Basics of Computer

System Software

Definition:
System software is a type of computer program designed to run hardware and application programs. It acts as an interface between hardware and user applications.

Examples:

- Operating Systems (Windows, Linux, macOS)
- Utility Programs (Antivirus, Disk Cleanup)
- Device Drivers
- Firmware

Functions:

- Manages hardware resources
- Provides essential services for applications
- Facilitates communication between software and hardware

BIOS (Basic Input/Output System)

Definition:
BIOS is firmware stored in a chip on the motherboard that initializes hardware components and loads the operating system.

Functions:

- Performs **Power-On Self-Test (POST)** to check hardware functionality
- Initializes system hardware (CPU, RAM, storage)
- Provides a user interface to configure hardware settings
- Loads the bootloader to start the operating system

Device Drivers

Definition:
A device driver is a special software program that allows the operating system to communicate with hardware devices.

Examples:

- Printer Drivers
- Graphics Card Drivers (NVIDIA, AMD)
- Audio Drivers
- Network Drivers

Functions:

- Acts as a bridge between hardware and software
- Converts OS commands into device-specific instructions
- Enables smooth functioning of peripherals

Features of System Software

- **Hardware Interaction:** Controls and manages computer hardware.
- **Platform for Applications:** Provides an environment for running application software.
- **Resource Management:** Manages CPU, memory, storage, and input/output devices.
- **Security & Protection:** Ensures system integrity by controlling access to resources.
- **Background Operation:** Runs continuously without direct user intervention.
- **Efficient Performance:** Optimizes system operations and improves speed.

Application Software

Definition:
Application software is a program designed to perform specific user tasks, such as word processing, web browsing, or gaming.

Examples:

- Microsoft Office (Word, Excel, PowerPoint)
- Web Browsers (Google Chrome, Firefox)
- Media Players (VLC, Windows Media Player)
- Games and Business Applications

Types:

- **General-Purpose Software** (MS Office, Photoshop)
- **Customized Software** (ERP for businesses)
- **Web-Based Applications** (Google Docs, Gmail)

Features of Application Software

- **User-Specific:** Designed for end-user tasks.
- **Easy to Use:** Provides an intuitive interface.
- **Interactivity:** Engages users through input and output operations.
- **Customization:** Some applications allow users to modify settings based on preferences.
- **Multitasking:** Supports running multiple applications simultaneously.

Operating System (OS)

Definition:
An operating system is system software that manages computer hardware and software resources while providing services for applications.

Examples:

- Windows, macOS, Linux (Desktop OS)
- Android, iOS (Mobile OS)
- UNIX, Ubuntu, Fedora (Server OS)

Functions:

- Manages memory, CPU, storage, and input/output devices.
- Provides a user interface (CLI or GUI).
- Handles file management.
- Ensures security through user authentication.
- Manages system errors and logs.

Objectives of Operating System

- **Resource Management:** Allocates CPU, memory, and devices efficiently.
- **User Convenience:** Provides an interface for easier interaction.
- **Multi-Tasking:** Runs multiple applications simultaneously.
- **Security & Protection:** Ensures data and user security.
- **Hardware Abstraction:** Hides complex hardware details from users.

Characteristics of Operating System

- **Multi-User:** Supports multiple users (e.g., UNIX, Windows Server).
- **Multi-Tasking:** Runs multiple processes at the same time.
- **Portability:** Can be installed on different hardware.
- **File System Management:** Organizes and controls file storage.
- **Process Scheduling:** Manages running processes efficiently.
- **Security Features:** Provides login authentication, firewalls, and encryption.

What Happens After You Push Power?

1. **Power Supply Activation:** Power button triggers the power supply unit (PSU) to send electricity to components.
2. **BIOS/UEFI Initialization:** BIOS/UEFI checks hardware status.
3. **POST (Power-On Self-Test):** Checks RAM, CPU, keyboard, and storage devices.
4. **Bootloader Execution:** BIOS locates and loads the bootloader from storage.
5. **Operating System Loading:** The OS is loaded into RAM.
6. **User Interface Activation:** The OS starts user services, drivers, and the GUI.

What is Bootstrapping?

Definition:
Bootstrapping is the process of starting a computer from the initial power-on state to a fully operational system.

Steps in Bootstrapping:

1. **BIOS/UEFI Loads:** Checks hardware and loads the bootloader.
2. **Bootloader Execution:** Finds and loads the operating system kernel.
3. **Kernel Initialization:** The OS starts background services.
4. **User Login Screen:** The OS is fully loaded and ready for user interaction.

Importance:

- Ensures proper system startup.
- Loads necessary system files.
- Provides access to user applications.

Basics of Computer Networking

What is a Computer Network?

A **computer network** is a collection of two or more computers and other devices connected to share resources, communicate, and transfer data.

Purpose of Networking:

- **Resource Sharing** (Printers, Files, Internet)
- **Communication** (Emails, Video Calls, Messaging)
- **Data Transfer** (Cloud Storage, File Sharing)
- **Security & Management** (Centralized Control in Organizations)

Types of Connections:

- **Wired Networks** (Ethernet, Fiber Optics)
- **Wireless Networks** (Wi-Fi, Bluetooth, Satellite)

The Network Diagram

A **network diagram** is a visual representation of how computers and devices are connected within a network.

Elements in a Network Diagram:

- **Nodes** (Computers, Servers, Printers, Mobile Devices)
- **Connections** (Cables, Wi-Fi signals)
- **Networking Devices** (Routers, Switches, Firewalls)
- **Cloud Services** (Internet, Data Centers)

A simple example:

📶 **Router** → 💻 **Computer** → 🖨️ **Printer**

The Three Types of Networks

A) Wide Area Network (WAN)

- Covers a **large geographic area** (cities, countries).
- Uses **public and private connections** (Internet, leased lines).
- Example: The **Internet**, corporate branch office connections.

B) Local Area Network (LAN)

- Covers a **small area** (home, office, school).
- Uses **Ethernet cables, Wi-Fi, or switches** for connectivity.
- Example: Office network, university campus Wi-Fi.

C) Peer-to-Peer (P2P) Network

- **No central server**, computers communicate **directly**.
- Suitable for **small networks** (home, small office).
- Example: File sharing over Bluetooth, torrents.

Fiber Optic Cable

A **fiber optic cable** is a high-speed data transmission cable made of glass or plastic fibers.

Advantages:

Faster than traditional copper cables.

Less interference, better signal quality.

Used for high-speed internet connections.

Types:

- **Single-mode fiber** (long-distance, high-speed communication).
- **Multi-mode fiber** (shorter distances, used in LANs).

Servers

A **server** is a computer or system that provides services or resources to other devices in a network.

Types of Servers:

- **Web Server** (Hosts websites – Apache, Nginx).
- **File Server** (Stores and shares files).
- **Database Server** (Manages databases – MySQL, SQL Server).
- **DNS Server** (Translates domain names to IP addresses).

Network Topologies

A **network topology** is the layout of how devices are connected in a network.

Common Topologies:

- **Bus Topology** – All devices share a single cable.
- **Star Topology** – Devices connect to a central hub/router.
- **Ring Topology** – Each device is connected in a circular fashion.
- **Mesh Topology** – Every device connects to every other device.

Firewalls

A **firewall** is a security device that monitors and controls network traffic.

Types of Firewalls:

- **Software Firewall** (Installed on computers – Windows Firewall).
- **Hardware Firewall** (Standalone devices – Cisco ASA, Fortinet).

Functions:

- Blocks unauthorized access.
- Filters malicious traffic.
- Prevents cyberattacks.

Routers

A **router** is a device that connects different networks and directs internet traffic.

Functions of a Router:

- **Connects devices to the Internet** (home/office networks).
- **Assigns IP addresses** (using DHCP).
- **Provides Wi-Fi connectivity** (Wireless Routers).

Popular Brands: Cisco, TP-Link, Netgear.

Wireless Networks

A **wireless network** allows devices to connect without physical cables.

Types:

📡 **Wi-Fi:** Used for home and office networks.

📶 **Cellular Networks (4G, 5G):** Used for mobile internet.

📍 **Bluetooth:** Used for short-range data transfer.

Advantages of Wireless Networks:

- No physical cables required.
- Easy to set up and expand.
- Supports mobile connectivity.

How Information Travels Through the Internet

When you send a request (e.g., opening a website), the process happens in multiple steps:

1. **Your Device:** Sends a request via a browser (e.g., typing google.com).
2. **Router:** Routes the request to your ISP (Internet Service Provider).
3. **ISP:** Connects to a **DNS Server**, which converts "google.com" into an IP address.
4. **Data Packets:** Travel through multiple routers and servers across the world.
5. **Destination Server:** Processes the request and sends back data.
6. **Your Browser:** Receives and displays the webpage.

Protocols Used:

🌐 **HTTP/HTTPS** – Web browsing.

📧 **SMTP/IMAP/POP3** – Email communication.

📡 **TCP/IP** – Ensures data reaches the correct device.

The Basics of Virtualization

Virtualization is a key technology in modern computing, allowing multiple virtual environments to run on a single physical system. This improves efficiency, flexibility, and resource utilization. Below is a detailed breakdown of virtualization concepts.

What is Virtualization?

Virtualization is the process of creating a **virtual version** of computer resources, such as **operating systems, storage, servers, or networks**, using software.

Key Concept: Instead of running directly on hardware, multiple virtual machines (VMs) can run on the same physical system, sharing its resources.

How Virtualization Works:

- A **Hypervisor** (virtualization software) creates and manages **virtual machines (VMs)**.
- Each VM runs its own **operating system and applications**, independent of others.
- Physical resources like **CPU, RAM, and storage** are allocated to VMs dynamically.

Example: Running **Windows and Linux on the same physical server** using virtualization software like VMware or VirtualBox.

Types of Virtualizations

1. Desktop Virtualization

Desktop virtualization separates the **desktop environment** from the physical computer.

- Users can access their **desktop OS remotely** from any device.
- Used in **corporate environments, call centers, and remote work setups**.

Examples:

- **Virtual Desktop Infrastructure (VDI)** – Employees use remote desktops on a central server.
- **Microsoft Remote Desktop, Citrix Virtual Desktops, VMware Horizon.**

2. Storage Virtualization

Storage virtualization pools multiple storage devices into a **single virtual storage system**.

- Makes storage easier to manage and scale.
- Enhances **performance, availability, and disaster recovery**.

Examples:

- **Software-defined storage (SDS)**
- **RAID (Redundant Array of Independent Disks)**
- **VMware vSAN, NetApp ONTAP, IBM Spectrum Virtualize.**

3. Data Virtualization

Data virtualization allows real-time access to data from **multiple sources without needing to move or copy it**.

- Used for **big data analytics, business intelligence, and cloud computing**.

Examples:

- **IBM Cloud Pak for Data, Denodo, TIBCO Data Virtualization.**

4. Application Virtualization

Application virtualization allows apps to run **without being installed on the local machine**.

- Users can access applications remotely, reducing compatibility issues.

Examples:

- **Microsoft App-V (Application Virtualization)**
- **VMware ThinApp**
- **Citrix XenApp**

Data Center Virtualization

Data center virtualization transforms **physical data centers into software-defined data centers (SDDC)**.

- **Virtual servers, storage, and networks** replace traditional hardware-based systems.

Examples:

- **VMware vSphere, Microsoft Hyper-V, Nutanix.**

Hypervisor

A **hypervisor** is software that enables virtualization by allowing multiple virtual machines (VMs) to share the same physical hardware.

Types of Hypervisors:

Type 1 (Bare-metal Hypervisor)

- Runs **directly on the hardware** (no operating system required).
- More **efficient, secure, and high-performing**.
- Used in **enterprise servers & data centers**.

Examples:

- **VMware ESXi**
- **Microsoft Hyper-V**
- **Xen**

Type 2 (Hosted Hypervisor)

- Runs **on top of an existing OS** (Windows/Linux).
- Easier to set up, but slightly slower than Type 1.
- Used for **testing, development, and personal use**.

Examples:

- **VMware Workstation**
- **Oracle VirtualBox**

VMware vMotion

VMware vMotion is a **live migration technology** that allows moving **running VMs from one server to another without downtime**.

- Used in **cloud computing, data centers, and enterprise IT environments**.
- Ensures **high availability** and **load balancing**.
- Reduces **hardware dependency and maintenance downtime**.

Example:

- If a server needs maintenance, **VMs can be moved to another server** without shutting down.

Benefits of VMware Virtualization

1. Better Resource Utilization

- Multiple VMs share **CPU, RAM, and storage**, reducing unused resources.

2. Cost Savings

- Reduces hardware costs since fewer physical servers are needed.
- Lowers electricity and cooling expenses in data centers.

3. Faster Deployment & Scalability

- New virtual machines **can be created instantly** without buying new hardware.
- Easily **scale resources** as needed.

4. Improved Disaster Recovery

- **Backup and restore VMs easily** in case of failures.
- Use **VM replication** for failover in case of disasters.

5. Increased Security

- VMs **are isolated** from each other, reducing security risks.
- **Snapshots and backups** help restore systems after an attack.

Conclusion

Virtualization is a game-changer in IT, enabling **efficient resource utilization, cost savings, and flexibility**. Technologies like **VMware, Hyper-V, and VirtualBox** help businesses run multiple virtual systems on the same hardware, making IT management more efficient.

Kaseya VSA (Virtual Systems Administrator)

What is Kaseya

Kaseya software enables a single framework for implementing IT policies, procedures and systems management across highly distributed collections of computers, servers, workstations, laptops or mobile devices. Kaseya was launched in 2000 in Silicon Valley, California by Mark Sutherland (Ex company President), Paul Wong (Ex-Chief Technical Officer), and Robert Davis (Ex-Chief Marketing Officer). Ex Kaseya CEO, Gerald Blackie, joined the company in 2003 by way of a 50/50 merger.

Working Port

Port 5721 is the default communication port used by the Kaseya VSA to facilitate communication between the Kaseya server and agents installed on target machines. It is an important part of the VSA's agent-server interaction and needs to be open for proper functioning.

Direct- KRC (Kaseya Remote Connect)

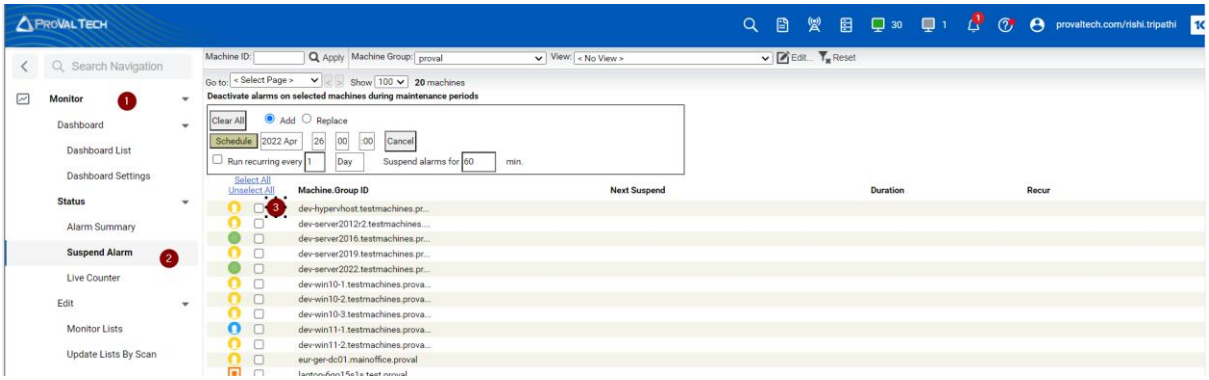
1. **KRC (Kaseya Remote Connect)** is a tool used to access remote systems securely. It provides remote desktop control and supports troubleshooting and support operations.
2. It's typically used for providing IT support to users without requiring them to be physically present at their machines.
3. KRC uses a secure connection and helps with tasks like resolving issues, performing system checks, or performing software installation remotely.

Live- KLC (Kaseya Live Connect)

- **KLC (Kaseya Live Connect)** is a tool that allows for live, real-time interactions with remote systems. It is a part of Kaseya VSA that provides the ability to view, control, and manage client machines remotely.
- Unlike KRC, KLC focuses on providing live, on-demand support, system monitoring, and control through a browser-based interface.

Suspend and Un-Suspend Alarm

- **Suspending an Alarm**: You can suspend an alarm in Kaseya VSA to temporarily stop the alarm from firing without completely disabling it. This is helpful for troubleshooting or when you don't want to receive notifications for a specific issue for a period of time.
- **Un-suspending an Alarm**: When an alarm needs to be re-enabled or resumed, it is unsuspended, and it will begin triggering again based on the configured conditions.
- To suspend for specific time and date
    1. Click on "monitor" tab
    2. Click on "Status" tab
    3. Click on "Suspend alarm" option
    4. Then check the check box of the machine and specify the "suspended alarm" time in minutes.
    5. Then click on schedule.



Windows Update

Windows Update is a **Microsoft service** that provides **security patches, bug fixes, driver updates, and feature enhancements** for Windows operating systems. Keeping your system updated ensures **better security, stability, and performance**.

- Installs **security patches** to protect against malware and hackers.
- Updates **device drivers** for better hardware compatibility.
- Delivers **feature updates** to improve Windows performance.
- Fixes **bugs and system issues** to ensure smooth operation.

Difference- Windows Update, Build Upgrade, Upgrade

- **Windows Update**: Refers to the process of applying security patches, bug fixes, and minor updates to a Windows operating system. This ensures the system remains protected and up-to-date.
- **Build Upgrade**: This refers to an upgrade to a new build of the same operating system. It could be an upgrade from Windows 10 version 20H2 to 21H1, for example. It includes significant updates or improvements to features.
- **Upgrade**: Refers to upgrading to a new version of the operating system entirely (e.g., upgrading from Windows 7 to Windows 10). It is a major change in the OS and might require more resources than a simple update or build upgrade.

Patch Management

- **Patch Management** in Kaseya VSA involves ensuring that operating systems and software installed on managed devices are up-to-date with the latest patches. It involves identifying missing patches, testing patches, deploying them, and ensuring they do not break any existing software.

Types of Approvals

- **Missing Approvals**: Refers to patches or updates that have not been approved yet for deployment.
- **Pending Approvals**: Refers to patches or updates that are waiting to be reviewed and approved for installation.
- **Denied**: Refers to patches that have been reviewed and explicitly denied for installation.
- **Manual (Machine Level)**: Refers to when patches are applied at the individual machine level rather than through automated processes. This is typically used for handling specific exceptions or configurations.

Classification of Windows Update

- **Classification** of Windows updates typically involves categorizing them into:
    - **Critical Updates**: Important for security and functionality.
    - **Security Updates**: Specific to vulnerabilities.
    - **Driver Updates**: Updates for device drivers.
    - **Feature Updates**: New features and enhancements.
    - **Quality Updates**: Bug fixes, improvements, and performance tweaks.

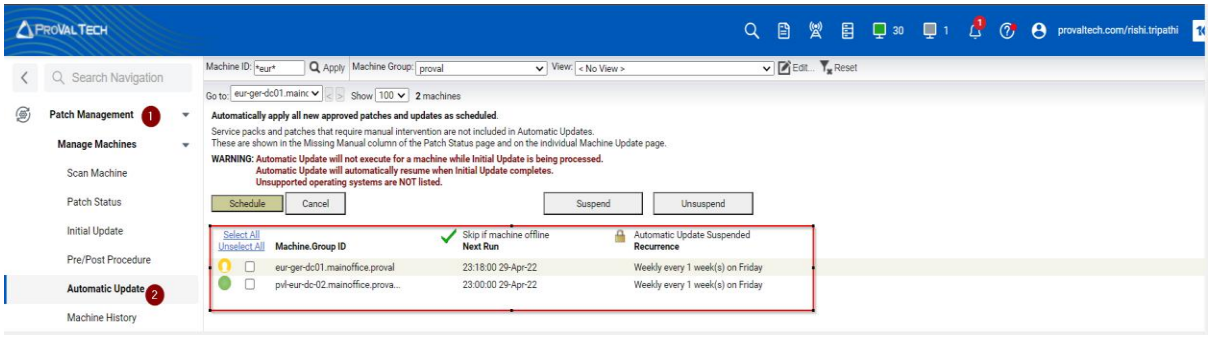
Online and Offline Patch Scan

- **Online Patch Scan**: The device is connected to the internet, allowing it to fetch the latest available patches and compare them to the current patch status.
- **Offline Patch Scan**: The device is not connected to the internet, and it relies on previously downloaded patches or a local repository to determine the missing updates.

Patch Installation Process

1. **Scan First**: The first step involves scanning the target systems to determine which patches are missing or need to be installed.
2. **Install**: After scanning, the approved patches are then deployed and installed on the systems.
3. **Patch Reboot**: Some patches require a system reboot to complete the installation process. This is common with updates that modify system files or settings.
4. **Patch Rescans**: After installation and reboot (if required), another scan is performed to ensure all patches have been correctly applied and there are no remaining issues.

- **How to check the patching schedule of the machine**



WUA (Windows Update Agent)

- The **Windows Update Agent (WUA)** is the system component responsible for detecting, downloading, and applying updates on Windows machines.
- It interacts with Windows Update servers, ensuring that the system receives the latest updates and patches.

Dependency of Windows Update Services

- **Dependency Services**: Windows Update depends on various system services to function correctly, including:
    - **Windows Update Service**: This service manages the download and installation of updates.
    - **Background Intelligent Transfer Service (BITS)**: Helps in downloading updates efficiently and reliably.
    - **Cryptographic Services**: Ensures the authenticity of updates.
    - **Windows Installer**: Handles the installation of software and patches.

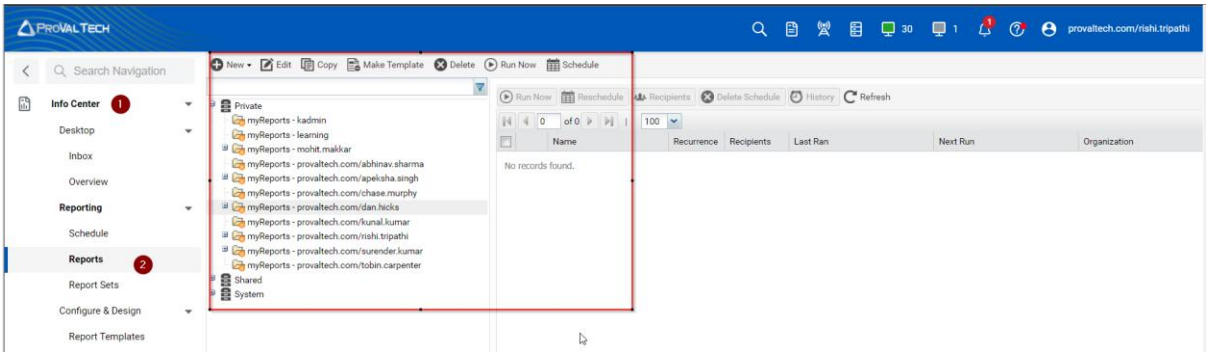
How to Perform Manual Patching

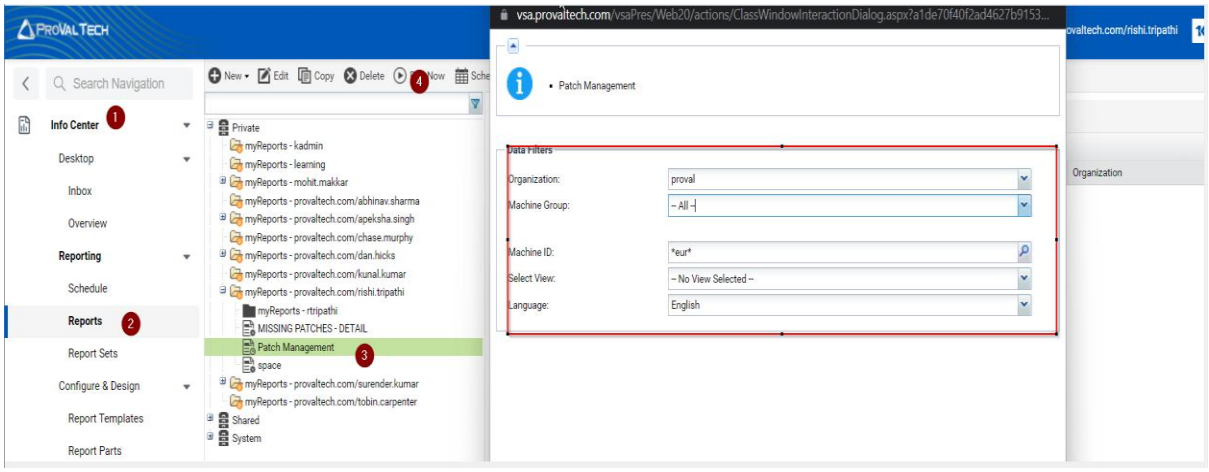
- **Manual Patching** involves applying patches to a system without relying on automated tools or processes:
    - Identify the missing patches using the Kaseya VSA or local scanning tool.
    - Download the necessary patches from the vendor's website or through a local repository.
    - Manually install each patch on the machine, ensuring that the system is rebooted if required.
    - Verify the installation by rescanning the system to ensure all patches have been applied.

How to export reports from Kaseya

1. Click on “Info Center” and then click on “Reporting” and then click on “Reports”.
2. Look for the desired report set and right click on the set and click on “Run Now”.
3. Then select the data filters and click on “submit”.

4. Report will start downloading





Server Backup

Server backup is critical to **data protection, disaster recovery, and business continuity**. It ensures that valuable data can be **recovered in case of system failure, cyberattacks, accidental deletion, or hardware damage**.

What is Backup?

A **backup** is a copy of important data stored in a **separate location** to prevent loss due to system failures, cyber threats, or accidental deletion.

Best Practices for Backup

- **Follow the 3-2-1 Backup Rule:**
  - **3 copies** of data (1 primary, 2 backups).
  - **2 different storage types** (HDD, SSD, cloud, tape, etc.).
  - **1 backup offsite** (for disaster recovery).
- **Automate Backups:** Use **backup scheduling** to ensure continuous data protection.
- **Use Encryption:** Protect backups from unauthorized access.
- **Test Backup & Recovery:** Regularly **test data restoration** to ensure reliability.
- **Store Backups Offsite:** Prevents loss due to disasters like fire, floods, or cyberattacks.

Benefits of Backup

- **Prevents Data Loss:** Protects against accidental deletion and hardware failure.
- **Business Continuity:** Ensures smooth operations after a disaster.
- **Ransomware Protection:** Allows **data restoration without paying ransom**.
- **Legal Compliance:** Meets regulatory requirements (GDPR, HIPAA, etc.).
- **Quick Recovery:** Reduces downtime and financial losses.

Causes of Data Loss

- **Hardware Failure:** Hard drive crashes, SSD corruption, and power failures.
- **Cyber Threats:** Ransomware, malware, and hacking.
- **Human Errors:** Accidental file deletion or overwriting.
- **Natural Disasters:** Floods, fires, and earthquakes.
- **Software Bugs:** Corruption due to faulty updates or application errors.

Types of Backups

1. **Full Backup**
    a. Creates a **complete copy of all data**.
    b. Requires **more storage and time**.
    c. Best for **initial backups or critical data**.
2. **Differential Backup**
    a. Backs up **only the data changed since the last full backup**.
    b. Faster than a full backup but **requires more space** over time.
3. **Incremental Backup**
    a. Backs up **only changes made since the last backup (full or incremental)**.
    b. **Fastest and most storage-efficient** backup type.
    c. Requires **multiple incremental backups for full recovery**.

Comparison:

Backup Type	**Storage Required**	**Speed**	**Recovery Time**
Full Backup	High	Slow	Fast
Differential Backup	Medium	Faster than Full	Moderate
Incremental Backup	Low	Fastest	Slowest

RAID (Redundant Array of Independent Disks)

RAID is a **data storage technology** that improves **redundancy, performance, and fault tolerance**.

RAID Level	**Description**	**Pros**	**Cons**
RAID 0	Data striping (no redundancy)	Fast read/write speed	No fault tolerance
RAID 1	Data mirroring (copies data to another drive)	High fault tolerance	50% storage efficiency
RAID 5	Data striping with parity	Balance of speed & redundancy	Needs 3+ drives
RAID 10	Combination of RAID 1 & 0	High performance & redundancy	Expensive (requires more drives)

- **RAID is NOT a Backup!** It provides redundancy, but **cannot replace a backup solution**.

Archive Bit

The **archive bit** is a file attribute that indicates whether a file has been modified since the last backup.

- **Full Backup** → Clears the archive bit (resets it).
- **Incremental & Differential Backup** → Checks archive bit to determine which files to back up.

Backup Repository

A **backup repository** is a dedicated storage location for backup data.

Types of Backup Repositories:

- **Local Storage:** External HDDs, NAS, RAID.
- **Cloud Backup:** Amazon S3, Google Drive, Microsoft Azure.
- **Hybrid Backup:** Combination of local & cloud storage.
- **Tape Backup:** Used for long-term archival storage.

Data Replication

Data replication creates **real-time copies of data** across multiple locations.

- **Synchronous Replication:** Data is copied instantly. Best for **critical systems**.
- **Asynchronous Replication:** Data is copied with a delay. Used for **disaster recovery**.

Difference Between Backup & Replication:

- **Backup** is used for **data recovery** (historical copies).
- **Replication** is used for **high availability** (real-time copies).

Backup Encryption

Backup encryption secures stored data against unauthorized access.

- **AES-256 Encryption:** Industry-standard encryption for backup files.\
- **End-to-End Encryption:** Encrypts data during **transmission & storage**.
- **Password Protection:** Ensures only authorized users can access backups.

Best Practice: Encrypt **both on-site and cloud backups**.

BDR (Backup and Disaster Recovery)

- **BDR is a complete backup solution that includes backup software and hardware**.
- It ensures **quick data restoration** after disasters like **cyberattacks or hardware failure**.

Where is Backup Software Installed?

- Installed on **physical servers, virtual machines (VMs), or cloud storage**.
- Can be managed through **dedicated backup appliances**.

Backup for Virtual Machines (VMs)

Type of Virtual Machines Used in Backup Jobs

- **VMware ESXi:** Most widely used enterprise-grade hypervisor.
- **Microsoft Hyper-V:** Windows-based virtualization platform.
- **KVM (Kernel-based Virtual Machine):** Open-source virtualization for Linux servers.

VM Backup Methods:

- **Snapshot-based Backup** – Captures the current state of a VM.
- **Agent-based Backup** – Uses software installed inside the VM.
- **Agentless Backup** – Backups entire VM without installing software inside it.

Backup Software

Backup software automates and manages data backups efficiently.

Veeam Backup & Replication

- Enterprise-grade backup solution for **VMware, Hyper-V, and cloud environments**.
- Features **Instant VM Recovery, Continuous Data Protection (CDP), and Ransomware Protection**.

Datto Backup

- Designed for **business continuity and disaster recovery (BCDR)**.
- Provides **cloud replication, ransomware detection, and automated backup testing**.

Data Retention

Data Retention Policy determines **how long backups are stored** before deletion.

- **Short-Term Retention:** Keeps recent backups for **days or weeks** (for quick recovery).
- **Long-Term Retention:** Stores backups for **months or years** (for compliance & auditing).
- **Regulatory Retention:** Some industries require **backup storage for years** (e.g., financial & healthcare sectors).

Example:

- Daily backups kept for **7 days**.
- Weekly backups stored for **3 months**.
- Monthly backups archived for **1-3 years**.

ConnectWise Automate (LabTech RMM)

ConnectWise Automate is a Remote Monitoring and Management (RMM) tool that helps IT administrators manage, monitor, and automate remote systems.

Supports Thin Client & Web Client for access and management.

Logging into the Control Center

- The **Control Center** is the main interface for managing LabTech agents and the server.
- Steps to log in:
  1. Open **LabTech Control Center** from the desktop.
  2. Enter **Username & Password** (default: 'Admin').
  3. Provide **Server FQDN or IP Address**.
  4. Click **Advanced** for extra options (e.g., **Slow Network Link** for low-bandwidth connections).
  5. Select **Database ('labtech')** and leave **Port as 3306**.
  6. Click **Login**.

LabTech Toolbar & Navigation

- The **toolbar** provides quick access to key areas like **Dashboard, Monitors, Tickets, Alerts, Search, and Patch Manager**.
- The **Navigation Tree** allows performing client-related tasks by expanding categories with the **[+] sign**.

Thin Client & Web Client

- **Thin Client**: A lightweight software interface used for remote access with minimal processing.
- **Web Client**: Browser-based interface that allows remote management from anywhere.
- **Workplace First Screen on Thin Client**: Displays an overview of the system's status and alerts.

Client Navigation Tree & Workplace (Two-Part Structure)

1. **Navigation Tree** (Left Panel) - Shows a list of **clients, locations, computers, and network devices**.
2. **Workplace** (Right Panel) - Displays **detailed information, monitoring tools, and control options**.

Client Screen Overview

- **Tracks client information**, including **general details, contacts, passwords, tickets, documents, and managed services**.
- Tabs include:
  - **General:** Contact & contract details.
  - **Passwords:** Securely stored, **AES encrypted**.
  - **Documents:** Store SLAs, network diagrams, etc.
  - **Tickets & Projects:** Track issues and projects.
  - **License Management:** Track software licenses & overuse alerts.
  - **Computers & Network Devices:** View and manage connected systems.

Onboarding Process

Manual Onboarding

1. Download the Agent
2. Install the Agent.
3. Register the Device
4. Configure Monitoring & Policies

Network Pro

1. Network Discovery
2. Install Network Probe
3. Enable SNMP & WMI Monitoring
4. Set Alerts & Reporting

Domain Controller

1. Install the Automate Agent on the Domain Controller
2. Enable Active Directory Monitoring
3. Set Up Group Policies (GPOs)
4. Monitor Event Logs & Security

CMS- Computer Manager Screen

- The **Computer Manager Screen (CMS)** displays **real-time system data** for each agent machine.
- Includes **CPU, RAM, disk usage, network activity, patch status, and backup details**.

SNMP (Simple Network Management Protocol)

- Used to **monitor and manage network devices (printers, routers, switches, etc.)**.
- Collects data on **device uptime, traffic, performance, and failures**.

Computer Management Screen

- Displays **real-time system data** (CPU, RAM, network activity, installed software, etc.).
- **Key tabs:**
    - **Hardware:** CPU, RAM, motherboard details.
    - **Drives:** Disk space, SSD/HDD status.'
    - **Network:** Network adapters, open ports.
    - **Printers:** List of installed printers & print jobs.'
    - **Processes & Services:** Manage running apps/services.
    - **Software & Patching:** Installed applications & Windows updates.

Monitoring & Alerts

- **Monitors tab:** Tracks system performance, failures, and alerts.
- **Alerts & Info tab:** Displays real-time alerts from **monitors & system logs**.
- **Patch Manager:** Manages system updates & missing patches.

Backup & Disaster Recovery (BDR)

- **LTBackup tab:** Manages backups using **ShadowProtect**.
- **Remote Backup:** Backs up important files like **My Documents** to a **local share or FTP server**.
- **Backup Logs:** Track backup history and failures.

Quick Access Toolbar Features

- **Refresh Button:** Updates system data.
- **FasTalk Mode:** Speeds up remote communication (5 seconds instead of 5 minutes).
- **LabVNC:** Connects remotely without additional software.
- **System & Event Logs:** View error logs, hardware/software changes.
- **Inventory:** Forces a system rescan for updates.

Command & Scripting Features

- **Command Prompt:** Execute system commands remotely.
- **Scripting Tab:** Run, schedule, and monitor scripts on client systems.
- **Process Control:** Start, stop, and monitor running processes.

Group Membership Control

Defines how a system manages power states and wake-on-LAN commands.

- **Master**: **Prevents wake-up packets**, ensuring the machine does not exit **sleep or hibernate mode**.
- **No Master**: Standard settings applied without wake-up controls.
- **Regular Master**: **Sends wake-up packets** to bring machines out of **sleep or hibernate mode**.

Patching Priority Settings

Controls how **Windows and third-party patches** are applied.

Code	Meaning
D	Deny (Block patch installation)
R	Remove (Uninstall existing patch)
A	Approve (Allow patch installation)
I	Ignore (No action taken)
N	Not Set (Default behavior)

- **Patching ensures security updates and fixes are applied correctly to prevent vulnerabilities.**

Monitors in ConnectWise Automate

Monitors help in **tracking system health, performance, and security**.

- **Remote Monitor** – Fetches data from a **live system using an agent**.
- **Internal Monitor** – Pulls data from **SQL database records** instead of live systems.

Reporting in ConnectWise Automate

Reports provide insights into **system performance, security, and IT asset management**.

- **Data View** – Allows filtering and analyzing data for insights.
- **Report Center** – Generates **customized reports** on **patching, system status, alerts, and performance metrics**.

Reporting & Audit Tools

- **License Tracking:** Alerts on software overuse.
- **History Logs:** Tracks **system changes, updates, and security logs**.
- **Network Tools:** Check network status and troubleshoot connectivity issues.

File Management & Transfers

- **Upload files by dragging & dropping** into LabTech Control Center.
- **Stored in LTShare directories** (for local or HTTP connections).

What is an operating system?

✅ It is a system software

What is a motherboard? (Select 2 options)

✅ It is an Integrated Circuit

✅ It is a Circuit board which is connecting all devices with each other.

SMPS stands for?

✅ Switched Mode Power Supply

NIC stands for?

✅ Network Interface Card

SSD stands for?

✅ Solid State Drive

What is CPU?

✅ It is a Central Processing Unit

What is the latest version of Microsoft Windows client OS?

✅ Windows 11

What is the latest version of Microsoft Windows server?

✅ Windows Server 2022

MCQ

RDC stands for?

✅ Remote Desktop Client

What is MMC?

✅ Microsoft Management Console

What is MCH?

✅ Memory Controller Hub

What is ICH?

✅ Input/output Controller Hub

BIOS stands for?

✅ Basic Input Output System

CMOS stands for?

✅ Complementary Metal Oxide Semiconductor

What is a file system?

✅ It creates an index of each file and provides information to the OS.

MBR stands for?

✅ Master Boot Record

UAC stands for?

✅ User Account Control

ASCII stands for?

✅ American Standard Code for Information Interchange

DDR stands for?

✅ Double Data Rate

SHA stands for?

✅ Secure Hash Algorithm