CompTIA Server+ (Plus) [SK0-005] Master Cheat Sheet

Domain1: Server hardware installation and management (18%)

This domain focuses on the physical and foundational aspects of server hardware. You must understand how to safely install equipment into a rack, manage power and cooling, configure storage for performance and redundancy, and perform routine maintenance without disrupting service. The exam tests scenario-based application, not just rote memorization.

1.1 Install Physical Hardware: Racking, Cabling, Power, and Cooling Management

Definition: Installing physical hardware involves safely mounting servers into equipment racks, ensuring proper cable management, and providing adequate power and thermal regulation to maintain operational stability.

Key Concepts

Rack Units (U) and Form Factors

- A **U** (Rack Unit) is the standard height measurement: **1U = 1.75 inches (44.45 mm)**.
- Common server form factors: **1U, 2U, 4U**, blade chassis, and tower.
- **Rack depth** and **rail kits** must match the server chassis. Always verify compatibility before mounting.

Cabling Management

- Use **structured cabling** practices: separate power and data cables to reduce electromagnetic interference (EMI).
- Label both ends of every cable.
- Use **cable management arms** for servers that slide in and out.
- Maintain **minimum bend radius** to prevent signal degradation (typically 4x the cable diameter for fiber).

Power Management

- **Redundant Power Supplies (PSUs):** Install servers with dual PSUs connected to **separate Power Distribution Units (PDUs)** on different circuits .
- **PDU Types:** Metered, monitored, and switched PDUs allow granular control and reporting.
- **UPS (Uninterruptible Power Supply):** Provides battery backup during outages. Size based on **VA rating** and runtime requirements.
- **Power load calculation:** Ensure circuit amperage is not exceeded. A server drawing 5A on a 20A circuit leaves little room for additional devices.

Cooling Management

- **Front-to-back airflow:** Cold air enters the front, hot air exhausts the rear. Never reverse airflow direction.
- **Hot aisle / cold aisle containment:** Physical separation improves cooling efficiency.
- **BTU calculation:** Server heat output in BTU/hr = Watts × 3.412. Match to HVAC capacity.
- **Blank panels:** Fill empty rack spaces to prevent hot air recirculation.

Practical Tips for the Exam

Notes

- **1U = 1.75 inches** is a memorization item.
- Redundant power means **separate circuits**, not just separate cables.
- **Airflow direction** is always front-to-back for rack servers.
- Fill empty rack spaces with **blank panels** to maintain thermal efficiency.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

1.2 Deploy and Manage Storage: RAID Levels, Shared Storage, and Capacity Planning

Definition: Storage deployment involves selecting appropriate RAID configurations for performance and redundancy, choosing between direct-attached and shared storage architectures, and planning capacity to meet current and future needs.

RAID Levels (Must Memorize)

RAID Level	Minimum Disks	Fault Tolerance	Read Performance	Write Performance	Usable Capacity	Key Notes
0	2	None	Excellent	Excellent	100%	Striping only; **no redundancy**

RAID Level	Minimum Disks	Fault Tolerance	Read Performance	Write Performance	Usable Capacity	Key Notes
1	2	1 disk	Good	Good	50%	Mirroring; simple and reliable
5	3	1 disk	Good	Moderate	(N-1)/N	Striping with **distributed parity**
6	4	2 disks	Good	Slower	(N-2)/N	**Dual parity**; higher write penalty
10	4	1 per mirror	Excellent	Good	50%	**Mirrored stripes**; best performance + redundancy

Exam Tip: RAID is **not a backup**. Always emphasize that redundancy ≠ data protection.

Shared Storage Types

Type	Definition	Protocol	Use Case
DAS	Direct Attached Storage	SAS, SATA, NVMe	Single server, low latency
NAS	Network Attached Storage	NFS, SMB/CIFS	File-level sharing across network
SAN	Storage Area Network	Fibre Channel, iSCSI, FCoE	Block-level storage; high performance

NAS vs. SAN Comparison:

- **NAS** presents **files**; **SAN** presents **blocks**.

- NAS is typically Ethernet-based; SAN historically uses Fibre Channel.
- iSCSI allows SAN over standard Ethernet.

Capacity Planning

Key Metrics:

- **Raw capacity:** Total physical disk space.
- **Usable capacity:** After RAID overhead and formatting.
- **IOPS (Input/Output Operations Per Second):** Critical for database and virtualization workloads.
- **Throughput:** MB/s; important for large file transfers.
- **Growth rate:** Monitor historical usage; plan for 20-30% headroom.

Thin vs. Thick Provisioning:

- **Thick:** Allocated space is reserved immediately.
- **Thin:** Space allocated on demand; risks over-subscription.

Practical Tips for the Exam

Scenario	Recommended RAID
Database requiring speed	RAID 10
File server needing balance	RAID 5
Critical data with no performance concern	RAID 6
Temporary scratch space	RAID 0

Notes:

- **RAID 5:** Minimum 3 disks, tolerates 1 failure.
- **RAID 6:** Minimum 4 disks, tolerates 2 failures.
- **RAID 10:** Minimum 4 disks, best performance + redundancy.
- **NAS = files; SAN = blocks.**
- **Capacity planning** requires monitoring growth and maintaining headroom.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

1.3 Perform Hardware Maintenance: Out-of-Band Management, Firmware Upgrades, and Hot-Swappable Components

Definition: Hardware maintenance involves using remote management tools for bare-metal access, applying firmware updates safely, and replacing components while the server remains operational.

Out-of-Band (OOB) Management

Definition: OOB management provides remote access to a server's console and hardware controls **independent of the operating system**.

Feature	Description
IP KVM	Keyboard, video, mouse over IP; full console redirection
Serial over LAN (SoL)	Console access via serial connection

Feature	Description
Virtual Media	Mount ISO images remotely for OS installation/recovery
Power Control	Remote power on/off/cycle/reset

Common Implementations:

- **IPMI:** Vendor-neutral interface; older standard.
- **iDRAC (Dell), iLO (HPE), XCC (Lenovo):** Vendor-specific OOB solutions.
- **Redfish:** Modern REST API-based OOB management.

Exam Scenario: A server administrator needs to perform bare-metal maintenance on a remote server. The answer is almost always **IP KVM** or the vendor OOB solution.

Firmware Upgrades

Definition: Firmware is low-level software embedded in hardware components (BIOS/UEFI, RAID controllers, NICs, PSUs).

Best Practices:

1. **Test in non-production first** whenever possible.
2. **Document current versions** before upgrading.
3. **Download from the vendor's official site**; verify checksums.
4. **Do not interrupt power** during firmware upgrade.
5. **Reboot after upgrade** and verify version.
6. **Have a rollback plan** (some components support firmware downgrade).

BIOS/UEFI Upgrade Methods:

- USB flash drive (bootable)
- Vendor OOB interface (virtual media)
- OS-based utility (vendor-specific)

Hot-Swappable Components

Definition: Components that can be removed and replaced **without powering down the server**.

Component	Hot-Swappable?	Notes
Power Supply	Yes (if redundant)	Remove one; system runs on remaining PSU
Hard Drive (SAS/SATA)	Yes (with RAID)	Rebuild occurs automatically
Fan	Yes (if redundant)	System monitors thermal thresholds
PCIe Card	No (usually)	Requires power-off
CPU/RAM	No	Requires power-off and often specialized handling

Exam Tip: Hot-swap capability requires **redundancy**. A single PSU is not hot-swappable in a meaningful sense.

Practical Tips for the Exam

Task	Tool/Method
Access console without OS	IP KVM / vendor OOB
Update RAID controller firmware	Vendor utility via OOB or OS
Replace failed drive	Hot-swap bay; RAID rebuilds
Replace failed PSU	Hot-swap if redundant

Notes

- **OOB management** is for OS-independent remote access.
- **Firmware upgrades** require careful planning and a rollback strategy.
- **Hot-swap** applies to redundant PSUs, fans, and drives.
- **IP KVM** is the standard answer for remote bare-metal access.

Exam Tip: For Domain 1, focus on **scenario recognition** rather than rote recall. The exam will present a situation and ask for the **best** or **most likely** action. Practice distinguishing between similar options (e.g., RAID 5 vs. RAID 6, IP KVM vs. RDP).

Domain2: Server administration (30%)

2.1 Install Server Operating Systems

Key Concepts

Partition Types:

- **MBR (Master Boot Record):** Legacy partition scheme. Supports up to 4 primary partitions, or 3 primary + 1 extended (with logical drives inside). Maximum 2 TB partition size. Requires Legacy BIOS boot mode.
- **GPT (GUID Partition Table):** Modern partition scheme. Supports up to 128 partitions. Maximum 9.4 ZB partition size. Requires UEFI boot mode.

File Systems:

File System	OS	Key Features
NTFS	Windows	Journaling, permissions, encryption (EFS), compression, quotas, large file support
ReFS	Windows Server	Resiliency, integrity streams, auto-repair; NOT bootable
ext4	Linux	Journaling, max 16 TB file, widely supported

File System	OS	Key Features
XFS	Linux	High-performance, large files, parallel I/O
ZFS	Linux/Unix	Pooled storage, checksumming, snapshots, RAID-Z

Installation Methods:

Method	Best For	Key Detail
Local Media (USB/DVD)	Single server deployments	Boot from physical media; simplest approach
PXE (Network Boot)	Large-scale deployments	Server boots from network; retrieves files from deployment server
Unattended Installation	Consistency across many servers	Uses answer files: `unattend.xml` (Windows), `kickstart` (Linux)
Image-Based Deployment	Fastest for identical servers	Pre-configured image captured and deployed (MDT/SCCM, Clonezilla)
Remote Installation	No physical access	Uses out-of-band management: iLO (HP), iDRAC (Dell), IMM (Lenovo)

Critical Pre-Installation Steps:

1. Verify hardware against vendor's **HCL (Hardware Compatibility List)**.
2. Check minimum and recommended OS requirements (CPU, RAM, disk).
3. Select correct OS edition (e.g., Windows Server Standard vs. Datacenter — Datacenter includes unlimited VM licensing rights).
4. Plan disk layout: separate OS, data, and log partitions.
5. Have license keys ready before installation.

Post-Installation Tasks (in order):

1. Apply all security updates and patches immediately.

2. Install latest drivers (storage controllers, NICs, management interfaces).
3. Configure static IP (servers should **not** rely on DHCP).
4. Configure NTP time synchronization (critical for Kerberos authentication).
5. Join domain/directory service as required.
6. OS hardening: disable unnecessary services, enable firewall, apply security baselines.

Exam Tips

- **GPT requires UEFI; MBR requires Legacy BIOS** — this is a frequently tested relationship.
- For production servers, always exceed minimum requirements.
- Use vendor-provided driver packages, not generic OS drivers.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

Notes

- Partition scheme and boot mode must match (MBR+Legacy, GPT+UEFI).
- Unattended installations use answer files; image-based is fastest for mass deployment.
- Servers need static IPs and accurate time sync before domain join.

2.2 Configure Network Services

Key Concepts

IP Addressing:

- **Private (RFC 1918) ranges:** `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`.
- **APIPA (169.254.x.x):** Assigned when DHCP fails; indicates network connectivity issue.
- **Static vs. Dynamic:** Servers should use static IPs for primary interfaces.

DNS (Domain Name System):

- Resolves hostnames to IP addresses.
- **Critical for Active Directory:** AD requires DNS SRV records to locate domain controllers. Pointing a domain member to a public DNS resolver instead of internal DNS causes domain join failures and intermittent logon issues.
- **A record:** Hostname → IPv4. **AAAA record:** Hostname → IPv6. **CNAME:** Alias. **MX:** Mail. **SRV:** Service location.

DHCP (Dynamic Host Configuration Protocol):

- Automatically assigns IP, subnet mask, gateway, DNS to clients.
- **DORA process:** Discover → Offer → Request → Acknowledge.
- DHCP **relay agents** forward DHCP broadcasts across VLANs.

VLANs (Virtual Local Area Networks):

- Logical segmentation of a physical network.
- **Trunk ports:** Carry traffic for multiple VLANs (802.1Q tagging).
- **Access ports:** Carry traffic for a single VLAN.
- Misconfigured VLAN assignment prevents DHCP traffic from reaching a server, causing APIPA fallback.

Practical Commands

```
# Linux — View IP configuration
```

```
ip addr show
ip route show

# Linux — DNS resolution test
nslookup servername
dig servername

# Windows — View IP configuration
ipconfig /all

# Windows — DNS cache operations
ipconfig /flushdns
ipconfig /displaydns
```

Exam Tips

- **APIPA address (169.254.x.x)** = DHCP failure → check VLAN assignment, DHCP server reachability, or relay configuration.
- A server that can resolve external names but fails to join domain → DNS is pointing to external resolver instead of AD-integrated DNS.
- **Amber link light** on switch port often indicates speed/duplex mismatch (NIC misconfiguration).

Notes

- Servers use static IPs; DNS must resolve AD SRV records for domain functionality.
- VLAN misconfiguration is a common cause of DHCP failure.
- APIPA = no DHCP = investigate Layer 2 connectivity first.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

2.3 Manage Server Functions

Key Concepts

Server Roles:

- **File/Print Server:** Shares files and printers via SMB/CIFS.
- **Web Server:** Hosts HTTP/HTTPS (IIS, Apache, Nginx).
- **Database Server:** Hosts DBMS (SQL Server, MySQL, PostgreSQL).
- **Directory Services:** Active Directory (Windows), LDAP (cross-platform).
- **DNS/DHCP Server:** Core network infrastructure roles.
- **Application Server:** Hosts line-of-business applications.

Monitoring — Key Performance Metrics:

Domain	Key Counters	Warning Signs
CPU	% Processor Time, Processor Queue Length	Sustained saturation, growing queue
Memory	Available MB, Pages/sec	Hard paging, low available memory
Disk	IOPS, latency (s/read, s/write), queue length	Rising latency is the leading indicator
Network	Bandwidth utilization, errors, discards	Errors/discards = physical or duplex fault

Baselining: A recorded set of performance counters under representative production load. Without a baseline, a metric like "CPU at 70%" is meaningless. With a baseline showing "25% for this hour on this weekday," 70% is a finding.

Data Migration:

- **Storage migration:** Moving data between storage tiers, arrays, or platforms.
- **Thin provisioning:** Allocates on write; improves utilization but creates over-subscription risk. If the pool fills, **all workloads stall**.

- **Thick provisioning:** Allocates full capacity up front; deterministic performance, no over-subscription.
- **Allocation unit size:** 4 KB default for general file service; 64 KB for large sequential workloads (backup targets, video). Cannot be changed without reformatting.

Exam Tips

- **Thin provisioning** saves space but risks catastrophic pool exhaustion.
- **Partitioning strategy:** OS on its own volume, application data on a second, logs on a third — transaction logs on their own volume so runaway log growth cannot halt the system.
- **Disk quotas** are best for user home directories, NOT database volumes (quota hit halts the service).

Notes

- Always baseline before troubleshooting performance.
- Disk latency is more meaningful than IOPS alone.
- Separate OS, data, and log volumes for availability and manageability.

2.4 High Availability

Key Concepts

Clustering:

- **Active-Active:** All nodes actively serve workloads simultaneously. Higher resource utilization.
- **Active-Passive:** One node serves; standby node takes over on failure. Simpler but wastes standby resources.

- **Heartbeat:** Private network connection between cluster nodes for health monitoring.

Failover vs. Failback:

- **Failover:** Automatic transfer of workload from failed node to healthy node.
- **Failback:** Return of workload to the original (repaired) node.

Load Balancing:

- Distributes incoming requests across multiple servers.
- **Algorithms:** Round Robin, Least Connections, Most Recently Used (MRU).
- **Software vs. Hardware:** Software load balancers (Nginx, HAProxy) vs. dedicated appliances (F5, Citrix NetScaler).

NIC Teaming / Link Aggregation:

- Combines multiple NICs into one logical interface.
- **Benefits:** Redundancy (if one NIC fails) and increased throughput.
- **Switch-dependent** (LACP/802.3ad) vs. **switch-independent**.

Fault Tolerance:

- **Server-level redundancy:** Multiple servers in a cluster.
- **Component redundancy:** Redundant PSUs, NICs, disks (RAID), paths.

Critical Latency Rule:

- Cluster heartbeats require **< 5 ms latency**. Latencies exceeding 5 ms cause heartbeat packet drops and cluster instability. Beyond 50–100 km, switch to **asynchronous replication** (which introduces non-zero RPO and eliminates automatic failover).

Key Availability Metrics:

Metric	Meaning
MTBF	Mean Time Between Failures — reliability measure
MTTR	Mean Time To Recover — how fast you restore service
RPO	Recovery Point Objective — max acceptable **data loss**
RTO	Recovery Time Objective — max acceptable **downtime**
SLA	Service Level Agreement — contractual uptime %
Five Nines	99.999% = ~5.26 min downtime/year

Exam Tips

- **Proper patching procedures** in clusters: patch passive node first, fail over, then patch the other node. Never patch both simultaneously.
- **RPO vs. RTO:** RPO = data loss tolerance (backup frequency). RTO = downtime tolerance (recovery speed). Do not confuse them.
- **Heartbeat network** should be a separate, dedicated connection.

Notes

- Active-Active maximizes resources; Active-Passive is simpler.
- Failover is automatic; failback is the return to normal.
- Cluster heartbeat latency must stay under 5 ms.
- RPO = data loss; RTO = downtime. Know the difference cold.

2.5 Virtualization

Key Concepts

Host vs. Guest:

- **Host:** The physical server (and its hypervisor) that provides compute, memory, storage, and network resources to virtual machines.
- **Guest:** The virtual machine (VM) running its own operating system, isolated from other guests.
- **Hypervisor:** Software layer that creates and runs VMs.
    - **Type 1 (Bare-Metal):** Runs directly on hardware. Best performance and security. Examples: VMware ESXi, Microsoft Hyper-V, Citrix XenServer, KVM.
    - **Type 2 (Hosted):** Runs on top of a host OS. Easier for labs/desktops. Examples: VMware Workstation, Oracle VirtualBox, Parallels.

Resource Allocation:

Resource	Key Considerations
vCPU	Over-subscription possible but monitor CPU Ready time; too many vCPUs per VM causes scheduling delays
Memory	Over-commit risky; use reservations, limits, and shares. Ballooning/swap degrades performance
Storage	Thin vs. thick provisioning; IOPS must be planned per workload (databases need high IOPS)
Network	Virtual switches, VLAN tagging, NIC teaming, SR-IOV for performance

Key Virtualization Concepts:

- **VM sprawl:** Uncontrolled growth of VMs → resource exhaustion and licensing issues. Control via approval workflows and lifecycle management.

- **Snapshot:** Point-in-time copy of a VM. **Not a backup** — snapshots degrade performance and grow over time. Delete promptly.
- **Live Migration / vMotion:** Move a running VM between hosts with no downtime.
- **Cloning / Templates:** Deploy identical VMs quickly; templates ensure consistency.
- **Resource Pools:** Group hosts for aggregated resource management.

Cloud Models:

Model	Description	Example
IaaS	Infrastructure as a Service — VMs, storage, network	AWS EC2, Azure VMs
PaaS	Platform as a Service — managed runtime/database	Azure App Service, Heroku
SaaS	Software as a Service — fully managed application	Microsoft 365, Salesforce

Cloud Deployment Models:

- **Public:** Shared provider infrastructure.
- **Private:** Dedicated to one organization.
- **Hybrid:** Mix of public and private with orchestration.
- **Community:** Shared by organizations with common requirements.

Exam Tips

- **Snapshots are NOT backups** — this is a frequently tested distinction.
- **Type 1 hypervisors** are for production; **Type 2** for testing/desktops.
- Over-committing memory is more dangerous than over-committing CPU.
- Know the difference between **live migration** (running VM) and **cold migration** (powered-off VM).

Notes

- Type 1 = bare-metal (production); Type 2 = hosted (lab).
- Over-subscription needs monitoring — CPU Ready and memory ballooning are warning signs.
- IaaS/PaaS/SaaS differ by how much the provider manages.
- Snapshots are temporary; use proper backups for recovery.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

2.6 Scripting Basics

Key Concepts

Why Scripting Matters for Server Admins:

- Automate repetitive tasks (user creation, log rotation, backups).
- Ensure consistency across many servers.
- Reduce human error.

Common Scripting Languages:

Language	Platform	Use Case
PowerShell	Windows	Server administration, AD, Exchange, Azure
Bash	Linux/Unix	System administration, automation
Python	Cross-platform	Automation, APIs, cloud

Language	Platform	Use Case
Perl	Cross-platform	Text processing, legacy scripts

Variables:

- Containers for storing data. Types include string, integer, boolean, array.
- **PowerShell:** `$name = "Server01"`
- **Bash:** `name="Server01"` (no spaces around `=`)
- **Scope:** Local vs. global vs. environment variables.

Loops:

Loop Type	Purpose
For	Iterate a fixed number of times
While	Repeat while condition is true
Do-While	Execute at least once, then check condition
ForEach	Iterate over items in a collection

Conditionals:

- **If/Else:** Execute code based on a condition.
- **Switch/Case:** Multiple condition branches.

Common Server Tasks to Automate:

1. **User account creation** — bulk import from CSV.
2. **Log rotation/cleanup** — delete logs older than N days.
3. **Backup scripts** — run backups, verify, notify.
4. **Service monitoring** — restart failed services.

5. **Patch management** — schedule and report updates.
6. **Disk space alerts** — notify when threshold exceeded.

Practical Examples

PowerShell — Restart a service if stopped:

```
powershell
$svc = Get-Service -Name "Spooler"
if ($svc.Status -ne "Running") {
    Start-Service -Name "Spooler"
}
```

PowerShell — Loop through servers:

```
powershell
$servers = @("SRV01","SRV02","SRV03")
foreach ($s in $servers) {
    Get-Service -ComputerName $s -Name "W3SVC"
}
```

Bash — Delete logs older than 30 days:

```
bash
find /var/log -name "*.log" -mtime +30 -delete
```

Bash — For loop:

```
bash
for server in srv01 srv02 srv03; do
    ping -c 1 $server
done
```

Exam Tips

- Know the **purpose** of each loop type, not just syntax.
- **Variables in Bash** cannot have spaces around `=` (`name="x"` not `name = "x"`).
- **PowerShell cmdlet naming:** Verb-Noun (e.g., `Get-Service`, `Start-Service`).
- Scripts should include **error handling** and **logging**.

Notes

- PowerShell for Windows, Bash for Linux, Python for cross-platform.
- Variables store data; loops repeat actions; conditionals make decisions.
- Automate repetitive tasks to reduce errors and save time.
- Always test scripts in a non-production environment first.

2.7 Asset Management

Key Concepts

Asset Management Defined:

The process of tracking, managing, and maintaining an organization's IT assets (hardware, software, licenses) throughout their lifecycle.

Documentation:

- **Asset inventory:** Record of all hardware/software (make, model, serial, location, owner).
- **Network diagrams:** Physical and logical topology.
- **Configuration documentation:** Server roles, IPs, dependencies.
- **Change logs:** Record of all modifications.
- **Runbooks:** Step-by-step procedures for common tasks.
- **SOPs (Standard Operating Procedures):** Documented repeatable processes.

Lifecycle Management:

Phase	Activities
Procurement	Purchase, receive, tag, record
Deployment	Configure, install, baseline

Phase	Activities
Maintenance	Patch, monitor, repair, upgrade
Retirement	Decommission, data wipe, dispose/recycle

Secure Storage of Documentation:

- Store in a **secure, access-controlled** location (password manager, encrypted repository).
- **Do not** store credentials in plain text.
- **Version control** for configuration files and scripts.
- **Backup** documentation separately from production systems.
- **RBAC (Role-Based Access Control)** — limit who can view/edit.

Key Asset Management Practices:

1. **Tag every asset** with a unique identifier (asset tag, barcode, RFID).
2. **Track warranty and support contracts** — know expiry dates.
3. **Software license tracking** — avoid compliance issues and audits.
4. **Depreciation tracking** — for budgeting and replacement planning.
5. **Disposal procedures** — secure data wiping (DoD 5220.22-M, degaussing, physical destruction).

CMDB (Configuration Management Database):

- Central repository of configuration items (CIs) and their relationships.
- Used in ITIL frameworks.
- Helps with impact analysis and change management.

Exam Tips

- **Asset tags** are the foundation of inventory tracking.

- **Data wiping** must be verified before disposal — deleting files is NOT sufficient.
- **Documentation must be backed up** — losing it can cripple recovery efforts.
- **CMDB** tracks relationships between assets, not just a list.

Notes

- Asset management covers the full lifecycle: procure → deploy → maintain → retire.
- Documentation must be secure, version-controlled, and backed up.
- Secure disposal requires verified data wiping or physical destruction.
- CMDB maps relationships, not just inventory.

Exam Strategy for Domain 2 (30%):

- Expect scenario-based questions on HA, virtualization, and network services.
- Memorize the RPO/RTO distinction and cluster latency threshold.
- Know your commands: `ipconfig`, `ip addr`, `nslookup`, `Get-Service`.
- Understand *why* each best practice exists — the exam tests reasoning, not just recall.

Domain3: Security and disaster recovery (24%)

Exam Context: Security and Disaster Recovery covers physical and data security, identity management, mitigation strategies, server hardening, and decommissioning. Expect scenario-based questions requiring you to apply concepts, not just recall definitions.

3.1 Data Security

Key Concepts

Encryption Paradigms:

Encryption protects data by scrambling it so only authorized parties can read it. The exam tests three core goals:

Goal	Definition	Practical Use
Confidentiality	Only authorized users can access/read data	Encrypting sensitive files, full-disk encryption
Integrity	Data has not been altered unexpectedly	Hashing (MD5, SHA) to verify file integrity
Non-repudiation	A user cannot deny performing an action	Digital signatures, audit logs

Data States — Two Critical Distinctions:

State	Definition	Encryption Tools
Data at Rest	Stored on physical media (drives, tapes, backups)	BitLocker (Windows), LUKS (Linux), EFS (file-level)
Data in Transit	Moving across networks	SSH, HTTPS/TLS, RDP (encrypted)

Drive Encryption vs. File Encryption:

- **Drive encryption** (BitLocker, LUKS): Protects entire volume when system is powered off. Decrypted at boot.
- **File encryption** (EFS, 7-Zip, GnuPG): Protects individual files even when system is running.

Retention Policies:

A data retention policy defines **how long data must be kept and when it must be deleted** . Key drivers:

- **Legal/regulatory compliance** (industry regulations, government mandates)
- **Business operational needs** (active projects, historical reference)

- **Disaster recovery planning** (backup retention windows)

Storage Location Trade-offs :

Location	Advantages	Disadvantages
On-Site	Immediate access, direct control	Vulnerable to site-wide disasters (fire, flood)
Off-Site	Survives local disasters, specialized security	Increased retrieval time, less direct control

Data Lifecycle Management:

Data passes through phases: **Creation** → **Storage** → **Usage** → **Sharing** → **Archiving** → **Destruction**. Policies govern each phase (who can access, how it's encrypted, when it's deleted).

Exam Tips

- **Know the three goals of encryption** — confidentiality, integrity, non-repudiation. A question may ask which goal hashing addresses (integrity).
- **Data at rest vs. in transit** — if a question mentions "backup tapes" or "hard drives," it's at rest. If it mentions "network" or "remote access," it's in transit.
- **Retention: "as long as required and no longer"** — retaining data longer than necessary incurs cost and legal risk.

Notes

- Encryption serves confidentiality, integrity, and non-repudiation.
- Data at rest needs drive/file encryption; data in transit needs network protocols.
- Retention policies balance legal requirements against storage cost and risk.
- On-site storage is fast but disaster-vulnerable; off-site is safer but slower to access.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

3.2 Physical Security

Key Concepts

Physical Access Control Layers (Defense in Depth):

A real data center stacks controls from outside in:

Layer (Outside → In)	Control	Purpose
Property Perimeter	Fencing, bollards	Stop vehicles, channel pedestrians
Building	Datacenter camouflage, reflective glass, signal blocking	Avoid attention, prevent electronic eavesdropping
Lobby	Security guards, cameras	Detect + deter
Inner Doors	Card reader + biometric (2-factor)	Authentication + audit
Trap Between Zones	Mantrap / airlock	Prevent tailgating
Server Hall	Locked cabinets, safes for KMS/HSM	Last line of defense

Key Physical Controls:

- **Bollards:** Anti-ram posts preventing vehicle attacks

- **Mantrap:** Admits one person at a time; inner door won't open until outer closes and person passes second factor. **Defeats tailgating** .
- **Cameras (CCTV):** Detective control (and deterrent if visible). Footage typically retained 30–90 days.

Lock Types Compared:

Lock Type	Authenticator	Replay-Resistant?	Notes
Mechanical Key	Physical key	No	Easy to duplicate
Card Reader	Magstripe/proximity card	No	Cards clonable
RFID	RFID badge (+ PIN)	Partly	Challenge protocols improve security
Biometric	Fingerprint, iris, face	Yes	Template database must be encrypted

Best Practice: Two-factor — card + biometric, or card + PIN.

Environmental Controls:

Control	Target / Specification
Fire Suppression	Inert gas (FM-200, Novec 1230) — **no water on electronics**
HVAC	18–27 °C, 40–60% relative humidity (ASHRAE TC 9.9)
Sensors	Temperature, humidity, smoke, water-leak, door-open

Control Categories:

- **Detective:** CCTV, motion sensors, door alarms, visitor logs
- **Deterrent:** Visible cameras, guards, fencing, signage

- **Preventive:** Locks, mantraps, bollards, biometrics

Exam Tips

- **Mantrap = anti-tailgating.** If a question describes someone following an authorized person through a door, the answer involves a mantrap.
- **Fire suppression for server rooms = gas-based, never water.** Water destroys electronics.
- **Biometrics are the most secure lock type** because they're replay-resistant, but the template database must be protected.
- **HVAC range: 18–27°C, 40–60% RH.** Know these numbers.

Notes

- Physical security uses layered defense: perimeter → building → lobby → doors → server hall.
- Mantraps prevent tailgating; two-factor access (card + biometric) is best practice.
- Environmental controls: gas fire suppression, precise HVAC, multiple sensor types.
- Detective controls (cameras, logs) detect breaches; preventive controls (locks, mantraps) stop them.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

3.3 Identity and Access Management (IAM)

Key Concepts

User Accounts and Groups:

- **User accounts** represent individual identities. Each should be unique (no shared accounts) for accountability.
- **Groups** simplify permission management by assigning rights to a collection of users. Users inherit group permissions.

Segregation of Duties (SoD):

No single person should control all aspects of a critical process. Example: the person who creates a user account should not also approve access to sensitive data.

Password Policies:

Policy Element	Typical Setting	Purpose
Minimum Length	14+ characters	Resist brute-force
Complexity	3 of 4: upper, lower, digit, special	Increase keyspace
Lockout Threshold	5 failed attempts	Block password guessing
Lockout Duration	15–30 minutes	Balance security vs. DoS
Maximum Age	90 days	Force rotation
Minimum Age	1 day	Prevent cycling to old password
History	24 passwords	Prevent reuse

Access Control Models:

Model	Definition	Use Case
RBAC (Role-Based)	Permissions assigned to roles; users assigned to roles	Most common in enterprises
Rule-Based	Access determined by system-enforced rules (time, location)	Conditional access
Scope-Based	Access limited by organizational scope (OU, department)	Delegation in AD
MAC (Mandatory)	OS enforces clearance levels (confidential, secret)	Government/military
DAC (Discretionary)	Resource owner controls access	Standard file permissions

Permissions and Access Controls:

- **File ACLs:** Fine-grained permissions on individual files/folders
- **Group permissions:** Assign rights to groups, not individuals
- **Least Privilege:** Users get exactly the access needed, nothing more

Delegation:

Assigning specific administrative tasks to users without giving full admin rights.

Example: help desk can reset passwords but cannot modify group memberships.

Auditing — Four Things to Track:

1. **User activity** (what actions were taken)
2. **Logins** (successful and failed)
3. **Group memberships** (changes to access rights)
4. **Deletions** (accounts, files, records)

Multi-Factor Authentication (MFA):

Factor	Example
Something you know	Password, PIN
Something you have	TOTP app, FIDO2 key, smart card
Something you are	Fingerprint, iris, face

MFA requires **two or more different factor types**. Password + PIN is NOT MFA (both are "something you know").

Single Sign-On (SSO):
One set of credentials authenticates to multiple services.

Aspect	Detail
Benefits	Fewer passwords, central revocation, central audit
Risks	One compromised account opens many services
Mitigation	**Combine SSO with MFA**
Technologies	Kerberos (AD), SAML/OIDC (web apps)

Exam Tips

- **MFA requires different factor types.** Password + security question = not MFA (both "know").
- **RBAC is the most common model** in enterprise server environments.
- **Least privilege** is a guiding principle, not a specific technology.
- **SSO + MFA** is the recommended combination — SSO for convenience, MFA for security.

- **Audit four targets:** user activity, logins, group memberships, deletions.

Notes

- Unique accounts + groups = accountable, manageable access.
- Password policies balance security (length, complexity) with usability (lockout duration).
- RBAC assigns permissions to roles; least privilege limits scope.
- MFA needs different factor types; SSO is convenient but requires MFA for security.
- Auditing tracks who did what, when, and to which resources.

3.4 Mitigation Strategies

Key Concepts

Malware Prevention:

Malware prevention is a layered defense strategy. No single tool catches everything.

Layer	Purpose	Examples
Antivirus/Anti-malware	Signature-based detection of known threats	Windows Defender, ClamAV
HIDS (Host Intrusion Detection System)	Monitors file integrity and system changes	AIDE (Linux), Tripwire
HIPS (Host Intrusion Prevention System)	Actively blocks suspicious behavior	fail2ban, auditd rules
EDR (Endpoint Detection and Response)	Behavioral analysis + automated response	CrowdStrike, SentinelOne
Application Whitelisting	Only approved apps can execute	Windows AppLocker

Key malware prevention practices:

1. **Keep signatures updated** — antivirus without current definitions is nearly useless.
2. **Disable AutoRun/AutoPlay** — prevents USB-borne malware from executing automatically.
3. **Apply least privilege** — malware running under a standard user account has limited impact.
4. **Scan regularly** — scheduled full scans, not just real-time protection.

Data Loss Prevention (DLP):

DLP prevents sensitive data from leaving the organization. It monitors, detects, and blocks unauthorized data transfers.

DLP Type	What It Monitors	Example
Network DLP	Data in transit (email, web, FTP)	Blocks emails containing credit card numbers
Endpoint DLP	Data at rest and in use on endpoints	Prevents copying files to USB drives
Storage DLP	Data on file servers and databases	Alerts on unusual access patterns

DLP content inspection methods:

- **Pattern matching:** Regex for SSNs, credit cards, API keys.
- **Fingerprinting:** Hashes of known sensitive documents.
- **Contextual rules:** Who is sending, to whom, when, from where.

SIEM (Security Information and Event Management):

SIEM aggregates logs from multiple sources, correlates events, and alerts on suspicious patterns.

Function	Description
Log Collection	Gathers logs from servers, firewalls, applications, endpoints
Correlation	Links events across sources (e.g., failed logins on multiple servers)
Alerting	Notifies security team of potential incidents
Dashboards	Visualizes security posture in real time
Retention	Stores logs for compliance and forensic analysis

Common SIEM tools: Splunk, IBM QRadar, Microsoft Sentinel, Elastic Security.

SIEM benefits:

- Central visibility across the entire infrastructure.
- Faster incident detection through correlation.
- Compliance reporting (PCI-DSS, HIPAA, SOX).
- Forensic investigation support.

Exam Tips

- **HIDS detects; HIPS prevents.** Know the difference — HIDS alerts, HIPS blocks.
- **DLP is about data exfiltration, not malware.** It stops sensitive data from leaving, regardless of whether malware is involved.
- **SIEM correlates logs.** If a question mentions "multiple log sources" and "alerts," SIEM is the answer.
- **AutoRun/AutoPlay should be disabled on servers** to block USB malware vectors.

Notes

- Defense in depth: antivirus + HIDS/HIPS + EDR + whitelisting.
- DLP prevents sensitive data from leaving; it's about confidentiality, not malware.
- SIEM = centralized log collection + correlation + alerting.
- Disable AutoRun and keep definitions current as baseline hygiene.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

3.5 Server Hardening

Key Concepts

Hardening Philosophy:

"Remove what you don't need and use the most current version of what's left."

Hardening reduces the **attack surface** — every unnecessary service, port, account, or feature is a potential entry point.

OS Hardening Checklist:

Step	Action	Commands/Tools
1. Patch	Apply all OS/security updates	`unattended-upgrades` (Linux), WSUS (Windows)

Step	Action	Commands/Tools
2. Disable unused services	Stop and disable services not required for the server role	`systemctl disable --now <service>`
3. Close unused ports	Firewall default-deny, allow only required ports	`ufw default deny incoming`
4. Remove unnecessary software	Uninstall unused packages	`apt purge telnet ftp`
5. Secure default accounts	Rename/disable admin, root, guest	Change default passwords immediately
6. Configure logging	Enable audit logging, forward to SIEM	Centralize logs, protect from tampering
7. Disable AutoRun	Prevent automatic execution from removable media	Group Policy / registry

Application Hardening:

Applications installed on servers must also be hardened. Unused features increase attack surface.

Application	Hardening Action
Web Server (Nginx/Apache)	Disable server tokens, add security headers, limit request size
Database	Remove sample databases, disable remote root access, enforce strong passwords
Any app	Install only required features, apply vendor hardening guides

Host Security Tools:

Tool Type	Purpose	Examples
Antivirus	Malware detection	ClamAV (Linux), Windows Defender
HIDS	File integrity monitoring	AIDE, Tripwire
Rootkit Scanner	Detect rootkits	chkrootkit
HIPS	Behavioral blocking	fail2ban, auditd

Hardware Hardening:

Action	Purpose
Set BIOS/UEFI password	Prevent unauthorized boot device changes
Set boot order	Restrict boot to internal disk only
Disable unused hardware	USB ports, optical drives, wireless NICs
Disable physical ports	Prevent unauthorized device connection

Patching Workflow (Server+ 3.5):

```
text
Vendor advisory → Test in staging (snapshot first) →
   Change ticket → Maintenance window →
      Apply in production (cluster-aware) → Verify → Close ticket
```

Practical Commands

Linux — Baseline scan and hardening:

```
bash
# Baseline scan with Lynis (hardening index 0-100)
```

```
lynis audit system --quick

# List enabled services
systemctl list-unit-files --type=service --state=enabled

# Disable unused services
systemctl disable --now cups bluetooth avahi-daemon

# Firewall: default deny, allow SSH only
ufw default deny incoming
ufw allow 22/tcp
ufw --force enable

# Check listening ports
ss -tulnp

# Remove unnecessary packages
apt purge -y telnet ftp rsh-client
apt autoremove -y
```

File integrity with AIDE:

```
bash
# Initialize baseline
aideinit -y -f
# Check for changes
aide --check
```

Exam Tips

- **"Remove what you don't need"** — this is the core hardening principle .
- **HIDS detects, HIPS prevents.** AIDE is HIDS; fail2ban is HIPS.
- **BIOS password prevents boot tampering** — a hardware-level control .
- **Patching must follow change management** — never patch production without testing.
- **Lynis gives a hardening index (0–100)** — useful for measuring baseline improvement.

Notes

- Hardening = remove unnecessary + patch everything remaining.
- Disable unused services, close unused ports, remove unused software.
- HIDS monitors integrity; HIPS blocks behavior; antivirus detects malware.
- Hardware hardening: BIOS password, boot order, disable unused ports.
- Patch workflow: advisory → staging → change ticket → production → verify.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

3.6 Decommissioning

Key Concepts

Decommissioning Workflow (Server+ 3.6):

Proper decommissioning is a **process**, not just pulling power.

```
[ ] Verify non-utilisation (no service depends on this server)
[ ] Open change ticket with rollback plan
[ ] Schedule downtime, notify users
[ ] Drain from load balancer / cluster
[ ] Final backup → tested restore → off-site copy
[ ] Capture as-built docs to asset record
[ ] Power off
[ ] Wipe media
[ ] Physical destruction OR repurposing
[ ] Update CMDB: status = retired, asset tag returned
[ ] Cable remediation: pull patch cables
[ ] Issue certificate of destruction
```

Critical First Step: Verify Non-Utilisation:

Before touching anything, confirm **no service still depends on this server**. Check DNS records, load balancer configs, monitoring systems, and application dependencies. Decommissioning a server still in use causes outages.

Media Destruction Methods:

Method	What It Does	Use For	Not For
Disk Wiping (Logical)	Overwrites data with random/zero patterns	Reusable drives	SSDs (wear-leveling)
Degaussing	Strong magnetic field randomizes platters	Magnetic HDDs, tapes	**SSDs — zero effect**
Shredding	Industrial shredder destroys physical media	Universal (HDD, SSD, tape, optical)	—
Crushing	Hydraulic press	Quick on-site destruction	—
Incineration	High-temperature furnace	Maximum assurance (top-secret)	—

Critical SSD Warning:

Degaussing an SSD does absolutely nothing. SSDs contain zero magnetic material — data is stored as electrical charges in NAND flash cells. A degausser leaves 100% of SSD data intact.

Why logical wiping fails on SSDs:

- **Wear-leveling:** Controller redirects writes to different physical cells.
- **Over-provisioning:** 10–30% hidden spare capacity not addressable by OS.
- **Result:** Original data remains in unmapped cells, recoverable by forensic analysis.

Proper SSD sanitization:

```bash
# NVMe Sanitize (Block Erase — Purge level)
sudo nvme sanitize /dev/nvme0n1 -a 2

# Cryptographic Erase (instant — destroys encryption key)
sudo nvme format /dev/nvme0n1 --ses=2
```

For self-encrypting drives (SED): Cryptographic erase — destroy the key, data becomes unreadable instantly.

Chain of Custody:

Documentation trail tracking every person who handled the media from decommission to destruction. Required for compliance. Must include: serial numbers, method used, date, witness signatures, certificate of destruction.

Electronics Recycling:

Type	Description
Internal Recycling	Organization repurposes components internally (test, wipe, redeploy)
External Recycling	Vendor handles disposal — requires due diligence (certifications: R2, e-Stewards)
Repurposing	Server gets a new role instead of being decommissioned

Cable Remediation:

After removing a server:

- Pull patch cables from switches and patch panels.
- Label removed PDU strips.
- Update cable management documentation.
- Prevent "ghost cables" that confuse future troubleshooting.

Asset Management Integration:

Action	Purpose
Update CMDB status to "retired"	Accurate inventory
Return asset tag	Reconcile physical vs. recorded assets
File certificate of destruction	Compliance proof
Capture as-built docs	Historical record

Exam Tips

- **D is often the answer for decommissioning questions:** "Review company policies" comes before any technical action. Policies dictate procedure.
- **Degaussing does NOT work on SSDs** — this is a high-probability exam question.
- **Logical wiping on SSDs is insufficient** — wear-leveling hides data. Use NVMe Sanitize or Cryptographic Erase.
- **Certificate of destruction** is required documentation after physical destruction.
- **Verify non-utilisation before anything else** — pulling a server still in use is a self-inflicted outage.

Notes

- Decommissioning is a documented process: verify → backup → wipe → destroy/recycle → update records.
- Degaussing = magnetic HDDs/tapes only. SSDs need sanitize/crypto-erase/shredding.
- Chain of custody tracks every handler of the media.
- Cable remediation prevents undocumented "ghost" connections.

- Always follow company policies and change management before technical action.

Exam Strategy for Domain 3:

- Expect scenario questions on decommissioning, hardening, and physical security.
- **Degaussing + SSD = wrong answer** — memorize this.
- **Policies before technical action** in decommissioning scenarios.
- Know the difference: HIDS (detect) vs. HIPS (prevent); DLP (data) vs. SIEM (logs).

Domain4: Troubleshooting (28%)

Exam Context: Troubleshooting tests your ability to identify symptoms, form hypotheses, test theories, and implement solutions using a consistent methodology. The exam presents realistic server failure scenarios and asks for the MOST likely cause or NEXT step.

4.1 Troubleshoot Hardware

Key Concepts

Troubleshooting Methodology (Apply to ALL Hardware Issues):

1. **Identify the problem** — Gather information from users, logs, and observations
2. **Establish a theory** — Question the obvious, research symptoms
3. **Test the theory** — Confirm or reject the hypothesis
4. **Establish a plan of action** — Determine resolution steps
5. **Implement the solution** — Execute with rollback plan ready
6. **Verify full functionality** — Confirm resolution and implement preventive measures

7. **Document findings** — Record actions and outcomes

Power Issues:

Symptom	Likely Cause	Diagnostic Step
Server won't power on	PSU failure, power cord, PDU issue	Check link lights, swap PSU, test outlet
Intermittent shutdowns	Overheating, failing PSU, power fluctuations	Check thermal logs, event viewer
CMOS battery failure	BIOS settings lost, clock resets on boot	Replace CMOS battery, reconfigure BIOS
Amber link light on NIC	Misconfigured NIC, speed/duplex mismatch	Check NIC settings, cable, switch port

Storage Failures:

Symptom	Likely Cause	Diagnostic Step
RAID degraded	Failed disk member	Identify failed drive via RAID controller, hot-swap
Boot failure, "no bootable device"	Failed boot drive, corrupted boot sector	Check BIOS boot order, test with recovery media
Slow performance	Failing drive, RAID rebuild in progress	Check SMART data, RAID status
Partition corruption	File system damage, power loss during write	Run chkdsk (Windows) or fsck (Linux)

Connectivity Problems:

Symptom	Likely Cause	Diagnostic Step
No network connectivity	Bad cable, misconfigured NIC, dead switch port	Check link lights, swap cable, test port

Amber link light	Speed/duplex mismatch	Set NIC to auto-negotiate or match switch
Intermittent connectivity	Failing NIC, bad cable, loose connection	Check event logs, replace NIC, reseat cable

Practical Commands

Linux — Hardware diagnostics:

```
bash
# Check disk health (SMART)
smartctl -a /dev/sda

# Check RAID status
cat /proc/mdstat
mdadm --detail /dev/md0

# Check PCI devices
lspci

# Check USB devices
lsusb

# Check memory
free -h
cat /proc/meminfo
```

Windows — Hardware diagnostics:

```
powershell
# Check disk health
Get-PhysicalDisk | Select FriendlyName, HealthStatus, OperationalStatus

# Check system events
Get-EventLog -LogName System -EntryType Error -Newest 20

# Check NIC status
Get-NetAdapter | Select Name, Status, LinkSpeed
```

Exam Tips

- **Amber link light = physical layer problem** (speed/duplex mismatch, bad cable, NIC misconfiguration) .
- **CMOS battery failure** causes clock resets, which breaks Kerberos authentication (time skew) .
- **Hot-swap drives** in RAID arrays without powering down the server.
- **Always verify backups** before hardware maintenance that risks data.

Notes

- Follow structured methodology for all hardware issues.
- Power issues often trace to PSU, cord, or CMOS battery.
- Amber link lights indicate Layer 1 problems.
- Check RAID status before replacing disks.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

4.2 Troubleshoot Software

Key Concepts

OS Errors:

Symptom	Likely Cause	Diagnostic Tool
Unable to log on	Account lockout, expired credentials, corrupted profile	Event Viewer, auth logs

Symptom	Likely Cause	Diagnostic Tool
Clock skew	CMOS battery failure, NTP misconfiguration	`chronyc tracking`, `w32tm /query /status`
System file corruption	Bad update, disk error	`sfc /scannow`, `dism /online /cleanup-image /restorehealth`
Service failures	Missing dependency, permission change	`systemctl status`, Event Viewer
Boot loops	Bad driver, failed patch	Recovery mode, safe mode

Patch/Update Failures:

Symptom	Likely Cause	Recovery Step
Stuck update	Missing dependency, held package	`dpkg --configure -a`, `apt -f install`
Boot loop after patch	Incompatible driver, kernel mismatch	Boot previous kernel, rollback update
Service won't start after patch	Permission change, removed dependency	Check logs, verify dependencies

Kerberos Clock Skew — Critical Concept:

Kerberos authentication **rejects logins if time drift exceeds 5 minutes**. This causes:

- Users "randomly can't log in"
- Domain trust relationship failures
- Authentication errors across the environment

Fix: Restart NTP/chrony service and force time synchronization.

Practical Commands

Linux — Software troubleshooting:

bash

```
# Check failed services
systemctl list-units --type=service --state=failed

# View service logs
journalctl -u sshd -n 30 --no-pager

# Check dependencies
systemctl list-dependencies sshd

# Fix broken packages
dpkg --configure -a
apt -f install

# Check package history
cat /var/log/apt/history.log

# Time synchronization
chronyc tracking
timedatectl
```

Windows — Software troubleshooting:

```
powershell
# Check system files
sfc /scannow

# Check update history
Get-WindowsUpdateLog
Get-HotFix

# Check Kerberos
klist
nltest /sc_query:DOMAIN

# Force time sync
w32tm /resync
```

Recovery Boot Modes:

Mode	Linux Equivalent	When to Use
Safe Mode	`systemd.unit=rescue.target`	Service failure prevents boot
Single-User	`systemd.unit=emergency.target`	Root password reset, emergency recovery
Last Known Good	Boot previous kernel	Bad driver/patch
Recovery Media	Install media	Corrupted OS beyond repair

Exam Tips

- **Clock skew > 5 minutes = Kerberos failure** — high-probability exam question.
- **Patch failure recovery order:** `dpkg --configure -a` → `apt -f install` → restart failed unit.
- **Corrupted profile ≠ hardware failure** — software symptoms can mimic hardware.
- **Always check logs first** — Event Viewer (Windows), `journalctl` (Linux).

Notes

- Clock skew is a common cause of authentication failures.
- Patch failures require dependency analysis and package manager repair.
- Recovery boot modes provide access when normal boot fails.
- Logs are your primary diagnostic tool for software issues.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

4.3 Troubleshoot Network

Key Concepts

Latency:

Symptom	Likely Cause	Diagnostic Tool
High latency to specific host	Network congestion, routing issue	`traceroute`, `mtr`
High latency to all hosts	NIC issue, duplex mismatch	Check NIC settings, switch port
Intermittent latency spikes	Packet loss, faulty cable	`ping -t`, packet capture

Misconfigurations:

Symptom	Likely Cause	Diagnostic Step
APIPA address (169.254.x.x)	DHCP failure, VLAN misconfiguration	Check DHCP server, relay, VLAN assignment
Can ping IP but not hostname	DNS resolution failure	`nslookup`, check DNS server
Domain join fails	DNS pointing to external resolver	Verify DNS points to AD-integrated DNS
VLAN traffic not passing	Trunk/access port misconfiguration	Check switch port VLAN assignment

Security Breaches (Network-Level):

Symptom	Likely Cause	Diagnostic Step
Unusual outbound traffic	Compromised host, malware	Check firewall logs, netstat

Symptom	Likely Cause	Diagnostic Step
Failed login attempts from external IPs	Brute force attack	Check auth logs, SIEM alerts
Unexpected open ports	Unauthorized service, backdoor	`ss -tulnp`, port scan
Rogue DHCP server	Unauthorized device	Check DHCP snooping, network scan

Key Network Diagnostics:

Tool	Purpose	Platform
`ping`	Basic connectivity	Both
`traceroute` / `tracert`	Path discovery	Both
`nslookup` / `dig`	DNS resolution	Both
`netstat` / `ss`	Open ports and connections	Both
`tcpdump` / **Wireshark**	Packet capture	Both
`ipconfig` / `ip addr`	IP configuration	Both

Practical Commands

Linux — Network troubleshooting:

```
bash
# Check IP configuration
ip addr show
ip route show

# DNS resolution test
nslookup servername
```

```
dig servername

# Check open ports
ss -tulnp

# Trace route
traceroute hostname

# Packet capture
tcpdump -i eth0 -w capture.pcap

# Check ARP
arp -a
```

Windows — Network troubleshooting:

```
powershell
# Check IP configuration
ipconfig /all

# DNS cache operations
ipconfig /flushdns
ipconfig /displaydns

# Test DNS
nslookup servername

# Check ports
netstat -ano

# Trace route
tracert hostname
```

Exam Tips

- **APIPA = DHCP failure** → check VLAN assignment, DHCP server, relay agent.
- **Amber link light = Layer 1 issue** → speed/duplex mismatch, bad cable, NIC config .
- **DNS must point to AD-integrated DNS** for domain functionality.
- `traceroute` **identifies WHERE latency occurs** (which hop).

Notes

- Latency can be localized with `traceroute`/`mtr`.
- APIPA indicates DHCP failure — investigate Layer 2 first.
- DNS misconfiguration breaks domain joins and name resolution.
- Security breaches often show as unusual traffic or failed logins.

4.4 Disaster Recovery

Key Concepts

Backup Strategies:

Type	What It Backs Up	Restore Complexity	Storage Efficiency
Full	Everything	Simplest (one set)	Worst (most space)
Incremental	Changes since last backup (any type)	Complex (full + all incrementals)	Best
Differential	Changes since last full backup	Moderate (full + latest differential)	Moderate

3-2-1 Backup Rule:

- **3** copies of data
- **2** different media types
- **1** copy off-site

Modern Variation (3-2-1-1-0):

- Add: 1 copy offline/immutable, 0 errors on verification

Recovery Testing:

Test Type	What It Validates	Scope
Backup Restore Test	Data integrity, restore process	Single file/database

Test Type	What It Validates	Scope
Tabletop Exercise	Team decision-making, communication	No production systems
Partial Recovery Drill	Critical workload restoration	One component
Full Recovery Exercise	Complete DR plan	Broad outage simulation

Critical Insight: Backup success logs do NOT prove recovery. Only actual restores prove recovery.

RTO vs. RPO:

Metric	Definition	Example
RPO	Max acceptable **data loss**	4 hours = backups every 4 hours
RTO	Max acceptable **downtime**	2 hours = service restored within 2 hours

Failover Validation:

Aspect	What to Verify
DNS updates	Failover host resolves correctly
Authentication	Domain logins work from alternate site
Storage latency	Acceptable performance from DR site
Application dependencies	All required services available
Failback	Return to primary site works

Recovery Test Metrics

Metric	What It Measures	Target
Backup success rate	Jobs completed	>99%
Restore success rate	Restores that worked	100% for critical systems
RPO attainment	Data loss within target	100%
Recovery duration	Time to restore service	≤ RTO
Test coverage	Critical systems tested	100%

Practical Commands

Linux — Backup verification:

```
bash
# Test restore (example with tar)
tar -tzf backup.tar.gz          # List contents without extracting
tar -xzf backup.tar.gz -C /tmp/restore_test  # Extract to test location

# Verify checksums
sha256sum backup.tar.gz
md5sum backup.tar.gz

# Check backup logs
cat /var/log/backup.log
```

Windows — Backup verification:

```
powershell
# Check backup status
Get-WBSummary
Get-WBJob

# Test restore (Windows Server Backup)
```

```
wbadmin get versions
wbadmin start recovery -version:MM/DD/YYYY-HH:MM -itemType:File -items:C:\test -re
coveryTarget:C:\restore_test
```

Exam Tips

- **RPO = data loss tolerance** (backup frequency). **RTO = downtime tolerance** (recovery speed). Know the difference cold.
- **Test restores, not just backups.** A successful backup job means nothing if the restore fails.
- **3-2-1 rule:** 3 copies, 2 media types, 1 off-site.
- **Failover validation must test DNS, authentication, storage, and applications**.

Notes

- Full + Incremental = most efficient storage; Full + Differential = simpler restore.
- 3-2-1 rule protects against site-wide disasters.
- RPO/RTO define recovery requirements.
- Regular restore testing is mandatory — backups without verified restores are worthless.

Exam Strategy for Domain 4:

- **Use the troubleshooting methodology** in every scenario question: identify → theory → test → plan → implement → verify → document.
- **Clock skew (Kerberos)** and **amber link lights (Layer 1)** are high-probability topics.
- **RPO vs. RTO** — memorize the distinction.
- **Backup success ≠ recovery success** — test restores.
- **APIPA address** always indicates DHCP failure.

We have 600 Practice test questions for CompTIA Server+ (Plus) [SK0-005] (Taken from previous exams)

Full Practice Set link below

https://skillcertpro.tech/product/comp-tia-serverplus-practice-test/

100% Money back Guarantee, If you don't pass the exam in 1st attempt, your money will be refunded back

Disclaimer: All data and information provided on this site is for informational purposes only. This site makes no representations as to accuracy, completeness, correctness, suitability, or validity of any information on this site & will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.