**Comprehensive IT Troubleshooting and Active Directory Guide**

**1. Hardware Troubleshooting**

**Windows:**

* Use **Device Manager** (devmgmt.msc) to check device status and update drivers.
* Run **Windows Memory Diagnostic** (mdsched.exe) for RAM issues.
* Check **Event Viewer** (eventvwr.msc) for hardware-related logs.
* Use chkdsk /f to scan and fix disk errors.
* Monitor **hardware performance** using **Task Manager** and **Resource Monitor**.

**Linux:**

* Use lshw or dmidecode to check hardware specifications.
* lsblk to list connected storage devices.
* dmesg for kernel hardware logs.
* memtest86+ to test RAM integrity.
* smartctl -a /dev/sdX to check hard disk health.

**2. Software Troubleshooting**

**Windows:**

* Run sfc /scannow (System File Checker) to fix corrupted system files.
* Use DISM /Online /Cleanup-Image /RestoreHealth for system component repair.
* Check **Event Viewer** (eventvwr.msc) for application errors.
* Boot into **Safe Mode** to isolate software conflicts.

**Linux:**

* Check logs in /var/log/syslog or /var/log/messages.
* Use strace to trace program execution.
* Run fsck /dev/sdX to repair file system errors.
* Use dpkg --configure -a or apt --fix-broken install to fix package issues.

**3. Networking**

**Windows:**

* ipconfig /all to check IP configuration.
* ping, tracert, and nslookup for network testing.
* Use netsh for advanced network configuration.

**Linux:**

* ifconfig or ip a to check IP details.
* ping, traceroute, and dig for network diagnostics.
* nmcli or nmtui for managing network connections.

**4. BSOD (Blue Screen of Death) / Kernel Panic**

**Windows:**

* Analyze crash dumps using **WinDbg** or **BlueScreenView**.
* Run sfc /scannow and chkdsk /f.
* Check system logs in **Event Viewer** (eventvwr.msc → Windows Logs → System).

**Linux:**

* View logs using journalctl -xe or dmesg | tail.
* Boot into **rescue mode** and check /var/log/syslog.
* Use fsck to fix file system corruption.

**5. DHCP (Dynamic Host Configuration Protocol)**

**Windows:**

* Use ipconfig /renew to request a new IP.
* Configure the **DHCP server** via **DHCP Manager** in Windows Server.

**Linux:**

* View DHCP leases using cat /var/lib/dhcp/dhclient.leases.
* Restart DHCP client: sudo systemctl restart networking.

**6. DNS (Domain Name System)**

**Windows:**

* nslookup domain.com to check DNS resolution.
* ipconfig /flushdns to clear DNS cache.

**Linux:**

* dig example.com or host example.com for DNS lookup.
* systemd-resolve --flush-caches to clear DNS cache.

**7. VPN (Virtual Private Network)**

**Windows:**

* Configure VPN in **Settings → Network & Internet → VPN**.
* Connect via command line using rasphone -d "VPN\_Name".

**Linux:**

* Use openvpn --config myvpn.ovpn for OpenVPN connections.
* Connect with **NetworkManager**: nmcli connection up myvpn.

**8. LAN (Local Area Network)**

* ping <IP> to test connectivity.
* **Windows**: netstat -an to check active connections.
* **Linux**: ss -tunlp to view network sockets.

**9. Active Directory (AD) Basics**

**What is Active Directory?**

Active Directory (AD) is a directory service by Microsoft for managing users, computers, and resources within a Windows domain.

**Core AD Features:**

* Centralized authentication and authorization.
* Group Policy for enforcing security.
* Organizational Units (OUs) for logical structuring.
* Replication across domain controllers.

**Common AD Commands:**

|  |  |
| --- | --- |
| **Task** | **Command** |
| List Domain Controllers | nltest /dclist:yourdomain.com |
| List Organizational Units | dsquery ou |
| Check Global Catalog Servers | nltest /dclist:yourdomain.com /GC |
| Check FSMO Role Holders | netdom query fsmo |

**10. Group Policies (GPO)**

**Windows:**

* Use gpedit.msc to configure local policies.
* Apply policy updates with gpupdate /force.

**Linux (Similar Policies with PAM & UFW):**

* visudo for managing sudo permissions.
* /etc/security/limits.conf for resource restrictions.

**11. NTFS vs FAT File Systems**

* **NTFS**: Supports permissions, encryption, and large files.
* **FAT32**: Universal compatibility but limited to **4GB file size**.

**12. Port Numbers**

|  |  |
| --- | --- |
| Service | Port Number |
| HTTP | 80 |
| HTTPS | 443 |
| SSH | 22 |
| RDP | 3389 |
| DNS | 53 |
| SMTP | 25 |

**13. Virtual Memory**

* **Windows**: Uses pagefile.sys.
* **Linux**: Uses **swap space** (swapon -s).

**14. Hosts File Location**

* **Windows**: C:\Windows\System32\drivers\etc\hosts
* **Linux**: /etc/hosts

**15. Active Directory Interview Questions**

**Basic Questions:**

1. What is Active Directory?
2. What are Organizational Units (OUs)?
3. What is a Domain Controller (DC)?
4. What is a Global Catalog (GC)?

**Intermediate Questions:**

1. What are FSMO roles?
2. What is Group Policy (GPO)?
3. Difference between Security Groups and Distribution Groups?

**Advanced Questions:**

1. How does AD replication work?
2. How do you restore deleted AD objects?
3. How do you back up and restore Active Directory?