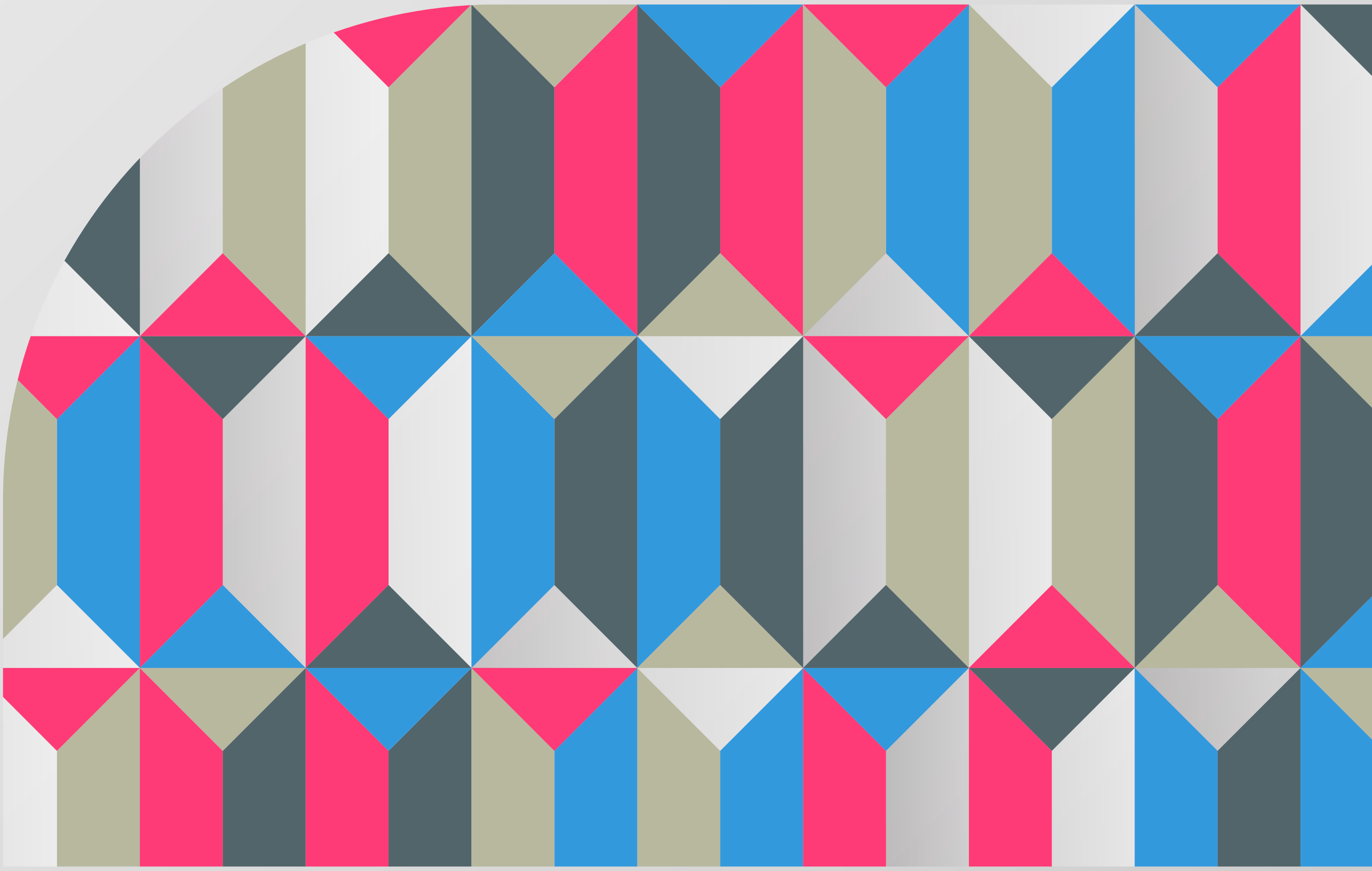
Student Manual

STL academy



Subject

Customer Support Engineer

Vol.01

Empowering Youth!

ISO 21001

GUINNESS WORLD RECORDS RECORD HOLDER

ASIA BOOK OF RECORDS

Skill & Assessment Partner
NASSCOM®

stl.tech | stlacad.tech

Customer Support Engineer

Submitted to :- **Bihar Skill Development Mission, Labour Resources Department, GoB**	Submitted By **:- Sterlite Technologies Ltd**
	Session : 2022-23

Course name:

- Course Id-
- Candidate Eligibility : Diploma/ Graduate
- Course Duration: (In hours) 525

CONTACT DETAILS OF THE BODY SUBMITTING THE QUALIFICATION FILE

Name and address of submitting body:

Sterlite Technologies Ltd

Name and contact details of individual dealing with the submission

Name	: Mrs./Mr. Srikant Pattnaik
Position in the organization	: Manager
Tel number (s) (Mobile no.)	: 9702048264
Website	: www.stlacad.tech
E-mail address	: **srikant.pattnaik@stl.tech**

CUSTOMER SUPPORT (IT) ENGINEER

STUDENT GUIDE

About the Student Guide

The student guide contains modules which will help you to acquire relevant knowledge and skills (generic and domain-specific skills) related to the 'Customer Support (IT) Engineer' job role. Knowledge in each module is easily understood and grasped by you before you move on to the next module. Comprehensible diagrams & images from world of work have been included to bring about visual appeal and to make the text lively and interactive for you. You can also try to create your own illustrations using your imagination or taking the help of your trainer.

Let us now see what the sections in the modules have for you.

Section 1: Learning Outcome

This section introduces you to the learning objectives and knowledge criteria covered in the module. It also tells you what you will learn through the various topics covered in the module.

Section 2: Relevant Knowledge

This section provides you with the knowledge to achieve relevant skill and proficiency to perform tasks of the Customer Support (IT) Engineer. The knowledge developed through the module will enable you to perform certain activities related to the job market. You should read through the textual information to develop an understanding on the various aspects of the module before you complete the exercise(s).

Section 3: Exercises

Each module has exercises, which you should practice on completion of the learning sessions of the module. You will perform the activities in the classroom, at home or at the workplace. The activities included in this section will help you to develop necessary knowledge, skills and attitude that you need for becoming competent in performing the tasks at workplace. The activities should be done under the supervision of your trainer who will guide you in completing the tasks and also provide feedback to you for improving your performance.

Section 4: Assessment Questionnaire

The review questions included in this section will help you to check your progress. You must be able to answer all the questions before you proceed to the next module.

CONTENTS

MODULE 1

Introduction to IT Help Desk

Section 1: Learning Outcomes

After completing this module, you will be able to:

- Introduce the significance of 'IT Help Desk'
- Troubleshoot PC issues
- Explore Screen Sharing with Team Viewer and Join me
- Explain about various Common Password Managers
- Manage passwords in Google Chrome and Wifi network
- Describe basic concepts of Networking and Internet
- Execute the Ping, TraceRt and Path Ping Command

Section 2: Relevant Knowledge

1.1 Introduction to IT Help Desk

- A Help desk are the external service, individual, group and organization function that an IT user calls to get help when he/she encounters a problem.
- It is also called a call center where customers call to track shipments, place orders, get help with products and so on.
- It can be as simple as a desk where a person in charge takes call from customers and help them with the relevant solution or a global organization where request is received from online or individuals around the world.
- An IT service desk is an integral part of an organization's IT operations. It's relevant for entities of all sizes and plays a key role in making sure that IT services meet key business objectives.
- In an organization, a service desk acts as a catalyst for digital transformation, which is a major trend affecting almost every industry.
- In a report from Forturum, 41.4% of their respondents (companies) had a dedicated digital transformation team.
- An IT service desk is a communications center that provides a single point of contact (SPOC) between a company, its customers, employees and business partners.
- In a nutshell, a service desk plays an important role in enhancing service delivery and user experience, and it will continue to do so in the coming years.
- According to Service Desk Benchmark Report V.9: 44% of their respondents have said that they expect an increase in the staff managing their service desk.

Examples of names that are related to help desk:

- ➢ Information Center
- ➢ Technical Supporter
- ➢ Resource Center
- ➢ IT Response Center
- ➢ Computer Support Center

What is an IT Service Desk?

- An IT service desk is a single point of contact for internal customers (employees) to get services from their IT department.
- In a service desk, requests are registered as tickets, which is why it's also called a ticket management system.

Information Technology Information Library (ITIL)

- Information technology infrastructure library (ITIL) is a series of best practices in IT Service Management (ITSM) for aligning operations and services.
- It standardizes the selection, planning, delivery, and support of IT services to maximize efficiency and maintain predictable levels of service.
- It helps organizations in all kinds of industries offer their services in a quality-driven and economical way.
- The most recent version of the ITIL framework, ITIL® 4, was released in February 2019.
- It's a significant update from ITIL V3 which was in widespread use for over a decade.
- ITIL has several key principles that are realized through five core components. Some key ITIL concepts and principles are:
  - Delivering maximum value to customers
  - Optimizing resources and capabilities
  - Offering services that are useful and reliable
  - Planning processes with specific goals in mind
  - Defining roles clearly for each task
- ITIL includes the Four Dimensions of Service Management, these include:
  - Organizations and People
  - Information and Technology
  - Partners and Suppliers
  - Value Streams and Processes

Types of Services Desks

- ITIL (Information Technology Information Library) has clearly stated that there are four types of service desk. They are as follows:

Local Service Desk

- Such a service desk is generally situated inside the premise of an organization and caters to the demands of users in close proximity.
- The capacity of such a service desk is limited and suitable for small and medium-size enterprises.

Centralize Service Desk

- A central service desk eliminates the requirement of maintaining multiple service desks across several locations.
- It allows greater efficiency and results in significant cost reduction.

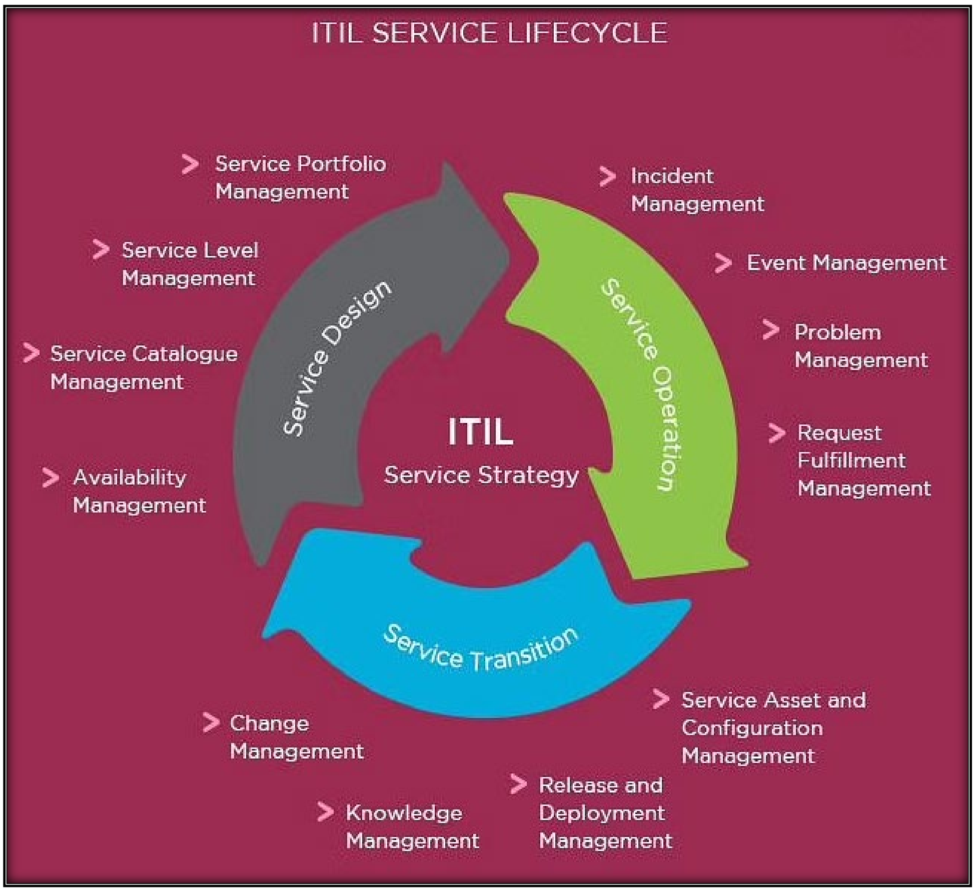
Virtual Service Desk

- When a service desk delivers services through online and gives the sense of a central service desk even though it might be distributed across multiple locations, then it is a virtual service desk.
- Most modern service desks are virtual service desk.

Follow the Sun

- This kind of service desk runs 24 hours.
- This is achieved by combining two or more service desks situated across multiple geographical locations.

ITIL Services Lifecycle



Features and Benefits of IT Service Desk

Service desks play a crucial role in business management. Here are some of the standard features and key benefits of a service desk:

Ticketing System

- Ticket management creates a ticket each time a user submits a support request.
- Service desk software also conducts ticket routing and automation.
- This helps in the organization and handling of queries.

Customer Service Knowledge Base

- Service desks create a database of information that promotes self-service.
- This knowledge management ensures that customers can come here to get an answer to common queries.

IT Asset Management

- This refers to the organization of a company's assets for easier access to relevant information. It includes a configuration management database (CMDB) and asset valuation.

Automation

- Day-to-day tasks are automated and escalated such that the team members can focus on valuable work.

Service-Level Agreement (SLA) Management

- Management of tickets based on SLAs provides an efficient workflow.

Service Catalog

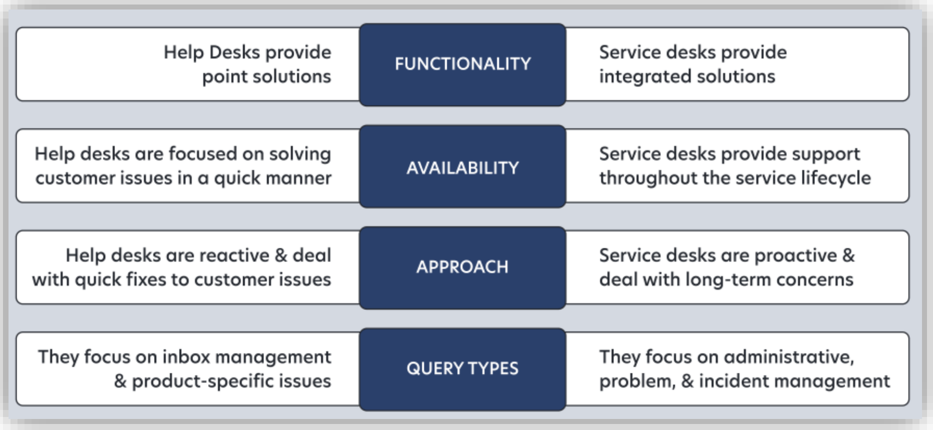
- This is an online catalog where the users have all the necessary information about the different services provided by the company.

Incident Management

- This manages unplanned incidents such that the customer issues are resolved quickly, and the typical workflow can continue.

Difference Between a Help Desk and Service Desk

- The service desk is one of three main options for customer and/or user support. The other two SPOC entities are call centers and help desks. Service desks offer a broad range of services to satisfy business needs. Their focus is on solving more problems in fewer steps. They enable the integration of business processes into the management infrastructure.
- The help desk serves as a point of contact for end users to resolve real-time queries and satisfy user needs. Help desk software streamlines this process. A call center, meanwhile, is simply a centralized department that manages inbound and outbound calls from current and potential customers.



Help Desks provide point solutions	FUNCTIONALITY	Service desks provide integrated solutions
Help desks are focused on solving customer issues in a quick manner	AVAILABILITY	Service desks provide support throughout the service lifecycle
Help desks are reactive & deal with quick fixes to customer issues	APPROACH	Service desks are proactive & deal with long-term concerns
They focus on inbox management & product-specific issues	QUERY TYPES	They focus on administrative, problem, & incident management

How does an IT Help Desk Work?

IT staff can use this software to create tickets for a wide range of events, including:

- Bugs in company software
- New feature requests
- General employee questions
- Problems with the network or VPN
- Issues with login credentials
- Device compatibility issues
- Scheduled maintenance updates
- The software creates a ticket for each issue in a central location, whether an employee picks up the phone or sends a text or email.

- On the IT team’s side, a simple user interface makes it easy for them to share information with one another and work on multiple tickets at once.
- A single issue may require input from multiple departments, so this is a useful feature to have.
- The best IT helpdesk software also helps development teams track bugs by grouping tickets with common problems.
- Chances are multiple employees will encounter issues related to the same bug, so you can save time by grouping tickets together.
- When you’ve patched the bug, you can resolve all related tickets at once.
- Having a searchable help centre makes IT service desk software even more valuable.
- You can provide quick answers to common issues, and you can also create a place for senior employees to share their knowledge with new recruits.
- An internal help centre like this can cut down on the total number of tickets and reduce new hire onboarding times.

Benefits of having an IT service desk

- It captures major incidents in an organization.
- Most modern service desks leverage a cloud architecture to give services anytime anywhere.
- With service desk, people can report their issues/service from a portal, via email or a mobile app anytime.
- A service desk ensures, services are delivered in a standardized way and that there are no gaps in the expectations of the end-users.
- A service desk brings in the power of workflow automation that automates repetitive processes and service level agreements so services are delivered on time.
- A service desk generates a lot of data and makes reporting a lot easier. Apart from that, it also gauges the sentiment of the end-users.

How a service desk fits into IT Service Management?

- IT service management deals with service planning, designing, delivering, supporting and managing.
- A service desk is a subset of IT Service Management that includes:
  - Incident management
  - Problem Management
  - Change Management
  - Knowledge Management
  - Self-service
  - Service Requests
  - Integration with a CMDB

1.2 How to Troubleshoot PC Issues

- Some problems may be easy while others may need the attention of a specialist.
- The thing to keep in mind is that many things can cause problems so troubleshooting is a process of trial and error.

Elimination Process

- In this process you make a list of the things that could be causing the problem then test one by one until you find the one causing the problem.
- When you identify the source of the problem it will be easier to find the solution.

Common Problems and Simple Solution

- It is really important to start with simple solution to problems rather than embarking on extreme solutions.
- Example of simple solutions are like closing and reopening a program.
- If the problem is not solved, you can try other troubleshooting techniques.

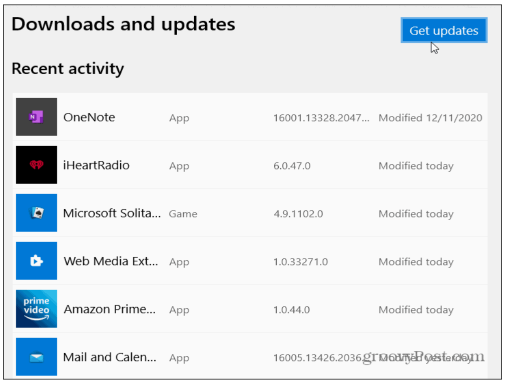
The Common Computer Problems

- Application running slowly
- Power button is not starting computer
- Application is frozen
- The computer is frozen
- Computer is running slowly

How to Troubleshoot PC Issues

Application Running Slowly

- If your application is running slowly, it might be in a loop, or waiting for a resource that is not available, or there might be a performance problem.
- Perhaps your system is operating near the limits of its capacity.



Downloads and updates

Recent activity

OneNote	App	16001.13328.2047...	Modified 12/11/2020
iHeartRadio	App	6.0.47.0	Modified today
Microsoft Solita...	Game	4.9.1102.0	Modified today
Web Media Ext...	App	1.0.33271.0	Modified today
Amazon Prime...	App	1.0.44.0	Modified today
Mail and Calen...	App	16005.13426.2036...	Modified yesterday

groovyPost.com

Solution 1: Close and reopen the application.

Solution 2: Update the application. To do this, click the **Help** menu and look for an option to check for **Updates**. If you don't find this option, another idea is to run an online search for application updates.

Power Button is not Starting Computer

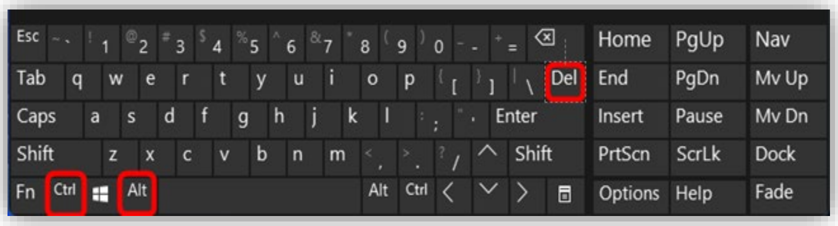
Solution 1: Try replacing the cables to your power button headers with those from the reset button. They operate in the same way, and if the problem is the power button in your case, wiring the reset button to the power switch headers might circumvent this issue.

Solution 2: Begin by checking the power cord to confirm that it is plugged securely into the back of the computer case and the power outlet.

Solution 3: If it is plugged into an outlet, make sure it is a working outlet. To check your outlet, you can plug in another electrical device, such as a lamp.

Application is Frozen

Solution 1: If a program has become completely unresponsive, you can press (and hold) Ctrl+Alt+Delete (the Control, Alt, and Delete keys) on your keyboard to open the Task Manager. You can then select the unresponsive application and click End task to close it.


Esc 1 2 3 4 5 6 7 8 9 0 - = Home PgUp Nav
Tab q w e r t y u i o p [ ] \ Del End PgDn Mv Up
Caps a s d f g h j k l ; ' Enter Insert Pause Mv Dn
Shift z x c v b n m , . / Shift PrtScn ScrLk Dock
Fn Ctrl Alt Alt Ctrl Options Help Fade

Solution 2: Restart the computer.

Computer is Frozen

Solution 1: Press Ctrl + Alt + Del to open the Windows Task Manager. If the Task Manager is opened, highlight the program that is not responding and choose End Task, which should unfreeze the computer. It could still take ten to twenty seconds for the unresponsive program to be terminated after choosing End Task.

Computer is Running Slowly

Causes

- Need of Restarting the Computer
- Too Many Active Programs or Browser Tabs
- Rogue Programs Hogging Processing Power
- Hard Drive/Memory Maxed Out
- Unnecessary Software Updates
- Too Many Apps Open Automatically When PC Starts
- Viruses Or In-Effective Anti-Virus
- Running In Low Power Mode
- Too Many Browsers Add-ons
- PC Being Used for Crypto Mining
- OS Visuals Too High
- Internal PC Dust
- Outdated Drivers
- Your PC May Be Too Old or out of Date
- PC Hardware Failure
- Keyboard or mouse has stopped working

Need of Restarting the Computer

- When is the last time you restarted your computer? If your computer is running slow, this could be a sign that it needs to be restarted, especially if it's been a long time since your last one.
- This is mainly because, as you use your computer, many processes run in the background.
- When too many of these background processes are not ended, they end up using huge amounts of your computer's resources, causing your computer to slow down over time.

Solution:

- Close all your programs and files, then restart your computer.
- Also, ensure that any time a software installation or upgrade asks you to either restart now or restart later, always choose to restart your PC at that moment.

Too Many Active Programs or Browser Tabs

- How many programs are you running at the same time? How many tabs are active on your browser?
- Every open tab and every open program take up a certain amount of space on your Random Access Memory (RAM).
- Having too many of them running at the same time means you are reducing the memory and processing power available for your computer to allow seamless transition from program to program or tab to tab.
- Yes, a computer is supposed to allow you to run several processes simultaneously, but that does not mean you should overload the system.

Solution:

- Only open the tabs you need to use at that moment on your browser. If you would like to save pages for future reference, simply bookmark them and close the tab.
- For further organization and easy access to saved pages, you can group your bookmarks into folders such as for work, recipes, to read, etc.
- For programs, have only those you are using at the moment running, and once you are done shut each program down.

Rogue Programs Hogging Processing Power

- Sometimes, there could be programs running in the background and taking so much of your RAM's memory and processing power, without your knowledge.
- These could be programs that encountered an error and did not completely shut down or programs stuck in a loop running in the background.

Solution:

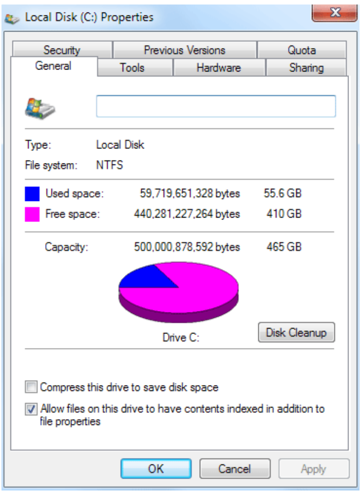
- For windows: press (Ctrl+Alt+Del) to open the Task Manager.
- For Mac: press (Cmd+Space, type 'into spotlight bar') to access the Active Monitor.
- Next press the CPU tab. This will allow you to see which programs are running and how much processing power they are consuming.
- To release the hogged processing power on your RAM end tasks that are running but not being actively used.

Hard Drive/Memory Maxed Out

- A hard drive that is at least 85% full can reduce the computer's processing speed by up to 50%.
- This is because, at this point, the virtual memory required for saving temporary files that facilitate the seamless running of programs is barely available.
- The drive space is mainly taken up by programs, updates to applications, downloads, files of deleted programs, and temporary files.
- When it comes to RAM, the biggest culprits are programs that require a lot of memory to run.
- Such include graphic design software like Photoshop or other industry-specific applications.

Solution:

- Start by first knowing the amount of free space on your hard drive.
- **For windows:** click on My Computer then right-click local disk C and go to properties.
- **For Mac:** click on the Apple then select About this Mac.



Type: Local Disk

File system: NTFS

Used space:	59,719,651,328 bytes	55.6 GB
Free space:	440,281,227,264 bytes	410 GB
Capacity:	500,000,878,592 bytes	465 GB

Drive C:

☐ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties

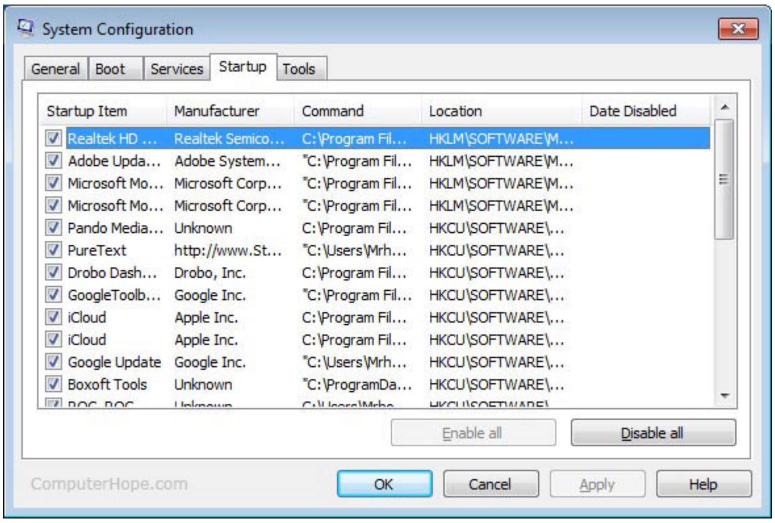
Unnecessary Software Updates

- Software updates are vital to keeping your installed applications running smoothly and secure.
- However, some of these programs come with pre-installed automatic updates that keep running in your background unnecessarily, taking up valuable space on your hard drive and resulting in your computer running slow.
- Find a proactive maintenance solution suitable for your computer.
- Essentially, this solution should be responsible for making the necessary updates and patches for all your software when the machine is not in use.
- Almost every program you download on your computer will come with a prompt requesting for permission to run when your PC starts, known as startup programs.
- This is how a lot of apps and programs on your computer end up automatically loading and running in the background as soon as you turn your PC on.
- This overload is what makes your computer slow right from the booting process.

Too Many Apps Open Automatically When PC Starts

Solution:

- Always be keen when downloading new programs and ensure to uncheck the box giving it permission to run when your PC starts if it is not necessary.
- You can also revoke the permission granted to existing app or programs through the following ways:
- **For windows:** Press CTRL+ALT+Delete and then select Task Manager. Go to your Start Up tab, right-click on the program you want to remove then select disable.
- **For Mac:** go to either Login Items or Applications then uncheck the unnecessary programs.



Startup Item	Manufacturer	Command	Location	Date Disabled
☑ Realtek HD ...	Realtek Semico...	C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Adobe Upda...	Adobe System...	"C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Microsoft Mo...	Microsoft Corp...	"C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Microsoft Mo...	Microsoft Corp...	"C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Pando Media...	Unknown	C:\Program Fil...	HKCU\SOFTWARE\...	
☑ PureText	http://www.St...	"C:\Users\Mrh...	HKCU\SOFTWARE\...	
☑ Drobo Dash...	Drobo, Inc.	C:\Program Fil...	HKCU\SOFTWARE\...	
☑ GoogleToolb...	Google Inc.	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ iCloud	Apple Inc.	C:\Program Fil...	HKCU\SOFTWARE\...	
☑ iCloud	Apple Inc.	C:\Program Fil...	HKCU\SOFTWARE\...	
☑ Google Update	Google Inc.	"C:\Users\Mrh...	HKCU\SOFTWARE\...	
☑ Boxoft Tools	Unknown	"C:\ProgramDa...	HKCU\SOFTWARE\...	

Viruses or In-Effective Anti-Virus

- If everything else in your computer is in order, then you should consider the presence of a virus or an in-effective antivirus that fails to detect and Prevent viruses from attacking your computer as the reason behind your computer running slow.
- Viruses can present themselves in various forms, from random pop-ups to the unauthorized encryption of files.
- There are also viruses that run in the background stealthily that could be eating up into your resources.

Solution:

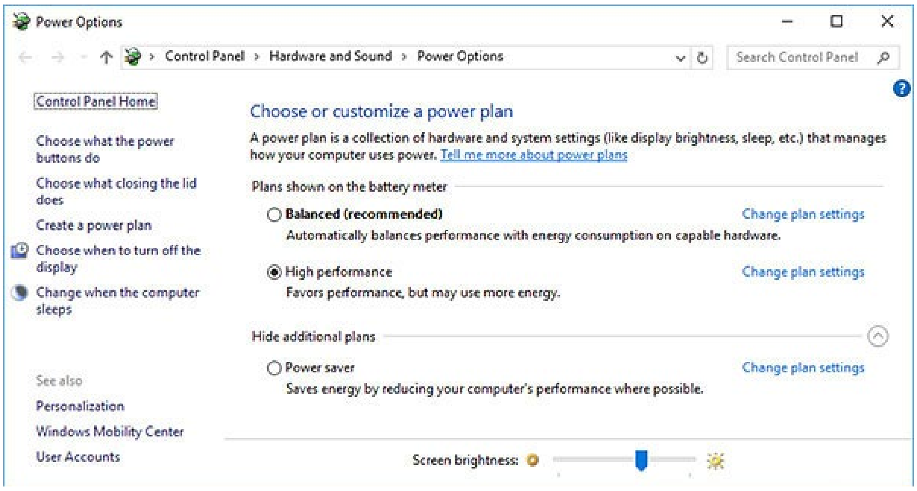
- Download a verified and recognized antivirus program as your cyber security tool.
- Use it to run a malware scan on your computer for viruses or malware frequently.

Running In Low Power Mode

- If you’re running your windows laptop in low power mode (power saver mode), then this may slow it down.
- Running in low power mode limits the performance of your laptop hence slowing it down.

Solution

- Click on Control Panel, choose Hardware and Sound, select Power Options, and then click on Create a Power Plan.
- There should be 3 options available; High Performance, Power Saver, and Balanced.
- Select High Performance or Balanced and enable it as your new power plan.



Power Options

Control Panel > Hardware and Sound > Power Options

Search Control Panel

Control Panel Home

Choose what the power buttons do

Choose what closing the lid does

Create a power plan

Choose when to turn off the display

Change when the computer sleeps

See also

Personalization

Windows Mobility Center

User Accounts

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

Plans shown on the battery meter

○ **Balanced (recommended)** Change plan settings

Automatically balances performance with energy consumption on capable hardware.

● High performance Change plan settings

Favors performance, but may use more energy.

Hide additional plans

○ Power saver Change plan settings

Saves energy by reducing your computer's performance where possible.

Screen brightness:

Too Many Browsers Add-ons

- Do you really need all the add-ons extended on your browser?
- And do your browser extensions effectively perform their required tasks?
- Too many inefficient browser extensions could be slowing down your computer instead of enhancing your browsing experience.

Solution

- Identify all the add-ons on your browser.
- Keep those that are necessary and efficient and disable those that are not.

PC Being Used for Crypto Mining

- It is very possible for your PC to be used to mine crypto currency without your knowledge or approval.
- This mainly occurs through downloaded programs that come with a malware embedded in the background of the program to facilitate crypto mining through your computer.
- Also, certain websites contain codes that mine cryptocurrency on computers as long as the site is open.

Solution

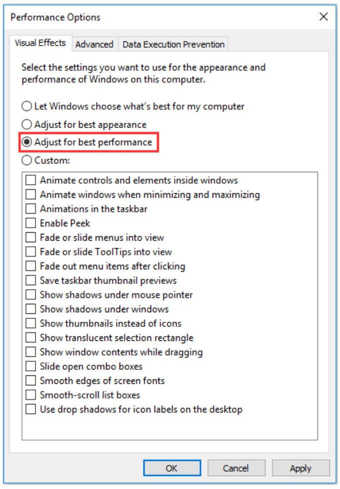
- Shutdown your browser when it is not in use to prevent crypto mining through websites on your PC.
- You can also identify if your PC is being used for crypto mining by searching for programs or tasks that are either suspicious or taking up processing power even when not in use on your Task Manager or Activity Monitor.
- Once you identify the program or task, you should end it.

OS Visuals Too High

Enabling visual effects on your computer can make it run slower than normal if your RAM is not big enough to support the effects.

Solution

- **For Windows:** go to Performance Settings or Advanced System Settings depending on your windows version. Click on Adjust visual effects then select Adjust for best performance.
- **For Mac:** go to System Preferences and uncheck the Animate Opening Application box.



Performance Options

Select the settings you want to use for the appearance and performance of Windows on this computer.

○ Let Windows choose what's best for my computer
○ Adjust for best appearance
● Adjust for best performance
○ Custom:

□ Animate controls and elements inside windows
□ Animate windows when minimizing and maximizing
□ Animations in the taskbar
□ Enable Peek
□ Fade or slide menus into view
□ Fade or slide ToolTips into view
□ Fade out menu items after clicking
□ Save taskbar thumbnail previews
□ Show shadows under mouse pointer
□ Show shadows under windows
□ Show thumbnails instead of icons
□ Show translucent selection rectangle
□ Show window contents while dragging
□ Slide open combo boxes
□ Smooth edges of screen fonts
□ Smooth-scroll list boxes
□ Use drop shadows for icon labels on the desktop

Internal PC Dust

- You may be dealing with a slow computer simply because you have forgotten to pay attention to the basic principles of proper ventilation.
- Accumulated dust in your CPU can prevent your processors from effectively cooling and prevent excessive heat from staying trapped inside your PC.
- This, in turn, can affect the speed at which your computer performs.

Solution

- Dust off your computer occasionally to clear its air vents.
- Also, once in a while have an IT professional clean inside of your PC.

Outdated Drivers

- Your computer uses drivers to communicate with hardware devices connected to it.
- If you are using outdated drivers, then the communication will most likely be faulty and take your computer longer than it should to have the connected hardware devices working properly.

Solution

- Browse the internet for the most recent drivers compatible with your computer hardware, download and install them or install driver updating software to locate and install the drivers for you.

Your PC May Be Too Old or Out of Date

- If your computer has been in use for more than 5 years, then running slow is more of a natural progression rather than a problem.
- At some point, due to the frequent releases of updates for programs, your computer will fail to meet the minimum requirements for certain updates leaving you to work with old and outdated programs.

Solution

You only have several options. Either purchase a new computer, update your computer’s hardware, or accept working with a slow computer.

PC Hardware Failure

- Your computer’s hard drive, RAM and CPU are prone to damage.

- If none of the above issues are the reason behind your computer running slow, then hardware failure could be imminent hence causing a slow down on your machine.

Solution

- It is advised to seek help from a computer support or IT professional.
- At Vintage IT services, we understand how frustrating the speed slump down must be to your productivity and business efficiency.
- As a leading provider of managed IT services, we can help take the burden away by troubleshooting, installing, and supporting your PC, so that you can focus on your core competencies.
- Would you love to learn more about how we can help you manage your IT resources? Contact us today and let us do the legwork for you.

Keyboard or Mouse has Stopped Working

Solution:

1. Reboot The Computer
2. Use Temporary Keyboard
3. Perform Basic Troubleshooting
4. Update Your Driver
5. Use Keyboard Troubleshooter
6. Check Mouse Properties

Reboot The Computer

- Have you tried restarting the computer? Sometimes users get overwhelmed when faced with computer issues that they forget about the most obvious solution.
- So, take a minute to reboot your PC before doing anything else.
- If you can’t move your mouse, you can shut down your computer by pressing **Windows** + **X** on your keyboard.
- This will bring up the **Start** menu. Go to **Shut Down or Sign Out** > **Restart** using the arrow keys.
- Or you can select **Alt** + **F4** to bring out the **Shut Down** window and use the arrow keys to select **Restart**.

Use Temporary Keyboard

- If restarting the computer doesn’t work and your keyboard has stopped working, you’ll need a temporary one that works. Fortunately, Windows has a built-in keyboard for such an occasion.
- The **On-Screen Keyboard** (OSK) can be accessed by going to **Windows Settings** > **Ease of Access** > **Keyboard**.
- Under **Use Your Device Without a Physical Keyboard**, switch **Use the On-Screen Keyboard** to the **On** position.
- You can also press **Windows** + **Ctrl** + **O** to open the virtual keyboard.

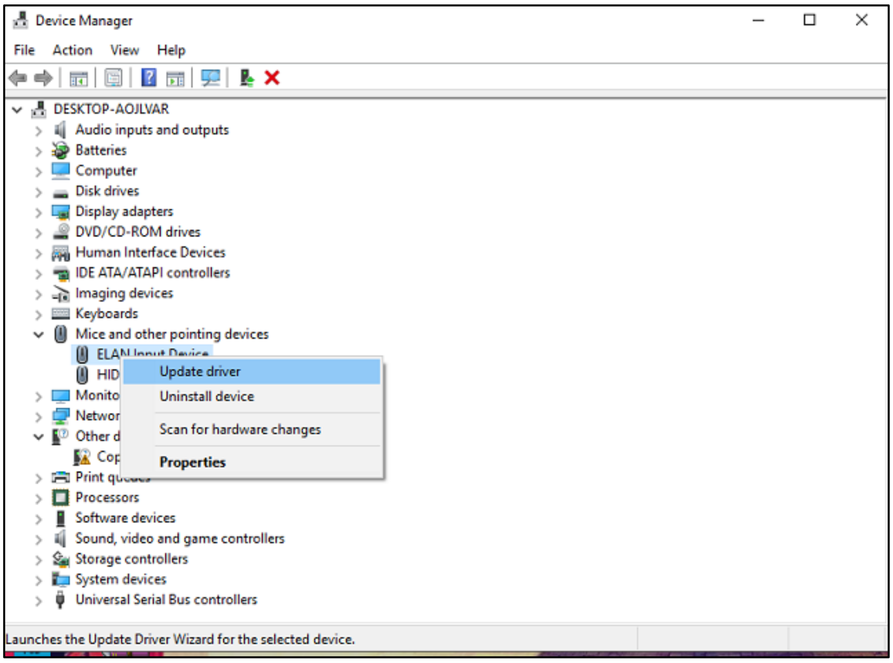
Perform Basic Troubleshooting

- First, check your mouse and keyboard cables. Are they disconnected? Are they showing signs of wear and tear? Have they been dislodged from their designated ports?
- If you’re using a wireless mouse or keyboard, have you tried replacing the batteries? Have you checked if your Bluetooth connection is still active? Those who are using external Bluetooth transmitters should see if that is causing the issue.

- You can try plugging in a different keyboard and mouse. If your computer does not respond to any keyboard or mouse, you might be having a software problem instead.

Update Your Driver

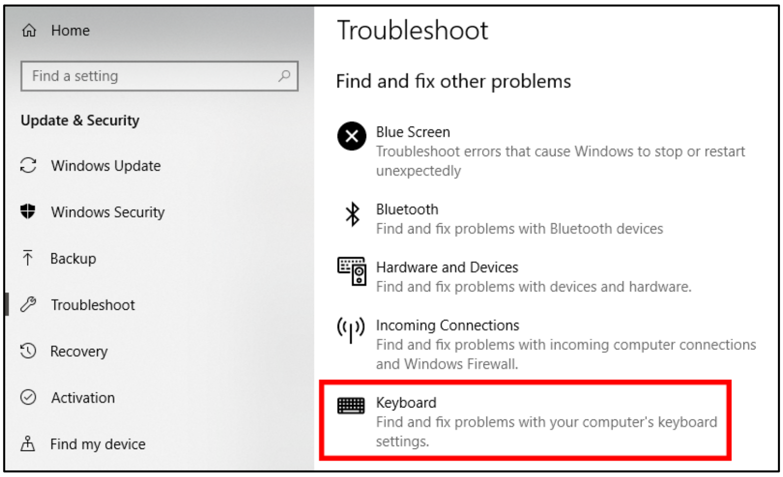
- Updating a device driver can potentially fix a problematic keyboard or mouse.
- Use **Search** to find and open **Device Manager**.
- Once open, expand **Keyboards** and **Mice and Other Pointing Devices**.
- Right-click on your device and select **Update Driver**.



Launches the Update Driver Wizard for the selected device.

Use Keyboard Troubleshooter

- Windows has a troubleshooter feature that deals with the nastiest of bugs and errors. It can also work out USB keyboard issues on your behalf.
- Go to **Windows Settings** > **Update & Security** > **Troubleshoot**. Under **Find and Fix Other Problems**, select **Keyboard**.
- Click **Run the Troubleshooter**.
- Windows will go on to find issues with your keyboard.
- If it finds an issue, just follow the on-screen commands so it can resolve the problem. If it cannot find anything, you will be shown a message that says so.
- If successful, the troubleshooter should make your keyboard work again.



Troubleshoot

Find and fix other problems

Blue Screen
Troubleshoot errors that cause Windows to stop or restart unexpectedly

Bluetooth
Find and fix problems with Bluetooth devices

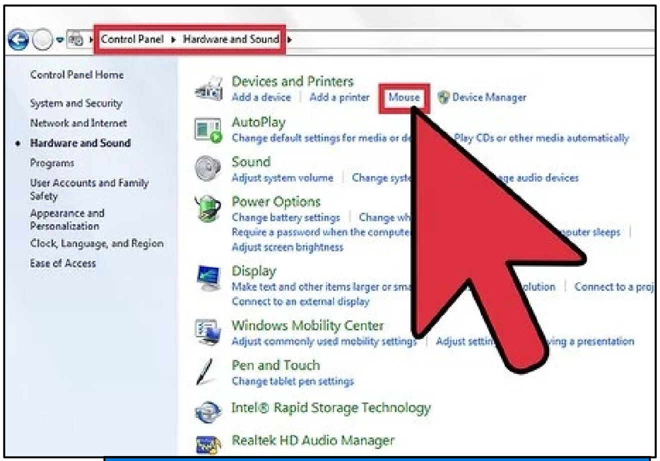
Hardware and Devices
Find and fix problems with devices and hardware.

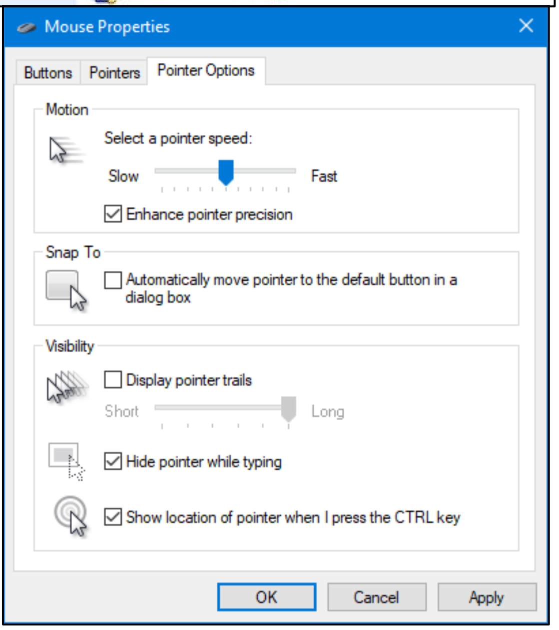
Incoming Connections
Find and fix problems with incoming computer connections and Windows Firewall.

Keyboard
Find and fix problems with your computer's keyboard settings.

Check Mouse Properties

- Open **Control Panel**. Go to **Hardware and Sound** > **Devices and Printers** > **Mouse.**
- Here you'll find a number of mouse properties that can impact its performance. You can make changes to your mouse buttons, pointers, pointer options, wheel, and hardware.
- Configure your mouse to your liking. If you find your mouse speed to be slow, for example, open the **Pointer Options** tab and select a more acceptable speed by moving the slider around.
- Hopefully, one of these mouse options will correct any of the perceived mouse errors.


Control Panel ▸ Hardware and Sound ▸
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Devices and Printers
Add a device | Add a printer | Mouse | Device Manager
AutoPlay
Change default settings for media or de... Play CDs or other media automatically
Sound
Adjust system volume | Change syst... ...ge audio devices
Power Options
Change battery settings | Change wh... ...puter sleeps |
Require a password when the compute...
Adjust screen brightness
Display
Make text and other items larger or sma... ...olution | Connect to a proj
Connect to an external display
Windows Mobility Center
Adjust commonly used mobility settings | Adjust settin... ...ing a presentation
Pen and Touch
Change tablet pen settings
Intel® Rapid Storage Technology
Realtek HD Audio Manager


Mouse Properties

Motion

Select a pointer speed:

☑ Enhance pointer precision

Snap To

□ Automatically move pointer to the default button in a dialog box

Visibility

□ Display pointer trails

☑ Hide pointer while typing

☑ Show location of pointer when I press the CTRL key

Other Common Issues

- Although most complex computer issues at work can often be solved by the business IT support team, there are many other small, but common, issues that occur on a regular basis on a personal computer.
- The following are the common computer problems that you shouldn't panic over.
  1. The Computer Won't Start
  2. The Screen is Blank
  3. Abnormally Functioning Operating System or Software
  4. Windows Won't Boot
  5. The Screen is Frozen
  6. Computer is Slow
  7. Strange Noises
  8. Slow Internet
  9. Overheating
  10. Dropped Internet Connections

The Computer Won't Start

- A computer that suddenly shuts off or has difficulty starting up could have a failing power supply.
- Check that the computer is plugged into the power point properly and, if that doesn't work, test the power point with another working device to confirm whether or not there is adequate power.

The Screen is Blank

- If the computer is on but the screen is blank, there may be an issue with the connection between the computer and the screen.
- First, check to see if the monitor is plugged into a power point and that the connection between the monitor and computer hard drive is secure.
- If the problem is on a laptop, then you may need to get a professional to fix it as some of the internal wires may be worn.

Abnormally Functioning Operating System or Software

- If the operating system or other software is either unresponsive or is acting up, then try restarting your computer and run a virus scan.
- To avoid having this happen, install reliable anti-virus software.

Windows Won't Boot

If you are having troubles booting Windows, then you may have to reinstall it with the Windows recovery disk.

The Screen is Frozen

- When your computer freezes, you may have no other option than to reboot and risk losing any unsaved work.
- Freezes can be a **sign of insufficient ram, registry conflicts**, **corrupt or missing files, or spyware**.
- Press and hold the power button until the computer turns off, then restart it and get to work cleaning up the system so that it doesn't freeze again.

Computer is Slow

- If your computer is slower than normal, you can often fix the problem simply by cleaning the hard disk of unwanted files.
- You can also ***install a firewall***, ***anti-virus*** and ***anti-spyware tools***, and ***schedule regular registry scans***.
- External hard drives are great storage solutions for overtaxed CPU's and will help your computer run faster.

Strange Noises

- A lot of noise coming from your computer is generally a sign of either hardware malfunction or a noisy fan.
- Hard drives often make noise just before they fail, so you may want to back up information just in case, and fans are very easy to replace.

Slow Internet

- To improve your Internet browser performance, you need to clear cookies and Internet temporary files frequently.
- In the Windows search bar, type '%temp%' and hit enter to open the temporary files folder.

Overheating

- If a computer case lacks a sufficient cooling system, then the computer's components may start to generate excess heat during operation.
- To avoid your computer burning itself out, turn it off and let it rest if it's getting hot.
- Additionally, you can check the fan to make sure it's working properly.

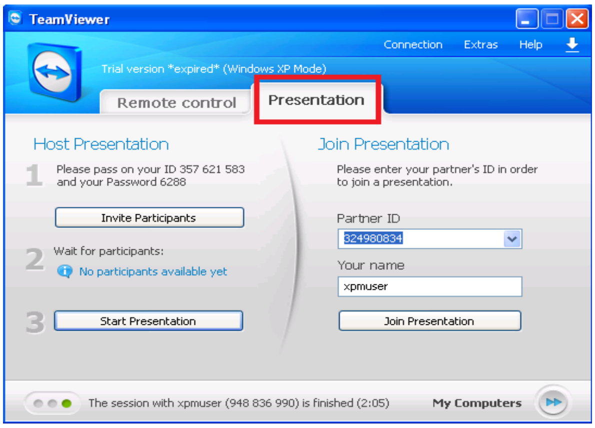
Dropped Internet Connections

- Dropped Internet connections can be very frustrating.
- Often the problem is simple and may be caused by a bad cable or phone line, which is easy to fix.
- More serious problems include viruses, a bad network card or modem, or a problem with the driver.

Screen Sharing with Team Viewer and Join me

What is Screen Sharing and How Does It Work?

- Screen share, also known as desktop sharing, is the practice of sharing the contents of your screen with another device or multiple devices.
- This can include all the elements on a screen or simply one window, which allows for complete control over the visibility of your desktop and guarantees privacy.
- By sharing your screen with Team Viewer, you have the ability to show friends, colleagues or clients any media that is on your device without ever having to send any files; this can include presentations, documents, images, and even videos.



Please pass on your ID 357 621 583 and your Password 6288

Wait for participants:

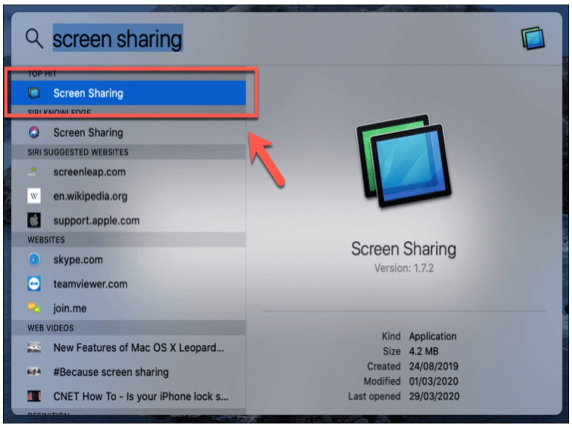
No participants available yet

Please enter your partner's ID in order to join a presentation.

Partner ID: 324980834

Your name: xpmuser

The session with xpmuser (948 836 990) is finished (2:05)



Kind	Application
Size	4.2 MB
Created	24/08/2019
Modified	01/03/2020
Last opened	29/03/2020

- What's more, this screen sharing software allows the recipient to not only view the material on the shared device, but also watch as the user interacts with it in real-time, navigating the interface and making changes.
- Online screen sharing works by breaking down the information depicted on the device screen into encoded packets of information and sending them across the internet to another device.
- The recipient device then rebuilds the image received from the other screen.
- Modern free screen sharing software is smart enough to both compress the data to minimize bandwidth requirements and carefully monitor activity on the screen: the software will only transmit information when a change or movement occurs.
- For this reason, Team Viewer's connection stability and image quality during remote screen sharing are excellent.

Screen Sharing & Remote Desktop Software

Here's a quick list of the screen sharing & remote desktop software

- TeamViwer
- Zoom (for a popular, secure, intuitive, feature-ful remote team choice)
- Google Meet (for more cloud storage)
- Microsoft Teams (for a focus on internal communication)
- Slack (for convenience if you're already Slack-centric)
- Screenleap (for sharing screens with anyone)
- Join.me (for frictionless new user access)
- GoToMeeting (for better security & encryption)
- Whereby (for better control over who enters your rooms)
- Mikogo (for a quick, simple, browser-based solution)
- Demodesk (for sales calls and presentations)
- Drovio (for creative collaboration)

Screen Sharing with Team Viewer

Use Case

- Screen share using TeamViewer is the optimal solution for webinars and online meetings, allowing you to share slides and other presentation materials with a large number of recipients in real time.
- It is also the ideal tool for software training, meaning educators can remotely connect to and guide their users through various stages of learning and development.
- Screen recording enables you to then recycle this material for future use.
- In this way, screen sharing software is not only an important business tool, but also a powerful learning aid.
- Online screen sharing means you can make the most of conference calls and meetings from anywhere in the world.
- No matter whether you are working remotely or your team is spread across multiple locations, enjoy instant collaborative communication that makes it seem as though you are in the same room together.
- Desktop sharing lets you demonstrate processes and share information in a practical and hands-on manner, without ever having to be physically present or compromise your time.

Requirements

- The TeamViewer screen sharing feature can support any device that runs the TeamViewer software.
- It is possible to share information from your mobile phone to your desktop computer, as well as from your tablet and vice versa.
- You can run screen sharing on multiple devices at once.
- Internet connection and TeamViewer installed on all participating devices.
- Online screen sharing is possible between Windows, macOS, Linux, and Chrome OS without any compatibility issues.
- You can even share your phone screen on iOS, Android and Blackberry devices.

Benefits of TeamViewer Screenshare Tool

Better Collaboration

- Enhance collaboration in your online meetings by sharing your computer screen.
- Colleagues can work on documents side-by-side while working from anywhere in the world.
- Presentations are made easy as all participants are able to follow in-line with the material being discussed.

More Effective Training

- Using screen sharing, instructors are able to give more engaging and effective training sessions.
- Trainees can view the exact workings of a product or specific processes to follow, rather than using static PowerPoint slides or recorded videos. In this way, screen sharing also allows for real-time feedback and discussion.

Streamlined Processes

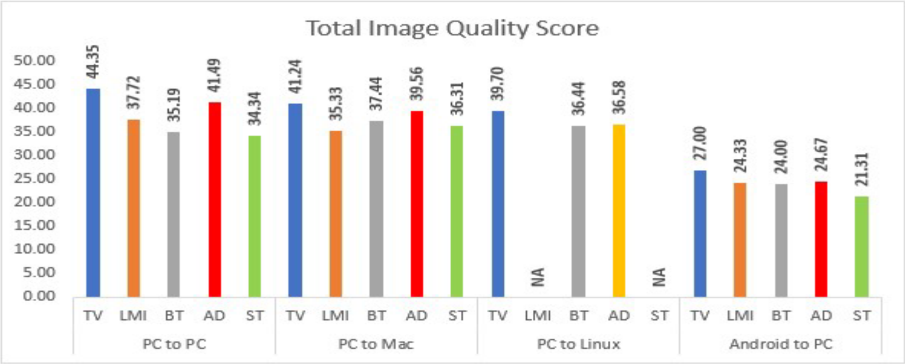
- Screen sharing software means there is no need to email presentations or documents for review.
- Share and discuss files in real time, saving time and improving the quality of outcomes while keeping your inbox clean.

- With no requirement to send or drop files using a web client, you never have to worry about compatibility issues.

Image Quality Performance

Best-in-Class for Image Quality Performance covering all consolidated tests consisting of:

- Screen latency
- Color grade
- Greyscale
- Image resolution



Results for total image quality score from TeamViewer 14 Qualitest Evaluation, 2019

Remote Access of Customer's Screen

You might require to get remote access to Customer's Device Screen to troubleshoot his desktop or laptop.

Windows

1. The first step is to install the Team Viewer application on your desktop.
2. Locate the downloaded file and click the file to install it. Go through the brief setup process.
3. Once the software is installed, access your desktop and click on the Team Viewer icon to launch the program.
4. Share the ID and password displayed on the app screen. This enables our agent to troubleshoot the issue.

MacOS

1. Download the TeamViewer set up for MacOS.
2. Click the file to install and launch the software.
3. Share the ID and password displayed on the TeamViewer screen with our support executive.
4. Once the agent is connected, select System Preferences from the Apple icon at the top left of the screen. Select Privacy below the Security and Privacy section. Click on the lock icon and log in using the computer sign-in password if needed.
5. Check the selection box for TeamViewer so that the agent can join the session and move the mouse and type if required.

- For using TeamViewer on Mojave and Catalina, you might have to allow three System Accesses types on your device: Screen Recording, Accessibility, and Full Disk Access.
- A user has to add these features correctly to enable remote access. Unless the screen will show only the desktop image and the top bar of the desktop.

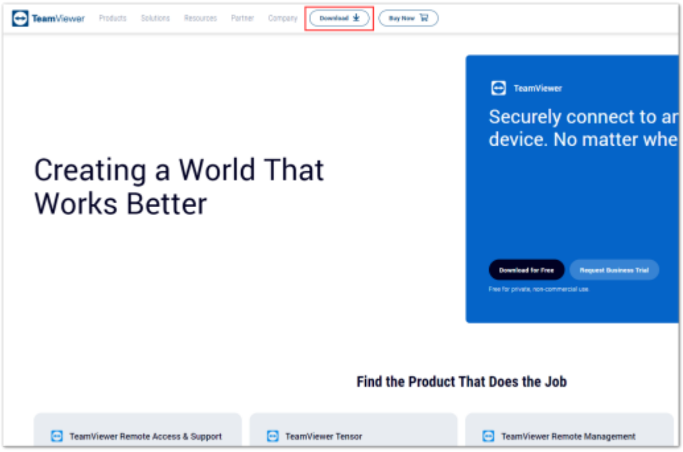
Browse Help -> Check system to access review accesses.

You can also make the changes in the following way:

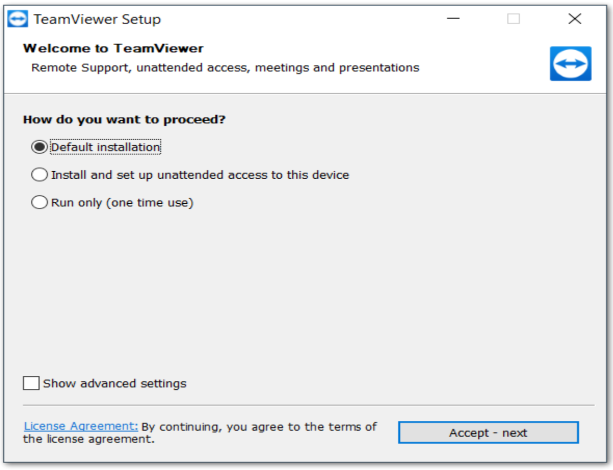
1. From Apple Icon select System Preferences and then select Security & Privacy.
2. Go to the Privacy section and click on the Lock Icon.
3. You might have to log in using your computer sign-in password if needed.
4. Place a check in the selection box for TeamViewer if it exists.

Installation of TeamViewer Win 7 and Above

1. Go https://www.teamviewer.com
2. Click the **Download** button at the top of the website
3. Follow the instructions to save the setup file


TeamViewer
Products
Solutions
Resources
Partner
Company
Download
Buy Now
Creating a World That Works Better
TeamViewer
Securely connect to ar device. No matter whe
Download for Free
Request Business Trial
Free for private, non-commercial use
Find the Product That Does the Job
TeamViewer Remote Access & Support
TeamViewer Tensor
TeamViewer Remote Management

4. Run the setup file downloaded previously
5. Select **Default Installation** under **How do you want to proceed?** and click **Accept – next**
6. Click the check-box to accept the TeamViewer EULA and DPA.
7. Click **Continue** to finish the installation and begin using TeamViewer.



TeamViewer Setup

Welcome to TeamViewer

Remote Support, unattended access, meetings and presentations

How do you want to proceed?

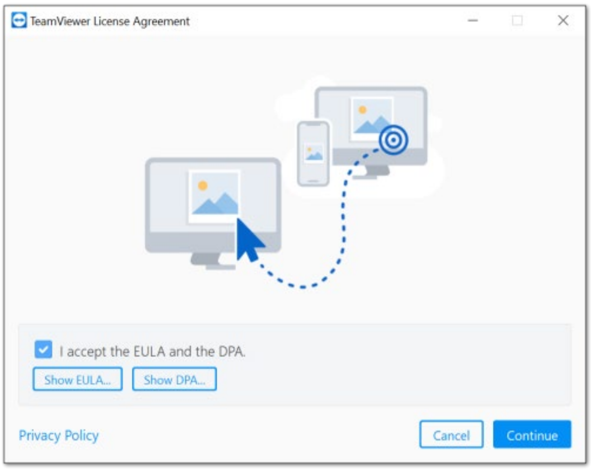
● Default installation

○ Install and set up unattended access to this device

○ Run only (one time use)

□ Show advanced settings

License Agreement: By continuing, you agree to the terms of the license agreement.



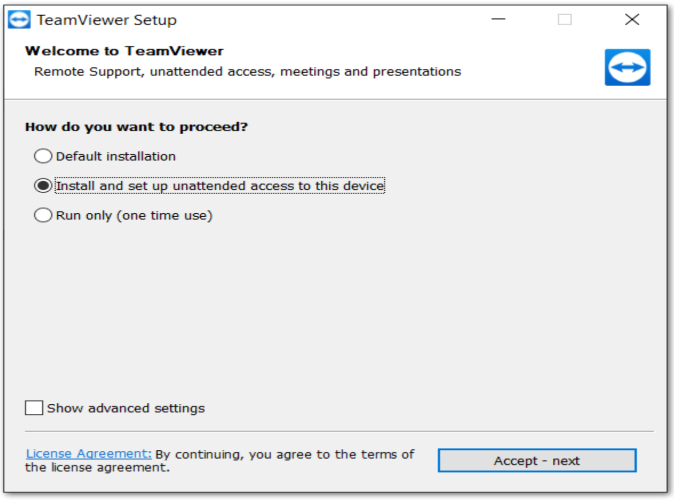
TeamViewer License Agreement

☑ I accept the EULA and the DPA.

Configure unattended access to the device

Note: Setting up unattended access is **optional**.

1) Run the setup file downloaded previously.
2) Select **Install and set up unattended access to this device** under **How do you want to proceed?** and click **Accept – next**



TeamViewer Setup

Welcome to TeamViewer

Remote Support, unattended access, meetings and presentations

How do you want to proceed?

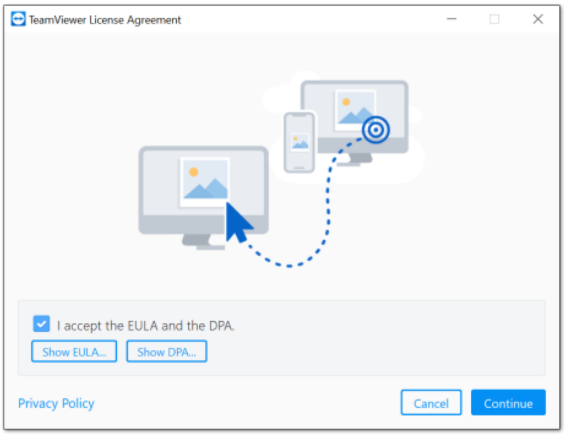
○ Default installation

● Install and set up unattended access to this device

○ Run only (one time use)

□ Show advanced settings

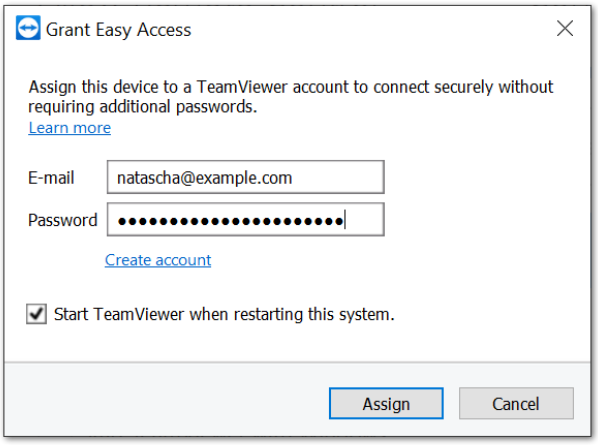
License Agreement: By continuing, you agree to the terms of the license agreement.



TeamViewer License Agreement

☑ I accept the EULA and the DPA.

3) Click the check-box to accept the **TeamViewer EULA and DPA.**
4) The TeamViewer full version opens and the popup **Grant Easy Access** appears
5) Enter the email address and password for the TeamViewer account for which you want to set up **unattended access** for this device.



Grant Easy Access

Assign this device to a TeamViewer account to connect securely without requiring additional passwords.

Learn more

E-mail: natascha@example.com

Password: ••••••••••••••••••••••

Create account

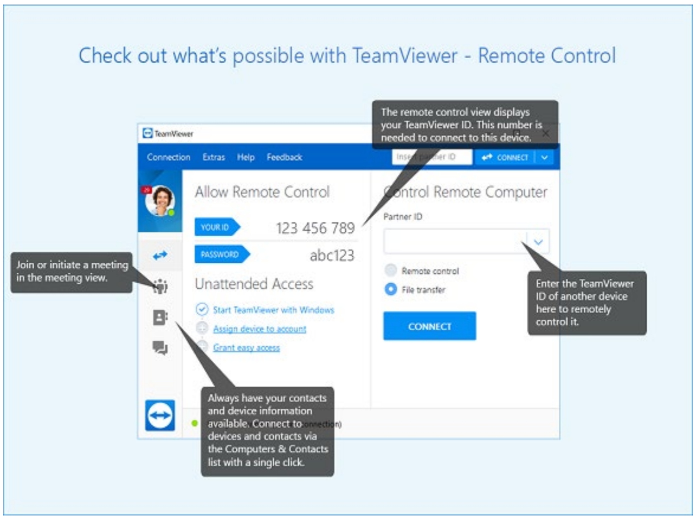
☑ Start TeamViewer when restarting this system.

Note: If you enable **Start TeamViewer when restarting this system**, TeamViewer will start automatically, and you can connect to it directly via Easy Access after the device booted.

6) Click **Assign** to finish the installation and begin using TeamViewer

Setting Up TeamViewer Remote Control

- In order to make a start with TeamViewer's remote-control functions, navigate to the Remote Control tab of the main interface.
- Here, you will find your TeamViewer ID and your temporary password, which you can change at any point.
- With this information, you can allow a partner remote control of your computer.
- In order to do this in reverse and control another computer remotely, you simply enter the partner computer ID and choose between various connection modes such as remote control, file transfer or VPN.
- Additionally, as soon as one or more remote connections have been established, each session will be displayed in the title bar of the Remote-Control window.


Check out what's possible with TeamViewer - Remote Control

The remote control view displays your TeamViewer ID. This number is needed to connect to this device.

Join or initiate a meeting in the meeting view.

Enter the TeamViewer ID of another device here to remotely control it.

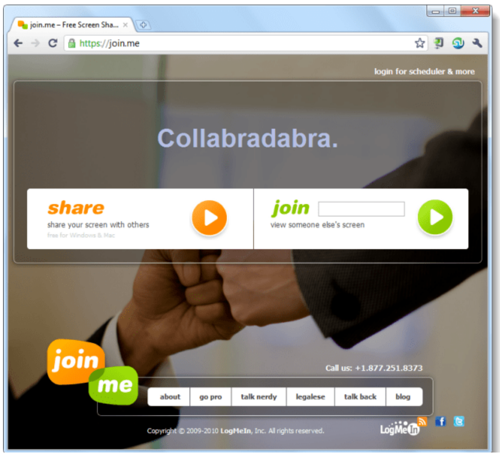
Always have your contacts and device information available. Connect to devices and contacts via the Computers & Contacts list with a single click.

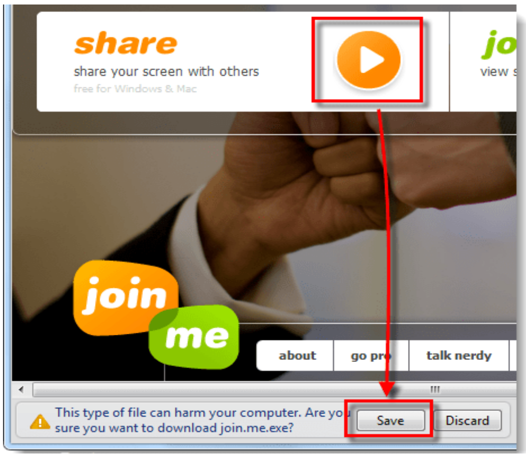
Screen Sharing with Join Me

- Join.me is a web-based collaboration software application for screen-sharing, file transfer and online meetings.
- To share a desktop or host a meeting, users must first download and install join.me software.
- Join.me allows you to simply send out a link to the participants which they can click on for instant access to your desktop.
- The service also includes a free conferencing bridge line that supports 250 participants.

How to Share screen using Join.me

Step 1 – Visit **https://join.me** to get started.



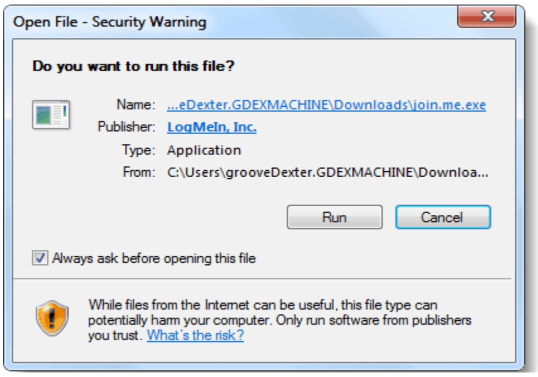

This type of file can harm your computer. Are you sure you want to download join.me.exe?

Step 2 – Share Your Screen

- Click the Share button on the join.me page and you'll be prompted to download a file (Chrome and Firefox users). It's completely safe.
- Start the file anywhere you like, it automatically deletes itself after you run it once.
- If you're running IE, you won't even be asked to download the file as it will use the Microsoft Click Once process to launch the file in your browser.

Step 3 – Run the downloaded file

- You'll likely encounter the famous Windows security pop-up when you run the join.me.exe file. That's ok, though, we know what to do here – *Click* **Run**.



Open File - Security Warning

Do you want to run this file?

Name: ...eDexter.GDEXMACHINE\Downloads\join.me.exe
Publisher: LogMeIn, Inc.
Type: Application
From: C:\Users\grooveDexter.GDEXMACHINE\Downloa...

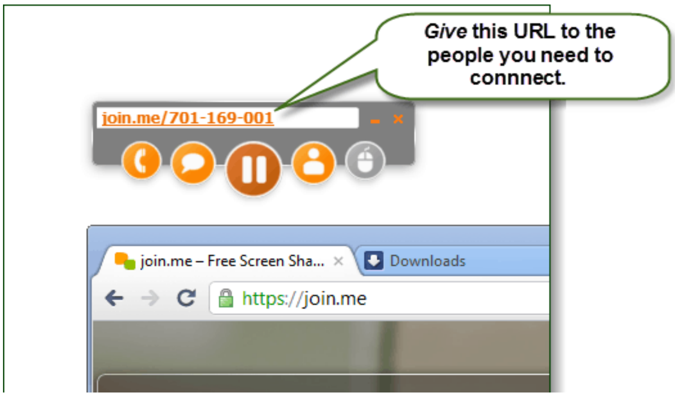
Run Cancel

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Step 4 – Invite others to view your screen

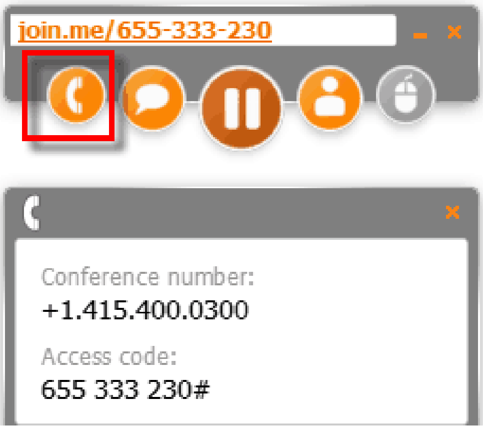
- Join.me lets you invite others easier than I've ever seen before.
- Each time you run the application, it generates a new and unique nine-digit number.
- All you have to do to let others connect is to give them that number.



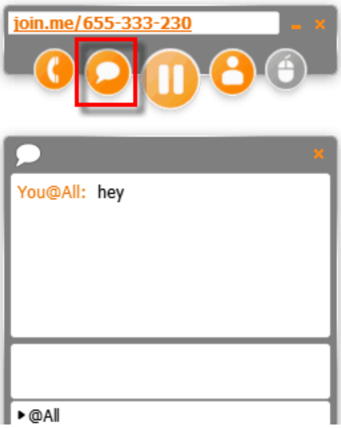
Give this URL to the people you need to connnect.

Step 5 – Conference calls and Chat

- Join.me gives you a conference line to call into; you can connect by dialing 1.415.400.0300 and entering your 9-digit unique id followed by the # sign.
- You'll notice in the screenshot below how the access code is the same as the orange text in the application box.
- Additionally, the chat window is real-time and displays the second you send it.
- Messages will appear both in the chat box and on the bottom-right of the screen as they appear.



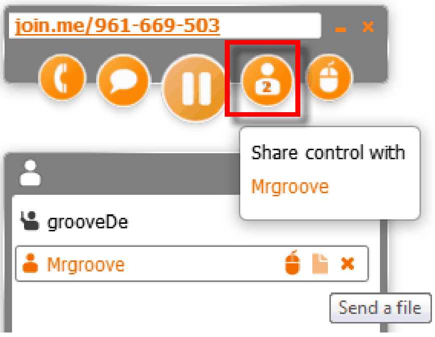
Conference number:
+1.415.400.0300
Access code:
655 333 230#

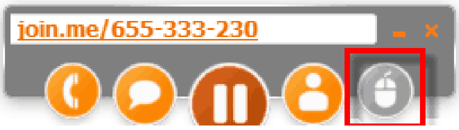


You@All: hey

Step 6 – User Management, File Sharing, and Screen Control

- If you want to see a list of everyone viewing your screen, you can click the people icon, and that will display.
- By default, it may not show the actual names of everyone, but they can manually change their name by visiting this same button.
- On the user list, you can also remove viewers, or send them files.
- Screen control works similar, select someone from the list and click the Control button to let them take the wheel.



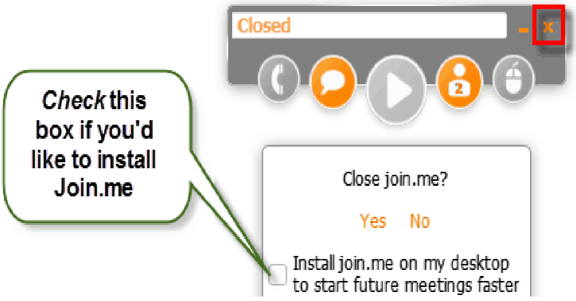


Note: *Only the host of the presentation can send files.*

Step 7 – Connect to someone's screen

- To connect to someone's screen, all you have to do is *visit* join.me and then *Type* their nine-digit number into the join box and *Press* **Enter**.
- There is no download; it just opens up in your browser.
- If the presenter sent you the link to their desktop session through email or chat, just clicking the link will instantly dump you into the session.

Step 8 – How to *Install* Join.me


Check this box if you'd like to install Join.me
Closed
Close join.me?
Yes No
Install join.me on my desktop to start future meetings faster

- You can download software from the join.me page.
- To install join.me, just share your screen once – it doesn't even have to be with any viewers.
- Once you've run the app, when you go to Close it an option will appear to Install join.me.
- Just *Check* the box labeled **Install join.me on my desktop to start future meetings faster**. It will then store it on your system and create a shortcut on the Start Menu and Desktop.

Common Password Managers

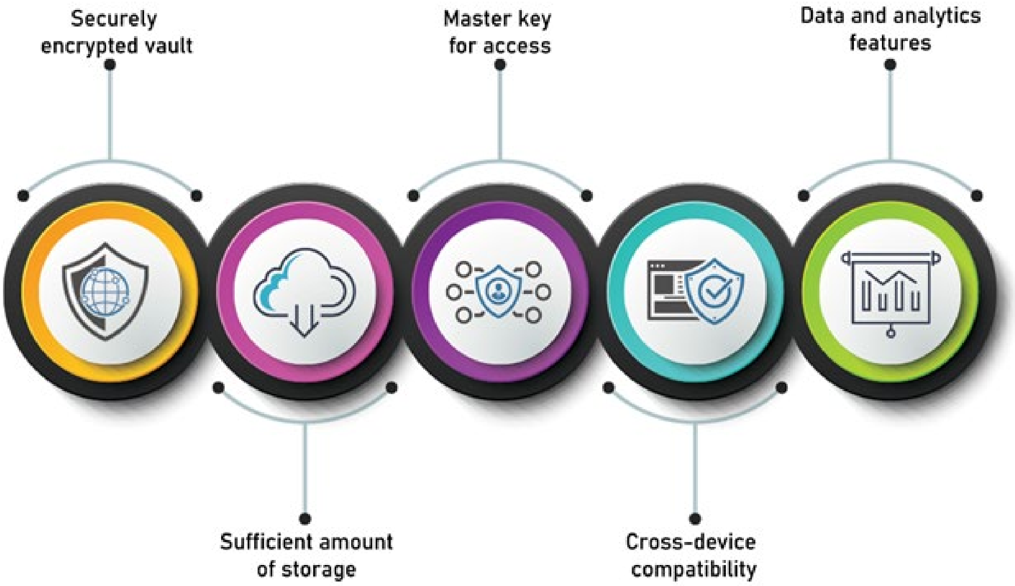
What is Password Manager

- A password manager is defined as a software application that securely stores user credentials in a cloud-based or on-premises vault, helping users stay safe online by following password creation and management best practices.
- It recommends password best practices to minimize the risk of the user forgetting the password as well as the risk of the password becoming exposed to entities with malicious intent.
- A password manager has two core purposes:
  - ➢ It ensures that passwords aren't lost or forgotten, reducing user frustration, loss of productivity, or even financial loss.

- ➢ It prevents unauthorized entities from getting hold of the passwords either through application vulnerabilities or social engineering.

- Password managers have emerged as a productivity staple.
- Storing passwords in your browsers, built-in storage, and auto fill engine is often the most common practice, but it is fraught with security risks.
- Instead, password managers offer a purpose-built solution to the security challenges arising from SaaS app sprawl, too many accounts, and multiple privileged users inside a business network.
- Studies reveal that 85% of people know that reusing the same password can be risky, but nearly 1 in 4 do it anyway.
- Indeed, it can be a hassle to generate a strong password for every account you create and keep track of, particularly when passwords have to be reset at regular intervals.
- Password management software combines convenience with security – often at competitive costs – to secure online experiences in a rapidly evolving digital world.
- In an enterprise setting, password managers come with sophisticated user authentication and access management capabilities to add another layer of protection.
- This further reduces the chances of user credentials getting breached.

Features of Password Manager


Securely encrypted vault
Master key for access
Data and analytics features
Sufficient amount of storage
Cross-device compatibility

1. Securely Encrypted Vault

- A built-in vault with at least AES encryption is where your passwords and credentials will be stored.
- In some solutions, the vault can store other file types like documents, imported Excel sheets, images, etc.
- But even if this value-added storage feature isn't available, a vault is a must-have for every password manager.

2. Sufficient Amount of Storage

- The password manager should be able to provide you with enough storage for all your access needs.
- If you access 10 to 15 SaaS apps (including social media) for your personal workflows and another 10 for work, a password manager that stores up to 20 records will fall short.
- You should look for software with unlimited storage for flexible and unrestricted use.

3. Master key for access

- A master key lets you access the entire repository of credentials, so you can modify, remove, or archive specific records.
- Some software platforms opt for an alphanumeric master key changed at regular intervals.
- Others follow a biometrics-based security protocol, while some even support physical keys stored on hardware peripherals.

4. Cross-device Compatibility

- You should be able to seamlessly switch from one device to another, one operating ecosystem to another, and one browser to another without losing access to your credentials.
- That's why a must-have feature for password managers is cross-device compatibility – it automatically fills in your credentials no matter which device you're on, as long as it is correctly verified.

5. Data and analytics

- The password manager must equip you with insights on credential patterns, access behavior, and repeat offenders for your security policies.
- This is particularly relevant to business use cases, where a large number of users can access data and leverage your network connectivity.
- Data and analytics are typically deployed through a centralized dashboard that is separate from the user UI client.

Commonly Used Password Manager

- A password manager can save you a lot of blood, sweat, and tears you'd otherwise spend on resetting lost credentials or trying to recover valuable assets to which you no longer have access.
- In 2022, password managers will be particularly important as cyberattacks continue to get more sophisticated and our reliance on credential-based saaS access grows.

> ***Please Note:*** *This is a curated list based on publicly available information from various sources and may include vendor websites that sell to mid-to-large enterprises. Readers are advised to conduct their own final research to ensure the best fit for their unique organizational needs.*

1. Dashlane

Overview:

- Dashlane comes in personal and business variants, equipping you with an easy-to-use password manager.
- Dashlane is available as a browser plugin for personal use and as a dashboard-enabled desktop integration for businesses.

Key features:

Some of Dashlane's key features include:

- Automatic password synchronization between devices and ecosystems
- Regular news updates about breaches and hacks
- A centralized dashboard for admins displaying password heath KPIs
- A Smart Spaces feature to keep professional and personal passwords separate
- SAML-based single sign-on (SSO)

USP:

- Dashlane is powered by a patented security architecture and AES 256-bit encryption, also protected by two-factor authentication.
- Dashlane supports in-app password sharing in case of emergencies without compromising on security.

Pricing:

- The pricing for personal accounts starts at $0 for up to 50 passwords, going up to $4.99 per month for up to 5 users (family).
- The pricing for businesses starts at $5 per user per month.

Editorial Comments:

- Dashlane is an excellent option for individuals and businesses looking to get started with password management technology, as it has a simple UI and next-to-zero learning curve.
- The dashboard equips admin roles with important information like average password strength, compromised passwords, and login activity – a hady feature at this price point.

2. <u>Kaspersky Password Manager</u>

Overview:

- In the world of cybersecurity and data protection, Kaspersky needs no introduction. It is particularly popular for its consumer-facing products, although it also offers security solutions for small/medium businesses and enterprises.
- Kaspersky Password Manager is meant for individual or family use; business users can find similar capabilities in the company's consolidated endpoint and cloud security offerings.

Key features:

Kaspersky Password Manager has the following key features:

- Consolidated storage for passwords, driver's license, bank card data, passports, etc.
- Master password and biometrics-based vault lock.
- Auto-detect technology to identify potentially sensitive information from screenshots.
- Password generator and duplicate password alerts.
- Automatic clipboard clearing after data entry.

3. <u>KeePass</u>

Overview:

- KeePass is among the few completely open-source and free password managers that are highly recommended by industry experts.
- It has won several awards and is also certified by the French Network and Information Security Agency.
- KeePass is currently in its 2.47 version with regular updates several times a year.

Key features:

KeePass enables the following password security features:

- Advanced Encryption Standard and the Two fish algorithm for encrypted databases
- Decryption using the master keyword or key files carried on a physical storage
- Lightweight software, with all races removed upon uninstallation.
- Exportable password lists in various formats like TXT, HTML, XML, and CSV.
- Clipboard clearing after you have copy-pasted a password

4. <u>Keeper</u>

Overview:

- Keeper is a versatile password management software that comes with dark web scanning capabilities.
- It is meant for password management and secure communication, ensuring that you do not accidentally reveal sensitive information through messaging.
- Keeper comes in several versions for personal and family use, as well as small/medium businesses, enterprises, and managed service providers.

Key features:

- A standard password manager and vault with secure document storage, auto-fill, and password generation.
- Dark web monitoring and account takeover protection.
- A private messaging app for sharing images, bank details, and other sensitive information (with message self-destruct capabilities).
- On-premise, cloud, and hybrid cloud environment support

5. <u>LastPass</u>

Overview:

- LastPass is the password management tool by communications and collaboration major, LogMeIn.
- It has two versions – personal and business-grade identity access management, with the latter including LastPass Identity.
- In addition to password management, LastPass also monitors the dark web and sends you timely alerts.

Key features:

- Cross-device access, password auto-fill, and string password generation.
- Secure password and note-sharing in-app, with optional one-to-many sharing
- Emergency access and encrypted file storage (i.e., vault).
- A password management dashboard in the family edition as well as business versions.
- 1200+ SSO integrations and 100+ customizable policies.

Password Manager – Google Chrome

- Chrome can help you identify and change passwords that were compromised by data breaches so that your credentials remain secure.
- Your credentials include your usernames and passwords for sites or apps that you sign in to.

How Password Protection Works

- If you’re signed in to Chrome, Chrome can warn you if the username and password you use to log in to a website were involved in a data breach. This setting is turned on by default.
- You can also use Chrome to check all of your saved credentials at the same time. Chrome checks your saved passwords and then lets you know if any of them were exposed in a data breach.
- To check your credentials, Chrome first encrypts your username and password. Then it sends the encrypted credentials to Google for comparison against an encrypted list of known breached data.
- If Chrome detects a match between the encrypted sets of data, it displays a warning that prompts you to change your password.
- Google never learns your usernames or passwords during this process.

Managing Password in Chrome

If you enter a new password on a site, Chrome will ask to save it. To accept, click **Save**.

- To see the password that will be saved, click Preview.
- If there are multiple passwords on the page, click the Down arrow. Choose the password you want saved.
- If your username is blank or incorrect, click the text box next to "Username." Enter the username you want saved.
- If you want to save a different password, click the text box next to "Password." Enter the password you want saved.

Manually Add a New Password

1. On your computer, open Chrome.
2. At the top right, click More and then Settings and then Autofill.
3. Click Passwords and then Add.
4. Enter a website, username, and password.
5. Click Save.

Tip: If you're signed in to your Google Account on your computer, you can save the password to your Google Account, or save the password locally on your device.

Sign in with a Saved Password

If you saved your password to Chrome on a previous visit to a website, Chrome can help you sign in.

1. On your computer, go to a site you've visited before.
2. Go to the site's sign-in form.
   - **If you've saved a single username and password for the site:** Chrome will fill in the sign-in form automatically.
   - **If you've saved more than one username and password:** Select the username field and choose the sign-in info you want to use.

Show, edit, delete, or export saved passwords

1. On your computer, open Chrome.
2. At the top right, click Profile and then Passwords.
   - If you can't find the Passwords icon, at the top right of your screen, click More and then Settings and then Autofill and then Passwords.
3. Show, edit, delete, or export a password:
   - **Show:** To the right of the website, click Show password Preview. If you lock your computer with a password, you'll be prompted to enter your computer password.
   - **Edit:** To the right of the website, click More and then Edit password.
   - **Delete:** To the right of the website, click More and then Remove.
   - **Export:** To the right of "Saved Passwords," click More and then Export passwords.

To clear all your saved passwords, clear browsing data and select "Passwords."

Start or Stop Saving Passwords

By default, Chrome offers to save your password. You can turn this option off or on at any time.

1. On your computer, open Chrome.
2. At the top right, click Profile and then Passwords.
- If you can’t find the Passwords icon, at the top right of your screen, click More and then Settings and then Autofill and then Passwords.
3. Turn Offer to save passwords on or off.

Sign in to Sites and Apps Automatically

- You can automatically sign in to any sites and apps where you have saved your credentials using "Auto sign-in."
- When you turn on "Auto sign-in," you do not need to confirm your username and password.
- If you want to confirm your saved credentials when you sign in, you can turn off "Auto sign-in."

1. On your computer, open Chrome.
2. At the top right, click Profile and then Passwords.
- If you can't find your Google Account
- If you can’t find the Passwords icon, at the top right of your screen, click More and then Settings and then Autofill and then Passwords.
3. Turn Auto sign-in on or off.

Check your Saved Passwords

- You can check all your saved passwords at once to find out if they're exposed in a data breach or potentially weak and easy to guess.

To check your saved passwords:

1. On your computer, open Chrome.
2. At the top right, click Profile and then Passwords.
- If you can’t find the Passwords icon, at the top right of your screen, click More and then Settings and then Autofill and then Passwords.
3. Click Check passwords.

You'll get details on any password exposed in a data breach and if any passwords may be weak.

To Start or Stop Notifications

1. On your computer, open Chrome.
2. At the top right, click More and then Settings.
3. Click Privacy and security and then Security.
4. Click Standard protection.
5. Turn Warn you if passwords are exposed in a data breach on or off.

Tip: This feature is only available if the "Safe Browsing" option is activated.

Password Manager – WiFi

- WiFi password can be changed through D-Link, TP-Link, and Netgear, among other routers configuration page. For this, you’ll need the IP address of your router.
- While you can open the configuration page on mobile phones as well, we would recommend you do it on Windows PC/ laptop or mac

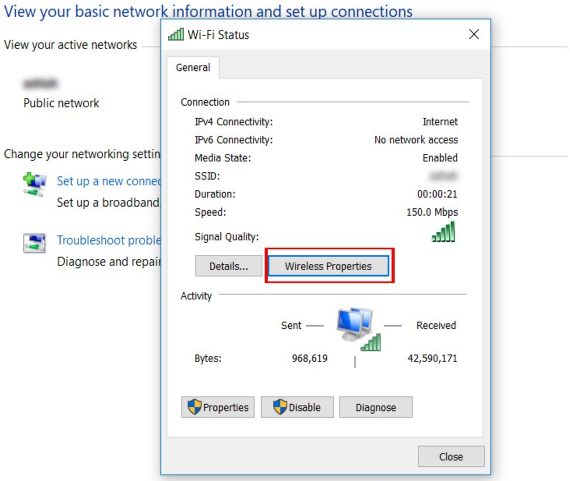
How to change WiFi password

1. Connect your Android mobile phone, iPhone, or PC/ laptop to the WiFi network and fire up your browser.
2. Type in the IP address on the search bar. This is usually 192.168.1.1 or 192.168.0.1, but you should confirm it by looking at the bottom of your router.
3. Login to the router using its username and password. They are commonly written at the bottom of your router.
4. In most scenarios, the username and password are ‘admin’ and ‘useradmin’ respectively. You should check with service provider if they don’t work.
5. Look for the “Wireless” or “Wireless Security” option. This should be either on the top menu or at the side menu under Advanced Settings or Security options.
6. You’ll see the old password in the WiFi Password or security key box.
7. Enter the new password in the box and hit the ‘Save’ button. The WiFi password will change and the network will log out from all the connected devices.
8. Reconnect the devices by entering the new WiFi password.

How to find WiFi password on Windows 10

One method is through the IP address. In addition to that, you can find the WiFi password in Windows 10 using these steps (presuming that your PC/ laptop is connected to the network):

1. Click on the WiFi network icon, next to date and time and other quick settings options, from the bottom right corner of the page. Alternatively, you can open the Control Panel and head to Network and Internet > Network Connections.
2. Select the WiFi network you’re connected to
3. Click on Status > Wireless Properties
4. Under the Security tab, you should see a password box with dots in it—click the Show Characters box to know the password appear in plain text.



View your basic network information and set up connections

View your active networks

[redacted]
Public network

Change your networking settin

Set up a new connec
Set up a broadband

Troubleshoot proble
Diagnose and repair

Wi-Fi Status

General

Connection

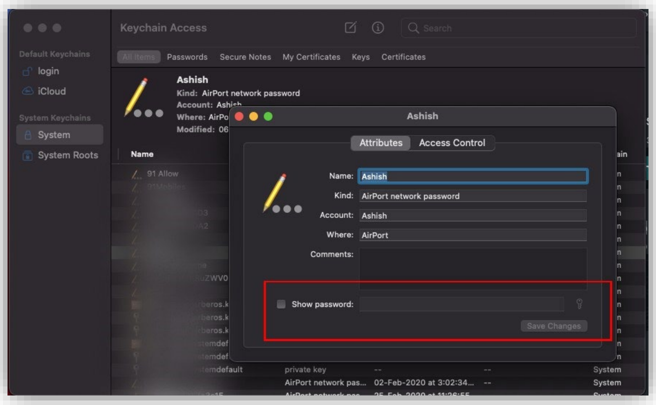
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
SSID: [redacted]
Duration: 00:00:21
Speed: 150.0 Mbps
Signal Quality:

Activity

Sent — — Received
Bytes: 968,619 | 42,590,171

How to check WiFi password in macOS

1. Open Spotlight Search using Command+Space and type “Keychain access”.
2. Select the app from the menu and click on System.
3. Here you’ll see all the saved passwords to applications as well as WiFi.
4. Double click on the WiFi network whose password you want to know. If you can’t locate the network, you can search it from the box at the top right corner.
5. Tick the box next to ‘Show Password’.
6. Verify that’s you by entering the password.
7. Your Wi-Fi password will then appear in the box next to “Show Password”.
8. You can also check WiFi password in macOS through the IP address.



Keychain Access

Default Keychains
login
iCloud
System Keychains
System
System Roots

Ashish
Kind: AirPort network password
Account: Ashish
Where: AirPo
Modified: 06

Name
91 Allow

Ashish

Name: Ashish
Kind: AirPort network password
Account: Ashish
Where: AirPort
Comments:

□ Show password:

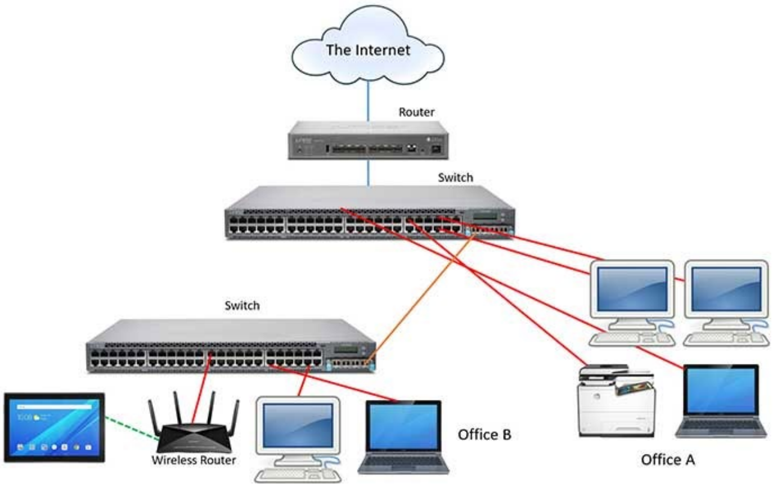
private key -- -- System
AirPort network pas... 02-Feb-2020 at 3:02:34... -- System

1.3 Basics of Networking

Basics of Networking

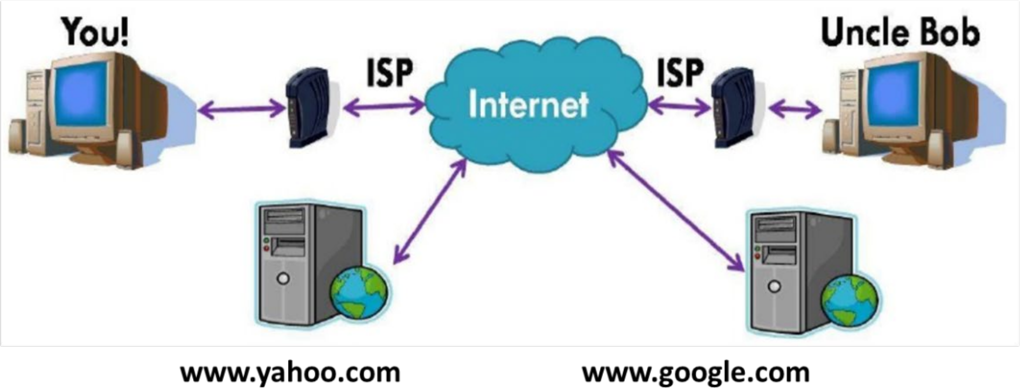
The foundations of Networking are:

1. Switches
2. Routers
3. Wireless Access Points



Internet

The Internet is a worldwide, publically accessible series of interconnected computers



CLIENT – knows how to communicate with a particular type of server to use the information stored on that server.

SERVER – handles requests for data, email, file transfer, and other network services. It stores information to be used by clients.

How did the Internet originate?

In 1969, the US Department of Defence started a project called ARPAnet to enable military communication and it is the foundation of the INTERNET.

What is the WWW?

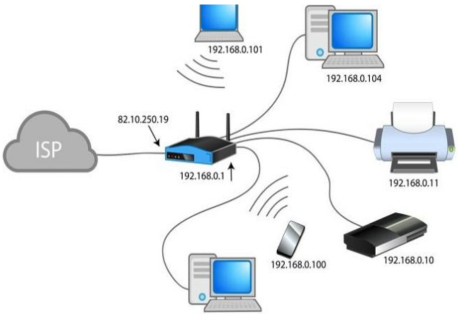
WORLD WIDE WEB. Collection of electronic documents, also called WEB. Each electronic document is called a Web page which contains text, graphics, audio, video, and built-in connections.

What is a Web Browser?

Application software that enables you to access and navigate the Web or the Internet by viewing web pages. ¤ Ex. Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, Opera, Safari etc.

What is IP Address?

- Internet Protocol (IP) address a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.
- Number that uniquely identifies each computer device connected to the internet
- Four groups of numbers, separated by a dot
- Number in each group is between 0 and 255
- Ex. 74.125.71.103



***Domain Name** is text version of an IP address. (www.google.com)*

Broadband

“Broadband is defined as a high bandwidth connection to the Internet. Broadband is easier and faster to use than the traditional telephone and modem as information can be sent and downloaded much quicker”

- Broadband speed is measured in megabits per second (Mbps)
- File sizes are measured in megabytes (MB) or gigabytes (GB)
- There are 8 bits in a byte (10101010)
- A download speed of 8 bits will shift 1MB per second

Wireless broadband transmits signals to a computer over radio waves

Mbps vs MBPS

- **Mbps** is used to specify Internet connection speeds, whereas **MBps** is used to specify how much of a file is downloaded/uploaded per second.
- Mbps vs. MBps. Mbps: (Small "b") A megabit per second (Mbit/s or Mbps) is a unit of data transfer rate equal to 1,000,000 bits per second or 1,000 kilobits per second.
- 8 Megabits per second is equivalent to 1 Megabyte per second (i.e., 8 Mbps = 1 MBps).

Switches

- Switches are the foundation of most business networks.
- A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.
- Switches allow devices on your network to communicate with each other, as well as with other networks, creating a network of shared resources.
- Through information sharing and resource allocation, switches save money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics: **on-premises** and **cloud-managed**.

- ➢ On-Premises

- Cloud-Managed

On-premises

A managed on-premises switch lets you configure and monitor your LAN, giving you tighter control of your network traffic.

Cloud-Managed

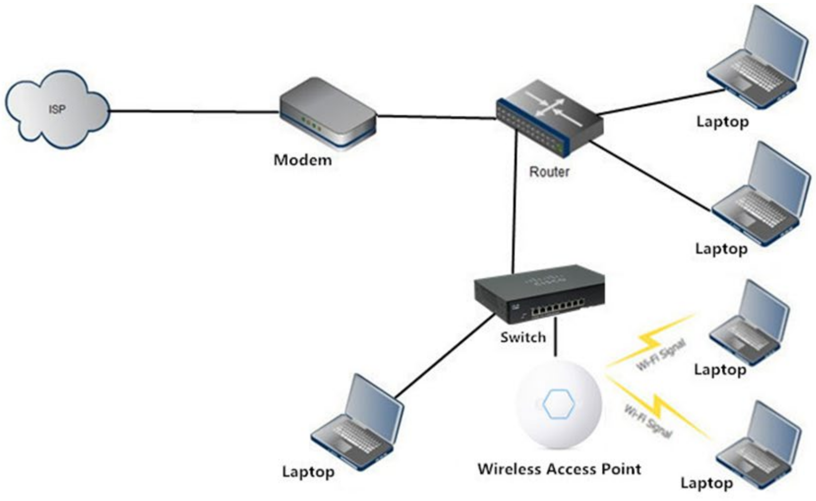
Have a small IT team? A cloud-managed switch can simplify your network management. You get a simple user interface, multisite full-stack management, and automatic updates delivered directly to the switch.

Routers

- Routers connect multiple networks together.
- They also connect computers on those networks to the Internet.
- Routers enable all networked computers to share a single Internet connection, which saves money.
- A router acts a dispatcher.
- It analyses data being sent across a network, chooses the best route for data to travel, and sends it on its way.
- Routers connect your business to the world, protect information from security threats, and can even decide which computers receive priority over others.
- Beyond those basic networking functions, routers come with additional features to make networking easier or more secure.
- Depending on your security needs, for example, you can choose a router with a firewall, a virtual private network (VPN), or an Internet Protocol (IP) communications system.

Wireless Access Point

- An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.
- An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a WiFi signal to a designated area.



Wireless Networking

To create your wireless network, you can choose between three types of deployment:

1. Centralized Deployment

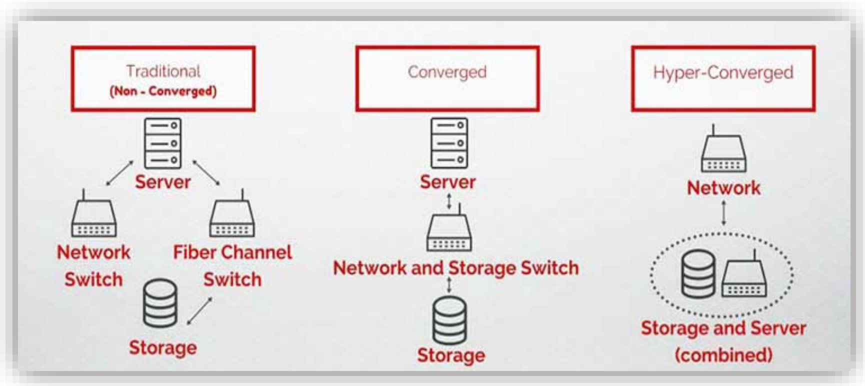
2. Converged Deployment
3. Cloud-based Deployment

1. Centralized Deployment

- Centralized deployments are traditionally used in campuses where buildings and networks are in proximity.
- This deployment consolidates the wireless network, which makes upgrades easier and facilitates advanced wireless functionality.
- Controllers are based on-premises and are installed in a centralized location.

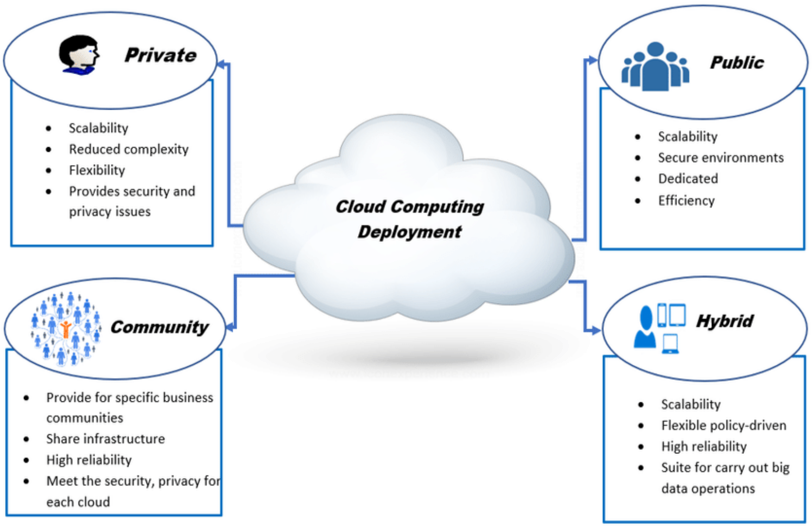
2. Converged Deployment

- For small campuses or branch offices, converged deployments offer consistency in wireless and wired connections.
- This deployment converges wired and wireless on one network device—an access switch—and performs the dual role of both switch and wireless controller.



3. Cloud-based Deployment

- This system uses the cloud to a manage network devices deployed on-premises at different locations.
- The solution requires Cisco Meraki cloud-managed devices, which provide full visibility of the network through their dashboards.

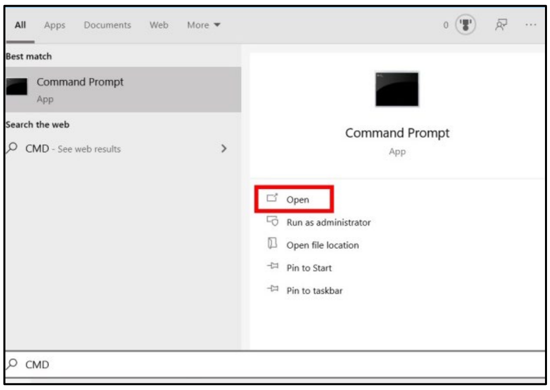


1.4 Ping, Traceroute and Path Ping Test

Ping Test

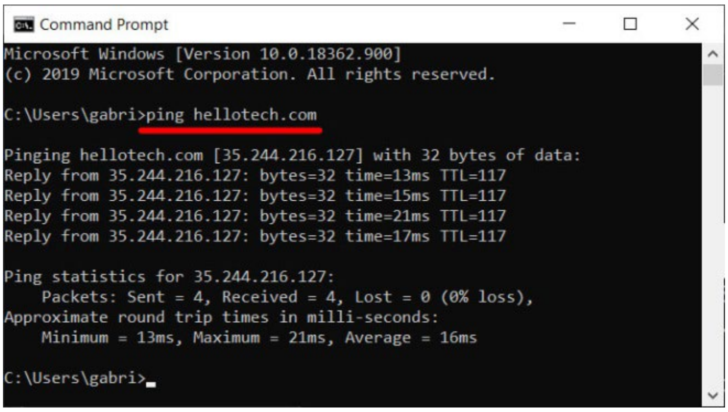
- Ping is used to testing a network host capacity to interact with another host.
- A ping test is used to measure latency of internet connection.
- Latency (or Ping) is the reaction time of your connection-how quickly your device gets a response after you've sent out a request.
- It tells you the quality of your connection.
- It is important to have a low latency connection for online gaming, loading web pages quickly, video chatting, and more.
- When you do a ping test, your computer sends a small packet of data to your host, a web domain, or another device in your network.
- The results will show you how fast your computer gets a “ping” response back in milliseconds. You want your ping response time to be as low as possible.
- This is performed by using the Internet Control Message Protocol, which allows the echo packet to be sent to the destination host and a listening mechanism.
- If the destination host reply to the requesting host, that means the host is reachable.

How to Do a Ping Test on a Windows 10 PC



- To do a ping test in Windows 10, open the Windows Search Bar, type CMD, and click Open.
- In the Command Prompt, type ping followed by a space and then the IP address or domain name you want to test and hit Enter.

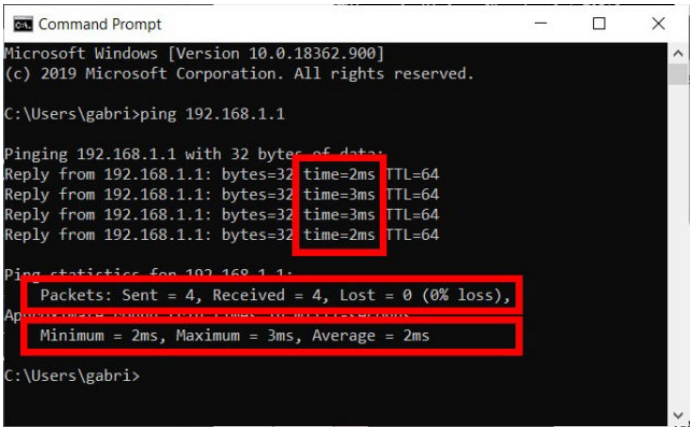
1. **Open the Windows Search Bar.** You can do this by clicking the magnifying glass icon in the bottom-left corner of your screen.
2. **Then type *CMD* into the search bar and click *Open*.** This will open a Command Prompt window with a black background, white text, and a flashing cursor.
3. **Type *ping* followed by a space and an IP address or domain name.** For example, you would enter “*ping 192.168.1.1*” or “*ping hellotech.com*”.
4. *Finally, hit Enter on your keyboard and wait for the ping test results.*
    - Type “cmd” to bring up the Command Prompt.
    - Open the Command Prompt.
    - Type “ping” in the black box and hit the space bar.
    - Type the IP address you’d like to ping (e.g., 192.XXX.X.X).
    - Review the ping results displayed.



```
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gabri>ping hellotech.com

Pinging hellotech.com [35.244.216.127] with 32 bytes of data:
Reply from 35.244.216.127: bytes=32 time=13ms TTL=117
Reply from 35.244.216.127: bytes=32 time=15ms TTL=117
Reply from 35.244.216.127: bytes=32 time=21ms TTL=117
Reply from 35.244.216.127: bytes=32 time=17ms TTL=117

Ping statistics for 35.244.216.127:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 21ms, Average = 16ms

C:\Users\gabri>_
```

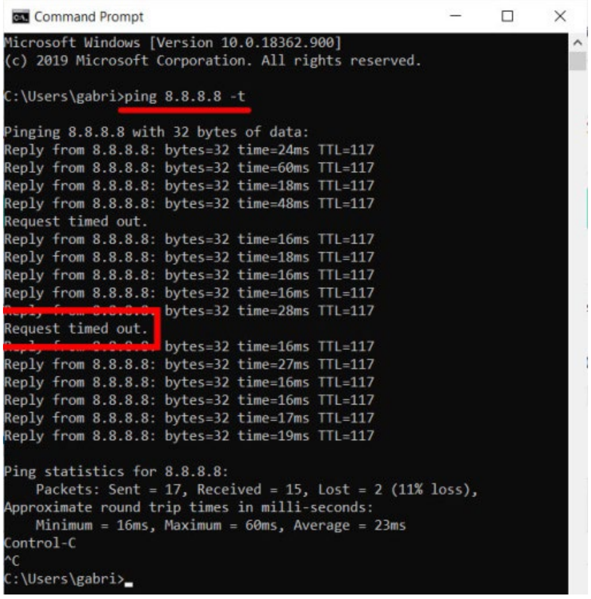
Understanding Ping Results

- The first thing you'll see is the server's host name. This will confirm you have an active connection to the server.
- Next are the number of bytes being sent to the server, which will typically show 32.
- The next four lines indicate the response time from the server. You'll see how many bytes of data were sent back, as well as how many milliseconds the response took to return.
- TTL means **"time to live"** This information shows you the total routers the packet will travel through before stopping.
- If you see **"request timed out"** it tells you that the packets couldn't find the host, which indicates a connection problem and the destination you're attempting to ping is unreachable.
- The Ping statistics section shows the overall numbers for the process.
- The packets line shows the number of packets sent and received, and tells you if any were lost. If they were, there's like a connection issue.
- Lastly, approximate round trip times show the connection speed. The higher the time, the worse the connection.



```
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gabri>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\gabri>
```

- If you are doing a ping test to check your internet connection, you can ping Google's DNS servers by entering "*ping 8.8.8.8*".
- In order to see continuous ping results, you can append your command with "*-t*". For example, you can enter "*ping 8.8.8.8 -t*" to see if your connection to Google's DNS servers ever times out. Then, to stop the test, simply hit the *Control* + *C* keys on your keyboard at the same time.



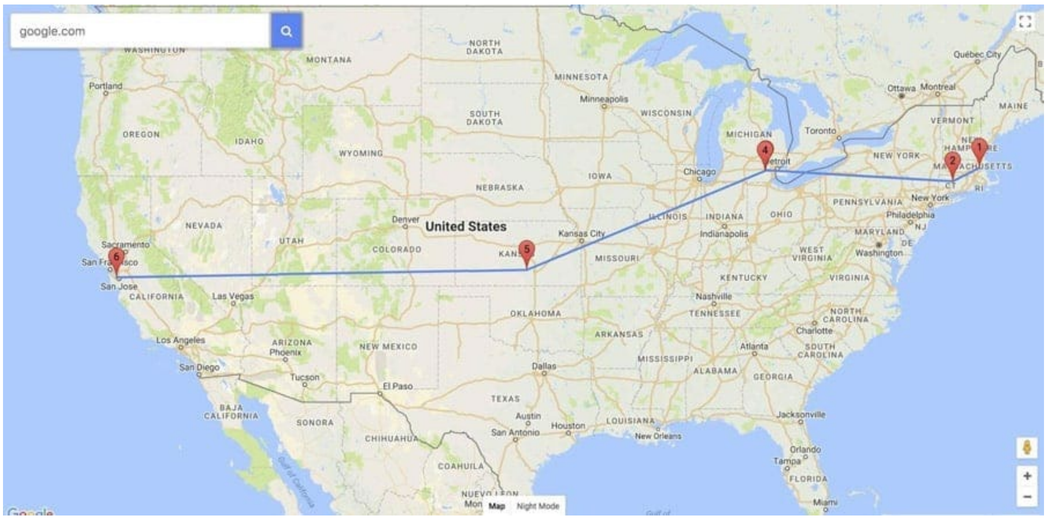
```
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gabri>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=60ms TTL=117
Reply from 8.8.8.8: bytes=32 time=18ms TTL=117
Reply from 8.8.8.8: bytes=32 time=48ms TTL=117
Request timed out.
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=18ms TTL=117
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=28ms TTL=117
Request timed out.
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=27ms TTL=117
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=16ms TTL=117
Reply from 8.8.8.8: bytes=32 time=17ms TTL=117
Reply from 8.8.8.8: bytes=32 time=19ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 17, Received = 15, Lost = 2 (11% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 60ms, Average = 23ms
Control-C
^C
C:\Users\gabri>_
```

Traceroute Command

- With Ping, you might be able to know whether you have connectivity or not. A simple binary, yes or no. But traceroute takes native-OS network analytics to a higher level.
- With Traceroute, you can?
  1. Get the complete path that a packet uses to reach its destination.
  2. Discover the names and identity of routers and devices within the path.
  3. Find the time it took to send and receive data to each device on the path.

> Traceroute gives you complete information about the path that your data will take to reach its destination, without actually sending data (other than ICMP).

For example, if the source of the path (your computer) is in Boston, Massachusetts and the destination in San Jose, California (a Server), Traceroute will identify the complete path, each hop (the computers, routers, or any devices that comes in between the source and the destination) on the path, and the time it takes to go and come back.



Running a Trace Route on Windows, Linux, or MacOS

For Windows

- You can run a traceroute command on almost all Windows platforms, including, XP, Vista, Server, Windows 7, 8, 10, etc.
  1. Start by opening the **“Command Prompt”.** Go to “Start”, type in “CMD” and press enter.
  2. Use the **“tracert”** command. Type in “tracert” along with a target to trace a route towards a destination.

For Linux

- To perform a traceroute on any Linux OS, such as Debian, Red Hat, Ubuntu, etc.
  1. **Start by opening the Terminal.** Press Ctrl + Alt + T or type in “terminal” in the search bar.
  2. **Install traceroute**

- If you do not have traceroute already installed, you may need to install it. For instance, in Ubuntu, the command to install traceroute is “sudo apt-get install traceroute”.
  3. **Use the traceroute command.** Type in “traceroute” along with a hostname or IP address.

For Mac OSX

You can also run a traceroute command in your macOS.

1. **Open the terminal**

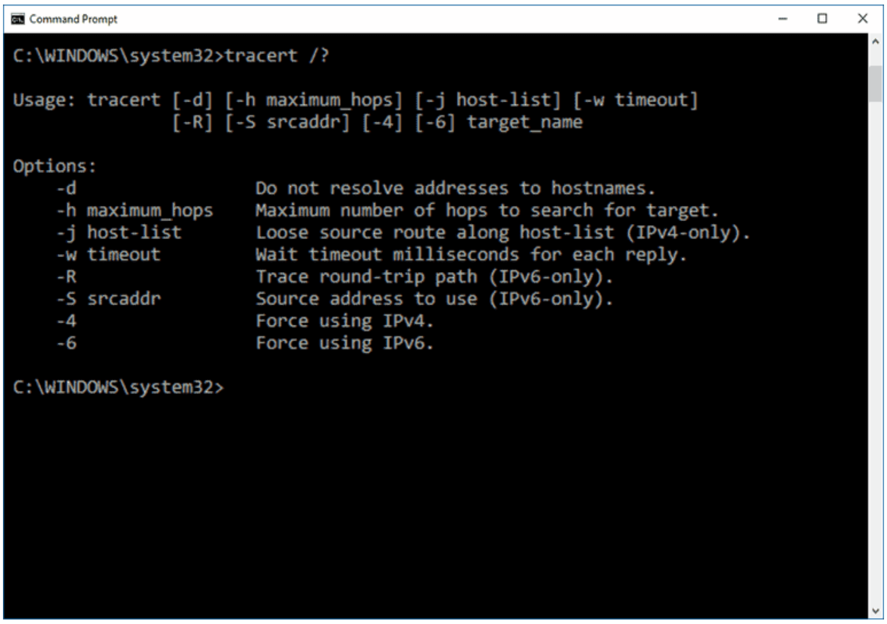
First, you need to open the Terminal. It can be done by going to "Applications", then "Utilities" and double-clicking on "Terminal".

2. **Type in the traceroute command.** Use the traceroute command and enter the target.

Traceroute Command Syntax and Options (for Windows)

The tracert command syntax is given below:

tracert [-d] [-h MaxHops][-j HostList] [-w TimeOut][-R RoundTrip] [-S Source] [-4] [-6] target [/?]



```
C:\WINDOWS\system32>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\WINDOWS\system32>
```

Below is a brief description with each tracert option in Windows…

Option	Description
-d	This tracert option prevents tracert from resolving IP addresses to hostnames, often resulting in much faster results.
-h MaxHops	This option specifies the maximum number of hops in the search for the target. If you do not specify MaxHops, and a target has not been found by the default max hops (30 for Windows), tracert will stop looking.
-w TimeOut	Using this tracert option, you can specify the time, in milliseconds, to allow each reply before timeout.
-4	It forces tracert to use IPv4 only.
-6	It forces tracert to use IPv6 only.
Target	A mandatory option. It is used to specify the destination, either an IP address or hostname.
/?	Use the help switch with the tracert command to show detailed help about the command's multiple options.

Reading the Traceroute Output

Example 1

The command:

```
C:\>tracert 11.1.0.1
```

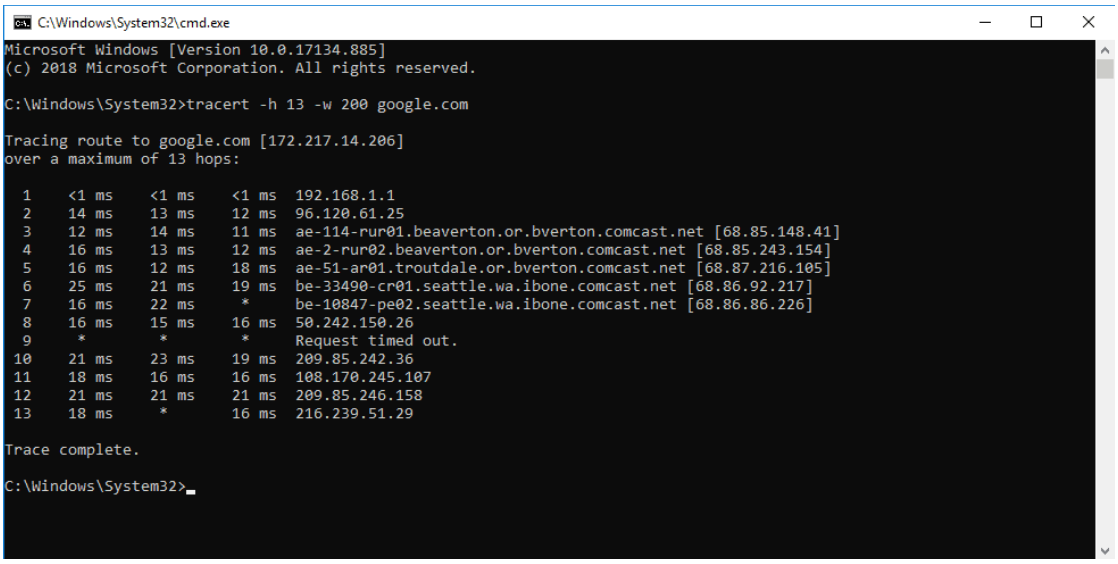
The output from the command:

```

Tracing route to 11.1.0.1 over a maximum of 30 hops
---------------------------------------------------
1 2 ms 3 ms 2 ms 157.54.48.1
2 75 ms 83 ms 88 ms 11.1.0.67
3 73 ms 79 ms 93 ms 11.1.0.1

Trace complete.
```

In the above example of the tracert command and its output, the packet travels through two routers (157.54.48.1 and 11.1.0.67) to get to host 11.1.0.1. The default gateway is 157.54.48.1 and the IP address of the router on the 11.1.0.0 network is at 11.1.0.67.

Example 2

With the tracert example shown below, we're requesting the command to display the path from the local computer to the network device with the hostname "www.google.com" (with additional requests).



```
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\System32>tracert -h 13 -w 200 google.com

Tracing route to google.com [172.217.14.206]
over a maximum of 13 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    14 ms    13 ms    12 ms  96.120.61.25
  3    12 ms    14 ms    11 ms  ae-114-rur01.beaverton.or.bverton.comcast.net [68.85.148.41]
  4    16 ms    13 ms    12 ms  ae-2-rur02.beaverton.or.bverton.comcast.net [68.85.243.154]
  5    16 ms    12 ms    18 ms  ae-51-ar01.troutdale.or.bverton.comcast.net [68.87.216.105]
  6    25 ms    21 ms    19 ms  be-33490-cr01.seattle.wa.ibone.comcast.net [68.86.92.217]
  7    16 ms    22 ms     *     be-10847-pe02.seattle.wa.ibone.comcast.net [68.86.86.226]
  8    16 ms    15 ms    16 ms  50.242.150.26
  9     *        *        *     Request timed out.
 10    21 ms    23 ms    19 ms  209.85.242.36
 11    18 ms    16 ms    16 ms  108.170.245.107
 12    21 ms    21 ms    21 ms  209.85.246.158
 13    18 ms     *       16 ms  216.239.51.29

Trace complete.

C:\Windows\System32>_
```

There are five columns, the first is the number of hops, the next three columns are three ICMP (pings) with the delay, and finally the IP or hostname.

- In the example shown above, we didn't reach our final destination (google.com). The last hop that sent us the "ICMP TTL Time Exceeded" message was number 13 or (public IP 74.125.242.179). This was because we limited the number of hops to 13, with (-h 13). Probably Google was at hop 14, or more.
- The other option we tested was timeout (-w 200). This is the maximum waiting time in milliseconds for each packet before it is considered lost.
- To read the delay columns, you can start with 1 ms, which is the hop to the gateway.

- The largest delay we can see here was on hop 5, which took 209 ms (from source 1 to hop 5). In other words, it took (209 – 8) 201 ms from hop 4 to 5.

Path Ping Command

- The pathping command which provides a combination of the best aspects of Tracert and Ping.
- The command provides details of the path between two hosts and ping-like statistics for each node in the path based on samples taken over a period, depending on how many nodes are between the start and end host.
- The advantages of PathPing over ping and traceroute are that each node is pinged as the result of a single command, and that the behavior of nodes is studied over an extended period, rather than the default ping sample of four messages or default traceroute single route trace.
- The disadvantage is that it takes a total of 25 seconds per hop to show the ping statistics.

The syntax for path ping is as follows:

```
pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
        [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
        [-4] [-6] target_name
```

g host- list	Loose source route along host list.
h maximum_hops	Maximum number of hops to search for target.
i address	Use the specified source address.
n	Do not resolve addresses to hostnames.
p period	Wait period milliseconds between pings.
q num_queries	Number of queries per hop.
w timeout	Wait timeout milliseconds for each reply.
P	Test for RSVP PATH connectivity.
R	Test if each hop is RSVP aware.
T	Test connectivity to each hop with Layer 2 priority tags.
4	Force using IPv4.
6	Force using IPv6.

Section 3: Exercises

Exercise 1: Draw ITIL Service Lifecycle.

Exercise 2: Draw basic network architecture.

Exercise 3: Participate in group discussion on following topics:

a) Types, Features and Benefits of IT Helpdesk
b) Common Computer Problems
c) Features and Types of Password Managers
d) Basics of Networking
e) Comparison between Ping, Traceroute and Path Ping Commands

Section 4: Assessment Questionnaire

1. How to troubleshoot a power supply issue?
2. How to troubleshoot motherboard errors?
3. How to troubleshoot RAM?
4. How to troubleshoot the HDD/ODD?
5. How to troubleshoot issues with monitor?
6. How to troubleshoot issues with graphics card?
7. How to troubleshoot issues with the keyboard/mouse?
8. What is the main cause of No display of a computer?
9. How to troubleshoot no display problem?
10. How to troubleshoot no power issue?
11. How to troubleshoot a wired keyboard?
12. How to troubleshoot a Mouse issue?
13. How to troubleshoot a wireless keyboard or mouse?
14. How to troubleshoot a Fatal error?
15. How to troubleshoot a printer no printing issue?
16. How do I fix random restarts in the Windows system?
17. What are the Main Causes of Win32 Errors?
18. How to troubleshoot the “not a valid Win32 application” error?
19. Troubleshoot why is my wi-fi is not working?
20. Troubleshoot when a computer freezes or locks up?
21. What are the ITIL four dimensions of service management?
22. What are the four types of service desk as per ITIL?
23. What are the common causes of slow computer?
24. _________ is the practice of sharing the contents of your screen with another device or multiple devices.
25. _______ is a web-based collaboration software application for screen-sharing, file transfer and online meetings.
26. A _________ is defined as a software application that securely stores user credentials in a cloud-based or on-premise vault, helping users stay safe online by following password creation and management best practices.
27. Storing passwords in your browsers, built-in storage, and auto fill engine is often the most common practice, but it is fraught with security risks. (True/False)
28. Tell some features of Password Manager.
29. What are two types of switches used in computer networking?
30. _______ analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way.
31. An _______ is a device that creates a wireless local area network, or WLAN, usually in an office or large building.
32. To create your wireless network, you can choose between which three types of deployment?
33. With _____ command you might be able to know whether you have connectivity or not, whereas, _______ command discovers the names and identity of routers and devices within the path.
34. _________ gives you complete information about the path that your data will take to reach its destination, without actually sending data.
35. The _______ command provides details of the path between two hosts.

----------End of the Module----------

MODULE 2

Tools We Will Use

Section 1: Learning Outcomes

After completing this module, you will be able to:

- Explain Importance and Benefits of IT Tickets
- Differentiate between various Types of IT Tickets
- Describe Ticket sources and Classification
- Route, Manage, Escalate the IT Tickets
- Explain Ticketing System Mechanism and Software
- Describe features of HelpDesk and SeamlessDesk Application
- Install HelpDesk and SeamlessDesk Application
- Generate ticket in HelpDesk and SeamlessDesk Application

Section 2: Relevant Knowledge

2.1 Ticketing System – Service Desk

What is an IT Ticketing?

- IT tickets is the generalized term used to refer to a record of work performed (or needing to be performed) by your IT support organization to operate your company's technology environment, fix issues and resolve user requests.
- Tickets may represent many different types of tasks or activities depending on the nature of your IT environment and the focus of your support team.
- They may go by other names like "service requests", "trouble tickets" or "support cases" but most organizations and users are familiar with the term "IT ticket" so we will use it for simplicity.

Importance of IT Ticketing

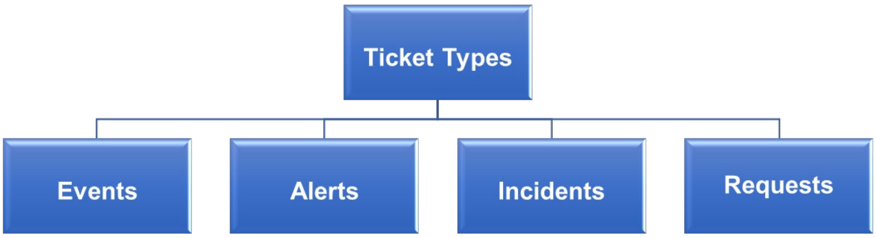
- IT tickets hey keep a record of each of the operations and support activities that take place to keep your IT environment up and running, adding value to the business.
- Tickets are typically captured in an IT Service Management where they are stored, managed and updated as the issue or activity is resolved.
- IT helpdesks use tickets as a means of capturing and recording interactions with users.
- Operations teams use tickets to track technical issues that need to be addressed.
- IT management uses ticket data to understand the workload of their teams, make resourcing decisions and facilitate vendor partnerships.

Benefits of IT Ticketing

- Service desk ticketing systems help streamline, centralize, and manage support tickets, saving time and manual effort for the help desk team and improving help desk agent productivity.
- IT technicians should also consider a ticket management system for its reporting capabilities. The right tool will offer a built-in reporting engine to monitor technician performance, ticket status, customer satisfaction, and other relevant key performance metrics.
- It should even be able to track customer support needs by location, real-time billing data, and incidence frequency.

- The benefit of using tickets as a general record for these things instead of treating each independently is that they all involve similar data, follow similar lifecycle/workflows, and are often addressed by the same people.
- Treating them all as tickets helps drive staff productivity, gives users fewer touchpoints into IT, and enables easier data analysis and reporting.

Ticket Types



Events

- Events are records of things that have happened in your IT environment.
- They may be point-in-time events or have an extended duration.
- Examples of events are releases, outages, maintenance activities and planned changes.

Alerts

- Alerts are indicators that something might have happened in your IT environment or that something is operating outside of pre-defined performance thresholds.
- Most alerts are system generated through automated monitoring and error handling.

Incidents

- Incidents are unplanned interruptions or reductions in quality of an IT service or failure of a component in your IT environment that has not yet affected service.
- Examples of incidents are outages, errors and performance issues. Incidents have a defined start and end that correspond to some sort of event.

Requests

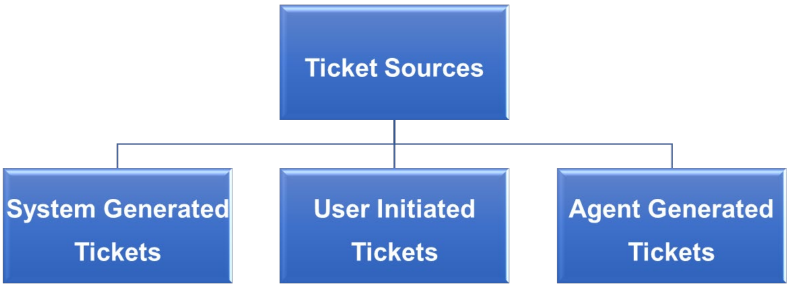
- Also called service requests are routine activities such as requesting access, resetting passwords, updating data or provisioning services that your IT support team performs on your operational systems and services.
- They don’t indicate that something is broken, only that something needs to be done.

Creating Tickets

- IT tickets are a record of activities and issues that need attention.
- The decision on whether to create a ticket or not doesn’t change whether the underlying task still needs to be performed.
- General IT ticketing best practices suggest that a ticket should be created if any of the following conditions exist:
  - Someone in IT needs to perform a task
  - An issue existed that impacted user productivity
  - A record is needed to enable analysis and decision making

Ticket Sources

- There are three primary sources of IT tickets.
- Since tickets are records of activities or issues, it is important to note that these are the sources of the ticket records and not the source or cause of the activity itself.



System Generated Tickets

Most modern IT systems include monitoring and error handling capabilities to automatically record tickets in an ITSM system when abnormal events or conditions occur.

User Initiated Tickets

The most common source of IT tickets is end users of IT systems and services requesting support through some sort of self-service portal, email or embedded “get help” capabilities.

Agent Generated Tickets

Helpdesk agents, operations staff and monitoring center employees record tickets for situations where a support activity is initiated but no record yet exists. Examples include calls into a helpdesk, maintenance activities and monitoring alerts.

Classifying Tickets

- Ticket classification data is used for establishing SLA expectations, routing tickets to the proper support teams and grouping tickets for analysis and reporting purposes.
- Rule-based workflow automation utilizes ticket classification data as a key tool for improving the efficiency of support processes.
- There are 4 key pieces of classification data that IT tickets should include:

Type – Event, Alert, Incident, Request or Question
Source – System, User or Agent generated
Priority – Assigned priority of the system, business process or activity the ticket relates to
Criticality – Rating of time sensitivity, degree of business impact and urgency of the issue.

Tickets need to be accurately and consistently classified so they receive the appropriate level of attention from your support team and ensure that the most important issues for the company get addressed first.

Routing Tickets

- Company's ITSM system will likely play an important role in facilitating tickets being routed between support teams.
- Business rules and automation can help ensure quick and effective handoffs but ultimately ticket routing is controlled by your support agents and the data they enter into the ticket.
- IT ticketing best practices suggest that the most effective way to avoid misrouting of tickets is through agent education on how ticket routing works.
- There are 3 common routing scenarios for IT tickets that your support agents should be familiar with.

Routing to internal support teams
Routing to external support partners
Follow-the-sun support

Routing to internal support teams

- Most of the ticket routing that takes place occurs within the helpdesk or IT support organization, directing tickets to specialized resources based on skills and/or experience.
- For example, tickets related to account permissions might be routed to an access management team, or complex software issues may get routed to experienced technical resources with access to source code.
- Internal routing is often referred to as re-assignment because the original agent transfers ownership and is relieved of responsibility for the issue when routing occurs.

Routing to external support partners

- Some companies leverage 3rd party support vendors and component suppliers to resolve tickets.
- These external partners typically do not use the same ticketing system as your helpdesk and routing issues to them often require creating a ticket in the partner's system and referencing it within the internal ticket.
- What makes this scenario unique is that the agent working on the ticket retains ownership and is responsible for brokering status updates to the requestor as the 3rd party resolves the underlying issue.

Follow-the-sun support

- At the end of the working hours in one location, open tickets are handed off to another support center for continued troubleshooting.
- This routing scenario is like internal support team routing except that active work-in-progress is expected to be transitioned so continuous support can be maintained (the ticket doesn't go back into the queue for re-prioritization).

- By ensuring that support agents understand how these routing scenarios work, how to initiate and control routing rules and what happens to ownership of the ticket, they will be able to transition tickets more effectively and assist the user in getting the issue resolved quickly.

Managing Ticket Queues

- When tickets are created and/or routed to a new support team, they are typically assigned to a queue or backlog instead of being assigned directly to an individual.
- Queueing enables managers and support team leaders to prioritize the work that their teams perform to ensure the most important issues are addressed first.
- Many organizations employ a first-in/first-out (FIFO) approach to queue management but IT ticketing best practices suggest using a combination of 7 key factors for prioritizing tickets in support queues (these are in no specific order):
    - Ticket Age – How long has the issue been in queue
    - Priority of the system or service impacted
    - Skills required to resolve the issue
    - Subject area – specialized knowledge or access requirements
    - Difficulty of the issue
    - Geographic location of the impacted business
    - Local language requirements

Ticketing SLAs

- Service level agreements (SLAs) are a measurement tool for evaluating ticket handling performance against a pre-defined set of criteria.
- More importantly, they are a tool for driving the behavior of how tickets are handled by your support team and external partners.
- The defined SLA measurement areas and performance targets will determine how both teams and individuals manage their support workload.
- It is common practice for IT tickets to be evaluated on 2 SLAs:

Response Time SLA – The elapsed time from a ticket being created and/or assigned to a queue until it is accepted by an individual and active troubleshooting begins.

Resolution Time SLA – The total elapsed time from ticket creation until it is set to a resolved state indicating the issue has been fully addressed.

- Both SLAs focus on the speed of response and ticket resolution and encourage the behavior of agents trying to close cases quickly.
- IT support can be costly and while these SLAs can help encourage cost control, companies must be careful that this doesn't lead to undesired behavior and quality issues.
- IT ticketing best practices suggest that SLAs, for the quality of support and customer satisfaction, should also be included to encourage agents to focus on resolving the underlying issue impacting the user instead of focusing on closing the support ticket.
- Ticket SLAs should be both measurable and include specific performance targets to be most effective.
- In addition to the SLA metrics, ticketing best practices suggest that the following metrics be tracked to help with evaluating the overall performance of your support operations and targeting areas for improvement:

- **Recurrence / Re-open rate –** a measure of quality support
- **Backlog count –** an indicator of both responsiveness and resource capacity issues
- **Effort (active support time) –** a simplified measure of ticket difficulty
- **# of handoffs –** effectiveness of support workflows and routing rules
- **User satisfaction –** a measure of communication effectiveness
- **First call resolution –** an indicator of agent skillset and data collection at ticket creation

Escalations

- IT tickets can be complex, and it is unreasonable to expect agents to be able to resolve every issue presented to them within the target SLAs.
- There are times when tickets need to be escalated, either internally (getting help from someone else on the team) or by routing the ticket to another group (internal or external) that is more qualified to address the issue.
- There are 3 key scenarios that trigger an escalation of IT tickets:
  - User requests escalation
  - Agent identifies that they lack the skills, access, knowledge to resolve the issue
  - SLA targets are missed (auto escalation)
- Ticket escalations should be treated as hand-offs (either internal or external) and should follow a similar process.
- The agent should summarize the current status of the ticket being sure to note any observations, assumptions and missing information along with any diagnostic and/or remediation actions taken.
- This information is critical for enabling the person receiving the ticket to quickly assess the situation and continue providing support.
- Ticketing best practices suggest that escalations should be treated as a positive action when the agent identifies the need early and avoids wasting time on tickets, they know they will be unable to resolve.

Workflow Integration with other ITSM processes

Solution Development

Tickets may include feature requests and user feedback that is helpful for developers in improving the performance and usability of IT systems and services.

Change Management

- Change requests are often directly related to the events that initiate and/or resolve many IT tickets.
- Integrating change management and ticketing workflows enables better insight into the effectiveness of planned changes.

Knowledge Management

- IT ticketing is most effective when agents leverage the experience and lessons learned from previous tickets.
- Your ticketing process should include provisions for both creating and consuming knowledge articles.

System Monitoring

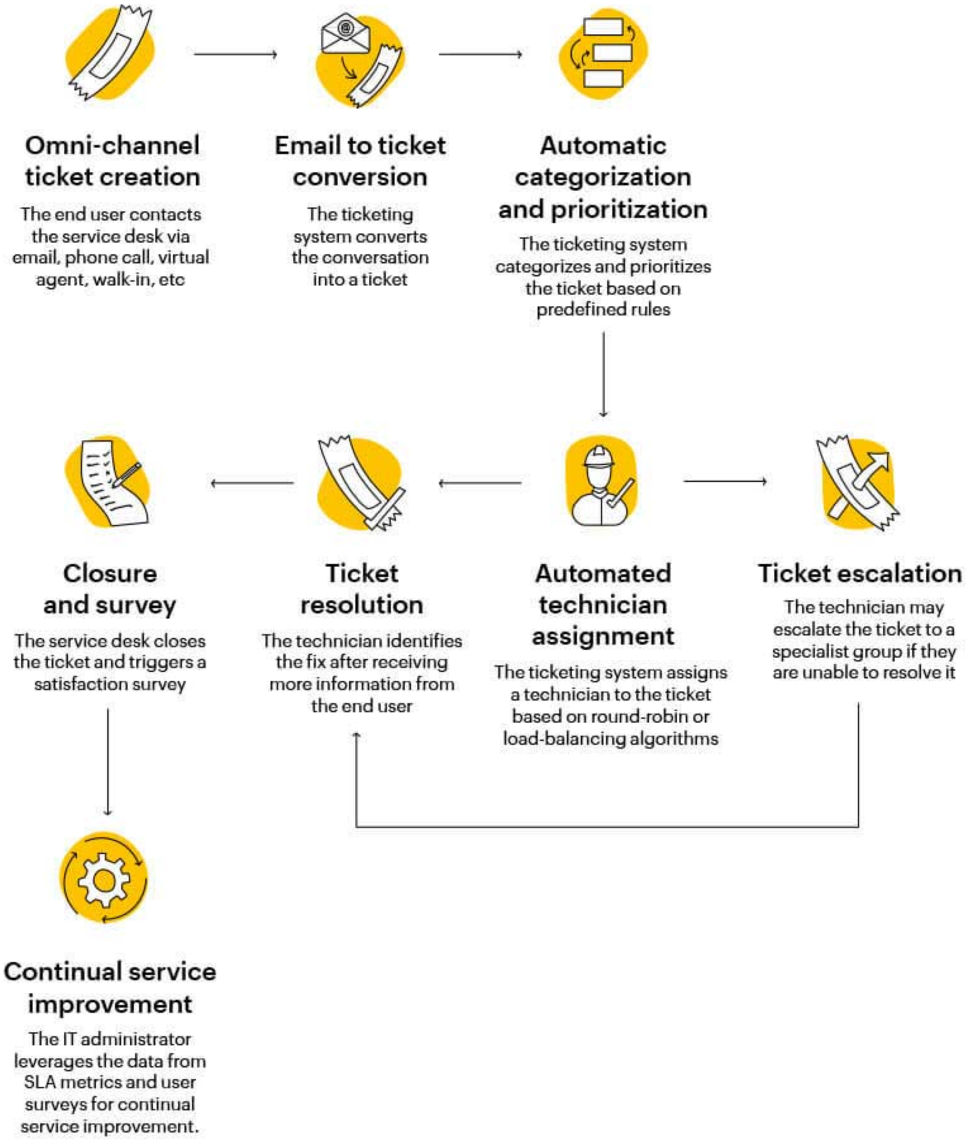
Ticketing integration with monitoring capabilities and system generated tickets is the foundation of proactive support (resolving issues before users notice an impact).

Problem Management

- IT tickets are a key source of data for identifying, diagnosing and resolving problems in your IT environment.
- Problem management is also the source of known-issue data for your IT systems.

Ticketing System Mechanism

- When converting requests into tickets, a help desk ticketing system automatically capture as much information as possible, such as the source email, phone number, and device name. This reduces the chance of errors and omissions that can easily occur with human data entry.
- It can also separate incoming tickets into more manageable categories, also known as “buckets”. Separating tickets into these buckets allows IT engineers to address tickets more efficiently, organizing them by team, priority, source, or user.
- Any number of combinations or buckets can be created so the best IT technician is assigned the right tickets at the right time. For example, you wouldn’t want your desktop team to receive tickets for server problems and vice versa.
- Assigning tickets properly makes sure you’re using all resources as efficiently as possible.
- Dividing tickets in this way can also allow you or your team to focus on higher priority tickets without the noise of less important tickets.


Omni-channel ticket creation
The end user contacts the service desk via email, phone call, virtual agent, walk-in, etc
Email to ticket conversion
The ticketing system converts the conversation into a ticket
Automatic categorization and prioritization
The ticketing system categorizes and prioritizes the ticket based on predefined rules
Automated technician assignment
The ticketing system assigns a technician to the ticket based on round-robin or load-balancing algorithms
Ticket escalation
The technician may escalate the ticket to a specialist group if they are unable to resolve it
Ticket resolution
The technician identifies the fix after receiving more information from the end user
Closure and survey
The service desk closes the ticket and triggers a satisfaction survey
Continual service improvement
The IT administrator leverages the data from SLA metrics and user surveys for continual service improvement.

Ticketing Management System

- Ticket management systems also allow you to track the status of your tickets. Knowing who is responsible for a job and how long a ticket has been sitting in the system are critical for accountability.
- A help desk ticketing system will enable you to see exactly where a ticket is in its lifecycle—whether it's new, awaiting user response, blocked, or even closed.
- Knowing how long a ticket has been in a certain status is often a trigger for action and important when considering Service Level Agreements (SLAs).
- With an IT help desk system, you can ensure the right IT technician is addressing the right ticket, allowing you to leverage your team's skillsets and resources more effectively.
- When a combination of priority and time elapsed threatens to breach the agreement, tickets that could negatively affect SLA will require immediate action be taken.
- Tracking ticket status using a help desk ticketing system allows you to calculate SLA status automatically.
- The system can notify you when an SLA breach is approaching, empowering you to set date-specific SLA reminders
- This further allows your team to focus on the most impactful work, without having to worry about manually having to prioritize tickets.

Ticketing Software

- Help desk ticket software helps you capture and organize service requests from your customers, employees, servers, networks, and more to help ensure greater end-user satisfaction and efficiency.
- IT ticketing software can provide insight into ticket status, such as who is responsible for a job and how long a ticket has been sitting in a system, as well as help with many of the tasks involved in effective ticket management, including alerting, responses to end users, and reporting.
- Who receives alerts is just as important as how they get alerted. A properly configured ticketing system only needs to alert the technicians that need to be alerted.
- For example, when a new ticket arrives and hasn't been responded to, a ticketing system can provide relevant, timely alerts to those involved without too much excess information and noise, so they have all the information they need to quickly resolve the issue.

2.2 Install Helpdesk Applications (Helpdesk and SeamlessDesk)

HelpDesk App

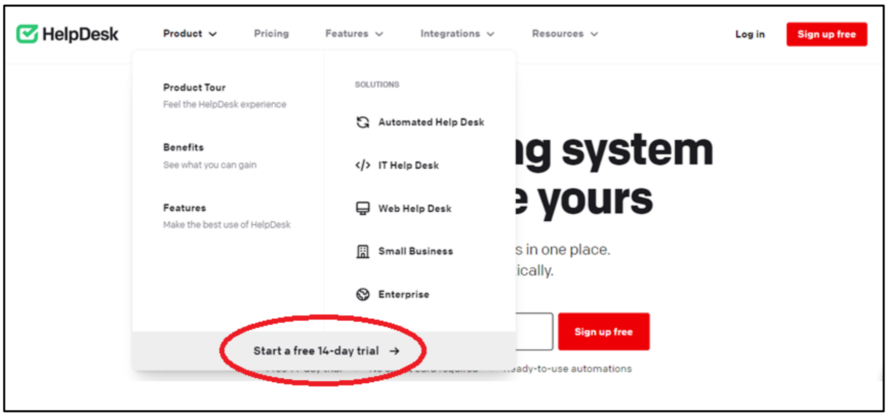
- HelpDesk Application is a ticketing system. It is a tool to manage email communication with customers.
- It works like a mailbox but has additional features designed to make customer support easier.
- When you implement HelpDesk, you get a powerful toolset that helps you organize your emails.
- At the same time, the responses you write in HelpDesk look just like regular emails, so your customers don't see any difference.

HelpDesk Features

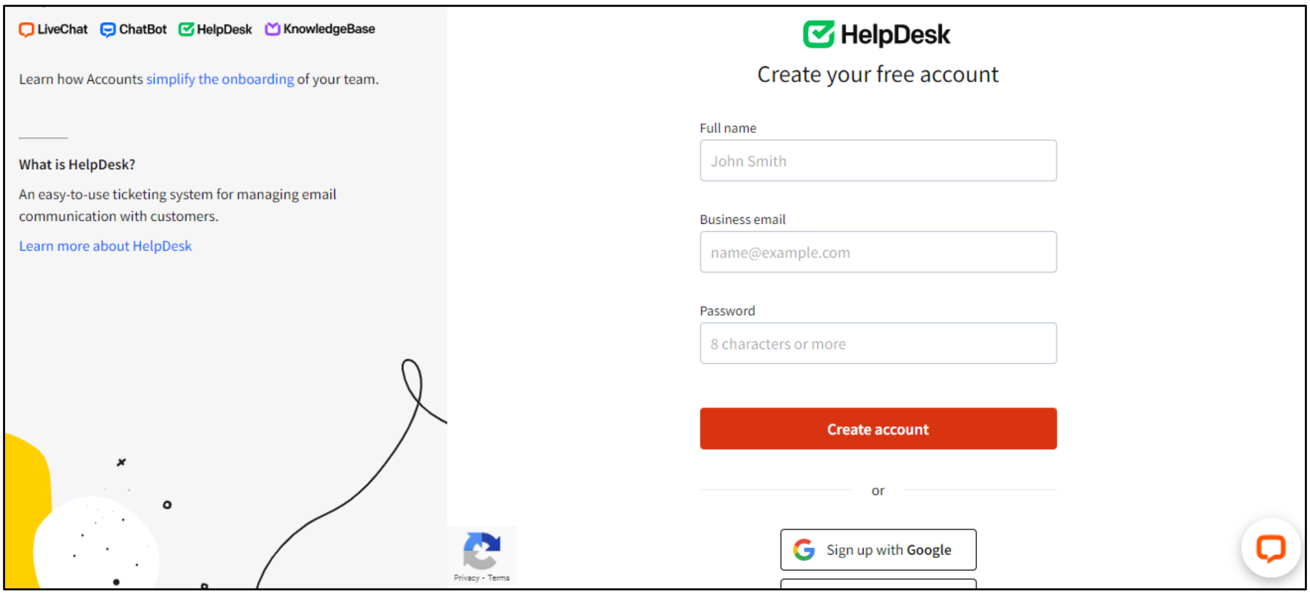
- Canned responses that allow you to prepare answers and use them later
- Statuses that help you identify which tickets need your attention
- Private notes that make it easier to talk to your teammates within the app
- Filters and tags that help you with organizing your tickets
- Teams that allow you to group your agents according to specific roles

Setup Account in HelpDesk App

Sign-up Process



- To install the application visit https://www.helpdesk.com/



Learn how Accounts simplify the onboarding of your team.

What is HelpDesk?

An easy-to-use ticketing system for managing email communication with customers.

Learn more about HelpDesk

HelpDesk

Create your free account

Full name

John Smith

Business email

name@example.com

Password

8 characters or more

- The sign-up process in HelpDesk is fast and easy. You can create an account using your email address or sign up with Google.

- **Sign up with email**
  4. Go to the sign-up page.
  5. Enter your business email, full name, and password.
  6. Click "Continue".

- **Sign up with Google**
  1. Go to the sign-up page.
  2. Click the "Sign up with Google" button.
  3. Choose your Google account.
  4. Complete the sign-up process via Google.

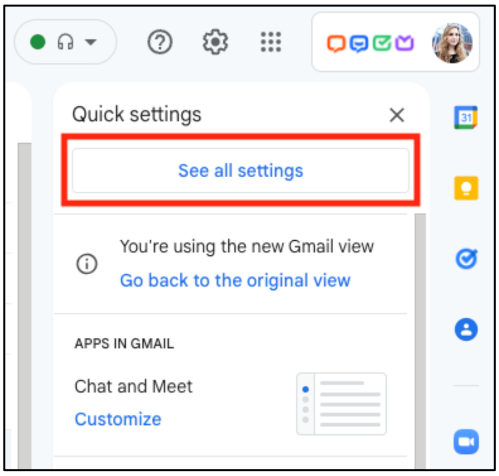
Sign up Email Forwarding

- To transfer all the messages to HelpDesk, set up forwarding or redirection rule in your current email client or directly from your own server.

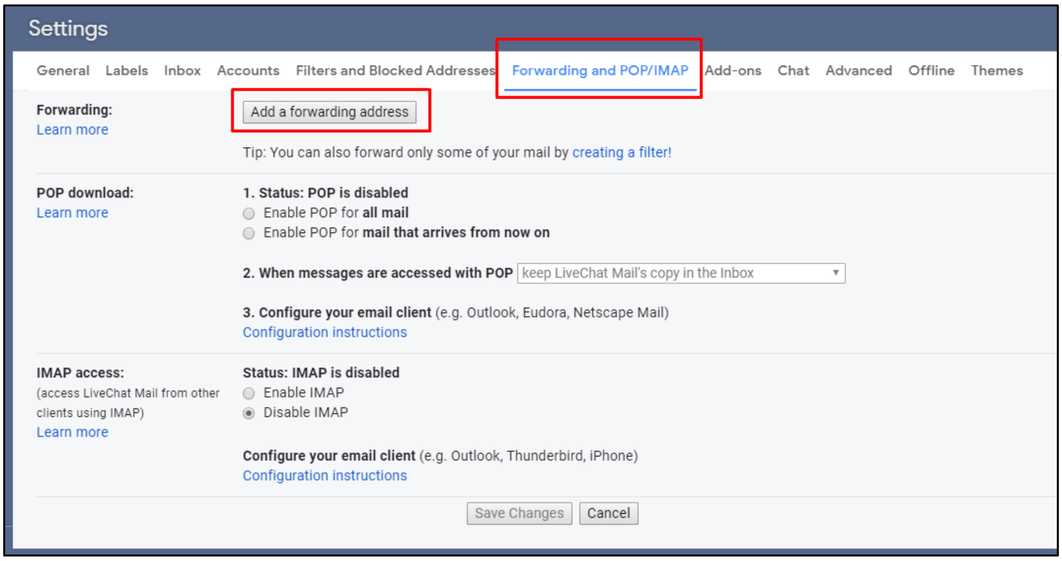
- This way, the emails that your customers send to your mailbox will be forwarded to HelpDesk as tickets.
- To keep and manage your entire email communication with customers in HelpDesk, you should set up email forwarding in your current email client (or your server).

<u>Sign up Email Forwarding in Gmail</u>

1. Open the Gmail application and click the gear icon in your inbox. Choose “See all settings.”



2. Choose the “Forwarding and POP/IMAP” tab.
3. Click “Add a forwarding address.”



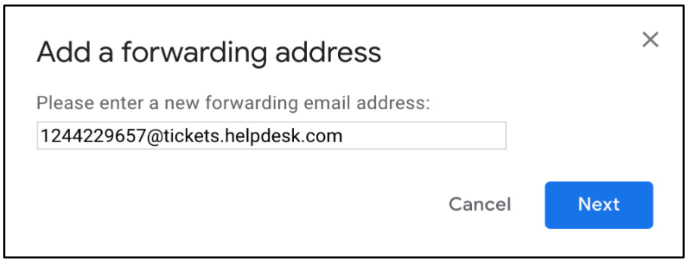
Forwarding: Learn more
Add a forwarding address
Tip: You can also forward only some of your mail by creating a filter!

POP download: Learn more
1. Status: POP is disabled
○ Enable POP for **all mail**
○ Enable POP for **mail that arrives from now on**
2. When messages are accessed with POP keep LiveChat Mail's copy in the Inbox
3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
Configuration instructions

IMAP access: (access LiveChat Mail from other clients using IMAP) Learn more
Status: IMAP is disabled
○ Enable IMAP
● Disable IMAP
Configure your email client (e.g. Outlook, Thunderbird, iPhone)
Configuration instructions

Save Changes Cancel

4. Enter your dedicated HelpDesk email address, which you can find in HelpDesk Settings > Email addresses. Click “Next,” and “Proceed.”



Add a forwarding address

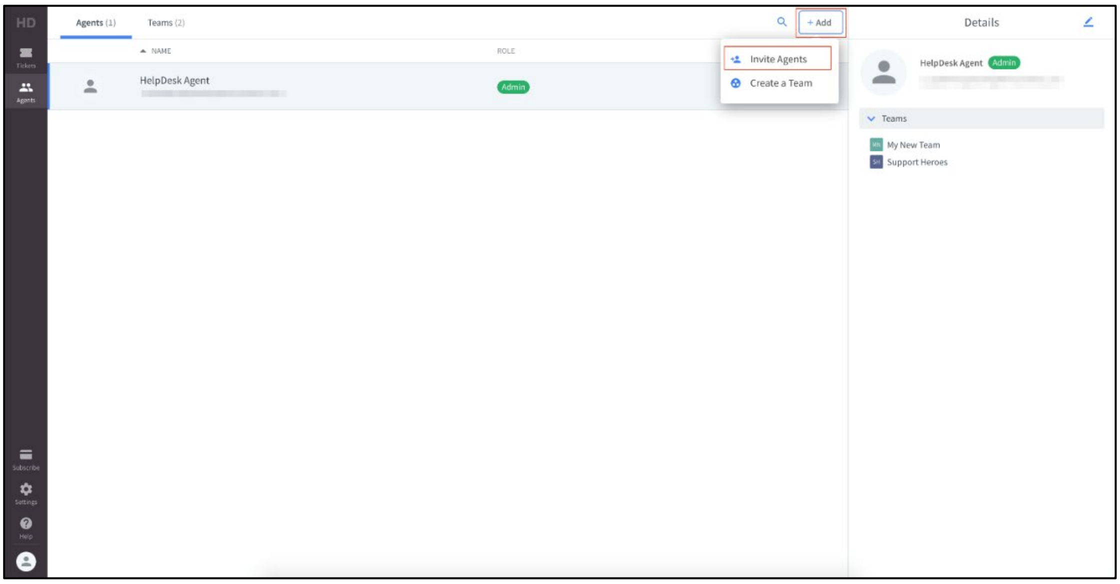
Please enter a new forwarding email address:

1244229657@tickets.helpdesk.com

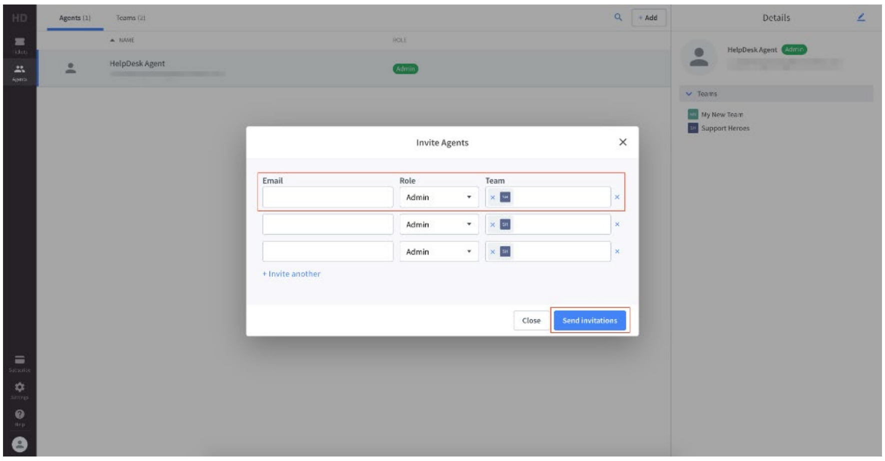
5. Check your HelpDesk dashboard — you'll then receive a message with a verification.
6. Enter the verification code in the Gmail settings and click "Verify."
7. Select "Forward a copy of incoming mail to "yourlicencenumber@tickets.helpdesk.com." Choose what to do with the forwarded messages: Keep them in your Gmail Inbox, mark them as "read," archive, or delete them.
8. Click "Save Changes." To learn more, visit the official Google support page.

Add New Agents to HelpDesk

- Agents are members of your organization who have access to your HelpDesk.
- The last step is to invite your teammates/agents. This way, you'll be able to work on your HelpDesk tickets together.
- You can add as many Agents as you need. HelpDesk has tools that support teamwork, therefore solving customers' issues and answering their questions is effortless.
- You don't have to leave the application to collaborate with your team.
- New agents can be added by admins. Here's how to invite your teammates to join you on HelpDesk via email.
  1. Go to Agents.
  2. Click "+Add" in the upper-right corner and click "Invite agents".



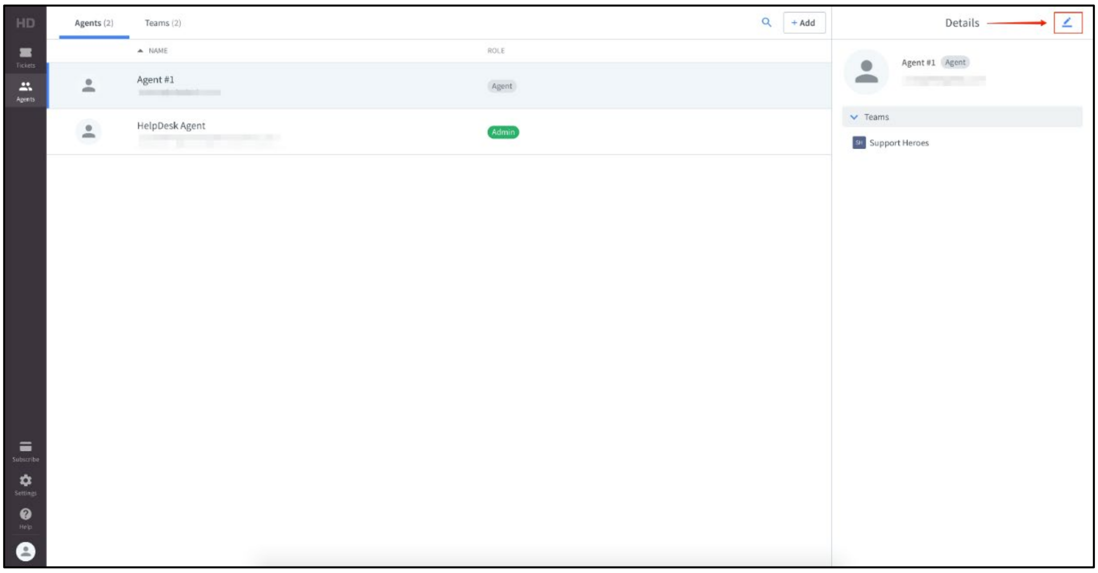
  3. Enter your teammate's email (an invitation link will be sent to this email address).



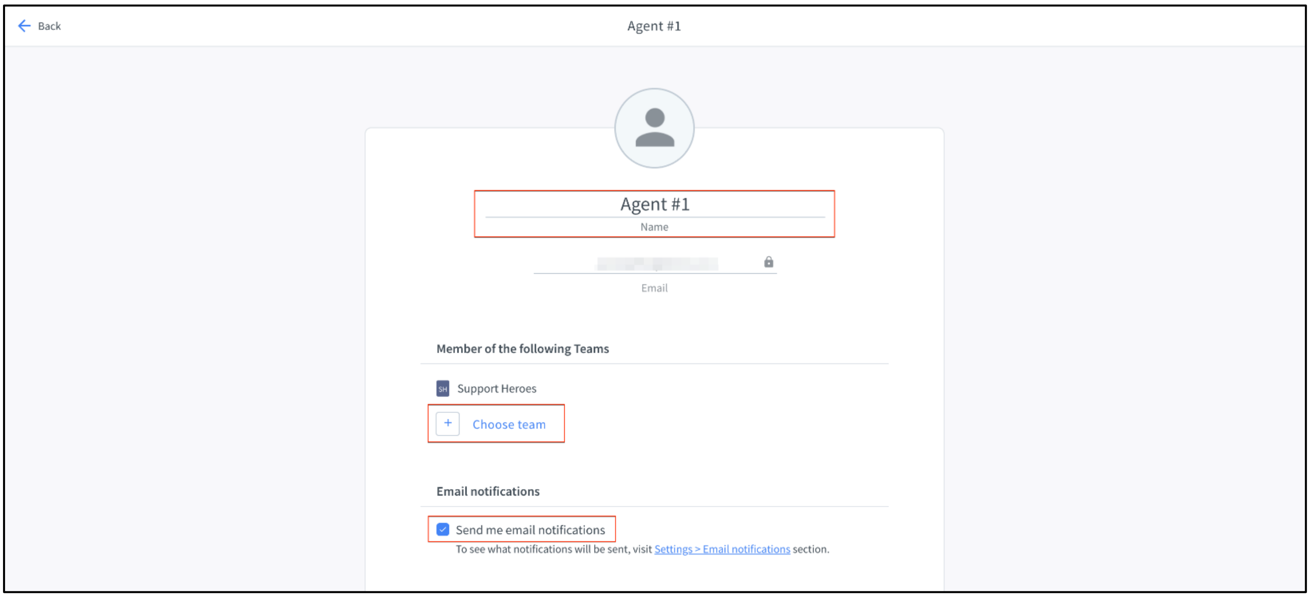
4. Assign them to a team (optional, if you have more than one Team).
5. Click “Send invitations”.
6. Your teammate(s) will receive an invitation email with a verification link. This link redirects to a login page where the Agent can choose a password and sign in.

Edit or Delete Agent Accounts

- Agents can customize their accounts in Settings. However, if it’s necessary the account settings can be edited by admins.
- To edit agent’s profile, go to the Agents section. Then, select an Agent from the list and click the edit icon in the upper-right corner.



- You can change the following settings:
  - **Name –** change the agent’s display name
  - **Teams –** assign the agent to teams
  - **Email notifications –** enable or disable email notifications



Agent #1
Name

Email

Member of the following Teams

Support Heroes

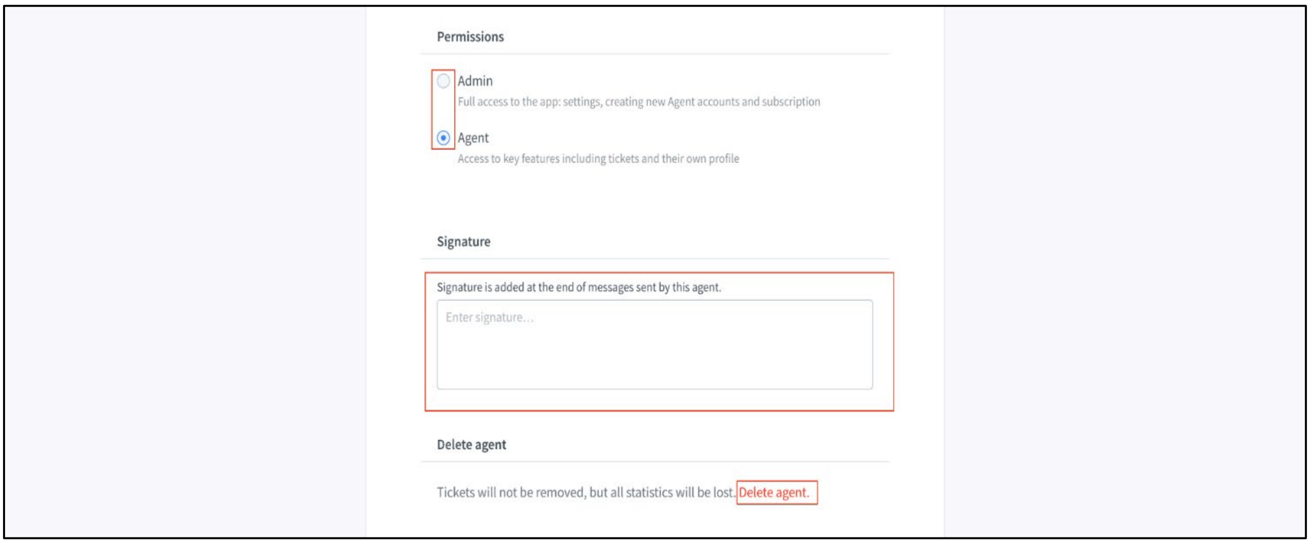
+ Choose team

Email notifications

☑ Send me email notifications
To see what notifications will be sent, visit Settings > Email notifications section.

- **Permissions –** change agent’s role to admin to give them access to advanced settings (billing, inviting other agents)
- **Signature –** a signature will be added at the bottom of agent’s messages
- **Delete agent –** delete the Agent’s account

When you apply the necessary changes, click “Save changes”.



Permissions

○ Admin
Full access to the app: settings, creating new Agent accounts and subscription

● Agent
Access to key features including tickets and their own profile

Signature

Signature is added at the end of messages sent by this agent.

Enter signature...

Delete agent

Tickets will not be removed, but all statistics will be lost. Delete agent.

After completing these three steps, you and your team are ready to solve tickets from your customers in HelpDesk.

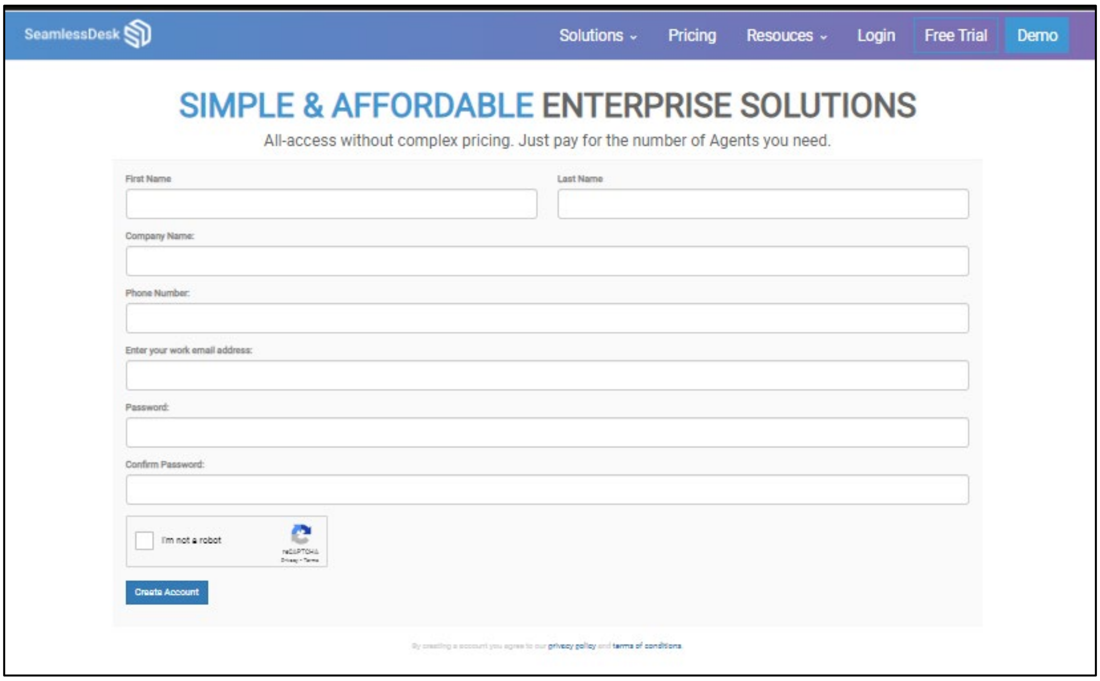
SeamlessDesk

Features

- Quickly and efficiently collaborate with your team and respond to tickets using a build-in rich text editor.
- View and update ticket requestor, status, priority, and Agent assignments.
- View details about the requestor, requestor history, assigned assets, and asset history.
- View past due or upcoming SLA deadlines.
- Create to-dos, reminders, and add notes.
- Unlimited custom ticket fields, enabling you to adapt the product to fit the needs of the business—regardless of your use case or industry.
- Agents can easily create and log tickets in the Help Desk module, which are useful when support requests come via phone calls.
- Tickets can be generated via email.
- Tickets can be created via the SeamlessDesk mobile app or social media platforms.
- Grant access to a self-service portal where end-users can view your Knowledge Base, submit new tickets, and view previously submitted ticket status.

Setup

1. Visit https://www.seamlessdesk.com/
2. Click on free trail and sign up.



SIMPLE & AFFORDABLE ENTERPRISE SOLUTIONS

All-access without complex pricing. Just pay for the number of Agents you need.

First Name

Last Name

Company Name:

Phone Number:

Enter your work email address:

Password:

Confirm Password:

□ I'm not a robot

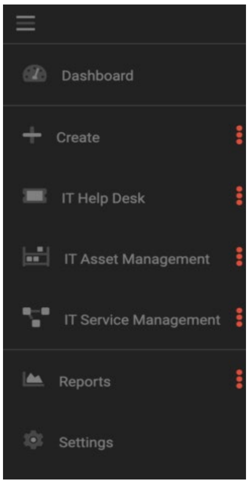
reCAPTCHA
Privacy - Terms

Create Account

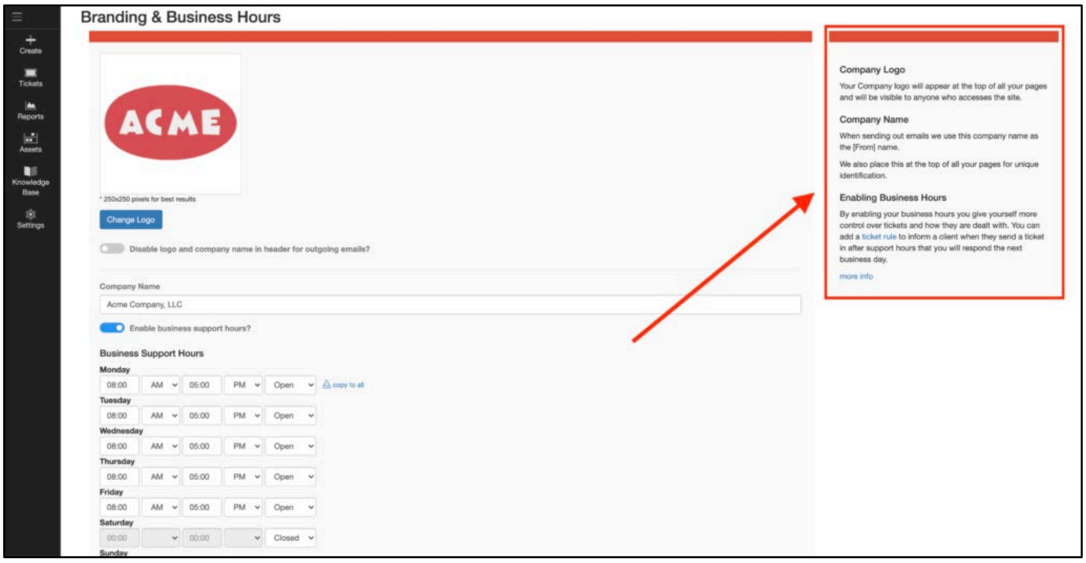
By creating a account you agree to our privacy policy and terms of conditions.

3. Once you sign up for a Seamless Desk account, an access code and link will be sent to the email that you used when you signed up.
4. Click the provided link, fill in all of the required fields, and sign in to your account.
5. You are now signed in and ready to start configuring your account.

- Once you are logged in, you are ready to begin configuring your account and settings. Here are a few helpful tips about how to navigate around your account.
- A navigation panel is there on the left side of screen to provide you quick access to the most commonly used tools.
- IT Help Desk modules, IT Asset Management Modules, IT Service Management models, and more can all be found here.



- In the top right-hand corner, you will find the account toolbar.
- Here you can perform quick searches, see your notifications, view your personal inbox, access your profile and profile settings, make changes to your account, and change your language.



Branding & Business Hours

* 250x250 pixels for best results

Change Logo

Disable logo and company name in header for outgoing emails?

Company Name

Acme Company, LLC

Enable business support hours?

Business Support Hours

Monday 08:00 AM 05:00 PM Open copy to all

Tuesday 08:00 AM 05:00 PM Open

Wednesday 08:00 AM 05:00 PM Open

Thursday 08:00 AM 05:00 PM Open

Friday 08:00 AM 05:00 PM Open

Saturday 00:00 00:00 Closed

Sunday

Company Logo

Your Company logo will appear at the top of all your pages and will be visible to anyone who accesses the site.

Company Name

When sending out emails we use this company name as the [From] name.

We also place this at the top of all your pages for unique identification.

Enabling Business Hours

By enabling your business hours you give yourself more control over tickets and how they are dealt with. You can add a ticket rule to inform a client when they send a ticket in after support hours that you will respond the next business day.

more info

2.3 Generate Ticket (Helpdesk and SeamlessDesk)

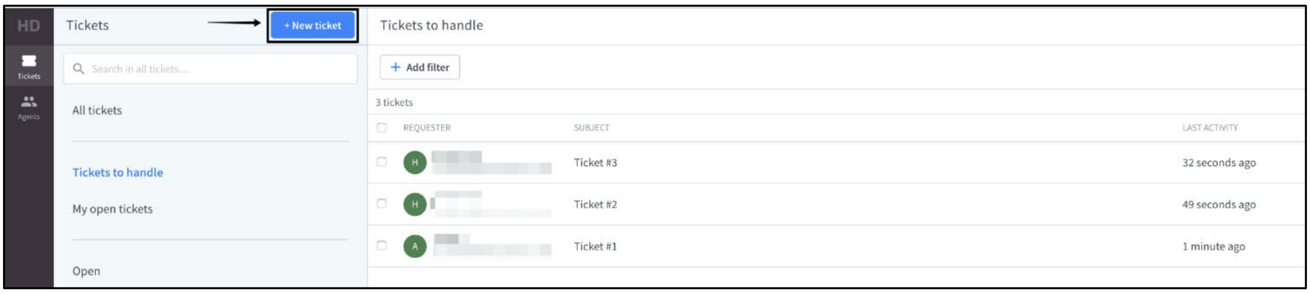
Generate Ticket - Helpdesk

How to collaborate with your team in HelpDesk?

- To see the maximum benefits of using HelpDesk, invite your team to join you and start working together on your customer support projects.
- You can assign one of three roles to your team members: Admin, Agent, or Viewer.

Create a Ticket

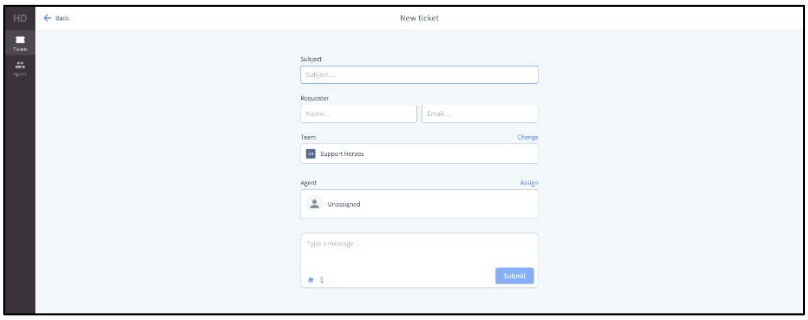
- If your customer reaches out to you using a different channel than email (e.g. phone), you can create a ticket to continue the conversation via email.
- To create a ticket, click the "+ New ticket" button in the Ticket dashboard in the Tickets section.



3 tickets

□	REQUESTER	SUBJECT	LAST ACTIVITY
□	H [redacted]	Ticket #3	32 seconds ago
□	H [redacted]	Ticket #2	49 seconds ago
□	A [redacted]	Ticket #1	1 minute ago

- This is the “New ticket” view:

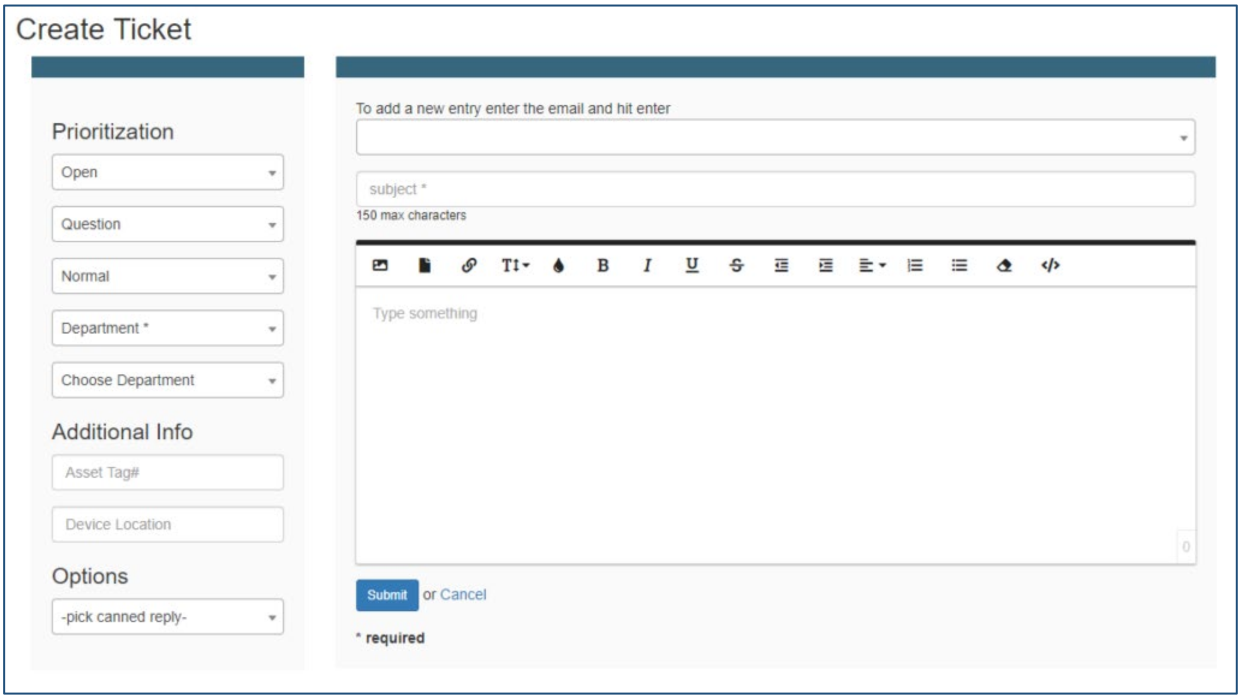


- Enter the following details:
  - ➢ Subject
  - ➢ Requester’s name
  - ➢ Requester’s Email
  - ➢ Assignee
  - ➢ Team
- Write your message
- Click “Send” (the message will be sent to the Requester’s email address)

Generate Ticket – SeamlessDesk

Create a Ticket

- When you are logged in to SeamlessDesk, you will see a panel to the left of your screen.
- Click on the plus sign labeled “Create.”
- You are now on the ticket creation page.



Create Ticket

Prioritization

Open

Question

Normal

Department *

Choose Department

Additional Info

Asset Tag#

Device Location

Options

-pick canned reply-

To add a new entry enter the email and hit enter

subject *

150 max characters

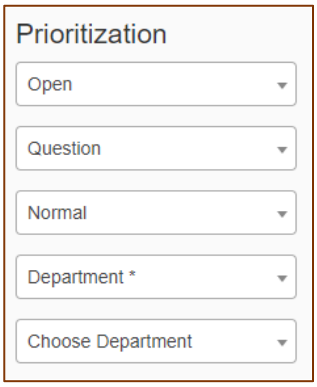
Type something

Submit or Cancel

* required

Prioritization

- Here is where you can specify the priority of the ticket.
- Options like whether or not the ticket is urgent, what department should the ticket be assigned to, and whether an individual agent needs to be assigned can be added here.



Prioritization

Open

Question

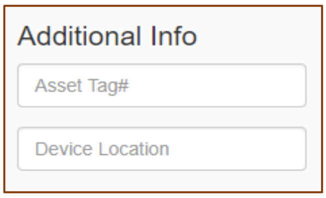
Normal

Department *

Choose Department

Additional Info

- You may or may not see this section. In order for this section to appear, a SeamlessDesk Admin would have needed to create custom ticket fields.
- These are additional fields of information that can be entered into a ticket and may even be required.



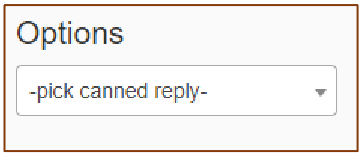
Additional Info

Asset Tag#

Device Location

Options

- In options, you can see things like Canned Replies or even Ticket templates.
- In this example, the Options section provides for Canned Replies so that Agents can answer commonly asked questions.

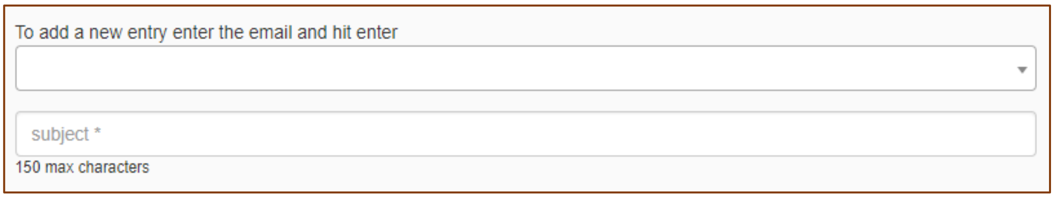


Options

-pick canned reply-

Ticket Recipient and Subject Line

- First, you need to specify a user to send the ticket to.
- In the drop-down, you will see a list of current users and their emails if they are within your organization.
- You can also add an email not currently registered in the system by typing it in and then hitting return on your keyboard.



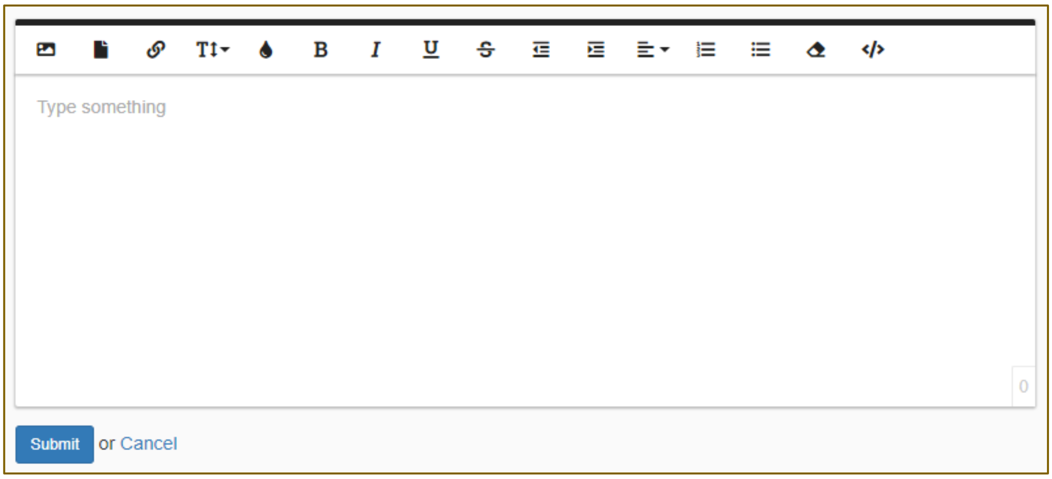
To add a new entry enter the email and hit enter

subject *

150 max characters

Ticket Body

- In the body, we provide an editor that allows the input of HTML.
- This will enable you to respond via plain text, or you can add custom HTML elements.



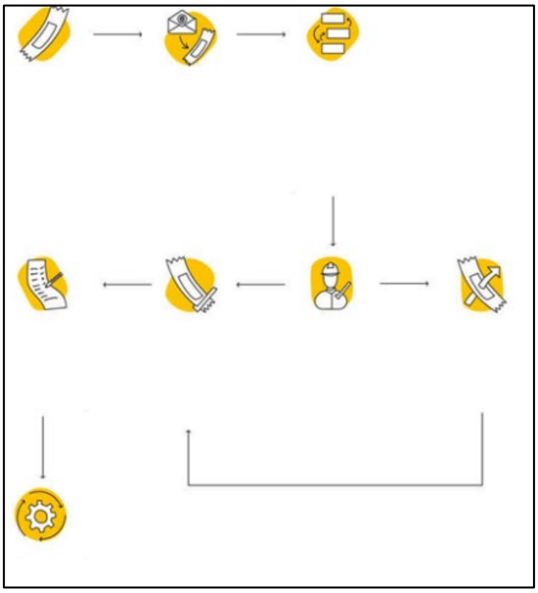
Type something

- Once you have completed your ticket simply his Send and you are done.
- Agents would use this option to create tickets if they were contacted outside of SeamlessDesk to resolve an issue or fix a problem.

An example of this could be someone calling into the office to report an issue, sending a text message, or any other way of notifying the team of an issue. Once users' issues have been identified, Agents can create tickets with the details included so that they can better track the issue and drive it to a successful resolution.

Section 3: Exercises

Exercise 1: Fill the details in following Ticketing System Mechanism.



Exercise 2: Participate in group discussion on following topics:

a) Importance and Benefits of IT Tickets
b) Types of IT Tickets
c) Ticket Sources and Classification
d) Route, Manage, Escalate the IT Tickets
e) Ticketing System Mechanism and Software

Section 4: Assessment Questionnaire

1. ________ is the generalized term used to refer to a record of work performed (or needing to be performed) by your IT support organization to operate your company's technology environment, fix issues and resolve user requests.
2. What are the Ticket Types?
3. _______ are indicators that something might have happened in your IT environment or that something is operating outside of pre-defined performance thresholds.
4. When an IT ticket is generated?
5. What are the types of Ticket Sources?
6. What are four key pieces of classification data that IT tickets should include?
7. What are three common routing scenarios for IT tickets that your support agents should be familiar with?
8. What are seven key factors for prioritizing tickets in support queues?
9. ____________ are a measurement tool for evaluating ticket handling performance against a pre-defined set of criteria.
10. Response Time SLA is the total elapsed time from ticket creation until it is set to a resolved state indicating the issue has been fully addressed. (True/False)
11. What are the three key scenarios that trigger an escalation of IT tickets?
12. Ticketing System Mechanism can also separate incoming tickets into more manageable categories, also known as:

----------End of the Module----------

MODULE 3

Virtualization

Section 1: Learning Outcomes

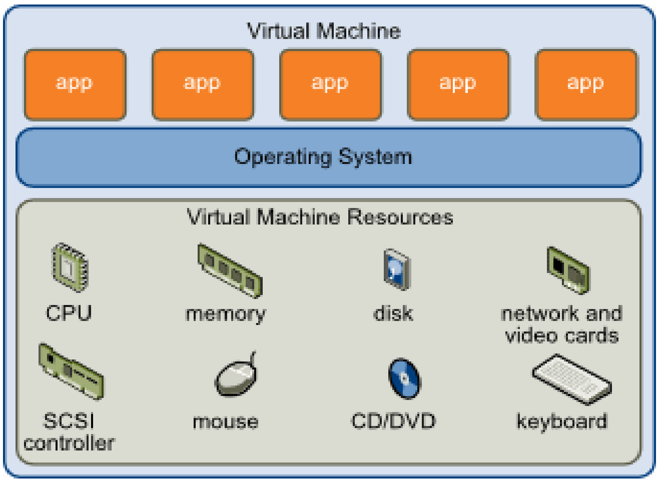
After completing this module, you will be able to:

- Explain Types, Advantage and Disadvantages of Virtual Machine
- Differentiate between Container and Virtual Machine
- Describe Benefits, Types and Need of Virtualization
- Explain VirtualBox Terminologies and Features
- Deploy a Virtual Machine
- Create and Run the Virtual Machine
- Explain Types and Applications of NAS
- Install and Configure TrueNAS

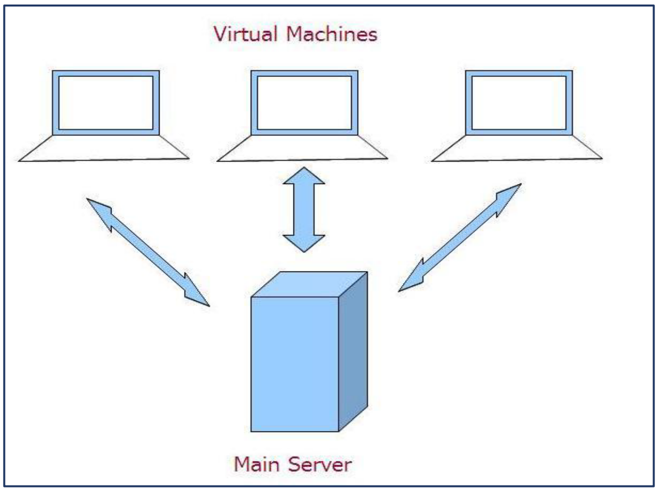
Section 2: Relevant Knowledge

3.1 What is a Virtual Machine?

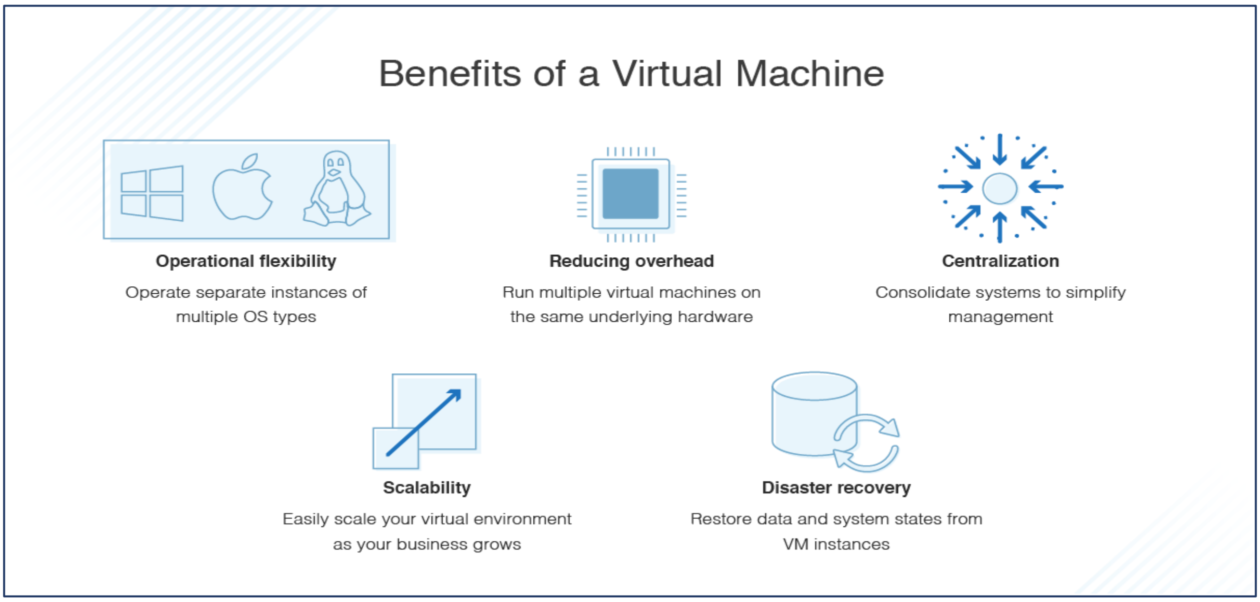
5. A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps.
6. One or more virtual “guest” machines run on a physical “host” machine.
7. Each virtual machine runs its own.
8. Operating system and functions separately from the other VMs, even when they are all running on the same host. This means that, for example, a virtual MacOS virtual machine can run on a physical PC.



- Virtual machine technology is used for many use cases across on-premises and cloud environments.
- More recently, public cloud services are using virtual machines to provide virtual application resources to multiple users at once, for even more cost efficient and flexible compute.



- Virtual machines (VMs) allow a business to run an operating system that behaves like a completely separate computer in an app window on a desktop.
- VMs may be deployed to accommodate different levels of processing power needs, to run software that requires a different operating system, or to test applications in a safe, sandboxed environment.



Benefits of a Virtual Machine

Operational flexibility
Operate separate instances of multiple OS types

Reducing overhead
Run multiple virtual machines on the same underlying hardware

Centralization
Consolidate systems to simplify management

Scalability
Easily scale your virtual environment as your business grows

Disaster recovery
Restore data and system states from VM instances

- Virtual machines have historically been used for server virtualization, which enables IT teams to consolidate their computing resources and improve efficiency.
- Additionally, virtual machines can perform specific tasks considered too risky to carry out in a host environment, such as accessing virus-infected data or testing operating systems.
- Since the virtual machine is separated from the rest of the system, the software inside the virtual machine cannot tamper with the host computer.

How do Virtual Machines Work?

- The virtual machine runs as a process in an application window, similar to any other application, on the operating system of the physical machine
- Key files that make up a virtual machine include a log file, NVRAM setting file, virtual disk file and configuration file.

Advantages of Virtual Machines

Virtual machines are easy to manage and maintain, and they offer several advantages over physical machines:

- VMs can run multiple operating system environments on a single physical computer, saving physical space, time and management costs.
- Virtual machines support legacy applications, reducing the cost of migrating to a new operating system. For example, a Linux virtual machine running a distribution of Linux as the guest operating system can exist on a host server that is running a non-Linux operating system, such as Windows.
- VMs can also provide integrated disaster recovery and application provisioning options.

Flexibility

- Snapshots can be created to travel back and forward in virtual machine time
- Run multiple operating systems (OS) and applications on one physical machine at the same time.
- Independent of hardware or software underneath the VM» Run legacy applications without having to changes current OS settings.

Scalability

- Multiple VMs can reside on one physical machine.

Portability

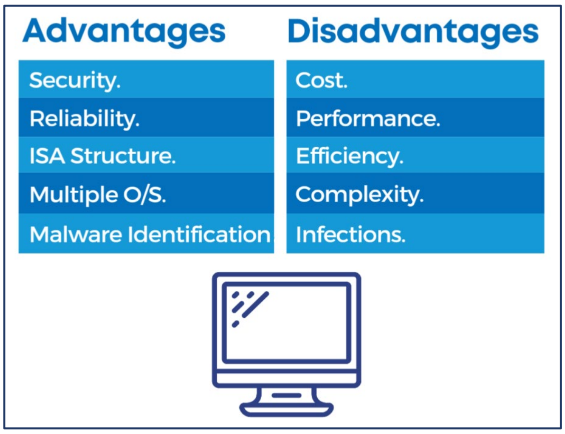
- Easily transported from one machine to another

Cost

- Less expensive than buying multiple machines (less hardware to purchase)
- Less power/electricity than having more physical machines
- Save time testing new software without it affecting your current configurations

Disadvantages of Virtual Machines

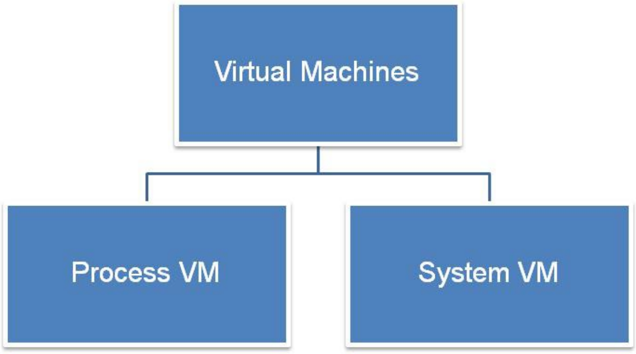
- While virtual machines have several advantages over physical machines, there are also some potential disadvantages:
- Running multiple virtual machines on one physical machine can result in unstable performance if infrastructure requirements are not met.
- Virtual machines are less efficient and run slower than a full physical computer.
- Most enterprises use a combination of physical and virtual infrastructure to balance the corresponding advantages and disadvantages.



Advantages	Disadvantages
Security.	Cost.
Reliability.	Performance.
ISA Structure.	Efficiency.
Multiple O/S.	Complexity.
Malware Identification	Infections.

Types of Virtual Machines

- Users can choose from two different types of virtual machines:



Process Virtual Machine

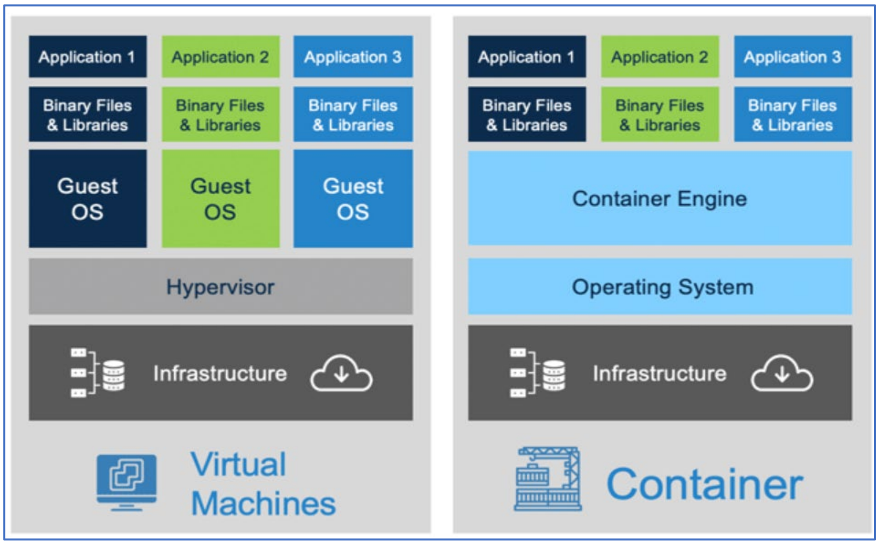
- A process virtual machine allows a single process to run as an application on a host machine, providing a platform-independent programming environment by masking the information of the underlying hardware or operating system.
- An example of a process VM is the Java Virtual Machine, which enables any operating system to run Java applications as if they were native to that system.

System Virtual Machine

- A system virtual machine is fully virtualized to substitute for a physical machine.
- A system platform supports the sharing of a host computer's physical resources between multiple virtual machines, each running its own copy of the operating system.

Container vs Virtual Machine

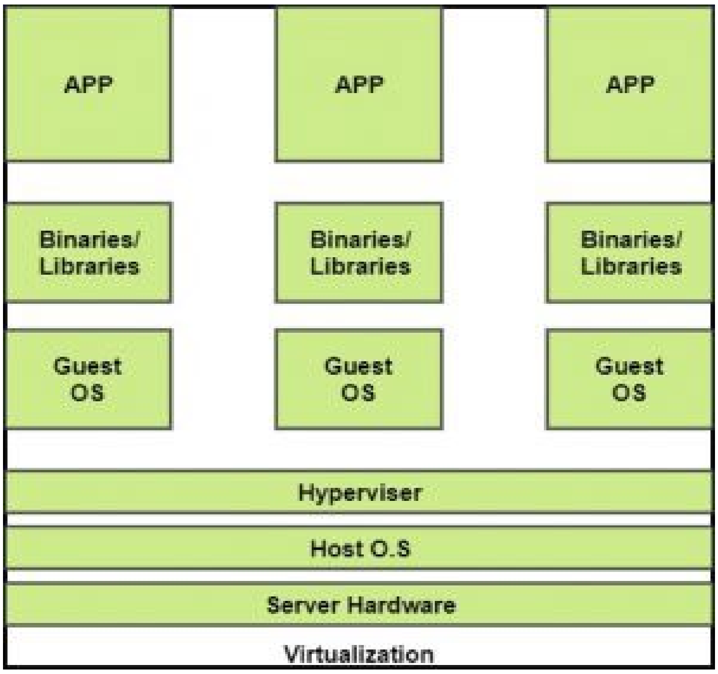
- Like virtual machines, container technology such as Kubernetes is similar in the sense of running isolated applications on a single platform.
- While virtual machines virtualize the hardware layer to create a "computer," containers package up just a single app along with its dependencies.
- Virtual machines are often managed by a hypervisor, whereas container systems provide shared operating system services from the underlying host and isolate the applications using virtual-memory hardware.



- Virtual machines are larger and slower to boot than containers.
- They are logically isolated from one another, with their own operating system kernel, and offer the benefits of a completely separate operating system.
- Virtual machines are best for running multiple applications together, monolithic applications, isolation between apps, and for legacy apps running on older operating systems.
- Containers and virtual machines may also be used together.

3.2 Virtualization

- Virtualization is a technique of how to separate a service from the underlying physical delivery of that service
- It is the process of creating a virtual version of something like computer hardware.
- It was initially developed during the mainframe era.
- It involves use of specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource.
- With the help of Virtualization, multiple operating systems and applications can run on same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.
- It is cost effective, hardware reducing, and energy saving techniques used by cloud providers is virtualization.
- Virtualization allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time.
- It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand.
- The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing.
- Virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.



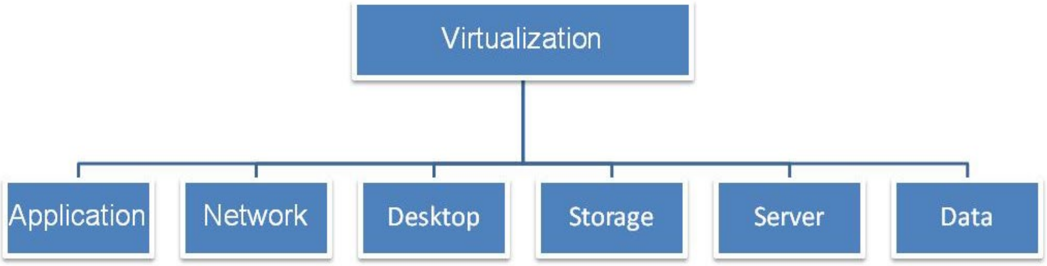
- The machine on which the virtual machine is going to be built is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**.

Benefits of Virtualization

- More flexible and efficient allocation of resources
- Enhance development productivity
- It lowers the cost of IT infrastructure
- Remote access and rapid scalability
- High availability and disaster recovery
- Pay peruse of the IT infrastructure on demand
- Enables running multiple operating systems

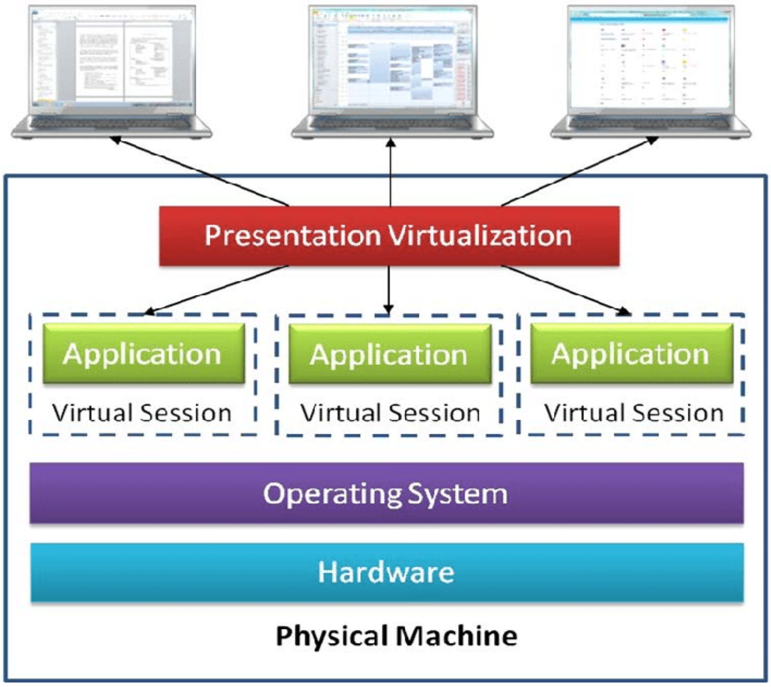
Types of Virtualizations

There are six types of Virtualizations.



Application Virtualization

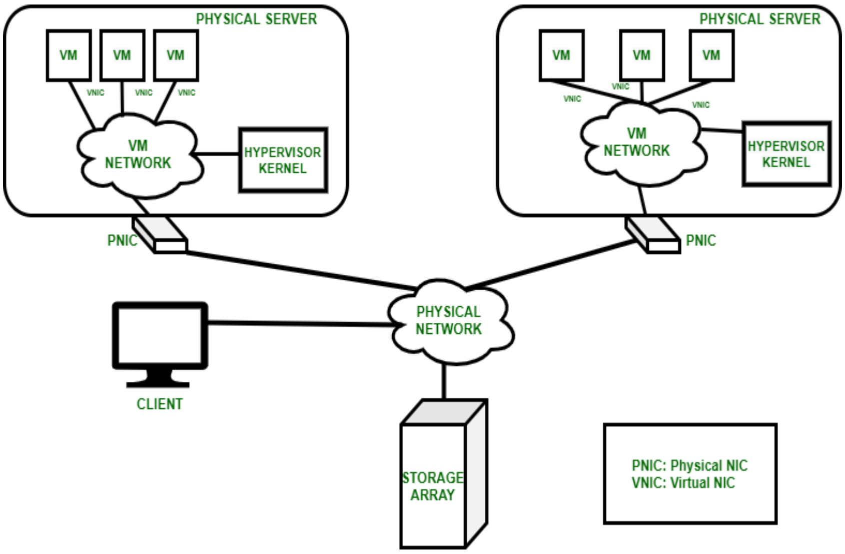
- Application virtualization helps a user to have remote access of an application from a server.
- The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet.
- Example of this would be a user who needs to run two different versions of the same software.
- Technologies that use application virtualization are hosted applications and packaged applications.



Network Virtualization

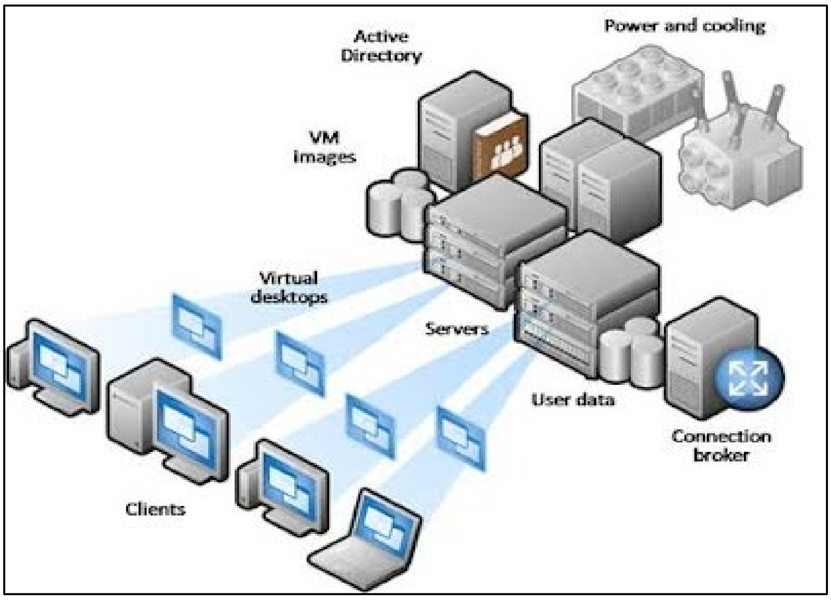
- The ability to run multiple virtual networks with each has a separate control and data plan.

- It co-exists together on top of one physical network. It can be managed by individual parties that potentially confidential to each other.
- Network virtualization provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.



Desktop Virtualization

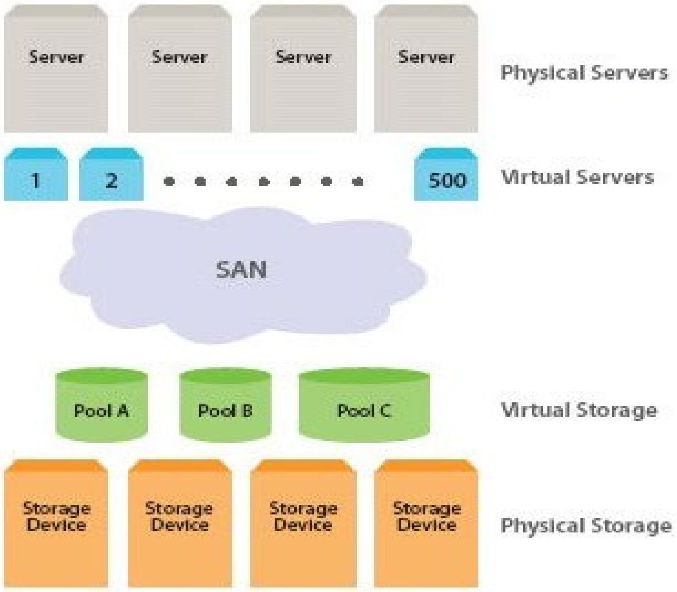
- Desktop virtualization allows the users' OS to be remotely stored on a server in the data centre.
- It allows the user to access their desktop virtually, from any location by a different machine.
- Users who want specific operating systems other than Windows Server will need to have a virtual desktop.
- Main benefits of desktop virtualization are user mobility, portability, easy management of software installation, updates, and patches.



Storage Virtualization

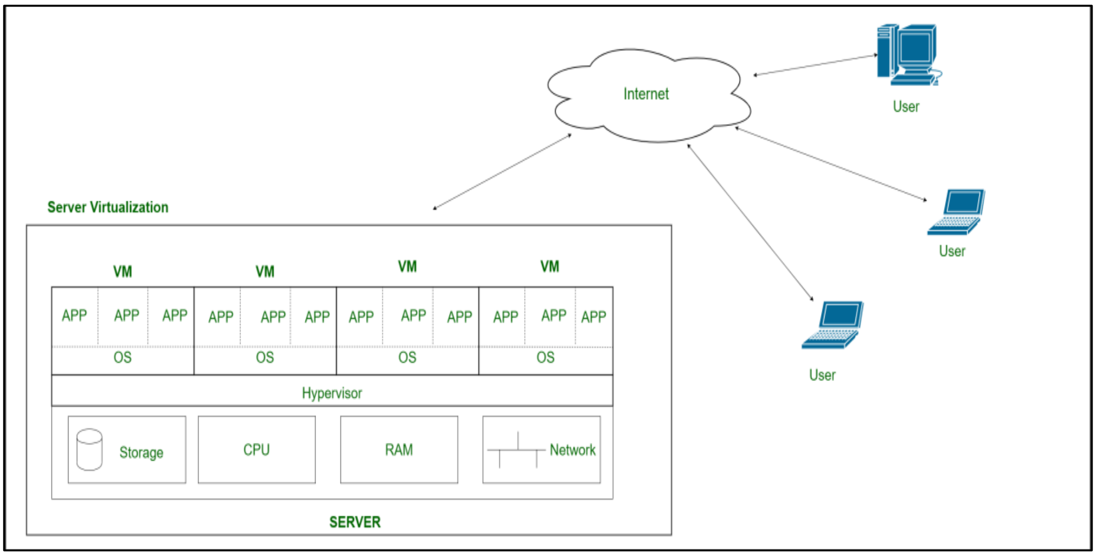
- Storage virtualization is an array of servers that are managed by a virtual storage system.
- The servers aren't aware of exactly where their data is stored, and instead function more like worker bees in a hive.
- It makes managing storage from multiple sources to be managed and utilized as a single repository.

- Storage virtualization software maintains smooth operations, consistent performance and a continuous suite of advanced functions despite changes, break down and differences in the underlying equipment.



Server Virtualization

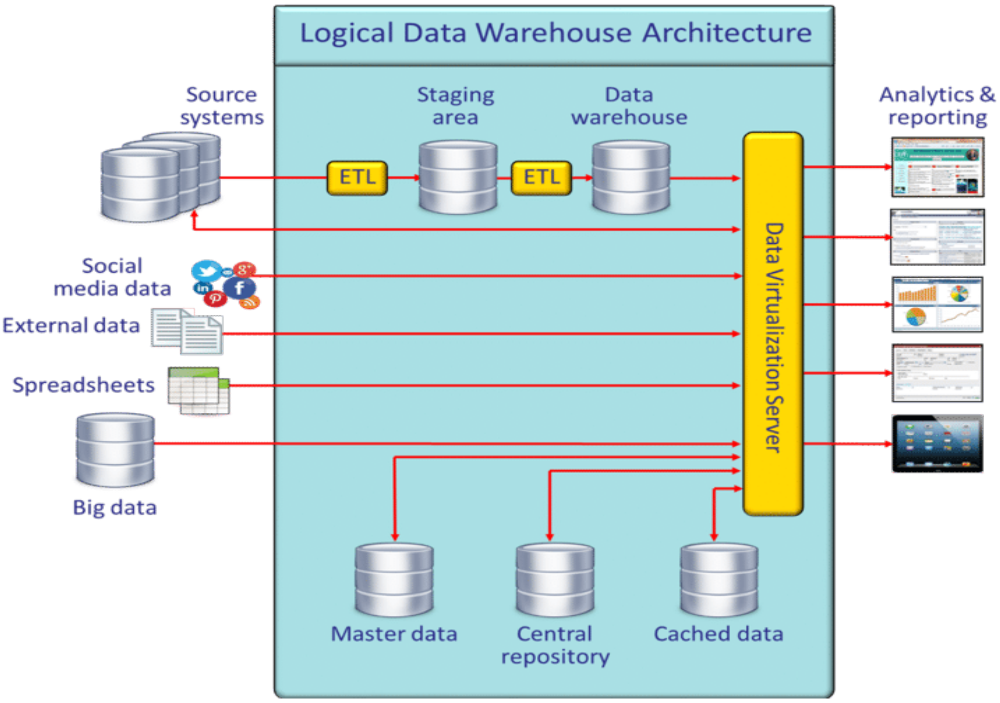
- This is a kind of virtualization in which masking of server resources takes place.
- The central-server (physical server) is divided into multiple different virtual servers by changing the identity number, processors.
- Each system can operate its own operating systems in isolate manner. Where each sub-server knows the identity of the central server.
- It causes an increase in the performance and reduces the operating cost by the deployment of main server resources into a sub-server resource.
- It’s beneficial in virtual migration, reduce energy consumption, reduce infrastructural cost, etc.



Data Virtualization

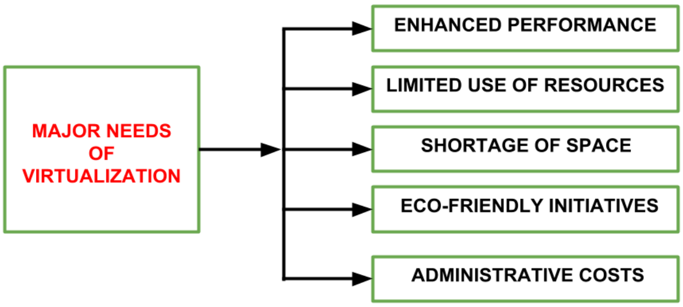
- In this virtualization, data is collected from various sources and managed at a single place without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely.

- Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata, etc.
- It can be used to performing various kind of tasks such as:
  - ➢ Data-integration
  - ➢ Business-integration
  - ➢ Service-oriented architecture data-services
  - ➢ Searching organizational data



3.3 Need of Virtualization

- There are five major needs of virtualization which are described below:



1. Enhanced Performance

- Currently, the end user system i.e. PC is sufficiently powerful to fulfill all the basic computation requirements of the user, with various additional capabilities which are rarely used by the user.
- Most of their systems have sufficient resources which can host a virtual machine manager and can perform a virtual machine with acceptable performance so far.

2. Limited Use of Hardware and Software Resources

- The limited use of the resources leads to under-utilization of hardware and software resources.
- As all the PCs of the user are sufficiently capable to fulfill their regular computational needs that's why many of their computers are used often which can be used 24/7 continuously without any interruption.

- The efficiency of IT infrastructure could be increase by using these resources after hours for other purposes.
- This environment is possible to attain with the help of Virtualization.

3. Shortage of Space

- The regular requirement for additional capacity, whether memory storage or compute power, leads data centers raise rapidly. Companies like Google, Microsoft and Amazon develop their infrastructure by building data centers as per their needs.
- Mostly, enterprises unable to pay to build any other data center to accommodate additional resource capacity.
- This heads to the diffusion of a technique which is known as server consolidation.

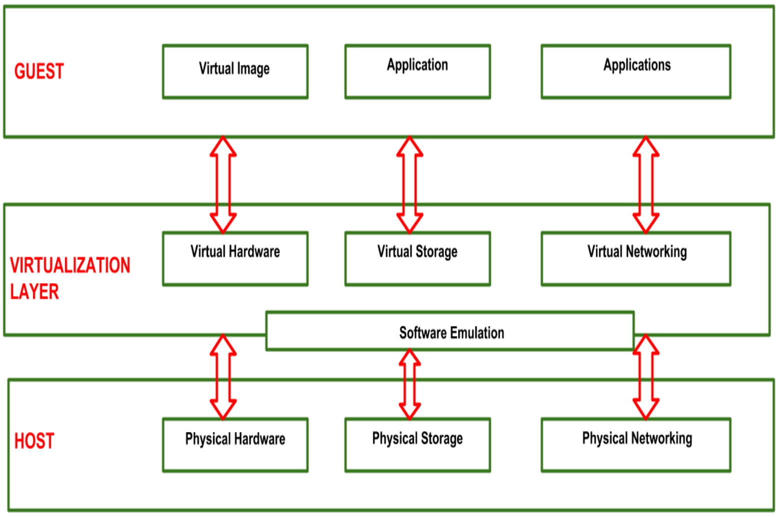
4. Eco-Friendly Initiatives

- At this time, corporations are actively seeking for various methods to minimize their expenditures on power which is consumed by their systems.
- Data centers are main power consumers and maintaining a data center operation needs a continuous power supply as well as a good amount of energy is needed to keep them cool for well-functioning.
- Therefore, server consolidation drops the power consumed and cooling impact by having a fall in number of servers.
- Virtualization can provide a sophisticated method of server consolidation.

5. Administrative Costs

- Furthermore, the rise in demand for capacity surplus, that convert into more servers in a data center, accountable for a significant increase in administrative costs.
- Hardware monitoring, server setup and updates, defective hardware replacement, server resources monitoring, and backups are included in common system administration tasks.
- These are personnel-intensive operations.
- The administrative costs are increased as per the number of servers.
- Virtualization decreases number of required servers for a given workload, hence reduces the cost of administrative employees.

6. Virtualization Reference Model



- Three major Components falls under this category in a virtualized environment:

1. Guest

- The guest represents the system component that interacts with the virtualization layer rather than with the host, as would normally happen.
- Guests usually consist of one or more virtual disk files, and a VM definition file.
- Virtual Machines are centrally managed by a host application that sees and manages each virtual machine as a different application.

2. Host

- The host represents the original environment where the guest is supposed to be managed.
- Each guest runs on the host using shared resources donated to it by the host.
- The operating system, works as the host and manages the physical resource management, and the device support.

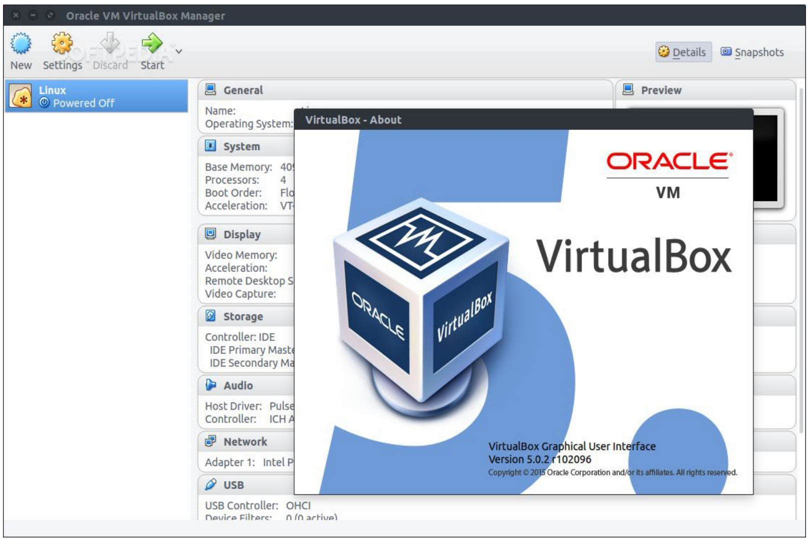
3. Virtualization Layer

- The virtualization layer is responsible for recreating the same or a different environment where the guest will operate.
- It is an additional abstraction layer between a network and storage hardware, computing, and the application running on it.
- Usually, it helps to run a single operating system per machine which can be very inflexible compared to the usage of virtualization.

3.4 Virtual Box

What is VirtualBox?

- Oracle VM VirtualBox is cross-platform virtualization software.
- It allows users to extend their existing computer to run multiple operating systems including Microsoft Windows, Mac OS X, Linux, and Oracle Solaris, at the same time.
- Designed for IT professionals and developers, Oracle VM VirtualBox is ideal for testing, developing, demonstrating, and deploying solutions across multiple platforms from one machine.
- It is freely available as Open-Source Software under the terms of the GNU General Public License (GPL) version 2.



Oracle VM VirtualBox Manager

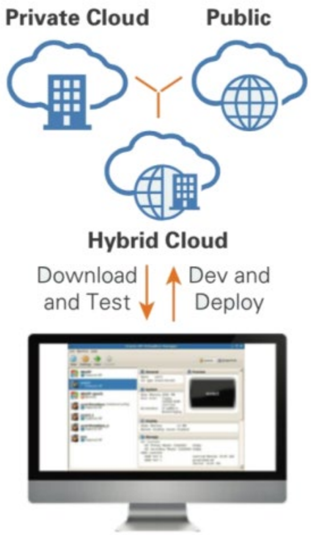
VirtualBox - About

VirtualBox Graphical User Interface
Version 5.0.2 r102096
Copyright © 2015 Oracle Corporation and/or its affiliates. All rights reserved.

- Oracle VM VirtualBox has been designed to take advantage of the innovations introduced in the x86 modern hardware platform, and it is lightweight and easy to install and use.
- Under the simple exterior lies an extremely fast and powerful virtualization engine.
- With a well-earned reputation for speed and agility, Oracle VM VirtualBox contains innovative features to deliver tangible benefits:
  - Excellent performance
  - A powerful virtualization system
  - A wide range of supported guest operating systems
- Oracle VM VirtualBox is a bridge to open source and cloud development.
- The latest release allows users to create and deploy virtual machines nearly everywhere, upload to the cloud, download from the cloud, and review and make changes offline.
- Oracle VM VirtualBox simplifies cloud deployment by allowing developers to create multiplatform environments and to develop applications for container and virtualization technologies within Oracle VM VirtualBox on a single machine.

Oracle VM VirtualBox Enterprise Use Cases

- Development platform for the cloud
- Software developers rely on Oracle VM VirtualBox Enterprise for the development and debugging of their applications in multiple operating systems and environments on one device.
- Developers can clone an environment on their personal desktop/laptop without impact to production services.



One Unique Solution for All Platforms

1. Solution on multiple platforms
2. QA and Testing
3. Demo system for pre-sales support
4. Secure and encrypted virtual machines
5. Training
6. Corporate compliance

- Oracle VM VirtualBox Enterprise is the only desktop virtualization solution available for x86 operating systems, like Microsoft Windows, Linux, Apple MAC OS X and Solaris x86 that provides the same solution on all platforms.

- Oracle VM VirtualBox Enterprise is the desktop virtualization solution that allows software QA teams to control source code, share it within the company and execute software testing on multiple platforms on one unique device.
- With Oracle VM VirtualBox Enterprise, VMs can be exported to Oracle Cloud Infrastructure and all the steps required can be managed through the Graphical User Interface.

VirtualBox runs on:

- Windows
- Linux
- Macintosh
- Solaris hosts
- 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
- OpenBSD

Some Terminology

Host operating system (host OS)

- This is the OS of the physical computer on which Oracle VM VirtualBox was installed.
- There are versions of Oracle VM VirtualBox for Windows, Mac OS X, Linux, and Oracle Solaris hosts.

Guest operating system (guest OS)

- This is the OS that is running inside the virtual machine.
- Oracle VM VirtualBox can run any x86 OS such as DOS, Windows, OS/2, FreeBSD, and OpenBSD.
- To achieve near-native performance of the guest code on your machine, we had to go through a lot of optimizations that are specific to certain OSes.

Host operating system (host OS)

- This is the OS of the physical computer on which Oracle VM VirtualBox was installed.
- There are versions of Oracle VM VirtualBox for Windows, Mac OS X, Linux, and Oracle Solaris hosts.

Guest operating system (guest OS)

- This is the OS that is running inside the virtual machine.
- Oracle VM VirtualBox can run any x86 OS such as DOS, Windows, OS/2, FreeBSD, and OpenBSD.
- To achieve near-native performance of the guest code on your machine, we had to go through a lot of optimizations that are specific to certain OSes.

Features

- Portability
- Guest Additions: shared folders, seamless windows, 3D virtualization
- Great hardware support

    - Guest multiprocessing (SMP)
    - USB device support
    - Hardware compatibility
    - Full ACPI support
    - Multiscreen resolutions
    - Built-in iSCSI support
    - PXE Network boot
  - Multigeneration branched snapshots
  - VM groups
  - Clean architecture and unprecedented modularity
  - Remote machine display

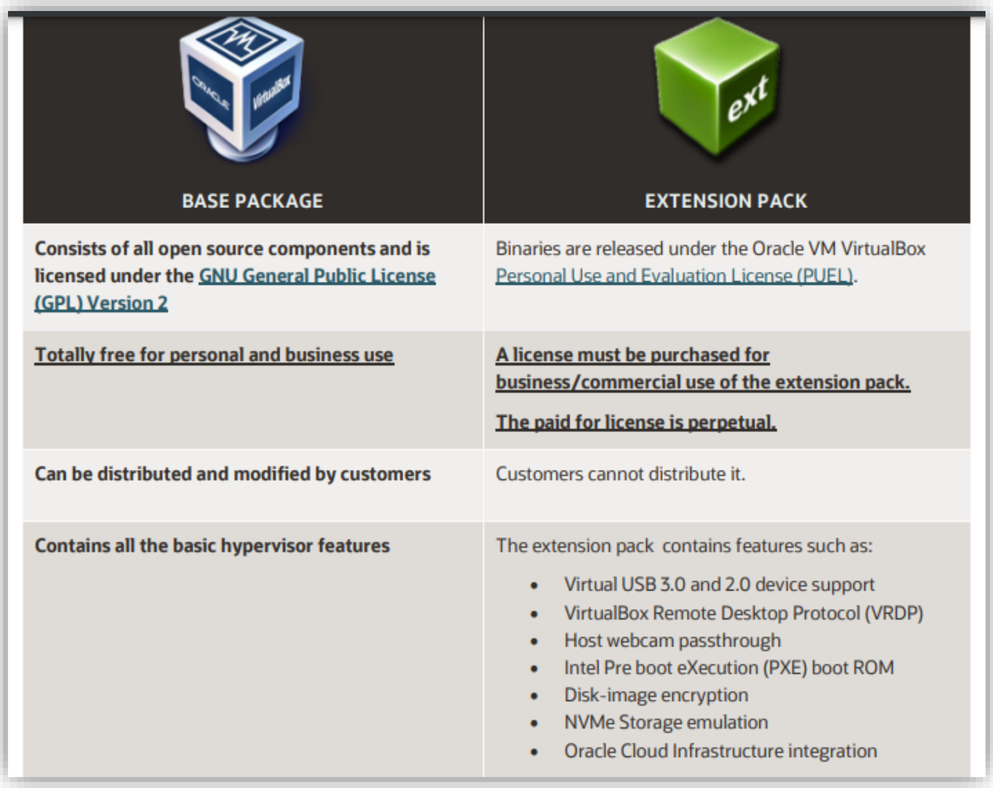
Installing Oracle VM VirtualBox and Extension Packs

- Oracle VM VirtualBox comes in many different packages, and installation depends on your host OS.
- Oracle VM VirtualBox is split into the following components:

Base package: The base package consists of all open-source components and is licensed under the GNU General Public License V2.

Extension packs:

- Additional extension packs can be downloaded which extend the functionality of the Oracle VM VirtualBox base package.
- Oracle VM VirtualBox extension packages have a .vbox-extpack file name extension.
- To install an extension, simply double-click on the package file and a Network Operations Manager window is shown to guide you through the required steps.

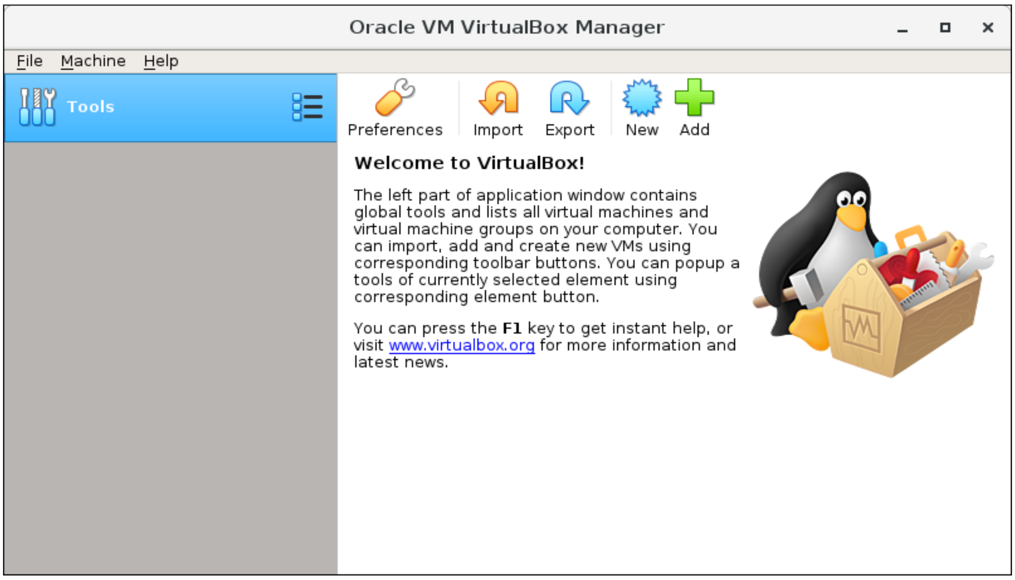


BASE PACKAGE	EXTENSION PACK
Consists of all open source components and is licensed under the GNU General Public License (GPL) Version 2	Binaries are released under the Oracle VM VirtualBox Personal Use and Evaluation License (PUEL).
Totally free for personal and business use	**A license must be purchased for business/commercial use of the extension pack.** **The paid for license is perpetual.**
Can be distributed and modified by customers	Customers cannot distribute it.
Contains all the basic hypervisor features	The extension pack contains features such as: • Virtual USB 3.0 and 2.0 device support • VirtualBox Remote Desktop Protocol (VRDP) • Host webcam passthrough • Intel Pre boot eXecution (PXE) boot ROM • Disk-image encryption • NVMe Storage emulation • Oracle Cloud Infrastructure integration

Starting Oracle VM VirtualBox

After installation, you can start Oracle VM VirtualBox as follows:

- On a Windows host, in the Programs menu, click on the item in the VirtualBox group. On some Windows platforms, you can also enter VirtualBox in the search box of the Start menu.
- On a Mac OS X host, in the Finder, double-click on the VirtualBox item in the Applications folder. You may want to drag this item onto your Dock.
- On a Linux or Oracle Solaris host, depending on your desktop environment, an Oracle VM VirtualBox item may have been placed in either the System or System Tools group of your Applications menu. Alternatively, you can enter VirtualBox in a terminal window.
- When you start Oracle VM VirtualBox for the first time, a window like the following is displayed:

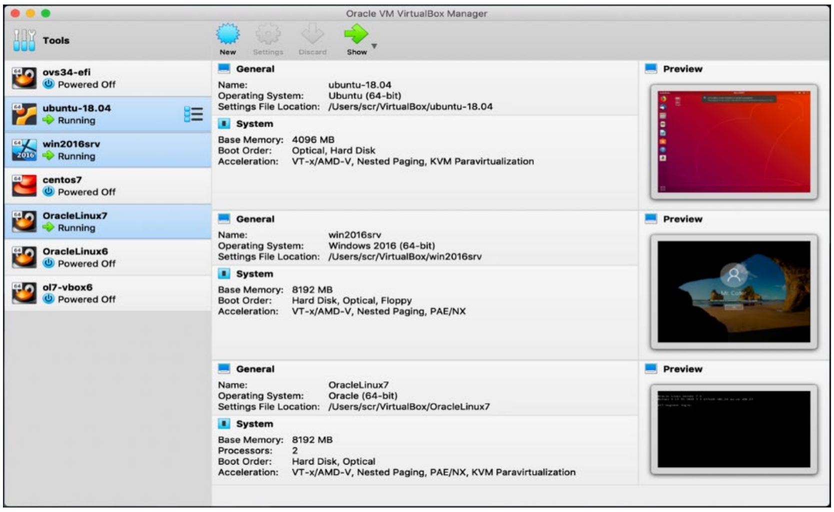


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

- This window is called the VirtualBox Manager.
- The left pane will later list all your virtual machines.
- Since you have not yet created any virtual machines, this list is empty.
- The Tools button provides access to user tools, such as the Virtual Media Manager.
- The pane on the right displays the properties of the currently selected virtual machine.
- Since you do not have any machines yet, the panel displays a welcome message.
- The buttons on the right pane are used to create and work with VMs.
- The following figure gives an idea of what Oracle VM VirtualBox might look like after you have created some VMs.



ovs34-efi — Powered Off
ubuntu-18.04 — Running
win2016srv — Running
centos7 — Powered Off
OracleLinux7 — Running
OracleLinux6 — Powered Off
ol7-vbox6 — Powered Off

General
Name: ubuntu-18.04
Operating System: Ubuntu (64-bit)
Settings File Location: /Users/scr/VirtualBox/ubuntu-18.04

System
Base Memory: 4096 MB
Boot Order: Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

General
Name: win2016srv
Operating System: Windows 2016 (64-bit)
Settings File Location: /Users/scr/VirtualBox/win2016srv

System
Base Memory: 8192 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

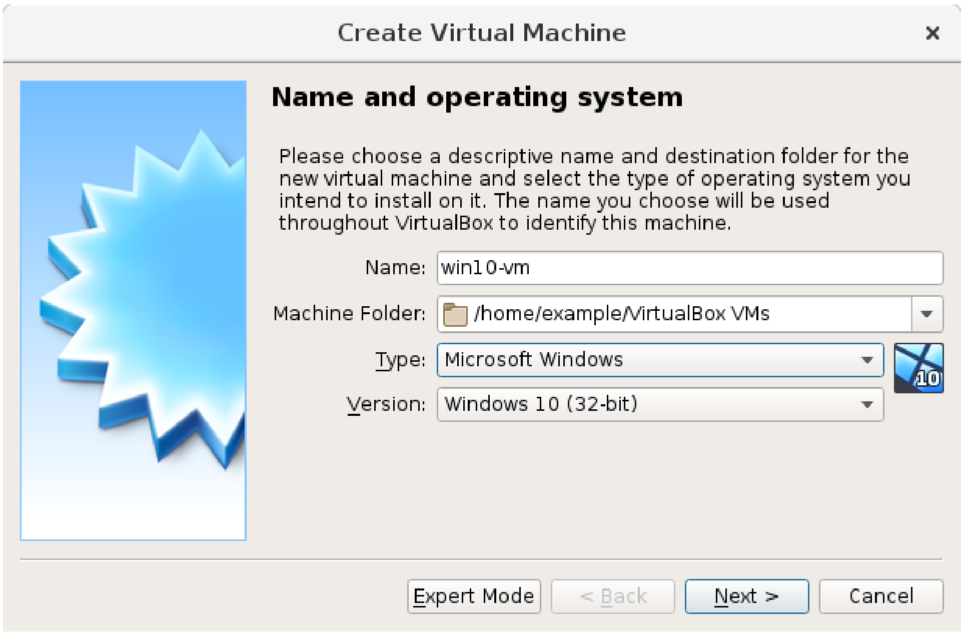
General
Name: OracleLinux7
Operating System: Oracle (64-bit)
Settings File Location: /Users/scr/VirtualBox/OracleLinux7

System
Base Memory: 8192 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

3.5 Deploying A Virtual Machine

Creating Your First Virtual Machine

- Click New in the VirtualBox Manager window. A wizard is shown, to guide you through setting up a new virtual machine (VM).



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

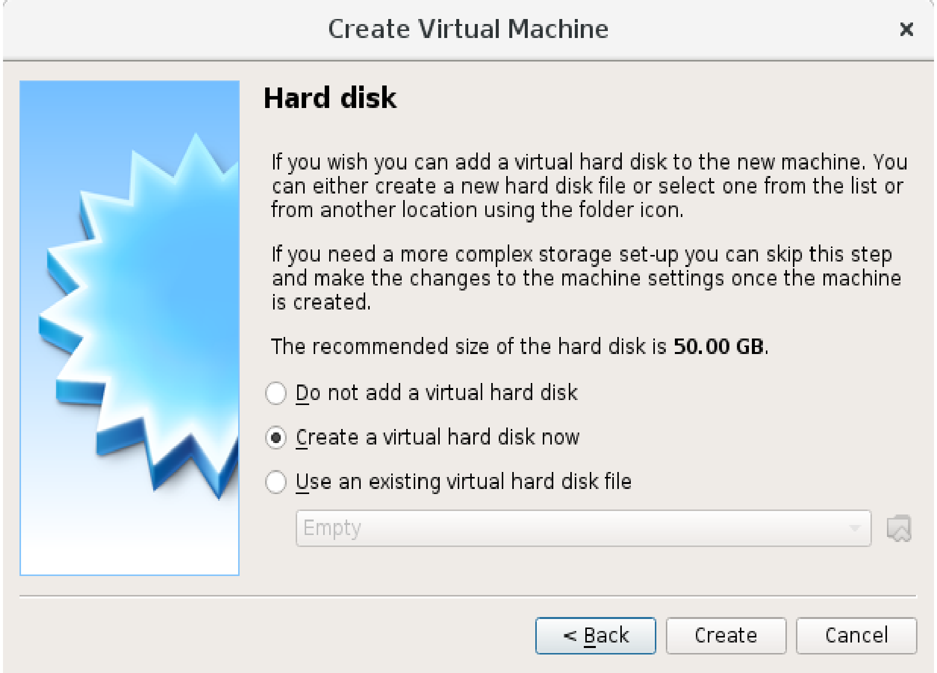
Name: win10-vm

Machine Folder: /home/example/VirtualBox VMs

Type: Microsoft Windows

Version: Windows 10 (32-bit)

- The Name of the VM you choose is shown in the machine list of the VirtualBox Manager window and is also used for the VM's files on disk.
- The Machine Folder is the location where VMs are stored on your computer.
- For Operating System Type, select the OS that you want to install.
- On the next page, select the Memory (RAM) that Oracle VM VirtualBox should allocate every time the virtual machine is started.
- The amount of memory given here will be taken away from your host machine and presented to the guest OS, which will report this size as the virtual computer's installed RAM.
- Next, you must specify a Virtual Hard Disk for your VM.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **50.00 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

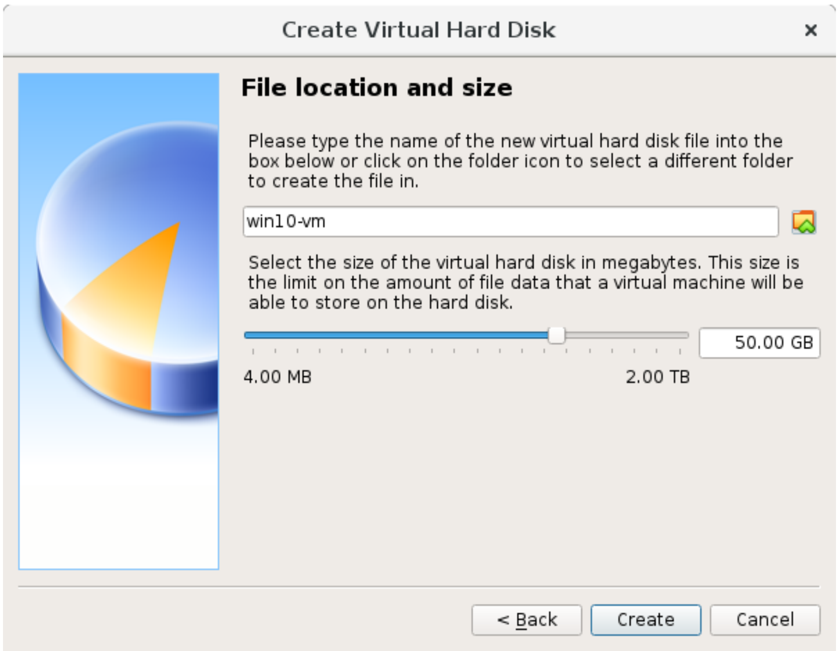
○ Use an existing virtual hard disk file

Empty

- To create a new, empty virtual hard disk, click the Create button.
- You can pick an existing disk image file.
- The drop-down list presented in the window lists all disk images which are currently remembered by Oracle VM VirtualBox. These disk images are currently attached to a virtual machine, or have been attached to a virtual machine.
- Alternatively, click on the small folder icon next to the drop-down list. In the displayed file dialog, you can click Add to select any disk image file on your host disk.
- If you are using Oracle VM VirtualBox for the first time, you will want to create a new disk image. Click the Create button.
- This displays another window, the Create Virtual Hard Disk Wizard wizard. This wizard helps you to create a new disk image file in the new virtual machine's folder.

Oracle VM VirtualBox supports the following types of image files:

- A dynamically allocated file only grows in size when the guest actually stores data on its virtual hard disk. Therefore, this file is small initially. As the drive is filled with data, the file grows to the specified size.
- A fixed-size file immediately occupies the file specified, even if only a fraction of that virtual hard disk space is actually in use. While occupying much more space, a fixed-size file incurs less overhead and is therefore slightly faster than a dynamically allocated file.
- To prevent your physical hard disk (host OS) from filling up, Oracle VM VirtualBox limits the size of the image file. But the image file must be large enough to hold the contents of the guest OS and the applications you want to install.
- For a Windows or Linux guest, you will probably need several gigabytes for any serious use. The limit of the image file size can be changed later.



Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

win10-vm

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

50.00 GB

- After having selected or created your image file, click Next to go to the next page.
- Click Create, to create your new virtual machine.
- The virtual machine is displayed in the list on the left side of the VirtualBox Manager window, with the name that you entered initially.
- After becoming familiar with the use of wizards, consider using the Expert Mode available in some wizards. Where available, this is selectable using a button, and speeds up the process of using wizards.

Running Your Virtual Machine

To start a virtual machine, you have several options:

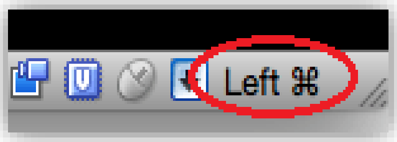
- Double-click on the VM's entry in the list in the VirtualBox Manager window.
- Select the VM's entry in the list in the VirtualBox Manager window, and click **Start** at the top of the window.
- Go to the VirtualBox VMs folder in your system user's home directory. Find the subdirectory of the machine you want to start and double-click on the machine settings file. This file has a **.vbox file** extension.
- Starting a virtual machine displays a new window, and the virtual machine which you selected will boot up. Everything which would normally be seen on the virtual system's monitor is shown in the window.

Starting a New VM for the First Time

- When a VM is started for the first time, the First Start Wizard, is displayed. This wizard helps you to select an installation medium.
- The wizard helps you to select a medium to install an OS from.
  - Physical CD or DVD media
  - Host Drive

Capturing and Releasing Keyboard and Mouse

- Oracle VM VirtualBox provides a virtual USB tablet device to new virtual machines through which mouse events are communicated to the guest OS.
- If you are running a modern guest OS that can handle such devices, mouse support may work out of the box without the mouse being captured.
- If the virtual machine detects only standard PS/2 mouse and keyboard devices, since the OS in the virtual machine does not know that it is not running on a real computer, it expects to have exclusive control over your keyboard and mouse.
- Below is the Host Key Setting on the Virtual Machine Task Bar:

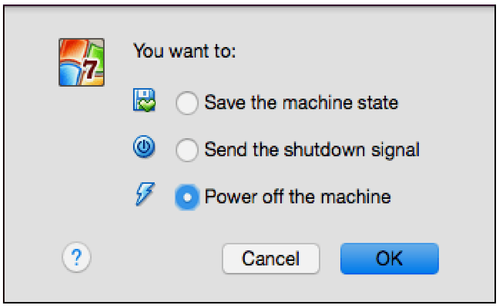


Changing Removeable Media

- While a virtual machine is running, you can change removable media in the Devices menu of the VM's window.
- Here you can select in detail what Oracle VM VirtualBox presents to your VM as a CD, DVD, or floppy drive.

Saving the State of the Machine

- When you click on the Close button of your virtual machine window, at the top right of the window, Oracle VM VirtualBox asks you whether you want to save or power off the VM.
- As a shortcut, you can also press Host key + Q.



You want to:

○ Save the machine state

○ Send the shutdown signal

● Power off the machine

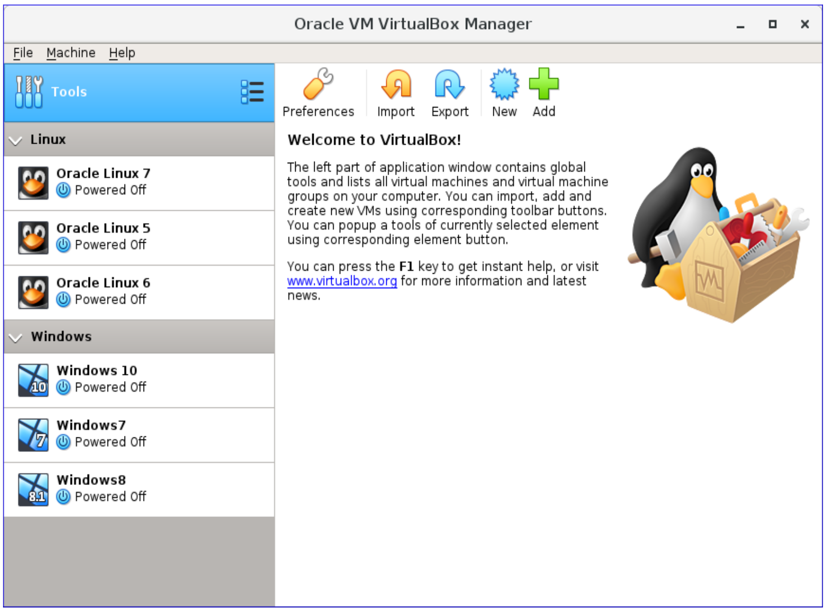
Save the machine state: Oracle VM VirtualBox freezes the virtual machine by completely saving its state to your local disk.

Send the shutdown signal: This will send an ACPI shutdown signal to the virtual machine, which has the same effect as if you had pressed the power button on a real computer.

Power off the machine: Oracle VM VirtualBox also stops running the virtual machine, but without saving its state.

Using VM Groups

- VM groups enable the user to create ad hoc groups of VMs, and to manage and perform functions on them collectively, as well as individually.
- The following figure shows VM groups displayed in VirtualBox Manager.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

- Create a group using the VirtualBox Manager. Do one of the following:
  - Drag one VM on top of another VM.
  - Select multiple VMs and select Group from the right-click menu.

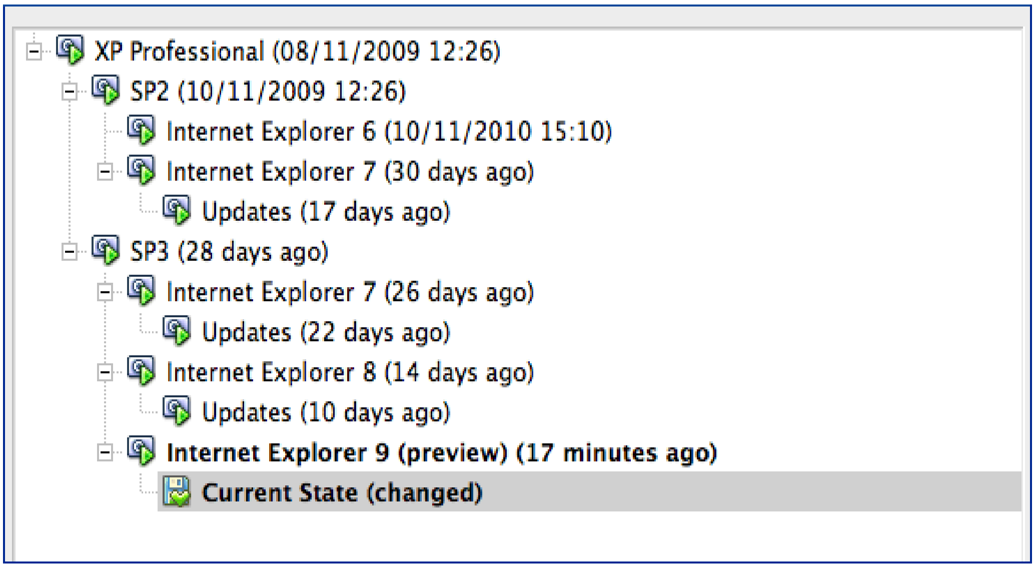
Snapshots

- With snapshots, you can save a particular state of a virtual machine for later use.
- At any later time, you can revert to that state, even though you may have changed the VM considerably since then.
- A snapshot of a virtual machine is thus similar to a machine in Saved state, but there can be many of them, and these saved states are preserved.
- To see the snapshots of a virtual machine, click on the machine name in VirtualBox Manager.
- Then click the List icon next to the machine name and select Snapshots. Until you take a snapshot of the machine, the list of snapshots will be empty except for the Current State item, which represents the "now" point in the lifetime of the virtual machine.

There are three operations related to snapshots, as follows:

- Take a snapshot. This makes a copy of the machine's current state, to which you can go back at any given time later.

- If your VM is running, select Take Snapshot from the Machine pull-down menu of the VM window.



XP Professional (08/11/2009 12:26)
SP2 (10/11/2009 12:26)
Internet Explorer 6 (10/11/2010 15:10)
Internet Explorer 7 (30 days ago)
Updates (17 days ago)
SP3 (28 days ago)
Internet Explorer 7 (26 days ago)
Updates (22 days ago)
Internet Explorer 8 (14 days ago)
Updates (10 days ago)
Internet Explorer 9 (preview) (17 minutes ago)
Current State (changed)

Removing and Moving Virtual Machines

Removing a VM

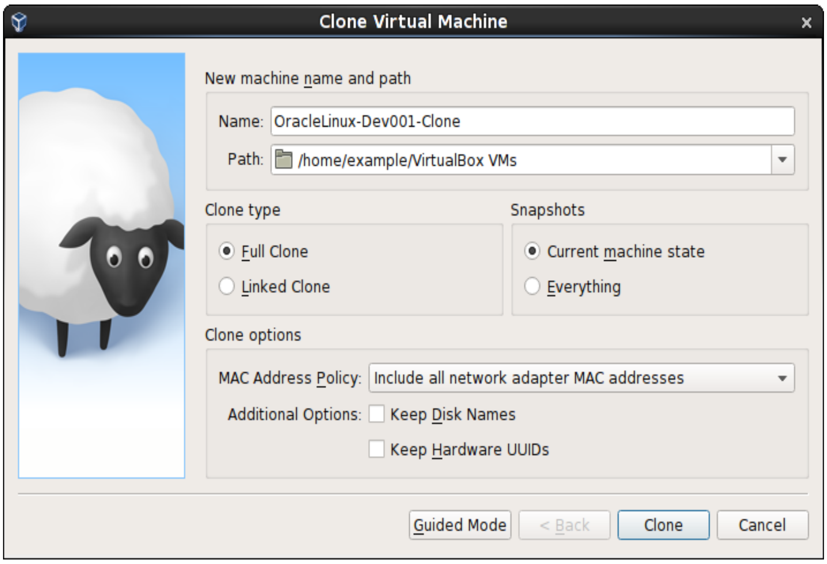
- To remove a VM, right-click on the VM in the VirtualBox Manager's machine list and select Remove.
- The confirmation dialog enables you to specify whether to only remove the VM from the list of machines or to remove the files associated with the VM.
- Remove menu item is disabled while a VM is running.

Moving a VM

- To move a VM to a new location on the host, right-click on the VM in the VirtualBox Manager's machine list and select Move.
- The file dialog prompts you to specify a new location for the VM.
- When you move a VM, Oracle VM VirtualBox configuration files are updated automatically to use the new location on the host.

Cloning Virtual Machines

- You can create a full copy or a linked copy of an existing VM. This copy is called a clone.
- You might use a cloned VM to experiment with a VM configuration, to test different guest OS levels, or to back up a VM.
- The Clone Virtual Machine wizard guides you through the cloning process.



Clone Virtual Machine

New machine name and path

Name: OracleLinux-Dev001-Clone

Path: /home/example/VirtualBox VMs

Clone type

● Full Clone
○ Linked Clone

Snapshots

● Current machine state
○ Everything

Clone options

MAC Address Policy: Include all network adapter MAC addresses

Additional Options: □ Keep Disk Names
□ Keep Hardware UUIDs

- Start the wizard by clicking Clone in the right-click menu of the VirtualBox Manager's machine list or in the Snapshots view of the selected VM.
- Specify a new Name for the clone. You can choose a Path for the cloned virtual machine, otherwise Oracle VM VirtualBox uses the default machines folder.
- The **Clone Type** option specifies whether to create a clone linked to the source VM or to create a fully independent clone:

  Full Clone: Copies all dependent disk images to the new VM folder. A full clone can operate fully without the source VM.

  Linked Clone: Creates new differencing disk images based on the source VM disk images. If you select the current state of the source VM as the clone point, Oracle VM VirtualBox creates a new snapshot.

The following clone options are available:

MAC Address Policy

- Specifies how to retain network card MAC addresses when cloning the VM.
- For example, the Generate New MAC Addresses for All Network Adapters value assigns a new MAC address to each network card during cloning. This is the default setting. This is the best option when both the source VM and the cloned VM must operate on the same network. Other values enable you to retain the existing MAC addresses in the cloned VM.

Keep Disk Names: Retains the disk image names when cloning the VM.

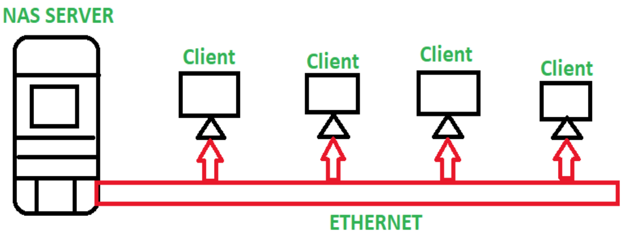
Keep Hardware UUIDs: Retains the hardware universally unique identifiers (UUIDs) when cloning the VM.

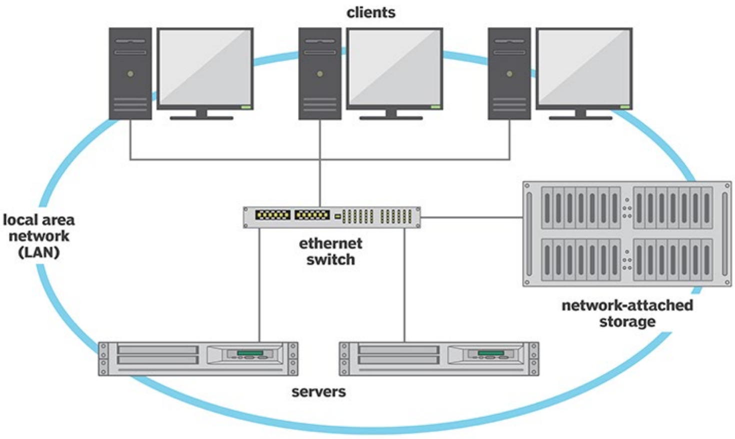
- The duration of the clone operation depends on the size and number of attached disk images.
- Note that the **Clone** menu item is disabled while a machine is running.

3.6 Introduction to Network Attached Storage (NAS)

What is Network-attached Storage (NAS)?

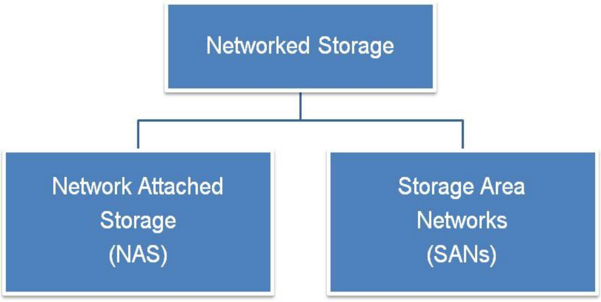
- Network-attached storage (NAS) is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity





- Users on a local area network (LAN) access the shared storage via a standard Ethernet connection.
- NAS devices typically do not have a keyboard or display and are configured and managed with a browser-based utility.
- Each NAS resides on the LAN as an independent network node, defined by its own unique Internet Protocol (IP) address.
- NAS stands out for its ease of access, high capacity and low cost.
- The devices consolidate storage in one place and support a cloud tier and tasks, such as archiving and backup.
- Prior to NAS, enterprises had to configure and manage hundreds or even thousands of file servers.
- To expand storage capacity, NAS appliances are outfitted with more or larger disks, known as scale-up NAS.
- Appliances are also clustered together for scale-out storage.
- In addition, most NAS vendors partner with cloud storage providers to give customers the flexibility of redundant backup.
- Network-attached storage relies on hard disk drives (HDDs) to serve data.
- Input/output (I/O) contention can occur when too many users overwhelm the system with requests at the same time.
- Newer systems use faster flash storage, either as a tier alongside HDDs or in all-flash configurations.

Types of Network-attached Storage (NAS)?



- NAS and storage area networks (SANs) are the two main types of networked storage.
- NAS handles unstructured data, such as audio, video, websites, text files and Microsoft Office documents.
- SANs are designed primarily for block storage inside databases, also known as structured data.

Application of Network-attached Storage (NAS)

- The purpose of NAS is to enable users to collaborate and share data more effectively.
- It is useful to distributed teams that need remote access or work in different time zones.
- NAS connects to a wireless router, making it easy for distributed workers to access files from any desktop or mobile device with a network connection.
- Organizations commonly deploy a NAS environment as the foundation for a personal or private cloud.
- Some NAS products are designed for use in large enterprises. Others are for home offices or small businesses.
- Devices usually contain at least two drive bays, although single-bay systems are available for noncritical data.

- Enterprise NAS gear is designed with more high-end data features to aid storage management and usually comes with at least four drive bays.
- The applications to be used determine the type of HDD selected for a NAS device.
- Sharing Microsoft Excel spreadsheets or Word documents with co-workers is a routine task, as is performing periodic data backup.
- Conversely, using NAS to handle large volumes of streaming media files requires larger capacity disks, more memory and more powerful network processing.

At home, people use a NAS system to store and serve multimedia files and to automate backups. Home users rely on NAS to do the following:

- Manage smart TV storage
- Manage security systems and security updates
- Manage consumer-based internet of things components
- Create a media streaming service
- Manage torrent files
- Host a personal cloud server
- Create, test and develop a personal website

In the enterprise, NAS is used:

- As a backup target, using a NAS array, for archiving and disaster recovery
- For testing and developing web-based and server-side web applications
- For hosting messaging applications
- For hosting server-based, open-source applications such as customer relationship management, human resource management, and enterprise resource planning applications
- For serving email, multimedia files, databases and print jobs

3.7 TrueNAS Installation

Minimum Requirements

Here are the basics of what you'll need to run TrueNAS:

1. **64-bit system**: Used solely for TrueNAS CORE. TrueNAS is NOT dual-boot friendly, so make sure you're only using the system for TrueNAS.

2. **Minimum 8 GB of RAM**: Use more if you're installing virtual machines or plugins.

3. **Boot device (SSD or HDD)**:

- Also known as the boot drive.
- At least 8 GB of storage capacity is required to serve as the boot device for TrueNAS.
- An SSD is an ideal choice for longevity; keep in mind that the entire disk will be used for the TrueNAS operating system.
- USB sticks are no longer recommended, due to the high amount of write tasks on TrueNAS.

4. **Storage drives (SSDs or HDDs):**

- At least one hard drive for storage of files, but multiple drives of the same capacity can be easily bundled together to provide redundancy, if a drive fails.
- Western Digital drives are a great choice for data storage, but as with any vendor, make sure to avoid drives using SMR technology in ZFS applications.

5. **Ethernet cord:**

- To connect your system to the network, through a router or modem. There is no wireless support in TrueNAS.

6. **Blank DVD or USB stick:**

- Required to create the TrueNAS installation media. The TrueNAS ISO image exceeds 700 MB so CDs will not work.
- Your USB stick should be at least 1 GB. Installation media is not the same as the boot device.

7. Monitor & Keyboard:

- After the setup is complete and you've written down your TrueNAS system's IP address, the monitor can be disconnected.
-

8. Computer or Laptop & Internet Browser:

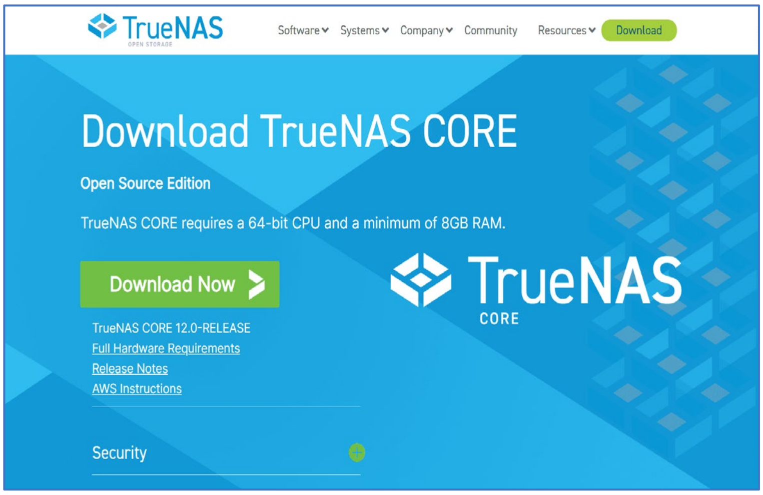
- To access the GUI and administer your TrueNAS system.

Creating the Installation Media and Operating System Device for TrueNAS

- It's important to understand that TrueNAS needs two devices during the installation process, the install media and the operating system device (boot device).
- The install media is used to install TrueNAS to the operating system device on a computer.
- A USB stick or DVD can be used as the install media. In this tutorial, we will be using an 8 GB USB stick as our install media.
- The minimum size required is 1 GB.
- The TrueNAS CORE operating system device can be an SSD or hard drive.

OR
+
TrueNAS.iso
At least 1GB
DVD

- The operating system device must have at least 8 GB of space, but we recommend 32 GB or more for operating system device storage capacity to provide room for logging, operating system environments, and future additions.
- The entire operating system device will be used for TrueNAS.
- TrueNAS reads and writes to the operating system device, so reliability counts.
- Using a small SSD or hard drive will provide the best longevity.
- Due to the high write tasks in TrueNAS CORE, USB sticks are not very reliable over the long term.



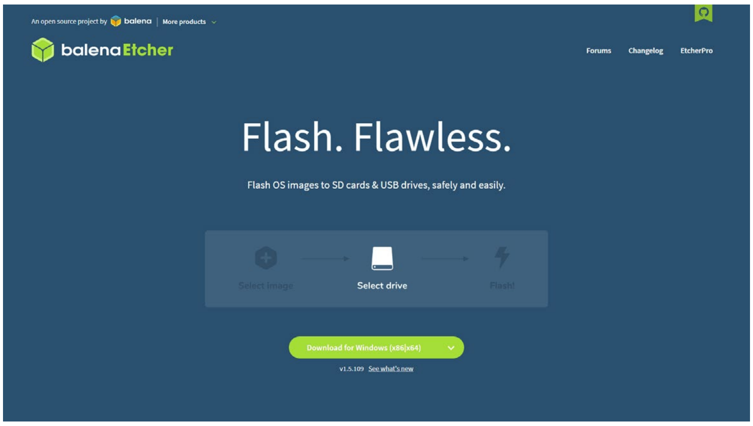
Download TrueNAS CORE

Open Source Edition

TrueNAS CORE requires a 64-bit CPU and a minimum of 8GB RAM.

TrueNAS CORE 12.0-RELEASE
Full Hardware Requirements
Release Notes
AWS Instructions

- Download the latest TrueNAS image from www.truenas.com/download.
- Make sure you have a USB stick ready to use as the install media.
- After you've downloaded the TrueNAS installation image, you'll need to burn the image to a blank DVD or write it to a blank USB drive.
- Writing a TrueNAS image to the USB stick erases all data on the device. Back up any files on the device before starting.

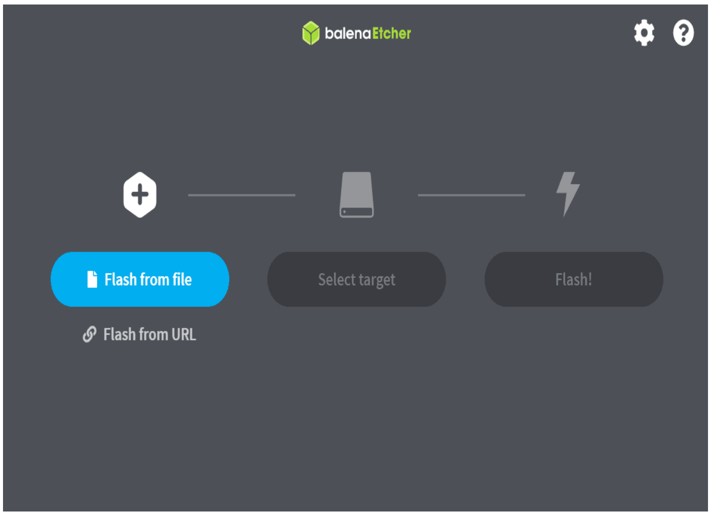


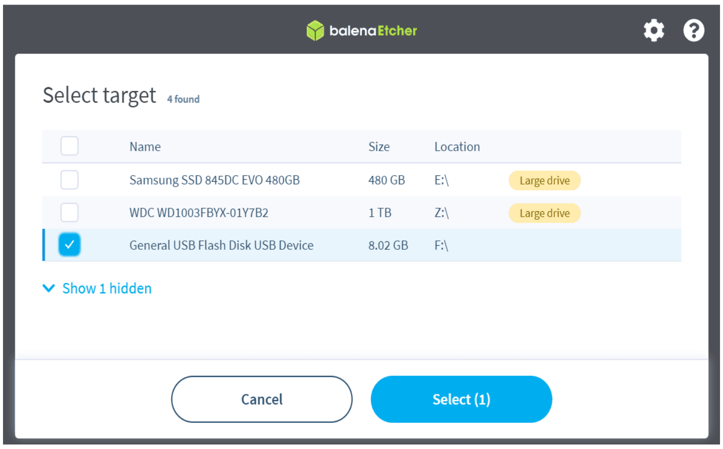
Flash. Flawless.

Flash OS images to SD cards & USB drives, safely and easily.

Etcher

- We will be using a tool called balenaEtcher also known as Etcher.
- Scroll down the web page and click on the Download button for Etcher. Download, install, and run Etcher.
- Now insert your USB stick into your machine. Verify the drive letter by going to "This PC".

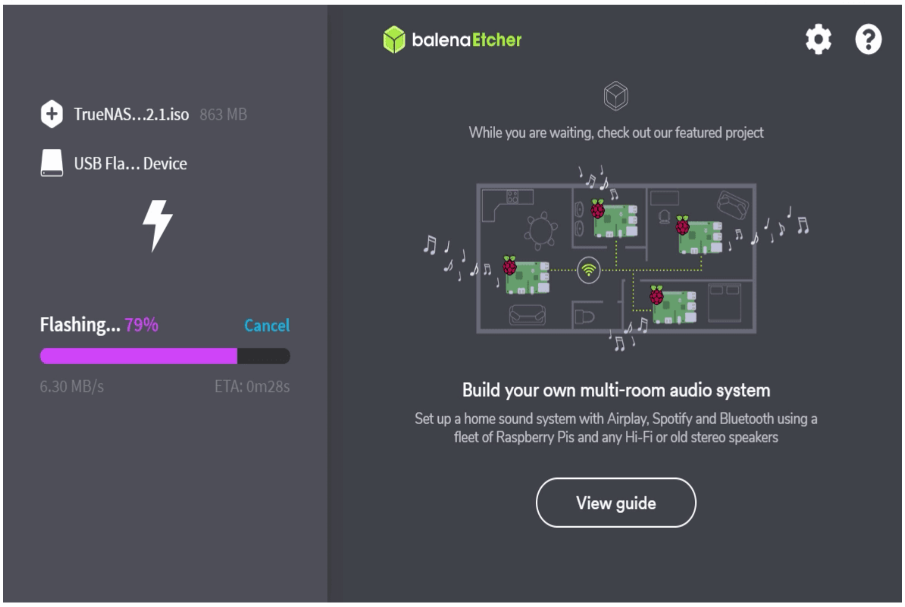




Select target 4 found

	Name	Size	Location	
□	Samsung SSD 845DC EVO 480GB	480 GB	E:\	Large drive
□	WDC WD1003FBYX-01Y7B2	1 TB	Z:\	Large drive
☑	General USB Flash Disk USB Device	8.02 GB	F:\	

- In the Etcher application, click “Flash from file” and browse to the TrueNAS .iso file that you downloaded earlier.
- If your USB stick is not already selected, click “Select Target” and choose the drive to use as the install media. Remember, this is the install media, not the operating system device.
- Now, click “Flash!” It takes a few minutes to write the image to the disk. A “Flash Complete!” message is shown when done.



TrueNAS...2.1.iso 863 MB

USB Fla... Device

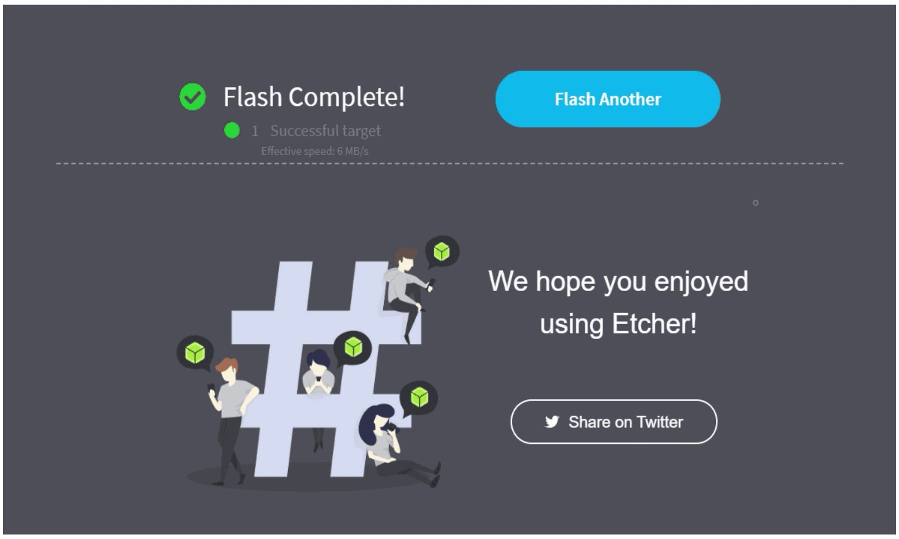
Flashing... 79%

6.30 MB/s ETA: 0m28s

While you are waiting, check out our featured project

Build your own multi-room audio system

Set up a home sound system with Airplay, Spotify and Bluetooth using a fleet of Raspberry Pis and any Hi-Fi or old stereo speakers



Flash Complete!

1 Successful target

Effective speed: 6 MB/s

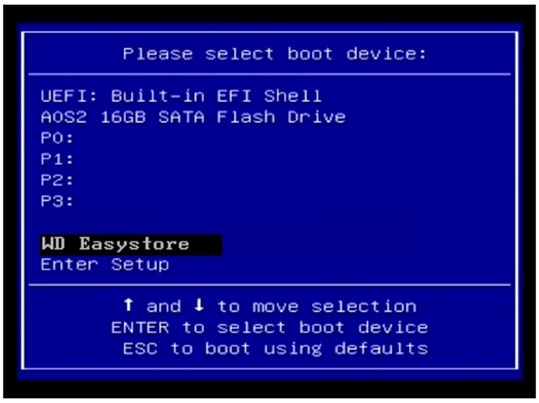
We hope you enjoyed using Etcher!

3.8 TrueNAS Basic Configuration

TrueNAS Installation

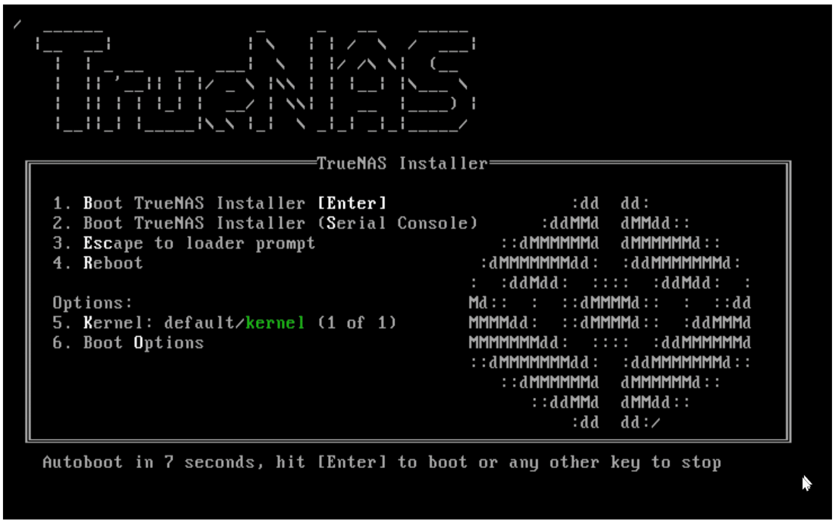
- Installing TrueNAS
- Now that we’ve gone through the basics of what you need to get started, let’s begin the installation of TrueNAS.

- Make sure that both the boot device and the TrueNAS installation media are inserted in the machine that you chose to run TrueNAS.

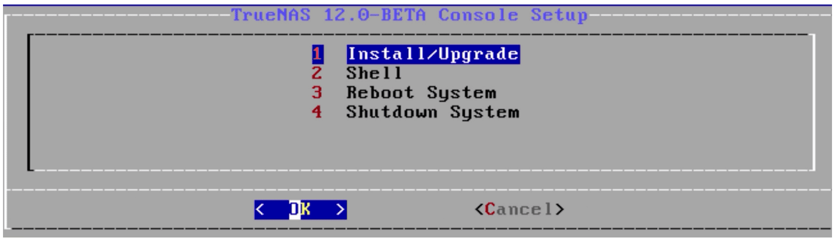


```
Please select boot device:

UEFI: Built-in EFI Shell
AOS2 16GB SATA Flash Drive
P0:
P1:
P2:
P3:

WD Easystore
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

- Boot into the BIOS of the system and double-check that your system is set to boot from the device that contains the TrueNAS installation media that you created earlier. After confirming, reboot the system.

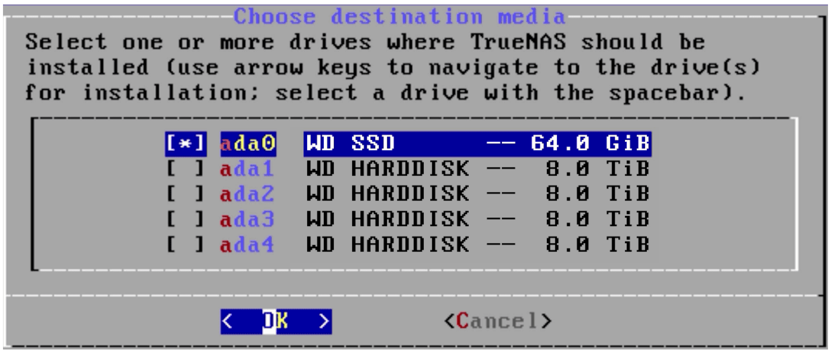


```
TrueNAS Installer

1. Boot TrueNAS Installer [Enter]
2. Boot TrueNAS Installer (Serial Console)
3. Escape to loader prompt
4. Reboot

Options:
5. Kernel: default/kernel (1 of 1)
6. Boot Options

Autoboot in 7 seconds, hit [Enter] to boot or any other key to stop
```



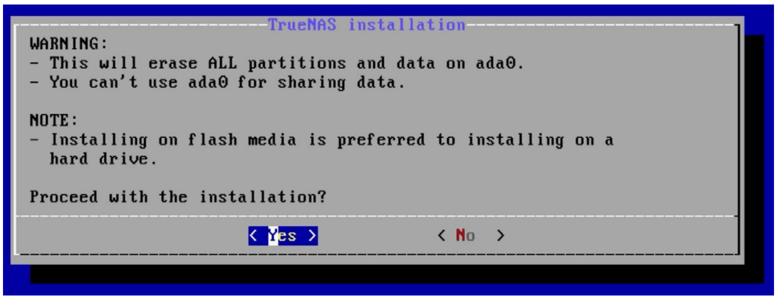
```
TrueNAS 12.0-BETA Console Setup

1 Install/Upgrade
2 Shell
3 Reboot System
4 Shutdown System

< OK >        <Cancel>
```

- The TrueNAS install menu will be displayed. Choose option 1 on the menu to begin the TrueNAS installation.
- This will load the Console Setup menu. Hit enter to choose the “Install/Upgrade” option.



```
Choose destination media
Select one or more drives where TrueNAS should be
installed (use arrow keys to navigate to the drive(s)
for installation; select a drive with the spacebar).

[*] ada0  WD SSD      -- 64.0 GiB
[ ] ada1  WD HARDDISK --  8.0 TiB
[ ] ada2  WD HARDDISK --  8.0 TiB
[ ] ada3  WD HARDDISK --  8.0 TiB
[ ] ada4  WD HARDDISK --  8.0 TiB

< OK >        <Cancel>
```

- The next menu asks which drive should be used for TrueNAS. Make sure to select the boot device and not the storage disk.
- This menu will show the size of the disks to make it easier to determine the boot device, which is generally a smaller size than the storage disks (which will be larger).
- The one you want will likely be the smallest on the list. Note that the names of your drives will be different.
- Press the arrow keys to select a drive, and press the spacebar to designate it as the drive you wish to use.



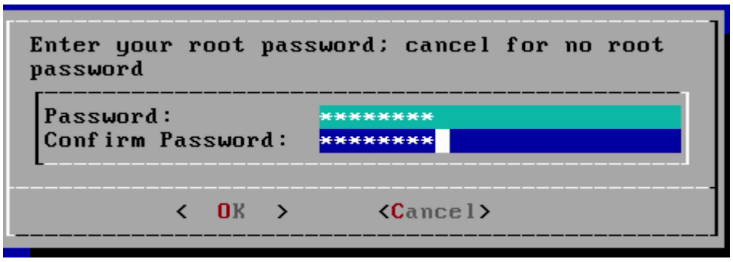
TrueNAS installation

WARNING:
- This will erase ALL partitions and data on ada0.
- You can't use ada0 for sharing data.

NOTE:
- Installing on flash media is preferred to installing on a hard drive.

Proceed with the installation?

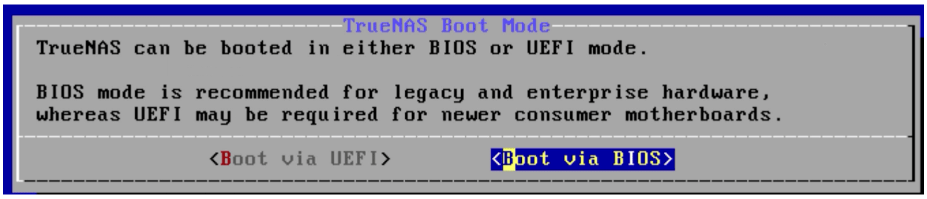
The boot device cannot be used for anything other than the operating system itself. Press OK, then YES, to proceed.



Enter your root password; cancel for no root password

Password: *********
Confirm Password: *********

Next, type in and confirm the password that will be used to login to TrueNAS.

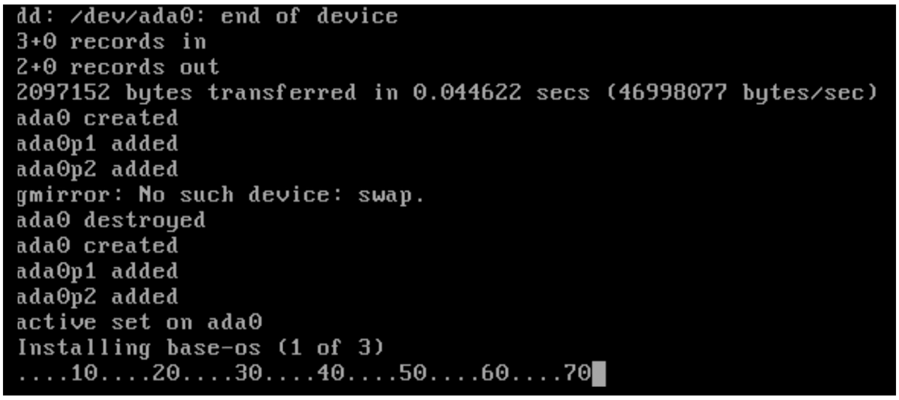


TrueNAS Boot Mode

TrueNAS can be booted in either BIOS or UEFI mode.

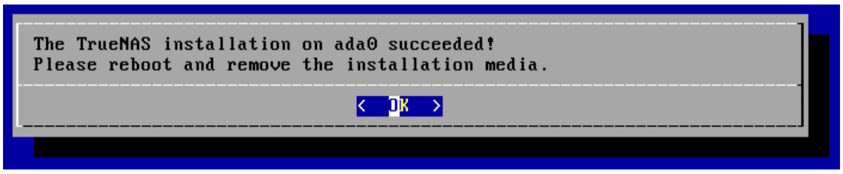
BIOS mode is recommended for legacy and enterprise hardware, whereas UEFI may be required for newer consumer motherboards.

- TrueNAS can be booted in either BIOS or UEFI mode.
- For the purposes of this video, I'll be choosing BIOS. BIOS works for almost all motherboards and is typically the option to choose for older hardware.
- Choosing UEFI will require that your motherboard is more modern and UEFI capable.



```
dd: /dev/ada0: end of device
3+0 records in
2+0 records out
2097152 bytes transferred in 0.044622 secs (46998077 bytes/sec)
ada0 created
ada0p1 added
ada0p2 added
gmirror: No such device: swap.
ada0 destroyed
ada0 created
ada0p1 added
ada0p2 added
active set on ada0
Installing base-os (1 of 3)
....10....20....30....40....50....60....70
```

- Once chosen, your installation will begin. Wait for a bit, all those commands popping up on the screen are perfectly normal. It should take a few minutes.
- A message will appear saying to reboot and remove the installation media. Choose OK to reboot.
- Remove the installation media from your system.
- As the system reboots, double-check the BIOS to make sure the boot order now defaults to the boot device.



```
The TrueNAS installation on ada0 succeeded!
Please reboot and remove the installation media.
```

Storage Configuration

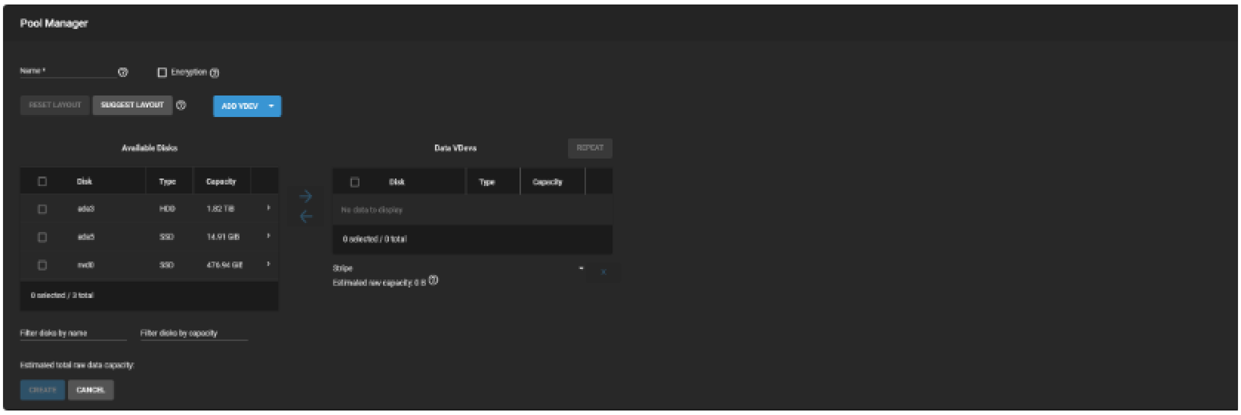
- Now that we’re logged in to the web interface, it’s time to set up TrueNAS storage.
- These instructions demonstrate a simple mirrored pool setup, where one disk is used for storage and the other for data protection.
- However, there are a vast number of configuration possibilities for your storage environment! You can read more about these options in the in-depth Pool Creation article.

Requirements

- At minimum, the system needs at least two identically sized disks to create a mirrored storage pool.
- While a single-disk pool is technically allowed, it is not recommended.
- The disk used for the TrueNAS installation does not count toward this limit.
- Data backups can be configured in several ways and have different requirements.
- Backing data up in the Cloud requires a 3rd party Cloud Storage provider account.
- Backups with Replication requires either additional storage on the TrueNAS system or (ideally) another TrueNAS system in a different location.

Simple Storage Setup

Go to Storage > Pools and click ADD. Set Create a new pool and click CREATE POOL.



Pool Manager

Name *

☐ Encryption

Available Disks

☐	Disk	Type	Capacity
☐	ada3	HDD	1.82 TiB
☐	ada5	SSD	14.91 GiB
☐	nvd0	SSD	476.94 GiB

0 selected / 3 total

Data VDevs

☐	Disk	Type	Capacity

No data to display

0 selected / 0 total

Stripe

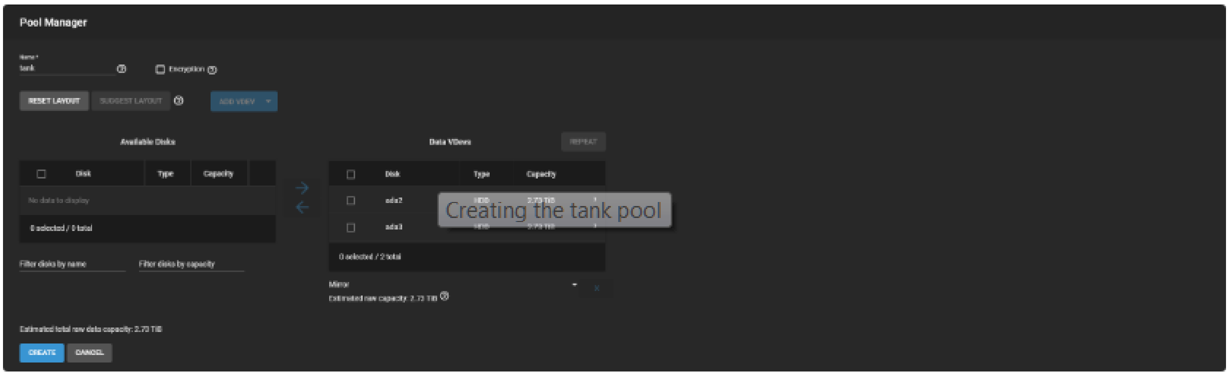
Estimated raw capacity: 0 B

Filter disks by name

Filter disks by capacity

Estimated total raw data capacity:

- For the Name, enter tank or any other preferred name. In the Available Disks, set two identical disks and click the to move them to the Data VDevs area.
- If the disks used have non-unique serial numbers, they do not populate the Available Disks section until the Show disk with non-unique serial numbers checkbox is selected.



Pool Manager

Name* tank

☐ Encryption

Available Disks

☐	Disk	Type	Capacity
No data to display			

0 selected / 0 total

Filter disks by name
Filter disks by capacity

Data VDevs

☐	Disk	Type	Capacity
☐	ada2	HDD	2.73 TiB
☐	ada3	HDD	2.73 TiB

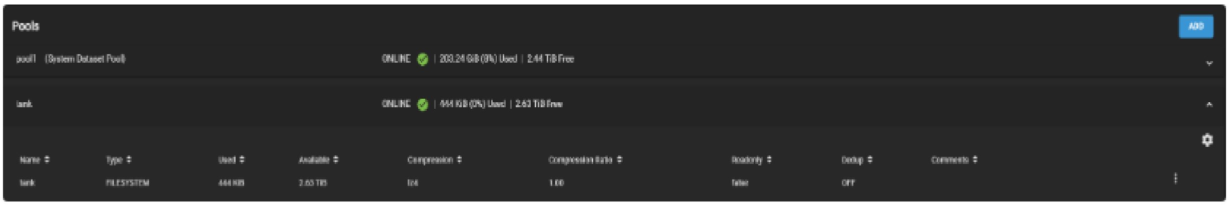
0 selected / 2 total

Mirror
Estimated raw capacity: 2.73 TiB

Estimated total raw data capacity: 2.73 TiB

TrueNAS automatically suggests Mirror as the ideal layout for maximized data storage and protection.

- Review the **Estimated total raw data capacity** and click **CREATE**.
- TrueNAS wipes the disks and adds *tank* to the **Storage > Pools** list.



Pools

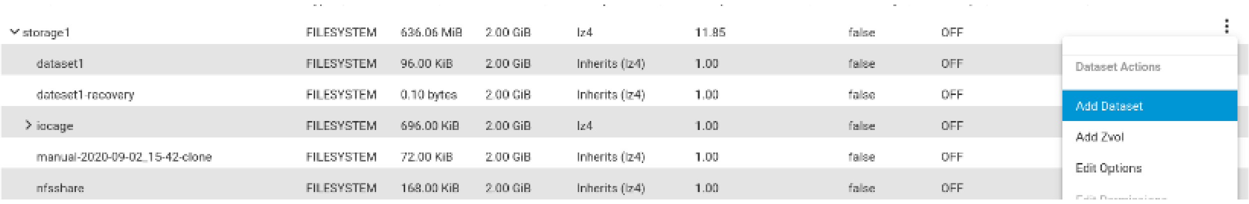
pool1 (System Dataset Pool) ONLINE ✓ | 203.24 GiB (0%) Used | 2.44 TiB Free

tank ONLINE ✓ | 444 KiB (0%) Used | 2.63 TiB Free

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
tank	FILESYSTEM	444 KiB	2.63 TiB	lz4	1.00	false	OFF	

Adding Datasets or Zvols

- New pools have a root dataset that allows further division into new datasets or zvols.
- A dataset is a file system that stores data and has specific permissions.
- A zvol is a virtual block device that has a predefined storage size.
- To create either one, go to Storage > Pools, click , and select Add Dataset or Add Zvol.



storage1	FILESYSTEM	636.06 MiB	2.00 GiB	lz4	11.85	false	OFF
dataset1	FILESYSTEM	96.00 KiB	2.00 GiB	Inherits (lz4)	1.00	false	OFF
dataset1-recovery	FILESYSTEM	0.10 bytes	2.00 GiB	Inherits (lz4)	1.00	false	OFF
iocage	FILESYSTEM	696.00 KiB	2.00 GiB	lz4	1.00	false	OFF
manual-2020-09-02_15-42-clone	FILESYSTEM	72.00 KiB	2.00 GiB	Inherits (lz4)	1.00	false	OFF
nfsshare	FILESYSTEM	168.00 KiB	2.00 GiB	Inherits (lz4)	1.00	false	OFF

These are often created as part of configuring specific data sharing situations:

- A dataset with a Share Type set to SMB optimizes that dataset for the Windows sharing protocol.
- Block device sharing (iSCSI) requires a zvol.
- Organize the pool with additional datasets or zvols according to your access and data sharing requirements before moving any data into the pool.
- When you're finished building and organizing your TrueNAS pools, move on to configuring how the system shares data.

Section 3: Exercises

Exercise 1: Draw Virtualization Reference Model.

Exercise 2: Participate in group discussion on following topics:

a) Types, Advantage and Disadvantages of Virtual Machine
b) Container vs Virtual Machine
c) Benefits, Types and Need of Virtualization

d) VirtualBox Terminologies and Features
e) Deploying the Virtual Machine
f) Creating and Running the Virtual Machine
g) Types and Applications of NAS
h) TrueNAS Installation and Configuration

Section 4: Assessment Questionnaire

1. __________ allow a business to run an operating system that behaves like a completely separate computer in an app window on a desktop.
2. VMs can run multiple operating system environments on a single physical computer. (True/False)
3. Key files that make up a virtual machine include:
4. What are the advantages of virtual Machines?
5. Running multiple virtual machines on one physical machine can result in unstable performance if infrastructure requirements are not met. (True/False)
6. What are the two types of Virtual Machines?
7. A _________ allows a single process to run as an application on a host machine, providing a platform-independent programming environment by masking the information of the underlying hardware or operating system.
8. Virtual machines are smaller and faster to boot than containers. (True/False)
9. ________ is a technique of how to separate a service from the underlying physical delivery of that service.
10. The machine on which the virtual machine is going to be built is known as _________and that virtual machine is referred as a_________.
11. What are the benefits of Virtualization?
12. What are the types of Virtualizations?
13. _______ virtualization is an array of servers that are managed by a virtual storage system.
14. _________ allows the users' OS to be remotely stored on a server in the data centre.
15. What are the five major needs of the virtualization?
16. Oracle ________ is cross-platform virtualization software.
17. What are the clone types?
18. ___________ is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity.
19. __________ are the two main types of networked storage.
20. What are applications of Network-attached Storage (NAS)?

----------End of the Module----------

MODULE 4

Cloud, Web and Security

Section 1: Learning Outcomes

After completing this module, you will be able to:

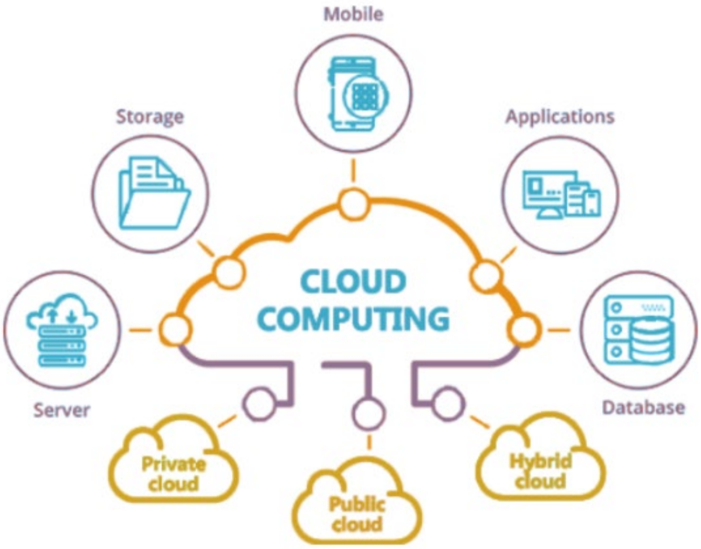
- Explain Concept, Need and Evolution of Cloud Computing
- Describe Concept and Types of Cloud Backup
- Explain Architecture and Working of File Transfer Protocol
- Run FTP Commands
- Define Fundamentals of Domain Name System
- Tell the Concept of DNS Filtering
- Accurately measure the Internet Connection Speed
- Find out reasons for High or Timed Out Ping

Section 2: Relevant Knowledge

4.1 Cloud Backups

Concept of Cloud Computing

- Cloud computing is the delivery of hosting services that are provided to a client over the Internet.
- Enable large-scale services without up-front investment.



What is Cloud Computing?

Cloud Computing is:

- Storing Data/ Application on Remote Servers
- Processing Data/Application from Servers
- Accessing Data/Application from Internet

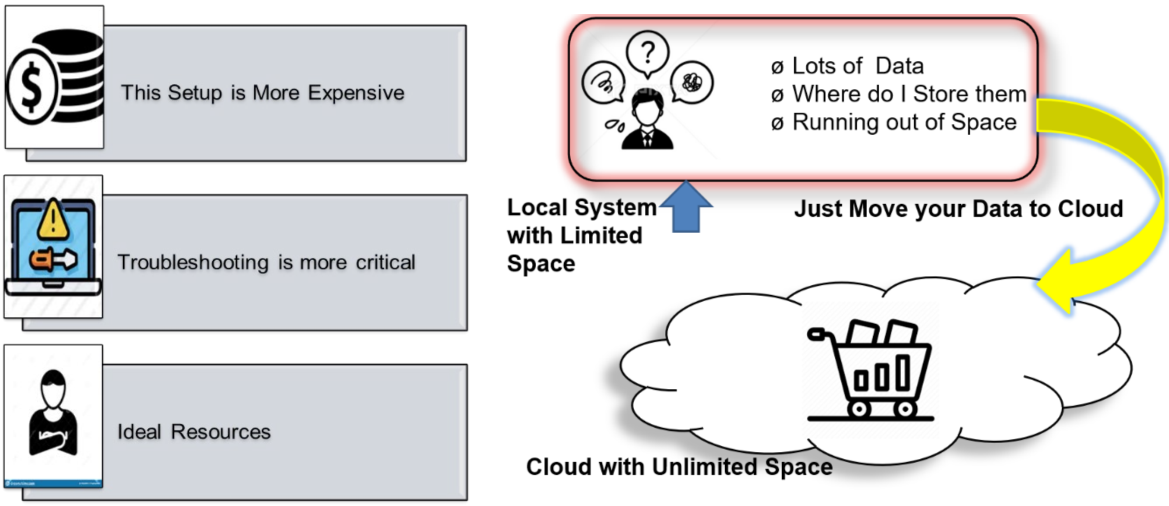
Why Cloud?

If you want to Host a website, following things we required:

- Buy Stack of Servers

- More Traffic: More Server
- Monitor & Maintain Server

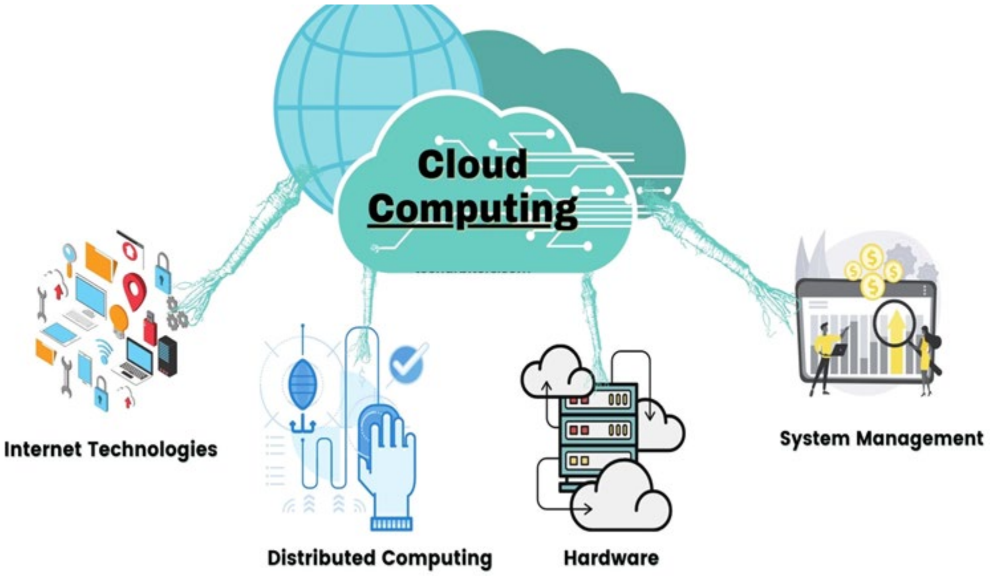
Before Cloud Computing: Disadvantages


This Setup is More Expensive
Troubleshooting is more critical
Ideal Resources
ø Lots of Data
ø Where do I Store them
ø Running out of Space
Local System with Limited Space
Just Move your Data to Cloud
Cloud with Unlimited Space

Roots of Cloud Computing

The roots of clouds computing by observing the advancement of several technologies, especially in:

- Hardware (virtualization, multi-core chips)
- Internet technologies (Web services, service-oriented architectures, Web 2.0)
- Distributed computing (clusters, grids)
- Systems management (autonomic computing, data center automation)



From Mainframes to Clouds

Computing delivered as a utility can be defined as —on demand delivery of infrastructure, applications, and business processes in a security-rich, shared, scalable, and based computer environment over the Internet for a fee.

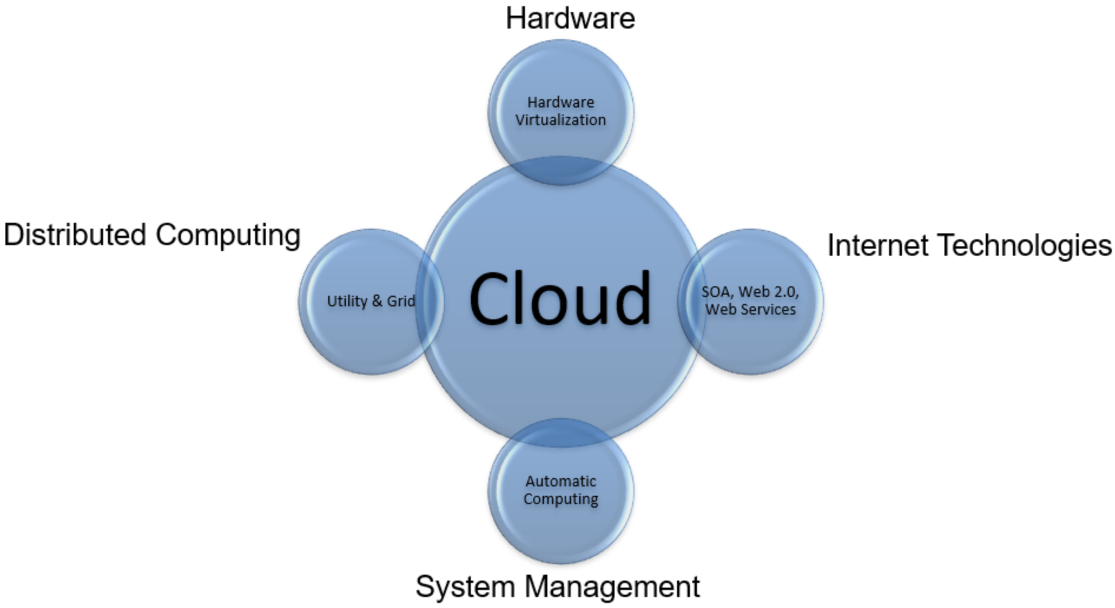
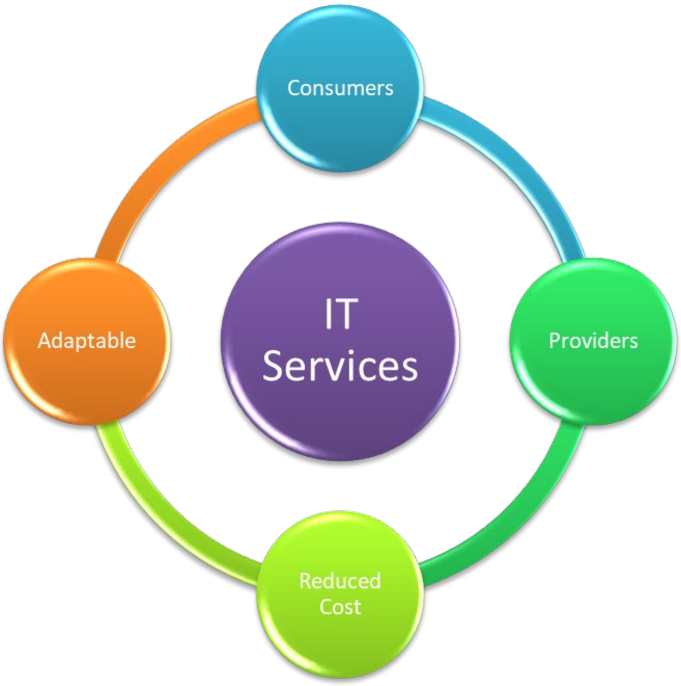
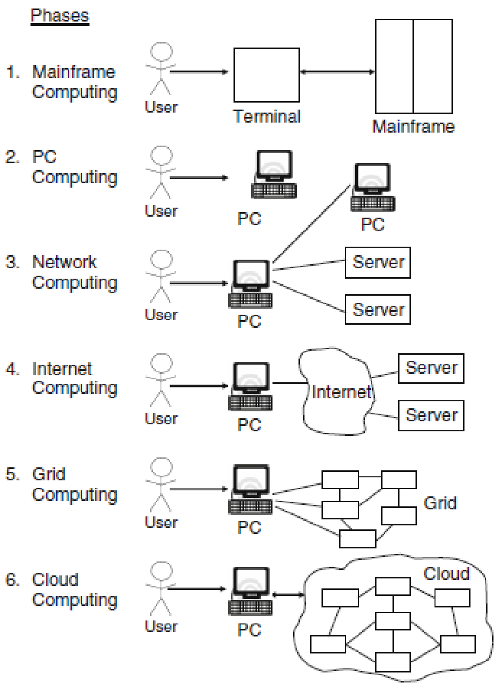


Fig.-Convergence of various advances leading to the advent of cloud computing.

- This model brings benefits to both consumers and providers of IT services.
- Consumers can attain reduction on IT-related costs by choosing to obtain cheaper services from external providers as opposed to heavily investing on IT infrastructure and personnel hiring.
- The on-demand component of this model allows consumers to adapt their IT usage to rapidly increasing or unpredictable computing needs.



- Providers of IT services achieve better operational costs; hardware and software infrastructures are built to provide multiple solutions and serve many users, thus increasing efficiency and ultimately leading to faster return on investment (ROI) as well as lower total cost of ownership (TCO).



- The mainframe era collapsed with the advent of fast and inexpensive microprocessors and IT data centres moved to collections of commodity servers.
- Apart from its clear advantages, this new model inevitably led to isolation of workload into dedicated servers, mainly due to incompatibilities.

Mainframe Era

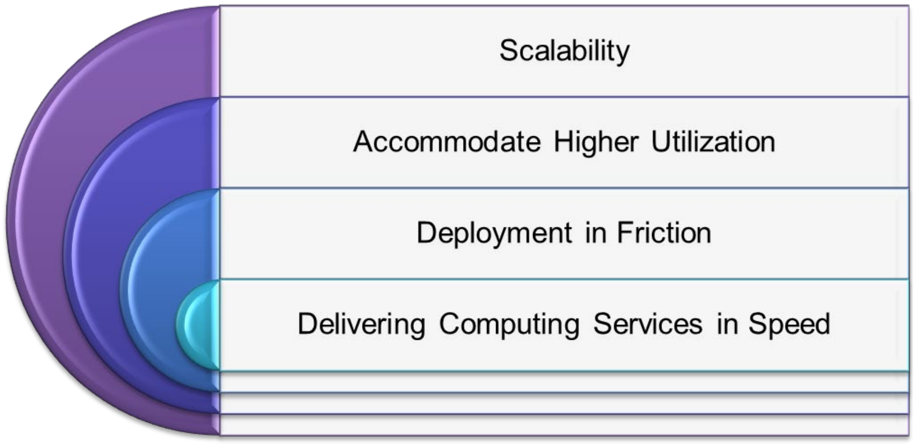
Fast & Inexpensive

IT Data Centres

Collection of Commodity Server

Between software stacks and operating systems

- These facts reveal the potential of delivering computing services with the speed and reliability that businesses enjoy with their local machines.
- The benefits of economies of scale and high utilization allow providers to offer computing services for a fraction of what it costs for a typical company that generates its own computing power.



Scalability

Accommodate Higher Utilization

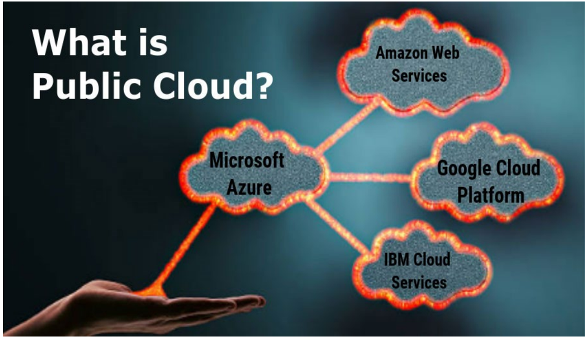
Deployment in Friction

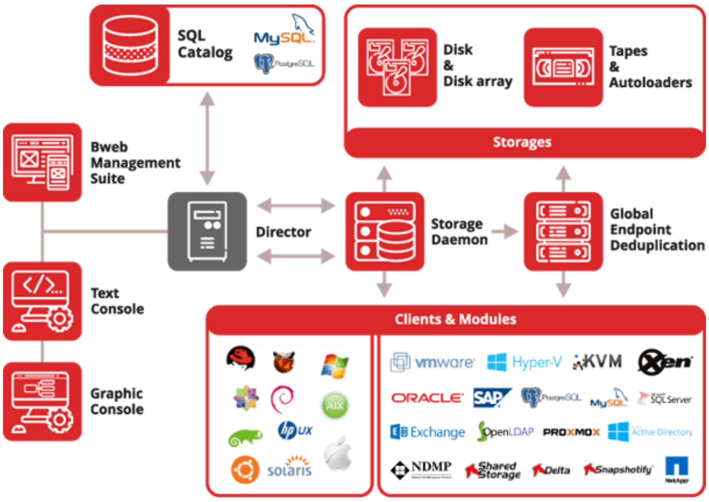
Delivering Computing Services in Speed

What is Cloud Backup?

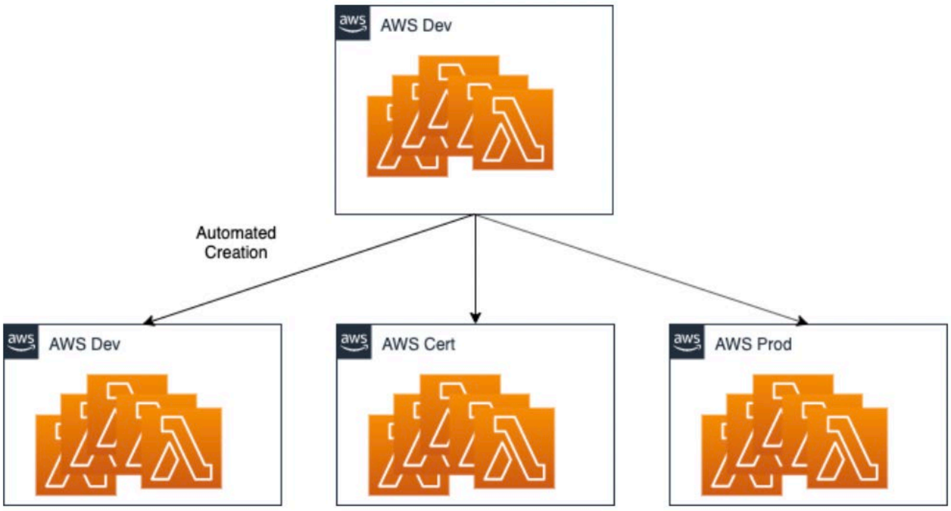
- There are many places you can back up your data files to. One of the simplest forms of computer backup is copying your files to an external drive using a USB cable.

- The next is to backup over a network - if the drive you are backing up to is in a different location, then all the better as this decreases the risk of your files being potentially subject to theft, fire, and flood etc.
- A Cloud backup is where a remote, online, or managed service provides users with a system for backing up, storing, and recovering data files.
- Cloud backup, also known as online backup or remote backup, is a strategy for sending a copy of a physical or virtual file or database to a secondary, off-site location for preservation in case of equipment failure or catastrophe.
- The secondary server and data storage systems are usually hosted by a third-party service provider, who charges the backup customer a fee based on storage space or capacity used, data transmission bandwidth, number of users, number of servers or number of times data is accessed.
- Implementing cloud data backup can help bolster an organization's data protection strategy without increasing the workload of information technology (IT) staff.
- The labor-saving benefit may be significant and enough of a consideration to offset some of the additional costs associated with cloud backup, such as data transmission charges.
- Most cloud subscriptions run on a monthly or yearly basis.
- While initially used mainly by consumers and home offices, online backup services are now commonly used by small and medium-sized businesses (SMBs) as well as larger enterprises to back up some forms of data.
- For larger companies, cloud data backup may serve as a supplementary form of backup.
- Different from traditional web hosting, the services on the cloud are sold on demand, are offered in an elastic manner, meaning the customer can use as much or as little of the service as needed and are managed completely by the service provider.
- A cloud can be private or public.
- A Public Cloud sells services to anyone on the internet, such as how Amazon Web Services (AWS) operates, while a Private Cloud supplies hosted services to a limited number of users.
- In an organization's data center, a backup application copies data and stores it on different media or another storage system for easy access in the event of a recovery situation.
- While there are multiple options and approaches to off-site backup, cloud backup serves as the off-site facility for many organizations.





- In an enterprise, the company might own the off-site server if it hosts its own cloud service, but the chargeback method would be similar if the company uses a service provider to manage the cloud backup environment.
- Backing up directly to the public cloud. One way to store organizational workloads is by duplicating resources in the public cloud. This method entails writing data directly to cloud providers, such as AWS or Microsoft Azure.



- The organization uses its own backup software to create the data copy to send to the cloud storage service.
- The cloud storage service then provides the destination and safekeeping for the data, but it does not specifically provide a backup application.
- Backup software should be capable of interfacing with the cloud's storage service.
- Additionally, with public cloud options, IT professionals may need to look into supplemental data protection procedures.
- Backing up to a service provider. An organization writes data to a cloud service provider that offers backup services in a managed data center.
- The backup software that the company uses to send its data to the service may be provided as part of the service, or the service may support specific commercially available backup applications.

Cloud - to - Cloud Backup

These services are among the newest offerings in the cloud backup arena.

- They specialize in backing up data that already lives in the cloud, either as data created using a software as a service (SaaS) application or as data stored in a cloud backup service.
- As its name suggests, a cloud-to-cloud backup service copies data from one cloud to another cloud.
- The cloud-to-cloud backup service typically hosts the software that handles this process.

Online Cloud Backup

- There are also hardware alternatives that facilitate backing up data to a cloud backup service.
- These appliances are all-in-one backup machines that include backup software and disk capacity along with the backup server.

- The appliances are about as close to plug-and-play as backup gets, and most of them also provide a seamless (or nearly so) link to one or more cloud backup services or cloud providers.
- The list of vendors that offer backup appliances that include cloud interfaces is long, with Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft and Asigra active in this arena.
- These appliances typically retain the most recent backup locally, in addition to shipping it to the cloud backup provider, so that any required recoveries can be made from the local backup copy, saving time and transmission costs.

Have I got a copy of my Cloud data?

- Always be aware that your access to any files stored, backed up, or synced in the Cloud is reliant not only on the robustness and availability of the Cloud service, but also on your own connectivity.
- Always maintain a local backup copy of your data.
- For those on a tight budget you'll find free backup software programs like SyncBackFree that will help protect you against data loss by copying to a local drive.

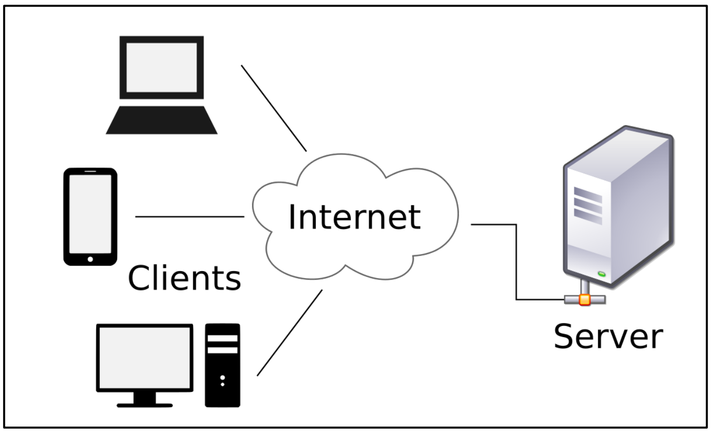
4.2 File Transfer Protocol (FTP)

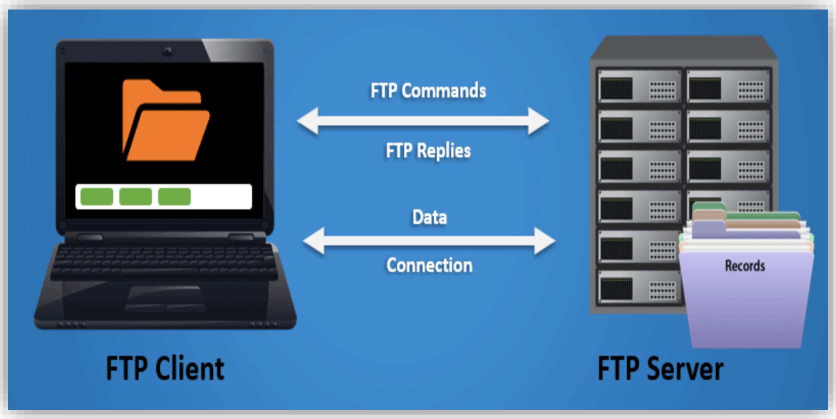
What is FTP?

- FTP means "File Transfer Protocol“.
- It refers to a group of rules (protocol) that govern how computers transfer files from one system to another over the internet.
- Businesses use FTP to send files between computers, while websites use FTP for the uploading and downloading of files from their website's servers.
- FTP is a software which allows every user to install and transfer files or folders from one system to the other.
- FTP is a communications protocol used for transferring or exchanging files between two computers. These transferring of files generally is authenticated by username and password credentials.
- Anonymous FTP allows users to access files, programs and other data from the Internet without the need for a user ID or password.
- Websites are sometimes designed to allow users to use ‘anonymous’ or ‘guest’ as a user ID and an email address for a password.
- FTP is used to encourage the use of remote computers, file sharing and transfers the data more reliably and efficiently.

FTP Architecture

- FTP is built on a client–server model architecture using separate control and data connections between the client and the server





FTP Server

- An FTP server which is also known as an FTP site is a computer having a File Transfer Protocol (FTP) address and is dedicated to receiving an FTP connection and exchanging files over the internet.
- To transfer file from one location to another through TCP/IP network, FTP uses the FTP server to store the data and transfer the file by following basic steps like login, connection, dataset, modes of transfer, security, etc.

FTP Client

- FTP clients are used to upload, download and manage files on a server.
- FTP clients include the following: FileZilla. This is a free FTP client for Windows, macOS and Linux that supports FTP, FTPS and SFTP.
- Many dedicated FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications such as HTML editors and file managers.

Why FTP?

- Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions.
- Two systems may have different ways to represent text and data. Two systems may have different directory structures.
- FTP protocol overcomes these problems by establishing two connections between hosts.
- One connection is used for data transfer, and another connection is used for the control connection.

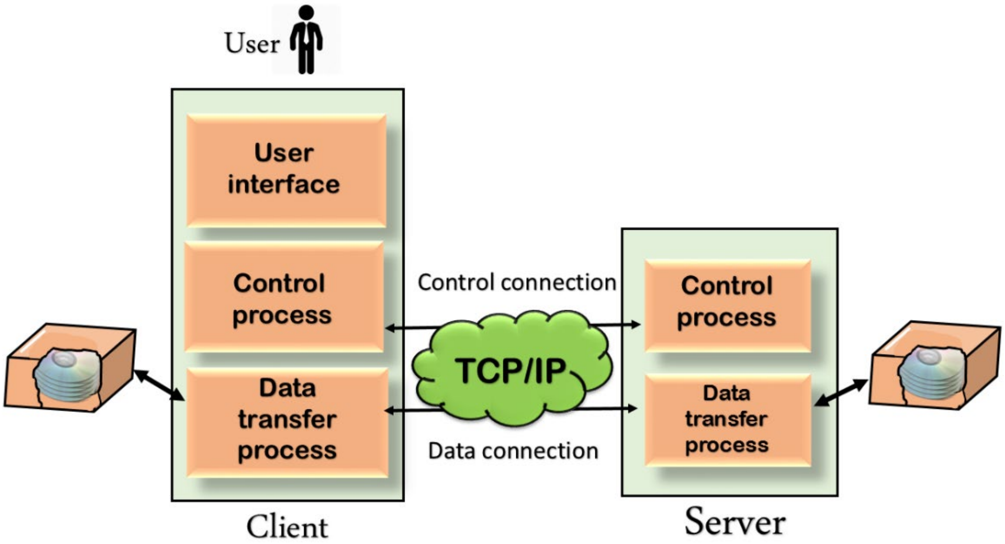
How FTP Works?

- FTP shows a few steps on how to take advantage of transferring personal files such as doc files or other types of files such as MP3 files.
- The way File Transfer Protocol works is by installing the software first on both machines and then simply taking files one by one and shift them.
- The software for FTP can be bought or downloaded from the web browser, however the requirements are a bit different.
- As soon as one file is received, the system confirms it by sending a confirmation message to the system next to it.
- In order to Setup an FTP Service one must do the following:

1. Install FTP software
2. Select file or files which need to be transferred
3. Send file or files by computer networks
4. Final step: File or files start to transfer

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- Control connection is made between control processes while Data Connection is made between FTP uses port 21 for the control connection and Port 20 for the data connection.



Privacy and Security

- Anti-virus and double firewall
- Identity/Data
- Contact/Server
  - Email Address

Advantages

- FTP can be used numerous amounts of time {Unlimited}
- FTP can be used any time of the day
- Files can be transferred without any hassle
- No limit as to how many files or folders can be transferred
- Any type of file or folder can be transferred
- Easy to install on machine

Disadvantages

- Mostly used on Unix and Linux computer systems
- Not compatible with every system and lacks support
- ASCII mode and Binary Mode are used and differ from the way they send data

4.3 Important Commands

FTP Command Prompt and Browser

ftp Command

- The ftp command-line parameters are case-sensitive.
- This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.
- The ftp command can be used interactively. After it is started, ftp creates a sub-environment in which you can use ftp commands. You can return to the command prompt by typing the quit command.
- When the ftp sub-environment is running, it is indicated by the ftp > command prompt. For more information, see the ftp commands.
- The ftp command supports the use of IPv6 when the IPv6 protocol is installed.

Windows Command Prompt

1. On the PC, start the command prompt window.
2. In the command prompt window, type, ftp <hostname> or <IP address>.

For example, ftp keysightVA1

After the command, the window displays instrument information such as model number, serial number hostname, IP address with the last line showing the following:
user (xxx.xxx.xxx.xxx (none)):
Where xxx.xxx.xxx.xxx is the IP address of the instrument.

3. Press Enter
4. If prompted for a password, type in the password.
   The default password from the factory is the empty set, so just press enter when prompted.
   If successful, the window shows the following:
   Successful login
   ftp>
   To see the available FTP commands, type help at the ftp> prompt.
5. At the ftp> prompt, type in the ftp command and press Enter.
6. Type quit or bye to end the session.
7. Type exit to end the command prompt session.

Web Browser

- The web server contains a button that performs the same function so that a URL does not have to be manually entered.

1. On the PC, start the web browser.
2. In the URL address field, type ftp:// <hostname> or <IP address>.
   For example, ftp://keysightVA1
   The web browser displays the FTP root directory.
3. Click USER to display the user directory.

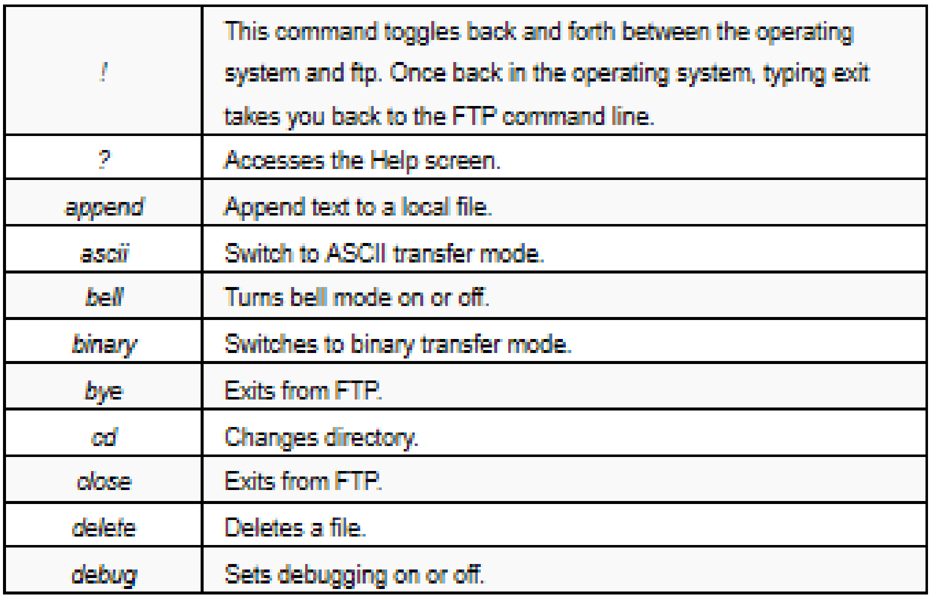
FTP Commands

USER – This command sends the user identification to the server.

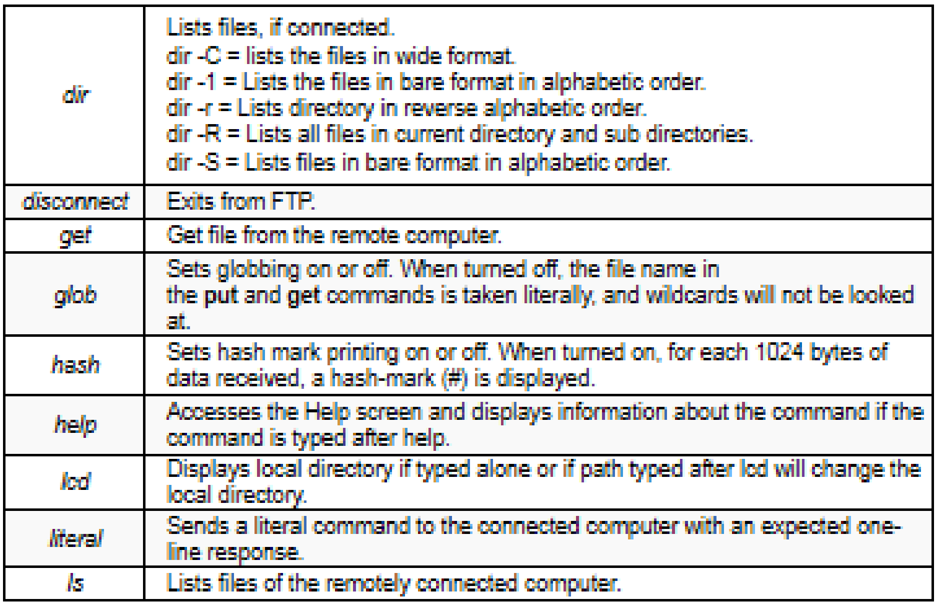
PASS – This command sends the user password to the server.

CWD – This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.
RMD – This command causes the directory specified in the path name to be removed as a directory.
MKD – This command causes the directory specified in the pathname to be created as a directory.
PWD – This command causes the name of the current working directory to be returned in the reply.
RETR – This command causes the remote host to initiate a data connection and to send the requested file over the data connection.
STOR – This command causes to store of a file into the current directory of the remote host.
LIST – Sends a request to display the list of all the files present in the directory.
ABOR – This command tells the server to abort the previous FTP service command and any associated transfer of data.
QUIT – This command terminates a USER and if file transfer is not in progress, the server closes the control connection.

FTP Commands for Windows



!	This command toggles back and forth between the operating system and ftp. Once back in the operating system, typing exit takes you back to the FTP command line.
?	Accesses the Help screen.
append	Append text to a local file.
ascii	Switch to ASCII transfer mode.
bell	Turns bell mode on or off.
binary	Switches to binary transfer mode.
bye	Exits from FTP.
cd	Changes directory.
close	Exits from FTP.
delete	Deletes a file.
debug	Sets debugging on or off.



dir	Lists files, if connected. dir -C = lists the files in wide format. dir -1 = Lists the files in bare format in alphabetic order. dir -r = Lists directory in reverse alphabetic order. dir -R = Lists all files in current directory and sub directories. dir -S = Lists files in bare format in alphabetic order.
disconnect	Exits from FTP.
get	Get file from the remote computer.
glob	Sets globbing on or off. When turned off, the file name in the **put** and **get** commands is taken literally, and wildcards will not be looked at.
hash	Sets hash mark printing on or off. When turned on, for each 1024 bytes of data received, a hash-mark (#) is displayed.
help	Accesses the Help screen and displays information about the command if the command is typed after help.
lcd	Displays local directory if typed alone or if path typed after lcd will change the local directory.
literal	Sends a literal command to the connected computer with an expected one-line response.
ls	Lists files of the remotely connected computer.

mdelete	Multiple delete.
mdir	Lists contents of multiple remote directories.
mget	Get multiple files.
mkdir	Make directory.
mls	Lists contents of multiple remote directories.
mput	Send multiple files.
open	Opens address.
prompt	Enables or disables the prompt.
put	Send one file.
pwd	Print working directory.
quit	Exits from FTP.

quote	Same as the literal command.
recv	Receive file.
remotehelp	Get help from remote server.
rename	Renames a file.
rmdir	Removes a directory on the remote computer.
send	Send single file.
status	Shows status of currently enabled and disabled options.
trace	Toggles packet tracing.
type	Set file transfer type.
user	Send new user information.
verbose	Sets verbose on or off.

FTP Replies

Some of the FTP replies are:

200 Command okay.

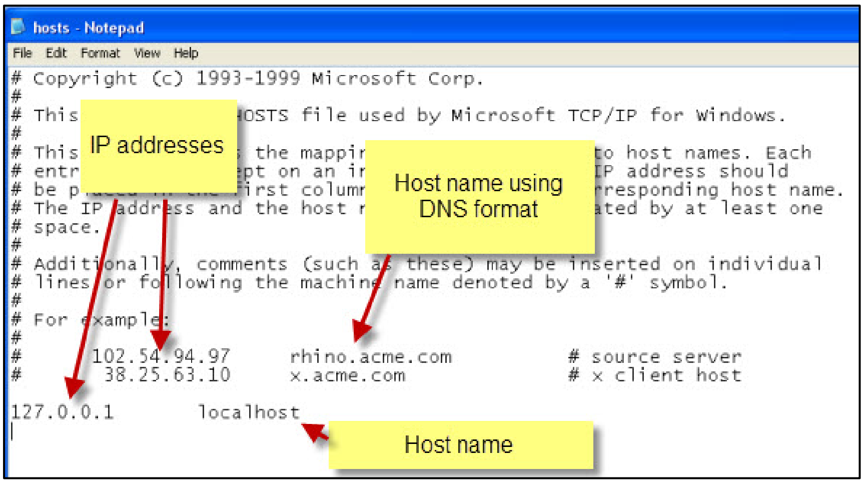
- 530 Not logged in.
- 331 User name okay, need a password.
- 225 Data connection open; no transfer in progress.
- 221 Service closing control connection.
- 551 Requested actions aborted: page type unknown.
- 502 Command not implemented.
- 503 Bad sequences of commands.
- 504 Command not implemented for that parameter.

4.4 DNS Filtering

Domain Name System

- The Domain Name System (DNS) is the phonebook of the Internet.
- Humans access information online through domain names, like nytimes.com or espn.com.
- The Domain Name System is the hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol networks.

- All devices (computers etc) that are connected to the Internet, your own network, or company network are identified by an IP address; which is a number.
- IP addresses are easy for computers to process but they are not so easy for people to remember.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This                 OSTS file used by Microsoft TCP/IP for Windows.
#
# This                 the mappir                       to host names. Each
# entr                 ept on an ir                     IP address should
# be p                 irst columr                      rresponding host name.
# The IP address and the host r                         ated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

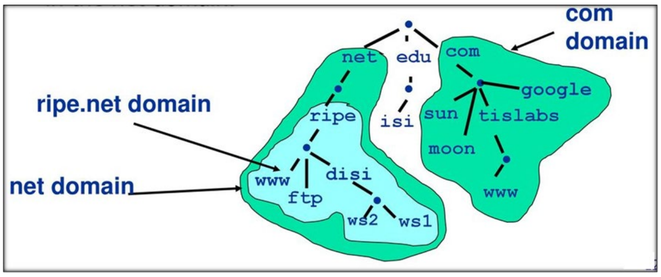
IP addresses

Host name using DNS format

Host name

Purpose of DNS

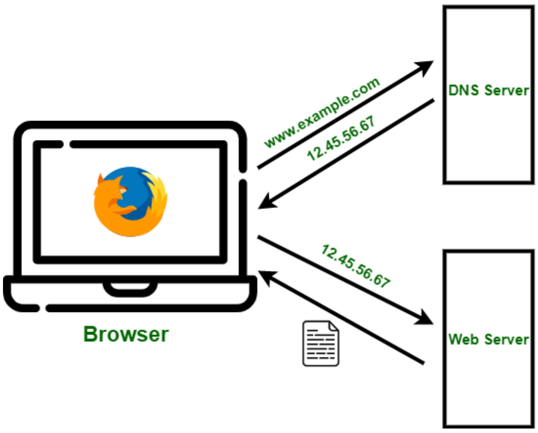
- Domains are “namespaces”
- Everything below .com is in the com domain.
- Everything below ripe.net is in the ripe.net domain and in the net domain.



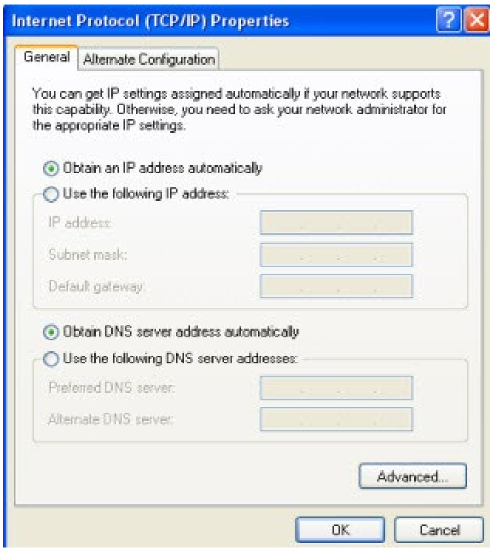
- The Domain Name System matches domain names, like cloudflare.com, to IP addresses, like 192.0.2.24.
- DNS is necessary in order to allow users to access websites without memorizing confusing lists of numbers – just as a person is able to store their friends' phone numbers in their smartphone contacts list instead of memorizing every individual phone number.
- Anytime a user opens up a website or accesses a web application, the process of loading the content only starts after the user's device has looked up the correct IP address.

Domain Name Server

- The DNS system consists of many Domain Name servers that together provide the name to IP address mapping for registered devices (usually servers) on the Internet.
- The main DNS severs (root servers) are owned and managed by a variety of different organizations, and are located mainly in the USA.
- Other companies including ISPs have their own DNS servers which are linked to the root servers in a hierarchical fashion providing a distributed system.



- To access a DNS server you will need the IP address of the DNS server.
- This is usually supplied to you by your ISP (Internet Service Provider).
- Most client computers/devices will be configured to obtain an IP and a DNS server address automatically.



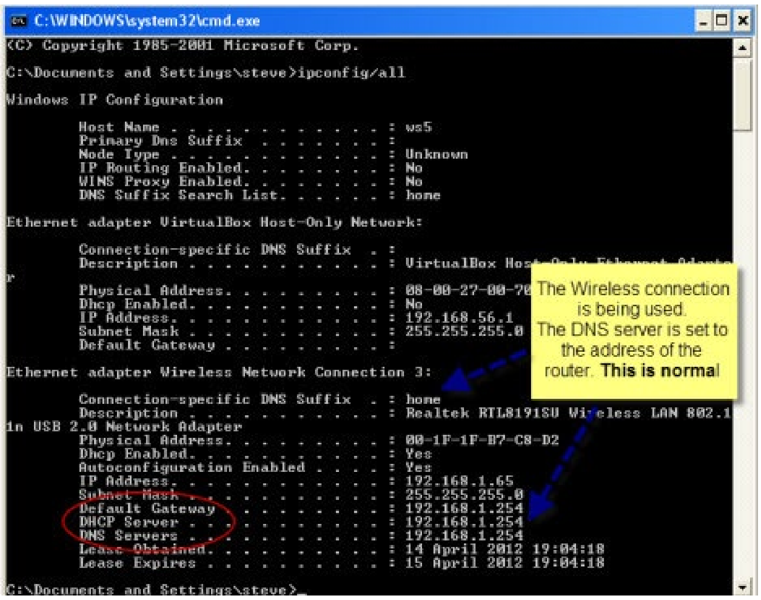
Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

- You can Check what IP address and what DNS address you have been assigned by typing ipconfig/all at the command line.



C:\WINDOWS\system32\cmd.exe

```
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\steve>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : ws5
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : home

Ethernet adapter VirtualBox Host-Only Network:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VirtualBox Hos
r
        Physical Address. . . . . . . . . : 08-00-27-00-70
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.56.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection 3:

        Connection-specific DNS Suffix  . : home
        Description . . . . . . . . . . . : Realtek RTL8191SU Wireless LAN 802.1
1n USB 2.0 Network Adapter
        Physical Address. . . . . . . . . : 00-1F-1F-B7-C8-D2
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.65
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
        DHCP Server . . . . . . . . . . . : 192.168.1.254
        DNS Servers . . . . . . . . . . . : 192.168.1.254
        Lease Obtained. . . . . . . . . . : 14 April 2012 19:04:18
        Lease Expires . . . . . . . . . . : 15 April 2012 19:04:18

C:\Documents and Settings\steve>_
```

The Wireless connection is being used. The DNS server is set to the address of the router. **This is normal**

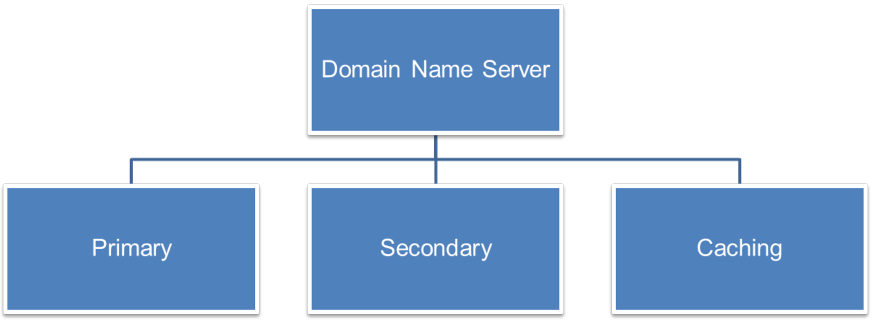
- When queried, a DNS Server will respond in one of three ways:
  - ➢ The server returns the requested name-resolution or IP-resolution data.
  - ➢ The server returns a pointer to another DNS Server that can service the request.
  - ➢ The server indicates that it does not have the requested data.
- Once the user types a domain name into their browser, the user's device creates a DNS query and sends it to a specialized web server called a DNS resolver.
- The DNS resolver matches the queried domain name to an IP address either by querying additional DNS servers or by checking its cache.
- The DNS resolver sends a reply to the user's device with the correct IP address – this is called "resolving" the domain.

Discovering IP Address to Load a Website

- The user's device contacts the server at that IP address to open a connection and begin loading the content.
- DNS is an essential part of accessing web content – no content can load before the DNS process occurs.
- This makes DNS filtering an effective way to exert control over what content users can access.

Types of Domain Name Server

- There are three main kinds of DNS Servers



Primary Server

- The primary server is the authoritative server for the zone.
- All administrative tasks associated with the zone (such as creating subdomains within the zone, or other similar administrative tasks) must be performed on the primary server.
- Any changes associated with the zone or any modifications or additions to RRs in the zone files must be made on the primary server.
- For any given zone, there is one primary server, except when you integrate Active Directory services and Microsoft DNS Server.

Secondary Server

- Secondary servers are backup DNS Servers. Secondary servers receive all of their zone files from the primary server zone files in a zone transfer.
- Multiple secondary servers can exist for any given zone — as many as necessary to provide load balancing, fault tolerance, and traffic reduction.
- Additionally, any given DNS Server can be a secondary server for multiple zones.
- In addition to primary and secondary DNS Servers, additional DNS Server roles can be used when such servers are appropriate for a DNS infrastructure.
- These additional servers are caching servers and forwarders.

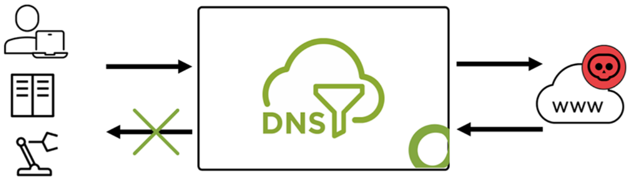
Caching Server

- Caching servers, also known as caching-only servers, perform as their name suggests; they provide only cached-query service for DNS responses.
- Rather than maintaining zone files like other secondary servers do, caching DNS Servers perform queries, cache the answers, and return the results to the querying client.
- The primary difference between caching servers and other secondary servers is that other secondary servers maintain zone files (and do zone transfers when appropriate, thereby generating network traffic associated with the transfer), caching servers do not.
- Most Home users will use the DNS severs provided by their ISP via their home router.

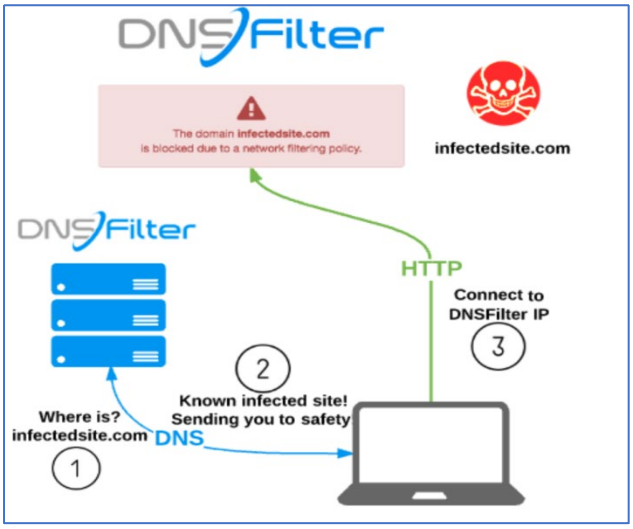
- However, you can use alternative DNS servers like OpenDNS and Google Public DNS.
- This does mean that you will need to manually add these server addresses to your DNS settings.

DNS Filtering

- DNS filtering is the process of using the Domain Name System to block malicious websites and filter out harmful or inappropriate content.



- DNS filtering can help keep malware, or malicious software, out of company networks and off of user devices.
- It can also help block some kinds of phishing attacks.
- This ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks.
- DNS filtering is often part of a larger access control strategy.



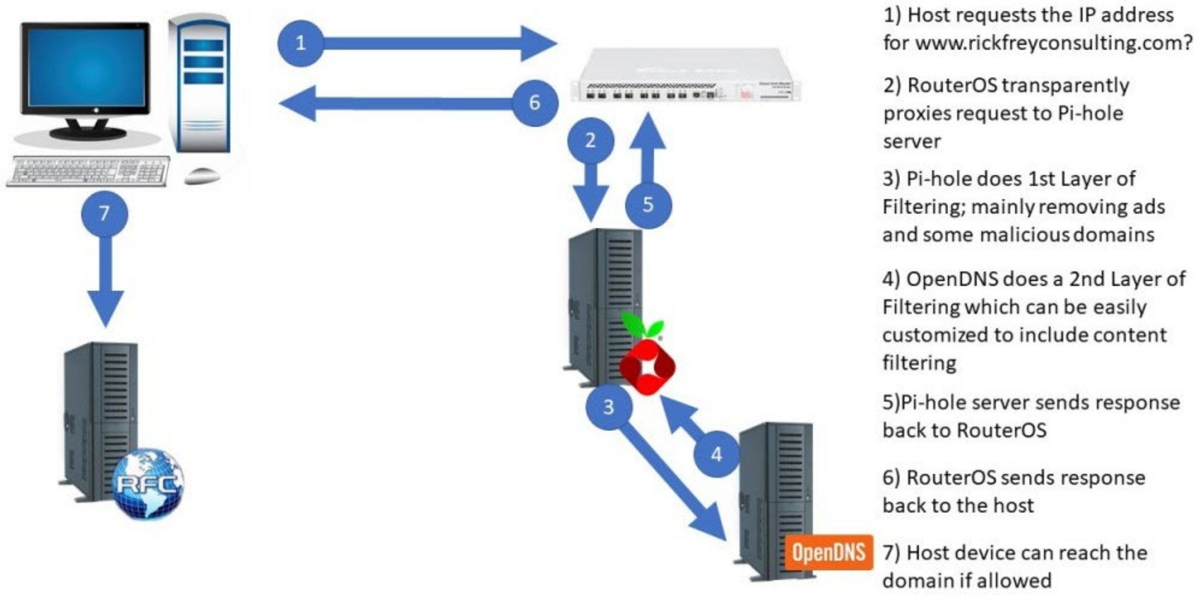
Difference Between Web and DNS Filtering

- Web filtering is a broad term that can refer to a number of methods for controlling web traffic.
- DNS filtering is one type of web filtering.
- Other kinds of web filtering include URL filtering, keyword filtering, and content filtering.

How DNS Filtering Works?

- All DNS queries go to a DNS resolver. Specially configured DNS resolvers can also act as filters by refusing to resolve queries for certain domains that are tracked in a blocklist, thus blocking users from reaching those domains.
- DNS filtering services can also use an allow list instead of a blocklist.
- A blocklist is a list of known harmful domains or IP addresses.
- Suppose a company employee receives a phishing email and is tricked into clicking a link that leads to malicious-website.com.
- Before the employee's computer loads the website, it first sends a query to the company's DNS resolving service, which uses DNS filtering.

- If that malicious site is on that company's blocklist, the DNS resolver will block the request, preventing malicious-website.com from loading and thwarting the phishing attack.
- DNS filtering can blocklist web properties either by domain name or by IP address:
- **By domain:** The DNS resolver does not resolve, or look up, the IP addresses for certain domains at all.
- **By IP address:** The DNS resolver attempts to resolve all domains, but if the IP address is on the blocklist, the resolver will not send it back to the requesting device.



1) Host requests the IP address for www.rickfreyconsulting.com?

2) RouterOS transparently proxies request to Pi-hole server

3) Pi-hole does 1st Layer of Filtering; mainly removing ads and some malicious domains

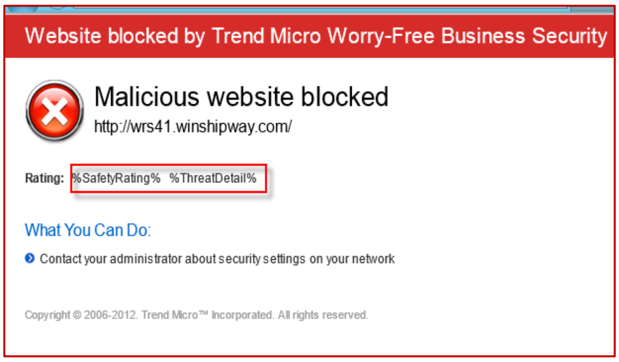
4) OpenDNS does a 2nd Layer of Filtering which can be easily customized to include content filtering

5)Pi-hole server sends response back to RouterOS

6) RouterOS sends response back to the host

7) Host device can reach the domain if allowed

- A website that hosts malware can either attempt to trick users into downloading a malicious program, or execute a drive-by download: a download of a malicious piece of software that is automatically triggered when the webpage loads.
- A number of other attacks are possible as well.
- For instance, webpages run JavaScript code, and as a full programming language, JavaScript can be used in a range of ways to compromise user devices.
- These capabilities are dependent upon the DNS filtering system knowing to identify the malicious IP addresses or domains as bad.
- While DNS filtering can block this malicious activity, attackers generate new domains very quickly and it is not possible to blocklist all of them.



Website blocked by Trend Micro Worry-Free Business Security

Malicious website blocked
http://wrs41.winshipway.com/

Rating: %SafetyRating% %ThreatDetail%

What You Can Do:

- Contact your administrator about security settings on your network

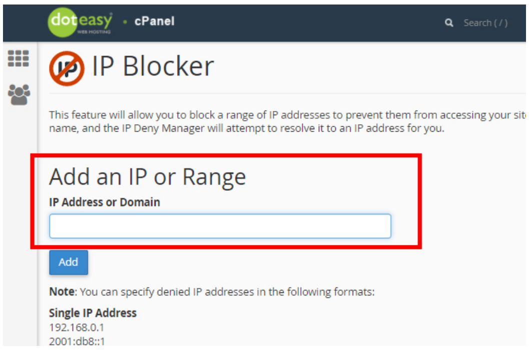
Copyright © 2006-2012. Trend Micro™ Incorporated. All rights reserved.

Blocking Phishing Websites

- A phishing website is a fake website that is set up to steal login credentials in phishing attacks.
- The domain used could be a spoofed domain or just an official-looking domain that most users will not think to question.
- Regardless of the method, the goal is to fool the user into giving their account credentials to an attacker.
- These websites can be blocked using DNS filtering.

Blocking Prohibited Content

- The process for restricting access to certain kinds of content is similar to the process described above; IP addresses or domain names that are known to host prohibited content are block listed, and users cannot access them.
- Alternatively, company-approved websites can be added to an allow list, with DNS filtering blocking all other websites.



IP Blocker

This feature will allow you to block a range of IP addresses to prevent them from accessing your sit
name, and the IP Deny Manager will attempt to resolve it to an IP address for you.

Add an IP or Range

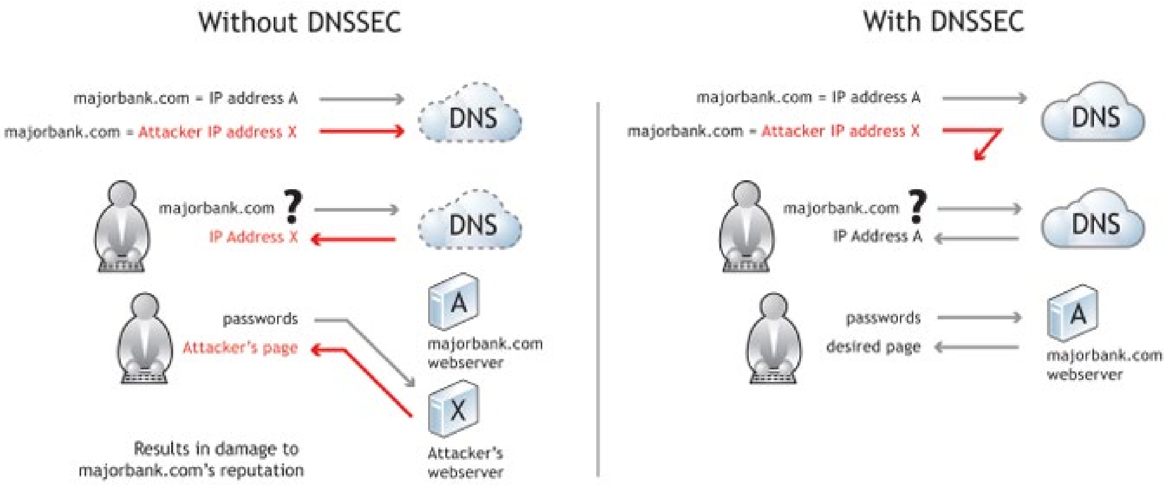
IP Address or Domain

Note: You can specify denied IP addresses in the following formats:

Single IP Address
192.168.0.1
2001:db8::1

Secure DNS Servers

- A secure DNS server is a DNS resolver that blocks malicious or prohibited websites as part of a DNS filtering service.
- Some secure DNS servers also offer increased privacy to protect user data; Cloudflare, for example, offers a DNS resolving service called 1.1.1.1 that purges all DNS query logs after 24 hours.
- Along with DNS filtering, there are additional ways of making the DNS process more secure, since DNS was not designed with security in mind.
- The DNSSEC protocol helps verify that DNS resolvers provide accurate information and have not been compromised by an attacker.



4.5 Measuring Connection Speed

Broadband Speed

- Broadband speeds are measured in 'megabits per second', often shortened to Mb Mbits p/s or Mbps.
- Bits are tiny units of data, with a megabit representing a million of them.
- The higher the number of Mbps (megabits per second) you have, the speedier your online activity should be.

- A high number should mean that downloads complete more quickly, webpages load faster, streaming of music or videos begins more rapidly and any video calls or online games played should display smoothly.

Global Median Speeds on Mobile - August 2022

No.	Country	Mbps
1	Norway	122
2	United Arab Emirates	118
3	Qatar	114
4	South Korea	112
5	Denmark	103
6	Netherlands	102
7	Bulgaria	95
8	Kuwait	94
9	China	92
10	Saudi Arabia	91
117	India	13.52

Global Median Speeds on Fixed Broadband - August 2022

No.	Country	Mbps
1	Singapore	219
2	Chile	211
3	Thailand	188
4	Hong Kong (SAR)	179
5	China	178
6	United States	167
7	Macau (SAR)	157
8	Denmark	156
9	New Zealand	133
10	Japan	131
78	India	48

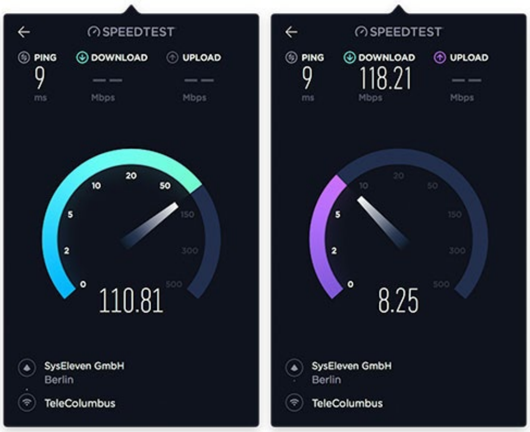
Measuring Connection Speed

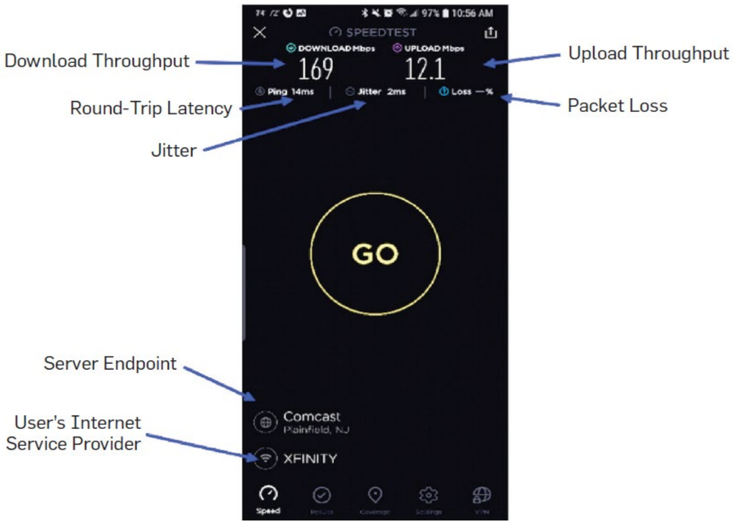
Broadband Speed

Internet connection speed	Time to load a typical web page	Time to download a typical 5 minute song	Streaming video quality
56k dial-up modem	14 seconds	12 mins 30 secs	Low quality
256k broadband	3 seconds	3 mins	
512k broadband	1.6 seconds	1 min 30 secs	
1Mbps broadband	0.8 seconds	41secs	
2Mbps broadband	0.4 seconds	20 secs	Medium quality
4Mbps broadband	0.1 seconds	5 secs	
6Mbps broadband	Instant	3.5 secs	
8Mbps broadband	Instant	2.5 secs	TV quality
12Mbps broadband	Instant	1 sec	
24Mbps broadband	Instant	Instant	Superfast
50Mbps broadband	Instant	Instant	
100Mbps broadband	Instant	Instant	
+100Mbps broadband	Instant	Instant	Ultrafast

Ookla SpeedTest

- This service can measure your connection's ping response and download and upload speeds from a remote server.
- It’s a good idea to conduct the test at more than one site.



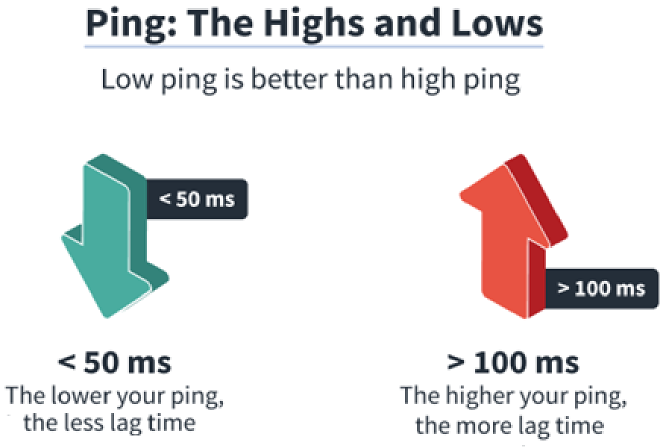


Tips for Accurate Results

- **Connect with wires** - For the most accurate results, your computer should be connected to your router using an Ethernet cable.
- **Disconnect other wireless devices** - Make sure no other devices or people use the broadband connection during the speed test.
- For the best results, close all other programs and internet browsers running on your computer and stop any active downloads.
- Be sure to run multiple tests over several days at different times.
- You also might find specific periods when it’s slow, depending on your area’s network congestion.
- This will give you an overall picture of your connection speed.
- Do multiple tests and if the average of the results is only about 5-10 Mbps off, then that should be tolerable.
- Factors like congestion during peak times and your distance from the relay hardware will contribute to slight variations on your speed.
- (For more accuracy, you could turn your Wi-Fi radios off during the wired tests.)
- If your wired results are way lower than advertised, a consistent 20 to 30 Mbps difference, perhaps, then there might be something else going on. Check your hardware and see if it’s compatible with your provider’s recommendations.

4.6 Ping Issues

- If you can't ping other computers in your network, it's always a big problem because it's a sign of lost connection.
- You will also not be able to share files in your network.
- A failed response indicates that a connection is broken somewhere.



Ping: The Highs and Lows

Low ping is better than high ping

< 50 ms
> 100 ms
< 50 ms
The lower your ping, the less lag time
> 100 ms
The higher your ping, the more lag time

Reasons your Ping might be High or Timed Out

Some reasons your ping might be high include:

- Routers and how updated they are, where they’re placed, and whether their firmware is up to date.
- Computers and whether they’re outdated, un-optimized for gaming, or need to be cleaned.
- Caches on your router or modems whether they’re full.
- Internet service provider connection quality
- The number of devices your network is supporting
- A Application’s settings and whether they’re over-optimized
- Applications and programs running in the background on your device
- Auto-updates that go into effect during your operations
- Firewall configuration (Probably your firewall is blocking ICMP echo request (ping) requests on your public IP address)
- Loss of Connection (Media not available)

Troubleshoot Ping Problems

Follow following steps to lower your internet connection speed and in turn lower the ping:

Conduct computer maintenance

Revisit your router setup

Run an internet speed test

Section 3: Exercises

Exercise 1: Draw flow chart of computing starting from Mainframe to Cloud.

Exercise 2: Fill the following ftp commands table:

cd	
lcd	
mkdir	
pwd	
type	

Exercise 3: Participate in group discussion on following topics:

a) Concept, Need and Evolution of Cloud Computing
b) Concept and Types of Cloud Backup
c) Architecture and Working of File Transfer Protocol
d) FTP Commands
e) Domain Name System
f) DNS Filtering
g) Tips for accurate measurement of internet connection speed
h) Reasons for Ping High or Timed Out

Section 4: Assessment Questionnaire

1. __________ is the delivery of hosting services that are provided to a client over the Internet.
2. What is Cloud Computing?
3. A __________ is where a remote, online, or managed service provides users with a system for backing up, storing, and recovering data files.
4. A _________ sells services to anyone on the internet, such as how Amazon Web Services (AWS) operates, while a _______ supplies hosted services to a limited number of users.
5. Which service copies data from one cloud to another cloud?
6. __________ refers to a group of rules (protocol) that govern how computers transfer files from one system to another over the internet.
7. What is FTP Server?
8. _________ are used to upload, download and manage files on a server.
9. FTP creates two processes such as:
10. What are the advantages of FTP?
11. All devices that are connected to the Internet are identified by an IP address. (True/False)
12. What are three main kinds of DNS Servers?
13. _______ servers are backup DNS Servers.
14. _________ is the process of using the Domain Name System to block malicious websites and filter out harmful or inappropriate content.
15. DNS filtering can blocklist web properties either by _________ or by ___________.
16. Phishing websites cannot be blocked using DNS filtering. (True/False)
17. A secure DNS server is a _________ that blocks malicious or prohibited websites as part of a DNS filtering service.
18. Broadband download speed is always less than upload speed. (True/False)
19. For the most accurate speed test results, your computer should be connected to your router using an:
20. Low Ping is better than High Ping. (True/False)

----------End of the Module----------

MODULE 5

Monitoring

Section 1: Learning Outcomes

After completing this module, you will be able to:

- Explain significance of monitoring in Helpdesk operations
- Describe Types of IT Monitoring
- Tell IT Monitoring Strategies and Best Practices
- Explain Benefits and Implementation of Continuous Monitoring
- Describe Features, Application and Benefits of Nagios
- Draw Architecture of Nagios
- Explain about Nagios Plugins and Products
- Install Nagios at AWS
- Brief on Advanced Monitoring Tools

Section 2: Relevant Knowledge

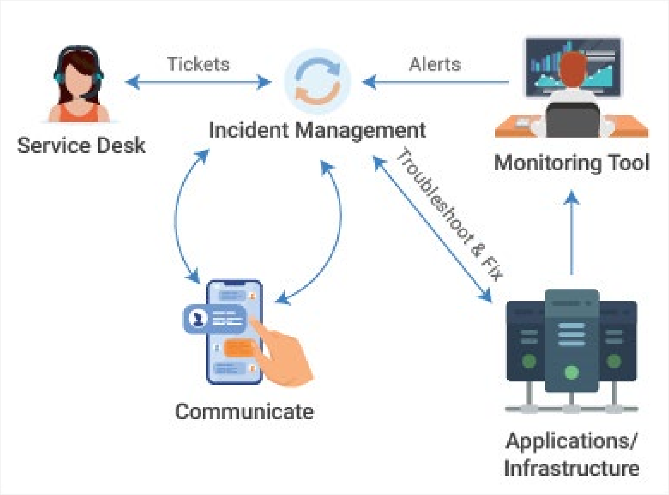
5.1 Introduction to IT Monitoring

What is Monitoring?

- Monitoring means observing and checking the progress or quality of something over a period of time.
- During monitoring, a system is kept under systematic review.
- It ensures regular observation and recording of activities taking place in a project or programme.
- Monitoring can also be defined as systematic and purposeful observation.

Helpdesk Monitoring

- Complete and thorough help desk monitoring involves focusing less on cost minimization and more on delivering excellent customer support.
- It is very important to ensure that IT team is able to provide excellent services and proactive support.
- Communication plays a vital role in this regard. However, integration of all helpful features is necessary, to include a fast ticketing system, self-help portal, SSL security features etc..
- The first win is that IT team will achieve excellence in providing great support and constantly looking for opportunities to help users before waiting for them to report problems.
- Helpdesk monitoring is so successful that customers do not feel frustrated when things go wrong.



Tips for Better Helpdesk Reporting and Monitoring

1. Identify Key Reporting Metrics

- **Ticket closure -** How many tickets is the help desk closing over a period of time?
- **Time-to-resolution -** How long, on average, does it take to resolve a ticket?
- **Incidents by category -** Where are teams spending the most time? What types of incidents are slowing down employee productivity?
- **SLA compliance -** How often is the help desk breaching targets for individual tickets?
- **Customer satisfaction (CSAT) -** Did the service live up to expectations for the end user?

2. Set Goals for Service Delivery
3. Measure and Respond to Customer Satisfaction (CSAT)
4. Create Actionable Help Desk SLAs
5. Automate Help Desk Report Distribution

What is IT Monitoring?

- IT monitoring comprises a broad class of products designed to let analysts determine whether IT equipment is online and performing to expected service levels, while resolving any detected problems.
- IT monitoring is the process to gather metrics about the operations of an IT environment's hardware and software to ensure everything functions as per fixed standards.

Types of IT Monitoring

The basic types of IT monitoring include:

- ➢ Availability Monitoring
- ➢ Web Performance Monitoring
- ➢ Application Performance Management
- ➢ API Management
- ➢ Real User Monitoring
- ➢ Security Monitoring
- ➢ Business Activity Monitoring
- ➢ Real Time Monitoring
- ➢ Trends Monitoring
- ➢ Point-in-time Monitoring
- ➢ IT Infrastructure Monitoring
- ➢ Network Monitoring

Availability Monitoring

- Often referred to as system monitoring, availability monitoring is arguably the most mature type of IT monitoring tool.
- This is designed to provide users with information about uptime and the performance of whatever is being monitored.
- Including categories such as:
  - ➢ Server management
  - ➢ Infrastructure monitoring/management
  - ➢ Network monitoring/management

Web Performance Monitoring

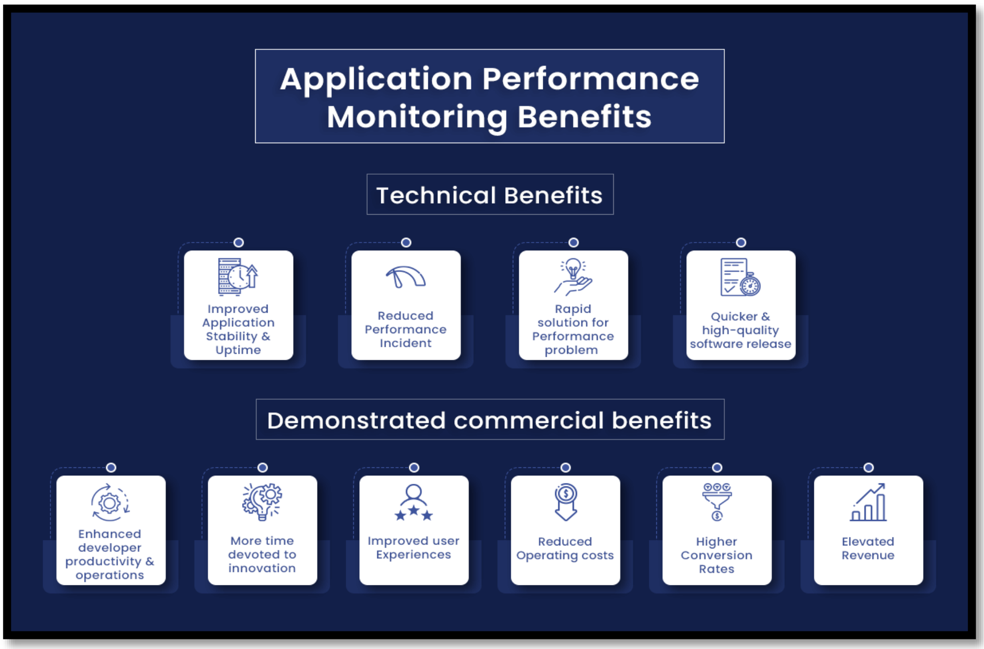
- A subset of availability monitoring, web performance monitoring is designed to monitor the availability of a web server or service, but also adds more fine-grained detail to the system.
- These tools can capture information such as page loading time, the location of errors that are generated, and individual load times of various web elements, helping analysts to fine-tune a website or a web-based app's performance.

Application Management/Application Performance Management (APM)

- Application performance monitoring (APM) gathers software performance metrics based on both end user experience and computational resource consumption.
- APM tools are similar to web performance monitoring tools, but they're designed with customer-facing applications in mind, allowing analysts to track the performance of an application and spot any issues before they become too severe for the user base.
- More modern APM tools can include automated routines to troubleshoot these issues without the intervention of a human developer.
- Examples of APM-provided metrics include average response time under peak load, performance bottleneck data and load and response times.

Benefits of Application Performance Monitoring

- An application performance monitor helps you track various metrics like:
  - ➢ Application Response Time
  - ➢ Throughput
  - ➢ Errors
  - ➢ Exceptions in real time



Application Performance Monitoring Benefits

Technical Benefits

- Improved Application Stability & Uptime
- Reduced Performance Incident
- Rapid solution for Performance problem
- Quicker & high-quality software release

Demonstrated commercial benefits

- Enhanced developer productivity & operations
- More time devoted to innovation
- Improved user Experiences
- Reduced Operating costs
- Higher Conversion Rates
- Elevated Revenue

How does an Application Performance Monitoring tool work?

- Application performance monitoring tools work by tracking the time taken by functions in your application code in real time.
- Typically, a monitoring agent is installed in the app servers that then instruments and collects performance metrics of key functions in well-known frameworks.

- The agent also allows customizing the instrumentation via configuration or API and groups the metrics by their event source, usually an HTTP/API request or a service/database call, to provide a bird's-eye view of the health and performance bottlenecks in the application.

Best Practices for Application Performance Monitoring

- To ensure the best outcome for your monitoring efforts, it is important to follow a set of rules, or rather best practices. Before you begin your monitoring journey:
  - Identify critical business functions and evaluate your needs and requirements.
  - Compare and analyze various vendors. Check if they are cloud-based, on-premises, are available on multiple platforms, and can integrate well with your existing tools and technologies.
  - Ensure that the tool can be customized to best fit your monitoring needs.
  - Ensure that your tool vendor has the resources and a great support team to help answer all your questions and accommodate your requests.

API Monitoring

- Enterprises that offer APIs to third-party developers will find it crucial to ensure the uptime of these services.
- API monitoring tools and monitoring software provide insight into whether an API is working properly, ensuring minimal downtime.

Real User Monitoring (RUM)

- Real user monitoring is designed to record actual end-user interactions with a website or application.
- By monitoring real-world load times and user behavior, it can pinpoint problems based on “real” user experience challenges, as opposed to simulations.
- This type of monitoring is designed to be backward-looking, not predictive, allowing analysts to spot problems only after they occurred.

Security Monitoring

- Security monitoring focuses on the detection and prevention of intrusions, typically at the network level.
- This includes monitoring for vulnerabilities, logging network access and identifying traffic patterns in real time to look for potential breaches.

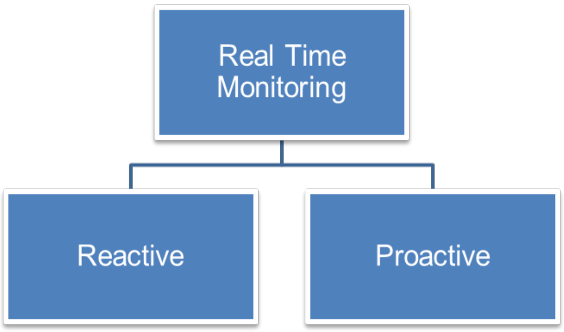
Business Activity monitoring (BAM)

- This type of monitoring tool takes key business performance metrics and tracks them over time.
- For example, these metrics could include information about retail sales, application downloads or the volume of financial transfers.

Real Time Monitoring

- Real-time monitoring is a technique whereby IT teams use systems to continuously collect and access data to determine the active and ongoing status of an IT environment.
- Measurements from real-time monitoring software depict data from the current IT environment, as well as the recent past, which enables IT managers to react quickly to current events in the IT ecosystem.
- Two extensions of real-time monitoring are reactive monitoring and proactive monitoring.
- The key difference is that reactive monitoring is triggered by an event or problem, while proactive monitoring seeks to uncover abnormalities without relying on a trigger event.

- The proactive approach can enable an IT staff to take action to address an issue, such as a memory leak that could crash an application or server, before it becomes a problem.

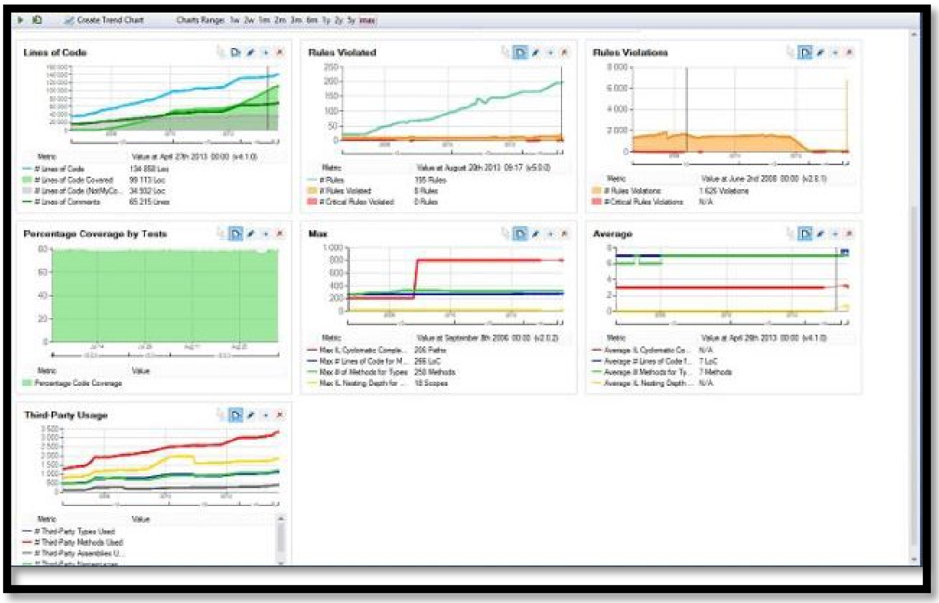

Real Time Monitoring

Reactive

Proactive

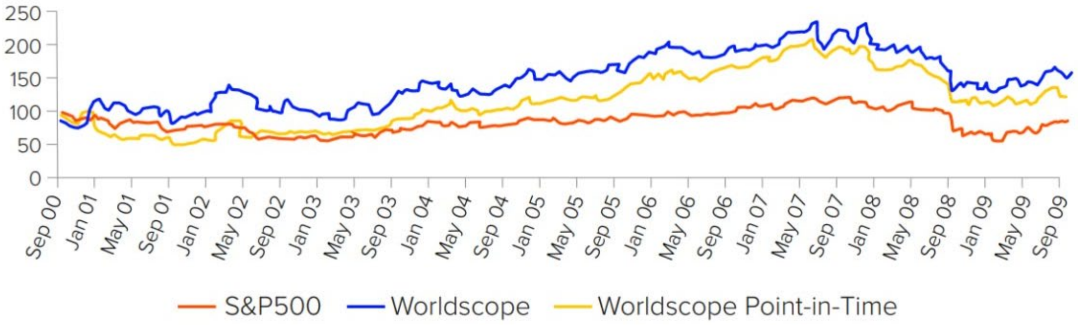
Trends Monitoring

- Historical monitoring data enables the IT manager to improve the environment or identify potential complications before they occur, because they identify a pattern or trend in data from a period of operation.
- Trend analysis takes a long-term view of an IT ecosystem to determine system uptimes, service-level agreement adherence and capacity planning.



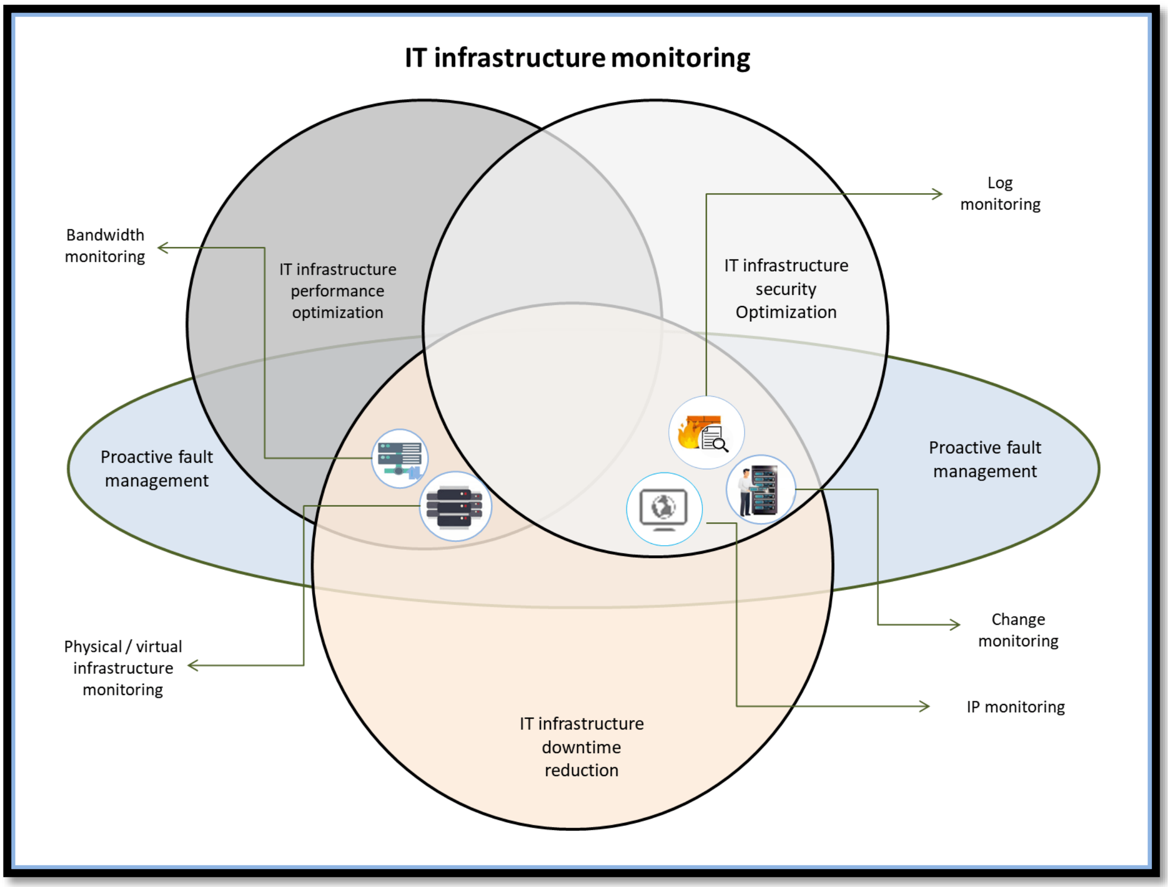
Point-in-time Monitoring

- Point-in-time analysis examines one specific event at a particular instant.
- It can be used to identify a problem that must be fixed immediately, such as a 100% full disk drive.
- Point-in-time analysis relies on fixed thresholds, while time-series analysis employs variable thresholds to paint a broader picture and better detect and even predict anomalies.



IT infrastructure Monitoring

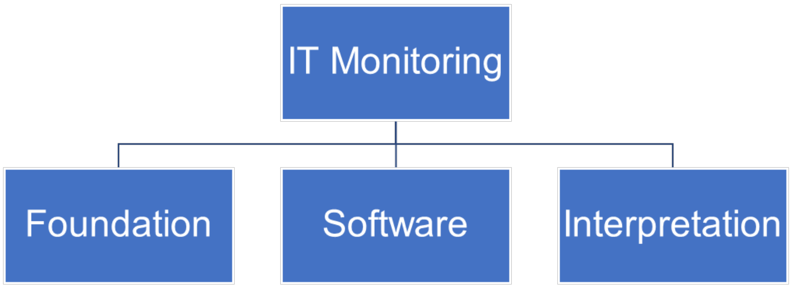
- IT infrastructure monitoring is a foundation-level process that collects and reviews metrics concerning the IT environment's hardware and low-level software.
- Infrastructure monitoring provides a benchmark for ideal physical systems operation, therefore easing the process to fine-tune and reduce downtime, and enabling IT teams to detect outages, such as an overheated server.
- Server monitoring and system monitoring tools review and analyze metrics, such as server uptime, operations, performance and security


IT infrastructure monitoring
Bandwidth monitoring
IT infrastructure performance optimization
IT infrastructure security Optimization
Log monitoring
Proactive fault management
Proactive fault management
Physical / virtual infrastructure monitoring
Change monitoring
IP monitoring
IT infrastructure downtime reduction

Network Monitoring

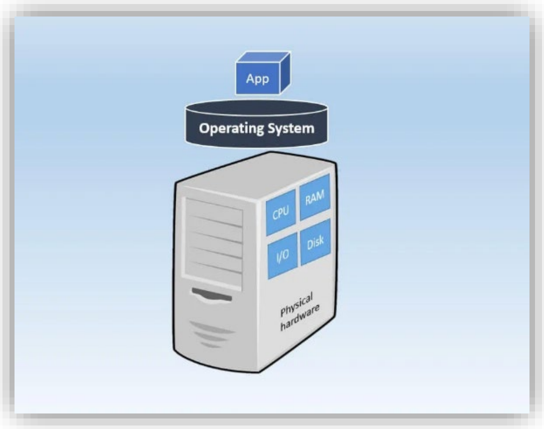
- Network monitoring seeks out issues caused by slow or failing network components or security breaches.
- Metrics include response time, uptime, status request failures and HTTP/HTTPS/SMTP checks.

Monitoring Entities



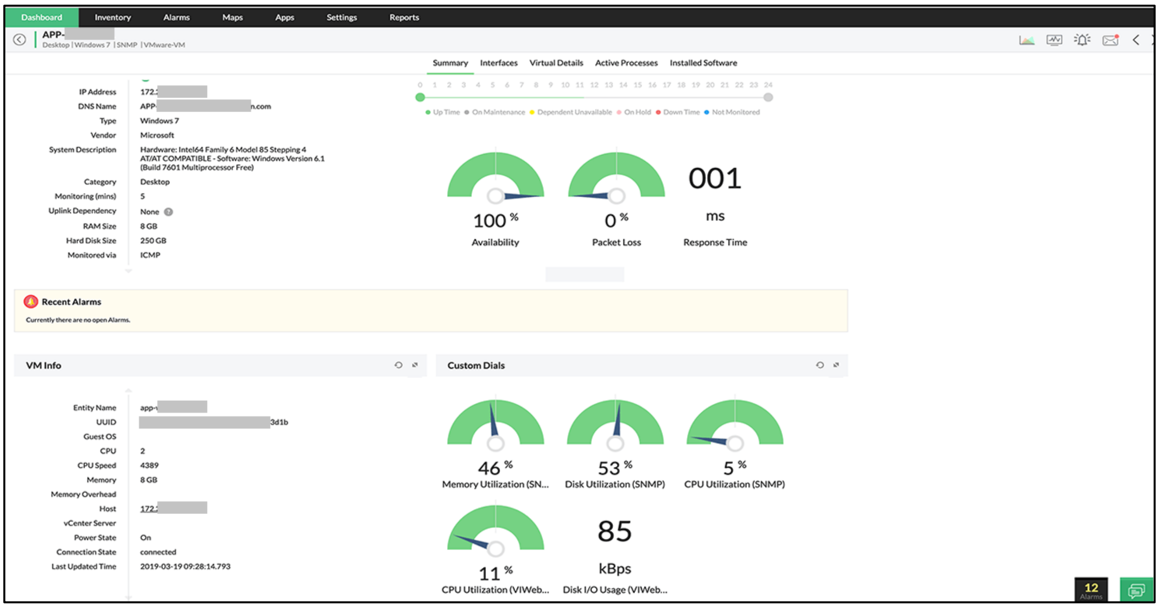
Foundation

- The infrastructure is the lowest layer of a software stack and includes physical or virtual devices, such as servers, CPUs and VMs.



Software

- This part is sometimes referred to as the monitoring section and it analyzes what is working on the devices in the foundation, including CPU usage, load, memory and a running VM count.



APP-[redacted]
Desktop | Windows 7 | SNMP | VMware-VM

IP Address	172.[redacted]
DNS Name	APP-[redacted]n.com
Type	Windows 7
Vendor	Microsoft
System Description	Hardware: Intel64 Family 6 Model 85 Stepping 4 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)
Category	Desktop
Monitoring (mins)	5
Uplink Dependency	None
RAM Size	8 GB
Hard Disk Size	250 GB
Monitored via	ICMP

100 % Availability

0 % Packet Loss

001 ms Response Time

Recent Alarms

Currently there are no open Alarms.

VM Info

Entity Name	app-[redacted]
UUID	[redacted]3d1b
Guest OS	
CPU	2
CPU Speed	4389
Memory	8 GB
Memory Overhead	
Host	172.[redacted]
vCenter Server	
Power State	On
Connection State	connected
Last Updated Time	2019-03-19 09:28:14.793

46 % Memory Utilization (SN...

53 % Disk Utilization (SNMP)

5 % CPU Utilization (SNMP)

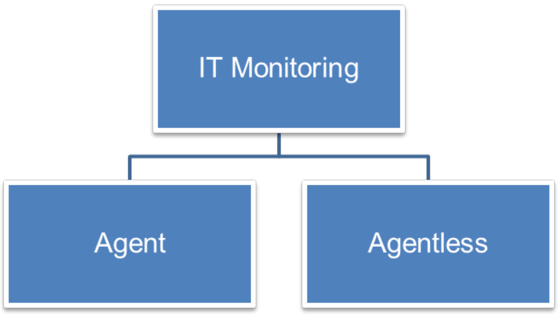
11 % CPU Utilization (VIWeb...

85 kBps Disk I/O Usage (VIWeb...

Interpretation

- Gathered metrics are presented through graphs or data charts, often on a GUI dashboard.
- This is often accomplished through integration with tools that specifically focus on data visualization.

Monitoring Reliance



- IT monitoring can rely on agents or be agentless.
- Agents are independent programs that install on the monitored device to collect data on hardware or software performance data and report it to a management server.
- Agentless monitoring uses existing communication protocols to emulate an agent, with many of the same functionalities.
- For example, to monitor server usage, an IT admin installs an agent on the server.
- A management server receives that data from the agent and displays it to the user via the IT monitoring system interface, often as a graph of performance over time.
- If the server stops working as intended, the tool alerts the administrator, who can repair, update or replace the item until it meets the standard for operation.

5.2 IT Monitoring Strategy and Best Practices

IT Monitoring Strategy

Determine Your Goals

- Do you merely want to be alerted if a single server goes down, or do you need to keep tabs on a hybrid environment that involves on-premises hardware and cloud services?
- Do you want to integrate your monitoring tool with other services?
- Do you want visibility into specific performance data?
- Do you want to use machine learning technology to automate corrective actions?

The answers to these questions will greatly impact the complexity of monitoring tools you should consider.

Bring Business Leaders on Board

- In conjunction with previous step, you'll want to involve stakeholders outside the IT organization to get buy-in on their IT monitoring goals as well.
- Consolidate these needs with IT's monitoring needs to create a single list of goals.

Identify Key Features You Need

- Most monitoring tools offer basic features like reporting and dashboards, but they vary in sophistication.
- If you have a special need for data retention, or want real-time, machine learning-driven insights, these types of features will also point the way to their own particular solutions.

Identify Data Sources that can be Used

- These data sources can range from servlogs to machine data to third-party data sources.
- Whatever you're trying to monitor, there should be at least one relevant data source that relates to it.

- Enumerate all of these sources so you can ensure that any tool you consider supports the desired information.

Evaluate Tools on a Trial basis

- Armed with all of this, you needn’t jump in whole hog with the first IT monitoring tool that sounds like a good fit.
- Most of these tools are available on a trial basis, so you can see how well they will work in your environment before you pull the trigger.
- This is particularly true for tools that are offered as a service, on a subscription basis.

IT Monitoring Strategy

Be Savvy with Alerts

- Too many alerts will quickly lead to fatigue and, even worse, ignored alerts.
- Take care to craft alert logic that is tripped when humans really need to get involved.

Consider Levels of Alerts

- Basic crashes or limited downtime can be routed to low-level analysts, but more serious problems need to be escalated to managers, and quickly.
- Assign problems along various severity levels to make this type of categorization and escalation easier.

Also consider the medium

- When is an emailed alert acceptable, and when does a text message or other mobile notification need to be used?
- Remember that too many texts can quickly lead to alert fatigue and missed alerts.

Refine your Dashboards

- The dashboard is where most analysts will spend the bulk of their work day, so it makes sense to expend effort to ensure the dashboard has the most critical information front and center, and secondary information within easy reach.

Create an escalation plan separate from the alerts system

- Your alerts may be designed with rudimentary escalation routines, but a seemingly simple problem with a server can quickly escalate into a major one.
- For example, your IT monitoring tool may only report that an offsite server is offline, not knowing that a Category 5 hurricane is bearing down on the data center. These are vastly different levels of problems that merit much different responses.

Remember that redundancy is good

- When possible, avoid relying on a single source of data to monitor the health of a particular node.
- If your monitoring tool loses access to a server log, does that mean the server is down, or that a network cable has been cut? You won’t know unless you have a secondary data source that can monitor network traffic, which can help to more quickly troubleshoot these kinds of issues.

Watch for outliers

- An average web page response time of 0.3 seconds is great, as long as that doesn’t mean that a small percentage of your users are actually seeing response times of 30 seconds or more and slipping through the cracks.

- A smart monitoring strategy needs to look at all the data, not just median information, and troubleshooting often needs to address the unique set of variables that might be causing trouble for a small portion of the end-user base.

5.3 Overview of Continuous Monitoring

What is Continuous Monitoring?

- Continuous monitoring is a process to detect, report, respond all the attacks which occur in IT infrastructure.
- Continuous monitoring, sometimes referred to as ConMon or Continuous Control Monitoring (CCM) provides security and operations analysts with real-time feedback on the overall health of IT infrastructure, including networks and applications deployed in the cloud.
- It is a technology and process that IT organizations may implement to enable rapid detection of compliance issues and security risks within the IT infrastructure.
- It empowers IT teams with real-time information from throughout public and hybrid cloud environments and supporting critical security processes like threat intelligence, forensics, root cause analysis, and incident response.

Benefits of using Continuous Monitoring

There are several benefits of using Continuous monitoring:

- It detects all the server and network problems.
- It finds the root cause of the failure.
- It helps in reducing the maintenance cost.
- It helps in troubleshooting the performance issues.
- It helps in updating infrastructure before it gets outdated.
- It can fix problems automatically when detected.
- It makes sure the servers, services, applications, network is always up and running.
- It monitors complete infrastructure every second.

Some other benefits of using Continuous monitoring are:

Increase Visibility and Transparency of Network

- Real-time monitoring gives IT teams a window of visibility into the inner workings of the IT infrastructure.
- The ability to aggregate, normalize and analyze data from throughout the network using automated processes ensures that important events and trends are not missed because of a lack of visibility into systems.

Enable Rapid Incident Response

- Continuous monitoring eliminates the time delay between when an IT incident first materializes and when it is reported to the incident response team, enabling a timelier response to security threats or operational issues.
- With access to real-time security intelligence, incident response teams can immediately work to minimize damage and restore systems when a breach occurs.

Reduce System Downtime

- The objective of IT operations is to maintain system uptime and performance.
- With continuous monitoring, IT Ops can react more quickly to application performance issues and rectify errors before they lead to service outages that negatively impact customers.

Drive Business Performance

- User behavior monitoring is a frequently overlooked benefit of continuous monitoring software tools.
- IT Ops teams can measure user behavior on the network using event logs and use that information to optimize the customer experience and direct users to their desired tasks and activities more efficiently.
- Software vendors create robust and versatile solutions that enable IT organizations to effectively monitor network traffic, detect anomalies or suspicious patterns of activity and develop actionable insights.
- The implementation of a continuous monitoring software solution can be described in following five basic steps:

How to Implement Continuous Monitoring?

- Software vendors create robust and versatile solutions that enable IT organizations to effectively monitor network traffic, detect anomalies or suspicious patterns of activity and develop actionable insights.
- The implementation of a continuous monitoring software solution can be described in following five basic steps:

1. System Definition

- The IT organization must determine the scope of its continuous monitoring deployment. Which systems are under the purview of the IT organization? Which systems should be subject to continuous monitoring?

2. Risk Assessment

- The IT organization should conduct a risk assessment of each asset it wishes to secure, categorizing assets based on the risk and potential impact of a data breach.
- Higher-risk assets will require more rigorous security controls
- Low-risk assets may not require security controls in general case.

3. Choosing and Implementing Security Control Applications

- Once a risk assessment has been completed, the IT organization should determine what types of security controls will be applied to each IT asset.
- Security controls can include things like passwords and other forms of authentication, firewalls, antivirus software, intrusion detection systems (IDS) and encryption measures.

4. Software Tool Configuration

- As the IT organization coordinates the desired security controls to protect key informational assets, it can begin to configure a continuous monitoring software tool to start capturing data from those security control applications.
- Continuous monitoring software tools incorporate a feature called log aggregation that collects log files from applications deployed on the network, including the security applications that are in place to protect information assets.
- These log files contain information about all events that take place within the application, including the detection of security threats and the measurement of key operational metrics.

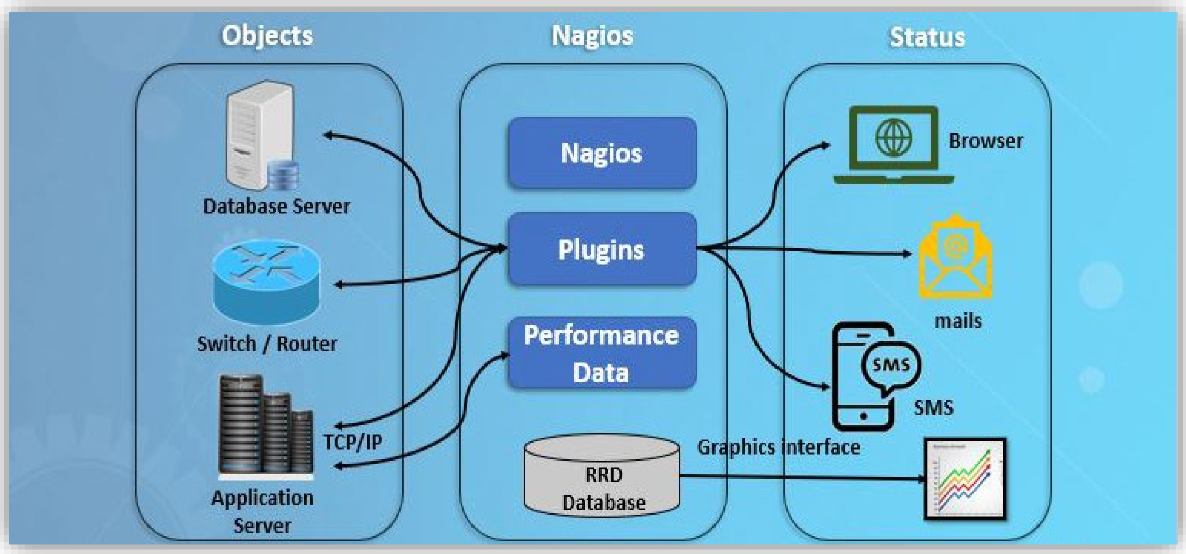
5. Ongoing Assessment

- Collecting data from throughout the IT infrastructure is not the ultimate goal of continuous monitoring.
- With millions of data points generated and centralized each day through log aggregation, information must be assessed on an ongoing basis to determine whether there are any security, operational or business issues that require attention from a human analyst.
- Many IT organizations today are leveraging big data analytics technologies, including artificial intelligence and machine learning, to analyze large volumes of log data and detect trends, patterns or outliers that indicate abnormal network activity.

5.4 Overview of Nagios

What is Nagios?

- Nagios is an open-source continuous monitoring tool which monitors network, applications and servers.
- It can find and repair problems detected in the infrastructure and stop future issues before they affect the end users.
- It gives the complete status of your IT infrastructure and its performance.



- Nagios is an open-source monitoring system for computer systems.
- It was designed to run on the Linux operating system and can monitor devices running Linux, Windows and Unix operating systems (OSes).
- It executes a continuous check on the crucial application, server resources, network, and tasks.
- The memory usage of monitor and disk, the load of the microprocessor, number of processors, and logs currently running.
- It can also check other services like Post office protocols 3, Simple Mail Transfer Protocol, HTTP protocols, and other available standard network protocols.
- Nagios software runs periodic checks on critical parameters of application, network and server resources.
- For example, Nagios can monitor memory usage, disk usage, microprocessor load, the number of currently running processes and log files.

- Active checks are initiated by Nagios, while passive checks come from external applications connected to the monitoring tool.
- Originally called NetSaint and released in 1999, Nagios was developed by Ethan Galstad and subsequently refined by numerous contributors as an open-source project.

Why Nagios?

Nagios offers the following features making it usable by a large group of user community:

- It can monitor Database servers such as SQL Server, Oracle, Mysql, Postgres
- It gives application-level information (Apache, Postfix, LDAP, Citrix etc.).
- Provides active development.
- Has excellent support form huge active community.
- Nagios runs on any operating system.
- It can ping to see if host is reachable.

Features

Nagios is the monitoring tool with multitude of features as given below:

- Nagios Core is open source, hence free to use.
- Powerful monitoring engine which can scale and manage 1000s of hosts and servers.
- Comprehensive web dashboard giving the visibility of complete network components and monitoring data.
- It has multi-tenant capabilities where multiple users have access to Nagios dashboard.
- It has extendable architecture which can easily integrate with third-party applications with multiple APIs.
- Nagios has a very active and big community with over 1 million + users across the globe.
- Fast alerting system sends alerts to admins immediately after any issue is identified.
- Multiple plugins available to support Nagios, custom coded plugins can also be used with Nagios.
- It has good log and database system storing everything happening on the network with ease.
- Proactive Planning feature helps to know when it’s time to upgrade the infrastructure.

Applications

Nagios can be applicable to a wide range of applications. They are given here:

- Monitor host resources such as disk space, system logs etc.
- Monitor network resources – http, ftp, smtp, ssh etc.
- Monitor log files continuously to identify infra-issue
- Monitor windows/linux/unix/web applications and its state
- Nagios Remote Plugin Executer (NRPE) can monitor services remotely
- Run service checks in parallel
- SSH or SSL tunnels can also be used for remote monitoring
- Send alerts/notifications
- via email, sms, pager of any issue on infrastructure
- Recommending when to upgrade the IT infrastructure

Benefits of Nagios

Nagios offers the following benefits for the users:

- It helps in getting rid of periodic testing.
- It detects split-second failures when the wrist strap is still in the “intermittent” stage.
- It reduces maintenance cost without sacrificing performance.

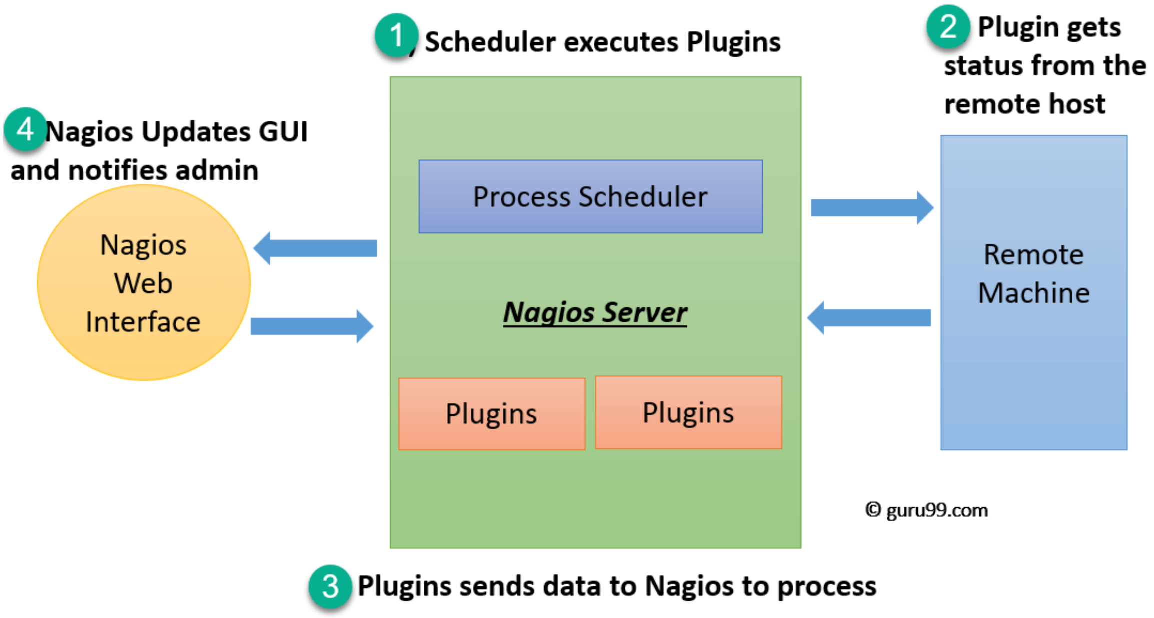
- ➢ It provides timely notification to the management of control and breakdown.

Architecture

The following points are worth notable about Nagios architecture:

- Nagios has server-agent architecture.
- Nagios server is installed on the host and plugins are installed on the remote hosts/servers which are to be monitored.
- Nagios sends a signal through a process scheduler to run the plugins on the local/remote hosts/servers.
- Plugins collect the data (CPU usage, memory usage etc.) and sends it back to the scheduler.
- Then the process schedules send the notifications to the admin/s and updates Nagios GUI.

The following figure shows Nagios Server Agent Architecture in detail:



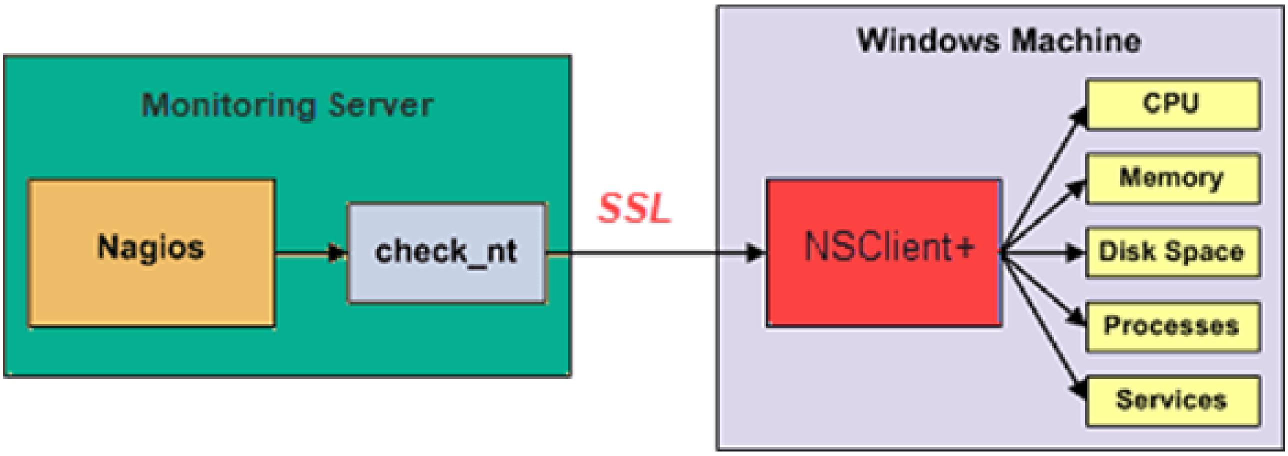
1 Scheduler executes Plugins
2 Plugin gets status from the remote host
4 Nagios Updates GUI and notifies admin
Nagios Web Interface
Process Scheduler
Nagios Server
Plugins
Plugins
Remote Machine
3 Plugins sends data to Nagios to process

© guru99.com

- The scheduler is a component of server part of Nagios. It sends a signal to execute the plugins at the remote host.
- The plugin gets the status from the remote host
- The plugin sends the data to the process scheduler
- The process scheduler updates the GUI and notifications are sent to admins

Plugins

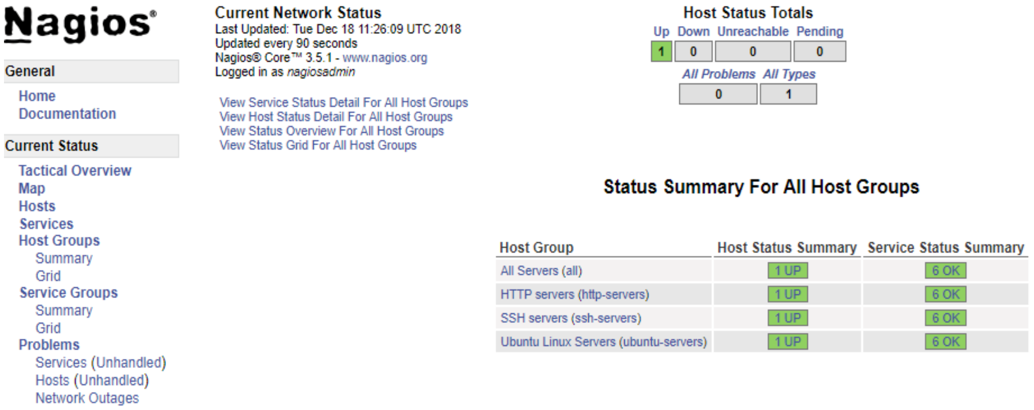
- Plugins are software additions that allow for the customization of computer programs, apps, and web browsers -- as well as the customization of the content offered by websites.
- Nagios plugins provide low-level intelligence on how to monitor anything and everything with Nagios Core.
- Plugins operate acts as a standalone application, but they are designed to be executed by Nagios Core.
- It connects to Apache that is controlled by CGI to display the result. Moreover, a database connected to Nagios to keep a log file.



- Check_nt is a plugin to monitor a windows machine which is mostly available in the monitoring server.
- NSClinet++ should be installed in every Windows machine that you want to monitor.
- There is an SSL connection between the server and the host which continuously exchange information with each other.
- Likewise, NRPE (Nagios Remote plug-in Executor) and NSCA plugins are used to monitor Linux and Mac OS X respectively.
- Nagios can also run remote scripts and plug-ins using the Nagios Remote Plugin Executor (NRPE) agent.
- NRPE enables remote monitoring of system metrics such as system load, memory and disk usage.
- It consists of the check_nrpe plug-in, which is stored on the local monitoring machine, and the NRDP, running on the remote machine.
- Nagios uses a plug-in to consolidate data from the NRPE agent before it goes to the management server for processing.
- NRPE can also communicate with Windows agents to monitor Windows machines
- Nagios supports plug-ins that are stand-alone add-ons and extensions so the user can define targets and which parameters on these targets to monitor.
- Nagios plug-ins process command-line arguments and communicate the commands with Nagios Core.
- There are around 50 plug-ins developed and maintained by Nagios, while there are over 3,000 from the community.
- These plug-ins are categorized into lists including hardware, software, cloud, OSes, security, log files and network connections.
- As an example, when used in conjunction with environmental-sensing systems, a Nagios plug-in can share data on environmental variables, such as temperature, humidity or barometric pressure.

GUI

- An interface of Nagios is used to display web pages generated by CGI.
- It can be buttons to green or red, sound, graph, etc.
- When the soft alert is raised many times, a hard alert is raised, then the Nagios server sends a notification to the administrator.



Current Network Status
Last Updated: Tue Dec 18 11:26:09 UTC 2018
Updated every 90 seconds
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	*All Types*
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
6	0	0	0	0

All Problems	*All Types*
0	6

Status Summary For All Host Groups

Host Group	Host Status Summary	Service Status Summary
All Servers (all)	1 UP	6 OK
HTTP servers (http-servers)	1 UP	6 OK
SSH servers (ssh-servers)	1 UP	6 OK
Ubuntu Linux Servers (ubuntu-servers)	1 UP	6 OK

Structure

- A user can choose to work in the command-line interface (CLI) or select a web-based graphical user interface (GUI) in some versions of Nagios and from third parties.
- Nagios' dashboard provides an overview of the critical parameters monitored on assets.
- Based on the parameters and thresholds defined, Nagios can send out alerts if critical levels are reached.
- These notifications can be sent in different ways, including email and text messages.
- An authorization system allows the administrator to restrict access.

Configuration

- Nagios runs both agent-based and agentless configurations.
- Independent agents are installed on any hardware or software system to collect data that is then reported back to the management server.
- Agentless monitoring uses existing protocols to emulate an agent.
- Both approaches can monitor file system usage, OS metrics, service and process states and more.
- Examples of Nagios agents include Nagios Remote Data Processor (NRDP), Nagios Cross Platform Agent (NCPA) and NSClient++.

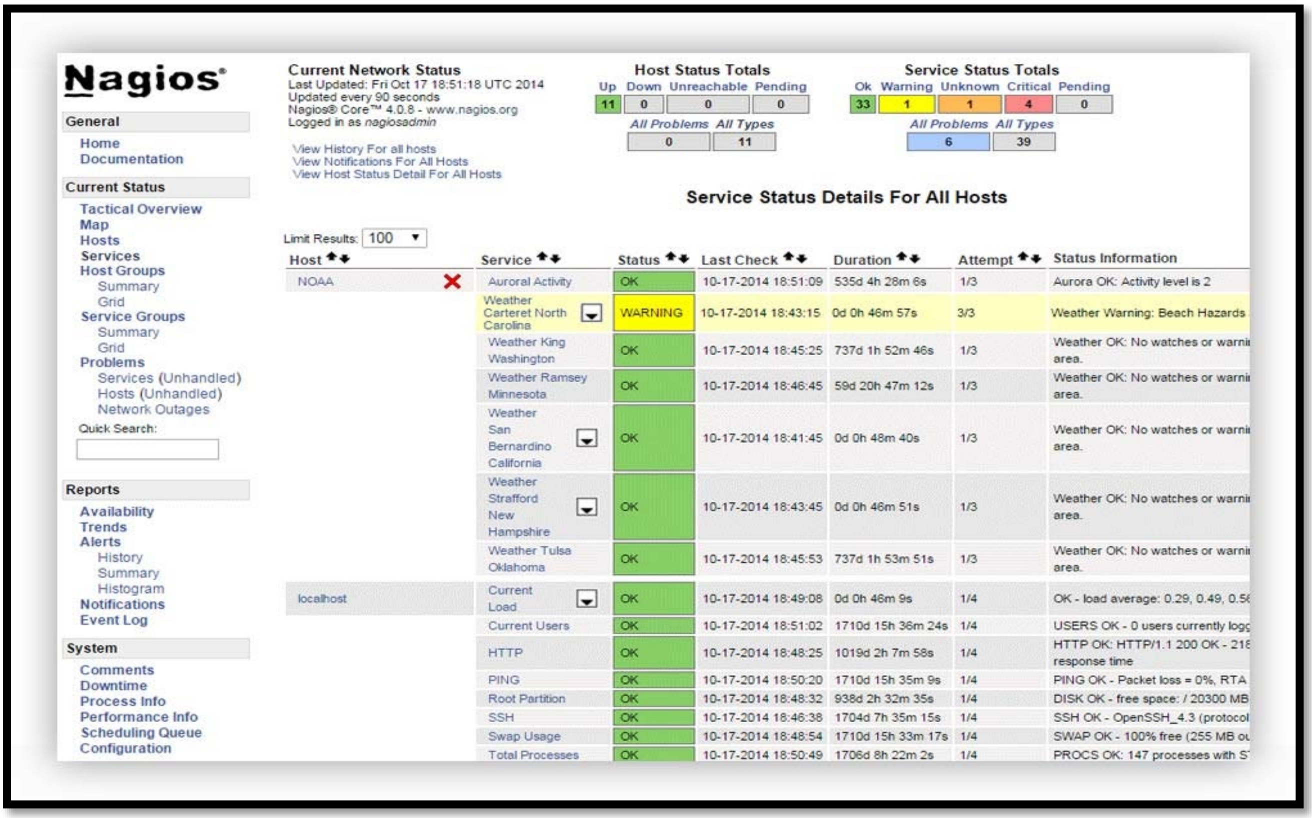
Products

Nagios XI

- It provides monitoring for complete IT infrastructure components like applications, services, network, operating systems etc.
- It gives a complete view of your infrastructure and business processes.
- The GUI is easily customizable giving the used flexibility.
- Plug-ins are supported for these infrastructure components to expand on XI's monitoring capabilities.

Nagios Core

- The service that was originally known as Nagios is now referred to as Nagios Core.
- It is the core on monitoring IT infrastructure.
- Core is freely available as an open-source monitoring software for IT systems, networks and infrastructure.
- Core contains a wide array of infrastructure monitoring through allowing plug-ins to extend its monitoring capabilities.
- Nagios XI product is also fundamentally based on Nagios core.
- Whenever there is any issue of failure in the infrastructure, it sends an alert/notification to the admin who can take the action quickly to resolve the issue.



Current Network Status
Last Updated: Fri Oct 17 18:51:18 UTC 2014
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
11	0	0	0

All Problems	*All Types*
0	11

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	1	4	0

All Problems	*All Types*
6	39

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
NOAA ✗	Auroral Activity	OK	10-17-2014 18:51:09	535d 4h 28m 6s	1/3	Aurora OK: Activity level is 2
	Weather Carteret North Carolina	WARNING	10-17-2014 18:43:15	0d 0h 46m 57s	3/3	Weather Warning: Beach Hazards
	Weather King Washington	OK	10-17-2014 18:45:25	737d 1h 52m 46s	1/3	Weather OK: No watches or warni area.
	Weather Ramsey Minnesota	OK	10-17-2014 18:46:45	59d 20h 47m 12s	1/3	Weather OK: No watches or warni area.
	Weather San Bernardino California	OK	10-17-2014 18:41:45	0d 0h 48m 40s	1/3	Weather OK: No watches or warni area.
	Weather Strafford New Hampshire	OK	10-17-2014 18:43:45	0d 0h 46m 51s	1/3	Weather OK: No watches or warni area.
	Weather Tulsa Oklahoma	OK	10-17-2014 18:45:53	737d 1h 53m 51s	1/3	Weather OK: No watches or warni area.
localhost	Current Load	OK	10-17-2014 18:49:08	0d 0h 46m 9s	1/4	OK - load average: 0.29, 0.49, 0.5
	Current Users	OK	10-17-2014 18:51:02	1710d 15h 36m 24s	1/4	USERS OK - 0 users currently log
	HTTP	OK	10-17-2014 18:48:25	1019d 2h 7m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 21 response time
	PING	OK	10-17-2014 18:50:20	1710d 15h 35m 9s	1/4	PING OK - Packet loss = 0%, RTA
	Root Partition	OK	10-17-2014 18:48:32	938d 2h 32m 35s	1/4	DISK OK - free space: / 20300 MB
	SSH	OK	10-17-2014 18:46:38	1704d 7h 35m 15s	1/4	SSH OK - OpenSSH_4.3 (protocol
	Swap Usage	OK	10-17-2014 18:48:54	1710d 15h 33m 17s	1/4	SWAP OK - 100% free (255 MB ou
	Total Processes	OK	10-17-2014 18:50:49	1706d 8h 22m 2s	1/4	PROCS OK: 147 processes with S

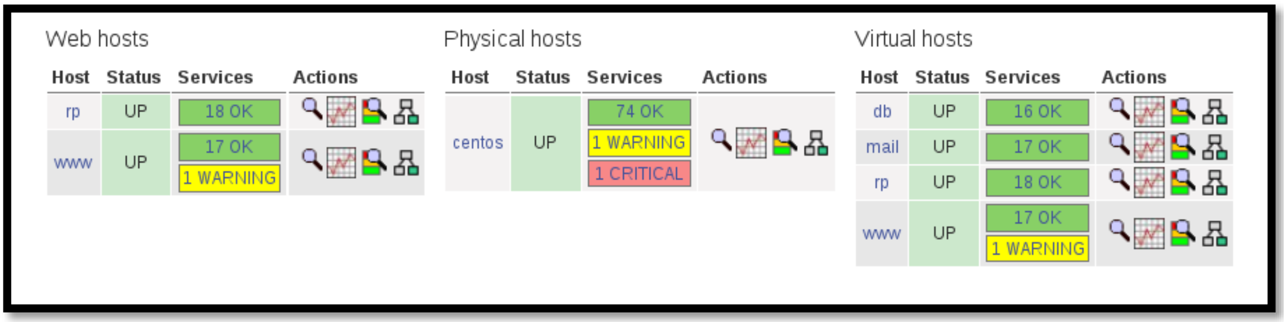
- Nagios Core has an optional web interface, which displays network status, notifications, log files and more.
- Core can notify its user when there are server or host issues.
- Additionally, Core can monitor network services such as SMTP, HTTP and Ping.

Nagios XI vs Nagios Core

- Nagios XI is an extended interface of Nagios Core, intended as the enterprise-level version of the monitoring tool.
- XI acts as monitoring software, configuration manager and toolkit.
- While Nagios Core is free, XI must be purchased from Nagios Enterprises.
- Atop the same features as Core, XI adds preconfigured virtual machines (VMs), a web configuration user interface (UI), performance graphing, a mobile application, dashboards, scheduled reporting, technical support through email and more.

Nagios Log Server

- Log Server is a log monitoring and management tool that enables an organization to view, sort and configure logs from its IT infrastructure, including Windows event logs.
- It makes searching of log data very simple and easy.
- It keeps all the log data at one location with high availability setup.
- It can easily send alerts if any issue is found in the log data.
- It can scale to 1000s of severs giving more power, speed, storage, and reliability to your log analysis platform.
- Log Server can analyze, collect and store logged data based off of custom and reassigned specifications.



Web hosts

Host	Status	Services	Actions
rp	UP	18 OK	
www	UP	17 OK 1 WARNING	

Physical hosts

Host	Status	Services	Actions
centos	UP	74 OK 1 WARNING 1 CRITICAL	

Virtual hosts

Host	Status	Services	Actions
db	UP	16 OK	
mail	UP	17 OK	
rp	UP	18 OK	
www	UP	17 OK 1 WARNING	

- The administrator can set alerts to notify Log Server users when there is a potential threat or malfunction on a monitored asset.
- For example, an alert goes out to the Microsoft Exchange administrator when there are three failed login attempts to Exchange Server, meaning there could be an unwarranted person trying to guess the password to the system.

Nagios Fusion

- This product provides a centralized view of complete monitoring system.
- With Nagios Fusion, you scan setup separate monitoring servers for separate geographies.
- It can be easily integrated with Nagios XI and Nagios core to give the complete visibility of the infrastructure.

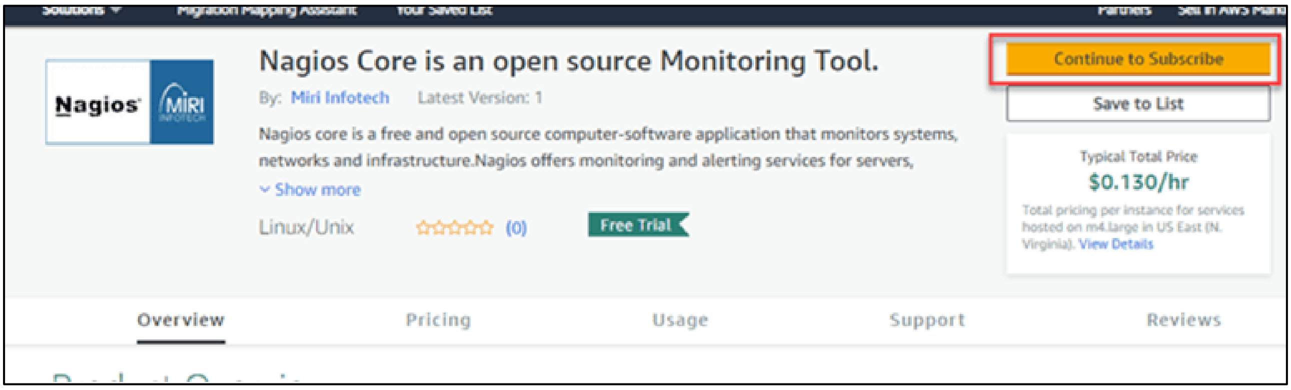
Nagios Network Analyser

- It gives the complete information of the network infrastructure to the admin with the potential threats on the network so that admin can take quick actions.
- It shares very detailed data about the network after in-depth network analysis.
- Nagios Network Analyzer tracks network traffic and bandwidth utilization.
- Network Analyzer can resolve network outages, abnormalities and security threats.
- Some features include automated security alerts, customizable application monitoring, integration with Nagios IX and a bandwidth utilization calculator.

5.5 How to Install Nagios Tool at AWS

Step 1) Subscribe to Nagios.

Go to https://aws.amazon.com/marketplace/pp/prodview-5d75bazindmew and click Continue to Subscribe



Nagios Core is an open source Monitoring Tool.

By: Miri Infotech Latest Version: 1

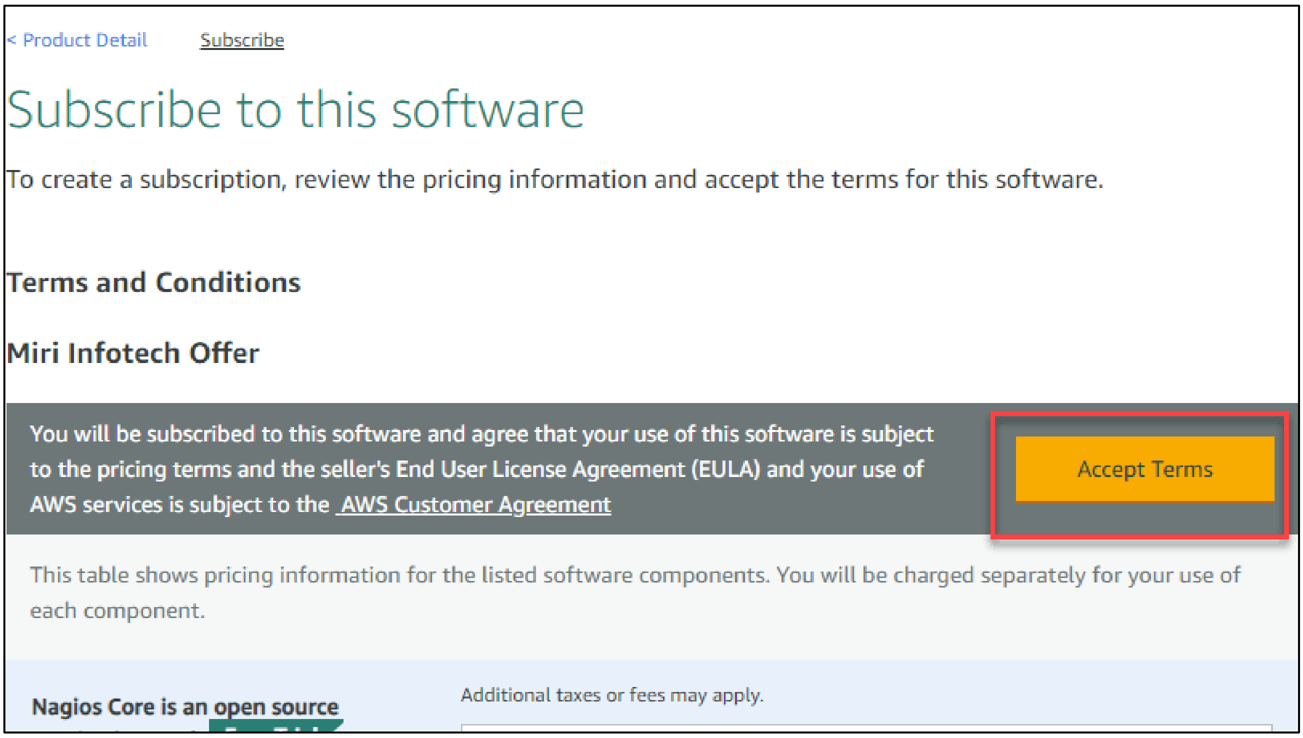
Nagios core is a free and open source computer-software application that monitors systems, networks and infrastructure.Nagios offers monitoring and alerting services for servers,

⌄ Show more

Linux/Unix ☆☆☆☆☆ (0)

Typical Total Price
$0.130/hr
Total pricing per instance for services hosted on m4.large in US East (N. Virginia). View Details

Step 2) Read terms and conditions.
Accept Terms.



< Product Detail Subscribe

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Miri Infotech Offer

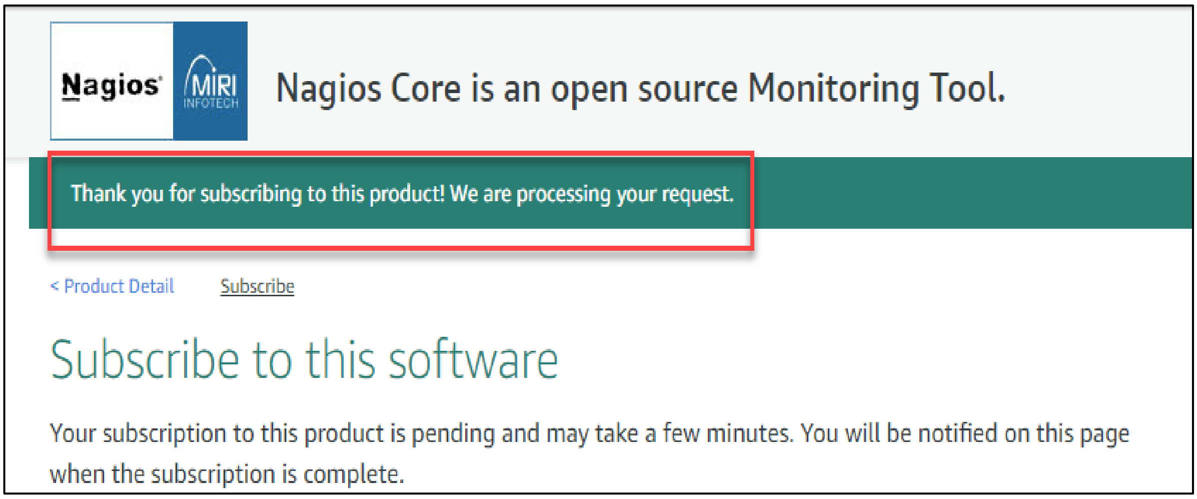
You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement

This table shows pricing information for the listed software components. You will be charged separately for your use of each component.

Nagios Core is an open source

Additional taxes or fees may apply.

Step 3) View message.
You will see subscription pending message



Nagios Core is an open source Monitoring Tool.

Thank you for subscribing to this product! We are processing your request.

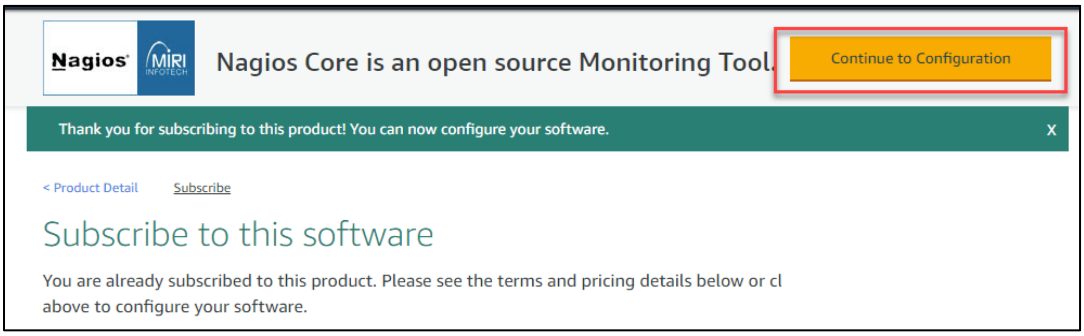
< Product Detail Subscribe

Subscribe to this software

Your subscription to this product is pending and may take a few minutes. You will be notified on this page when the subscription is complete.

Step 4) Do configuration.

Refresh the same page after a few minutes



Nagios Core is an open source Monitoring Tool.

Thank you for subscribing to this product! You can now configure your software.

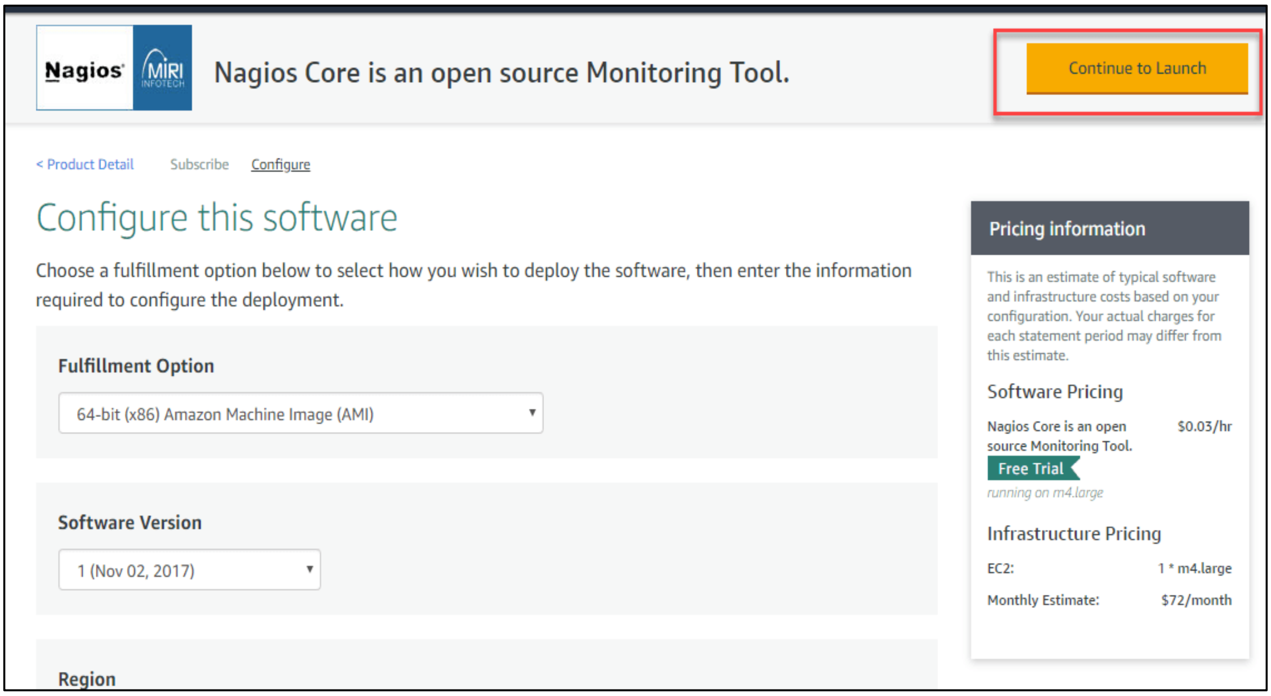
< Product Detail Subscribe

Subscribe to this software

You are already subscribed to this product. Please see the terms and pricing details below or cl above to configure your software.

and click “Continue to Configuration

Step 5) Launch the nagios.
Keep the settings default and click Continue to Launch



Nagios Core is an open source Monitoring Tool.

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option: 64-bit (x86) Amazon Machine Image (AMI)

Software Version: 1 (Nov 02, 2017)

Region

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

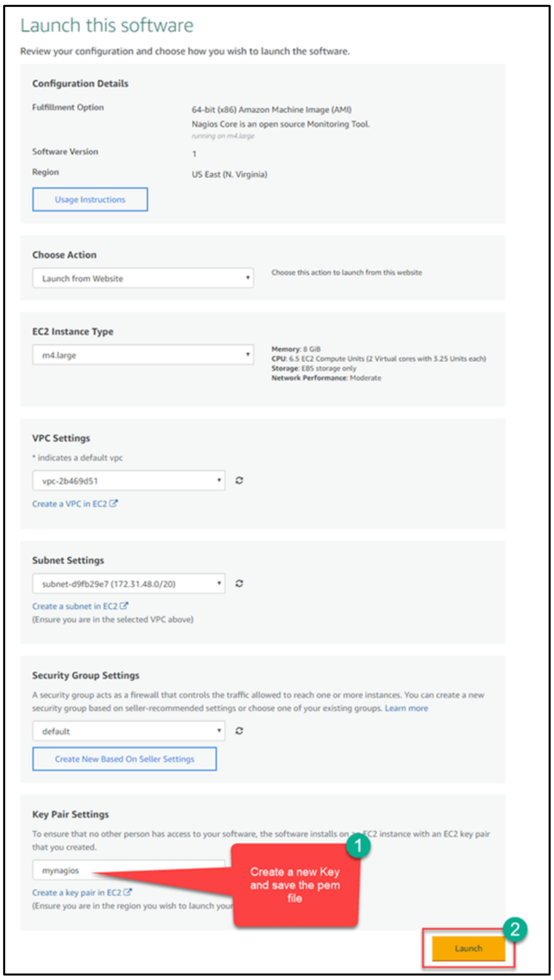
Software Pricing

Nagios Core is an open source Monitoring Tool. $0.03/hr
Free Trial
running on m4.large

Infrastructure Pricing

EC2: 1 * m4.large
Monthly Estimate: $72/month

Step 6) Review settings.
Review the settings. Create a new Key and click launch



Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option: 64-bit (x86) Amazon Machine Image (AMI)
Nagios Core is an open source Monitoring Tool.
running on m4.large

Software Version: 1

Region: US East (N. Virginia)

Choose Action

Launch from Website ▾ — Choose this action to launch from this website

EC2 Instance Type

m4.large ▾

Memory: 8 GiB
CPU: 6.5 EC2 Compute Units (2 Virtual cores with 3.25 Units each)
Storage: EBS storage only
Network Performance: Moderate

VPC Settings

* indicates a default vpc

vpc-2b469d51 ▾

Create a VPC in EC2

Subnet Settings

subnet-d9fb29e7 (172.31.48.0/20) ▾

Create a subnet in EC2
(Ensure you are in the selected VPC above)

Security Group Settings

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. You can create a new security group based on seller-recommended settings or choose one of your existing groups. Learn more

default ▾

Key Pair Settings

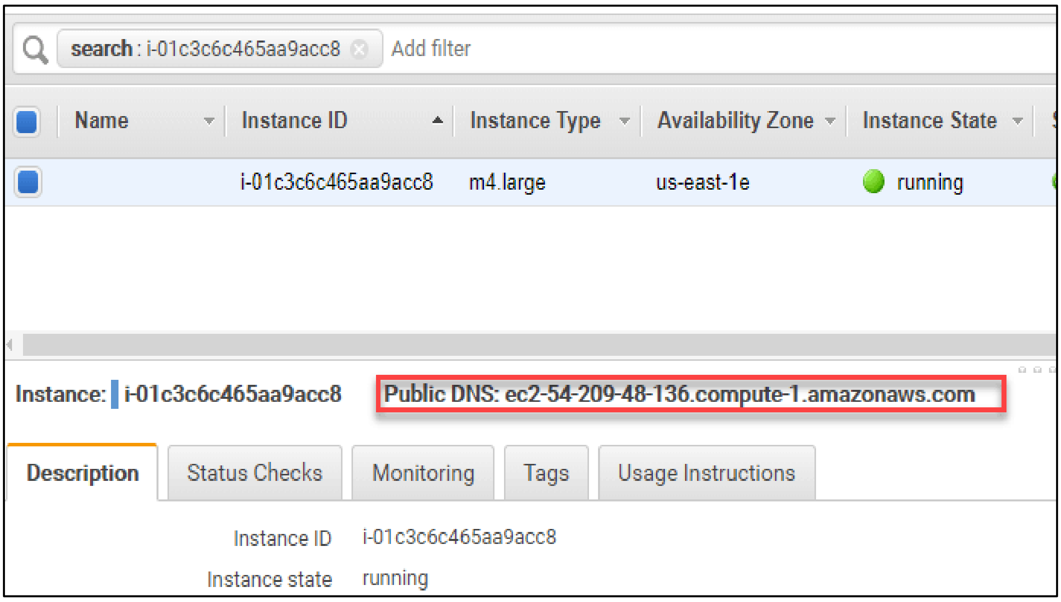
To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created.

mynagios

Create a key pair in EC2
(Ensure you are in the region you wish to launch your

1 Create a new Key and save the pem file

Step 7) Note public DNS. Note the public DNS of your instance



search : i-01c3c6c465aa9acc8 Add filter

☐	Name	Instance ID ▲	Instance Type	Availability Zone	Instance State
☐		i-01c3c6c465aa9acc8	m4.large	us-east-1e	● running

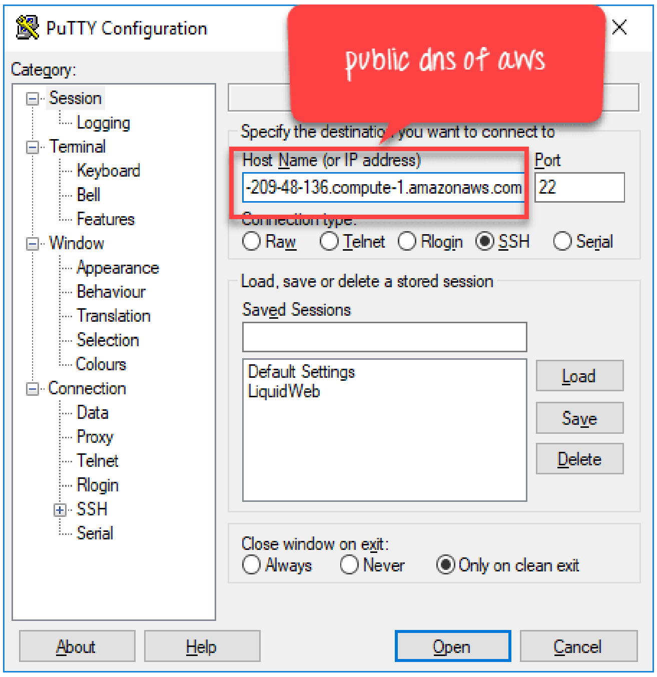
Instance: i-01c3c6c465aa9acc8 Public DNS: ec2-54-209-48-136.compute-1.amazonaws.com

Instance ID i-01c3c6c465aa9acc8
Instance state running

Step 8) Convert pem file to ppk.

In your windows machine, use the tool putty generator to convert pem file to ppk

Step 9) Enter public DNS.
In putty, enter the public DNS



public dns of aws

Specify the destination you want to connect to

Host Name (or IP address): -209-48-136.compute-1.amazonaws.com

Port: 22

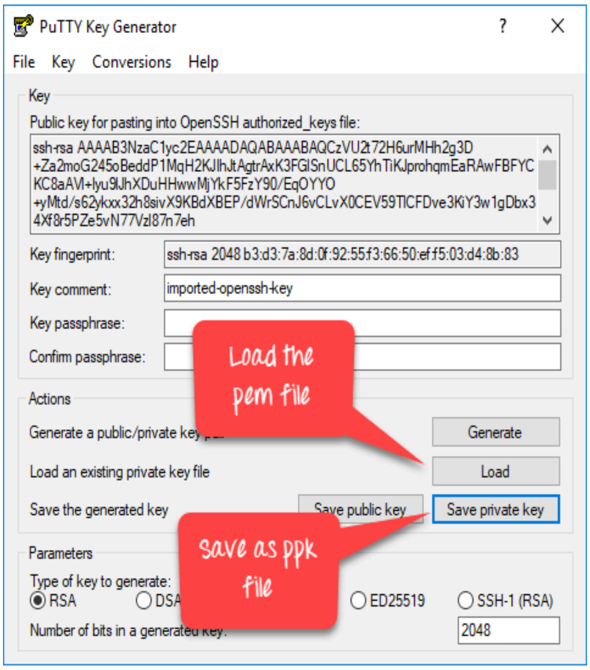
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
LiquidWeb

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



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzVU2t72H6urMHh2g3D
+Za2moG245oBeddP1MqH2KJlhJtAgtrAxK3FGlSnUCL65YhTiKJprohqmEaRAwFBFYC
KC8aAVl+lyu9lJhXDuHHwwMjYkF5FzY90/EqOYYO
+yMtd/s62ykxx32h8sivX9KBdXBEP/dWrSCnJ6vCLvX0CEV59TICFDve3KiY3w1gDbx3
4Xf8r5PZe5vN77Vzl87n7eh
```

Key fingerprint: ssh-rsa 2048 b3:d3:7a:8d:0f:92:55:f3:66:50:ef:f5:03:d4:8b:83

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

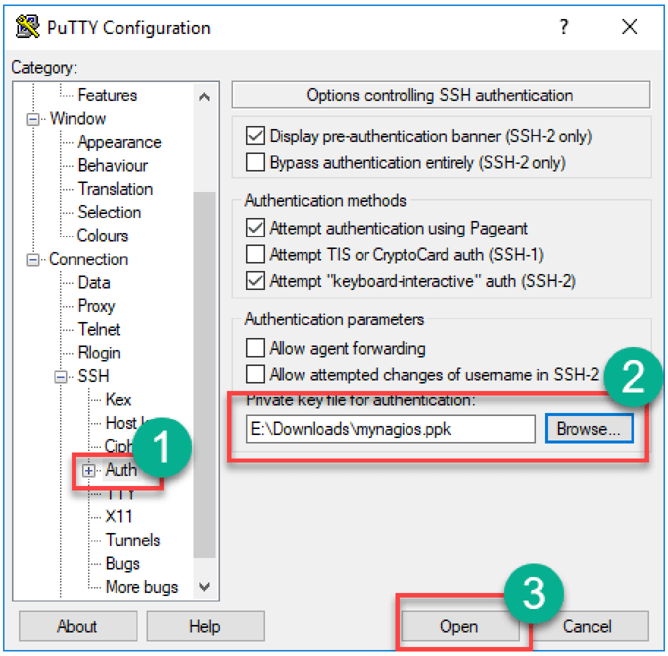
Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Load the pem file

save as ppk file

Step 10) Enter ppk key.
In Auth section, enter the ppk key and click open



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

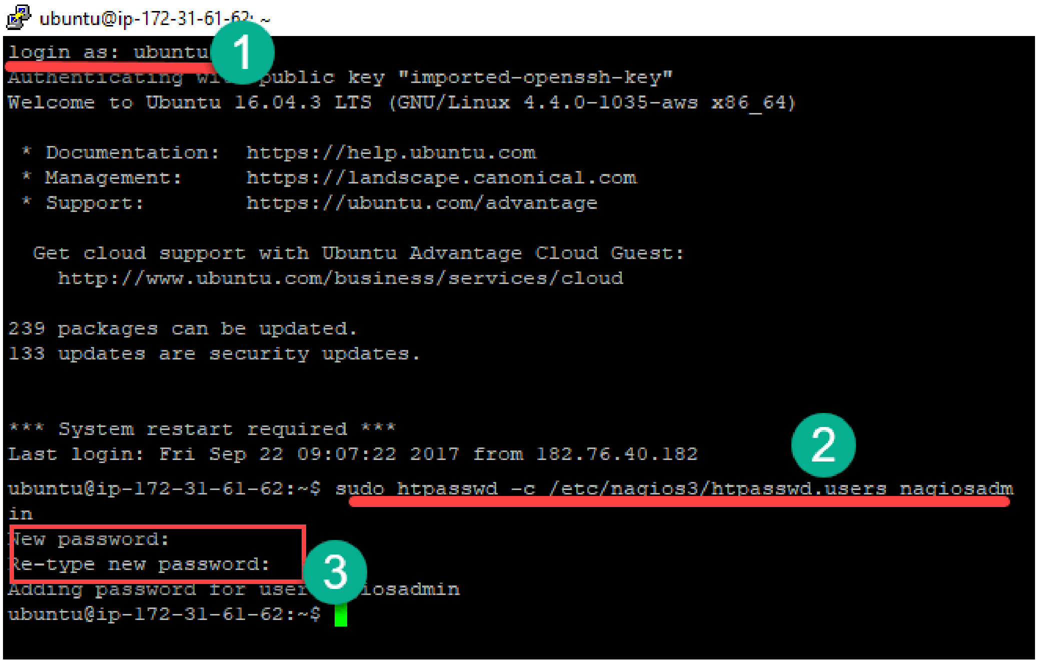
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

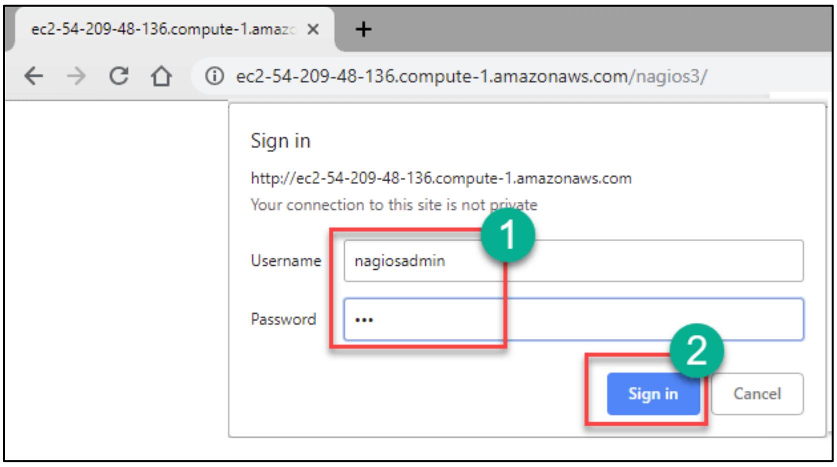
Private key file for authentication: E:\Downloads\mynagios.ppk

Step 11) In terminal,
Enter login name as ubuntu and run command.
Run this command sudo htpasswd -c /etc/nagios3/htpasswd.users nagiosadmin
Enter a new password of your choice



```
login as: ubuntu
Authenticating wi   public key "imported-openssh-key"
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-1035-aws x86_64)

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

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

239 packages can be updated.
133 updates are security updates.


*** System restart required ***
Last login: Fri Sep 22 09:07:22 2017 from 182.76.40.182
ubuntu@ip-172-31-61-62:~$ sudo htpasswd -c /etc/nagios3/htpasswd.users nagiosadm
in
New password:
Re-type new password:
Adding password for user  iosadmin
ubuntu@ip-172-31-61-62:~$
```

Step 12) Open your browser.
In your browser, Go to location http://<Public DNS>/nagios3 in my case http://ec2-54-209-48-136.compute-1.amazonaws.com/nagios3/
Enter Username: nagiosadmin
pass: set in the previous step



Sign in

http://ec2-54-209-48-136.compute-1.amazonaws.com

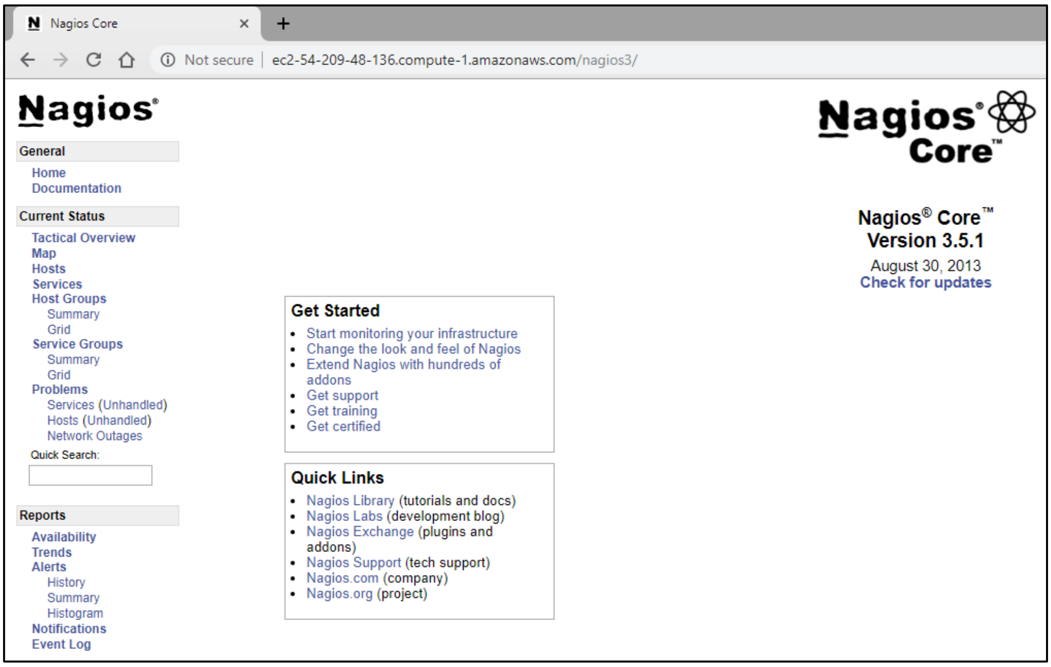
Your connection to this site is not private

Username: nagiosadmin

Password: •••

ec2-54-209-48-136.compute-1.amaz
ec2-54-209-48-136.compute-1.amazonaws.com/nagios3/
1
2
Sign in
Cancel

Step 13) Nagios installation done.
Nagios Loads.



Nagios® Core™
Version 3.5.1
August 30, 2013
Check for updates

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links

- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

5.6 Advanced Monitoring Tools and Devices

- Cloud providers largely support APM capabilities with their own native tools.
- Cloud customers can also choose from many third-party APM tools to see metrics on resource availability, response times and security.
- Application monitoring is within the scope of application performance management, a concept that involves more broadly controlling an application's performance levels.
- IT infrastructure monitoring tools can be broken down into three general categories or types of network devices observational, analysis and engagement based on how they're used.

Observational Tools

- These are the most basic types of IT monitoring tools, used to observe hardware, software or services and report back on their operational effectiveness.
- Most availability monitoring tools, including infrastructure monitoring and management tools, application performance monitoring tools, and web performance monitoring tools fall into this category.

Analysis Tools

- This type of IT monitoring tool is tasked with taking observational data and analyzing it further.
- This data may be analyzed to determine where problems are originating or more critically, to determine why those problems might be occurring.
- Advanced analysis tools, such as AIOps systems, are tasked with forecasting where problems are likely to arise based on historical trends and patterns.

Engagement Tools

- As the final tier of IT monitoring tools, engagement tools are designed to act upon information created by both analysis and observational tools.
- This may take a simple form, in the case of service tickets or alerts that are intelligently delivered to the appropriate analyst or business manager, or more commonly, be used to spin up additional services, reboot troublesome hardware or software, or run backups.
- Some APM vendors also offer IT infrastructure monitoring capabilities, and vice versa.

- Other tools are designed specifically to watch over the network or CPU performance and so on. Some monitoring tools incorporate AI capabilities.
- Following list is not comprehensive, however, and many tools incorporate capabilities typically seen in other segments, such as AI or the ability to track cloud and on-premises infrastructure.

APM Tools

- ➢ BMC TrueSight
- ➢ Cisco AppDynamics
- ➢ Datadog
- ➢ Dynatrace
- ➢ ManageEngine Applications Manager Microsoft Azure Application Insights
- ➢ New Relic
- ➢ SolarWinds APM

IT infrastructure tools

- ➢ LogicMonitor
- ➢ ManageEngine OpManager
- ➢ Microsoft System Center Operations Manager (SCOM)
- ➢ Nagios XI
- ➢ SolarWinds
- ➢ VMware vRealize Operations
- ➢ Zabbix

Cloud monitoring tools

- ➢ Amazon CloudWatch
- ➢ Google Stackdriver (now folded into Google Cloud Console)
- ➢ Microsoft Azure Monitor
- ➢ Cisco CloudCenter
- ➢ Oracle Application Performance Monitoring Cloud Service

Containers/microservices/distributed app monitoring tools

- Confluent Kafka
- Jaeger
- LightStep
- Prometheus

Alops Tools

- BigPanda
- Datadog
- Dynatrace
- Moogsoft
- New Relic

Log Monitoring Tools

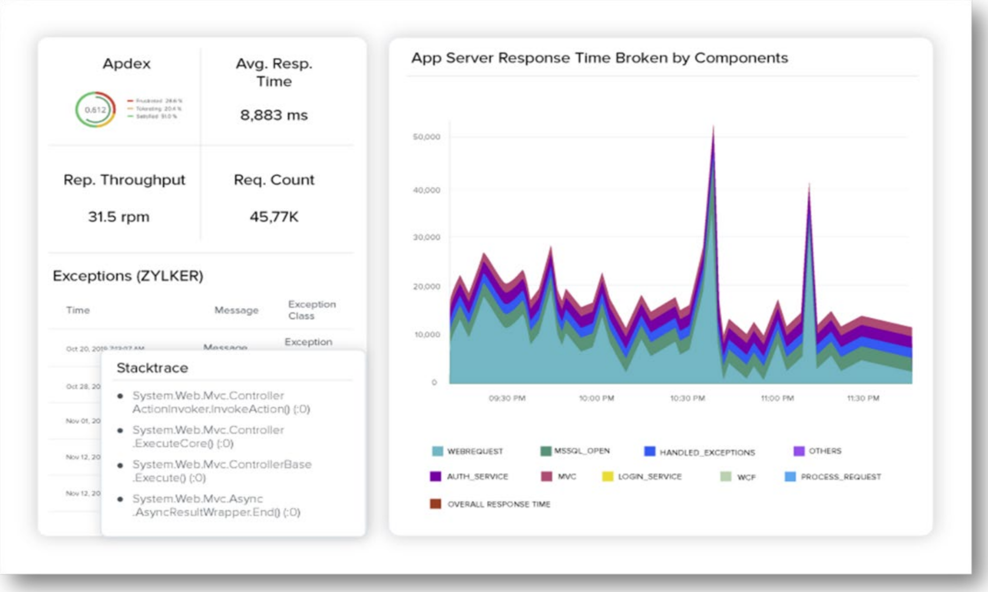
- Elastic Stack
- Fluentd
- Splunk
- Sumo Logic

Network Security Monitoring Tools

- Cisco DNA Analytics and Assurance
- LiveAction LiveNX
- LogRhythm
- PRTG Network Monitor

Optimize Response Time

- Monitor individual transactions across micro services and distributed architecture.
- Use distributed tracing to understand the ripple effect: how a request from one service leads to an error in another.
- Instantly identify and resolve errors and reduce mean time to detect (MTTD) and mean time to resolve (MTTR).



Apdex: 0.612

Avg. Resp. Time: 8,883 ms

Rep. Throughput: 31.5 rpm

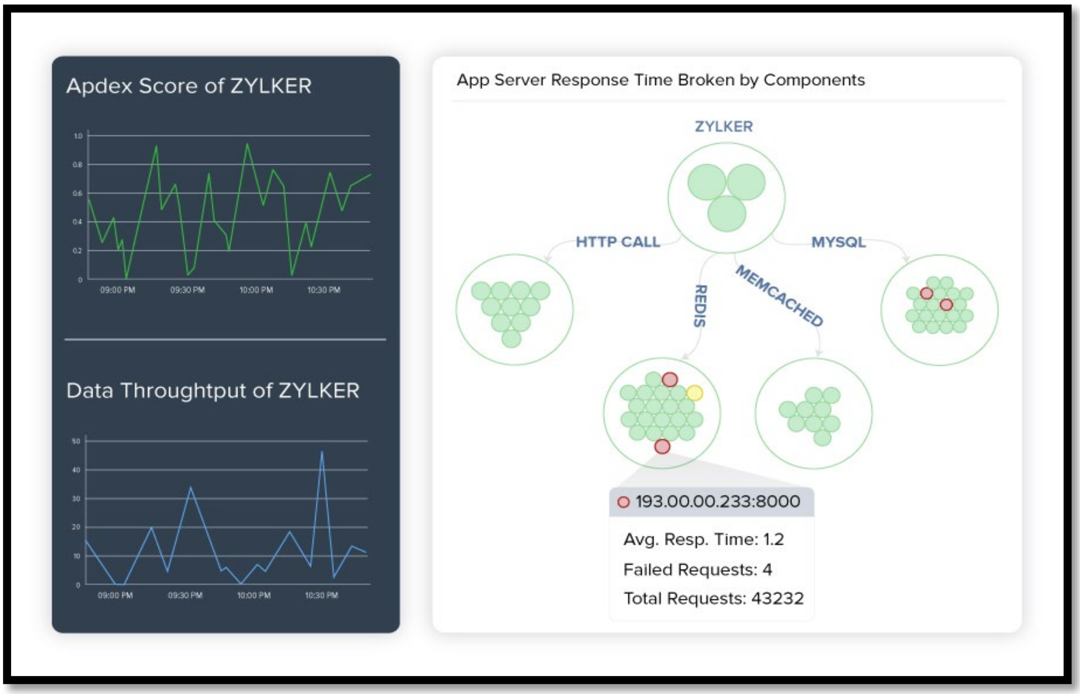
Req. Count: 45,77K

Exceptions (ZYLKER)

Time	Message	Exception Class
Oct 20, 2019 [illegible] AM	Message	Exception
Oct 28, 20		
Nov 01, 20		
Nov 12, 20		
Nov 12, 20		

Stacktrace

- System.Web.Mvc.Controller ActionInvoker.InvokeAction() (:0)
- System.Web.Mvc.Controller .ExecuteCore() (:0)
- System.Web.Mvc.ControllerBase .Execute() (:0)
- System.Web.Mvc.Async .AsyncResultWrapper.End() (:0)



○ 193.00.00.233:8000

Avg. Resp. Time: 1.2

Failed Requests: 4

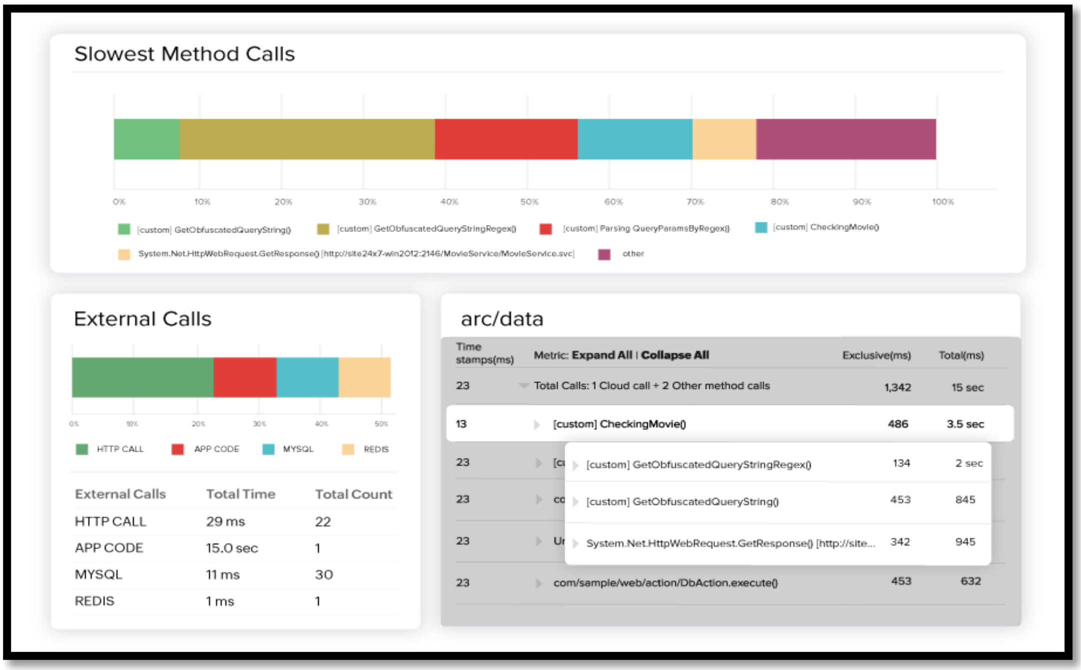
Total Requests: 43232

Understand External Dependencies

- Visualize application topology and gain a holistic view of your application architecture, from URLs to SQL queries.
- Identify component failure at a single glance and debug method level errors.

Monitor custom components and metrics

- Monitor custom components and metrics
- Mark business critical transactions as key transactions and track their performance at a glance.
- Instrument custom frameworks, components, and exceptions from custom logs and analyze their performance with ease.
- Group key metrics using custom dashboards and debug issues contextually.

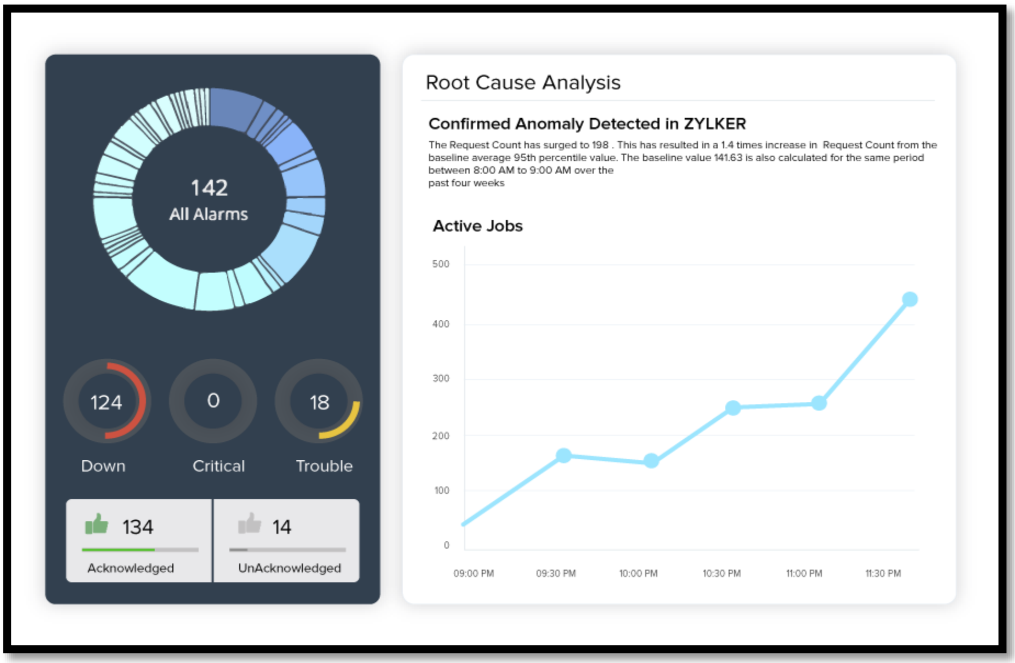

Slowest Method Calls
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
🟩 [custom] GetObfuscatedQueryString()
🟨 [custom] GetObfuscatedQueryStringRegex()
🟥 [custom] Parsing QueryParamsByRegex()
🟦 [custom] CheckingMovie()
🟧 System.Net.HttpWebRequest.GetResponse() [http://site24x7-win2012:2146/MovieService/MovieService.svc]
🟪 other
External Calls
0%
10%
20%
30%
40%
50%
🟩 HTTP CALL
🟥 APP CODE
🟦 MYSQL
🟧 REDIS
arc/data

External Calls	Total Time	Total Count
HTTP CALL	29 ms	22
APP CODE	15.0 sec	1
MYSQL	11 ms	30
REDIS	1 ms	1

Time stamps(ms)	Metric: **Expand All** | **Collapse All**	Exclusive(ms)	Total(ms)
23	Total Calls: 1 Cloud call + 2 Other method calls	1,342	15 sec
13	[custom] CheckingMovie()	486	3.5 sec
23	[cı [custom] GetObfuscatedQueryStringRegex()	134	2 sec
23	co [custom] GetObfuscatedQueryString()	453	845
23	Ur System.Net.HttpWebRequest.GetResponse() [http://site...	342	945
23	com/sample/web/action/DbAction.execute()	453	632

AI-powered Alerts and Reports

- Prevent potential catastrophes with AI-powered alerts.
- Our anomaly detection engine, powered by machine learning and forecasting techniques, detects any unusual behavior or spikes in your application performance and notifies you immediately.
- This helps you take corrective action before your customers are affected.

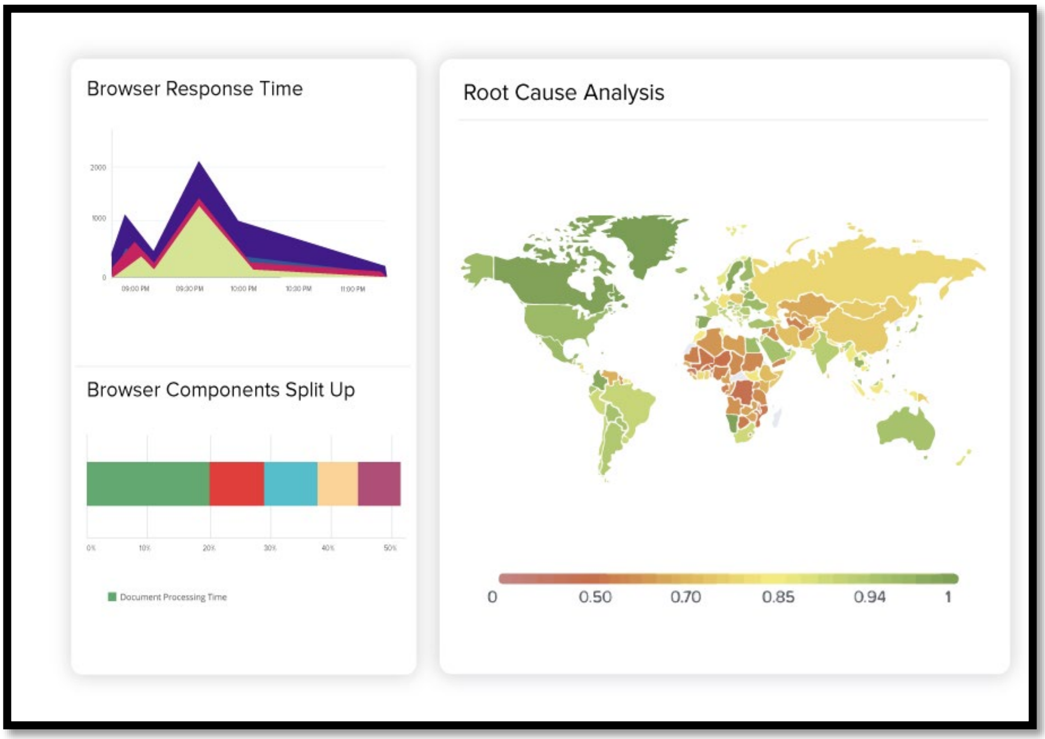


Confirmed Anomaly Detected in ZYLKER

The Request Count has surged to 198 . This has resulted in a 1.4 times increase in Request Count from the baseline average 95th percentile value. The baseline value 141.63 is also calculated for the same period between 8:00 AM to 9:00 AM over the past four weeks

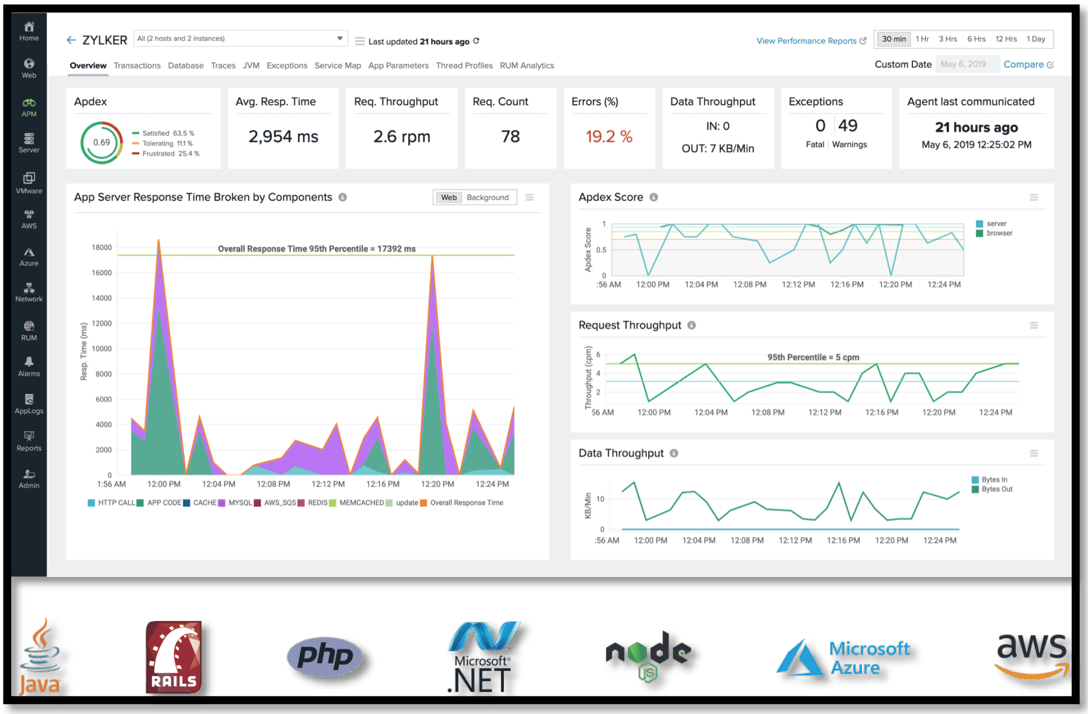
Obtain Complete Context

- Understand how your application performance is perceived by end users across various geographies, in real time.
- Improve front-end performance by fixing JS errors, AJAX calls, and optimize page load time.
- Integrate APM Insight with Real User Monitoring (RUM) to obtain a unified view.



What is application performance monitoring?

- Application performance monitoring (APM) is the process of understanding and optimizing your application behavior.
- APM helps you analyze application performance, gain a holistic view of how application components connect and communicate and in turn, helps you optimize end-user experience.



Apdex: 0.69 — Satisfied 63.5 %, Tolerating 11.1 %, Frustrated 25.4 %

Avg. Resp. Time: 2,954 ms

Req. Throughput: 2.6 rpm

Req. Count: 78

Errors (%): 19.2 %

Data Throughput: IN: 0 OUT: 7 KB/Min

Exceptions: 0 Fatal | 49 Warnings

Agent last communicated: 21 hours ago May 6, 2019 12:25:02 PM

Section 3: Exercises

Exercise 1: Enlist types of IT monitoring.

Exercise 2: Draw Nagios architecture.

Exercise 3: Participate in group discussion on following topics:

a) Types of IT Monitoring
b) IT Monitoring Strategies and Best Practices
c) Benefits and Implementation of Continuous Monitoring
d) Features, Application and Benefits of Nagios
e) Architecture of Nagios
f) Nagios Plugins
g) Nagios Products
h) Advanced Monitoring Tools

Section 4: Assessment Questionnaire

1. What is the necessity of Continuous monitoring?
2. Explain the working of Nagios?
3. What are Plugins in Nagios?
4. Explain the NRPE (Nagios Remote Plugin Executor) in Nagios?
5. Explain how is Nagios helpful in Distributed Monitoring?

6. Justify the statement — Nagios is Object-Oriented?
7. What are the tips for better helpdesk reporting and monitoring?
8. ________ is the process to gather metrics about the operations of an IT environment's hardware and software to ensure everything functions as per fixed standards.
9. Web performance monitoring is designed to monitor the availability of a ______.
10. API monitoring tools and monitoring software provide insight into whether an API is working properly, ensuring minimal downtime. (True/False)
11. Measurements from ______ monitoring software depict data from the current IT environment.
12. What are the two extensions of real-time monitoring?
13. _______ analysis examines one specific event at a particular instant.
14. _______ monitoring is a foundation-level process that collects and reviews metrics concerning the IT environment's hardware and low-level software.
15. What are three IT monitoring entities?
16. _______ are independent programs that install on the monitored device to collect data on hardware or software performance data and report it to a management server.
17. What services can Nagios check?
18. What are the benefits of Nagios?
19. The ______ is a component of server part of Nagios. It sends a signal to execute the plugins at the remote host.
20. Nagios runs both agent-based and agentless configurations. (True/False)

----------End of the Module----------

MODULE 6

Advanced Topics

Section 1: Learning Outcomes

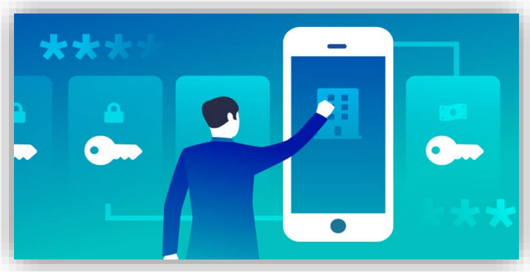
After completing this module, you will be able to:

- Explain tactics of Enterprise Password Management
- Describe significance of using Enterprise Password Management Software
- Protect Privileged Accounts
- Tell various Password Managers used for Business
- Manage Credentials
- Manage Ports and define various Port Numbers
- Explain how do network ports affect cybersecurity?
- Configure Firewalls for Data Traffic
- Open and Close the Local, Outgoing Ports in Windows Firewall
- Change the Default COM Port setting for Multiport Serial Boards
- Set Web Help Desk to run on port 80
- Describe Certificate Lifecycle
- Explain Digital Certificate Creation Process
- Enlist Benefits and Types of Digital Certificates
- Compare the Best IT Service Management Software Tools

Section 2: Relevant Knowledge

6.1 Enterprise Password Managers

What is Enterprise Password Management?



- In any organization, employees must keep their business-related passwords and sensitive information secure.
- That means not reusing passwords, creating unique and strong credentials, and keeping all that information somewhere safe.
- Enterprise Password Management is a password security method that goes beyond simply storing your company's passwords in a secure password vault.
- Managing human and non-human privileged accounts is critical, yet tedious for enterprise IT and security teams.
- Without a centralized password management system, you have no visibility or control to protect privileged accounts from attack.
- Password management software built for the enterprise gives visibility and control to lower privileged account risk.
- A business-grade password manager allows everyone in an organization to spend less time trying to remember strong, unique passwords for all their accounts.
- The password manager stores credentials for each person and helps them generate new, random passwords.

- The best password managers for businesses also let administrators keep an eye on employees' password hygiene.
- You can see which employees have weak or reused passwords, and who's not using multi-factor authentication to secure their accounts, which allows you to prompt them to improve their security.

Enterprise Password Management Software

- Enterprise password management software essentially closes the number-one hole in your attack surface and protects your passwords without slowing down your business by inconveniencing your users.
- Strong passwords are an important security practice. But they aren't enough to prevent a data breach.
- Alarmingly, 20% of companies fail to change default passwords, such as "admin" and "12345."
- Hackers use password cracking techniques, brute-force attacks, and social engineering trickery to steal enterprise passwords.
- If they get their hands on a password that uses an authentication token (password hash), they can "pass-the-hash" to breach multiple systems without requiring multiple passwords.
- Password management software for the enterprise uses security controls to prevent internal and external threats from capturing master passwords, credentials, secrets, tokens, and keys to gain access to confidential systems and data.
- These centralized password management systems can be on-premises or in the cloud. Most important is that they provide password security for all types of privileged accounts throughout your enterprise.
- The more complex the software, the higher the risk of failure.

Automation

- To keep your corporate passwords safe, you just store them in a protected password vault and hide the key.
- You also need to manage role-based access provided by those passwords and keep that access up to date.
- As people leave and projects change, enterprise password management software allows you to change or remove passwords in real-time.
- To mitigate the risk of a data breach, enterprise-level password management solutions monitor password activity and rotate passwords regularly and automatically.
- Password management best practices like password creation, rotation, monitoring, and removal must happen with no disruption to people's work and no downtime for your systems.
- An enterprise password management solution designed to keep people productive eliminates the temptation to share passwords and skirt security controls.

Privileged Access Management (PAM)

- Privileged Access Management (PAM) solutions simplify IT password management.
- Your help desk and IT teams save time with:
  - Automated account provisioning and deprovisioning
  - Automated account discovery
  - Automated password rotation
  - Consolidated reporting and auditing

- IT password management can be further streamlined as your PAM solution is integrated with other critical IT systems, such as IT ticketing systems, and diverse operating systems and platforms.
- PAM is a comprehensive solution for enterprise password management that eliminates drudgery and decreases your risk of attack.
- With PAM software you can rotate passwords without spending hundreds of hours manually changing them and simultaneously update credentials used for services and applications without downtime.
- PAM software has built-in capabilities for workflow and detailed reporting that gives you maximum control and flexibility.
- Modern PAM solutions are available both on-premises and, in the cloud, so you save time and secure privileges across your entire attack surface.

Application Password Management (APM)

- Privileged Access Management extends to non-human account credentials, such as those needed for applications and services to run.
- Application password management is critical because those credentials are not tied to a human.
- As such, they are more difficult to track and can sometimes be found in plain text in the code, applications, and services where they are needed.
- It’s critical to store these credentials in a high-speed vault so they are managed, monitored, and removed according to your security policies.

Auditing and Reporting

- To demonstrate compliance to auditors and return on investment to executives, enterprise password security software provides detailed reporting on security practices you use to manage and protect passwords.

Securing Third Party Access

- Enterprise password protection goes beyond managing internal employee passwords.
- Contractors and partners may also need limited or temporary passwords, which you need to create, manage, and remove when their lifespan is over.
- To keep tabs on third-party behavior in real-time, you may want to require an internal employee to authorize their access or even monitor and record sessions.

On Premises and In Cloud

- Enterprises operate both on-premises and in the cloud. So, enterprise password security software must be designed for both.
- Cloud password management is particularly important for enterprises that have privileged accounts managing cloud-based systems, applications, and development tools.

Managing and securing non-human master passwords

- In addition to users, systems such as databases, applications, and networks all require a robust enterprise password management solution to authenticate and exchange information.
- These accounts aren’t tied to a unique human identity, which means you can’t rely on Identity and Access Management tools to manage them.

Protection of Privileged Accounts

Service Accounts

- Run application services such as Windows Services, scheduled tasks, batch jobs, and Application Pools within IIS.
- Changing passwords for service accounts is tricky because applications are dependent on credentials for daily operations.

Domain Administrator Accounts

- Manage servers and control Active Directory users.
- They also include local domain accounts at the workstation level, which are included by default and allow everyday users excess privileges.

Root Accounts

- Manage Unix/Linux platforms that can be challenging to synchronize and map to Active Directory to ensure accountability.

Networking Accounts

- Represent a full-access pass to critical infrastructures such as firewalls, routers, and switches.
- When these accounts are breached you may never recover.

System Administrator Accounts

- Manage databases that can be difficult to secure and rotate because credentials are often shared among a group of IT administrators who need access in real-time.
- Managing Windows administrator accounts is particularly difficult in a virtualized environment as machines are rapidly deployed.

Application Accounts

- Access and share sensitive information with databases and other applications.
- They include database logins, certificates for software signing, embedded build script passwords, configuration files, and application services used during software development.
- Default privileged credentials or SSH keys are often embedded in clear text or hard coded in applications and can be easily exploited.

Password Managers for Business

Keeper Password Manager & Digital Vault

Keeper Password Manager & Digital Vault helps you generate custom security reports for every user on your business team.

PROS

- Well-designed apps and browsers extensions with cross-platform syncing
- Multi-factor authentication
- Secure password sharing and inheritance
- Optional secure file storage and messaging

- Retains a full history of passwords and files
- Offers a wide variety of record type templates

CONS

- Limited free version

Zoho Vault

Zoho Vault is known for its password-sharing capabilities and integrations with well-known business software.

PROS

- Syncs across Windows, macOS, Android, and iOS devices
- Supports multi-factor authentication
- Accessible across all browsers on any platform
- Handles multipage logins
- Imports passwords from browsers
- Substantial free plan

CONS

- Lacks web form filling
- Unintuitive mini password generator

LastPass

LastPass for Business makes it easy for people who are unfamiliar with password managers to start using it right away and features a comprehensive real-time reporting breakdown of employee password health for managers.

PROS

- Supports many platforms and browsers
- Password strength report and dark web monitoring tools
- Secure sharing and password inheritance
- Two-factor authentication

CONS

- Syncing limitations for free users
- Some personal data types can’t be used for form-filling
- No U2F support
- Some components list out-of-date options

Bitwarden

Bitwarden offers no-frills password management software for businesses and teams which includes a free Families account for each employee.

PROS

- Offers apps for all popular platforms and browsers
- Free tier and inexpensive paid plan
- Supports multi-factor authentication
- Send sharing feature is effective
- Open source

CONS

- Some struggles with automatic capture and autofilling in testing
- Multi-factor authentication via hardware keys limited to paid users
- Premium users only get 1GB encrypted storage by default

Best Password Managers for Business

- Signing up for a business password manager is similar to signing up for a personal or family account.
- You need to create a master password for your account, which is used to encrypt the contents of your business' password vault.
- LastPass allows users to access their vaults with passwordless methods such as a code from an authenticator app or biometric data, which is more secure than using a password.
- After creating the vault, you send out invitations to your employees, asking them to make their accounts.
- Some business password managers include free family plans for employees to encourage proper password hygiene at home.
- After your employees are in the system, ask them to enable multi-factor authentication for their accounts.
- Multi-factor authentication can be biometric, SMS-based, or via time-based one-time passwords via an authenticator app.
- Many business password managers support authentication via hardware security keys, too.

How to Manage Credentials?

- Once you or an employee has a password manager installed and set up, the password manager does much of its job automatically.
- When you log into a secure site, your password manager offers to save your credentials, so it can fill in the information when you return to the site later.
- Many password managers offer a browser extension that saves a list of your logins so you can click on a web address and log in automatically.
- Most password managers can also fill in personal or company data on web forms, which is more secure and less prone to errors than typing in information manually.
- You can edit and store sensitive company information in the password manager's encrypted vault.
- Storing payment and identity details in your company's vault is more secure than saving them to your browser.
- People come and go from workplaces, and sometimes the partings are less than amicable.

- What happens when an employee refuses to relinquish logins when they leave? Having one person holding all the keys to the castle is a recipe for disaster.
- Some password managers for business clients have a feature allowing managers to take control of employees' credentials located in their work vaults.
- This makes it easier for administrators to transfer logins to new hires and maintain a secure digital workplace.

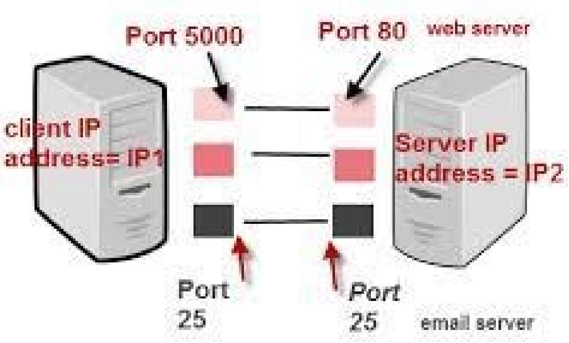
Password Managers: Enterprise-Focused Features

- Sharing is an important function for business-related password managers. We don’t recommend sharing passwords, but if you must do it, a password manager is your safest option.
- Employees often need to share company information and notes with other employees and administrators.
- Some password managers let you share a login without making the password visible and let you revoke the shared details once the other person has used them or make the recipient the owner of the credential.
- Many password managers offer single sign-on or integrations with business software such as Zoom or Google Workspace.
- These integrations add another layer of convenience and security for your business as employees don’t have to enter passwords whenever they need to use various work-related applications.

6.2 Managing Ports

What is Port?

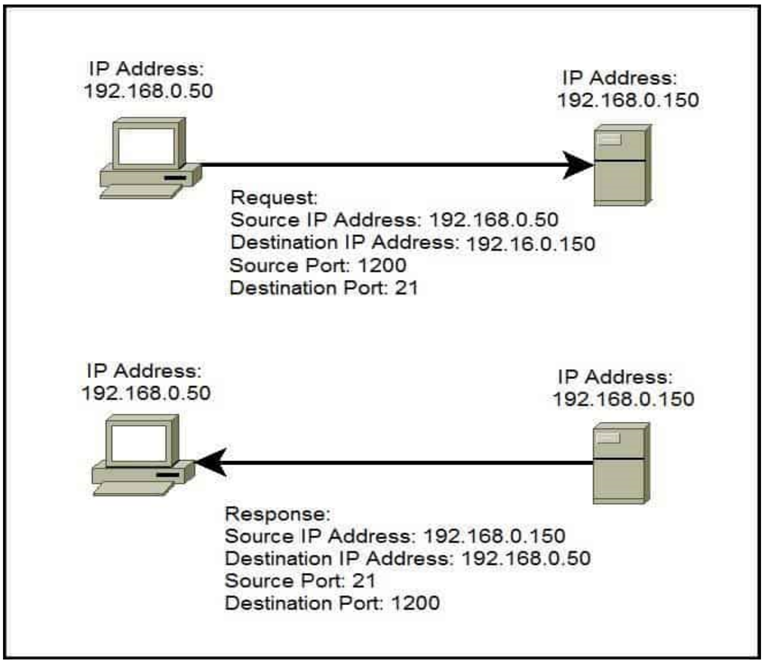
- A port in **networking** is a software-defined number associated to a network protocol that receives or transmits communication for a specific service.
- A port in **computer hardware** is a jack or socket that peripheral hardware plugs into.
- A port in **computer software** is when a piece of software has been translated or converted to run on different hardware or operating system (OS) than it was originally designed for.
- Between the protocols User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), there are 65,535 ports available for communication between devices.



IP Address + Port number = Socket

TCP/IP Ports And Sockets

- A port in computer networking is how a computer can use a single physical network connection to handle many incoming and outgoing requests by assigning a port number to each. The numbers go from 0 to 65535, which is a 16-bit number.



- Some of these port numbers are specifically defined and always associated with a specific type of service.
- For example, File Transfer Protocol (FTP) is always port number 21 and Hypertext Transfer Protocol web traffic is always port 80. These are called *well-known ports* and go from 0 to 1023.

Well-known Ports

Ports in the range 0 to 1023 are assigned and controlled.

Registered Ports

Ports in the range 1024 to 49151 are not assigned or controlled but can be registered to prevent duplication.

Dynamic Ports

- Ports in the range 49152 to 65535 are not assigned, controlled, or registered. They are used for temporary or private ports.
- They are also known as private or non-reserved ports.
- Clients should choose ephemeral port numbers from this range, but many systems do not.
- The port is specified by having the URL or IP address followed by a colon then the port number -- as examples, 10.0.0.1:80 or www.techtarget.com:443.
- With all internet communication, there is always an associated port, but it may not be shown to the user as it is often implied by the type of communication.
- A computer can manage many simultaneous connections on a single inbound port. This is because the local IP address, local port, remote IP address and remote port specify each connection.
- A listening port is when the computer is actively waiting for inbound requests on that port number, allowing those connections.
- Port forwarding is when communication to one address on a specific port is then sent, or forwarded, to another computer for processing.

Port Numbers

Some of the most commonly used ports, along with their associated networking protocol, are:

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Port 25:** Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.
- **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
- **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.
- **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.
- **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.
- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

How do network ports affect cybersecurity?

Network ports are a major factor in network security and cybersecurity in general.

Port Scanning

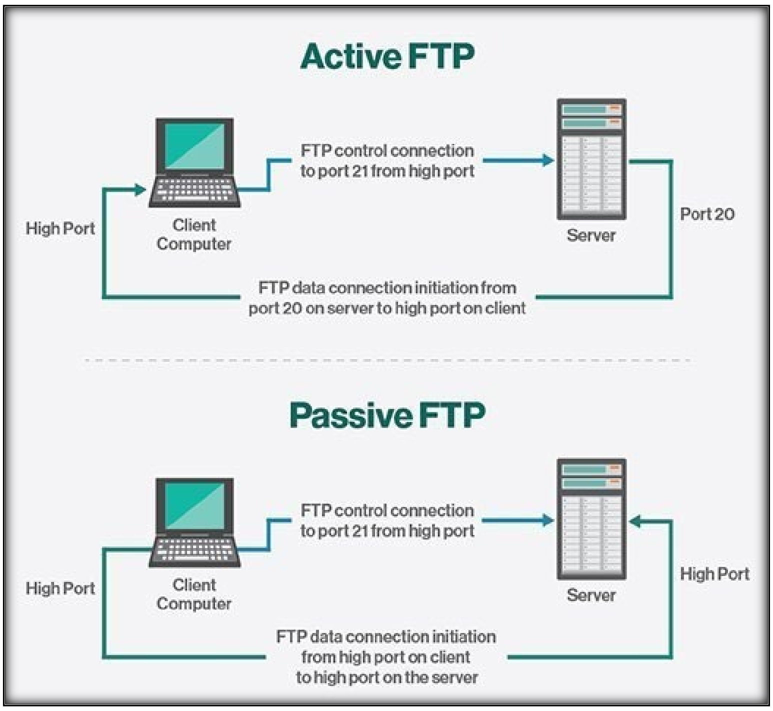
Tries all ports at an address to see which ones are open and listening. Attackers can use this to find vulnerable services that they can then attack.

Firewalls

- Firewalls take the port number into consideration when determining to allow or block communication.
- They are configured to only allow communication to the specific ports needed for a service and block other unneeded ports so they cannot be exploited.

Example

- A company wants to have a website, email and secure file transfer service on the internet.
- Its firewall would allow inbound connections to ports 80 and 443 for web traffic, port 25 for inbound email and port 22 for Secure Shell FTP (SFTP).
- It forwards these ports to the specific servers for each type of service.
- The firewall will block all other ports.
- So, if an employee incorrectly tries to use FTP on port 21 instead of SFTP, it will be blocked.
- For instance, if an attacker tries to connect to port 3389 for Windows Remote Desktop to gain control of a server, the firewall will block the connection.


Active FTP
FTP control connection to port 21 from high port
High Port
Client Computer
Server
Port 20
FTP data connection initiation from port 20 on server to high port on client
Passive FTP
FTP control connection to port 21 from high port
High Port
Client Computer
Server
High Port
FTP data connection initiation from high port on client to high port on the server

Web Helpdesk Ports (Solarwinds)

The following table lists the Web Help Desk ports for secure and non-secure interface traffic.

Port	Type	Description
80	TCP	Non-secure traffic from the Web Help Desk Console (VA)
135	TCP	Asset Discovery using Windows Management Instrumentation (WMI)
389	TCP	Non-secure traffic from the Web Help Desk server to a designated server (usually a domain controller) for use with the Directory Service tool (LDAP and Active Directory)
443	TCP	Secure traffic from the Web Help Desk Console
8081	TCP	Non-secure traffic from the Web Help Desk Console (Windows, Linux and OSX)
8443	TCP	(Default) Secure traffic from the Web Help Desk Administrator Console (Windows, Linux and OS X)
17778	TCP	Communications from the SolarWinds Orion server (Orion integration only)
61616	TCP	Web Help Desk Discovery engine (JMS queue port)

Databases (Solarwinds)

The following table lists the Web Help Desk ports for external and embedded database communications.

Port	Type	Description
1433	TCP	Communications with a Microsoft SQL external database, including: ▪ Microsoft SQL Server ▪ Microsoft Systems Management Server ▪ Microsoft System Center Configuration Manager (SCCM) ▪ SolarWinds Network Configuration Manager (NCM) ▪ SolarWinds Network Performance Monitor (NCM) ▪ SolarWinds Server and Application Monitor (SAM)
3306	TCP	External MySQL database
5432	TCP	Communication with an External PostgreSQL database
20293	TCP	Communications with an embedded PostgreSQL database

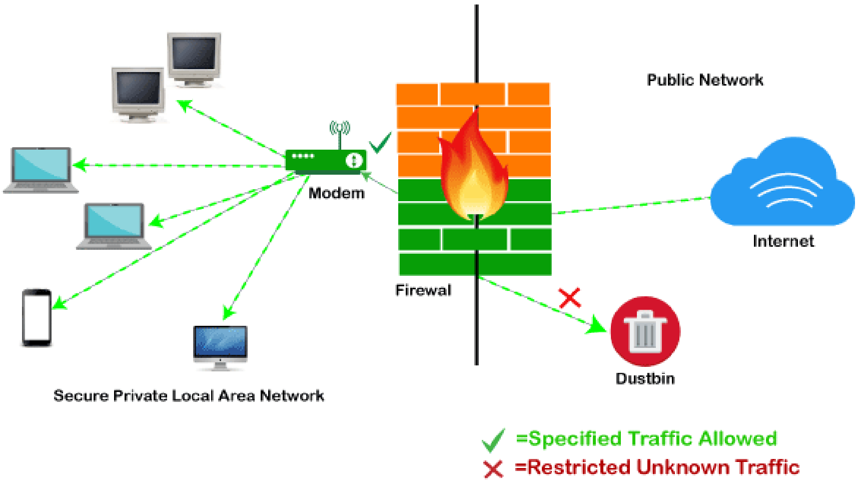
Email (Solarwinds)

The following table lists the Web Help Desk ports for email traffic.

Port	Type	Description
25	TCP	Traffic from the Web Help Desk server to your email server for automated email notifications
80	TCP	Non-secure connection with Microsoft Exchange Web Services (EWS)
110	TCP	Non-secure traffic with the POP3 mail server
143	TCP	Non-secure traffic with the Internet Message Access Protocol (IMAP) mail server
443	TCP	Secure traffic with EWS
993	TCP	Secure traffic with the IMAP mail server
995	TCP	Secure traffic with the POP3 mail server

Configure Firewalls for Data Traffic

- A firewall is a security system that blocks or allows network traffic based on a set of security rules.
- Firewalls usually sit between a trusted network and an untrusted network; often the untrusted network is the Internet.
- For example, office networks often use a firewall to protect their network from online threats.
- Firewalls between any two points of communication must have the requisite ports open to inbound or outbound traffic according to the relative direction of the communication traffic.
- Properly configured firewalls block traffic to all ports by default except for a few predetermined ports known to be in common use.
- For instance, a corporate firewall could only leave open ports 25 (email), 80 (web traffic), 443 (web traffic), and a few others, allowing internal employees to use these essential services, then block the rest of the 65,000+ ports.

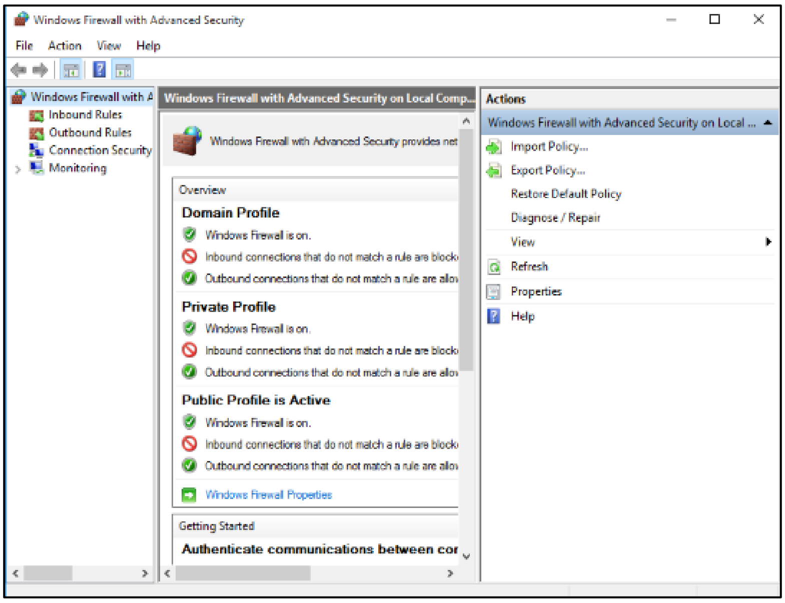

Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

Open Local Ports in Windows Firewall

To open local port 80 in Windows Firewall, please refer to the following detailed steps:

1. From the **Start** menu, click **Control Panel**, click **System and Security**, and then click **Windows Firewall**. Control Panel is not configured for 'Category' view, you only need to select **Windows Firewall**.
2. Click **Advanced Settings**.

3. Click **Inbound Rules**.
4. Click **New Rule** in the **Actions** window.
5. Click **Rule Type** of **Port**.



Windows Firewall with Advanced Security provides net

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are block
- Outbound connections that do not match a rule are allov

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are block
- Outbound connections that do not match a rule are allov

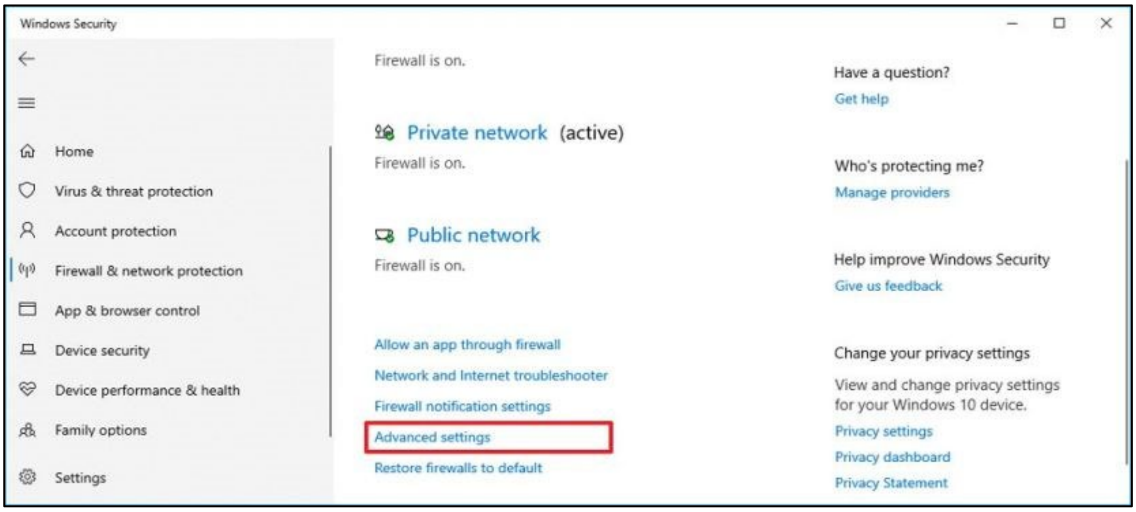
Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are block
- Outbound connections that do not match a rule are allov

Windows Firewall Properties

Getting Started

Authenticate communications between cor


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Get help
Manage providers
Give us feedback
Privacy settings
Privacy dashboard
Privacy Statement

Firewall is on.

Private network (active)

Firewall is on.

Public network

Firewall is on.

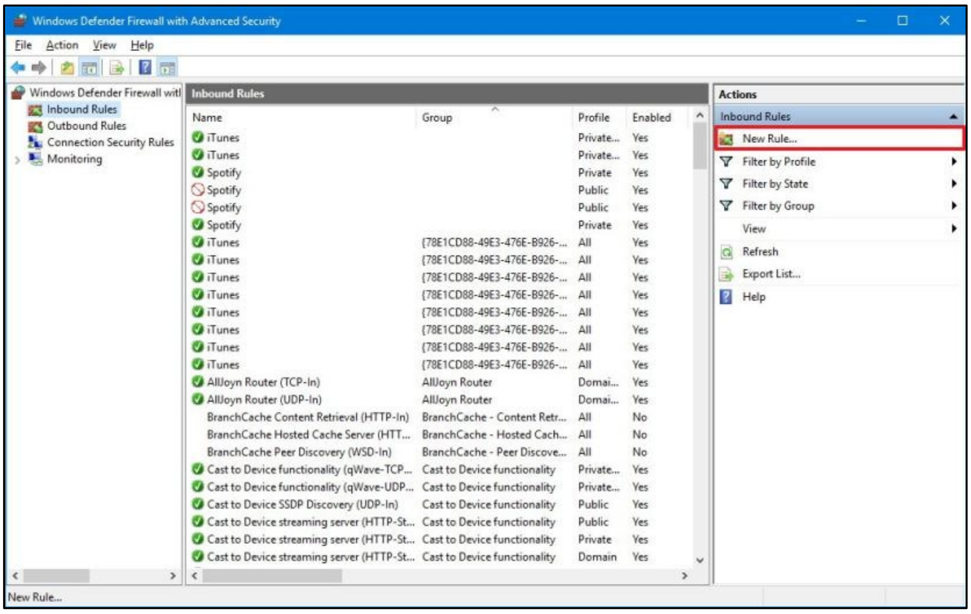
Have a question?

Who's protecting me?

Help improve Windows Security

Change your privacy settings

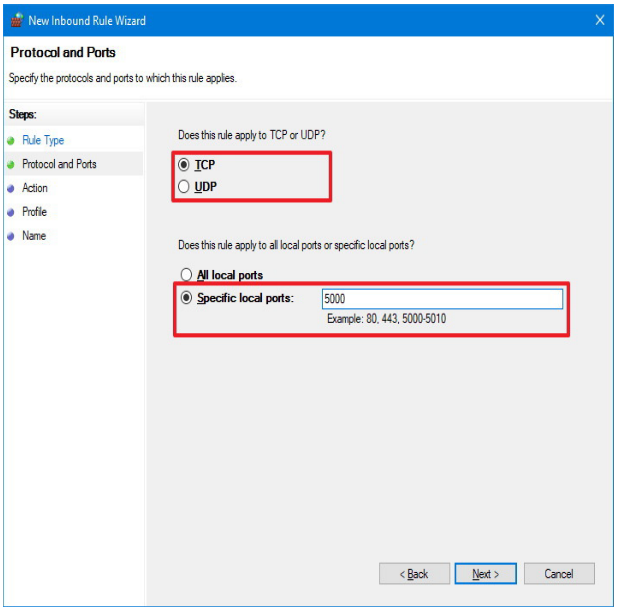
View and change privacy settings for your Windows 10 device.



Inbound Rules

Name	Group	Profile	Enabled
iTunes		Private...	Yes
iTunes		Private...	Yes
Spotify		Private	Yes
Spotify		Public	Yes
Spotify		Public	Yes
Spotify		Private	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes

6. Click Next.
7. On the Protocol and Ports page click TCP.
8. Select Specific Local Ports and type a value of 80.
9. Click Next.
10. On the Action page click Allow the connection.
11. Click Next



Protocol and Ports

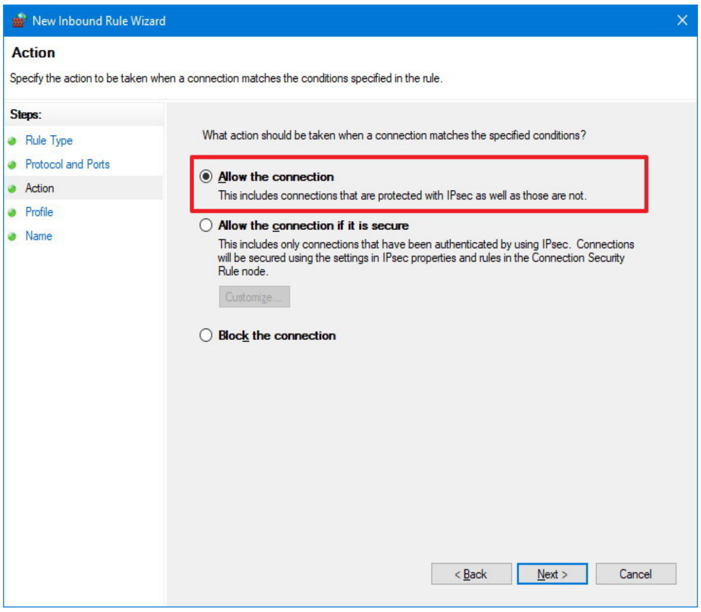
Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 5000
Example: 80, 443, 5000-5010



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

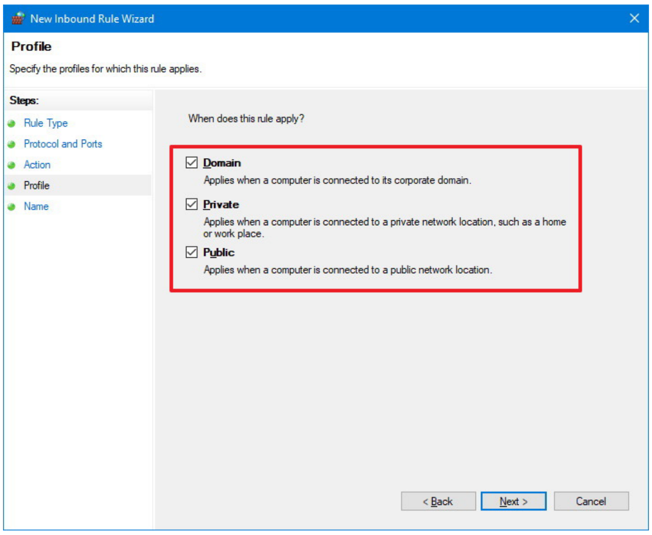
● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

12. On the **Profile** page click the appropriate options for your environment.
13. Click **Next**
14. On the **Name** page enter a name
15. Click **Finish**.

16. Restart the computer.


New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

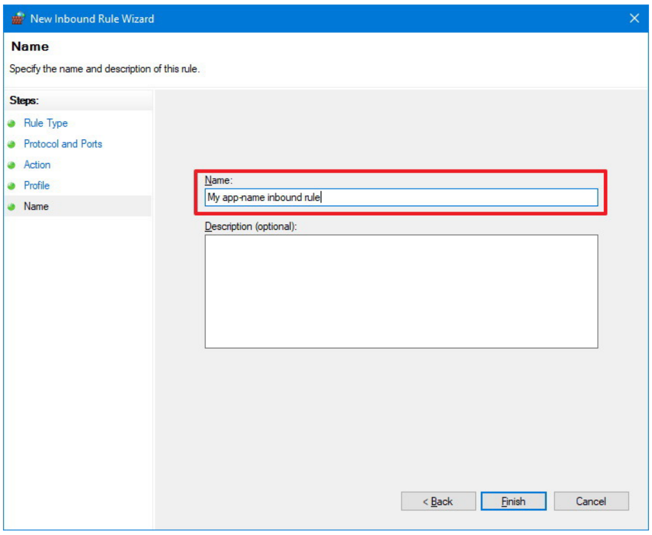
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.


New Inbound Rule Wizard

Name

Specify the name and description of this rule.

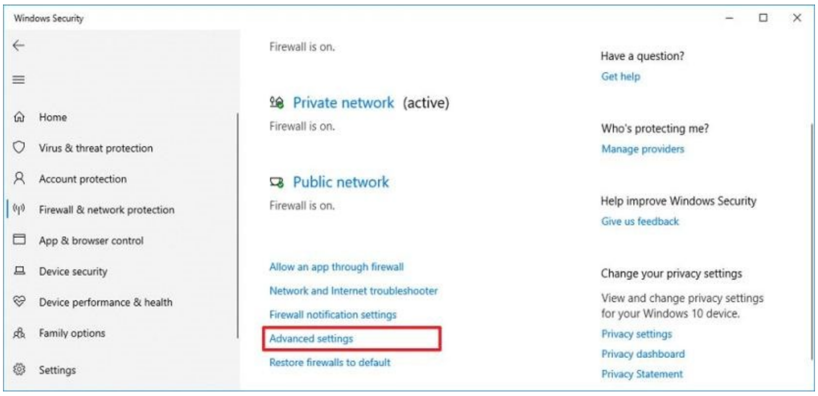
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: My app-name inbound rule

Description (optional):

Open Outgoing Ports in Windows Firewall

1. Open Windows Security.
2. Click on Firewall & network protection.
3. Click the Advanced settings option.
4. Click on Outbound Rules in the left navigation pane.

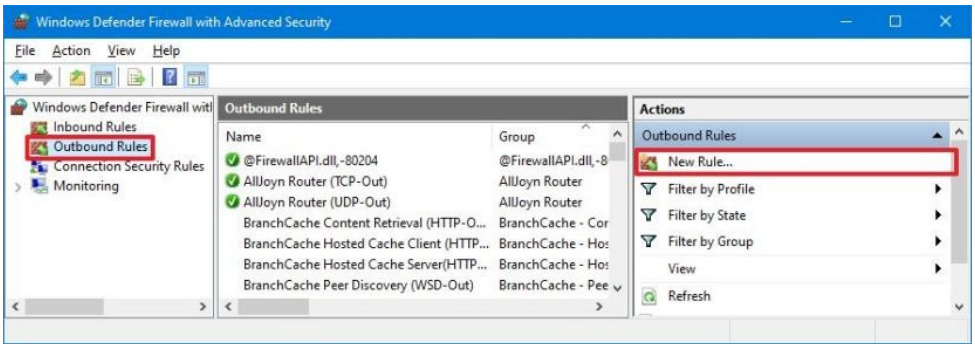

Windows Security

Firewall is on.

Private network (active)
Firewall is on.

Public network
Firewall is on.

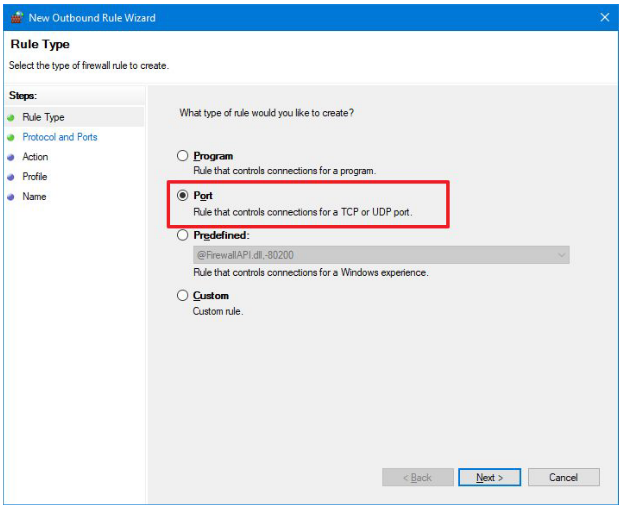
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement


Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-8
AllJoyn Router (TCP-Out)	AllJoyn Router
AllJoyn Router (UDP-Out)	AllJoyn Router
BranchCache Content Retrieval (HTTP-O...	BranchCache - Cor
BranchCache Hosted Cache Client (HTTP...	BranchCache - Ho:
BranchCache Hosted Cache Server(HTTP...	BranchCache - Ho:
BranchCache Peer Discovery (WSD-Out)	BranchCache - Pee

5. Under the “Actions” section, click the New Rule option in the right pane.
6. Select the Port option.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

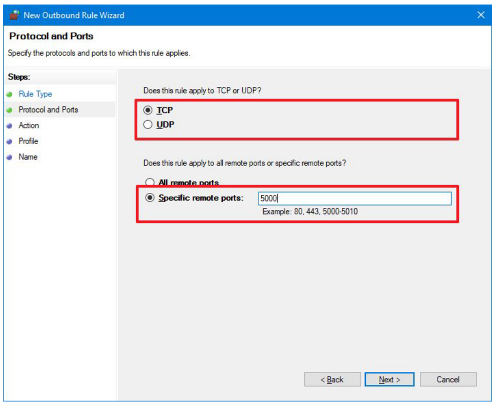
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

7. Click the Next button.
8. Select the appropriate protocol (TCP or UDP) depending on the application.



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

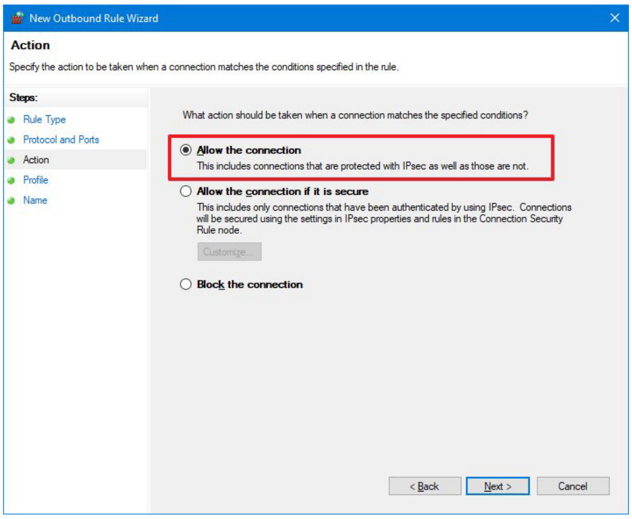
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all remote ports or specific remote ports?

○ **All remote ports**
● **Specific remote ports:** 5000
Example: 80, 443, 5000-5010

9. In the Specific local ports setting, type the port number.
10. Click the Next button.
11. Select the Allow the connection option.
12. Click the Next button.
13. Select the network type to apply the new rule.
14. Click the Next button.
15. Type a descriptive name for the rule.
16. Click the Finish button.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

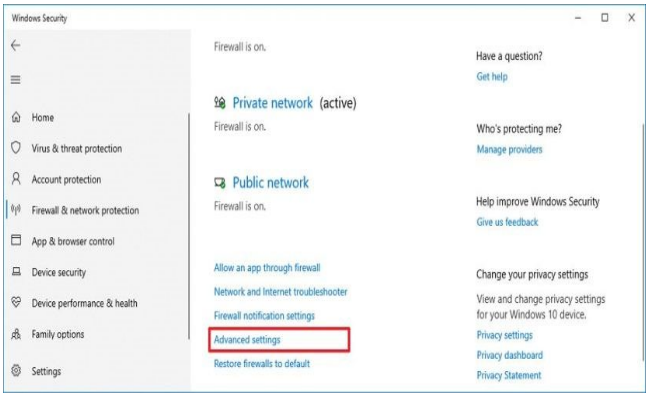
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

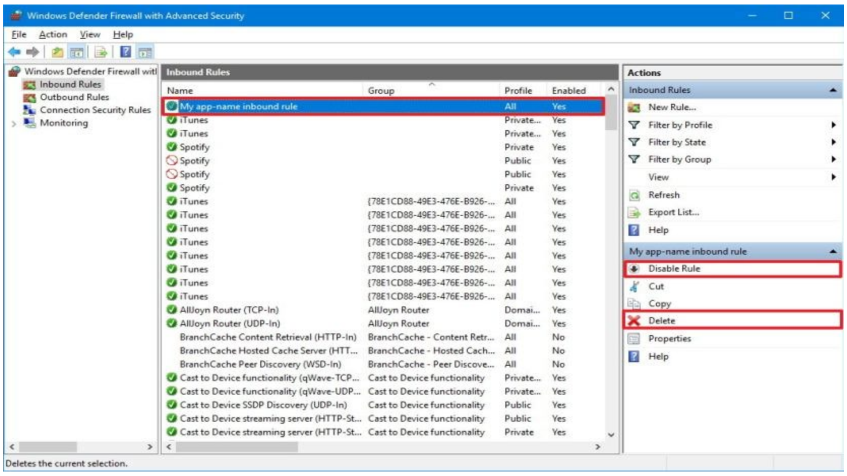
○ **Block the connection**

Close Firewall Port on Windows 10



To close the port in the Microsoft Defender Firewall, use these steps:

1. Open Windows Security.
2. Click on Firewall & network protection.
3. Click the Advanced settings option.
4. Click on Inbound Rules or Outbound Rules from the left navigation pane, depending on where you open the firewall port.
5. Select the rule you want.
6. Under the "Actions" section, click the Disable Rule to close the port while keeping the rule. Or click the Delete Rule option to close the port and remove the rule from the firewall.



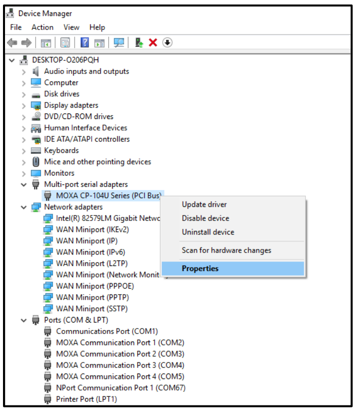
Name	Group	Profile	Enabled
My app-name inbound rule		All	Yes
iTunes		Private...	Yes
iTunes		Private...	Yes
Spotify		Private	Yes
Spotify		Public	Yes
Spotify		Public	Yes
Spotify		Private	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
iTunes	{78E1CD88-49E3-476E-B926-...	All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes

After you complete the steps, the app or service will no longer have access to the network or internet because it'll be blocked by the Windows firewall.

Changing the default COM port setting for multiport serial boards

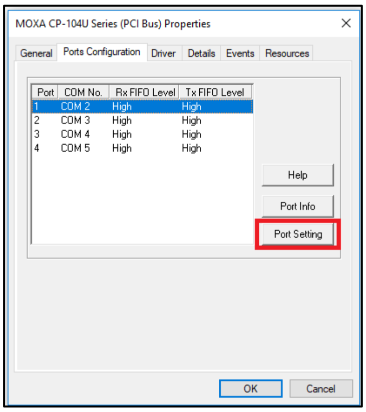
- Some user applications may use a specific COM port requiring a change in the default COM port setting for multiport serial boards.

- To change the default COM port used to communicate with multiport serial boards, perform given actions:



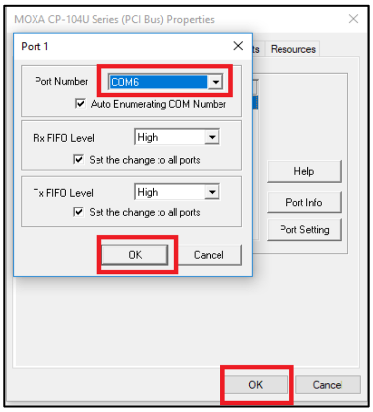
Device Manager

- DESKTOP-O206PQH
  - Audio inputs and outputs
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Multi-port serial adapters
    - MOXA CP-104U Series (PCI Bus)
  - Network adapters
    - Intel(R) 82579LM Gigabit Netwc
    - WAN Miniport (IKEv2)
    - WAN Miniport (IP)
    - WAN Miniport (IPv6)
    - WAN Miniport (L2TP)
    - WAN Miniport (Network Monit
    - WAN Miniport (PPPOE)
    - WAN Miniport (PPTP)
    - WAN Miniport (SSTP)
  - Ports (COM & LPT)
    - Communications Port (COM1)
    - MOXA Communication Port 1 (COM2)
    - MOXA Communication Port 2 (COM3)
    - MOXA Communication Port 3 (COM4)
    - MOXA Communication Port 4 (COM5)
    - NPort Communication Port 1 (COM67)
    - Printer Port (LPT1)



MOXA CP-104U Series (PCI Bus) Properties

Port	COM No.	Rx FIFO Level	Tx FIFO Level
1	COM 2	High	High
2	COM 3	High	High
3	COM 4	High	High
4	COM 5	High	High



MOXA CP-104U Series (PCI Bus) Properties

Port 1

Port Number: COM6

☑ Auto Enumerating COM Number

Rx FIFO Level: High

☑ Set the change to all ports

Tx FIFO Level: High

☑ Set the change to all ports

1. Go to **Windows Device manager > Multi-port serial adapters**.
2. Select the adapter and right click to open the menu.
3. Click on the **Properties** link.
4. Open the **Ports Configuration** tab.
5. Click on the **Port Setting** button.
6. Select the **Port Number** and click **OK**.
7. Click **OK** to apply the changes.

Set Web Help Desk to run on port 80

- This article describes how to configure Web Help Desk to run on HTTP port 80 instead of HTTPS port 8081.
- By default, Web Help Desk runs on HTTPS port 8081.
- If you do not need Microsoft Internet Information Services (IIS), you can configure Web Help Desk to run on HTTP port 80.

Environment

- WHD 12.4;WHD 12.5;WHD 12.6;WHD 12.7

RESOLUTION

By default, Web Help Desk runs on HTTPS port 8081. To configure Web Help Desk to run on HTTP port 80:

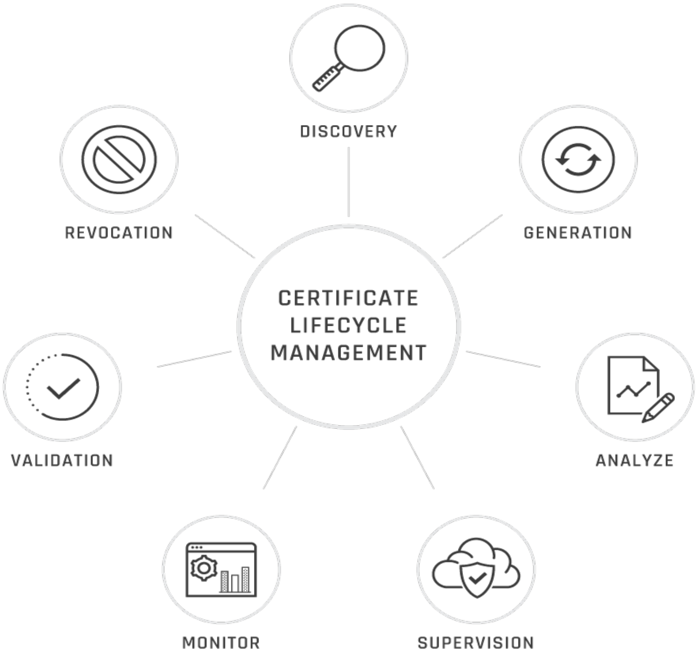
1. Log in to the Web Help Desk server as an administrator.
2. Stop IIS.
   - Open Services in the Windows operating system.
   - Stop the Word Wide Web Publishing Service.
   - Close the Services window.
3. Stop Web Help Desk.
4. Navigate to the Web Help Desk home directory.
   - **Apple OSX:** /Library/WebHelpDesk
   - **Microsoft Windows:** \Program Files\WebHelpDesk\conf\
   - **Linux:** /user/local/webhelpdesk
5. In the home directory, open the whd.conf file in a text editor.

6. Set the DEFAULT_PORT variable to 80, and then save the file.
7. Start Web Help Desk. You can now access Web Help Desk through port 80. If you cannot access Web Help Desk, clear your browser cache and try again.

6.3 Managing Certificates

What is Certificate Management in IT?

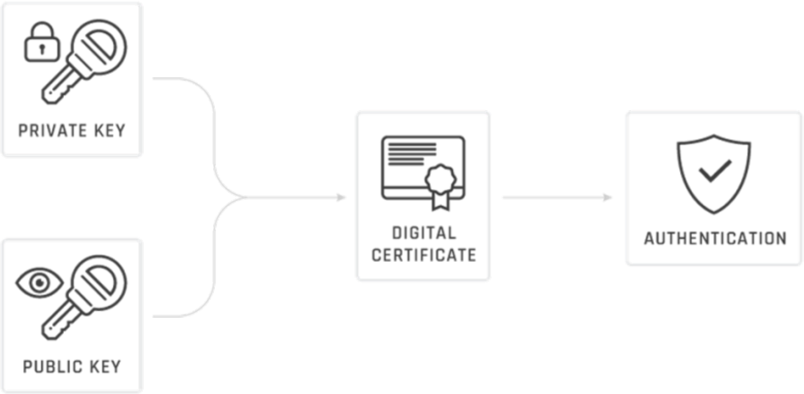
- Certificate management is the process through which an organization monitors and manages the lifecycle of all certificates deployed in a network.



- Management Certificate is the process of monitoring, processing, and executing every process in a certificate's lifecycle.
- Certificate management is responsible for issuing, renewing, and deploying certificates to endpoints (servers, appliances, devices, etc.) so that network services are uninterrupted.
- Certificate management should also automate tasks (issuing, renewal, and so on), as well as provide real time status of the infrastructure of the network.
- Certificate management helps manage the network and prevent interruptions and downtime, while providing a detailed monitoring of the whole infrastructure.
- Good certificate management plans should be able to handle any network, even ones with thousands of devices.
- If a certificate expires or is misconfigured, catastrophic outages all over the network may occur.

Digital Certificate

- A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).
- Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks.



- Certificates are linked with a public/private key pair and verify that the public key, which is matched with the valid certificate, can be trusted.
- The main job of a certificate is to ensure that data sent across a connection between a user and a server is kept private.
- Use of digital certificates is to confirm the authenticity of a website to a web browser, which is also known as a secure sockets layer or SSL certificate.
- A digital certificate contains identifiable information, such as a user's name, company, or department and a device's Internet Protocol (IP) address or serial number.
- Digital certificates contain a copy of a public key from the certificate holder, which needs to be matched to a corresponding private key to verify it is real.
- A public key certificate is issued by certificate authorities (CAs), which sign certificates to verify the identity of the requesting device or user.

Benefits of Digital Certification

- Digital certificates can be requested by individuals, organizations, and websites.
- To do so, they provide the information to be validated and a public key through a certificate signing request.
- The information is validated by a publicly trusted CA, which signs it with a key that provides a chain of trust to the certificate.
- This enables the certificate to be used to prove the authenticity of a document, for client authentication, or to provide proof of a website's credential.

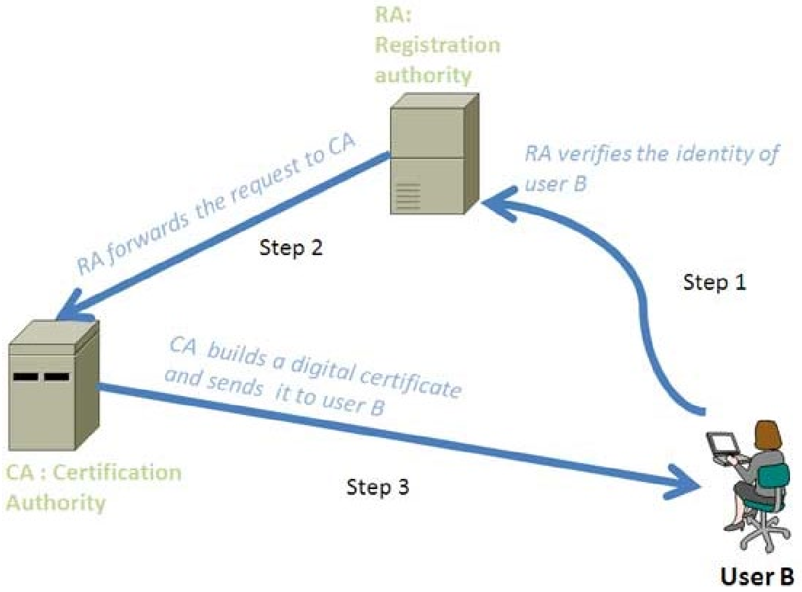
Who can Issue Digital Certificate?

- Digital certificates are issued by CAs, which sign a certificate to prove the authenticity of the individual or organization that issued the request.
- A CA is responsible for managing domain control verification and verifying that the public key attached to the certificate belongs to the user or organization that requested it.
- They play an important part in the PKI process and keeping internet traffic secure.
- To ensure a certificate authority can be trusted, the chain of trust of the CA can be followed back to the source CA.
- A chain of trust is a chain of certificates published by trusted CAs, leading all the way back to the Root CA.
- The other option to get a certificate is to create one yourself using the same information, and then to self-sign it.
- This is used less often, because the identity of the signer cannot be verified with other trusted CAs, thus rendering the self-signed certificate suspicious.

- Due to this, many will not accept a self-signed certificate, so using a CA to create a certificate is the suggested method.

Digital Certificate Creation Process

- A digital certificate is a way to confirm the identity of a public key owner.
- Normally, a third-party organization, known as CA (certification authority), is responsible for confirming or binding the identity of a digital certificate owner.
- It is used to establish secure communication between two parties who are unknown to each other or have lack of trust.
- Digital certificate can assure that the person who you can want to establish communication is actually the person who he claims to be.
- The main reason of using digital certificate is building trust between two parties who want to communicate securely.


RA: Registration authority
RA verifies the identity of user B
Step 1
RA forwards the request to CA
Step 2
CA builds a digital certificate and sends it to user B
Step 3
CA : Certification Authority
User B

For example, user A wants to communicate with user B securely. User B needs a digital certificate for secure communication. At first, user B needs to acquire a digital certificate from a CA (certificate authority). In order to receive a certificate user B use the following process:

Step 1

- In order to obtain a digital certificate, for the first time, user B sends a request to RA (registration authority).
- RA is responsible for verifying the requester’s identity; it does not issue any certificate. B may use its driving license, business document or any other identity information to prove its identity to the RA.
- Once the RA is satisfied with B’s identity information, it sends the request to the CA, on behalf of user B, for issuing a digital certificate.

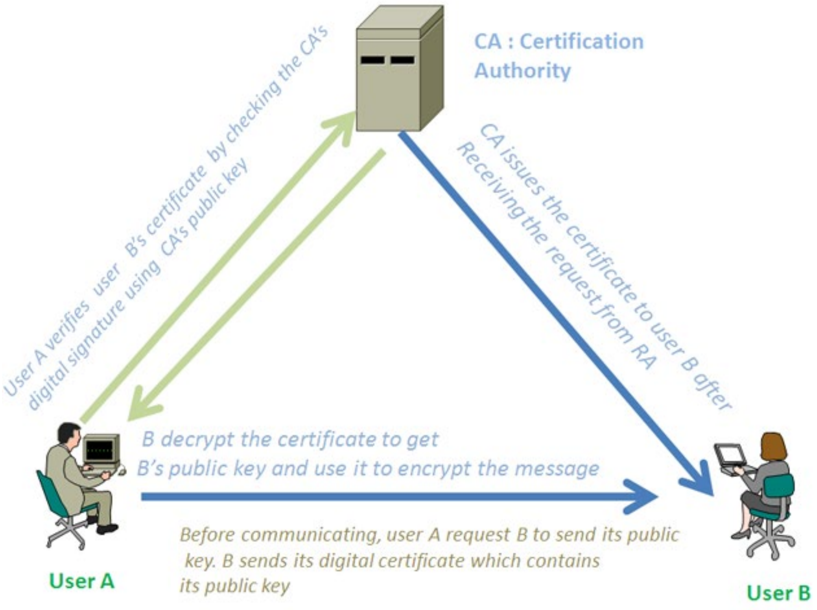
Step 2

- CS creates the digital certificate using B’s public key and other identity information.
- The standard used to create this certificate is x.509.
- The public/private key pair can be create either by the CA or by the user B.
- When the CA created the public key on behalf of the user, then it needs to send the private key securely to B.

- If B creates public and private key pair, it needs to send the public key securely to the CA in order to create the digital certificate.

Step 3

- The CA signs the certificate with its own private key in order to ensure the authenticity, integrity and non-repudiation of the digital certificate.
- Finally, the CA sends back the certificate to B, which can be used to establish secure communication.


CA : Certification Authority
User A verifies user B's certificate by checking the CA's digital signature using CA's public key
CA issues the certificate to user B after Receiving the request from RA
B decrypt the certificate to get B's public key and use it to encrypt the message
Before communicating, user A request B to send its public key. B sends its digital certificate which contains its public key
User A
User B

Simplified diagram: Secure communication with digital certificate

The above steps make sure the user B has a digital certificate that another user A can use to start communicating with B. To start a communication using B's digital certificate, A uses the following steps:

1. A sends a request for B's digital certificate to a certificate repository, also known as public directory, which is a part of CA.
2. When A receives B's certificate it verifies it with the help of web browser by checking digital signature of the CA using the public key of the CA. Then A uses the B's public key supplied by the certificate to encrypt the message.
3. When B receives the encrypted message, it uses its own private key to decrypt the message. Remember that no one except A will be able to decrypt this message because A's private key is not shared with anyone.

Beneficial Features of Digital Certificate

Digital certificates are becoming increasingly important, as cyberattacks continue to increase in both volume and sophistication. Key benefits of digital certificates include:

Security

- Digital certificates encrypt internal and external communications to prevent attackers from intercepting and stealing sensitive data.
- For example, a TLS/SSL certificate encrypts data between a web server and a web browser, ensuring an attacker cannot intercept website visitors' data.

Scalability

- Digital certificates provide businesses of all shapes and sizes with the same encryption quality.
- They are highly scalable, which means they can easily be issued, revoked, and renewed in seconds, used to secure user devices, and managed through a centralized platform.

Authenticity

- Digital certificates are crucial to ensuring the authenticity of online communication in the age of widespread cyberattacks.
- They make sure that users' messages will always reach their intended recipient—and only reach their intended recipient.
- TLS/SSL certificates encrypt websites, Secure/Multipurpose Internet Mail Extensions (S/MIME) encrypt email communication, and document-signing certificates can be used for digital document sharing.

Reliability

- Only publicly trusted CAs can issue digital certificates.
- Obtaining one requires rigorous vetting, which ensures hackers or fake organizations cannot trick victims that use a digital certificate.

Public Trust

- Using a digital certificate provides confirmation that a website is genuine, and that documents and emails are authentic.
- This projects public trust, assuring clients that they are dealing with a genuine company that values their security and privacy.

Digital Certificate and Digital Signature

- A digital certificate is a file that verifies the identity of a device or user and enables encrypted connections.
- A digital signature is a hashing approach that uses a numeric string to provide authenticity and validate identity.
- A digital signature is typically fixed to a document or email using a cryptographic key.
- The signature is hashed, and when the recipient receives it, it performs that same hash function to decrypt the message.

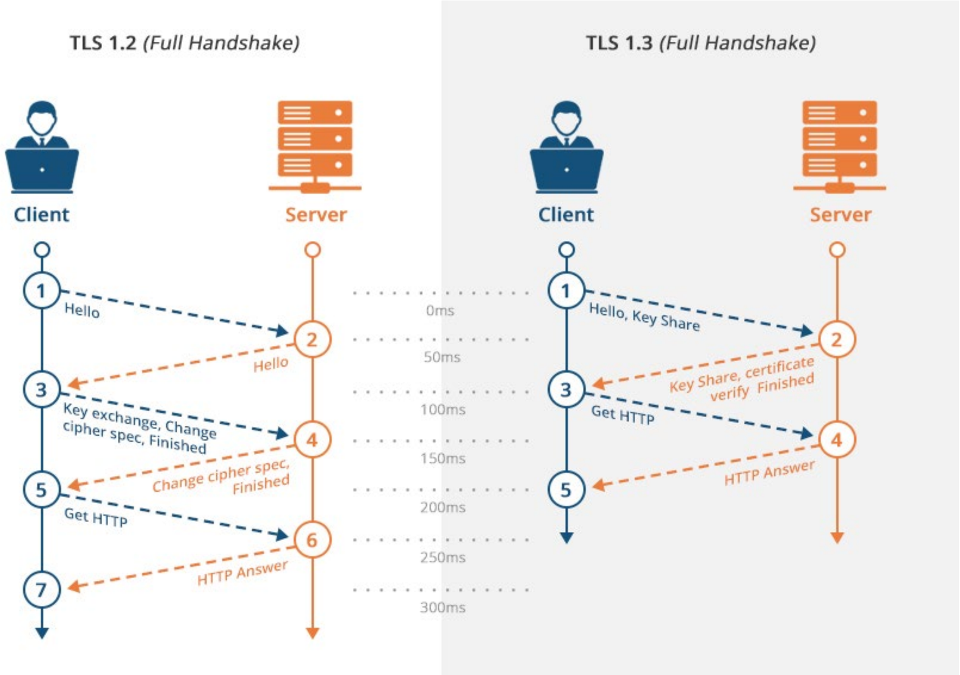
Types of Digital Certificates

There are three different types of public key certificates:

- Transport Layer Security (TLS /SSL) Certificate
- Code Signing Certificate
- Client Certificate

TLS/SSL Certificate

- A TLS/SSL certificate sits on a server, such as an application, mail, or web server to ensure communication with its clients is private and encrypted.
- The certificate provides authentication for the server to send and receive encrypted messages to clients.
- The certificates do this by encrypting and decrypting data as it is sent across the connection. This is achieved through something called an SSL/TLS Handshake.
- SSL/TLS certificate is a digital identifier for users, devices, and other endpoints within a network.



- The existence of a TLS/SSL certificate is signified by the Hypertext Transfer Protocol Secure (HTTPS) designation at the start of a Uniform Resource Locator (URL) or web address. It comes in three forms.
  - Domain
  - Organization
  - Extended

Domain Validated

- A domain validated certificate is a quick validation method that is acceptable for any website.
- It is cheap to obtain and can be issued in a matter of minutes.

Organization Validated

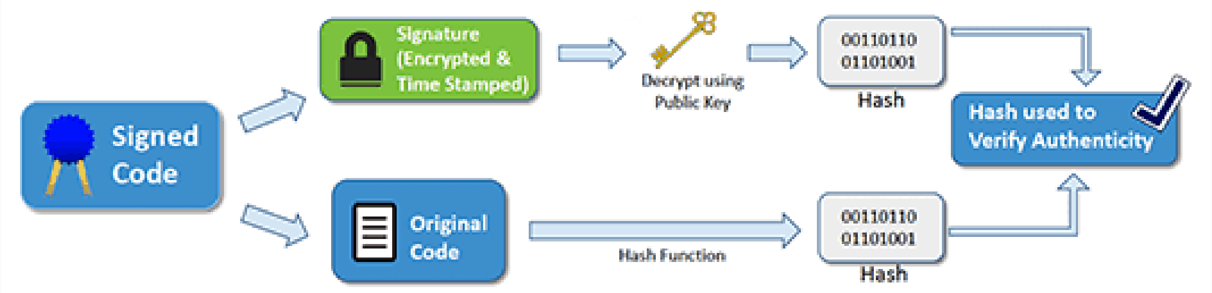
- This provides light business authentication and is ideal for organizations selling products online through e-commerce.

Extended Validation

- This offers full business authentication, which is required by larger organizations or any business dealing with highly sensitive information.
- It is typically used by businesses in the financial industry and offers the highest level of authentication, security, and trust.

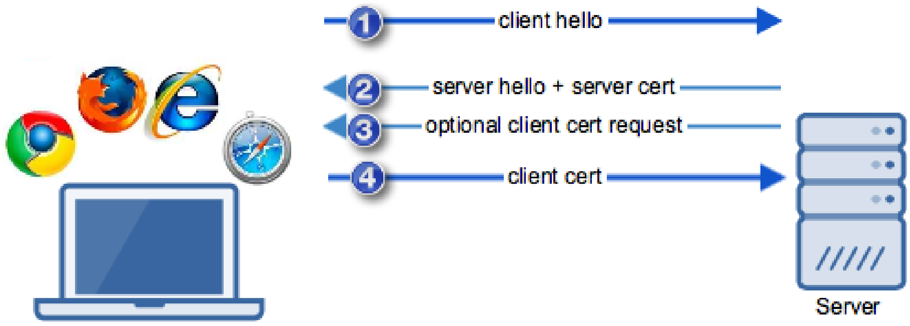
Code Signing Certificate

- A code signing certificate is used to confirm the authenticity of software or files downloaded through the internet.
- The developer or publisher signs the software to confirm that it is genuine to users that download it.
- This is useful for software providers that make their programs available on third-party sites to prove that files have not been tampered with.



Client Certificate

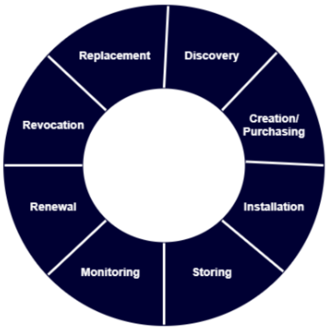
- A client certificate is a digital ID that identifies an individual user to another user or machine, or one machine to another.
- A common example of this is email, where a sender signs a communication digitally and its signature is verified by the recipient.
- Client certificates can also be used to help users access protected databases.



Certificates Lifecycle

There are several distinct stages to the certificate lifecycle, which are shown below:

- Discovery
- Creation/Purchasing
- Installation
- Storing
- Monitoring
- Renewal
- Revocation
- Replacement



Discovery

- Discovery is the first stage of the certificate lifecycle. In the discovery phase, the network is scanned for missing, expired, or unusable certificates.
- This phase also ensures any certificates already in place have been deployed properly.

- Certificates with vulnerabilities and other weaknesses can also be detected and fixed or replaced. The different certificates are commonly inventoried together in this phase to allow for tracking of certificate statuses, or grouping of related certificate types.

Creation/Purchasing

- In this stage the CA creates the certificate itself, or the user purchases a certificate from a trusted CA.
- The key pair for the certificate is created and the public key, CSR, and personally identifiable information are sent to the CA for certificate creation.
- If an organization or user does not have or does not wish to create a chain of trusted CAs, a certificate is purchased instead of being created.

Installation

- One of the most important stages of the certificate lifecycle is the storing phase. Certificates must be accessible, but not reusable by attackers, thus they must be kept in a secure and centralized location.
- The storing phase can also inventory the certificates into groups, if inventorying was not done in the discovery phase.

Storing

- This stage deals with the distribution and installation of the certificate in its proper place.
- All aspects of the certificate's configuration are checked in the installation phase, including the key pairs, the cipher suites, and the digital signature.
- The certificate is then installed onto the appropriate endpoint it was created for, and begins authentication of that endpoint.

Monitoring

- This is the longest phase, where the certificates are monitored throughout the duration of their expiration period.
- Once the expiration date is reached, or sometimes right before, certain certificate management systems will automatically renew certificates.
- If automatic certificate management systems are not being used, then a system administrator will need to monitor the network's certificates and renew, revoke, or replace any certificate that reaches its expiration date.

Renewal

- The renewal process of certificates begins once the validity of the certificate has run out.
- Once the user or automated systems decide to renew the certificate, a CSR is resent to the original issuing CA to get the certificate renewed.
- The process occurs as it did with originally creating the certificate, but much more quickly.

Revocation

- If the issuing CA has be decommissioned, a certificate is being misused, or for a host of other reasons, then a certificate can be revoked.
- Once revoked, the certificate is placed on a Certificate Revocation List, or CRL, if a CRL is in use.
- A CRL is a list of certificates revoked by the CA that should no longer be trusted.

Replacement

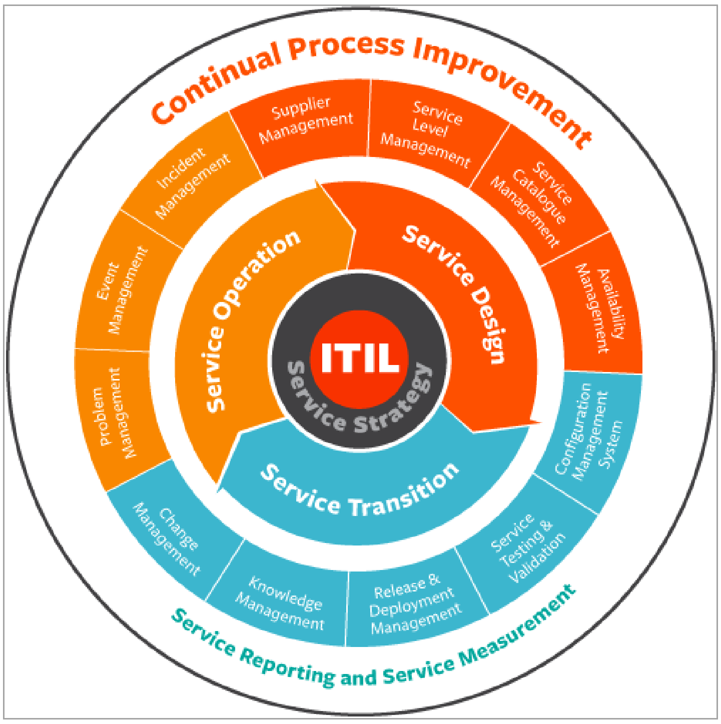
- If a CA's certificate is revoked or if the certificate owner wishes to move from paid certificates to their own Public Key Infrastructure, then the replacement phase occurs.
- This occurs less often, as it is easier to just renew a certificate with the original issuing CA.

6.4 ITSM Software

ITSM Software

- IT Service Management Tools help infrastructure and operations (I&O) organizations manage the consumption of IT services, the infrastructure that supports the IT services, and the IT organization's responsibility in delivering business value with these services.
- These are most heavily used by IT service desks and IT service delivery functions to support the tasks and workflows for processes including incident, request, problem, change, service level, knowledge, and configuration management.
- IT Service Management (ITSM) is the process of implementing, managing and providing IT services.
- It is used to improve customer service according to business goals.
- IT Services include services like the use of the printer by the entire team, installing apps on your laptop, changing passwords, etc.
- IT support team not only performs the task of solving day-to-day issues but is also accountable for performing the end-to-end management of these services.
- IT Services include services like the use of the printer by the entire team, installing apps on your laptop, changing passwords, etc.
- IT support team not only performs the task of solving day-to-day issues but is also accountable for performing the end-to-end management of these services.

ITIL Processes



- ITSM tools will benefit your business with improved efficiency, improved effectiveness, increased control, better service, and customer experience.

ITSM Tools

There are multiple ITSM tools available in the market. Enlisted below are the most popular ITSM ticketing tools:

- NinjaOne
- Salesforce
- Zendesk ITSM
- Wrike
- SuperOps.ai
- ManageEngine
- HaloITSM
- ServiceNow
- Freshservice
- HubSpot
- SolarWinds Service Desk
- SysAid
- SolarWinds MSP
- Cherwell
- InvGate Service Desk
- BMC Remedy
- Jira

Comparison of the Best IT Service Management Software Tools

ITSM	Best For	Features	Deployment
NinjaOne	Small to large businesses	RMM, IT asset management, end-point management, patch management, etc.	Cloud-based
Salesforce	Small to Large Businesses	Workflow automation, AI chatbots, self service center, appointment assistant.	Cloud-based
Zendesk ITSM	Small to Large Businesses	Ticketing System, Knowledgebase, Help Desk Software, Security.	Cloud & On-premises
Wrike	Small to large-sized businesses	IT service management templates, Interactive Gantt charts, Custom workflows, etc.	Cloud-Hosted and Open API.
SuperOps.ai	Small to medium-sized IT teams and consultants	Streamlined invoicing and billing, Service Catalog to inventory, Modern native app for iOS and Android devices.	Cloud-hosted
ManageEngine	Small to Large Businesses	Problem management, project management, Service catalog, visual workflows, Advanced Analytics.	Linux, Mac, Windows, Web-Based, Cloud-Based, SaaS.
Freshservice	Small to Large Businesses	Incident Management, SLA Management, Knowledge Management, Service Catalog, Self-service portal, Team Huddle, & Automation.	Cloud
SolarWinds Service Desk	Small to Large Businesses	Incident Management, Service Portal, Change Management, IT Asset Management, Problem Management, Knowledgebase.	Cloud & On-premises

- Once a business system has been set up, you need to monitor its performance to ensure that the resources that have been installed are sufficient to meet the needs of the business.
- Detected shortfalls may require resources to be adjusted or supplemented.
- You need to cover the performance of networks, the internet, servers, software, services, applications and network, and endpoint hardware. That monitoring also needs to be able to track the activities on any Cloud-based services that your company might use.
- In a modern business network, you will also need to control the activities on mobile devices and protect your network from intrusion and infection.
- Legal requirements demand that you protect the data held in your business, block access to it, and record every event that might compromise the integrity and security of that data.

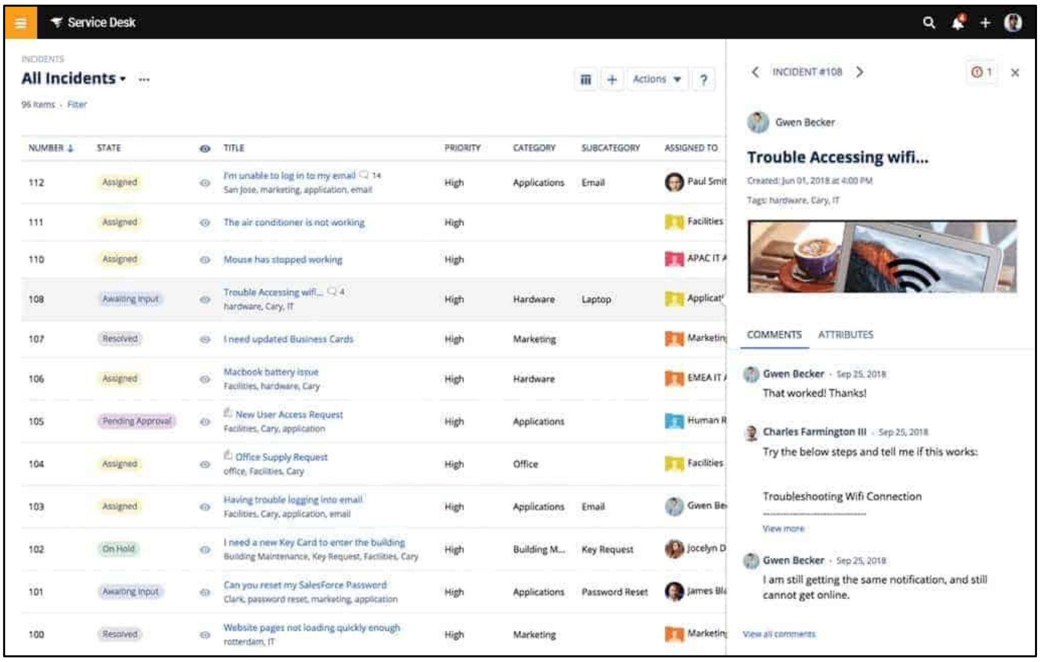
ITSM Tool Criteria

- As an IT Engineer, your search for ITSM tools should focus on software that supports ITIL Service Operation and ITIL Continual Service Improvement topics.
- Automated asset discovery processes that assemble a device inventory
- Scanning for the contents of all devices to establish a software inventory
- Software license management
- The ability to manage assets on multiple sites
- Routines to keep operating systems up to date
- A free trial or money-back guarantee for a no-cost assessment period
- A good price for the functions that are included

6.5 Solarwinds Service Desk Software

Solarwinds Service Desk

- SolarWinds Service Desk is a Cloud-based service desk solution that provides a central contact point for your Help Desk and includes asset management features.
- SolarWinds Service Desk is a powerful tool for consolidating, managing and prioritizing incoming tickets which is great for streamlining processes.



NUMBER	STATE	TITLE	PRIORITY	CATEGORY	SUBCATEGORY	ASSIGNED TO
112	Assigned	I'm unable to log in to my email 14 San Jose, marketing, application, email	High	Applications	Email	Paul Smit
111	Assigned	The air conditioner is not working	High			Facilities
110	Assigned	Mouse has stopped working	High			APAC IT A
108	Awaiting Input	Trouble Accessing wifi... 4 hardware, Cary, IT	High	Hardware	Laptop	Applicat'
107	Resolved	I need updated Business Cards	High	Marketing		Marketin
106	Assigned	Macbook battery issue Facilities, hardware, Cary	High	Hardware		EMEA IT A
105	Pending Approval	New User Access Request Facilities, Cary, application	High	Applications		Human R
104	Assigned	Office Supply Request office, Facilities, Cary	High	Office		Facilities
103	Assigned	Having trouble logging into email Facilities, Cary, application, email	High	Applications	Email	Gwen Be
102	On Hold	I need a new Key Card to enter the building Building Maintenance, Key Request, Facilities, Cary	High	Building M...	Key Request	Jocelyn D
101	Awaiting Input	Can you reset my SalesForce Password Clark, password reset, marketing, application	High	Applications	Password Reset	James Bl
100	Resolved	Website pages not loading quickly enough rotterdam, IT	High	Marketing		Marketin

Gwen Becker

Trouble Accessing wifi...

Created: Jun 01, 2018 at 4:00 PM

Tags: hardware, Cary, IT

Gwen Becker · Sep 25, 2018
That worked! Thanks!

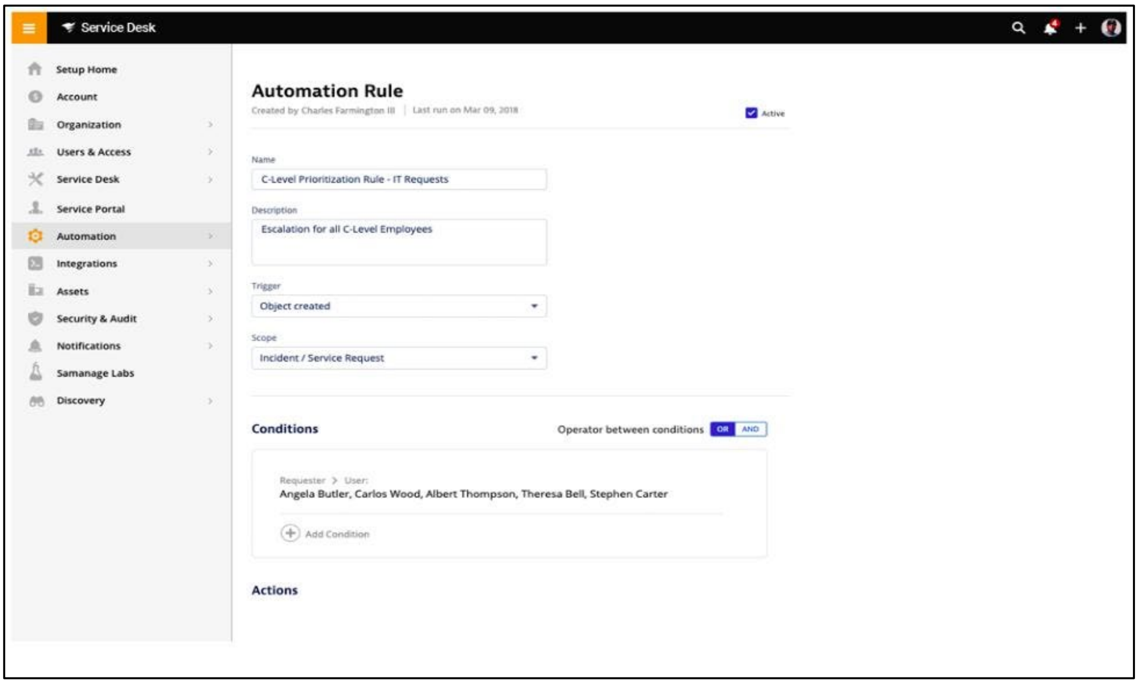
Charles Farmington III · Sep 25, 2018
Try the below steps and tell me if this works:

Troubleshooting Wifi Connection

Gwen Becker · Sep 25, 2018
I am still getting the same notification, and still cannot get online.

Key Features:

- Cloud-based
- Asset management
- Task automation
- Integrates with 200 apps
- Risk detection
- The help desk functions of the utility include a ticketing system with automation that allows you to input technician and operator availability to get an automated task allocation workflow distributing work for you.
- The system includes a task tracker to ensure that calls are responded to and solved promptly.
- Other technical support features include a self-service portal and a knowledge base utility to solve problems for users without the need for Help Desk resources.
- This Service Desk recently made it to the top spot in a recent industry comparison list.



Automation Rule

Created by Charles Farmington III | Last run on Mar 09, 2018

☑ Active

Name: C-Level Prioritization Rule - IT Requests

Description: Escalation for all C-Level Employees

Trigger: Object created

Scope: Incident / Service Request

Conditions

Operator between conditions: OR AND

Requester > User:
Angela Butler, Carlos Wood, Albert Thompson, Theresa Bell, Stephen Carter

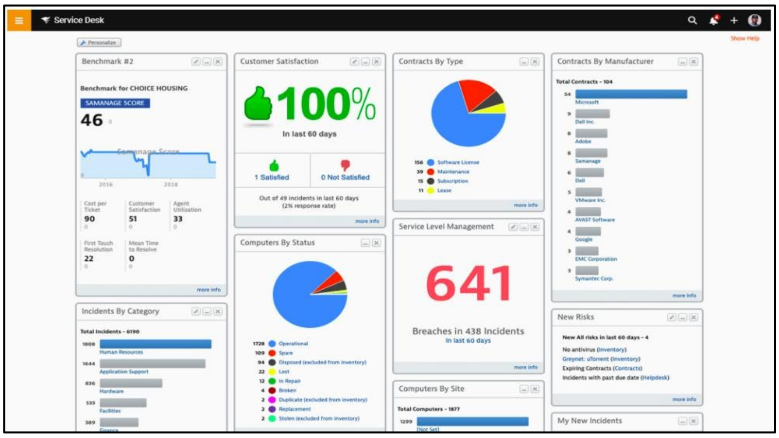
Add Condition

Actions

Package includes:

- ➢ Configuration management
- ➢ Change management
- ➢ Release management
- ➢ Service level management
- ➢ IT asset management

- A benchmarking tool helps you track performance and plan for expansion and a reporting module helps you track system utilization.
- A great feature of the tool is its Risk Detection module.
- This continuous assessment tracks the configurations and software installed on all of the devices in your system.
- It identifies illegal software and checks on the versions of all permitted software to ensure that all is up to date.
- The tool also monitors the versions of your AV software and threat databases to ensure that you have the very latest versions.



Pros:

- Designed for MSPs using ITIL standards
- Automated workflows help NOC teams prioritize tickets based on SLAs or custom rules
- Continuous scans of endpoints help reduce stress on the NOC
- Flexible pricing and cloud hosting make this one of the most flexible ITSM options
- Works well for both small and large networks

Cons:

- Search functionality

Subscription

- SolarWinds Service Desk is charged on a subscription basis and is available in three packages:
  - Team
  - Business
  - Professional
- The cheapest of these plans gives you a Help Desk and the SolarWinds Service Desk self-service portal and knowledgebase platform.
- To get the full ITSM package, you need to get the Professional plan.

Section 3: Exercises

Exercise 1: Draw digital certificate creation process.

Exercise 2: Draw diagram of secure communication with digital certificate.

Exercise 3: Draw certificate lifestyle.

Exercise 4: Participate in group discussion on following topics:

a) Enterprise Password Management
b) Various Password Managers for Business
c) Ports and Port Numbers
d) How do network ports affect cybersecurity?
e) Firewall Configuration
f) Certificate Management
g) Digital Certificate Creation Process
h) Benefits and Types of Digital Certificates

i) Certificates Lifecycle

j) Comparison of the Best IT Service Management Software Tools

Section 4: Assessment Questionnaire

1. What is Enterprise Password Management
2. To keep your corporate passwords safe, you just store them in a protected password vault and hide the key. (True / False)
3. With _________ you can rotate passwords without spending hundreds of hours manually changing them and simultaneously update credentials used for services and applications without downtime.
4. What are the two types of Password Management?
5. Storing payment and identity details in your company's vault is less secure than saving them to your browser. (True/False)
6. What is a port in networking?
7. A port in _________ is a jack or socket that peripheral hardware plugs into.
8. Between the protocols User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), there are _______ ports available for communication between devices.
9. A port number is ___ bit number.
10. What are Well-known, Registered and Dynamic Ports?
11. A _______ port is when the computer is actively waiting for inbound requests on that port number, allowing those connections.
12. Which port number is used for SMTP?
13. Port number _______, NTP allows computer clocks to sync with each other, a process that is essential for encryption.
14. A _______ is a security system that blocks or allows network traffic based on a set of security rules. It usually sits between a trusted network and an untrusted network; often the untrusted network is the Internet.
15. What is Digital Certificate?
16. The main job of a certificate is to ensure that data sent across a connection between a user and a server is kept ______. (Public / Private)
17. Use of digital certificates is to confirm the authenticity of a website to a web browser, which is also known as:
18. A digital certificate contains identifiable information, such as:
19. A public key certificate is issued by__________, which sign certificates to verify the identity of the requesting device or user.
20. Digital certificates cannot be requested by individuals. (True/False)
21. What is the main reason of using digital certificate?
22. What are the benefits of digital certificates?
23. Differentiate between Digital Certificate and Digital Signature.
24. What are three different types of public key certificates?
25. A _______ certificate sits on a server, such as an application, mail, or web server to ensure communication with its clients is private and encrypted.
26. What are three forms of TLS/SSL certificate validation?
27. A _________ certificate is used to confirm the authenticity of software or files downloaded through the internet.
28. A ______ certificate is a digital ID that identifies an individual user to another user or machine, or one machine to another.
29. In the _________phase, the network is scanned for missing, expired, or unusable certificates.
30. The _______ process of certificates begins once the validity of the certificate has run out.

----------End of the Module----------

NOTES

STL academy

Empowering Youth!

STL is one of the industry's leading integrators of digital networks providing All-in 5G solutions. Our capabilities across optical networking, services, software, and wireless connectivity place us amongst the top optical players in the world. These capabilities are built on converged architectures helping telcos, cloud companies, citizen networks, and large enterprises deliver next-gen experiences to their customers. STL collaborates with service providers globally in achieving a green and sustainable digital future in alignment with UN SDG goals. STL has a global presence in India, Italy, the UK, the US, China, and Brazil

ISO 21001 | GUINNESS WORLD RECORDS RECORD HOLDER | ASIA BOOK OF RECORDS | Skill & Assessment Partner NASSCOM®

stl.tech | stlacad.tech