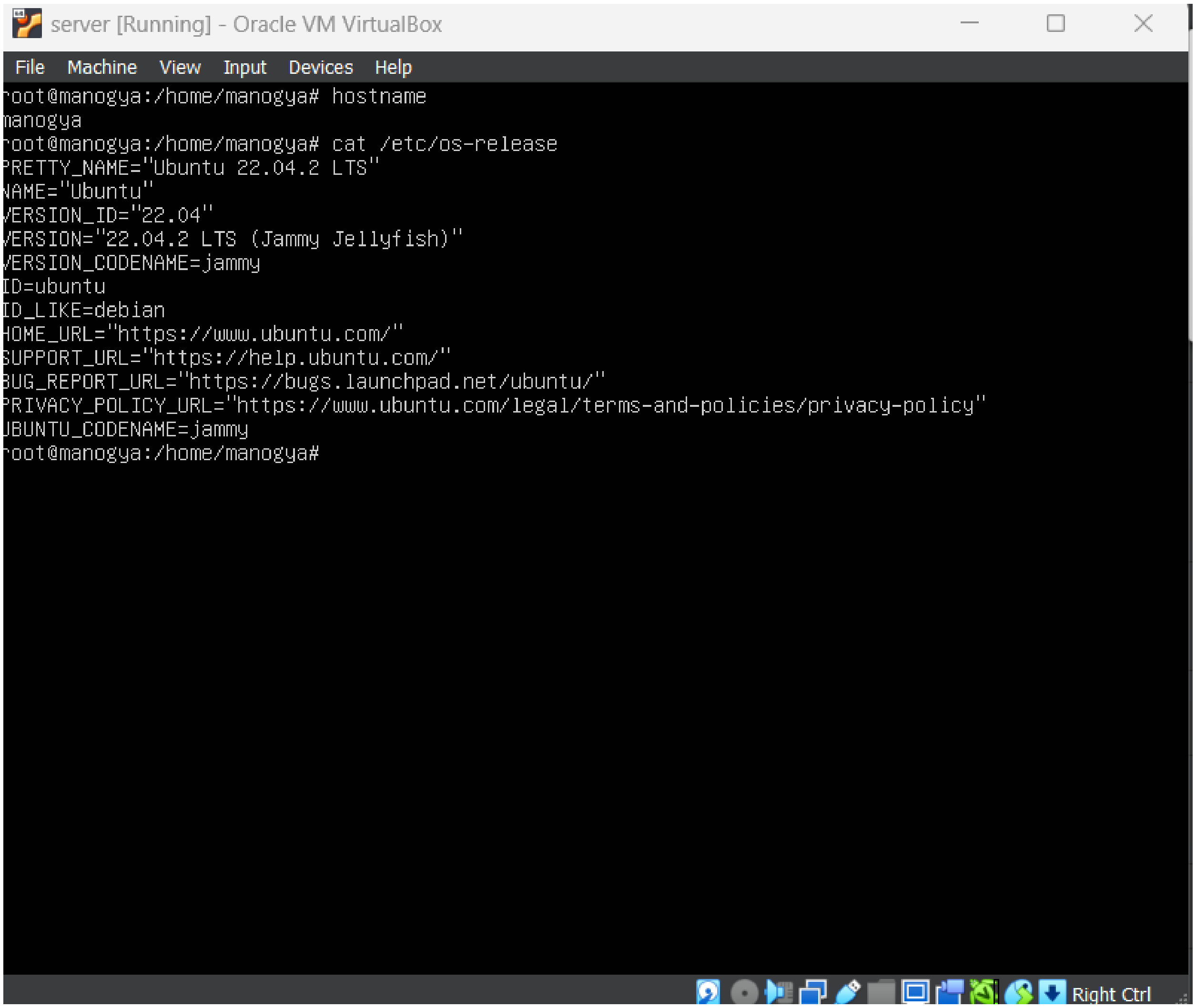
```
root@manogya:/home/manogya# hostname
manogya
root@manogya:/home/manogya# _
```

Figure 26

- To check the hostname of a Linux system, you can use the hostname command. Open a terminal and run the following command:
- hostname
- This command will display the current hostname of the system.
- If you want to see the fully qualified domain name (FQDN), which includes the hostname and the domain name, you can use the -f option with the hostname command:
- hostname -f

11. To check the version of the operating system in Linux

- Using the lsb_release command:
- Open a terminal and run the following command:
- lsb_release -a
- This command will display detailed information about the Linux distribution, including the release version.
- Checking the /etc/os-release file:
- Open a terminal and run the following command:
- cat /etc/os-release
- This command will display the contents of the /etc/os-release file, which contains information about the operating system, including the version.

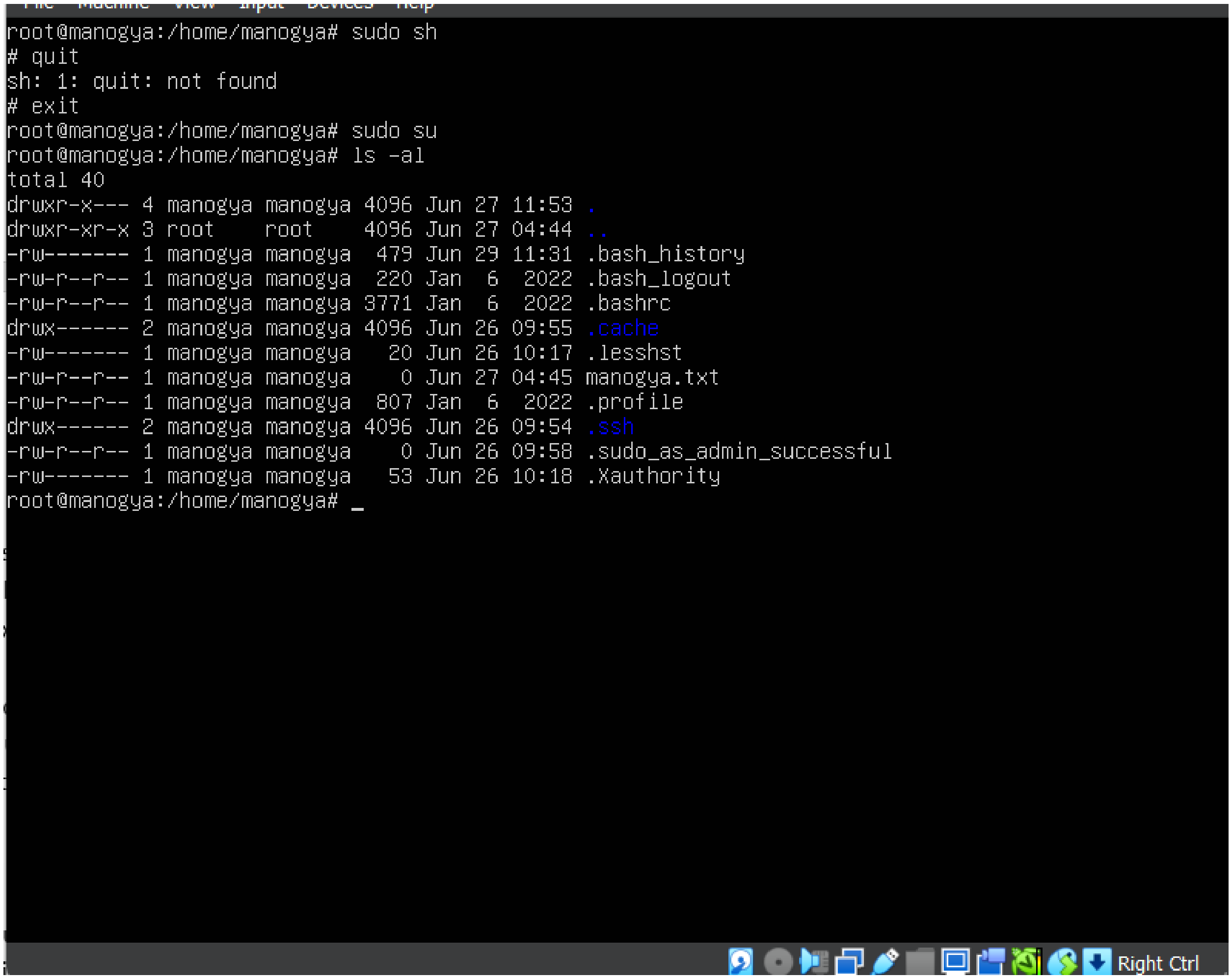
- 

```
root@manogya:/home/manogya# hostname
manogya
root@manogya:/home/manogya# cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.2 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
root@manogya:/home/manogya#
```

Figure 27

12. To change the user ownership of a file in Linux

- sudo chown newuser: filename



```
root@manogya:/home/manogya# sudo sh
# quit
sh: 1: quit: not found
# exit
root@manogya:/home/manogya# sudo su
root@manogya:/home/manogya# ls -al
total 40
drwxr-x--- 4 manogya manogya 4096 Jun 27 11:53 .
drwxr-xr-x 3 root    root    4096 Jun 27 04:44 ..
-rw------- 1 manogya manogya  479 Jun 29 11:31 .bash_history
-rw-r--r-- 1 manogya manogya  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 manogya manogya 3771 Jan  6  2022 .bashrc
drwx------ 2 manogya manogya 4096 Jun 26 09:55 .cache
-rw------- 1 manogya manogya   20 Jun 26 10:17 .lesshst
-rw-r--r-- 1 manogya manogya    0 Jun 27 04:45 manogya.txt
-rw-r--r-- 1 manogya manogya  807 Jan  6  2022 .profile
drwx------ 2 manogya manogya 4096 Jun 26 09:54 .ssh
-rw-r--r-- 1 manogya manogya    0 Jun 26 09:58 .sudo_as_admin_successful
-rw------- 1 manogya manogya   53 Jun 26 10:18 .Xauthority
root@manogya:/home/manogya# _
```

Figure 28

- Replace newuser with the username of the user you want to assign as the new owner, and filename with the name of the file or directory you wish to change.
- To create a new user in Linux, you can use the useradd command. Here's the general syntax:
- sudo useradd username
- Replace username with the desired username for the new user. By default, the useradd command will create a new user with the same name as the username
- However, creating a user with just the useradd command will not set a password or create a home directory for the user. To set a password for the new user, you can use the passwd command:

- sudo passwd username
- Replace username with the username of the user you want to set a password for. You will be prompted to enter and confirm the new password for the user.
- To create a home directory for the new user, you can use the -m option with the useradd command:
- sudo useradd -m username
- This will create a new user with the specified username and create a home directory for the user.
- After creating the new user, you can log in with the new user credentials and start using the account.

13. Installing MYSQL in ubuntu

- Update the package list to make sure you have the latest information about available packages:
  sudo apt update
- Install the MySQL Server package using the following command:
  sudo apt install mysql-server
- During the installation process, you will be prompted to set a root password for MySQL. Choose a strong password and confirm it.
- After the installation is complete, you can check the MySQL service status with the following command:
  sudo systemctl status mysql
- This command will show you whether MySQL is active and running.
- To secure your MySQL installation, run the MySQL security script:
  sudo mysql_secure_installation
- You can also start and enable the MySQL service
  sudo systemctl start mysql
  sudo systemctl enable mysql
- Finally, you can log in to the MySQL server with the following command, using the root user and the password you set earlier:
  sudo mysql -u root -p

14. Installing apache2 on ubuntu

- Update the package list to ensure you have the latest information about available packages:
  sudo apt update
- Install Apache 2 by running the following command:
  sudo apt install apache2
- After the installation is complete, Apache 2 should be up and running automatically. You can check the status of the Apache service to make sure it's active:
  sudo systemctl status apache2
- This command will display information about the Apache service, including whether it's active and running.

15. DNS (Domain Name System)

DNS (Domain Name System) translates human readable domain names for eg www.facebook.com to machine learning readable Ip address for e.g. (19.2.0.2.44)

All computers on the Internet, from your smart phone or laptop to the servers that serve content for massive retail websites, find and communicate with one another by using numbers

DNS record types

A (Address) Record: It maps a domain name to an IPv4 address. For example, it translates "example.com" to the corresponding IPv4 address like "192.0.2.1".

AAAA (IPv6 Address) Record: Similar to the A record, but it maps a domain name to an IPv6 address. It allows the translation of domain names to IPv6 addresses.

CNAME (Canonical Name) Record: It is used to create an alias for a domain name. Instead of pointing directly to an IP address, it points to another domain name. This is often used when multiple domain names need to resolve to the same IP address

MX (Mail Exchange) Record: It specifies the mail server responsible for accepting email messages on behalf of a domain. It includes the priority of mail servers when multiple servers are available.

TXT (Text) Record: It allows the addition of arbitrary text to a DNS record. It is commonly used for verification purposes, such as SPF (Sender Policy Framework) records used for email authentication.

NS (Name Server) Record: It specifies the authoritative name servers for a domain. These name servers store the DNS records for the domain and handle the resolution of queries.

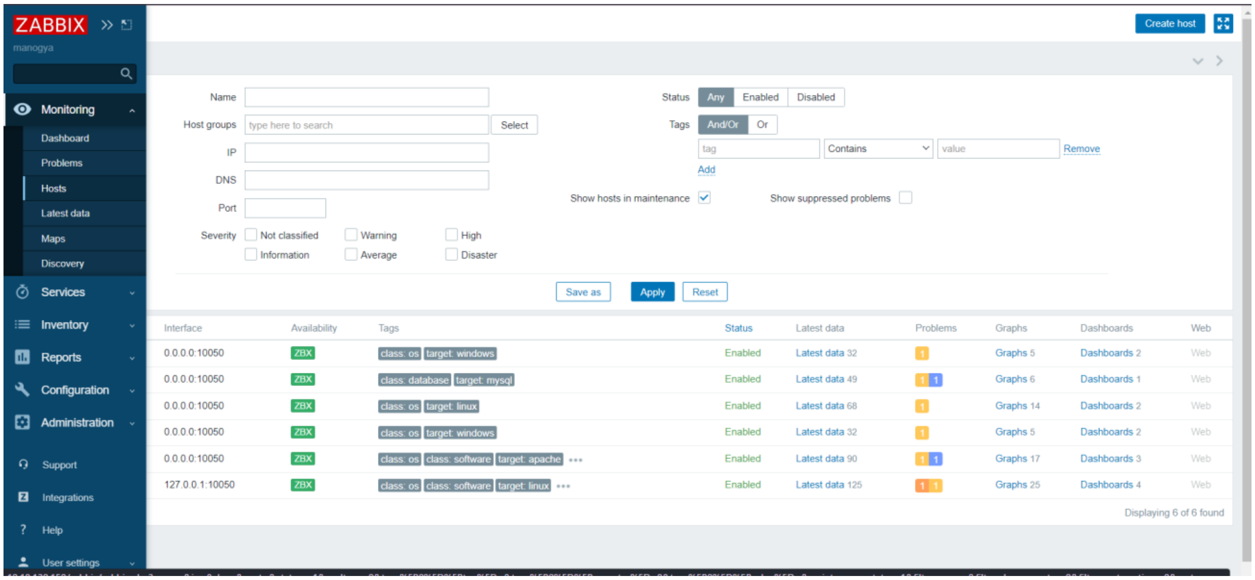
SOA (Start of Authority) Record: It contains administrative information about a DNS zone, such as the primary name server, contact email address, serial number, and other settings.

PTR (Pointer) Record: It is used for reverse DNS lookup. Instead of translating a domain name to an IP address, it maps an IP address to a domain name.

SRV (Service) Record: It defines the location of a specific service within a domain. It is commonly used for services like VoIP, SIP, or other network protocols.

16. Creating host in Zabbix server

- Log into your Zabbix server
- Navigate to the Configuration tab in the top menu.



Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
0.0.0.0:10050	ZBX	class: os target: windows	Enabled	Latest data 32	1	Graphs 5	Dashboards 2	Web
0.0.0.0:10050	ZBX	class: database target: mysql	Enabled	Latest data 49	1 1	Graphs 6	Dashboards 1	Web
0.0.0.0:10050	ZBX	class: os target: linux	Enabled	Latest data 68	1	Graphs 14	Dashboards 2	Web
0.0.0.0:10050	ZBX	class: os target: windows	Enabled	Latest data 32	1	Graphs 5	Dashboards 2	Web
0.0.0.0:10050	ZBX	class: os class: software target: apache •••	Enabled	Latest data 90	1 1	Graphs 17	Dashboards 3	Web
127.0.0.1:10050	ZBX	class: os class: software target: linux •••	Enabled	Latest data 125	1 1	Graphs 25	Dashboards 4	Web

Displaying 6 of 6 found

Figure 29

- Click on the "Create Host "Tab

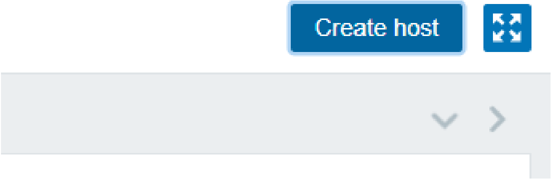
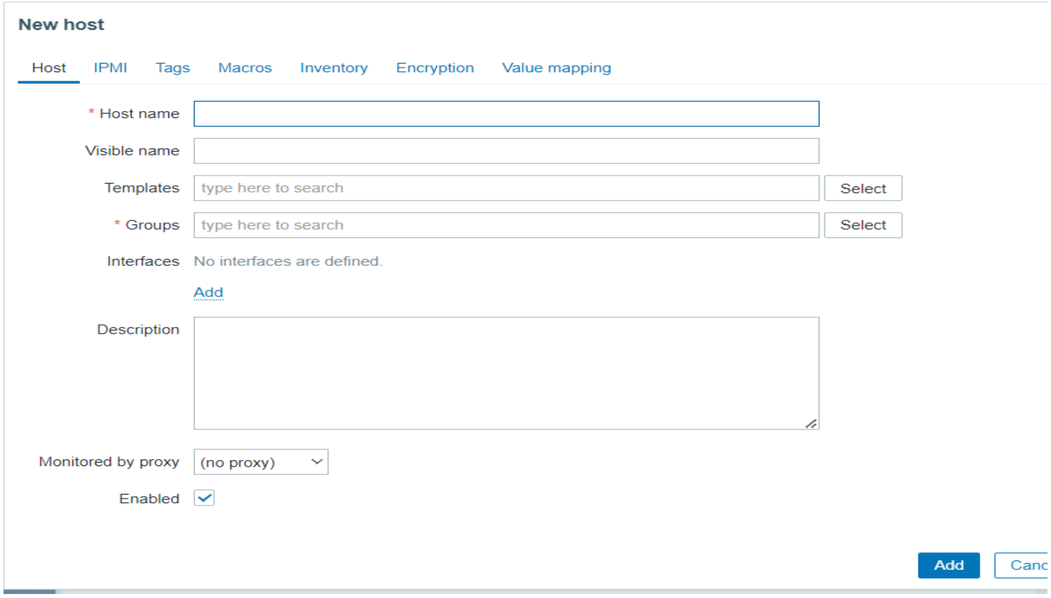


Figure 30

- you will need to fill in the necessary information for the host



* Host name

Visible name

Templates: type here to search [Select]

* Groups: type here to search [Select]

Interfaces: No interfaces are defined.

Add

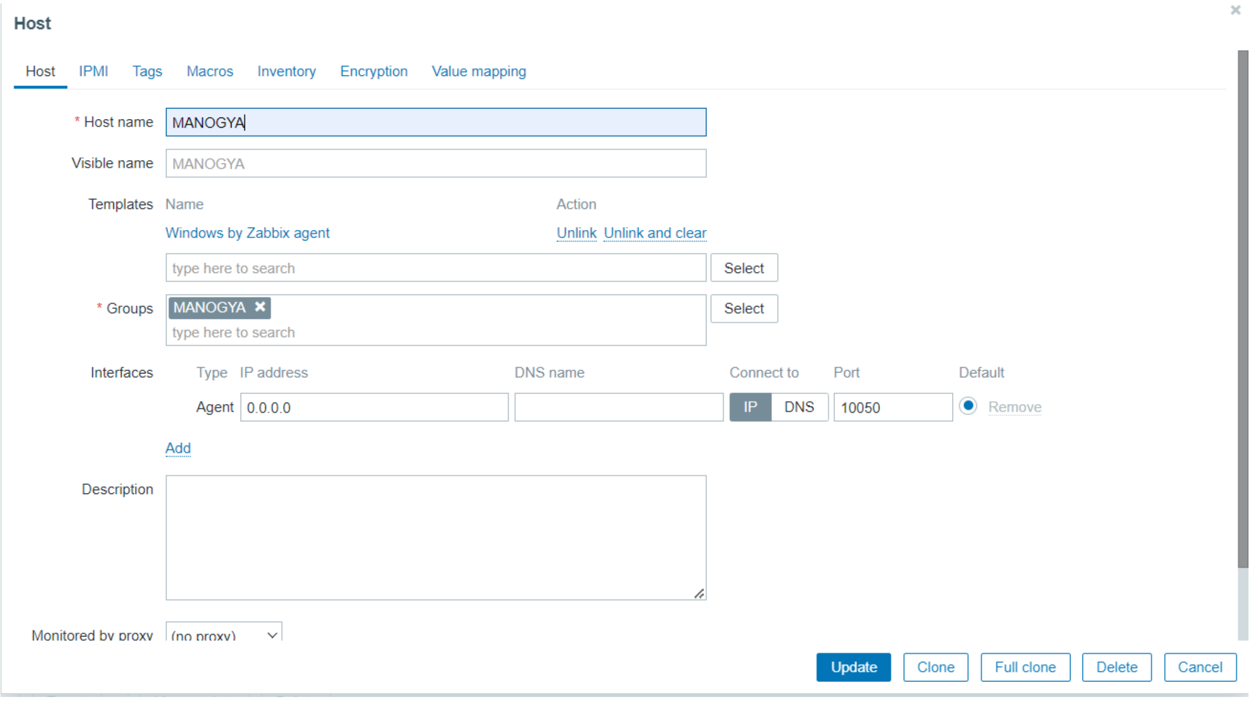
Description

Monitored by proxy: (no proxy)

Enabled: ☑

Figure 32

- Think of a name for the host, Type that name in the "Host name" field.
- Next, you need to pick a group for your host.
- Now, enter the IP address or DNS name of the host in the "IP address" field.
- use the default port for the monitoring method you choose or you can set it to 0.0.0.0
- Select the monitoring method from the options available, like Zabbix agent, SNMP, JMX, and others in templet option
- At last click “Add" button to save the host configuration.



* Host name: MANOGYA

Visible name: MANOGYA

Templates:

Name	Action
Windows by Zabbix agent	Unlink Unlink and clear

type here to search [Select]

* Groups: MANOGYA ✖ type here to search [Select]

Interfaces:

Type	IP address	DNS name	Connect to	Port	Default	
Agent	0.0.0.0		IP DNS	10050	●	Remove

Add

Description

Monitored by proxy: (no proxy)

Figure 33

17. Solution of some Zabbix problems

Fix SNMP timeout: ensuring that he device running the snmp manager can reach the device being monitored via snmp. Verify the network configuration, including IP addresses, subnets, gateways, and firewall settings. Make sure that SNMP is properly configured on both the SNMP manager and the SNMP agent device

Download-IN traffic on IF TMS-58-2158: Identify the source of the traffic: Determine which devices or applications are generating the high "Download-IN" traffic on interface TMS-58-2158. Use network monitoring tools or traffic analysis tools to identify the top talkers or applications consuming the bandwidth

Upload-OUT traffic on IF RTR_1: Identify the source of the traffic: Determine which devices or applications are generating the high "Upload-OUT" traffic on interface RTR_1. Use network monitoring tools or traffic analysis tools to identify the top talkers or applications generating the traffic.

Available Memory on TMS_57: Identify memory-consuming processes: Use system monitoring tools or commands specific to the operating system running on TMS_57 to identify processes or applications that are consuming a significant amount of memory. This will help you pinpoint the source of the memory usage

Wildfly service is down on TMS_58_WF3 : Check the service status: Verify the current status of the Wildfly service on TMS_58_WF3. This can be done by checking the service status command or using service management tools specific to the operating system running on TMS_58_WF3

DISK SIZE LESS THAN 10 % IN E: Check disk usage: Verify the current disk usage on drive E to determine how much space is being utilized. This can be done by right-clicking on the drive and selecting "Properties" or by using a disk usage analysis tool

High memory utilization: Restart or terminate memory-intensive processes: If you identify specific processes or applications consuming excessive memory, consider restarting or terminating them. This can help free up memory resources and alleviate the high memory utilization

18. IMPORTANT PORTS

20 and 21: file transfer protocol (FTP)

22: Secure Shell (SSH)

53: Domain Name System (DNS

80: Hypertext Transfer Protocol (HTTP)

23: Network Time Protocol (NTP)

Port 179: Border Gateway Protocol (BGP)

443: HTTP Secure (HTTPS)

500: Internet Security Association and Key Management Protocol (ISAKMP)

587: Modern, secure SMTP

3389: Remote Desktop Protocol (RDP)

143 IMAP

110: POP

19. Type 1 Hypervisor Examples

- VMware hypervisors like vSphere, ESXi and ESX.
- Microsoft Hyper-V.
- Oracle VM Server.
- Citrix Hypervisor/XEN
- KVM
- RHEV
- Oracel VM Server
- IBM PowerVM

20. Examples of Type 2 hypervisors

- Microsoft Virtual PC.
- Oracle Virtual Box.
- VMware Workstation.
- Oracle Solaris Zones.
- VMware Fusion.
- Oracle VM Server for x86.
- CentOS Virtualization.

21. Linux OS distros

- Ubuntu
- Debian
- Fedora
- Redhat
- Arch Linux
- Linux Mint
- openSUSE
- Manjora

22. INSTALLING ZABBIX

- Install Zabbix repository

- # wgethttps://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
- wget: It is a command-line utility for downloading files from the web.
- https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb: This is the URL of the file you are trying to download. It points to a Debian package file (deb) for the Zabbix repository and contains the necessary information to install and configure Zabbix monitoring software.
- When you execute this command, wget will retrieve the specified file (zabbix-release_6.0-4+ubuntu22.04_all.deb) and save it to your current working directory.
- After downloading the file, you can typically install it using a package manager like dpkg or apt to add the Zabbix repository to your system and gain access to the Zabbix monitoring software and related packages.
- # dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb
- dpkg: It is a package management command-line tool used in Debian-based systems, including Ubuntu, to install, remove, and manage software packages.
- -i: It is an option for dpkg that specifies that the package file should be installed.
- zabbix-release_6.0-4+ubuntu22.04_all.deb: This is the name of the Debian package file you want to install.
- #apt update
- This command is used to update the package information

- **Install Zabbix server, frontend, agent**

- # apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
- apt: It is a command-line package management tool used in Debian-based systems, including Ubuntu, for managing software packages.
- install: It is a command for apt that instructs it to install the specified packages.
- zabbix-server-mysql: This package contains the Zabbix server component that uses MySQL as the database backend.
- zabbix-frontend-php: This package provides the PHP-based frontend for the Zabbix monitoring system.

- zabbix-apache-conf: This package includes the Apache configuration files required to host the Zabbix frontend.
- zabbix-sql-scripts: This package contains SQL scripts used to set up the necessary database schema and initial data for Zabbix.
- zabbix-agent: This package includes the Zabbix agent, which is installed on the monitored hosts to collect data and send it to the Zabbix server.

  - **Create initial database**

-
  ```
  # mysql -uroot -p
  password
  mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
  mysql> create user zabbix@localhost identified by 'password';
  mysql> grant all privileges on zabbix.* to zabbix@localhost;
  mysql> set global log_bin_trust_function_creators = 1;
  mysql> quit;
  ```
- mysql -uroot -p: This command starts the MySQL command-line client and connects to the MySQL server using the root user. The -p flag prompts you to enter the password interactively.
- password: Here, you should enter the password for the root user when prompted. The actual pssword should be provided here.
- mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;: This command is executed within the MySQL command-line client. It creates a new database named zabbix with the character set utf8mb4 and collation utf8mb4_bin. These settings ensure that the database can handle Unicode characters properly.

- mysql> create user zabbix@localhost identified by 'password';: This command creates a new MySQL user named zabbix and assigns it a password. The zabbix user is configured to connect from the localhost (the same machine where MySQL is running).
- mysql> grant all privileges on zabbix.* to zabbix@localhost;: This command grants all privileges to the zabbix user on the zabbix database. This allows the zabbix user to perform any operation on the zabbix database.

- mysql> set global log_bin_trust_function_creators = 1;: This command sets the log_bin_trust_function_creators system variable to 1. It enables the creation of stored functions and triggers by non-superusers, such as the zabbix user.
- mysql> quit;: This command exits the MySQL command-line client and returns you to the regular command prompt.
- # zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p Zabbix
- This command is used to import and execute the Zabbix server database schema and initial data in a MySQL database.
- mysql -uroot -p: This command starts the MySQL command-line client and connects to the MySQL server using the root user. The -p flag prompts you to enter the password interactively.
- password: Here, you should enter the password for the root user when prompted. The actual password should be provided here.
- mysql> set global log_bin_trust_function_creators = 0;: This command is executed within the MySQL command-line client. It modifies the global system variable log_bin_trust_function_creators and sets its value to 0. This variable controls whether non-superusers can create or modify stored functions and triggers. By setting it to 0, non-superusers will not be able to create or modify these objects.
- mysql> quit;: This command exits the MySQL command-line client and returns you to the regular command prompt.

- **Configure the database for Zabbix server**
- Edit file /etc/zabbix/zabbix_server.conf

- DBPassword=

- **f. Open Zabbix UI web page**
- The default URL for Zabbix UI when using Apache web server is http://host/zabbix

23. INSTALLING ZABBIX AGENT

Install Zabbix repository

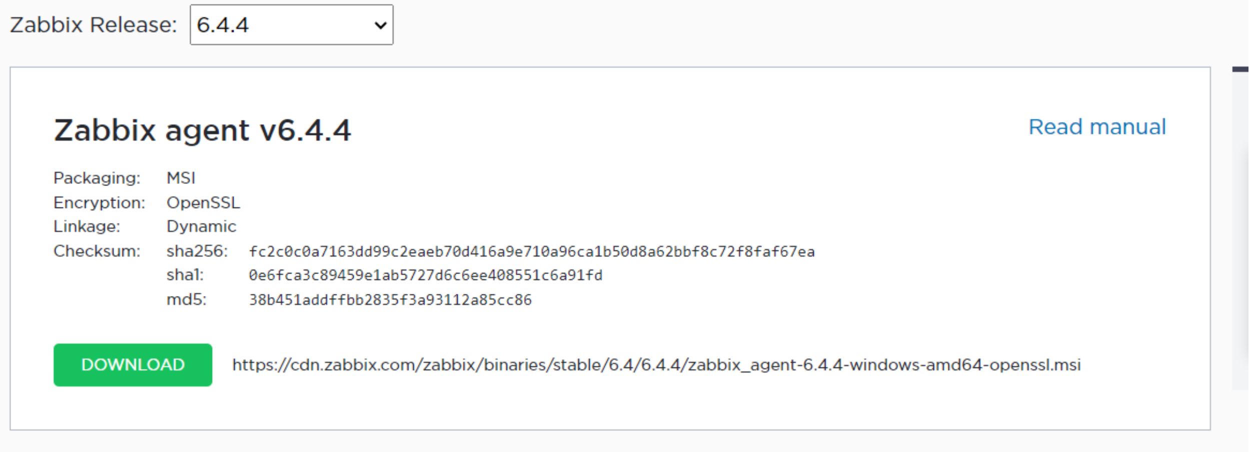
- # wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
- wget": The command itself, which initiates the file download.
- "https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb": The URL of the file you want to download. In this case, it points to a specific Debian package file for the Zabbix monitoring software, version 6.0-4, designed for Ubuntu 22.04.
-

  # dpkg -i The command "dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb" is used to install a Debian package file with the name "zabbix-release_6.0-4+ubuntu22.04_all.deb". zabbix-release_6.0-4+ubuntu22.04_all.deb
  # apt update
- This commands updates that package cache
- **Install Zabbix agent**
- # apt install zabbix-agent
- By running "apt install Zabbix-agent," you install the Zabbix agent, which is a component of the Zabbix monitoring system. The agent allows the Zabbix server to collect data from the monitored system, enabling monitoring and management of various metrics such as CPU usage, memory utilization, network activity, and more.
- **Start Zabbix agent process**
- # systemctl restart zabbix-agent
- This command restarts the zabbix agent
  # systemctl enable zabbix-agent
- This command is used to enable zabbix agent
- Making changes in Zabbix configure files
- Hostname
- Server active ip address
- Start agent two parameters 0 and 3 (0 for active and 3 for passive)
- TLSConnect = unencrypted

- TLSAccept= unencrypted

24. Monitor windows by using Zabbix

- Download Zabbix agent for windows



Zabbix Release: 6.4.4

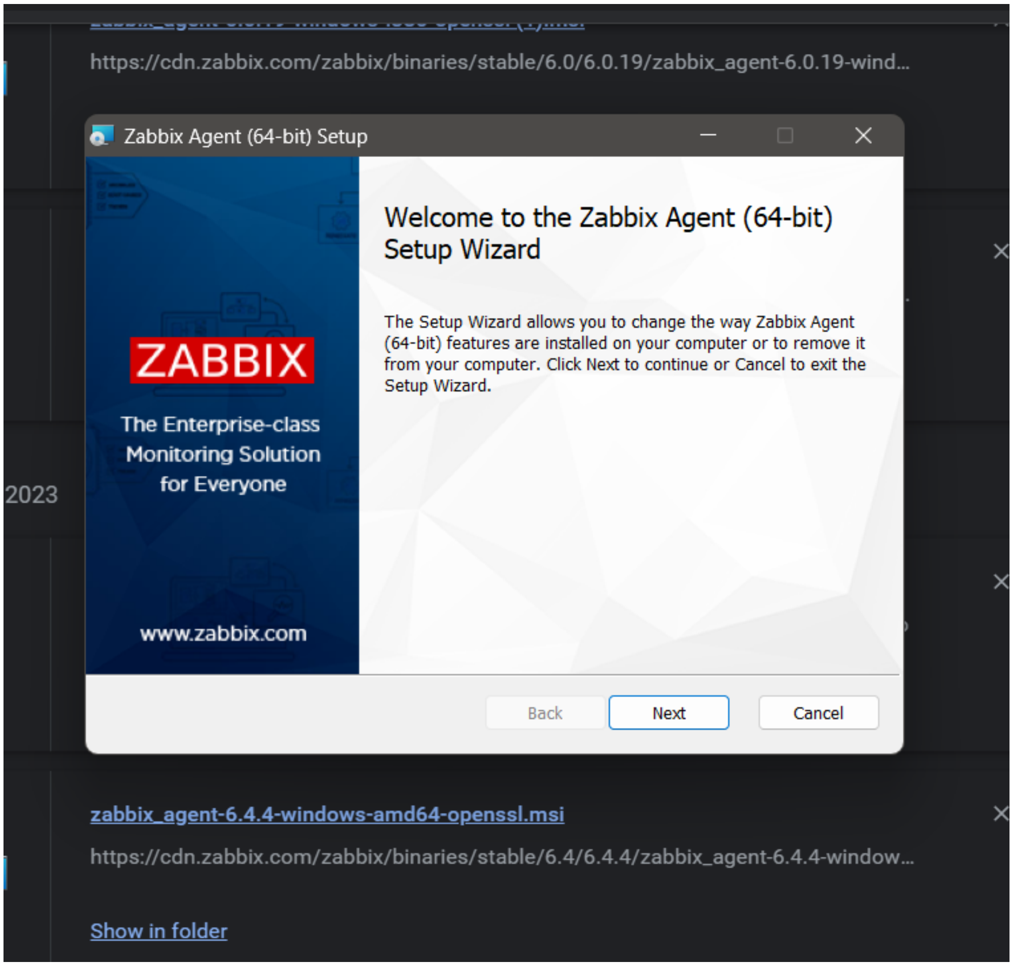
Zabbix agent v6.4.4

Packaging:	MSI	
Encryption:	OpenSSL	
Linkage:	Dynamic	
Checksum:	sha256:	fc2c0c0a7163dd99c2eaeb70d416a9e710a96ca1b50d8a62bbf8c72f8faf67ea
	sha1:	0e6fca3c89459e1ab5727d6c6ee408551c6a91fd
	md5:	38b451addffbb2835f3a93112a85cc86

https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.4/zabbix_agent-6.4.4-windows-amd64-openssl.msi

Figure 34

- Complete the installation



https://cdn.zabbix.com/zabbix/binaries/stable/6.0/6.0.19/zabbix_agent-6.0.19-wind...

Zabbix Agent (64-bit) Setup

Welcome to the Zabbix Agent (64-bit) Setup Wizard

The Setup Wizard allows you to change the way Zabbix Agent (64-bit) features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

zabbix_agent-6.4.4-windows-amd64-openssl.msi

https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.4/zabbix_agent-6.4.4-window...

Show in folder

Figure 35

- Edit the Zabbix configuration file
- Locate Zabbix.gentd.conf file in your local disk c and modify the parameters as shown below :

Server=<IP address of the Zabbix server>

ServerActive=<IP address of the Zabbix server>

Hostname=<The FQDN of the Windows server>

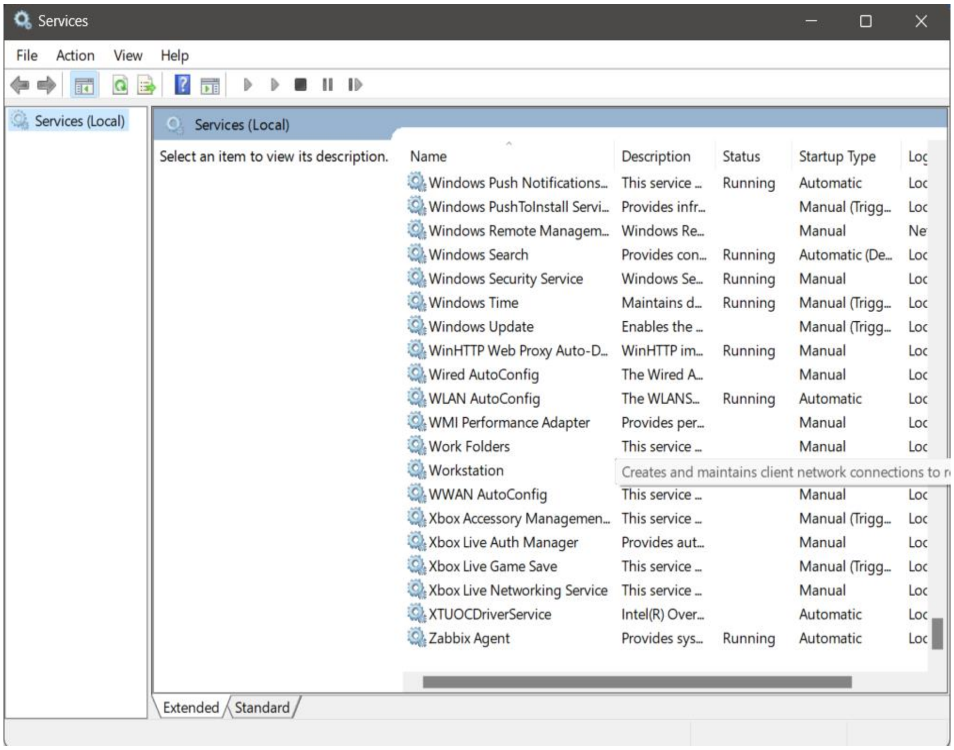
- Save the changes and exit the file
- With all the configurations in order, run command prompt as administrator and install Zabbix using the syntax as shown:

```
C:\> {full system path to zabbix_agentd.exe) –config  {full system path to zabbix_agentd.win.conf} –install
```

- After the installation start the Zabbix using this syntax:

```
C:\> {full system path to zabbix_agentd.exe) –start
```

- To confirm that the Zabbix agent is running, head out to the ‘Windows Services’ application and confirm that the Zabbix agent is up and running.



Select an item to view its description.

Name	Description	Status	Startup Type	Loc
Windows Push Notifications...	This service ...	Running	Automatic	Loc
Windows PushToInstall Servi...	Provides infr...		Manual (Trigg...	Loc
Windows Remote Managem...	Windows Re...		Manual	Ne
Windows Search	Provides con...	Running	Automatic (De...	Loc
Windows Security Service	Windows Se...	Running	Manual	Loc
Windows Time	Maintains d...	Running	Manual (Trigg...	Loc
Windows Update	Enables the ...		Manual (Trigg...	Loc
WinHTTP Web Proxy Auto-D...	WinHTTP im...	Running	Manual	Loc
Wired AutoConfig	The Wired A...		Manual	Loc
WLAN AutoConfig	The WLANS...	Running	Automatic	Loc
WMI Performance Adapter	Provides per...		Manual	Loc
Work Folders	This service ...		Manual	Loc
Workstation	Creates and maintains client network connections to r			
WWAN AutoConfig	This service ...		Manual	Loc
Xbox Accessory Managemen...	This service ...		Manual (Trigg...	Loc
Xbox Live Auth Manager	Provides aut...		Manual	Loc
Xbox Live Game Save	This service ...		Manual (Trigg...	Loc
Xbox Live Networking Service	This service ...		Manual	Loc
XTUOCDriverService	Intel(R) Over...		Automatic	Loc
Zabbix Agent	Provides sys...	Running	Automatic	Loc

Figure 36

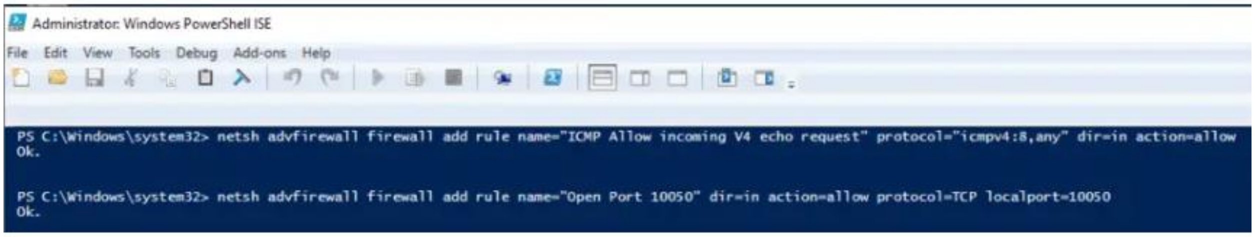
- Configure Windows firewall for Zabbix Agent
- Run the following command in windows powershell

```
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo
request" protocol="icmpv4:8,any" dir=in action=allow
```

- By default, the Windows firewall is enabled and blocks incoming and going connections. We are therefore going to make a few changes to allow traffic from the Windows Server host to the Zabbix server.
- First, we are going to allow ICMP protocol for the Zabbix server to establish network communication with the Windows host and report any errors when they occur. Therefore, run Windows Powershell with Administrative privileges and execute the command as shown

- Next, allows port 10050 – which is the default port that Zabbix listens to – on the firewall.

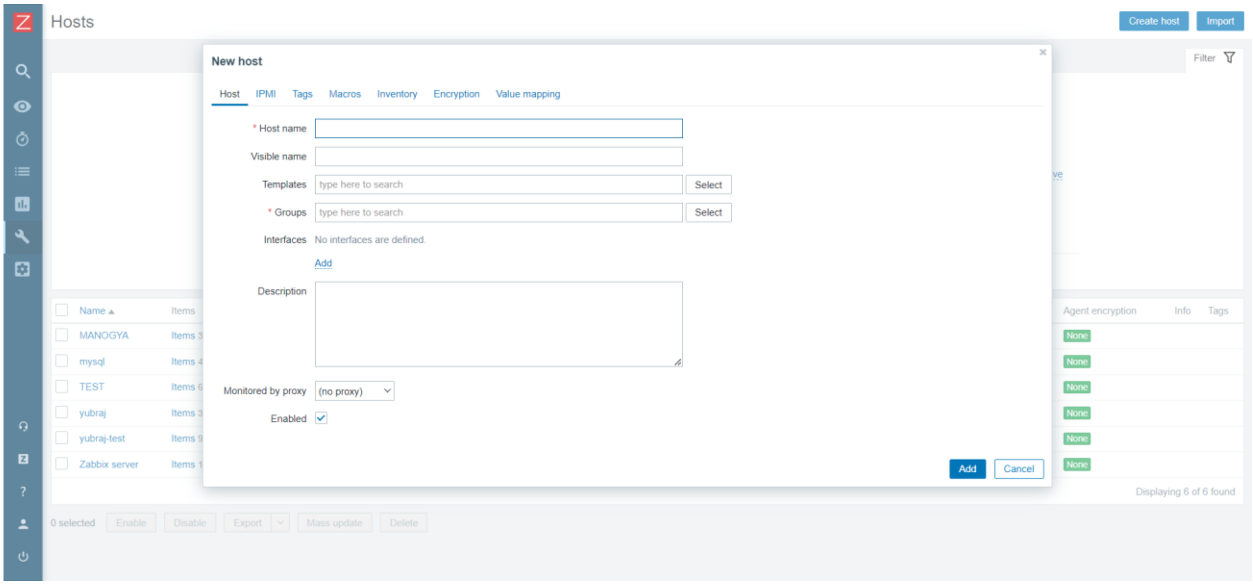
netsh advfirewall firewall add rule name="Open Port 10050" dir=in action=allow protocol=TCP localport=10050


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
PS C:\Windows\system32> netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol="icmpv4:8,any" dir=in action=allow
Ok.

PS C:\Windows\system32> netsh advfirewall firewall add rule name="Open Port 10050" dir=in action=allow protocol=TCP localport=10050
Ok.
```

Figure 37

- Add a Windows host on Zabbix Server



* Host name

Visible name

Templates: type here to search

* Groups: type here to search

Interfaces: No interfaces are defined.

Description

Monitored by proxy: (no proxy)

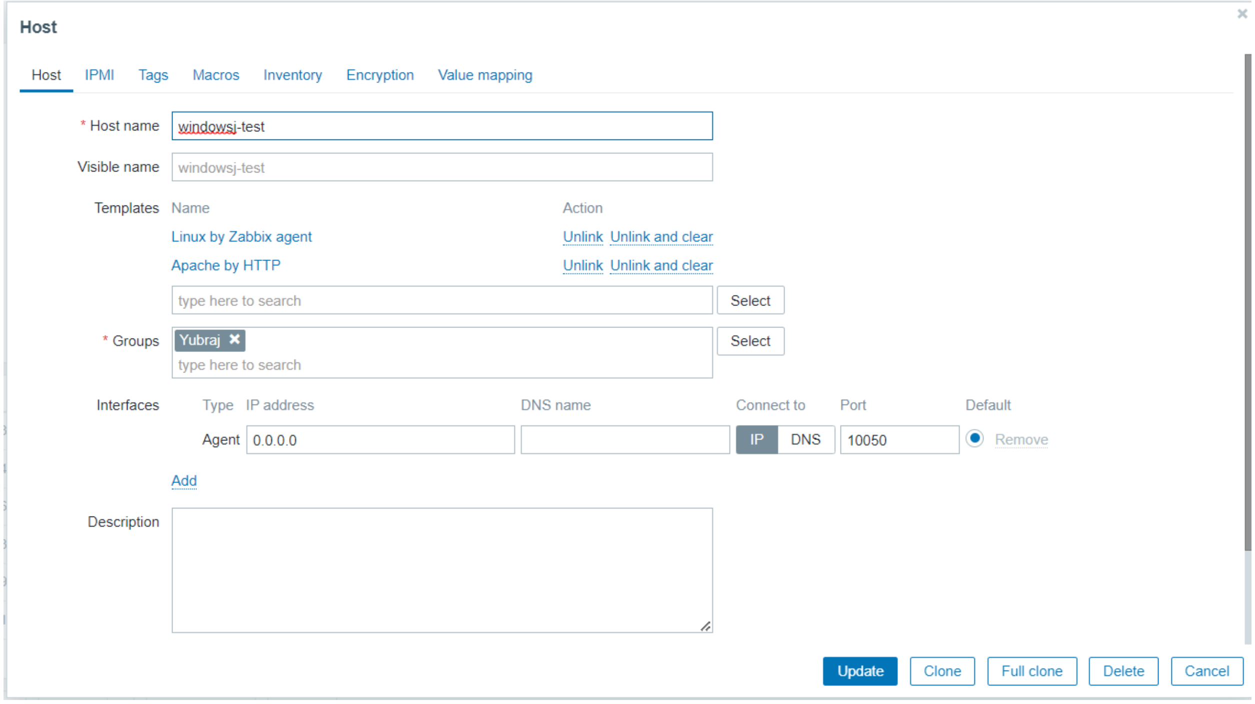
Enabled: ☑

Name ▲	Items	Agent encryption	Info	Tags
MANOGYA	Items 3	None		
mysql	Items 4	None		
TEST	Items 6	None		
yubraj	Items 3	None		
yubraj-test	Items 9	None		
Zabbix server	Items 1	None		

Displaying 6 of 6 found

Figure 38

- fill out the Windows host details such as hostname, visible name and IP address



* Host name: windowsj-test

Visible name: windowsj-test

Templates

Name	Action
Linux by Zabbix agent	Unlink Unlink and clear
Apache by HTTP	Unlink Unlink and clear

type here to search

* Groups: Yubraj ✖

type here to search

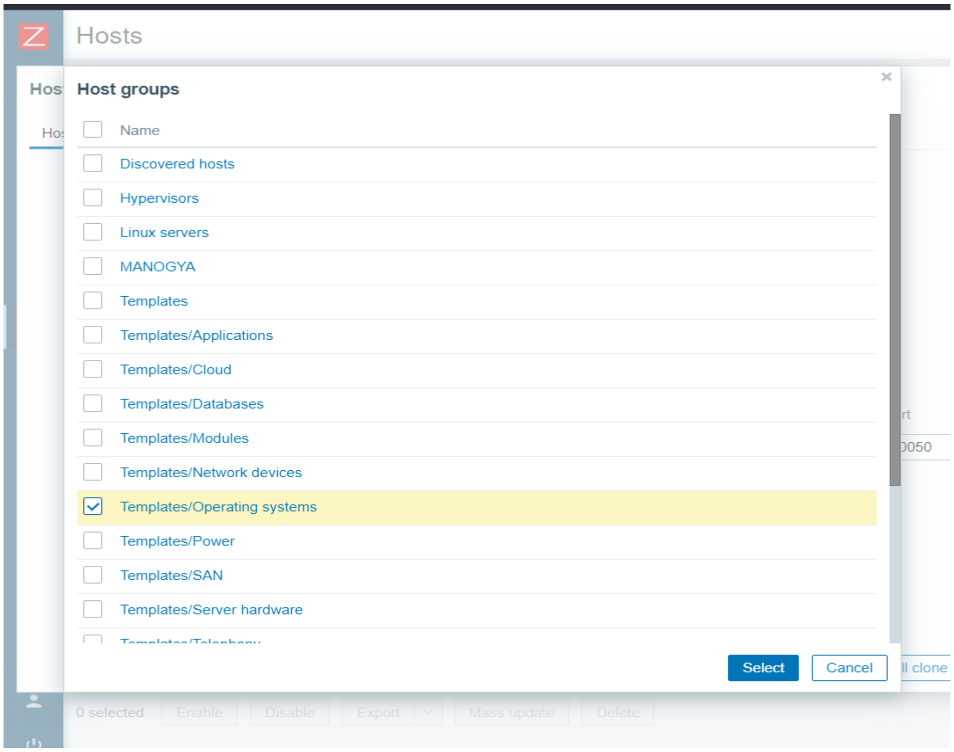
Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	0.0.0.0		IP DNS	10050	● Remove

Description

Figure 39

- For the ‘Groups’ section, click on the ‘Select’ button and click on the ‘Templates/Operating system’ option or you can create your own group



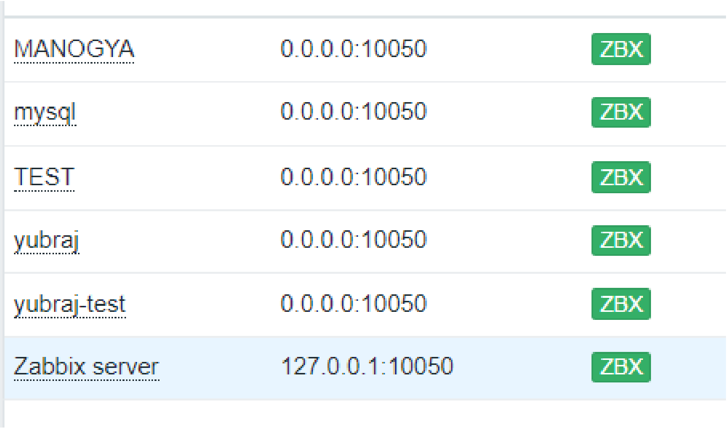
Hosts

Host groups

☐	Name
☐	Discovered hosts
☐	Hypervisors
☐	Linux servers
☐	MANOGYA
☐	Templates
☐	Templates/Applications
☐	Templates/Cloud
☐	Templates/Databases
☐	Templates/Modules
☐	Templates/Network devices
☑	Templates/Operating systems
☐	Templates/Power
☐	Templates/SAN
☐	Templates/Server hardware
☐	Templates/Telephony

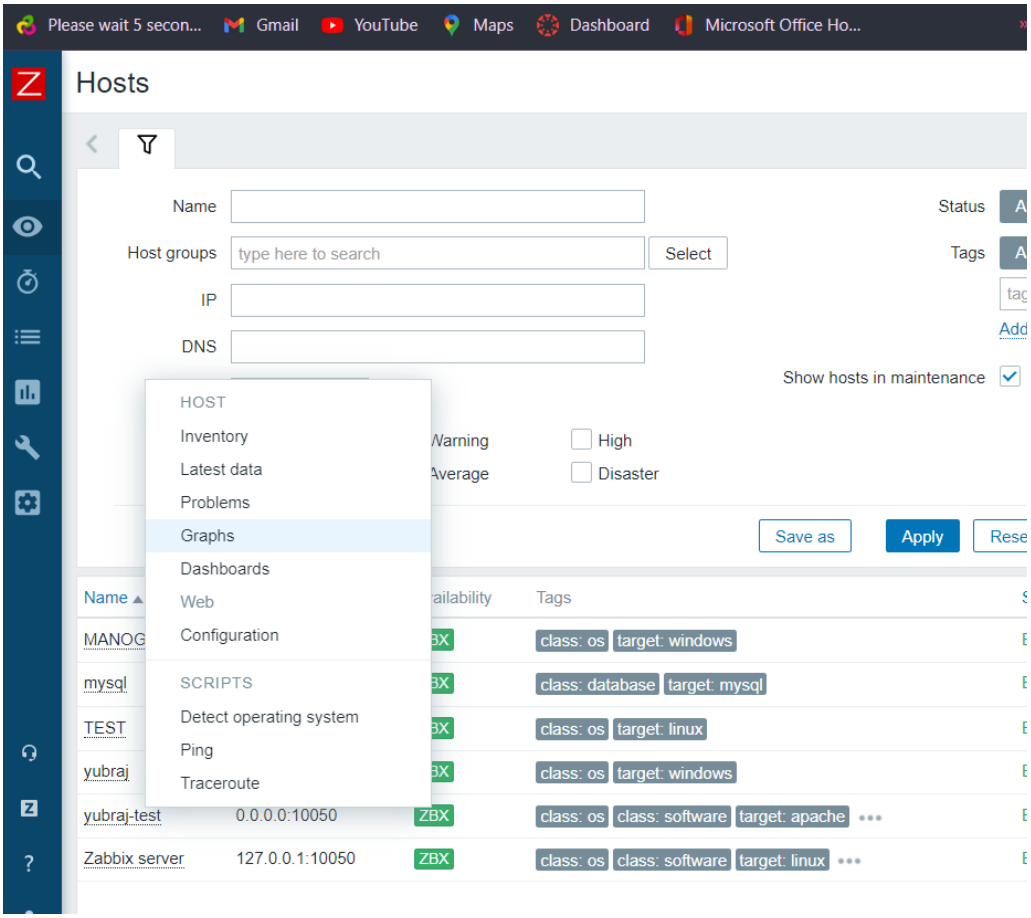
Figure 40

- After selecting host create a host click on the select button
- On the dashboard, check the Windows host listed as shown below. Note that the state is indicated 'Enabled' with the Zabbix icon 'ZBX' in green color.



MANOGYA	0.0.0.0:10050	ZBX
mysql	0.0.0.0:10050	ZBX
TEST	0.0.0.0:10050	ZBX
yubraj	0.0.0.0:10050	ZBX
yubraj-test	0.0.0.0:10050	ZBX
Zabbix server	127.0.0.1:10050	ZBX

- To graph the metrics associated with the Windows host system, click on 'Monitoring' –> 'Hosts'. Click on the Windows host and select 'Graphs'.



Name ▲		ailability	Tags
MANOG		BX	class: os target: windows
mysql		BX	class: database target: mysql
TEST		BX	class: os target: linux
yubraj		BX	class: os target: windows
yubraj-test	0.0.0.0:10050	ZBX	class: os class: software target: apache •••
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux •••

Figure 41

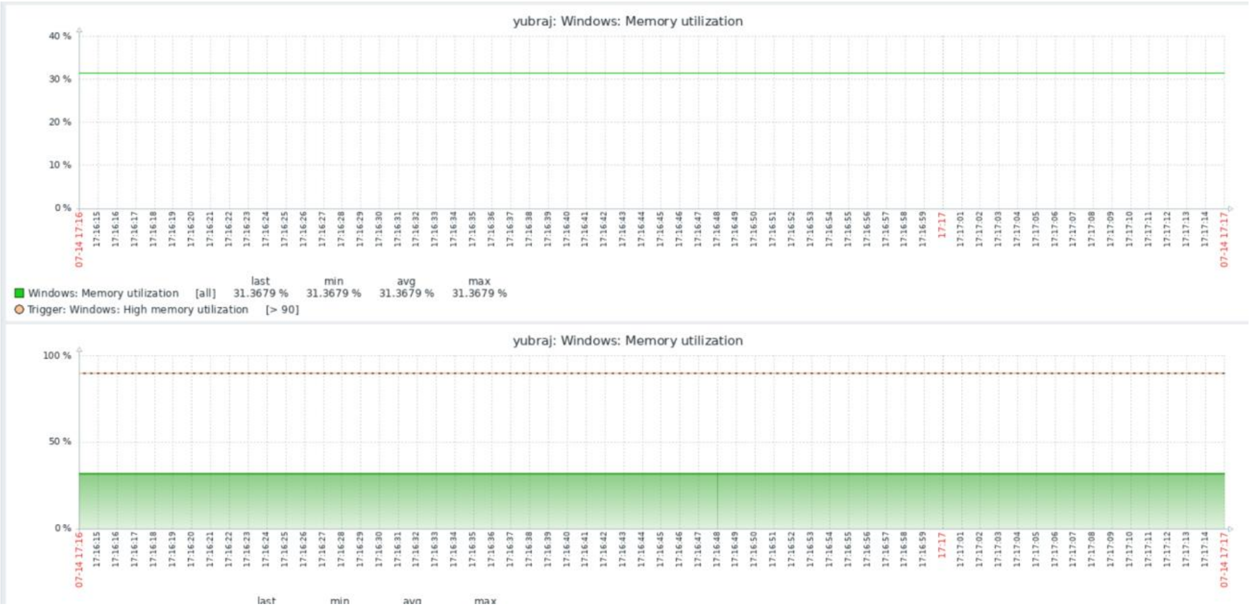
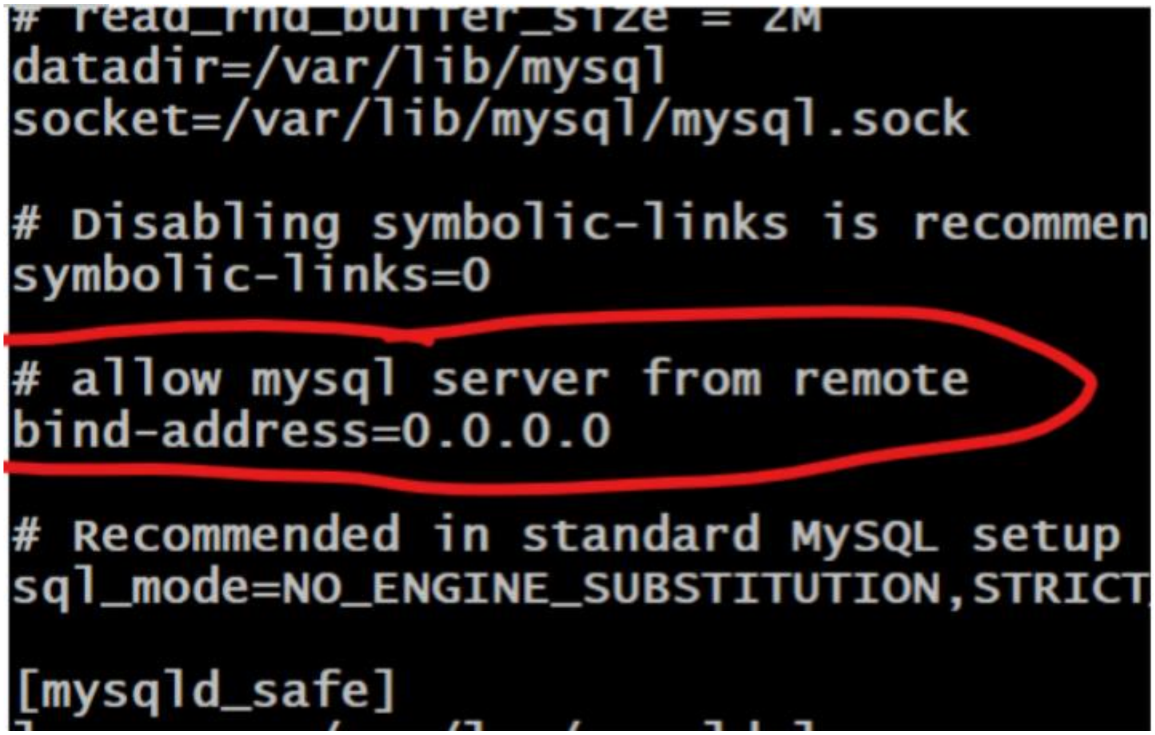


Figure 42

- Finally, the Zabbix server will start graphing the system metrics shipped by the Zabbix agent which is residing on the Windows server host system. There are various metrics that you can monitor including network Interface statistics, CPU usage and utilization, Disk space usage and Memory utilization to mention a few.

25. Monitoring MySQL server using Zabbix

- First you should Install MySQL in ubuntu
- Run the following command to install MySQL
    1. **sudo apt update**
    2. **sudo apt upgrade**
    3. **sudo apt install mysql-server**
    4. **sudo systemctl status mysql**
    5. **sudo mysql_secure_installation**
    6. **sudo mysql -u root -p (enter the root password to login)**
- working on template_db_mysql.conf
    1. **$ sudo apt install mlocate**
    2. **$ locate userparam**
    3. **$ cp /usr/share/doc/zabbix-agent/userparameter_mysql.conf /etc/zabbix/zabbix_agentd.d/template_db_mysql.conf**
- locate my.cnf
- open my.cnf with vim editor locate vi /etc/my.cnf
- add bind-address =0.0.0.0



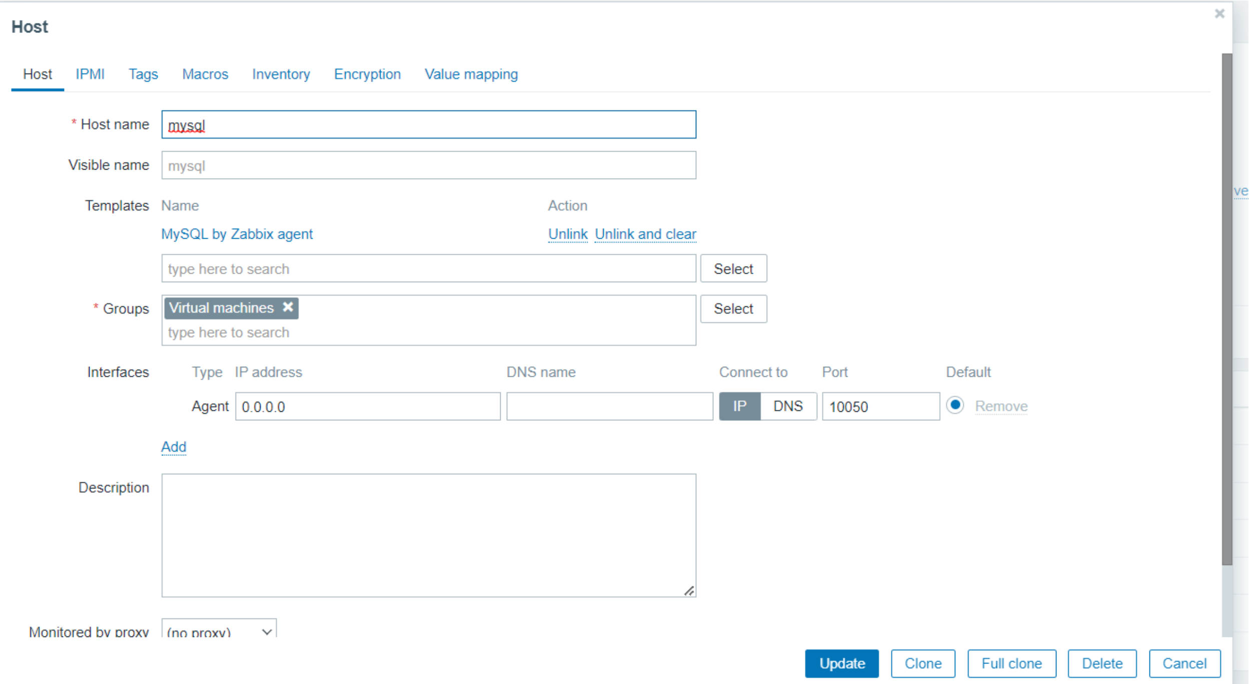
```
# read_rnd_buffer_size = 2M
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

# Disabling symbolic-links is recommen
symbolic-links=0

# allow mysql server from remote
bind-address=0.0.0.0

# Recommended in standard MySQL setup
sql_mode=NO_ENGINE_SUBSTITUTION,STRICT

[mysqld_safe]
```

Figure 43

- now run systemctl stop mysql to stop mysql server
- restart the mysql server systemctl start mysql
- now create a database in mysql command
    1. **mysql -u root -p**
    2. **CREATE USER 'zabbix'@'%' IDENTIFIED BY 'manogya';**
    3. **GRANT ALL PRIVILEGES ON *.* TO 'zabbixr'@'%' IDENTIFIED BY 'manogya' WITH GRANT OPTION;**
    4. **FLUSH PRIVILEGES;**
    5. **quit;**
- now create “.mycnf” in the home directory of Zabbix agent

  $ mkdir /var/lib/Zabbix
- and open the file with vim text editor

  $ vim /var/lib/zabbix/.my.cnf
- now change the user and password, the one you used to create Zabbix database
    1. **username =\`zabbix\`**
    2. **password =\`Manogya\`**
- now restart Zabbix agent by running the following command
    1. **service zabbix-agent start**
    2. **systemctl enable zabbix-agent**
    3. **service zabbix-agent restart**
- Add MySQL host in Zabbix



Host

Host | IPMI | Tags | Macros | Inventory | Encryption | Value mapping

* Host name	mysql
Visible name	mysql

Templates

Name	Action
MySQL by Zabbix agent	Unlink Unlink and clear

type here to search Select

* Groups: Virtual machines ✕ type here to search Select

Interfaces

Type	IP address	DNS name	Connect to	Port	Default	
Agent	0.0.0.0		IP DNS	10050	●	Remove

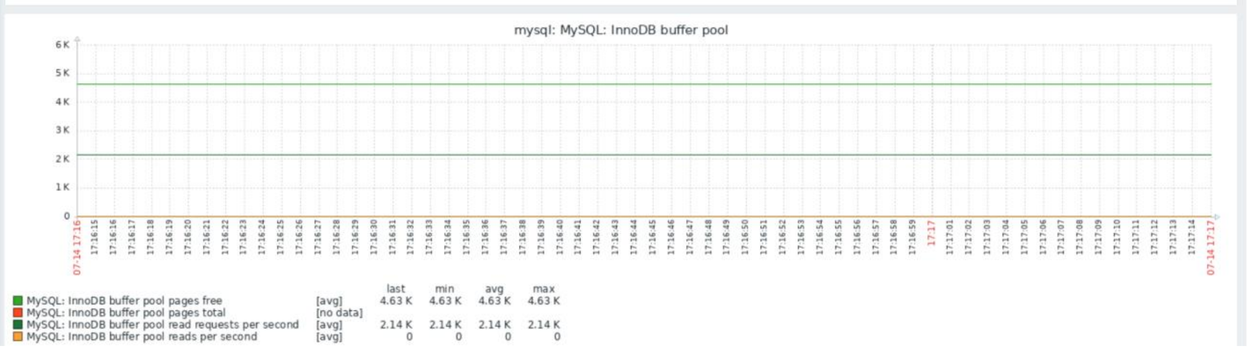
Add

Description

Monitored by proxy: (no proxy)

Figure 44

- Vaidate MySql data in Zabbix

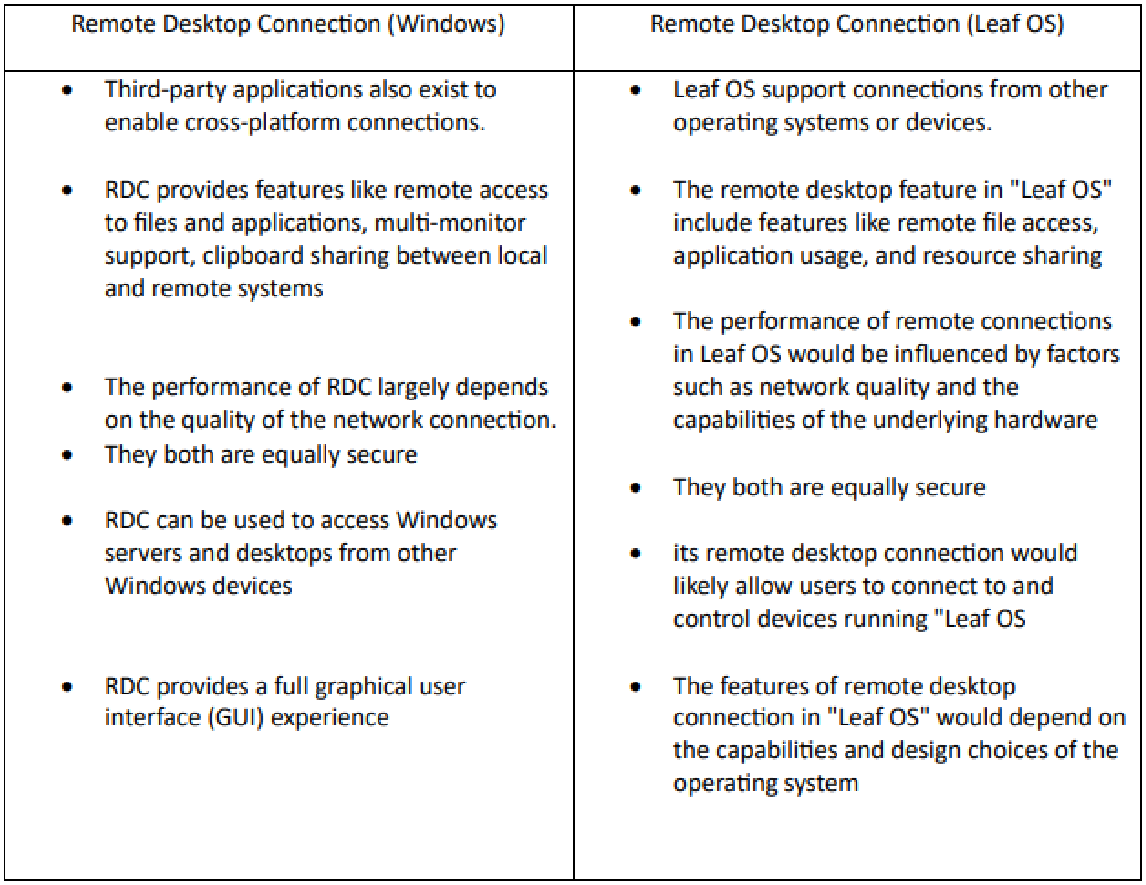


mysql: MySQL: InnoDB buffer pool

		last	min	avg	max
🟩 MySQL: InnoDB buffer pool pages free	[avg]	4.63 K	4.63 K	4.63 K	4.63 K
🟥 MySQL: InnoDB buffer pool pages total	[no data]				
🟩 MySQL: InnoDB buffer pool read requests per second	[avg]	2.14 K	2.14 K	2.14 K	2.14 K
🟧 MySQL: InnoDB buffer pool reads per second	[avg]	0	0	0	0

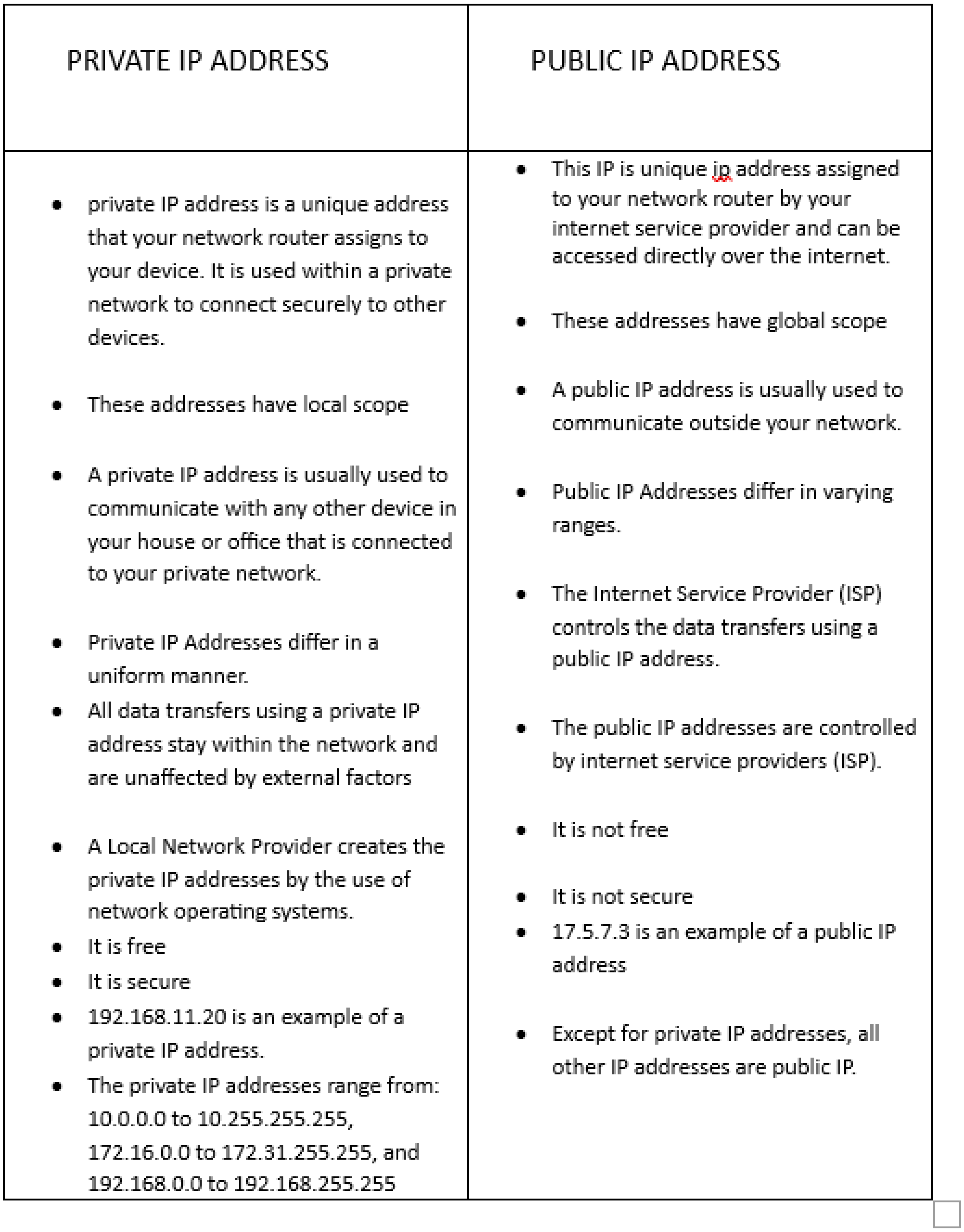
Figure 45

26. Remote Desktop Connection Windows vs Leaf OS



Remote Desktop Connection (Windows)	Remote Desktop Connection (Leaf OS)
• Third-party applications also exist to enable cross-platform connections. • RDC provides features like remote access to files and applications, multi-monitor support, clipboard sharing between local and remote systems • The performance of RDC largely depends on the quality of the network connection. • They both are equally secure • RDC can be used to access Windows servers and desktops from other Windows devices • RDC provides a full graphical user interface (GUI) experience	• Leaf OS support connections from other operating systems or devices. • The remote desktop feature in "Leaf OS" include features like remote file access, application usage, and resource sharing • The performance of remote connections in Leaf OS would be influenced by factors such as network quality and the capabilities of the underlying hardware • They both are equally secure • its remote desktop connection would likely allow users to connect to and control devices running "Leaf OS • The features of remote desktop connection in "Leaf OS" would depend on the capabilities and design choices of the operating system

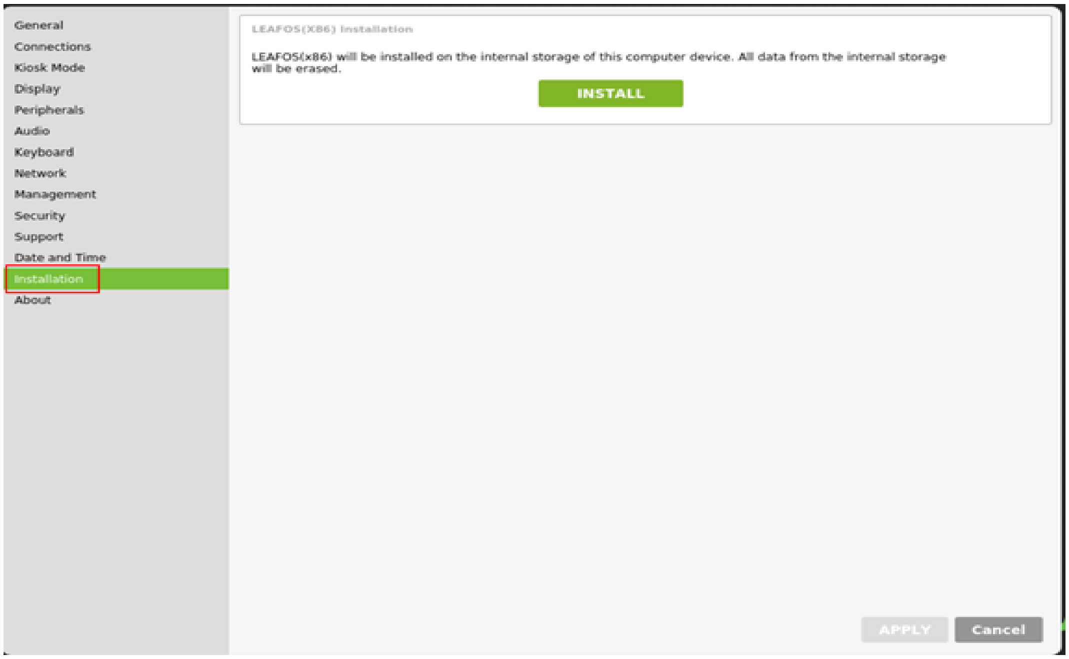
27. Difference between Private and Public IP Address



PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
• private IP address is a unique address that your network router assigns to your device. It is used within a private network to connect securely to other devices. • These addresses have local scope • A private IP address is usually used to communicate with any other device in your house or office that is connected to your private network. • Private IP Addresses differ in a uniform manner. • All data transfers using a private IP address stay within the network and are unaffected by external factors • A Local Network Provider creates the private IP addresses by the use of network operating systems. • It is free • It is secure • 192.168.11.20 is an example of a private IP address. • The private IP addresses range from: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255	• This IP is unique ip address assigned to your network router by your internet service provider and can be accessed directly over the internet. • These addresses have global scope • A public IP address is usually used to communicate outside your network. • Public IP Addresses differ in varying ranges. • The Internet Service Provider (ISP) controls the data transfers using a public IP address. • The public IP addresses are controlled by internet service providers (ISP). • It is not free • It is not secure • 17.5.7.3 is an example of a public IP address • Except for private IP addresses, all other IP addresses are public IP.

28. Download and prepare LEAF OS installation.

- From NComputing Software Download page, select “LEAF OS” and download the compressed image (i.e.ZIP)
- 2.Extract the .IMG file (~2.5GB) in the downloaded .ZIP file
- 3.Create a bootable LEAF OS installer USB memory stick (use at least 4GB or higher capability):
- 1.Use a flashing application using win32 disk
- 4.Pick an x86-64 PC/laptop (BIOS or UEFI).
- 1.Access the PC/laptop's Boot Menu or change the PC/laptop BIOS setting to set external USB storage device at the top of the booting priority list.
- Installation option #2 (flash LEAF OS into HDD/SSD/eMMC/NVMe internal storage to boot from)
- Your device’s internal drive will be wiped and flashed with LEAF OS. When you boot the device, the LEAF OS will be directly booted from the internal HDD/SSD/eMMC/NVMe storage.



LEAFOS(X86) Installation

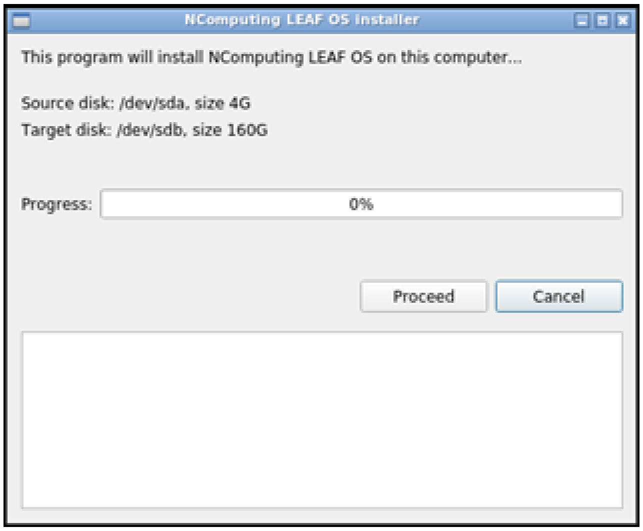
LEAFOS(x86) will be installed on the internal storage of this computer device. All data from the internal storage will be erased.

Figure 46

- Follow the same procedures above to live boot LEAF OS on the device using the connected USB memory stick.

- Once the LEAF OS UI is up, navigate to the 'Installation' tab and click 'Install' (see screenshot below). There are additional warning messages to inform the admin/user that the 'install' process will erase the internal storage of the selected device.

- Once you click on 'Install' and click 'okay' on the warning message, wait a few seconds until the NComputing LEAF OS installer window appears. It will prompt you to confirm to proceed flashing LEAF OS to the internal storage. Click the [Proceed] button to confirm and proceed. Once the internal storage is flashed, you will be prompted to shut the PC/laptop down and reboot. The installation process may take several minutes. Please be patient.



NComputing LEAF OS Installer

This program will install NComputing LEAF OS on this computer...

Source disk: /dev/sda, size 4G
Target disk: /dev/sdb, size 160G

Progress: 0%

- *Figure 47*

- Remove the USB stick with LEAF OS installer and power up the computer again. LEAF OS will boot directly from the internal storage.

- Once the LEAF OS UI is up, you can connect to any desktop virtualization environment.

29. Installing cacti on ubuntu server

Update your Ubuntu 22.04 server

- **sudo apt update && sudo apt upgrade**

- Install Apache for Cacti

  sudo apt install apache2

- Start and enable Apache Web server:

  sudo systemctl enable --now apache2

Install PHP and MariaDB

sudo apt install php php-{mysql,curl,net-socket,gd,intl,pear,imap,memcache,pspell,tidy,xmlrpc,snmp,mbstring,gmp,json,xml,common,ldap}

sudo apt install libapache2-mod-php

- Configure PHP memory and execution time:
- Edit the php.ini file:

```
sudo nano /etc/php/*/apache2/php.ini
```

- change its value from 128 to 512M

```
• memory_limit = 512M
```

- search for max_execution_time and change its value from 30 to 300.

```
• max_execution_time = 300
```

```
date.timezone = Asia/Kathmandu
```

- Save the file by pressing Ctrl+O after that hit the Enter key and use Ctrl+X to exit.
- Now, also edit the PHP CLI php.ini file and set the time zone there as well.

```
sudo nano /etc/php/*/cli/php.ini
```

- Fins and Set time zone again:

```
date.timezone = Asia/Kathmandu
```

- Save the file by pressing Ctrl+O after that hit the Enter key and use Ctrl+X to exit.

- Install MariaDB

```
sudo apt install mariadb-server -y
```

- Start and enable the Database server:

```
sudo systemctl enable --now mariadb
```

- To check its status:

```
sudo systemctl status mariadb
```

- Create MariaDB Database for Cacti

```
sudo mysql -u root -p
```

- **CREATE DATABASE cacti DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci ;**

- **GRANT ALL PRIVILEGES ON cacti.* TO 'cacti_user'@'localhost' IDENTIFIED BY 'strongpassword';**

- **GRANT SELECT ON mysql.time_zone_name TO cacti_user@localhost;**

- **ALTER DATABASE cacti CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;**

- **FLUSH PRIVILEGES;**

- **EXIT;**

Configure MariaDB for Cacti:

- **sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf**

- **Copy and Add the following given line under– [mariadb]**

- **innodb_file_format=Barracuda**

- **innodb_large_prefix=1**

- **collation-server=utf8mb4_unicode_ci**

- **character-set-server=utf8mb4**

- innodb_doublewrite=OFF

- **max_heap_table_size=128M**

- **tmp_table_size=128M**

- **join_buffer_size=128M**

- **innodb_buffer_pool_size=1G**

- **innodb_flush_log_at_timeout=3**

- **innodb_read_io_threads=32**

- **innodb_write_io_threads=16**

- **innodb_io_capacity=5000**

- **innodb_io_capacity_max=10000**

- **innodb_buffer_pool_instances=9**

- Also, add # tag in front of these two lines available in the same file to make them unreadable:

- **#character-set-server = utf8mb4**
- **#collation-server = utf8mb4_general_ci**

- Save the file: Ctrl+O, hit the Enter Key, and then Ctrl+X to exit.

- Now, set the timezone in MySQL

```
sudo su -

mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -u root -p mysql
```

Install SNMP and other tools for Cacti

```
sudo apt install snmp snmpd rrdtool
```

Configure Cacti Software on Ubuntu 22.04 or 20.04

```
sudo apt install git

git clone -b 1.2.x https://github.com/Cacti/cacti.git
```

- Move the cloned Cacti files to your Web directory:

```
sudo mysql -u root cacti < /var/www/html/cacti/cacti.sql
```

- Create PHP configuration file for Cacti:

```
cd /var/www/html/cacti/include

cp config.php.dist config.php
```

- Now, edit the config.php and add the Database details you have created for Cacti.

```
sudo nano config.php
```

- Change the Database values – Database name, username, and password.
- Save the file Ctrl+O, hit the Enter key, and exit: Ctrl+x.

```
sudo chown -R www-data:www-data /var/www/html/cacti
```

Create Cacti Systemd service

```
sudo nano /etc/systemd/system/cactid.service
```

- Add the following lines:

```
[Unit]

Description=Cacti Daemon Main Poller Service
```

```
After=network.target

[Service]

Type=forking

User=www-data

Group=www-data
```

```
EnvironmentFile=/etc/default/cactid

ExecStart=/var/www/html/cacti/cactid.php

Restart=always

RestartSec=5s

[Install]

WantedBy=multi-user.target
```

- Save the file Ctrl+O, press Enter key, and then exit Ctrl+X.
- Create an environment file:

```
sudo touch /etc/default/cactid
```

- Start and enable Cacti Service

```
sudo systemctl daemon-reload

sudo systemctl enable cactid

sudo systemctl restart cactid
```

- To check status:

```
sudo systemctl status cactid
```

- Also restart Mariadb and Apache services:

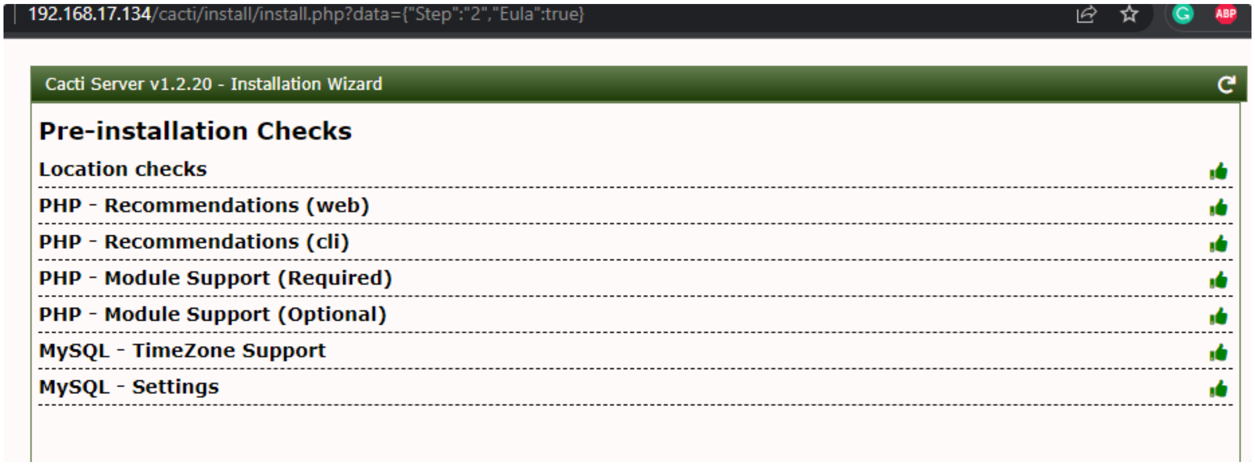
```
sudo systemctl restart apache2 mariadb
```

Login Cacti monitoring on Ubuntu 22.04 or 20.04

```
http://your-server-IP-address/cacti/
```

username – admin and password – admin

1. Start Cacti web installation



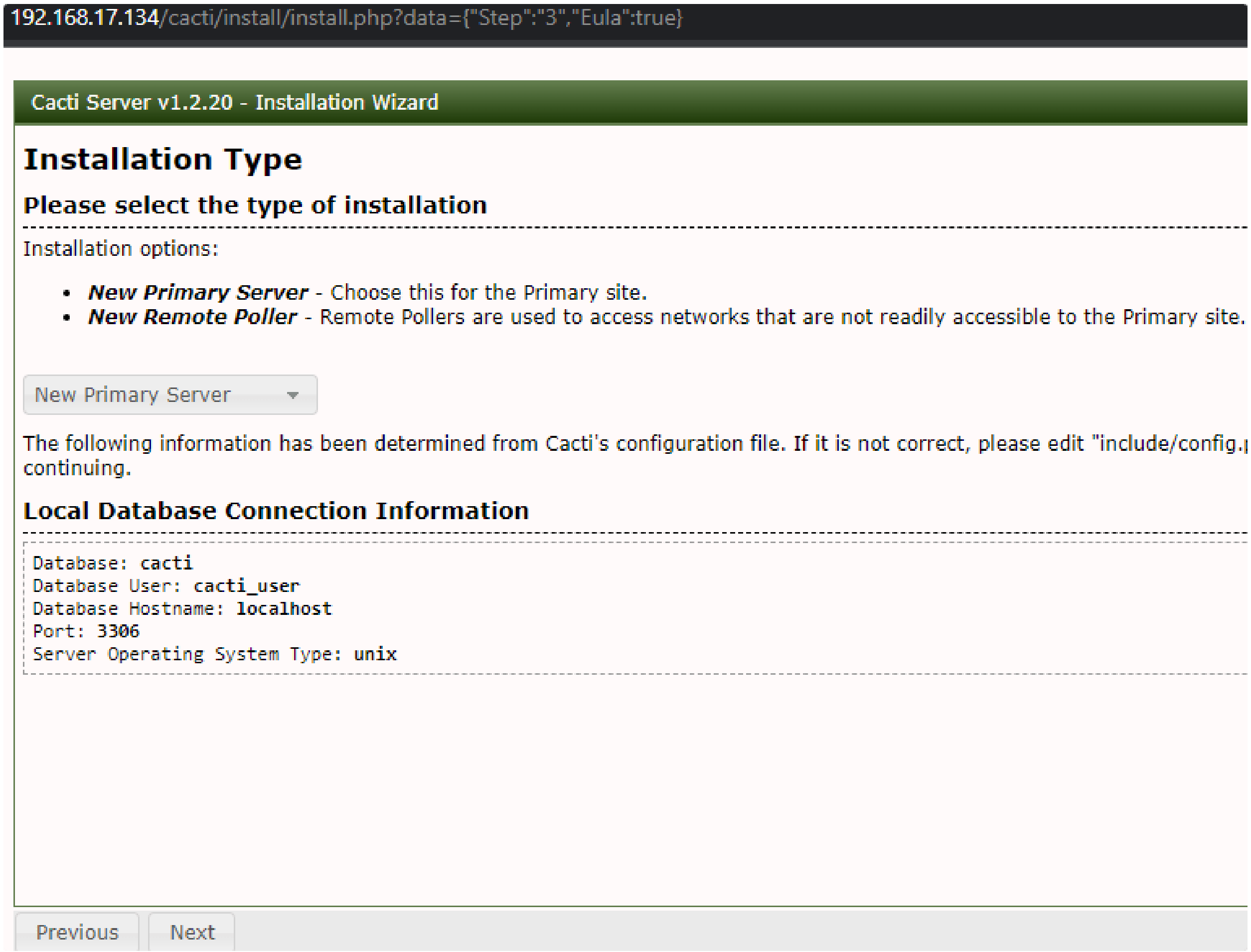
192.168.17.134/cacti/install/install.php?data={"Step":"2","Eula":true}

Cacti Server v1.2.20 - Installation Wizard

Pre-installation Checks

Location checks ✓
PHP - Recommendations (web) ✓
PHP - Recommendations (cli) ✓
PHP - Module Support (Required) ✓
PHP - Module Support (Optional) ✓
MySQL - TimeZone Support ✓
MySQL - Settings ✓

Figure 48



192.168.17.134/cacti/install/install.php?data={"Step":"3","Eula":true}

Cacti Server v1.2.20 - Installation Wizard

Installation Type

Please select the type of installation

Installation options:

- ***New Primary Server*** - Choose this for the Primary site.
- ***New Remote Poller*** - Remote Pollers are used to access networks that are not readily accessible to the Primary site.

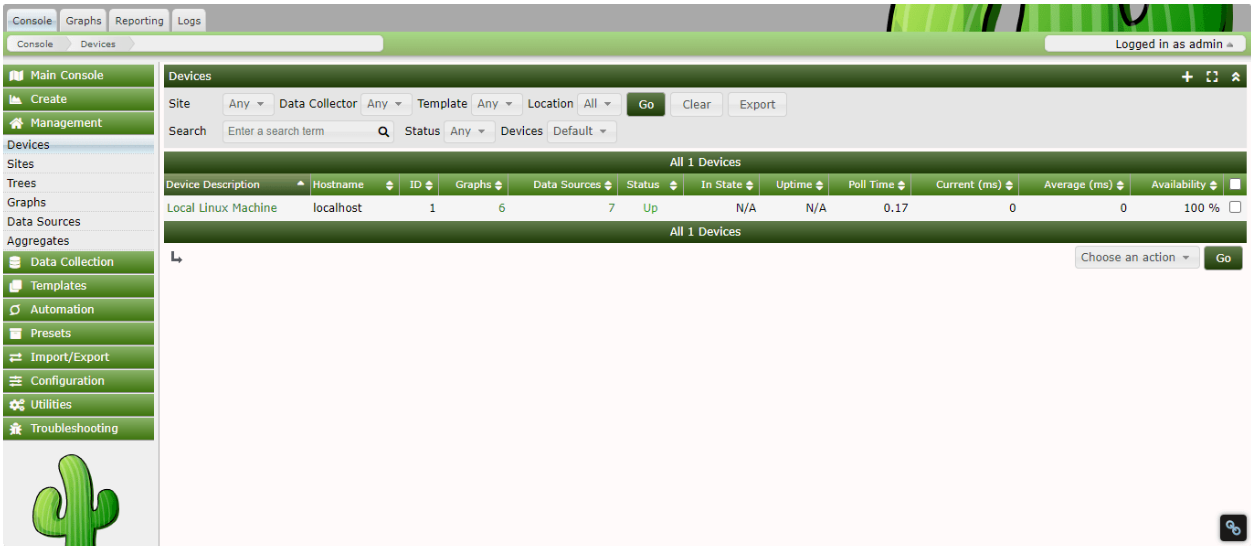
New Primary Server ▾

The following information has been determined from Cacti's configuration file. If it is not correct, please edit "include/config.p continuing.

Local Database Connection Information

```
Database: cacti
Database User: cacti_user
Database Hostname: localhost
Port: 3306
Server Operating System Type: unix
```

Figure 49



Site Any Data Collector Any Template Any Location All

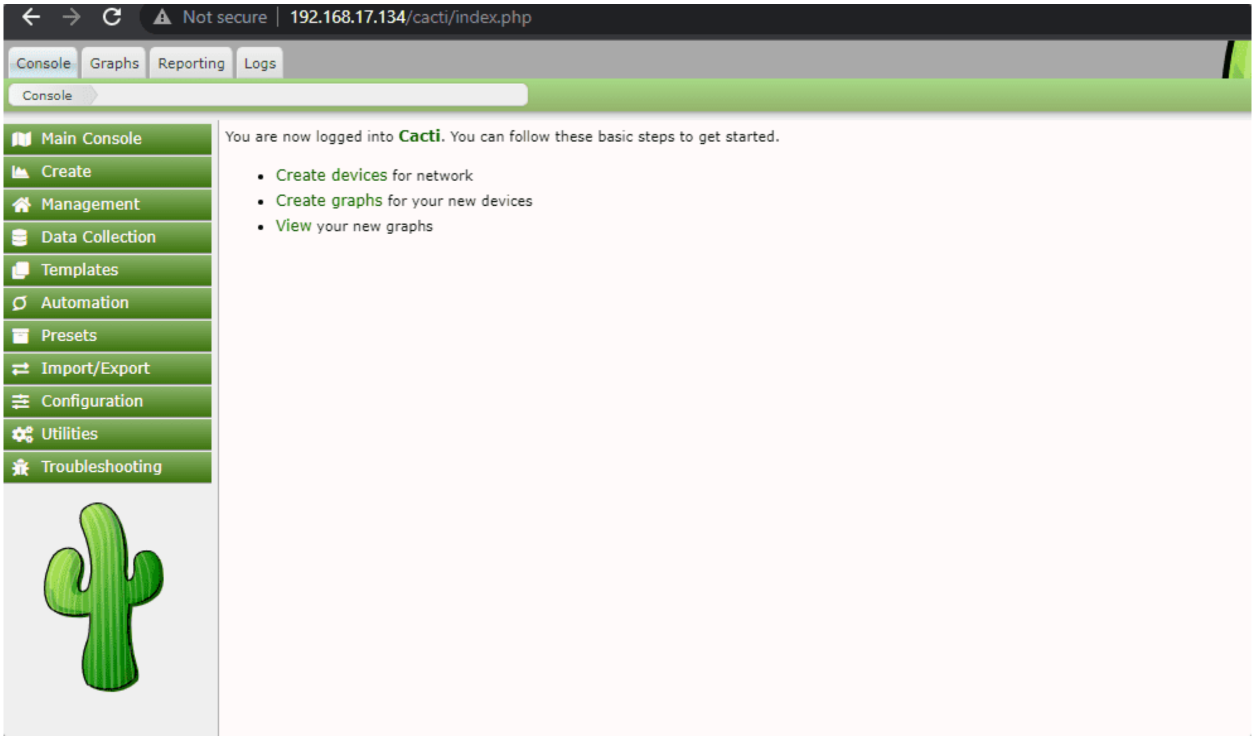
Search Enter a search term Status Any Devices Default

All 1 Devices

Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability	□
Local Linux Machine	localhost	1	6	7	Up	N/A	N/A	0.17	0	0	100 %	□

All 1 Devices

Figure 50



You are now logged into **Cacti**. You can follow these basic steps to get started.

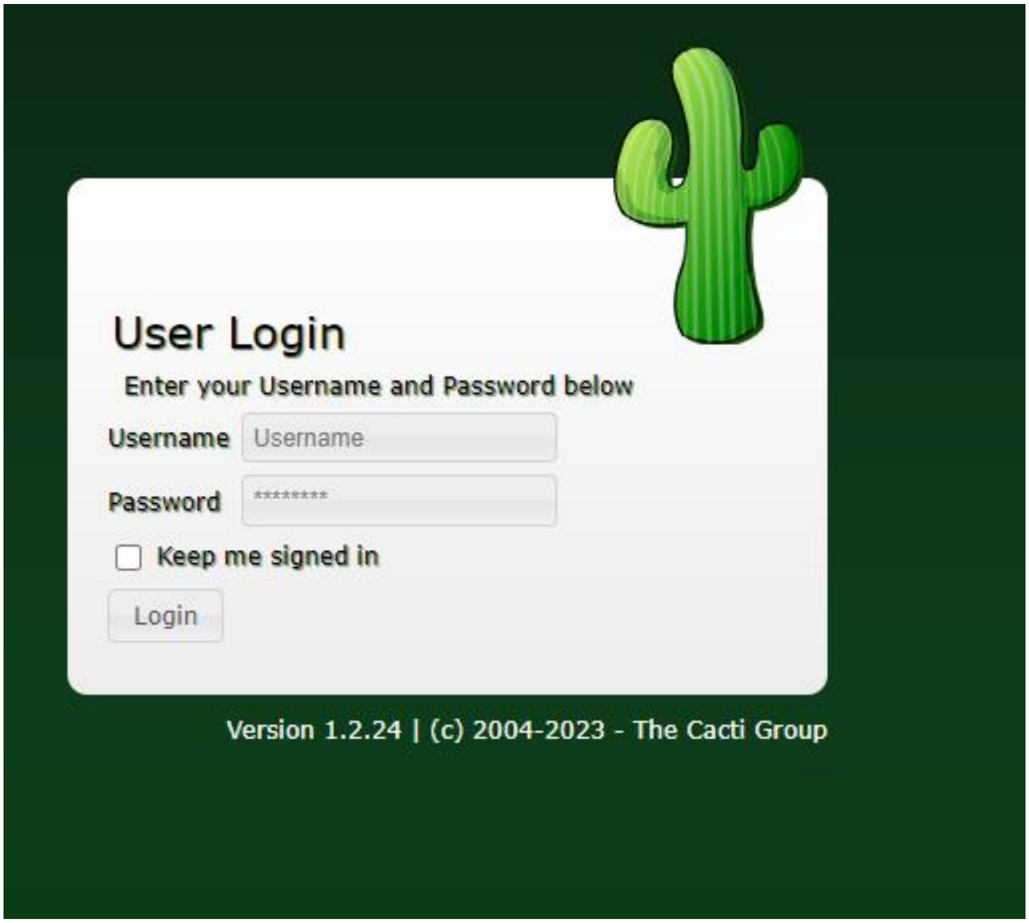
- Create devices for network
- Create graphs for your new devices
- View your new graphs

Figure 51

30. Making a network weathermap in cacti

Step 1 : Configure Cacti

- Access the Cacti web interface and log in as an admin user.



User Login

Enter your Username and Password below

Username: Username

Password: ********

□ Keep me signed in

Login

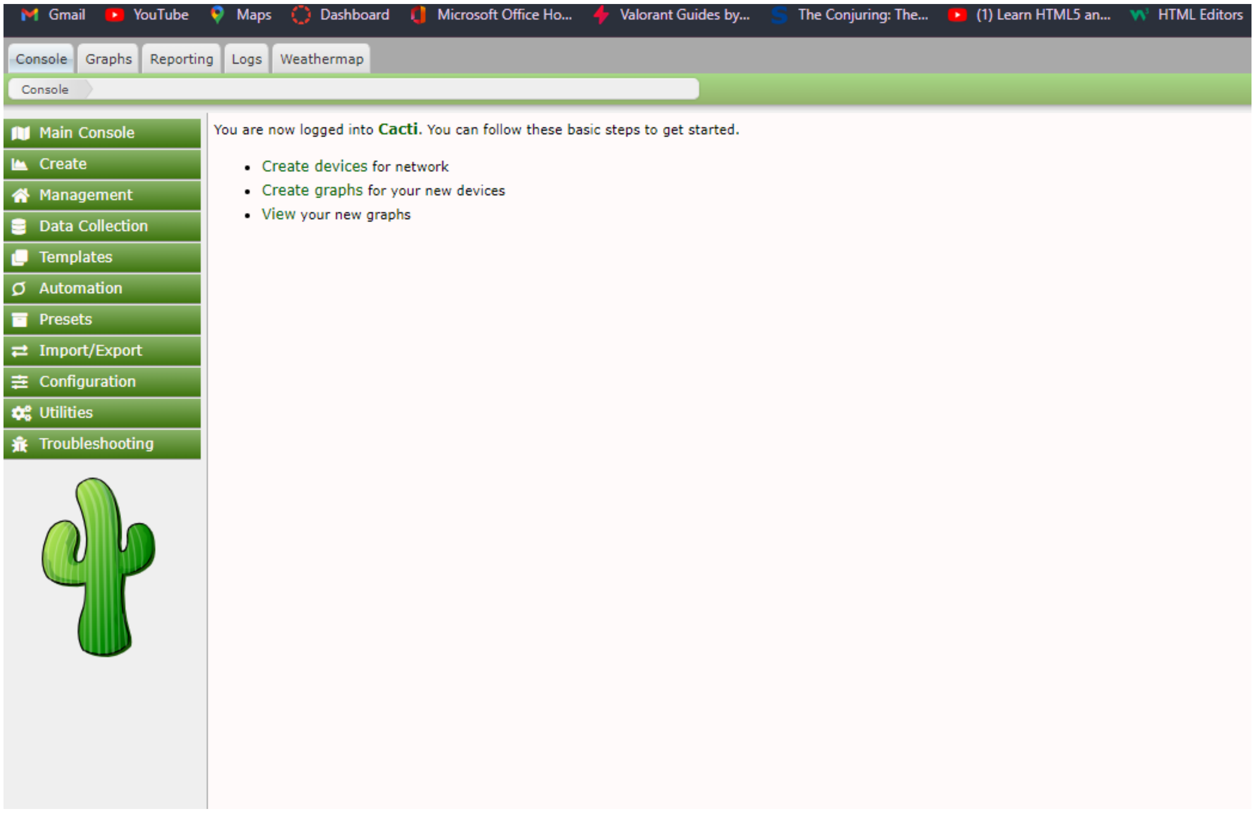
Version 1.2.24 | (c) 2004-2023 - The Cacti Group

Figure 52

Step 2 : Install and Configure the Weathermap Plugin

- The Weathermap plugin is not included by default in Cacti, so you need to install it separately. Here's how to do it:
- Download the Weathermap plugin from the Cacti website or a trusted source.
- Extract the contents of the downloaded archive and copy them to the Cacti plugin directory. On Linux, this directory is typically located at /var/www/html/cacti/plugins.

- In your web browser, log in to the Cacti web interface.
- Go to "Console" > "Configuration" > "Plugin Management."
- Find the Weathermap plugin in the list and click the "Install" button.
- Navigate to "Configuration" and set up your data sources and data templates. You may need to configure data sources for your weather data, such as temperature and humidity.

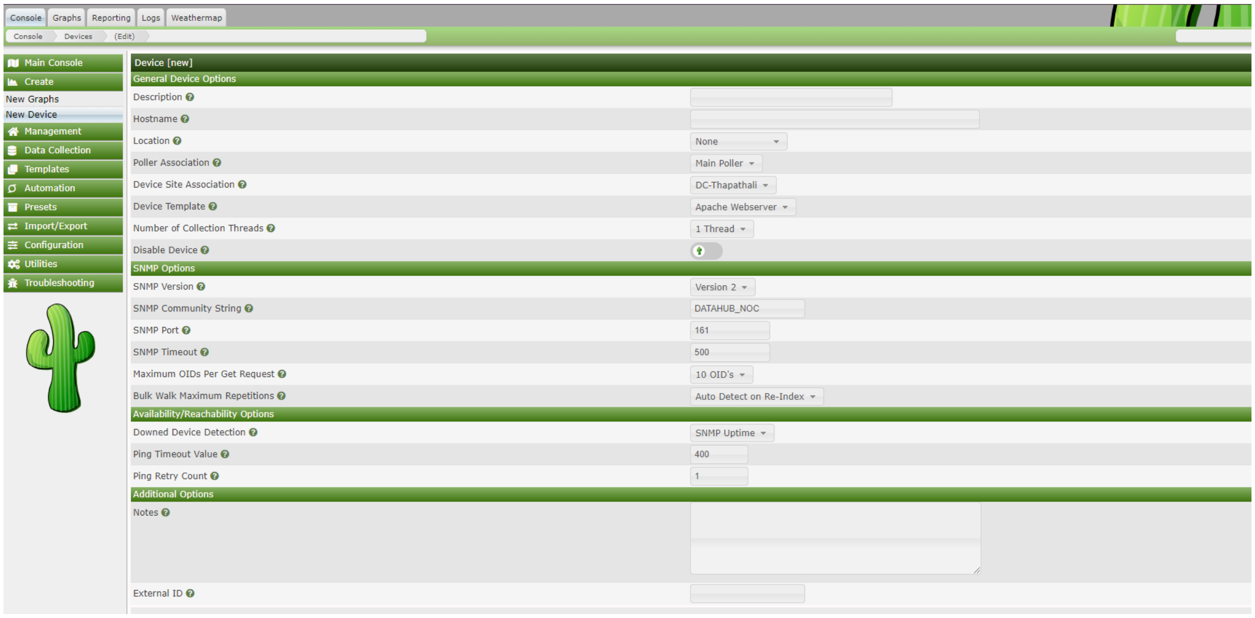


You are now logged into **Cacti**. You can follow these basic steps to get started.

- Create devices for network
- Create graphs for your new devices
- View your new graphs

Figure 53

Step 3 : Add a device to see the graph

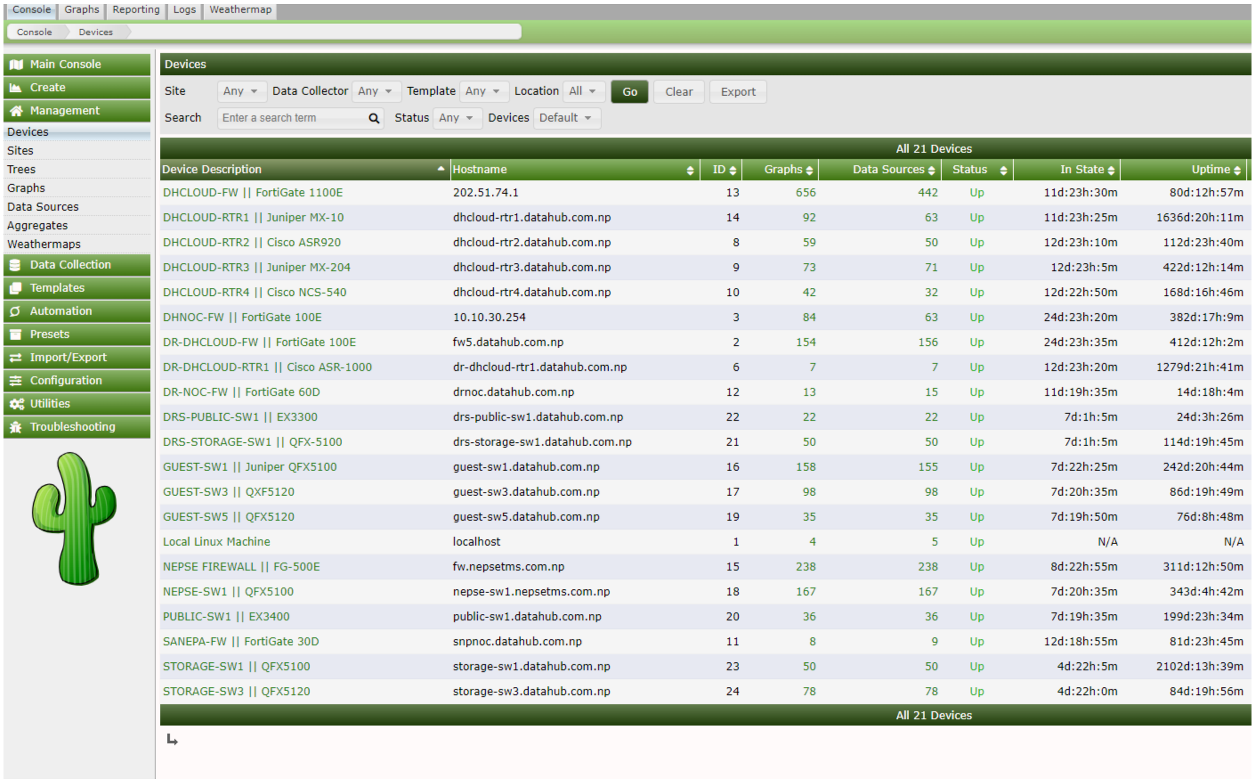


Device [new]

General Device Options	
Description	
Hostname	
Location	None
Poller Association	Main Poller
Device Site Association	DC-Thapathali
Device Template	Apache Webserver
Number of Collection Threads	1 Thread
Disable Device	
SNMP Options	
SNMP Version	Version 2
SNMP Community String	DATAHUB_NOC
SNMP Port	161
SNMP Timeout	500
Maximum OIDs Per Get Request	10 OID's
Bulk Walk Maximum Repetitions	Auto Detect on Re-Index
Availability/Reachability Options	
Downed Device Detection	SNMP Uptime
Ping Timeout Value	400
Ping Retry Count	1
Additional Options	
Notes	
External ID	

Figure 54

- Now the added device will be visible here.



Devices

Site Any Data Collector Any Template Any Location All

Search Enter a search term Status Any Devices Default

All 21 Devices

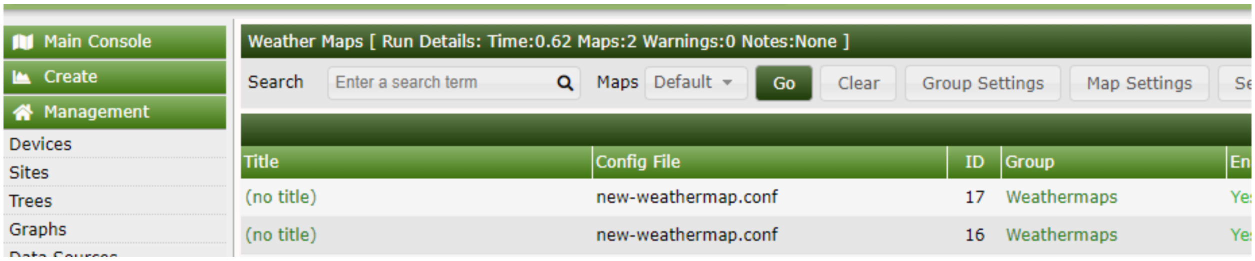
Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime
DHCLOUD-FW || FortiGate 1100E	202.51.74.1	13	656	442	Up	11d:23h:30m	80d:12h:57m
DHCLOUD-RTR1 || Juniper MX-10	dhcloud-rtr1.datahub.com.np	14	92	63	Up	11d:23h:25m	1636d:20h:11m
DHCLOUD-RTR2 || Cisco ASR920	dhcloud-rtr2.datahub.com.np	8	59	50	Up	12d:23h:10m	112d:23h:40m
DHCLOUD-RTR3 || Juniper MX-204	dhcloud-rtr3.datahub.com.np	9	73	71	Up	12d:23h:5m	422d:12h:14m
DHCLOUD-RTR4 || Cisco NCS-540	dhcloud-rtr4.datahub.com.np	10	42	32	Up	12d:22h:50m	168d:16h:46m
DHNOC-FW || FortiGate 100E	10.10.30.254	3	84	63	Up	24d:23h:20m	382d:17h:9m
DR-DHCLOUD-FW || FortiGate 100E	fw5.datahub.com.np	2	154	156	Up	24d:23h:35m	412d:12h:2m
DR-DHCLOUD-RTR1 || Cisco ASR-1000	dr-dhcloud-rtr1.datahub.com.np	6	7	7	Up	12d:23h:20m	1279d:21h:41m
DR-NOC-FW || FortiGate 60D	drnoc.datahub.com.np	12	13	15	Up	11d:19h:35m	14d:18h:4m
DRS-PUBLIC-SW1 || EX3300	drs-public-sw1.datahub.com.np	22	22	22	Up	7d:1h:5m	24d:3h:26m
DRS-STORAGE-SW1 || QFX-5100	drs-storage-sw1.datahub.com.np	21	50	50	Up	7d:1h:5m	114d:19h:45m
GUEST-SW1 || Juniper QFX5100	guest-sw1.datahub.com.np	16	158	155	Up	7d:22h:25m	242d:20h:44m
GUEST-SW3 || QXF5120	guest-sw3.datahub.com.np	17	98	98	Up	7d:20h:35m	86d:19h:49m
GUEST-SW5 || QFX5120	guest-sw5.datahub.com.np	19	35	35	Up	7d:19h:50m	76d:8h:48m
Local Linux Machine	localhost	1	4	5	Up	N/A	N/A
NEPSE FIREWALL || FG-500E	fw.nepsetms.com.np	15	238	238	Up	8d:22h:55m	311d:12h:50m
NEPSE-SW1 || QFX5100	nepse-sw1.nepsetms.com.np	18	167	167	Up	7d:20h:35m	343d:4h:42m
PUBLIC-SW1 || EX3400	public-sw1.datahub.com.np	20	36	36	Up	7d:19h:35m	199d:23h:34m
SANEPA-FW || FortiGate 30D	snpnoc.datahub.com.np	11	8	9	Up	12d:18h:55m	81d:23h:45m
STORAGE-SW1 || QFX5100	storage-sw1.datahub.com.np	23	50	50	Up	4d:22h:5m	2102d:13h:39m
STORAGE-SW3 || QFX5120	storage-sw3.datahub.com.np	24	78	78	Up	4d:22h:0m	84d:19h:56m

All 21 Devices

Figure 55

Step 4 : Configure Weathermap

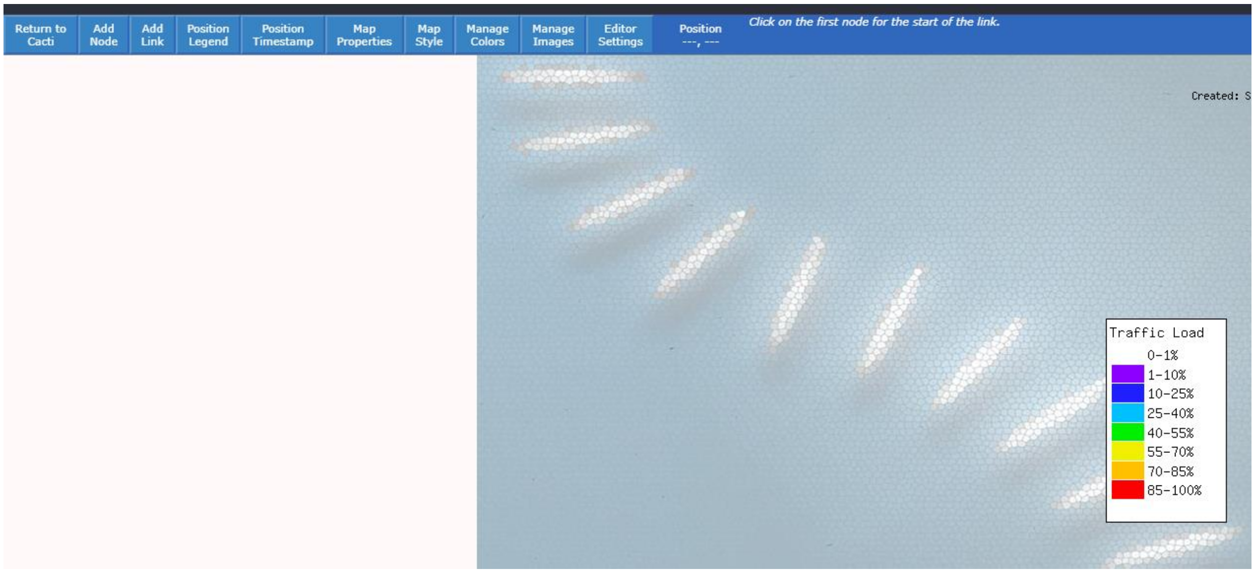
- After installing the Weathermap plugin, you need to configure it to create your network weather map:
- In the Cacti web interface, go to "Console" > "Weathermap."
- Click on "Create a new Map."
- Give your map a name and configure its properties. You will need to specify the map size, units (e.g., pixels, percent), and other display options.
- Add devices and links to your map. You can drag and drop devices from your Cacti inventory and connect them with links to represent network connections. Configure the links to display the relevant data, such as bandwidth usage.
- e. Customize the appearance of your map by setting colors, line styles, and other visual elements.



Weather Maps [Run Details: Time:0.62 Maps:2 Warnings:0 Notes:None]

Title	Config File	ID	Group	En
(no title)	new-weathermap.conf	17	Weathermaps	Yes
(no title)	new-weathermap.conf	16	Weathermaps	Yes

Figure 56



Click on the first node for the start of the link.

Figure 57

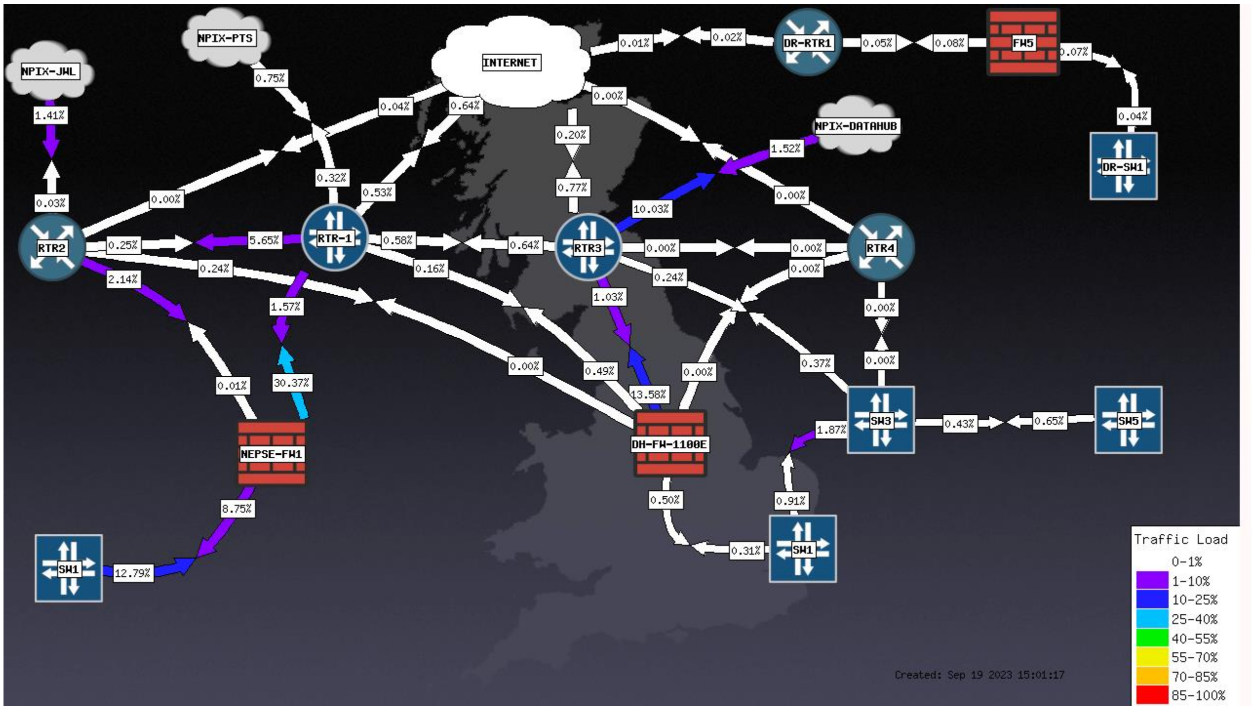


Figure 58

A network weathermap serves multiple crucial functions in the realm of network management and monitoring. It acts as a visual dashboard, offering network administrators a clear and intuitive representation of the network's health and performance. This visualization aids in the swift identification of issues such as congestion, latency, or security vulnerabilities, streamlining the troubleshooting process. Moreover, network weathermaps play a pivotal role in capacity planning, helping organizations anticipate future network demands and make informed infrastructure decisions. Beyond technical insights, these maps also serve as effective communication tools, allowing both technical and non-technical stakeholders to grasp network status and performance effortlessly. They can trigger alerts and notifications when network thresholds are crossed, facilitating proactive issue resolution. In essence, network weathermaps are indispensable instruments for optimizing network operations, enhancing security, and ensuring seamless connectivity in today's interconnected world

The picture above shows a network weather map. In this map, you can see the there are three routers connected to the internet. Routers are important devices in a network. You can also see three brick wall icons, which represent firewalls protecting the routers. This map helps us see how long it takes for data to travel in the network and lets us watch the network traffic. It's a useful tool for checking how well the network is working and if it's secure.