

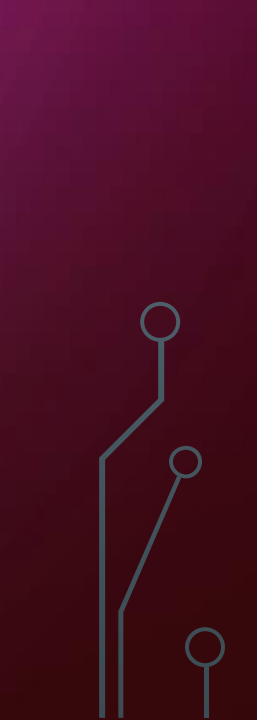


The background is a solid purple color with a subtle gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks. These elements consist of thin lines connecting small circles, creating a geometric, abstract pattern. The lines are more prominent in the top-left and bottom-left corners, and less so in the top-right and bottom-right corners.

MODULE 5B: AUDITING STORAGE

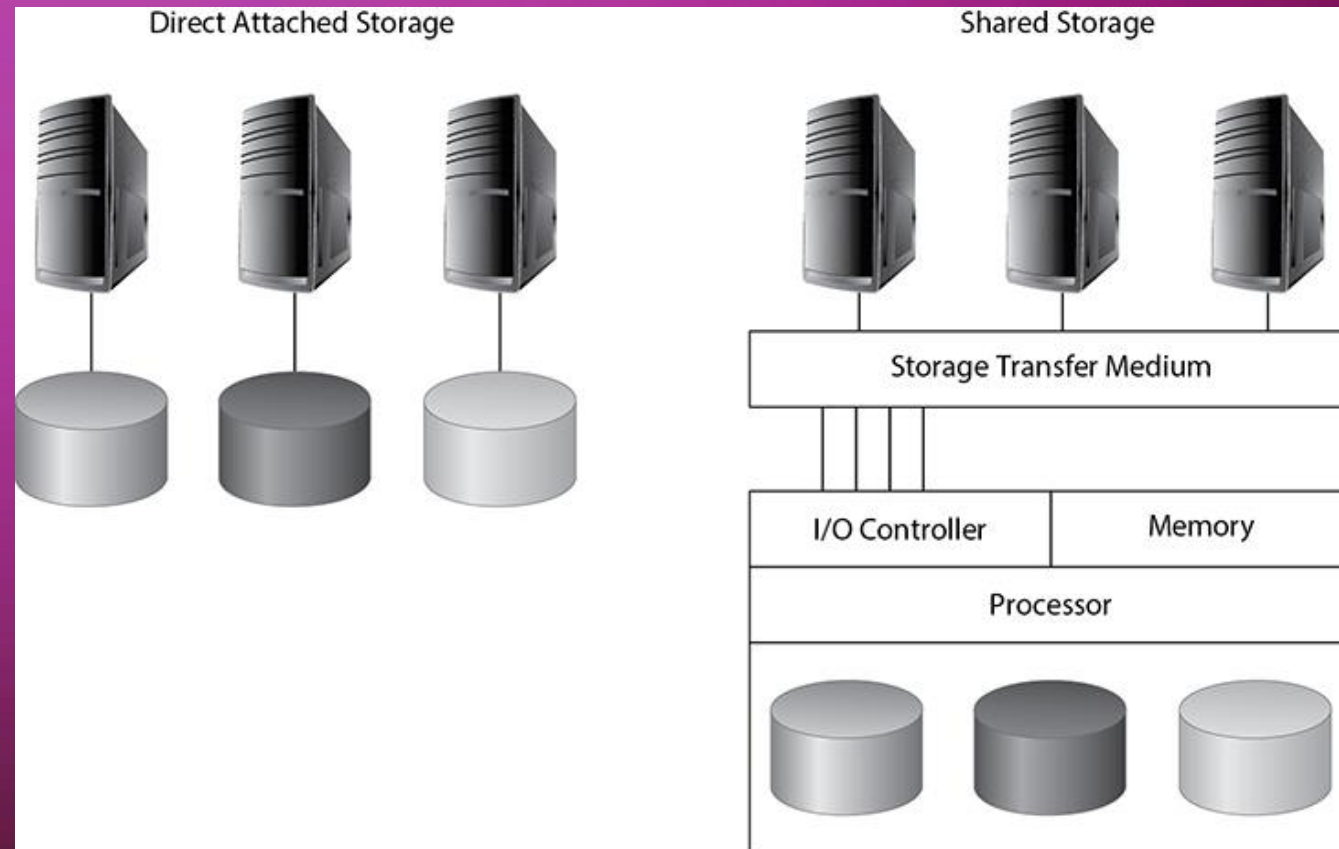


OBJECTIVES

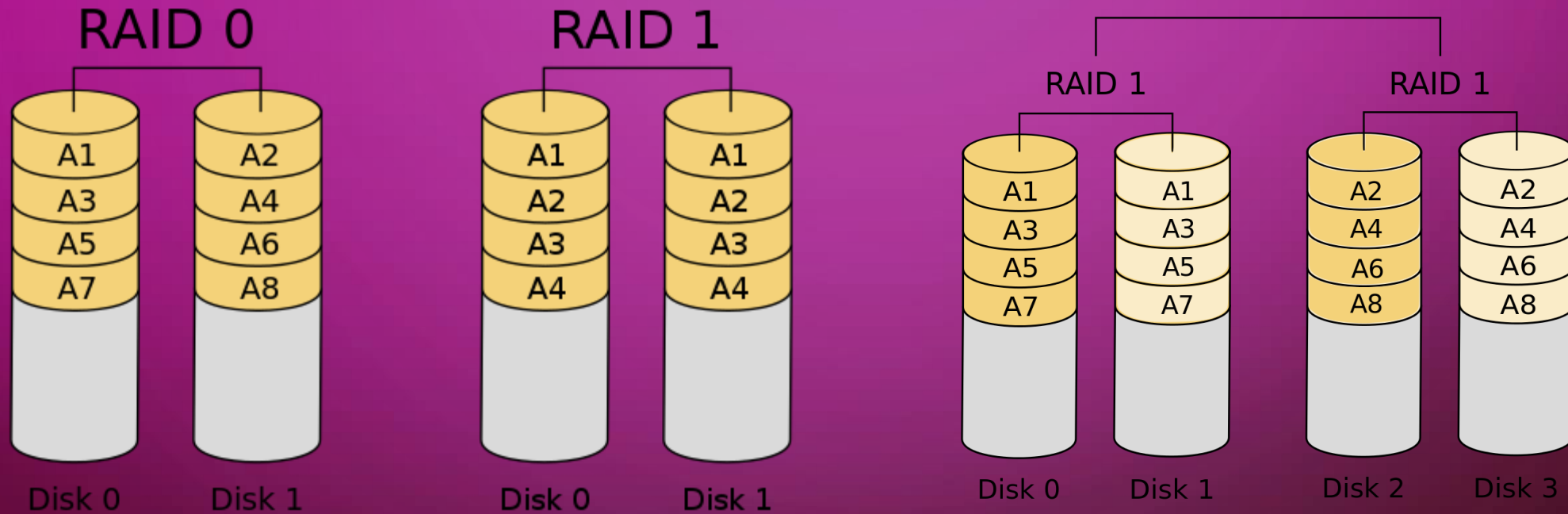
- Overview of RAID
 - Storage Systems
 - How to audit the storage environment
 - Tools and resources for enhancing your storage audits
- 
- 
- 

STORAGE SYSTEMS

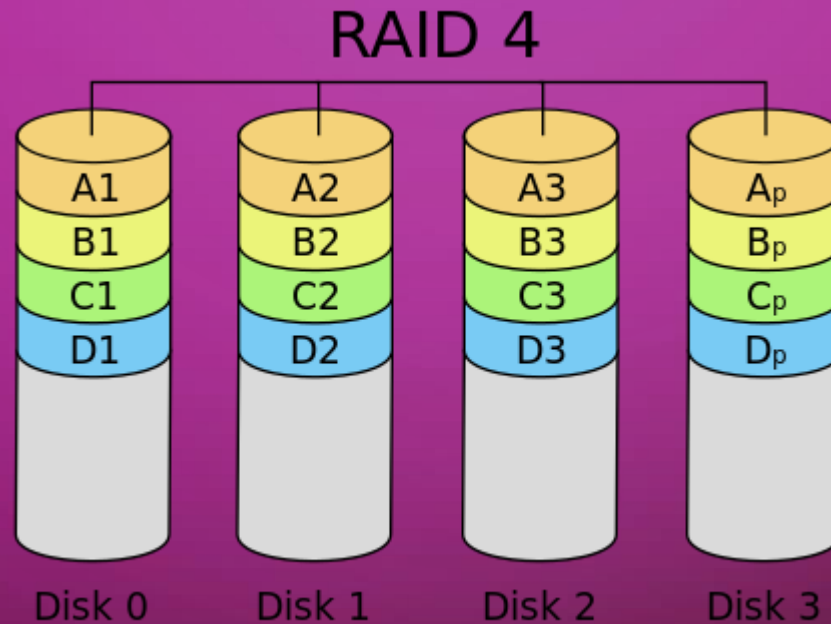
- Storage extends the boundaries of the computing environment to allow data to be shared among users and applications. Storage platforms have grown so efficient that servers can use network-based storage platforms, as opposed to the storage native to the server and other forms of direct attached storage, for their primary storage requirements.



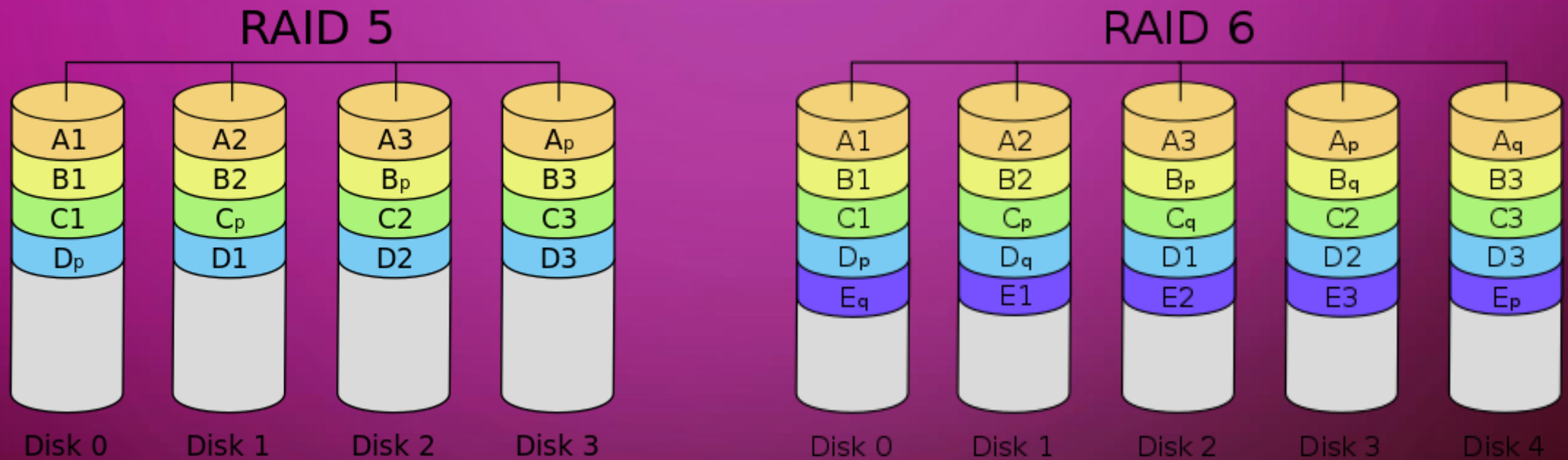
REDUNDANT ARRAY OF INEXPENSIVE DISKS



REDUNDANT ARRAY OF INEXPENSIVE DISKS



REDUNDANT ARRAY OF INEXPENSIVE DISKS



DIRECT ATTACHED STORAGE (DAS)

- Directly attached to the server by connectivity media such as parallel Small Computer System Interface (SCSI) cables. The media can either be internal drives or a dedicated RAID or JBOD (just a bunch of disks). This type of storage is the most limited and doesn't allow for the efficiencies that the other types of storage offer, because DAS is not networked.



<https://netappnotesark.blogspot.com/p/blog-page.html>

NETWORK ATTACHED STORAGE (NAS)

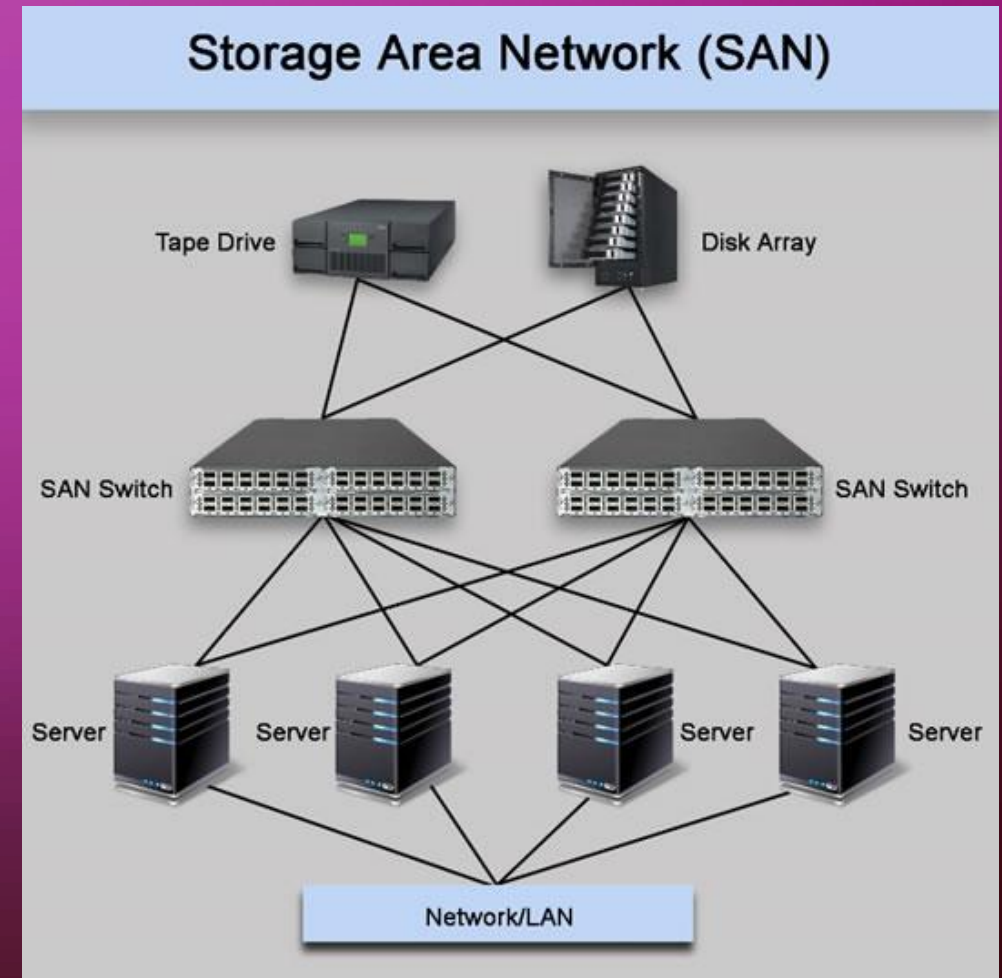
- A *network attached storage* (NAS) device runs an operating system specifically designed to handle files and make them accessible to the network. NAS is also known as file storage and is often accessed by users and applications as mapped drives. Common protocols used in a NAS include Network File System (NFS) for Unix operating systems and Common Internet File System (CIFS) for Microsoft operating systems. Common NAS vendors include Dell EMC and NetApp.



<https://www.indiamart.com/proddetail/qnap-nas-drive-15929034191.html>

STORAGE AREA NETWORK (SAN)

- A *storage area network* (SAN) is a scalable and flexible storage subsystem generally available to more than one host at the same time. The SAN operates using unique block-level communication protocols that require special hardware to work properly. The SAN comprises specialized devices such as host bus adapters (HBAs) in the host servers, switches that help route storage traffic, and disk storage subsystems that understand how to manage the special protocols required for SAN storage. Common protocols used in a SAN include SCSI and Fibre Channel (FC).



RPO & RTO

- Recovery point objective (RPO) determines how much data you will lose should an incident occur.
- Recovery time objective (RTO) determines how long it will take to recover data should an incident occur.
- Organizations should have documented RPOs and RTOs for storage, servers, and critical systems.
 - Typically, in a BCP or DRP

AUDITING STORAGE

What are we looking for?

- Redundancy
- Adequate physical security controls
 - Secured DAS/NAS/SAN systems (if on premise)
- RPO and RTO measures in a DRP or BCP
- Access permissions to storage
- Backup Plan
- Encryption

Checklist for Auditing Storage

- ☐ 1. Document the overall storage management architecture, including the hardware and supporting network infrastructure.
- ☐ 2. Obtain the software version and compare it against policy requirements.
- ☐ 3. Determine what services and features are enabled on the system and validate their necessity with the system administrator.
- ☐ 4. Review and evaluate procedures for creating administrative accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
- ☐ 5. Evaluate the process and policies used for granting and revoking access to storage.
- ☐ 6. Evaluate how capacity is managed for the storage environment to support existing and anticipated business requirements.
- ☐ 7. Evaluate how performance is managed and monitored for the storage environment to support existing and anticipated business requirements.
- ☐ 8. Evaluate the policies, processes, and controls for data backup frequency, handling, and remote storage.
- ☐ 9. Verify that encryption of data-at-rest is implemented where appropriate.
- ☐ 10. Verify that network encryption of data-in-motion is implemented where appropriate.
- ☐ 11. Evaluate the low-level and technical controls in place to segregate or firewall highly sensitive data from the rest of the storage environment.
- ☐ 12. Review and evaluate system administrator procedures for security monitoring.
- ☐ 13. Verify that policies and procedures are in place to identify when a patch is available and to evaluate and apply applicable patches. Ensure that all approved patches are installed per your policy.
- ☐ 14. Perform the steps from Chapter 5 as they pertain to the system you are auditing.