CHEAT SHEETS HERO

System Administration Tools & Utilities Cheatsheet

A comprehensive cheat sheet covering essential system administration tools and utilities for managing and maintaining computer systems effectively, covering various operating systems and common tasks.

Process Management

Linux Process Commands

`ps`	Display a snapshot of the current processes.
`top`	Display dynamic real-time view of running processes.
`htop`	Interactive process viewer (needs installation).
`kill PID`	Terminate a process by its PID (Process ID).
`killall process_name`	Kill all processes by name.
`pkill pattern`	Kill processes matching a pattern.
`nice -n priority command`	Run a command with modified scheduling priority. (priority range: -20 to 19)
`renice priority PID`	Change the priority of an already running process.

Windows Task Manager

Access by pressing `Ctrl + Shift + Esc`.

Provides a GUI for viewing and managing processes, performance metrics, and startup applications.

Key features include:

- **Processes tab**: Shows running applications and background processes.
- **Performance tab**: Displays CPU, memory, disk, and network utilization.
- **Startup tab**: Manages applications that run at startup.

Command-line equivalent: `tasklist` (lists processes) and `taskkill` (terminates processes).

Process Monitoring

`vmstat`	Virtual memory statistics - reports memory, swap, IO, system, and CPU activity.
`iostat`	Input/output statistics for block devices.
`netstat` or `ss`	Network statistics.
`iotop`	Monitor disk I/O usage by process. (needs installation)
`iftop`	Display bandwidth usage by host. (needs installation)
`free -m`	Display the amount of free and used memory in the system (in MB).

Networking Tools

Basic Networking Commands

`ping hostname`	Test network connectivity.
`traceroute hostname`	Trace the route packets take to a host.
`netstat -tulnp`	Display listening ports and associated processes (Linux).
`ss -tulnp`	Another tool to display listening ports and associated processes (Linux).
`ip addr`	Show network interfaces and IP addresses (Linux).
`ifconfig`	Configure network interface parameters (deprecated, but still used).
`nslookup hostname`	Query DNS servers to find IP addresses or other DNS records.
`dig hostname`	More advanced DNS lookup utility.

Windows Networking Commands

`ipconfig`	Display network configuration information.
`ping hostname`	Test network connectivity.
`tracert hostname`	Trace the route packets take to a host.
`netstat -ano`	Display active network connections and listening ports.
`nslookup hostname`	Query DNS servers.
`pathping hostname`	Provides information about network latency and packet loss at intermediate hops.

Network Monitoring Tools

Wireshark: A powerful network protocol analyzer. Captures and analyzes network traffic in real-time.

tcpdump: A command-line packet analyzer. Captures network traffic and saves it to a file for later analysis.

Nmap: A network scanner. Discovers hosts and services on a computer network by sending packets and analyzing the responses.

Nagios/Zabbix: Comprehensive network monitoring solutions. Monitor network services, servers, and other network devices.

Disk and File System Management

Linux Disk Commands

`df -h`	Display disk space usage in a human-readable format.
`du -sh directory`	Display the disk usage of a directory in a human-readable format.
`lsblk`	List block devices.
`fdisk /dev/sda`	Partition table manipulator (replace /dev/sda with the appropriate device).
`mkfs.ext4 /dev/sda1`	Create an ext4 filesystem on a partition (replace /dev/sda1 with the appropriate partition).
`mount /dev/sda1 /mnt`	Mount a filesystem (replace /dev/sda1 and /mnt with appropriate values).
`umount /mnt`	Unmount a filesystem.
`fsck /dev/sda1`	Check and repair a filesystem.

Windows Disk Management

Access via `diskmgmt.msc` or through the Control Panel.

Provides a GUI for managing disks, partitions, and volumes.

Key features include:

- Creating and deleting partitions.
- Formatting volumes.
- Assigning drive letters.
- Converting disks between basic and dynamic.

Command-line equivalent: `diskpart` (powerful disk partitioning tool).

File System Utilities

`find /path -name filename`	Find files by name in a directory.
`grep pattern filename`	Search for a pattern in a file.
`tar -czvf archive.tar.gz directory`	Create a compressed tar archive.
`tar -xzvf archive.tar.gz`	Extract a compressed tar archive.
`rsync -av source destination`	Synchronize files and directories. Can be used for backups.
`chmod`	Change file permissions.
`chown`	Change file owner and group.

User and Group Management

Linux User Management

`useradd username`	Create a new user.
`passwd username`	Change a user's password.
`usermod -aG groupname username`	Add a user to a group.
`userdel username`	Delete a user.
`id username`	Show user's ID and group memberships.
`su username`	Switch to another user.
`sudo command`	Execute a command as the superuser.

Linux Group Management

`groupadd groupname`	Create a new group.
`groupmod -n new_groupname old_groupname`	Rename a group.
`groupdel groupname`	Delete a group.
`groups username`	Display the groups a user belongs to.
`getent group groupname`	Get group information.

Windows User Management

GUI: Use the 'Local Users and Groups' management console (`lusrmgr.msc`). Command line:

`net user username password /add` – Adds a new user.
`net localgroup groupname username /add` – Adds a user to a local group.
`net user username /delete` – Deletes a user.

PowerShell:

`New-LocalUser -Name "username" -Password "password"` – Creates a new local user.
`Add-LocalGroupMember -Group "groupname" -Member "username"` – Adds a user to a local group.
`Remove-LocalUser -Name "username"` – Removes a local user.