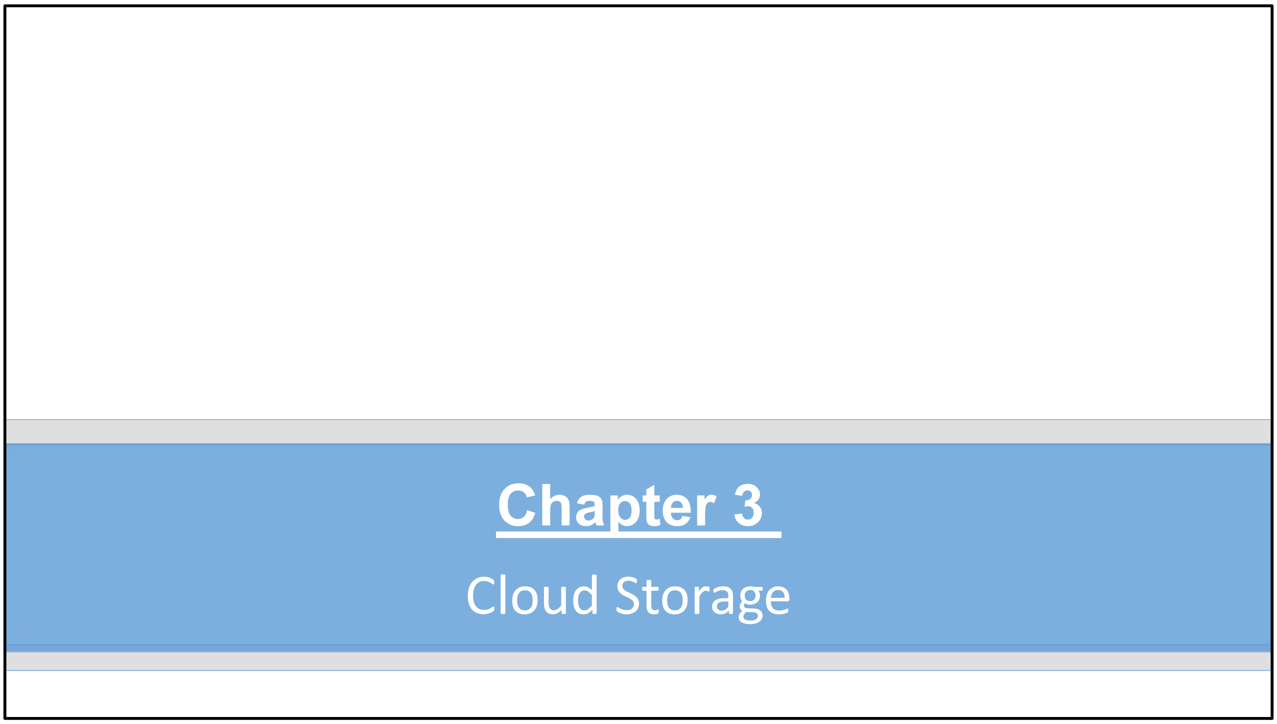
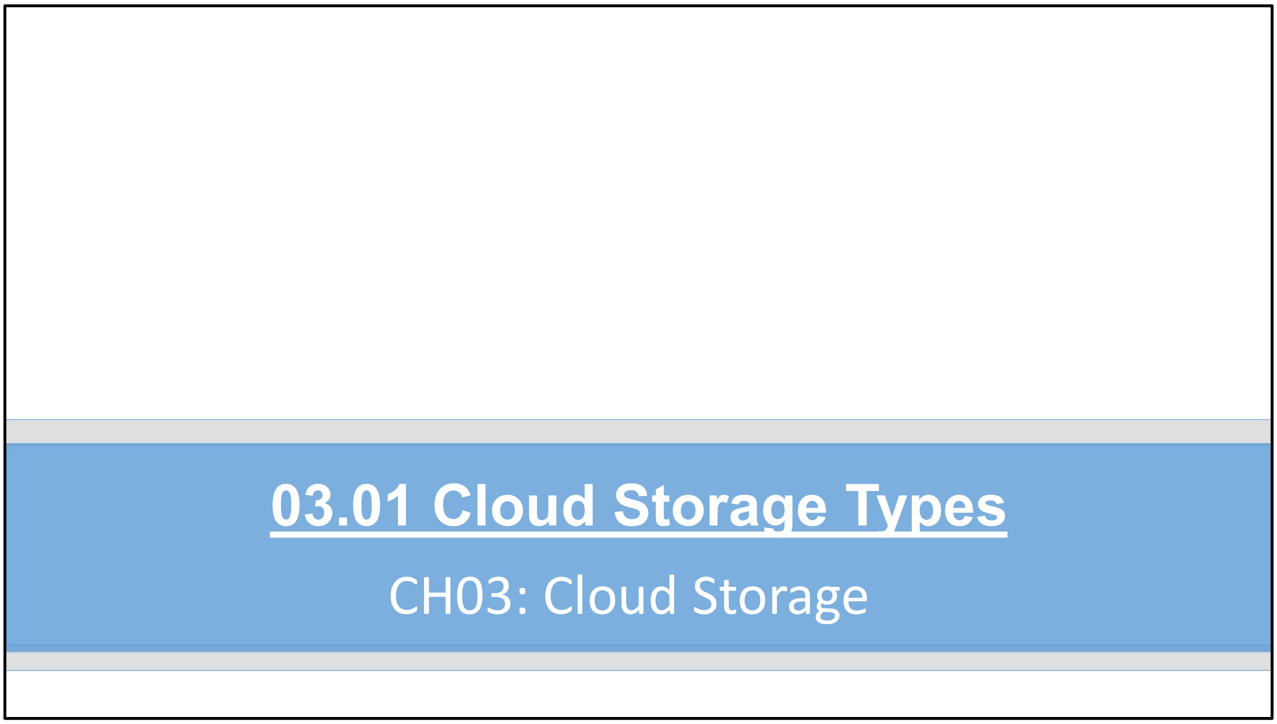


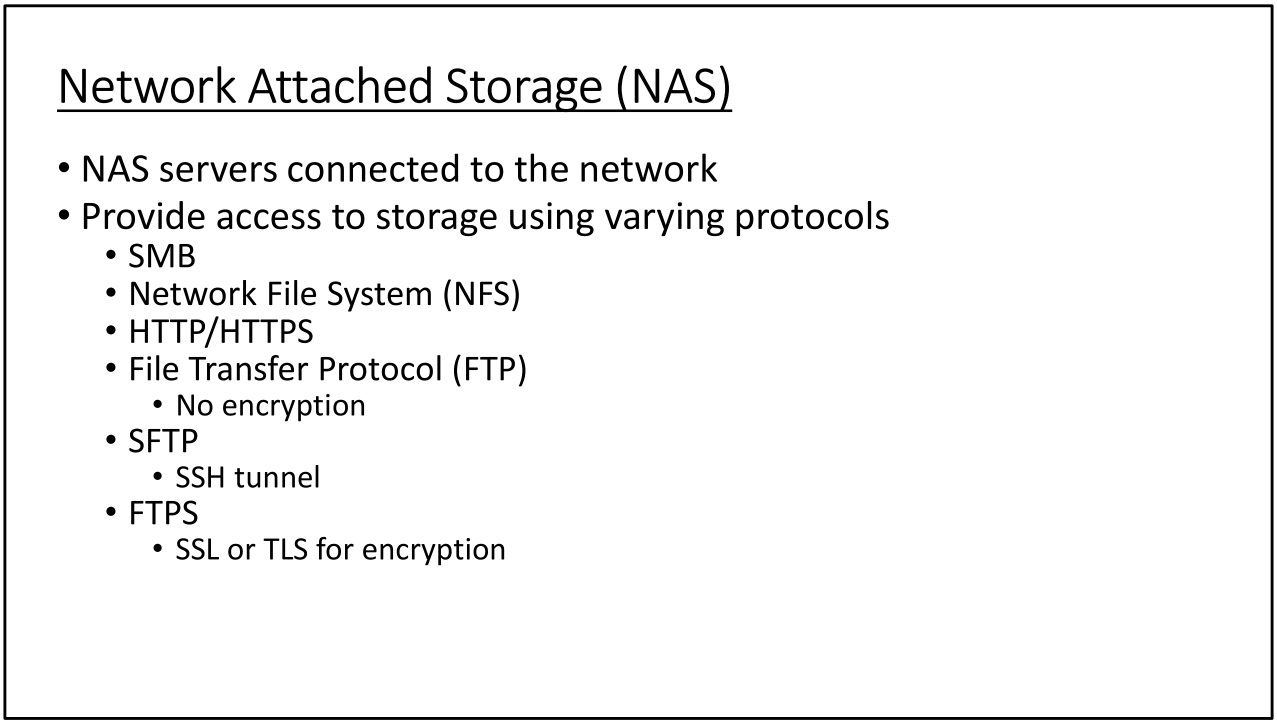
Chapter 3

Cloud Storage



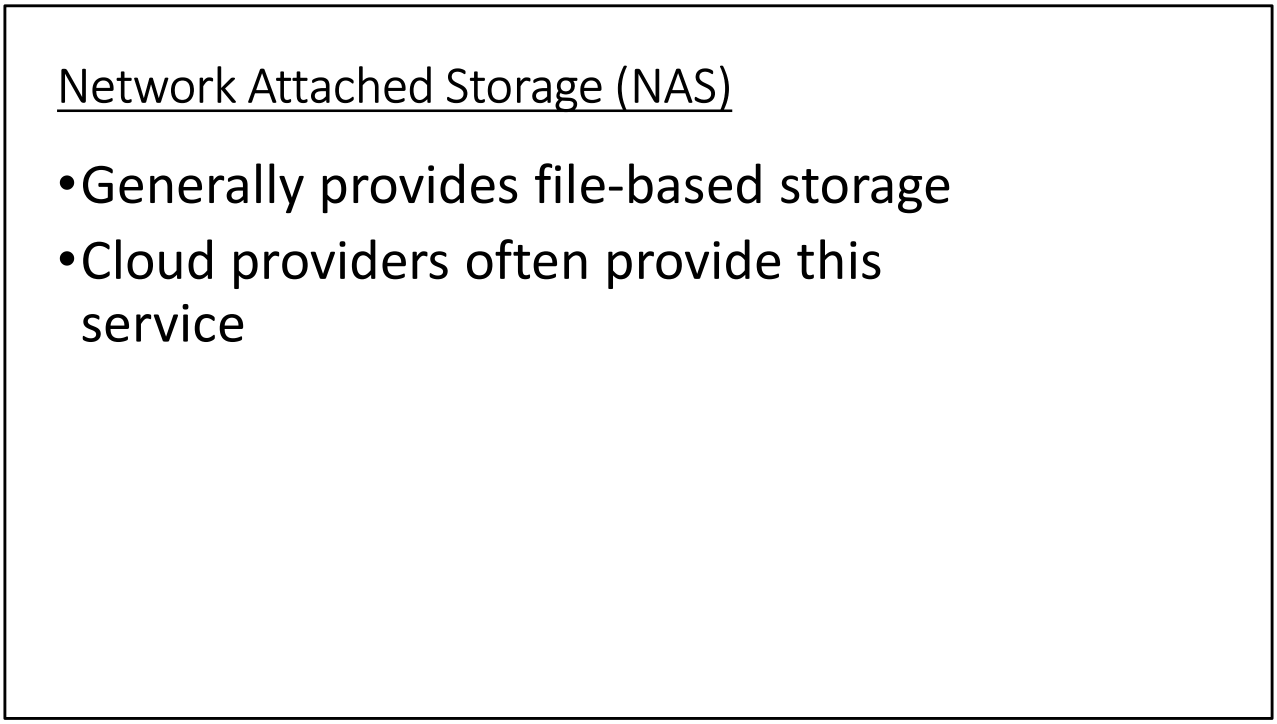
03.01 Cloud Storage Types

CH03: Cloud Storage



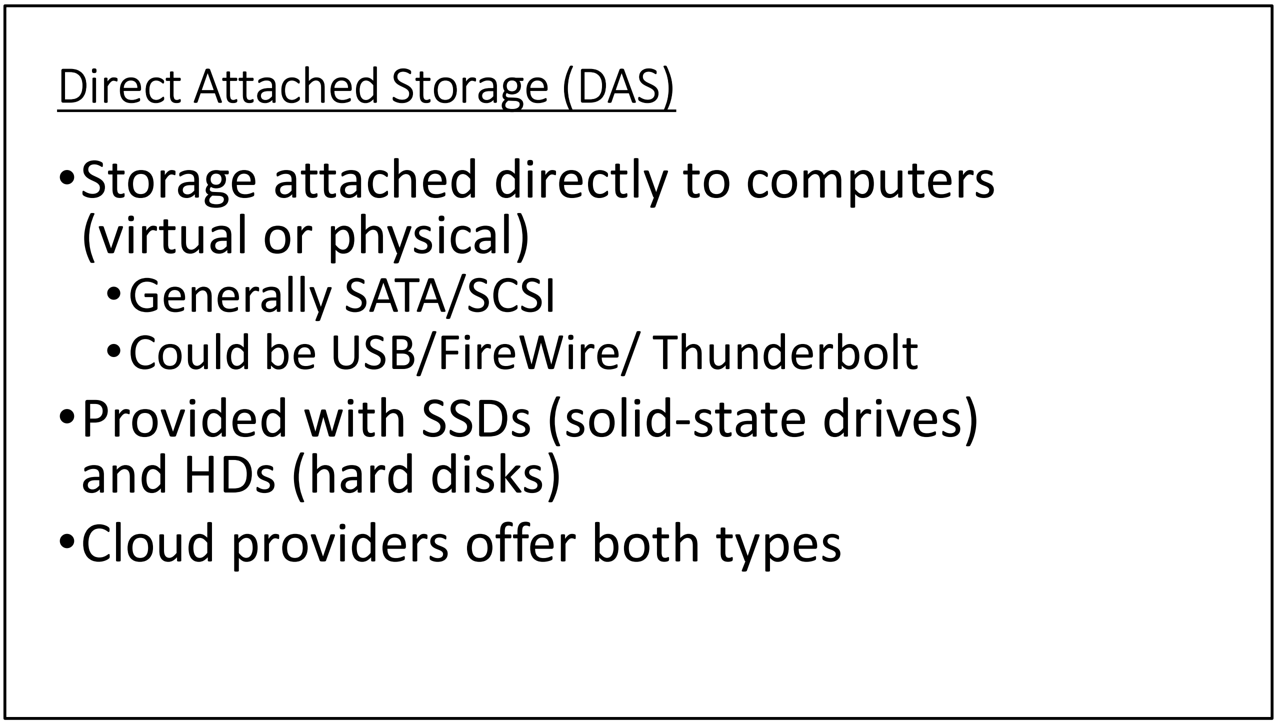
Network Attached Storage (NAS)

- NAS servers connected to the network
- Provide access to storage using varying protocols
  - SMB
  - Network File System (NFS)
  - HTTP/HTTPS
  - File Transfer Protocol (FTP)
    - No encryption
  - SFTP
    - SSH tunnel
  - FTPS
    - SSL or TLS for encryption



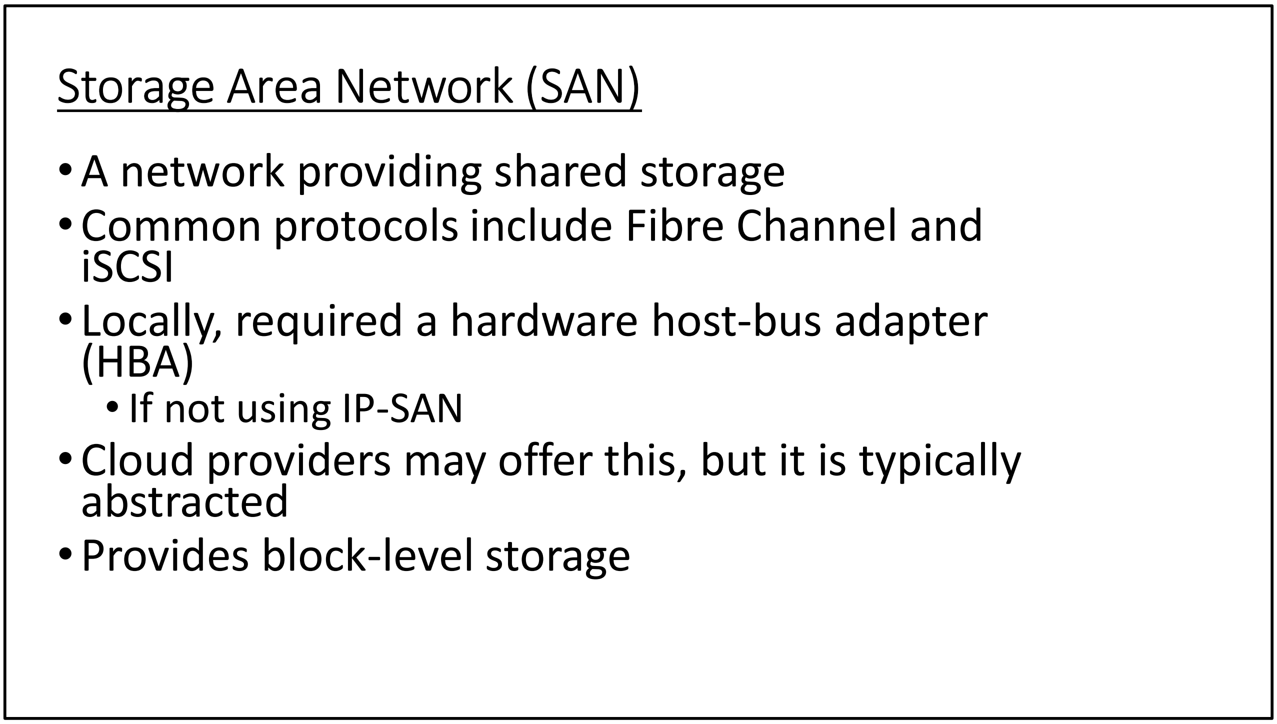
Network Attached Storage (NAS)

- Generally provides file-based storage
- Cloud providers often provide this service



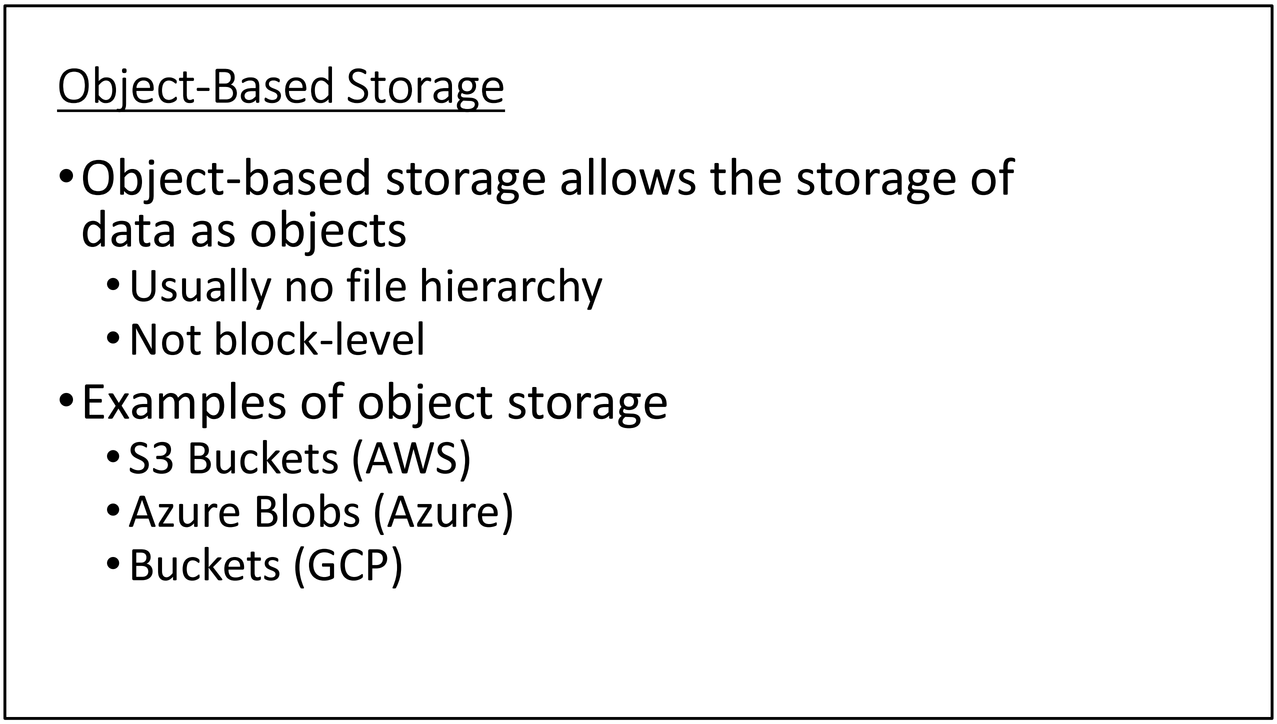
Direct Attached Storage (DAS)

- Storage attached directly to computers (virtual or physical)
  - Generally SATA/SCSI
  - Could be USB/FireWire/ Thunderbolt
- Provided with SSDs (solid-state drives) and HDs (hard disks)
- Cloud providers offer both types



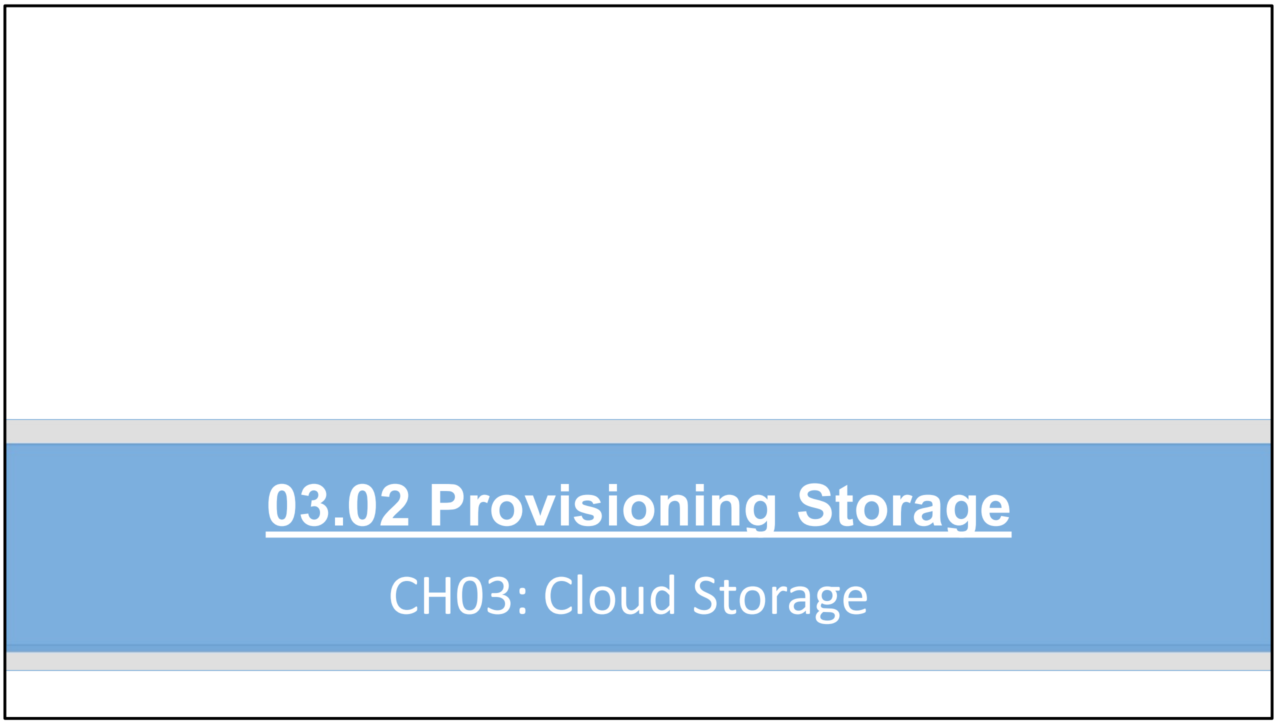
Storage Area Network (SAN)

- A network providing shared storage
- Common protocols include Fibre Channel and iSCSI
- Locally, required a hardware host-bus adapter (HBA)
  - If not using IP-SAN
- Cloud providers may offer this, but it is typically abstracted
- Provides block-level storage



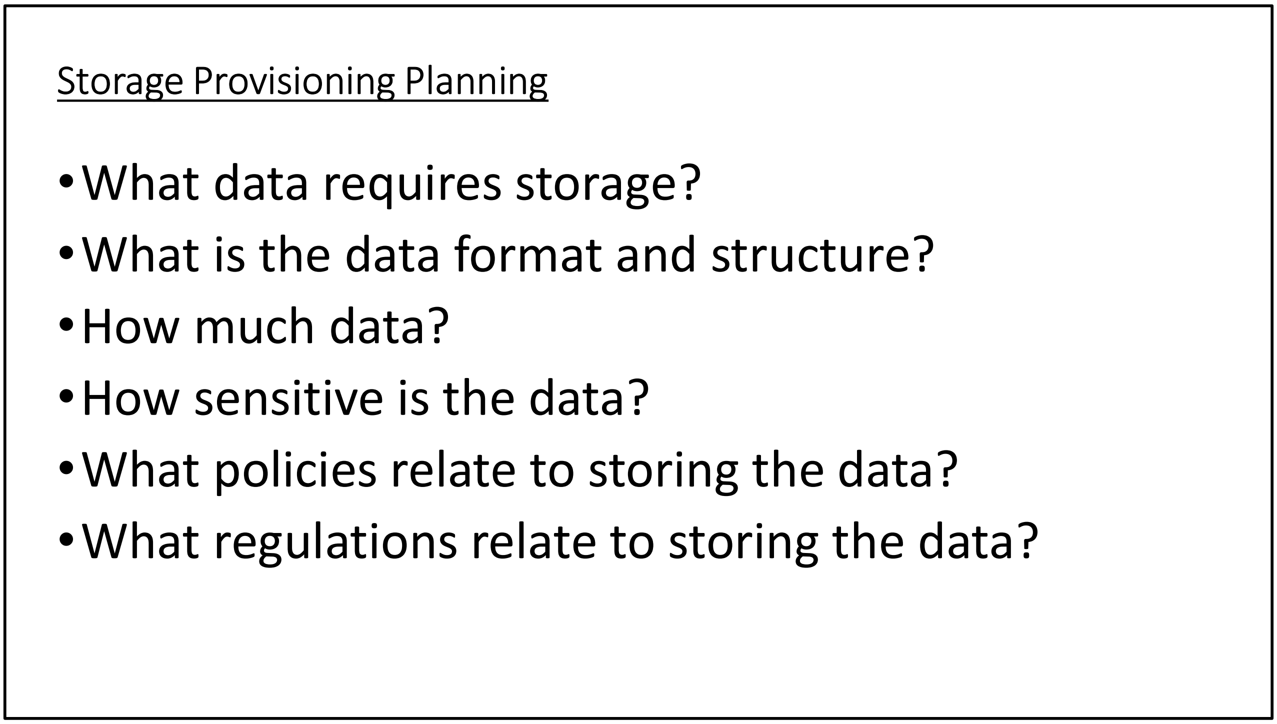
Object-Based Storage

- Object-based storage allows the storage of data as objects
  - Usually no file hierarchy
  - Not block-level
- Examples of object storage
  - S3 Buckets (AWS)
  - Azure Blobs (Azure)
  - Buckets (GCP)



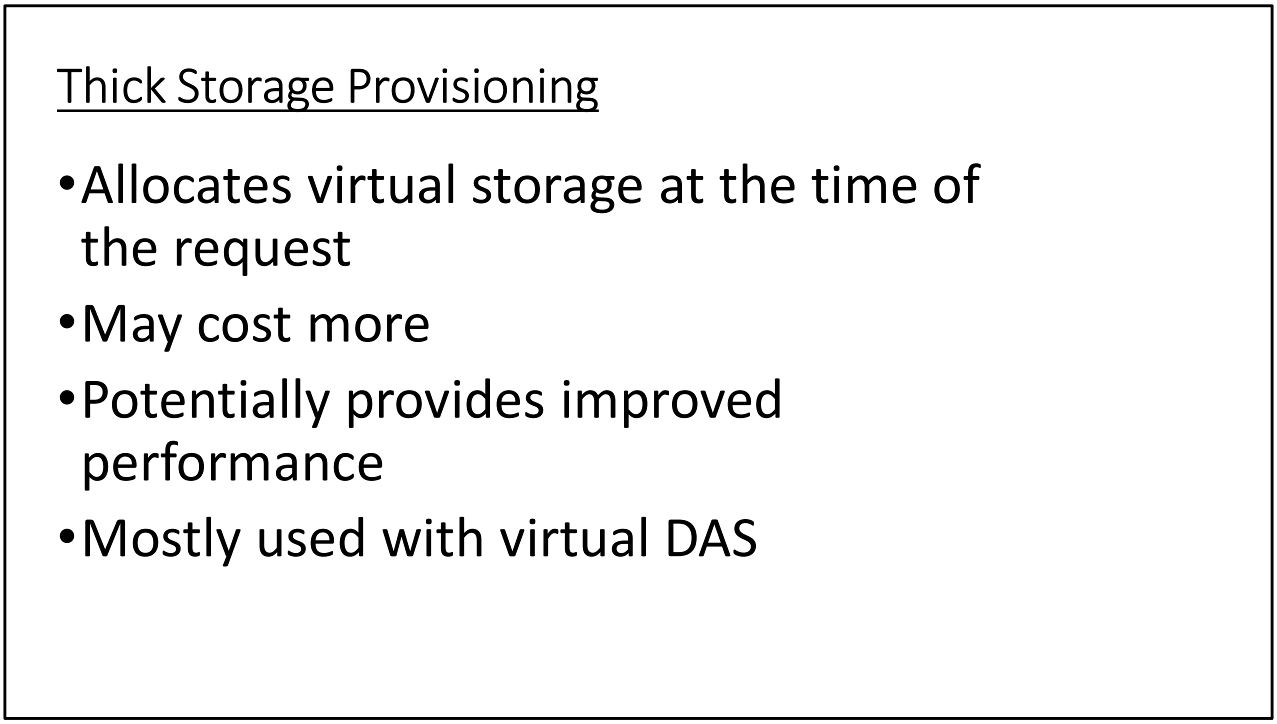
03.02 Provisioning Storage

CH03: Cloud Storage



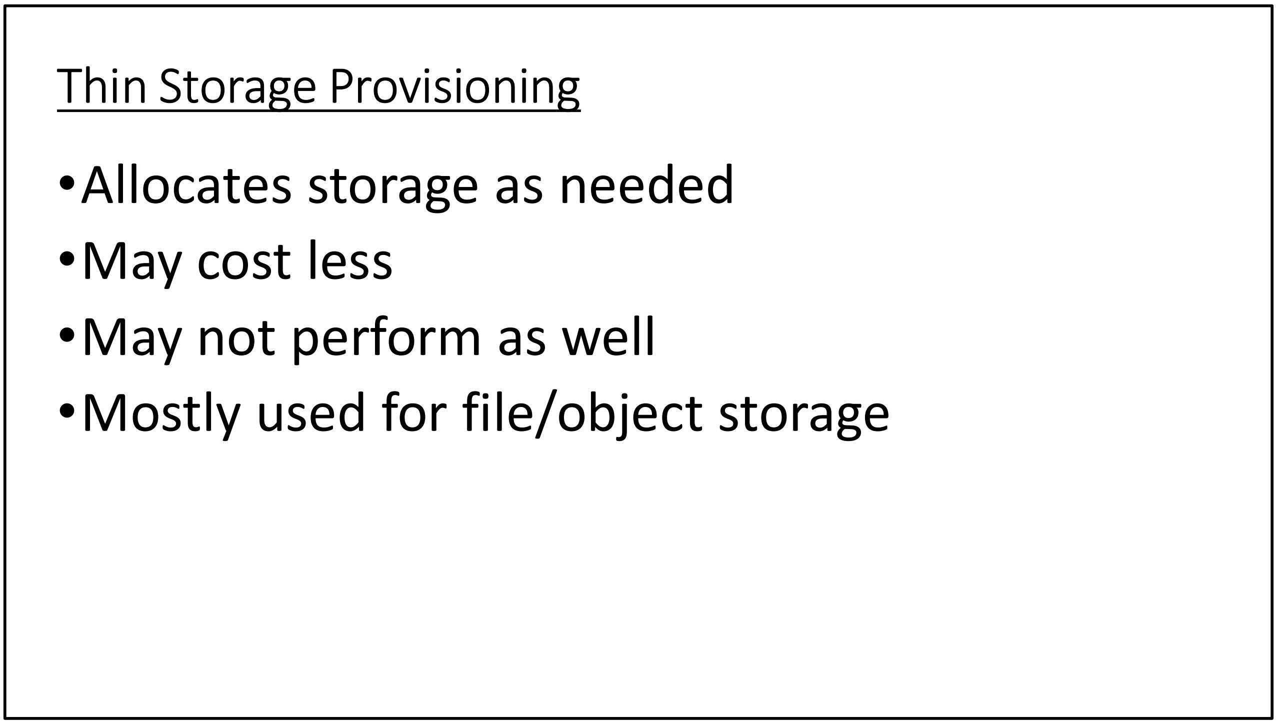
Storage Provisioning Planning

- What data requires storage?
- What is the data format and structure?
- How much data?
- How sensitive is the data?
- What policies relate to storing the data?
- What regulations relate to storing the data?



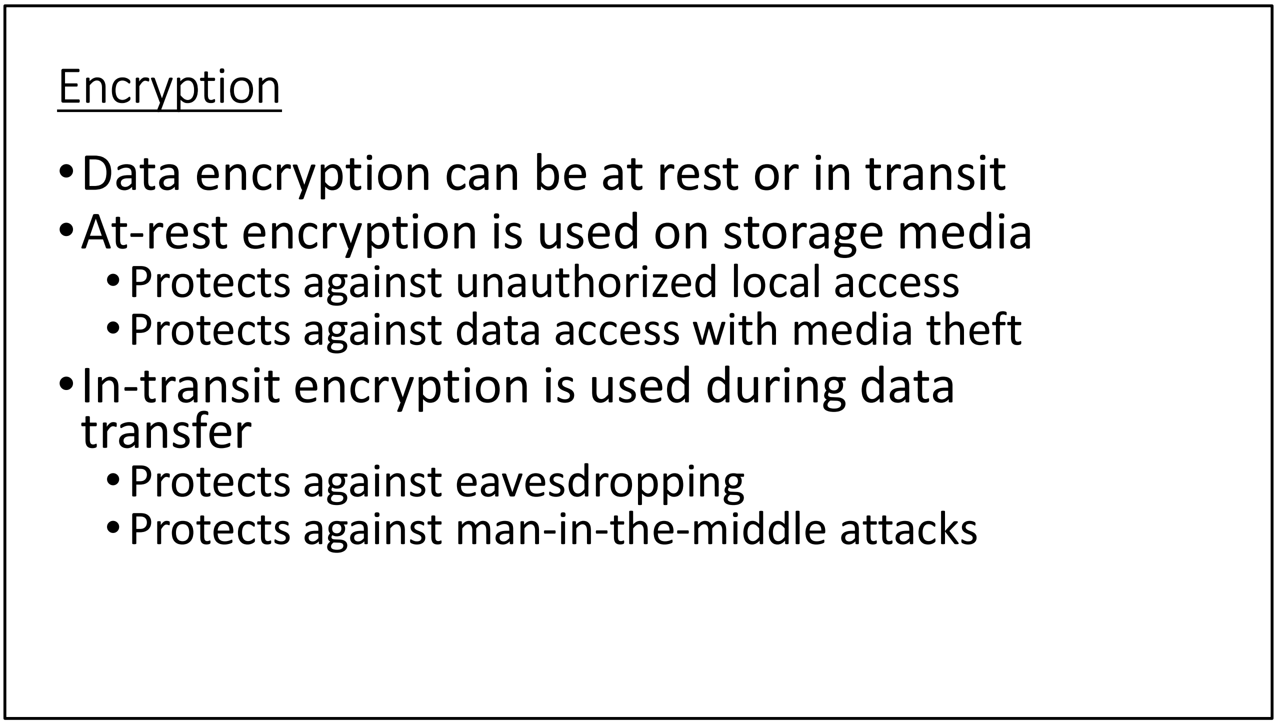
Thick Storage Provisioning

- Allocates virtual storage at the time of the request
- May cost more
- Potentially provides improved performance
- Mostly used with virtual DAS



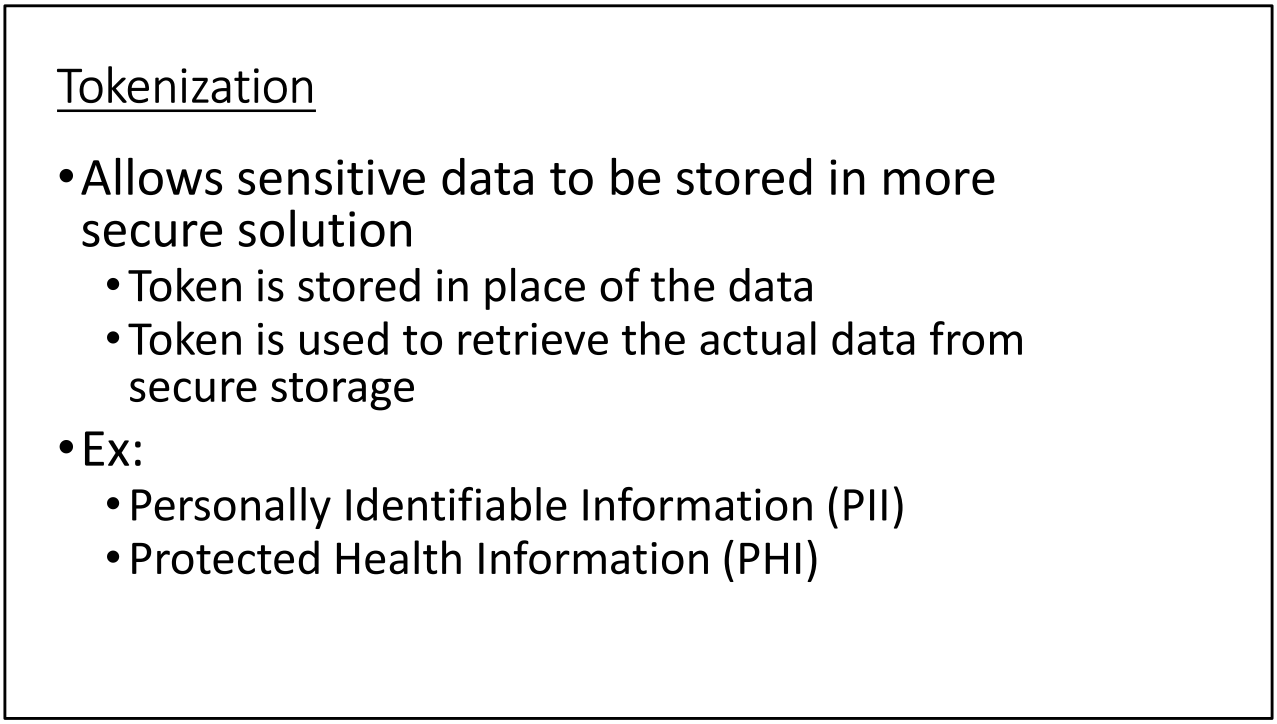
Thin Storage Provisioning

- Allocates storage as needed
- May cost less
- May not perform as well
- Mostly used for file/object storage



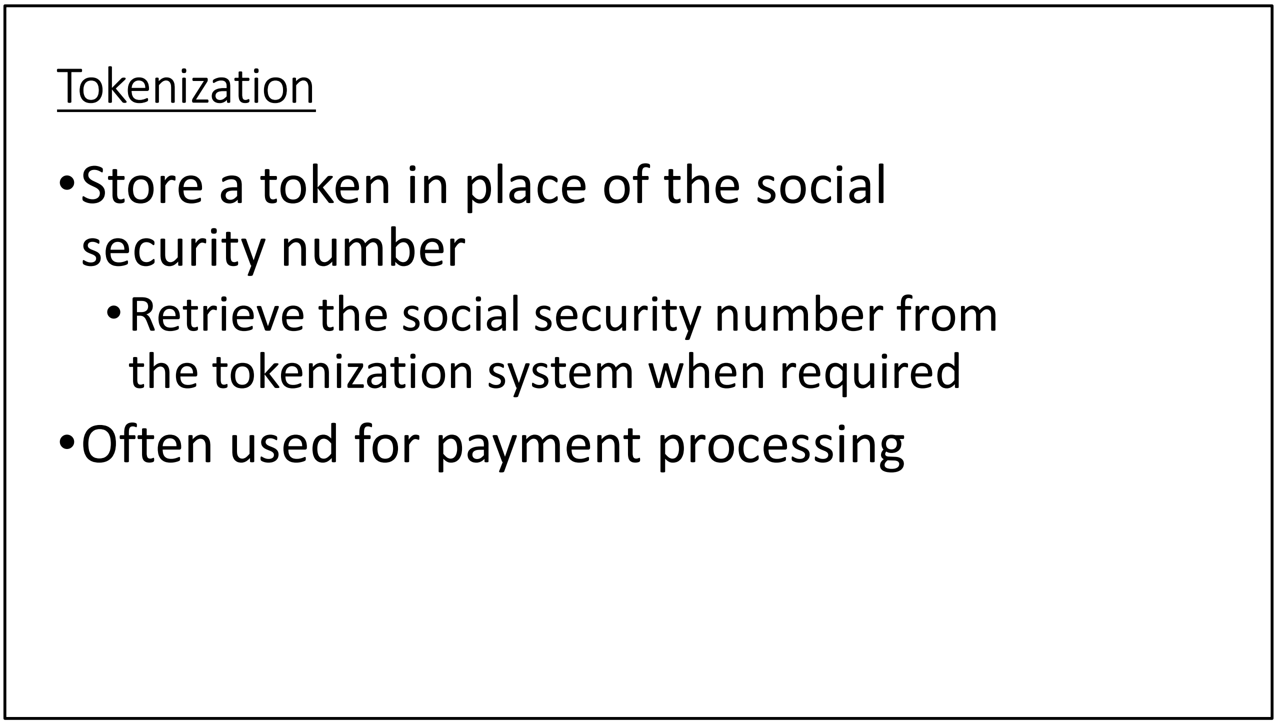
Encryption

- Data encryption can be at rest or in transit
- At-rest encryption is used on storage media
  - Protects against unauthorized local access
  - Protects against data access with media theft
- In-transit encryption is used during data transfer
  - Protects against eavesdropping
  - Protects against man-in-the-middle attacks



Tokenization

- Allows sensitive data to be stored in more secure solution
  - Token is stored in place of the data
  - Token is used to retrieve the actual data from secure storage
- Ex:
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)

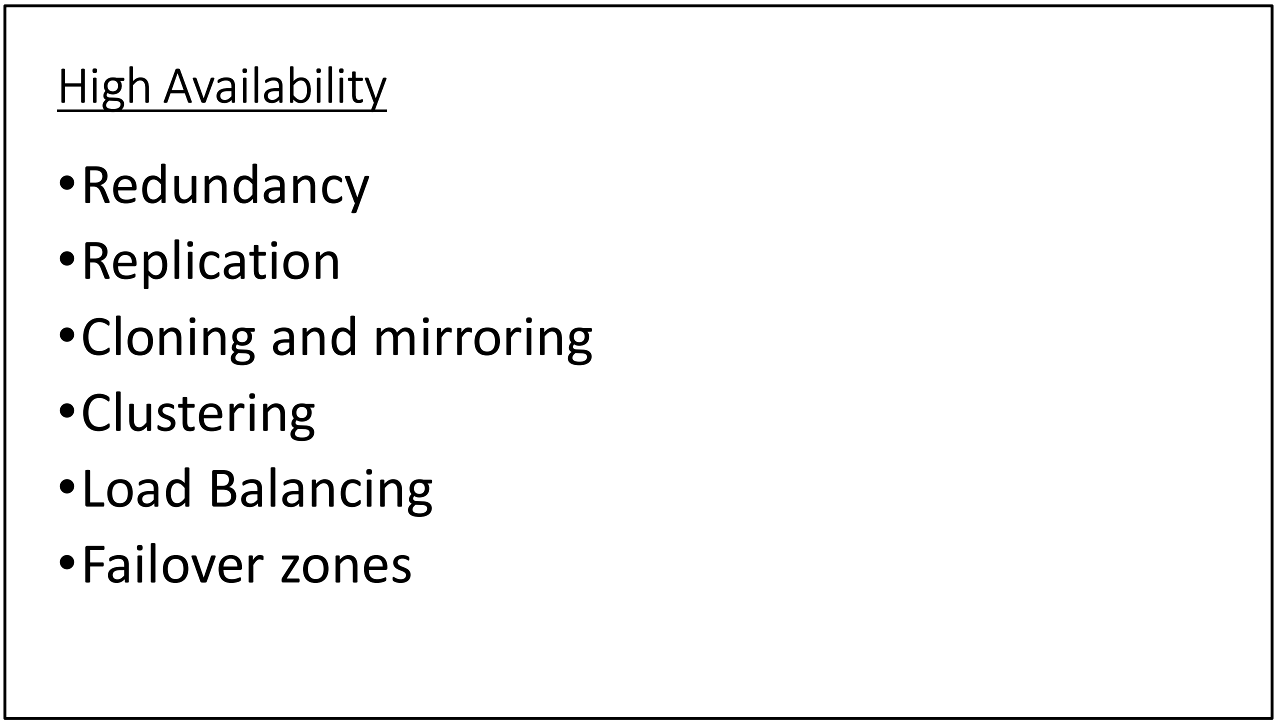


Tokenization

- Store a token in place of the social security number
  - Retrieve the social security number from the tokenization system when required
- Often used for payment processing

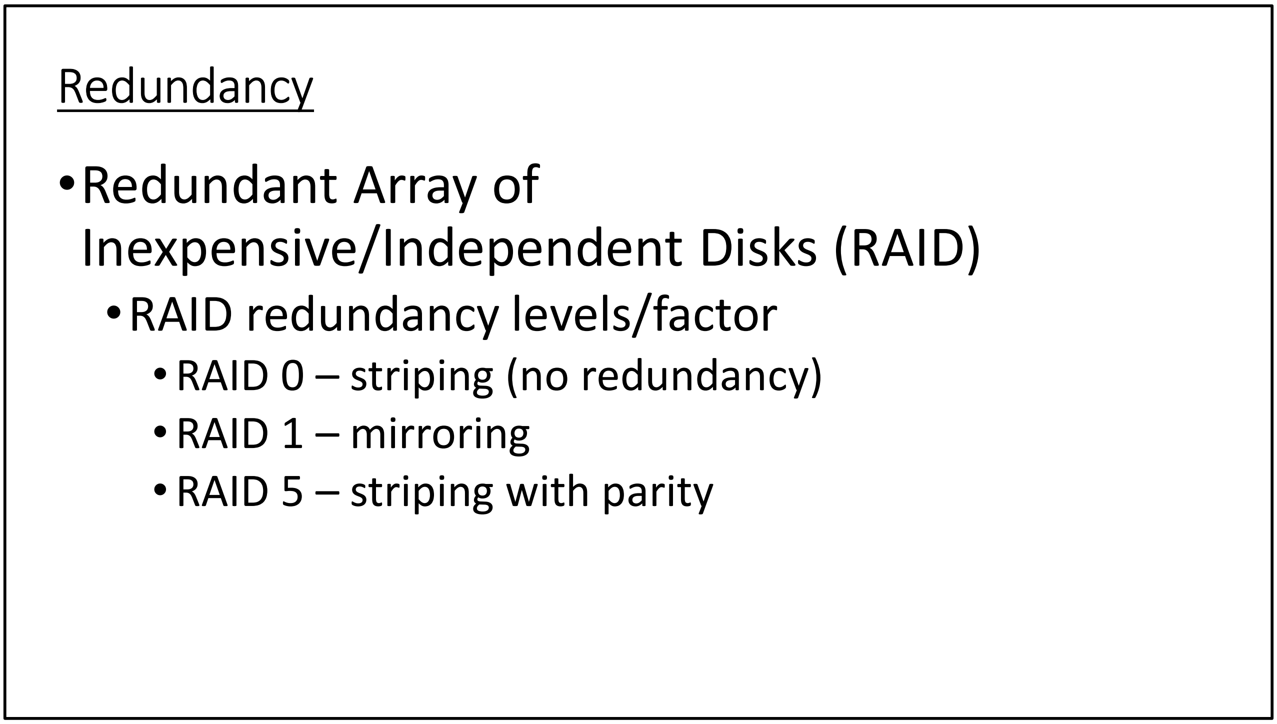
3.03 Storage Protection Capabilities

CH03: Cloud Storage



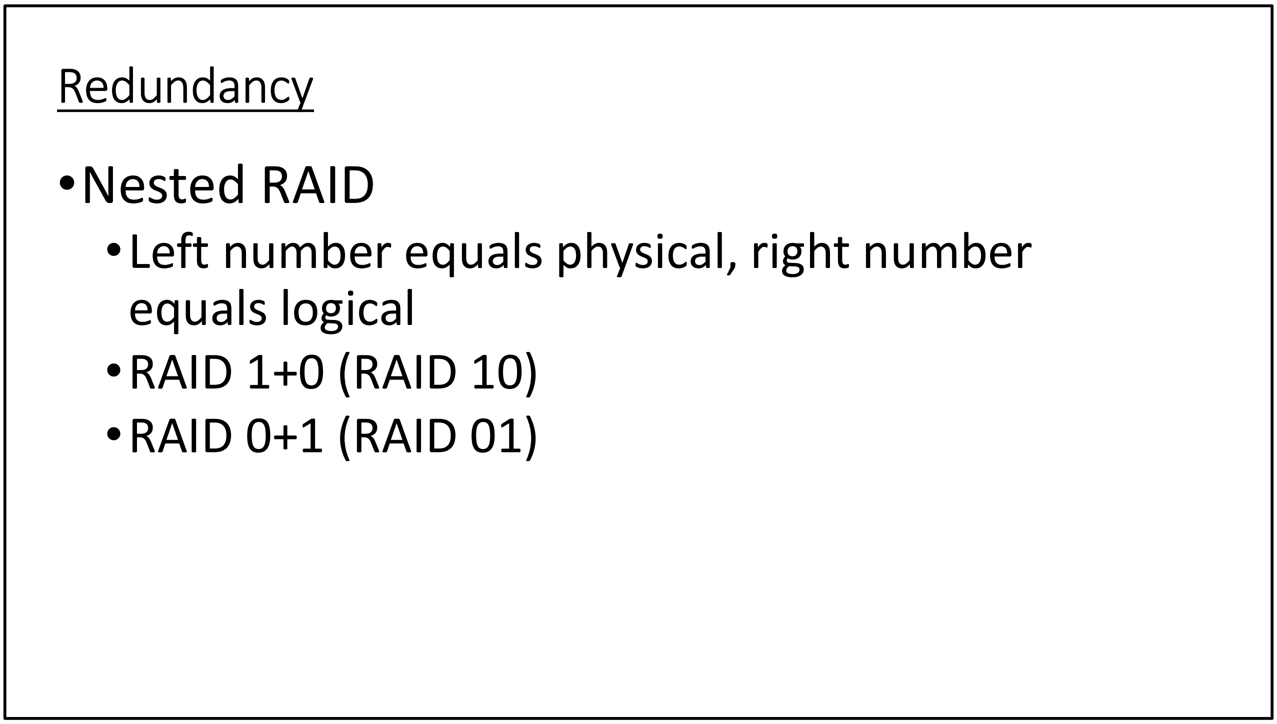
High Availability

- Redundancy
- Replication
- Cloning and mirroring
- Clustering
- Load Balancing
- Failover zones



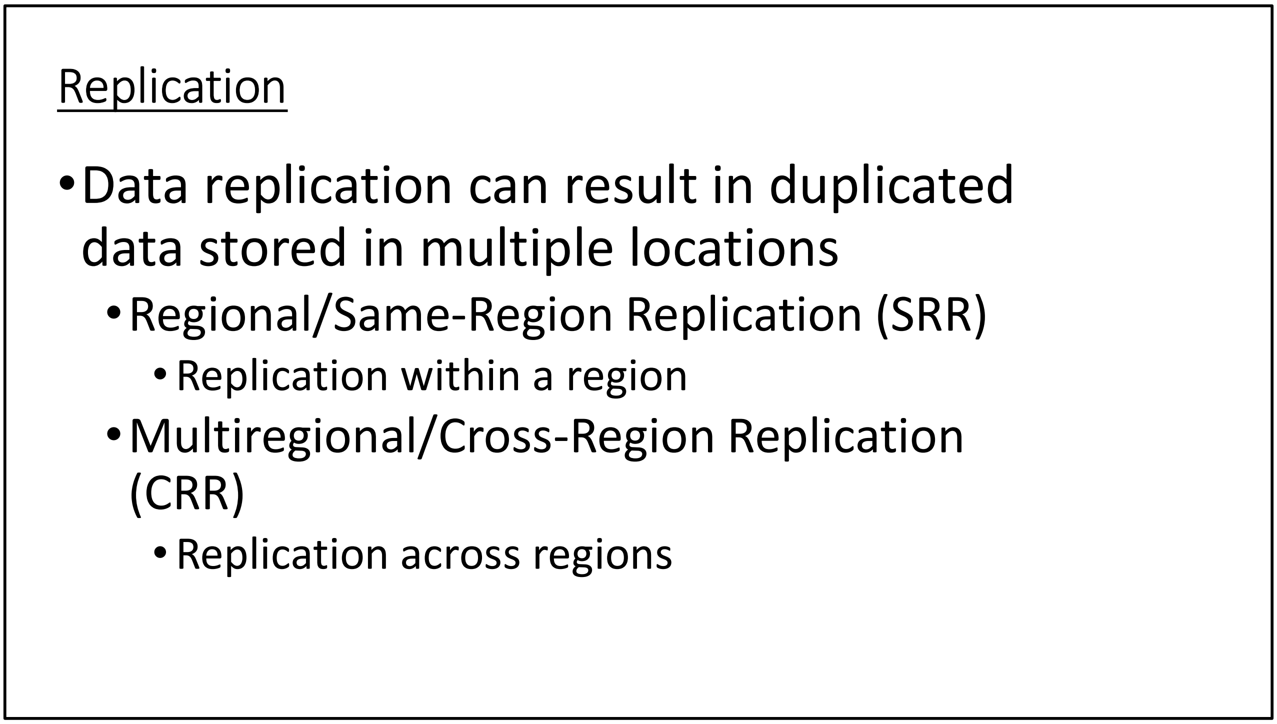
Redundancy

- Redundant Array of Inexpensive/Independent Disks (RAID)
  - RAID redundancy levels/factor
    - RAID 0 – striping (no redundancy)
    - RAID 1 – mirroring
    - RAID 5 – striping with parity



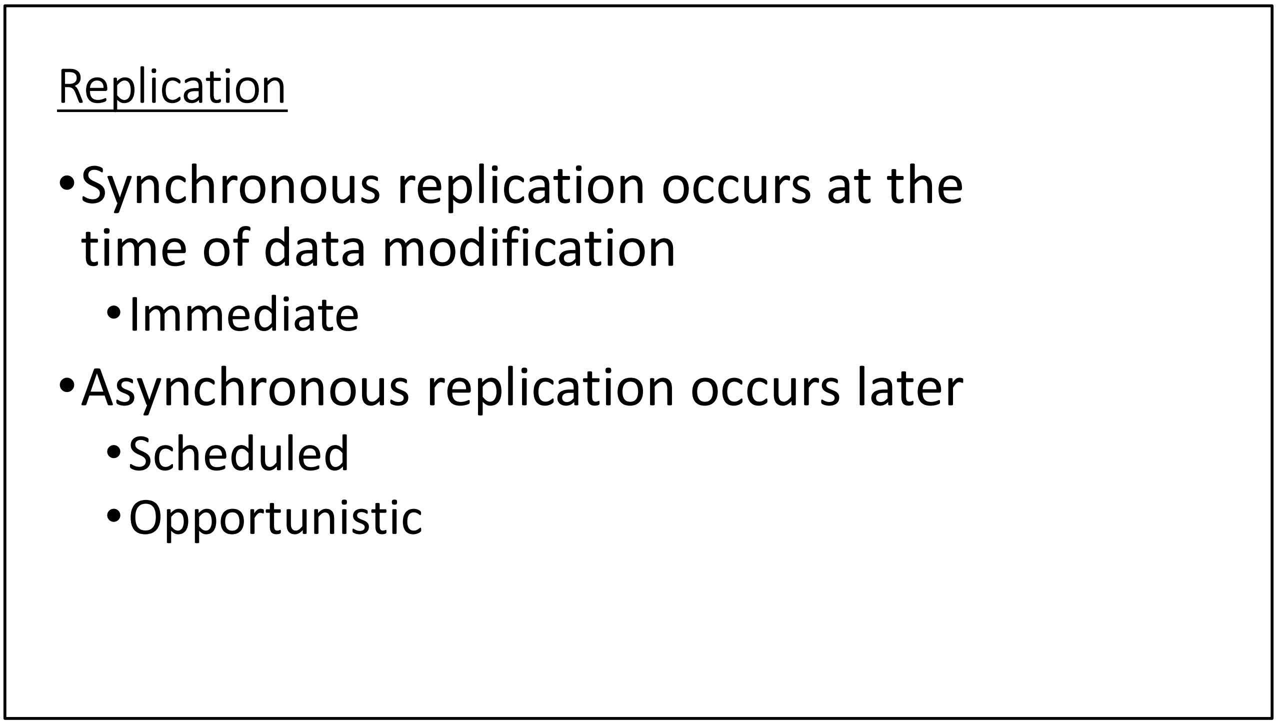
Redundancy

- Nested RAID
  - Left number equals physical, right number equals logical
  - RAID 1+0 (RAID 10)
  - RAID 0+1 (RAID 01)



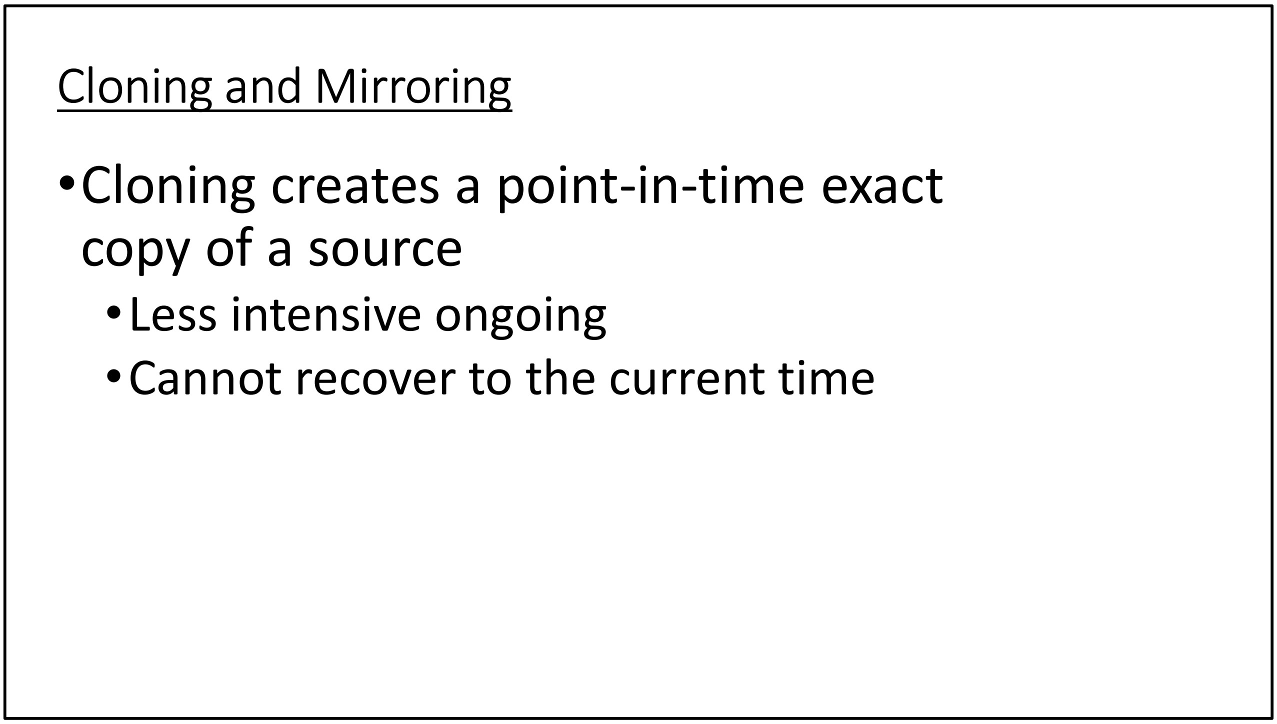
Replication

- Data replication can result in duplicated data stored in multiple locations
  - Regional/Same-Region Replication (SRR)
    - Replication within a region
  - Multiregional/Cross-Region Replication (CRR)
    - Replication across regions



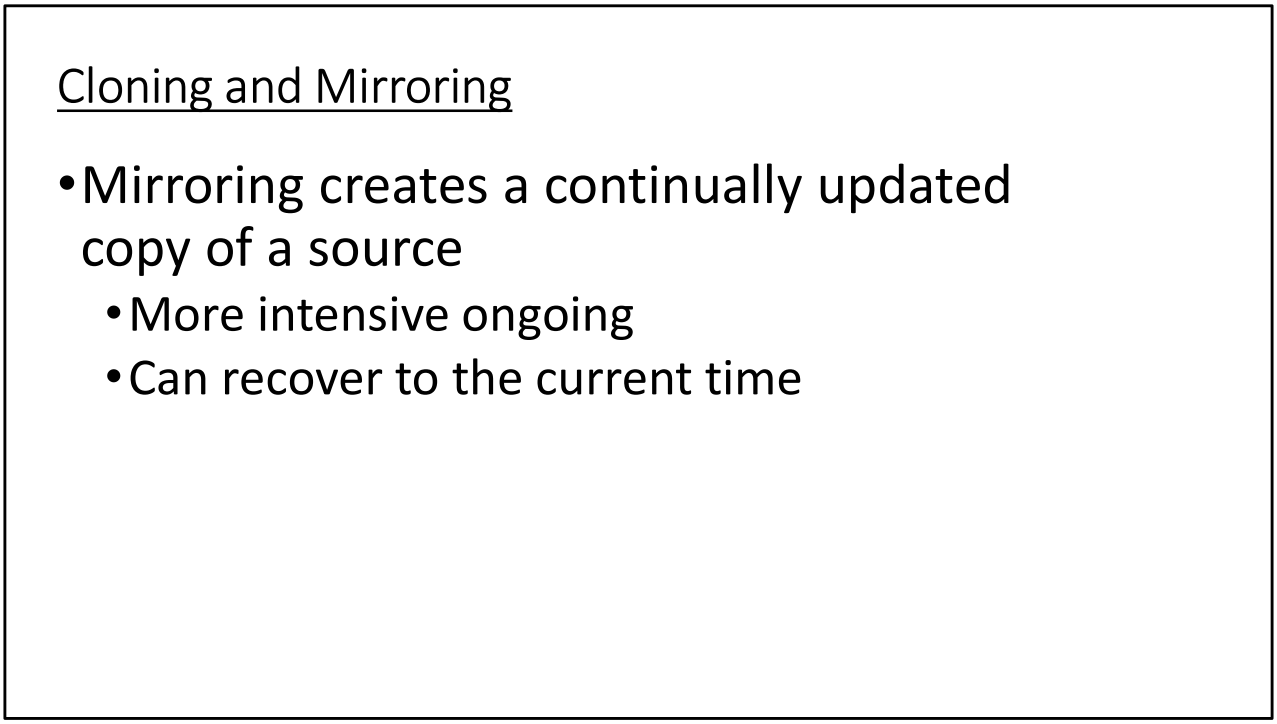
Replication

- Synchronous replication occurs at the time of data modification
  - Immediate
- Asynchronous replication occurs later
  - Scheduled
  - Opportunistic



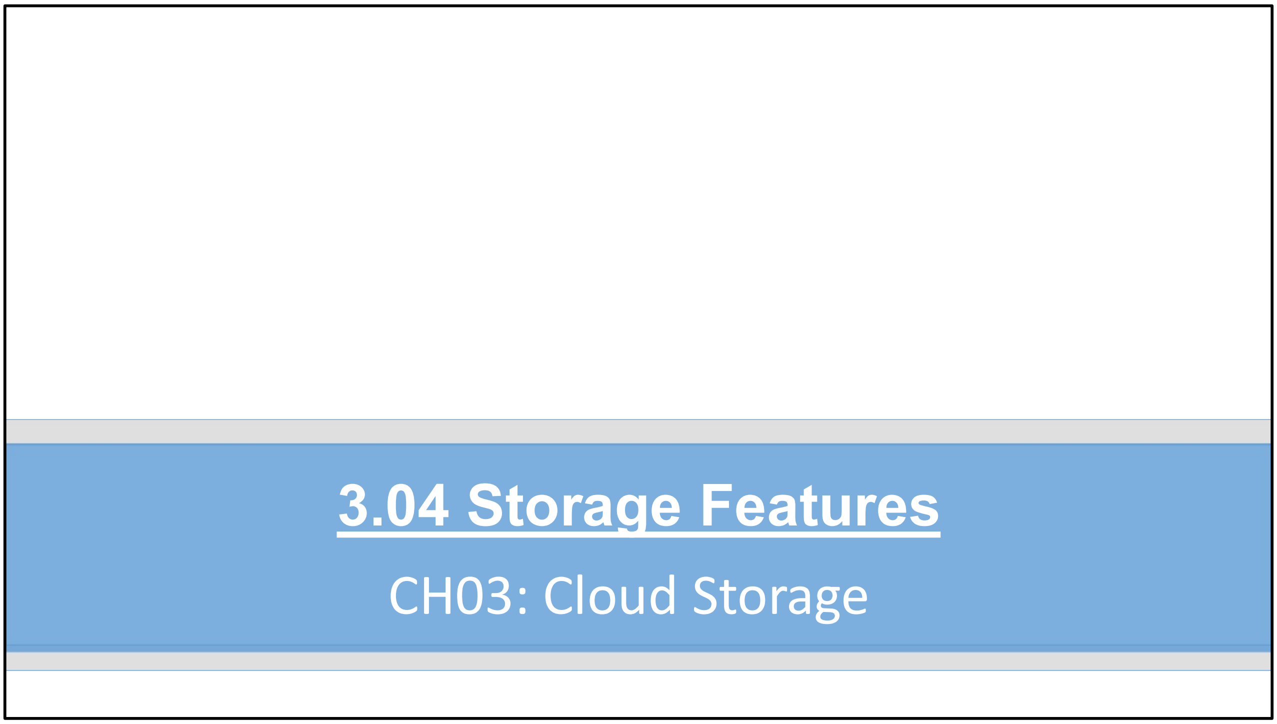
Cloning and Mirroring

- Cloning creates a point-in-time exact copy of a source
  - Less intensive ongoing
  - Cannot recover to the current time



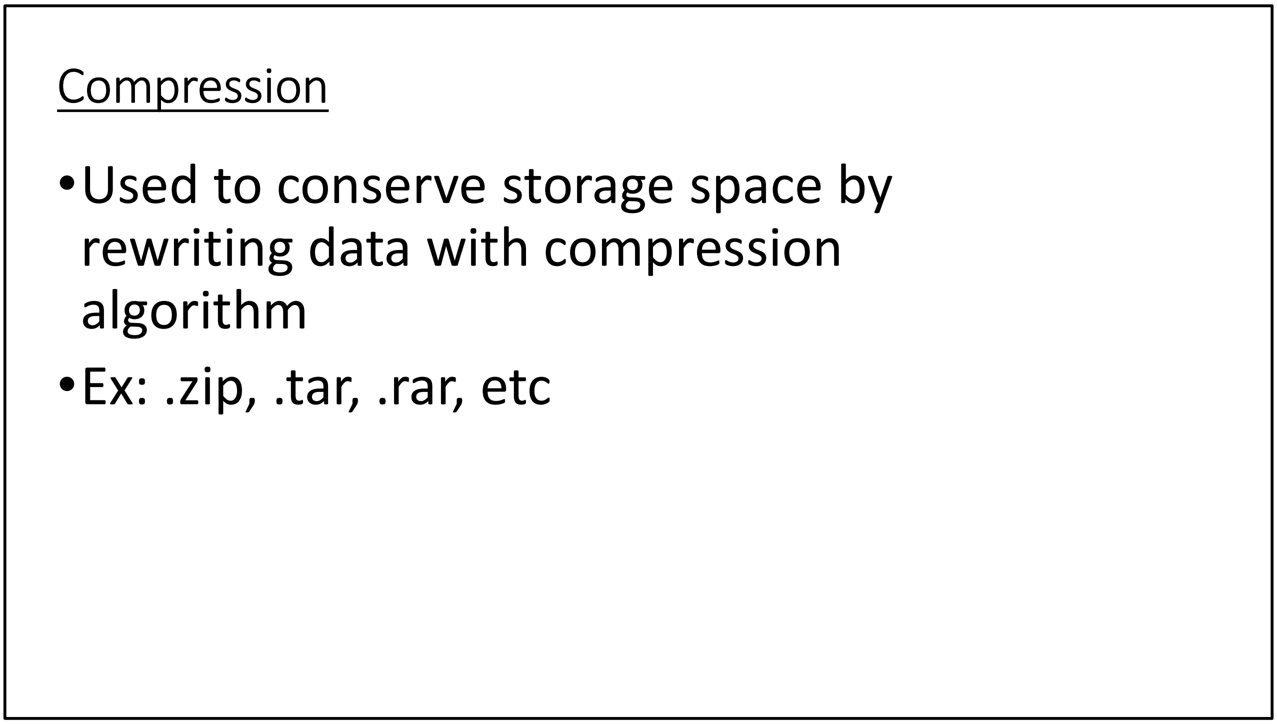
Cloning and Mirroring

- Mirroring creates a continually updated copy of a source
  - More intensive ongoing
  - Can recover to the current time



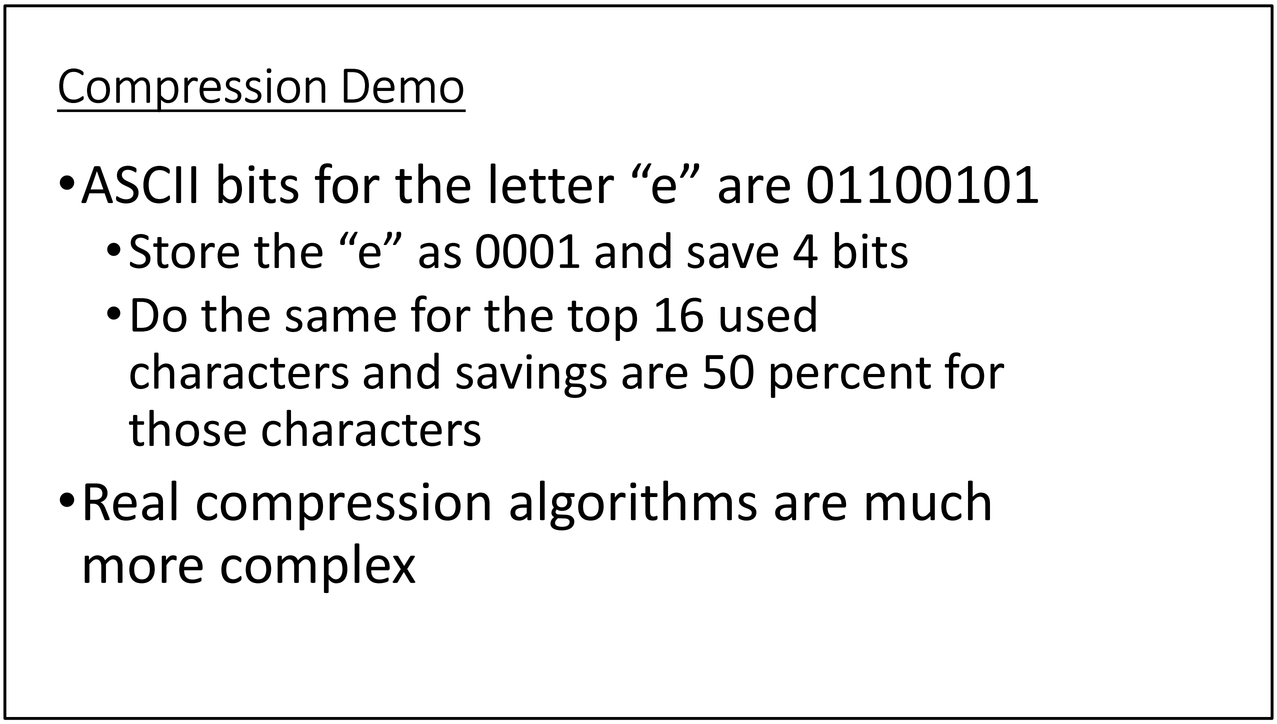
3.04 Storage Features

CH03: Cloud Storage



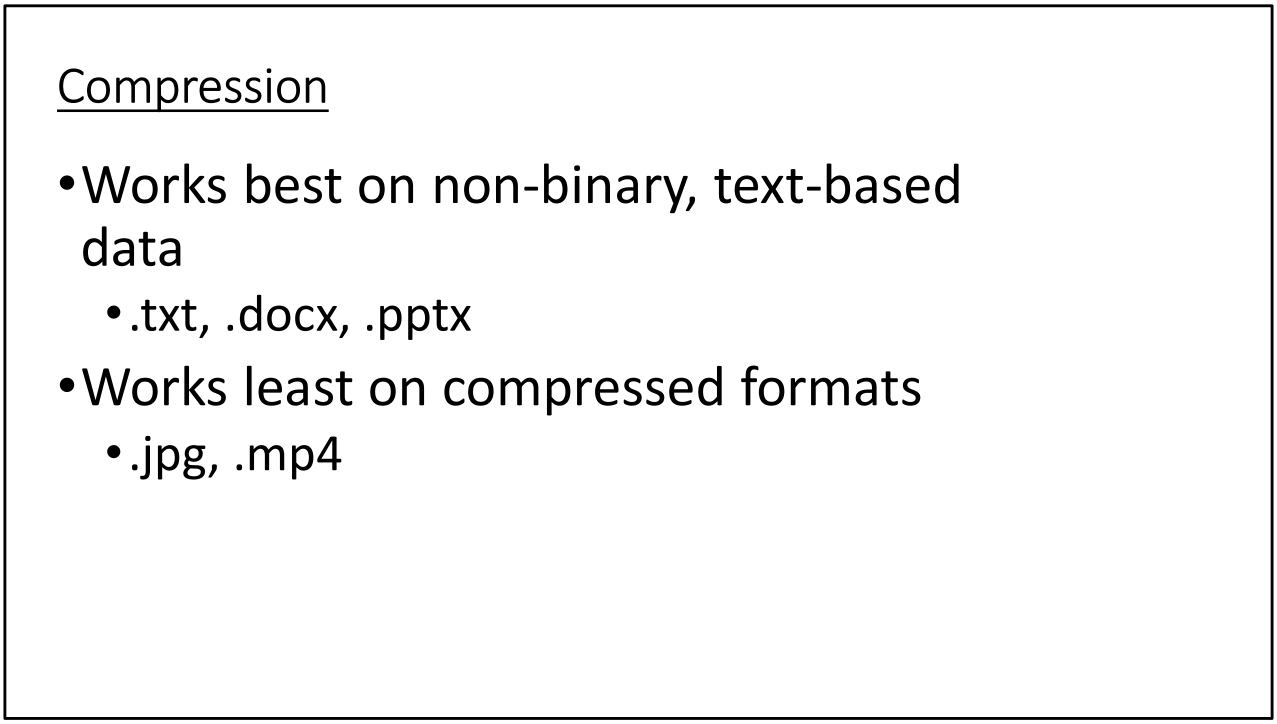
Compression

- Used to conserve storage space by rewriting data with compression algorithm
- Ex: .zip, .tar, .rar, etc



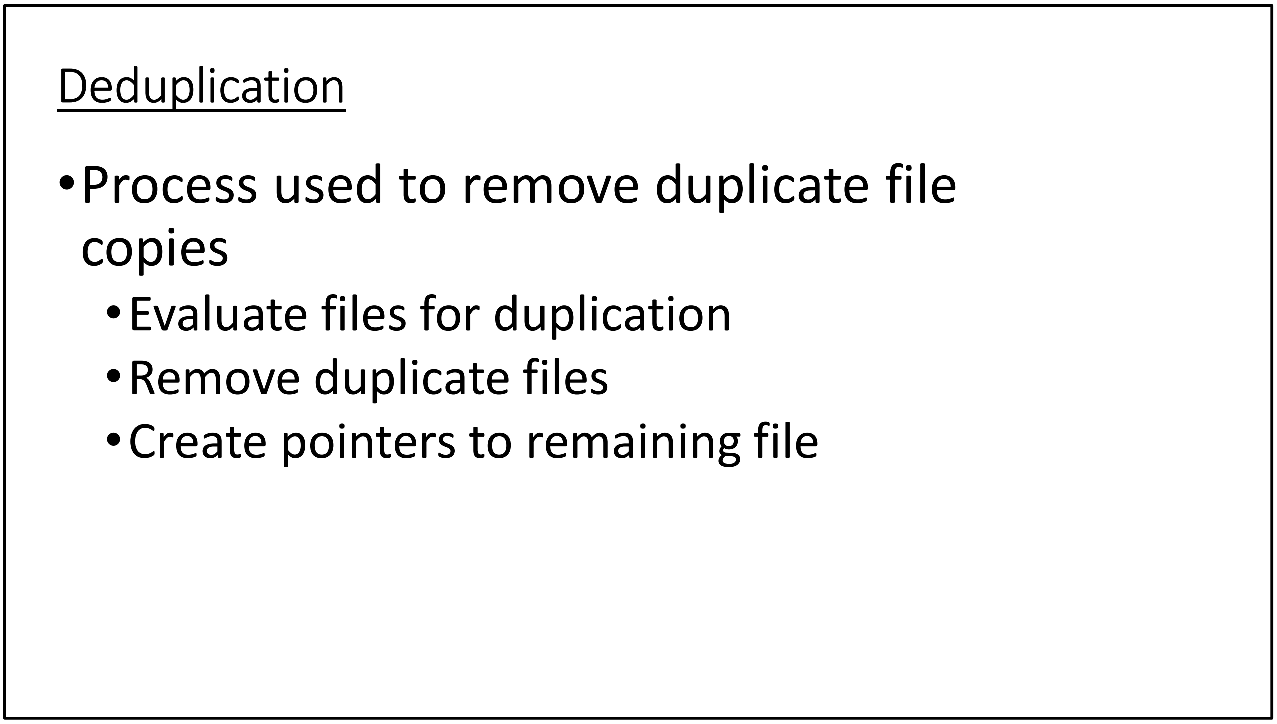
Compression Demo

- ASCII bits for the letter “e” are 01100101
  - Store the “e” as 0001 and save 4 bits
  - Do the same for the top 16 used characters and savings are 50 percent for those characters
- Real compression algorithms are much more complex



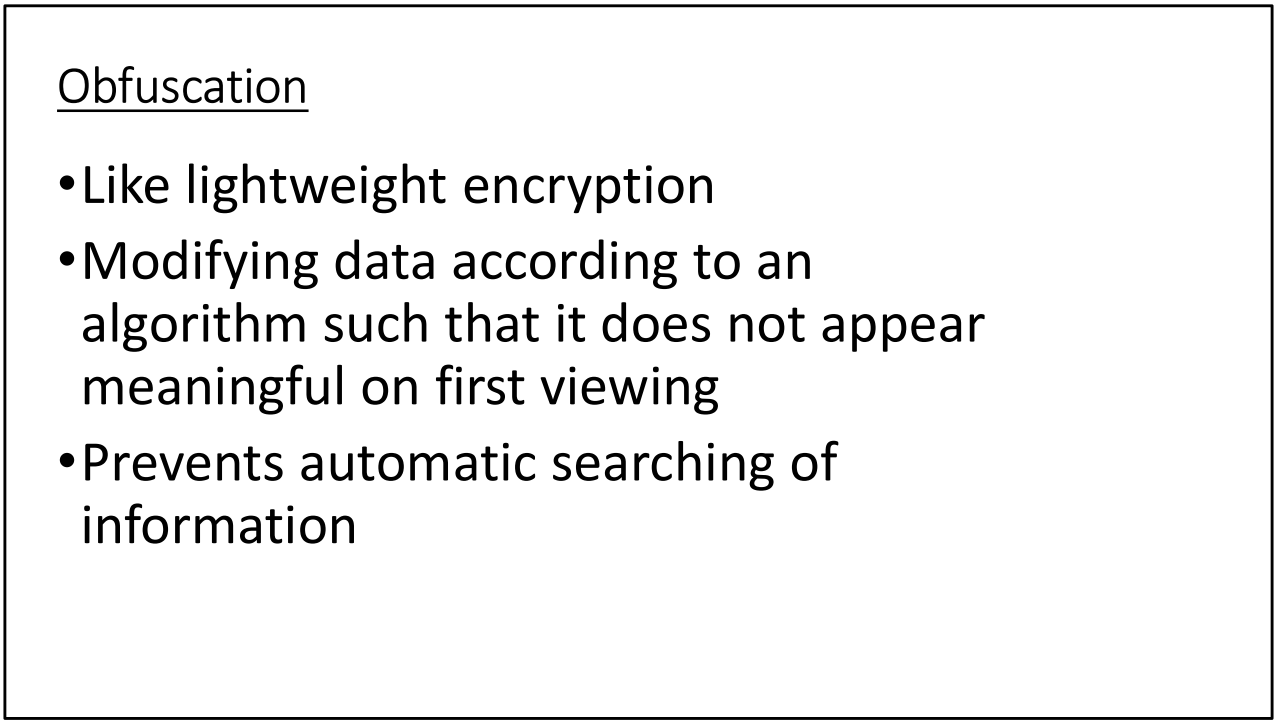
Compression

- Works best on non-binary, text-based data
  - .txt, .docx, .pptx
- Works least on compressed formats
  - .jpg, .mp4



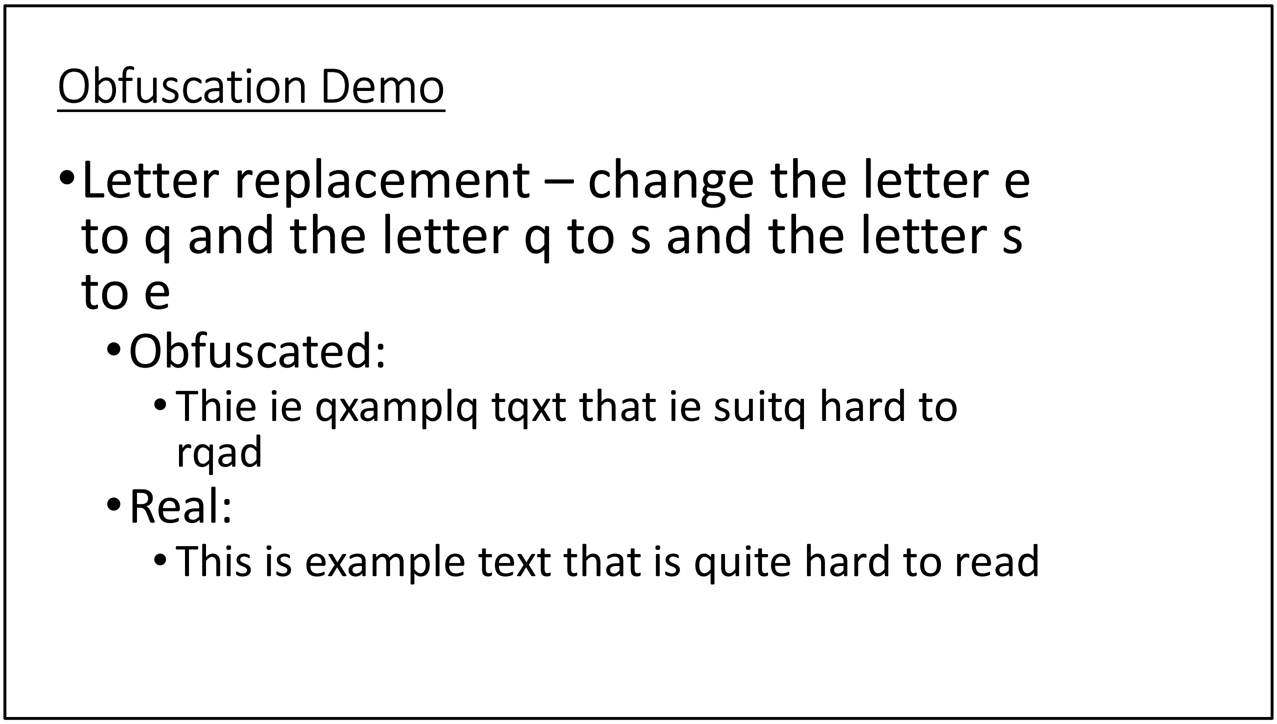
Deduplication

- Process used to remove duplicate file copies
  - Evaluate files for duplication
  - Remove duplicate files
  - Create pointers to remaining file



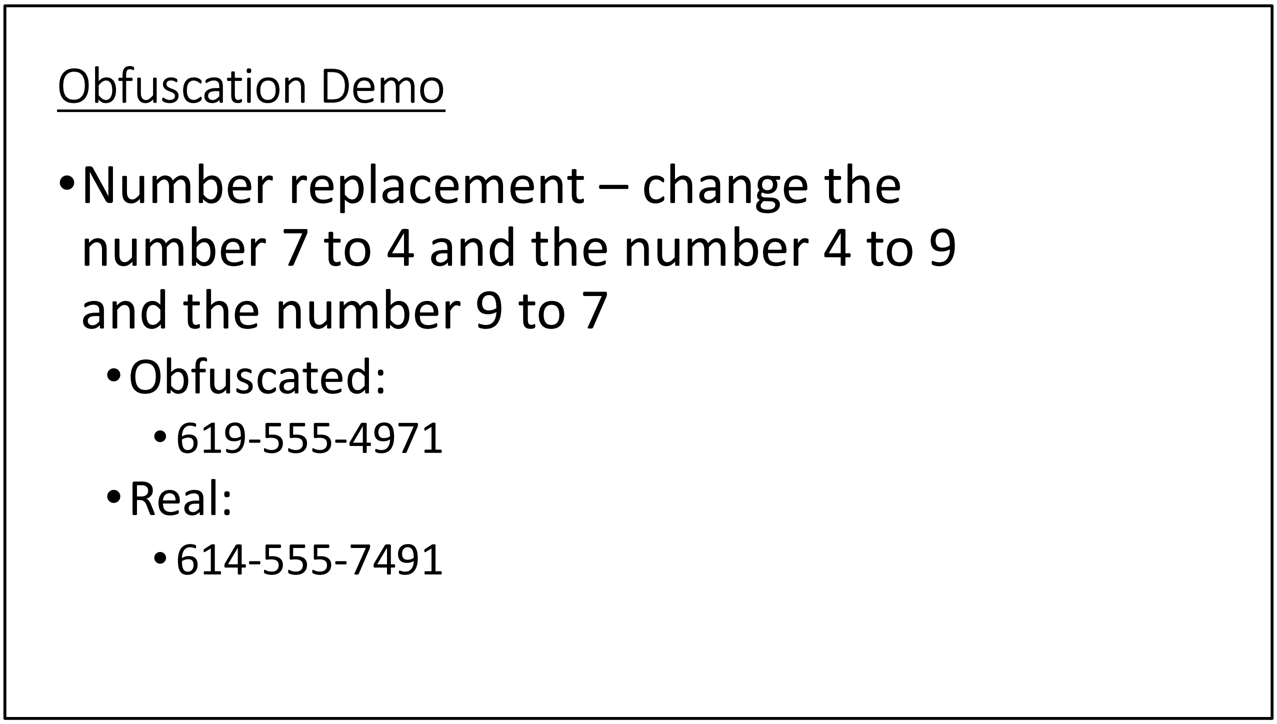
Obfuscation

- Like lightweight encryption
- Modifying data according to an algorithm such that it does not appear meaningful on first viewing
- Prevents automatic searching of information



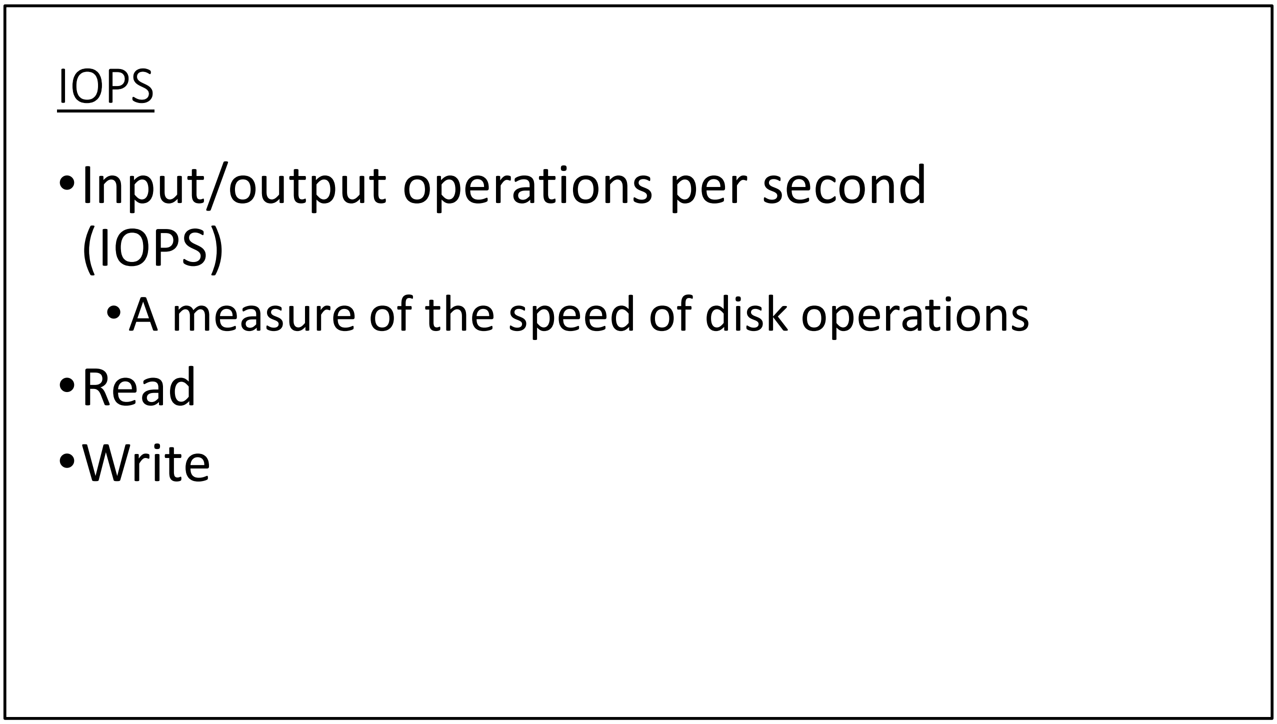
Obfuscation Demo

- Letter replacement – change the letter e to q and the letter q to s and the letter s to e
  - Obfuscated:
    - Thie ie qxamplq tqxt that ie suitq hard to rqad
  - Real:
    - This is example text that is quite hard to read



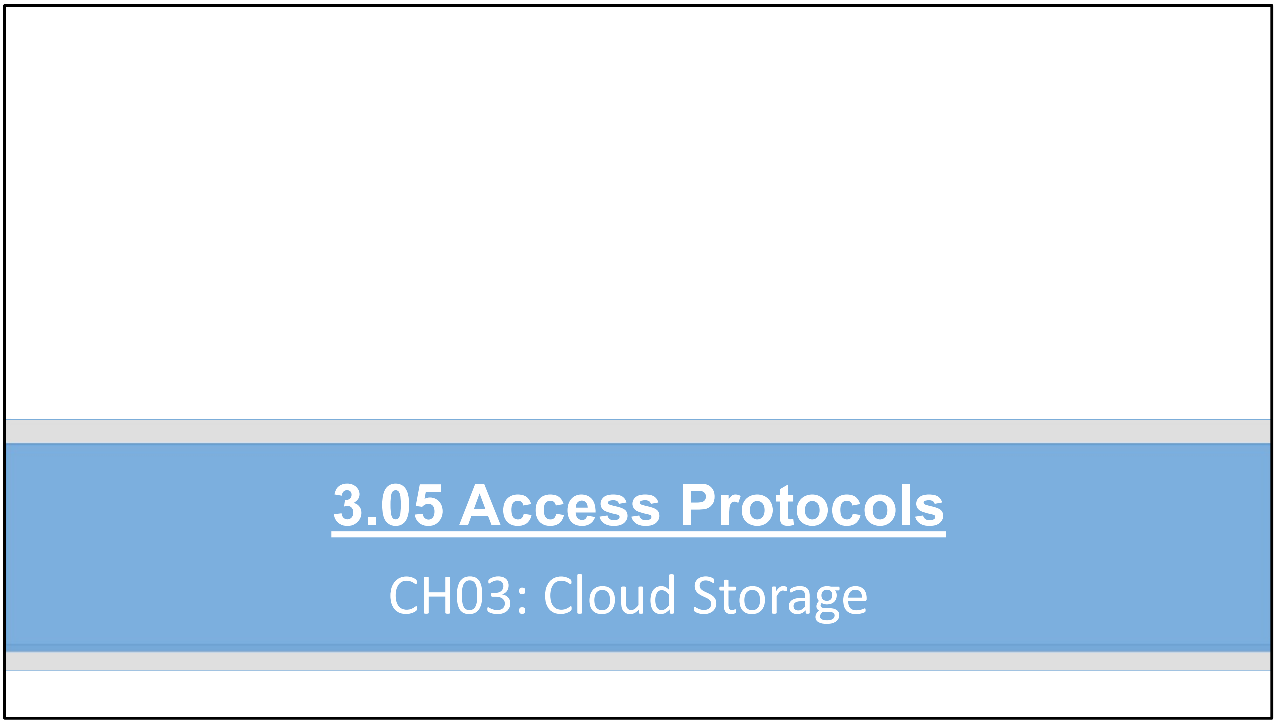
Obfuscation Demo

- Number replacement – change the number 7 to 4 and the number 4 to 9 and the number 9 to 7
  - Obfuscated:
    - 619-555-4971
  - Real:
    - 614-555-7491



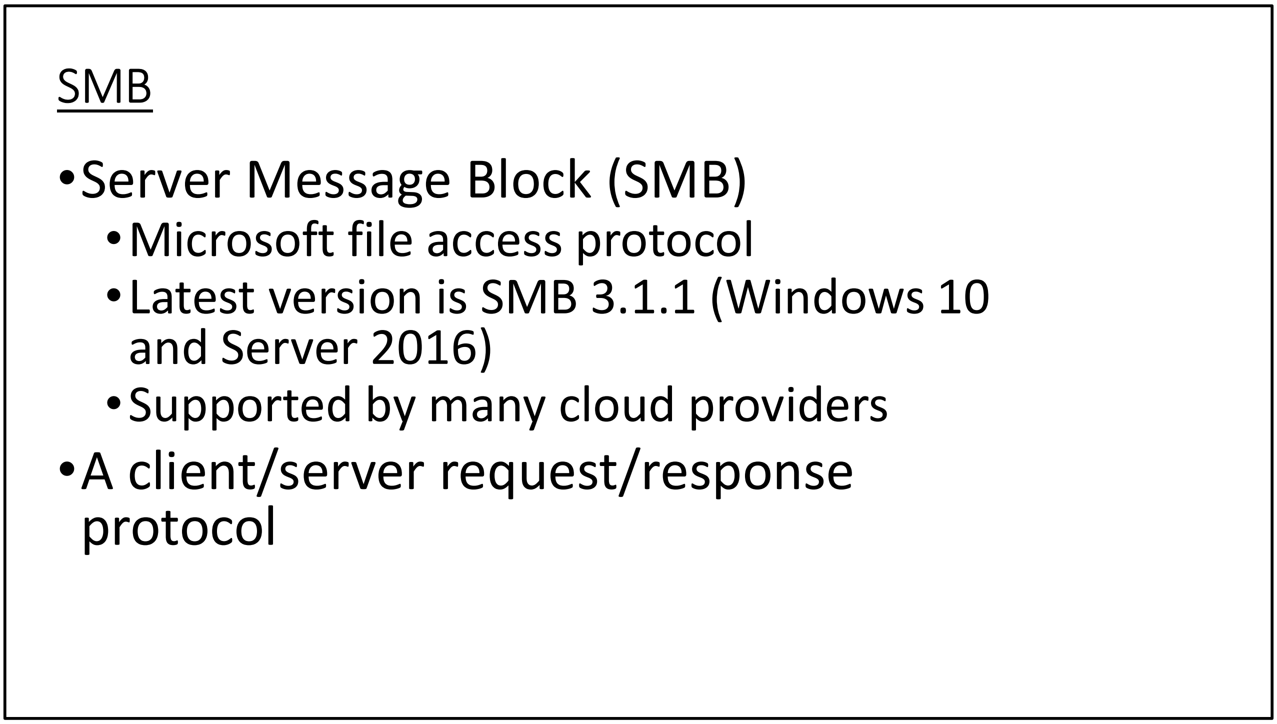
IOPS

- Input/output operations per second (IOPS)
  - A measure of the speed of disk operations
- Read
- Write



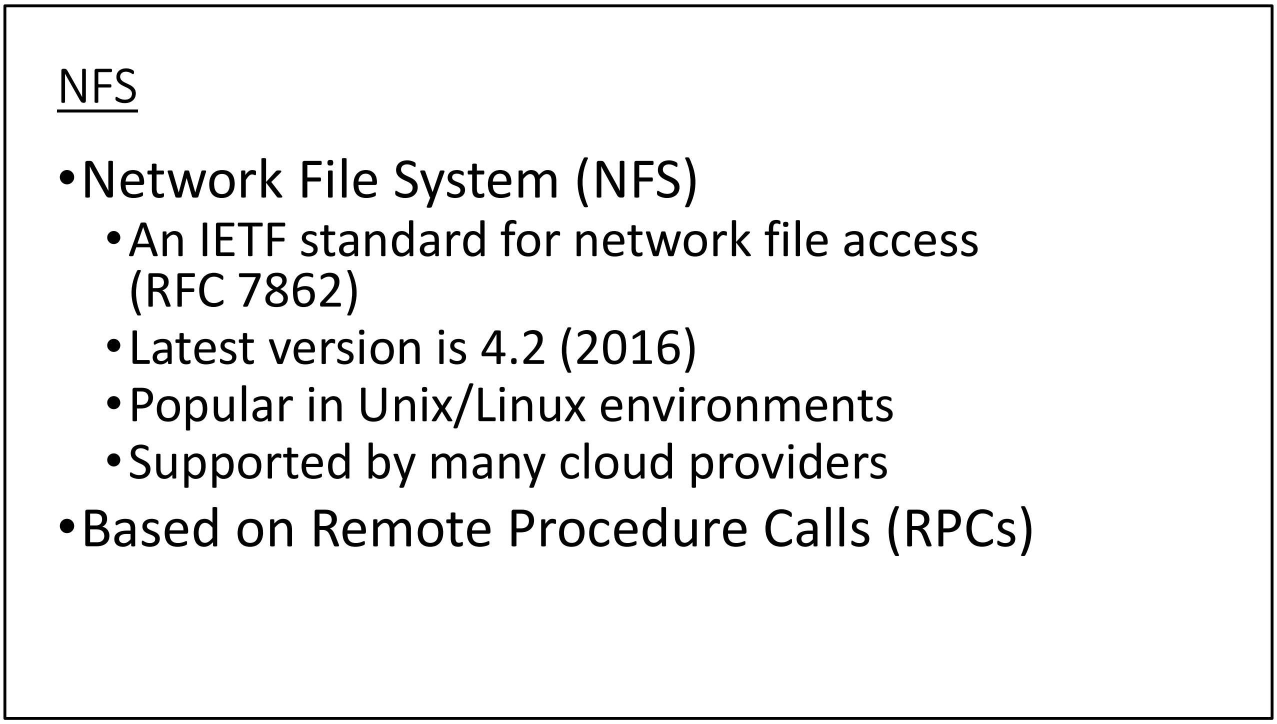
3.05 Access Protocols

CH03: Cloud Storage



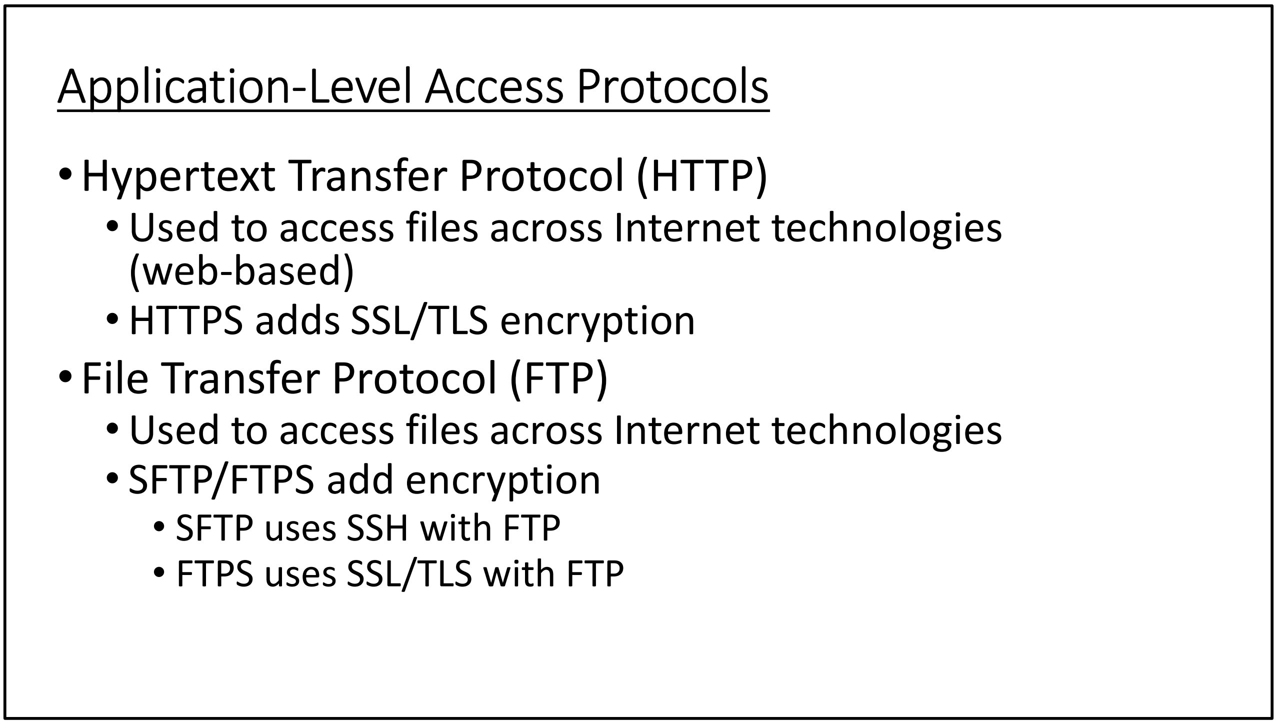
SMB

- Server Message Block (SMB)
  - Microsoft file access protocol
  - Latest version is SMB 3.1.1 (Windows 10 and Server 2016)
  - Supported by many cloud providers
- A client/server request/response protocol



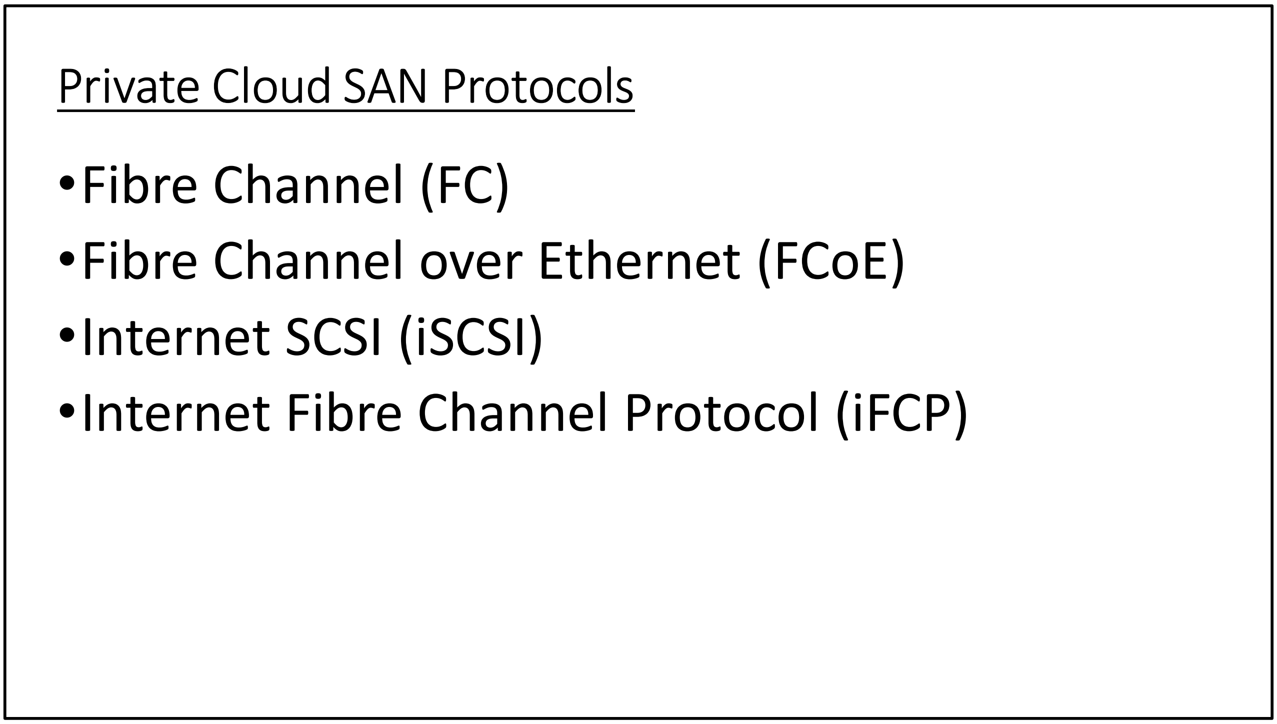
NFS

- Network File System (NFS)
  - An IETF standard for network file access (RFC 7862)
  - Latest version is 4.2 (2016)
  - Popular in Unix/Linux environments
  - Supported by many cloud providers
- Based on Remote Procedure Calls (RPCs)



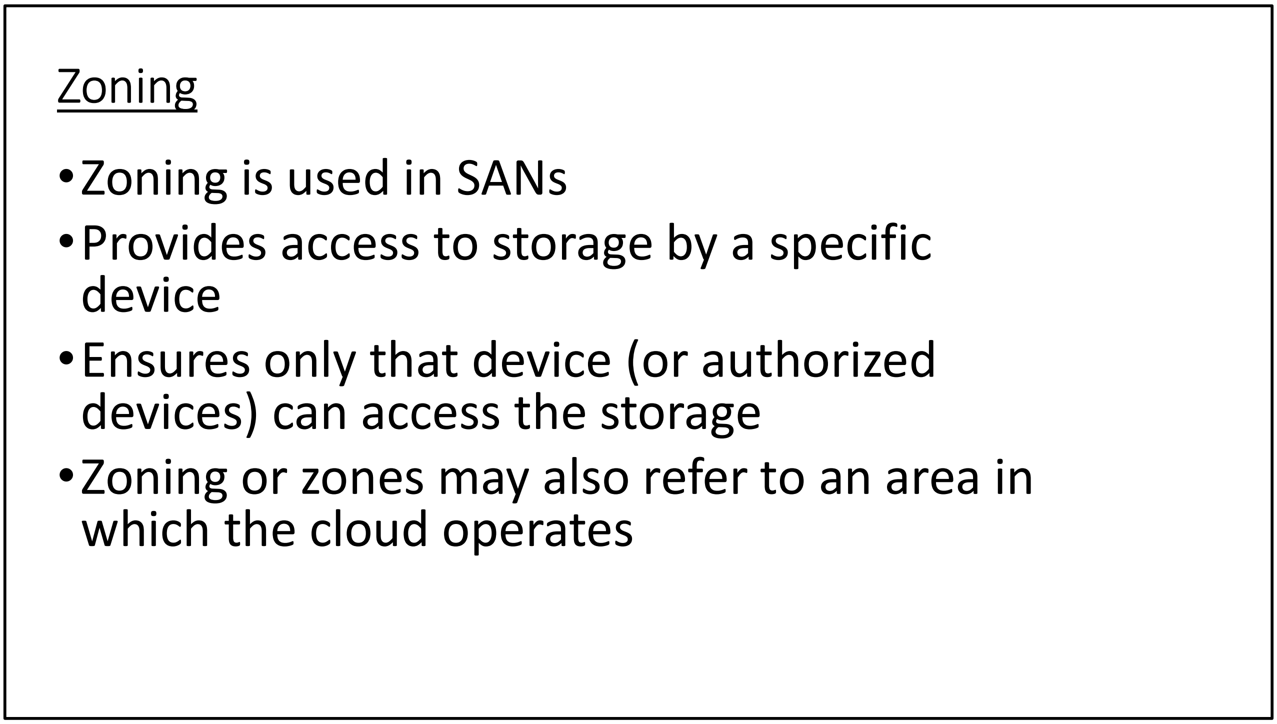
Application-Level Access Protocols

- Hypertext Transfer Protocol (HTTP)
  - Used to access files across Internet technologies (web-based)
  - HTTPS adds SSL/TLS encryption
- File Transfer Protocol (FTP)
  - Used to access files across Internet technologies
  - SFTP/FTPS add encryption
    - SFTP uses SSH with FTP
    - FTPS uses SSL/TLS with FTP



Private Cloud SAN Protocols

- Fibre Channel (FC)
- Fibre Channel over Ethernet (FCoE)
- Internet SCSI (iSCSI)
- Internet Fibre Channel Protocol (iFCP)

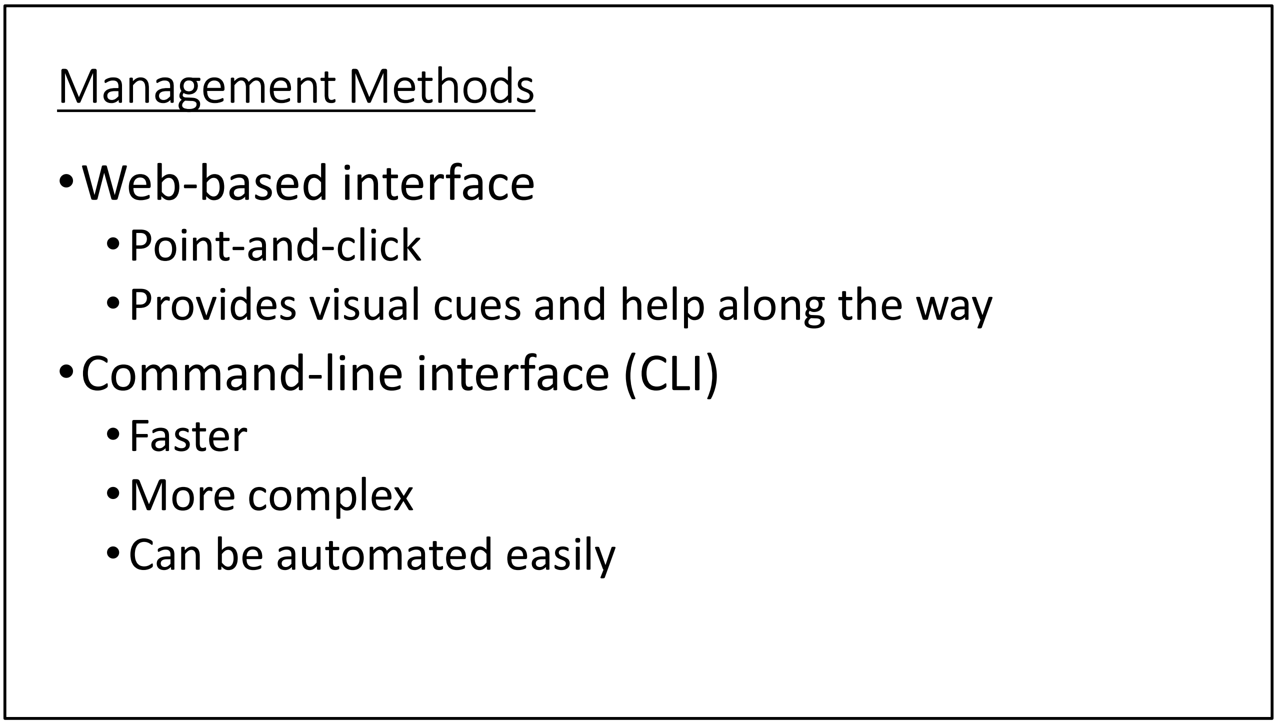


Zoning

- Zoning is used in SANs
- Provides access to storage by a specific device
- Ensures only that device (or authorized devices) can access the storage
- Zoning or zones may also refer to an area in which the cloud operates

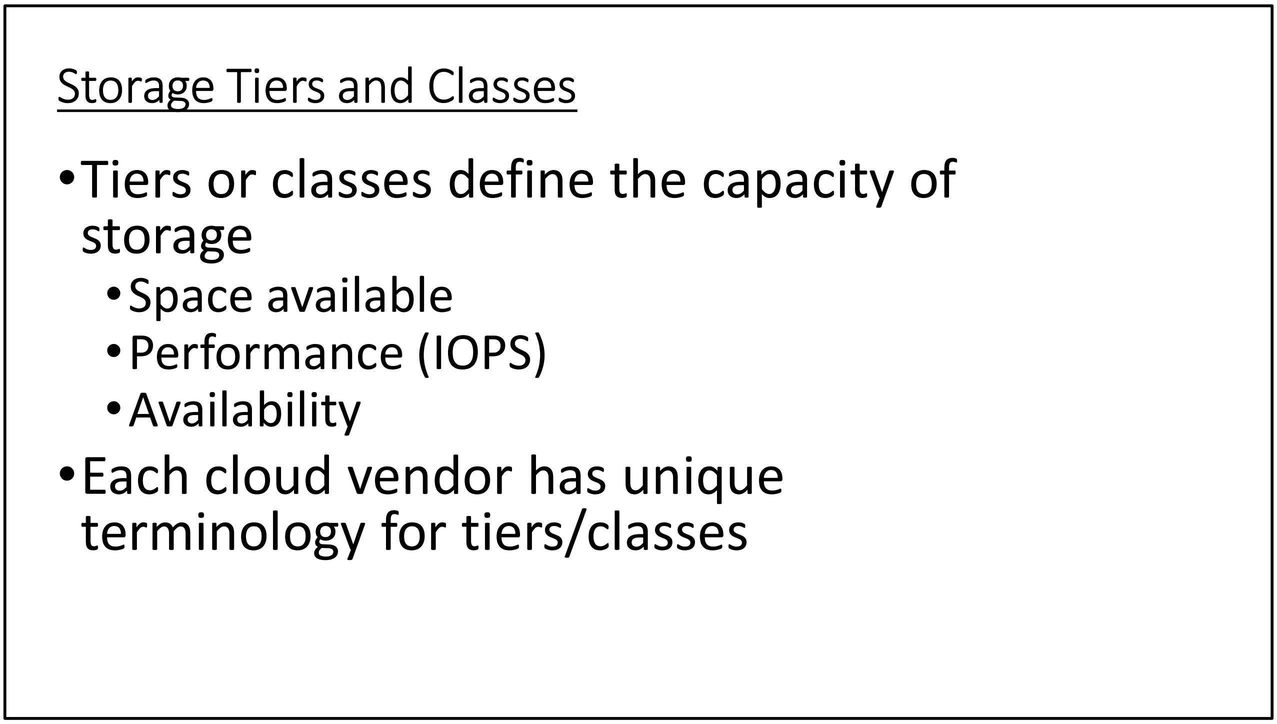
3.06 Storage Management (Demo)

CH03: Cloud Storage



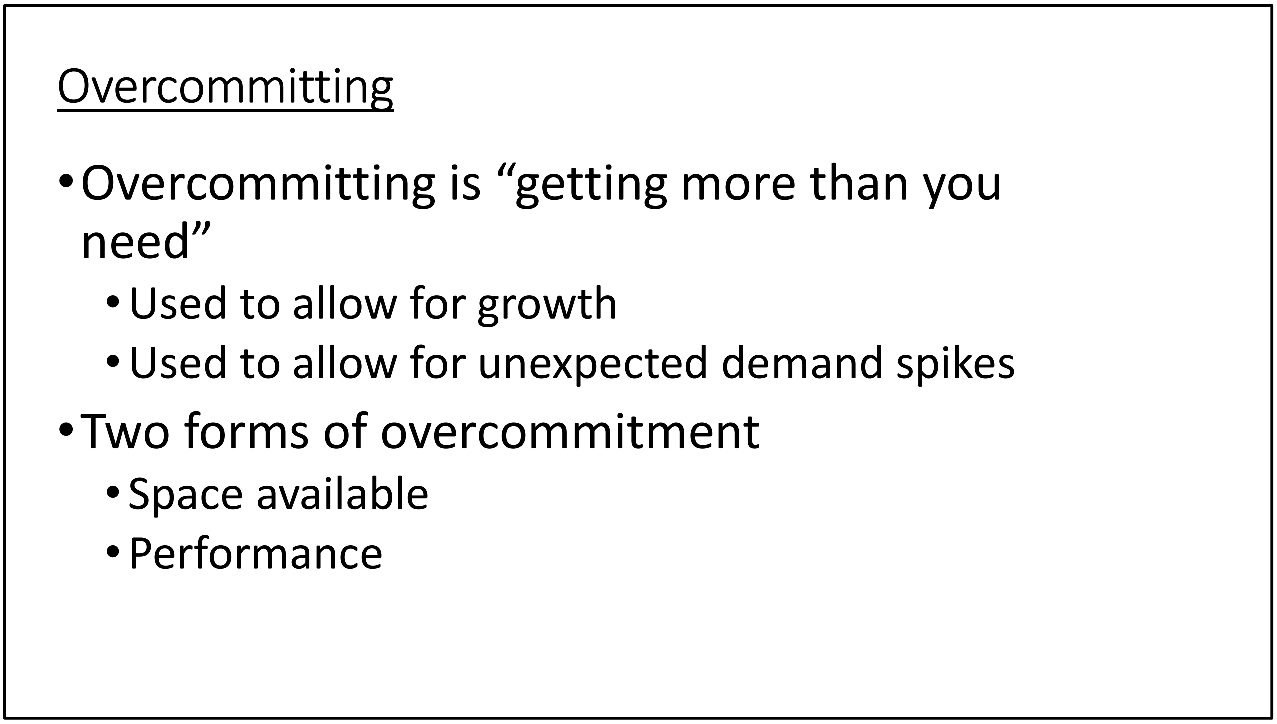
Management Methods

- Web-based interface
  - Point-and-click
  - Provides visual cues and help along the way
- Command-line interface (CLI)
  - Faster
  - More complex
  - Can be automated easily



Storage Tiers and Classes

- Tiers or classes define the capacity of storage
  - Space available
  - Performance (IOPS)
  - Availability
- Each cloud vendor has unique terminology for tiers/classes

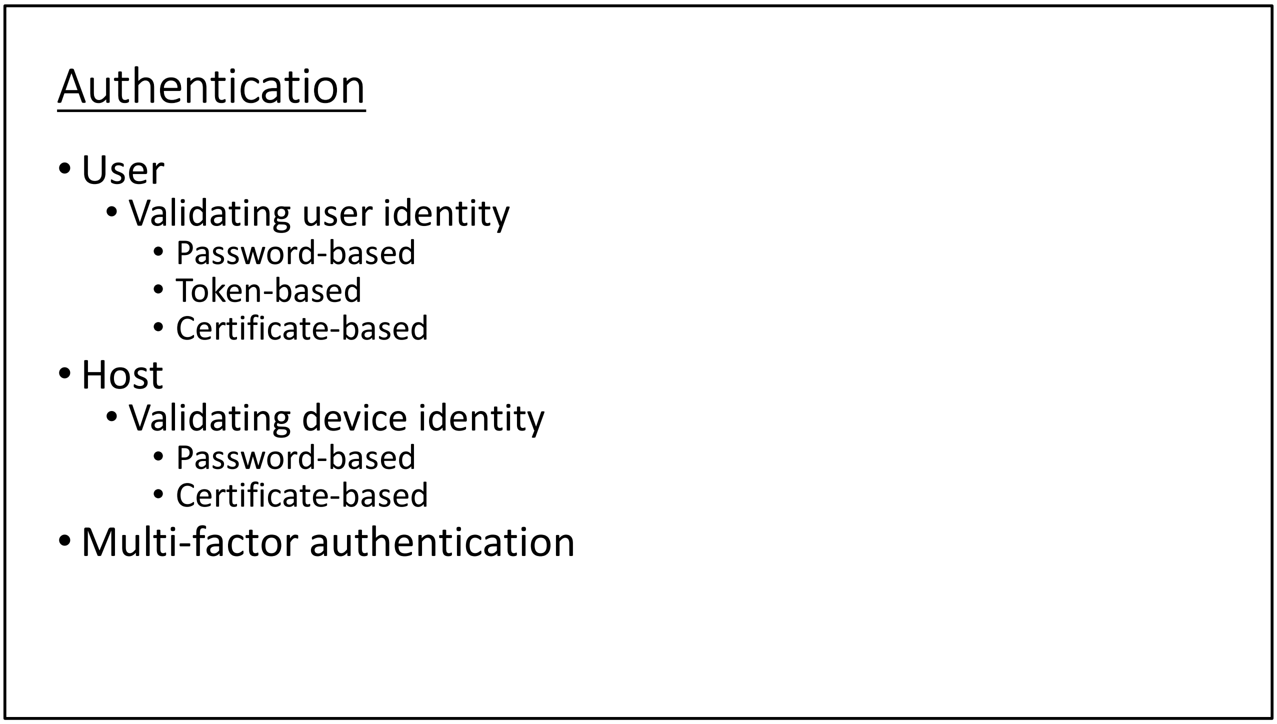


Overcommitting

- Overcommitting is “getting more than you need”
  - Used to allow for growth
  - Used to allow for unexpected demand spikes
- Two forms of overcommitment
  - Space available
  - Performance

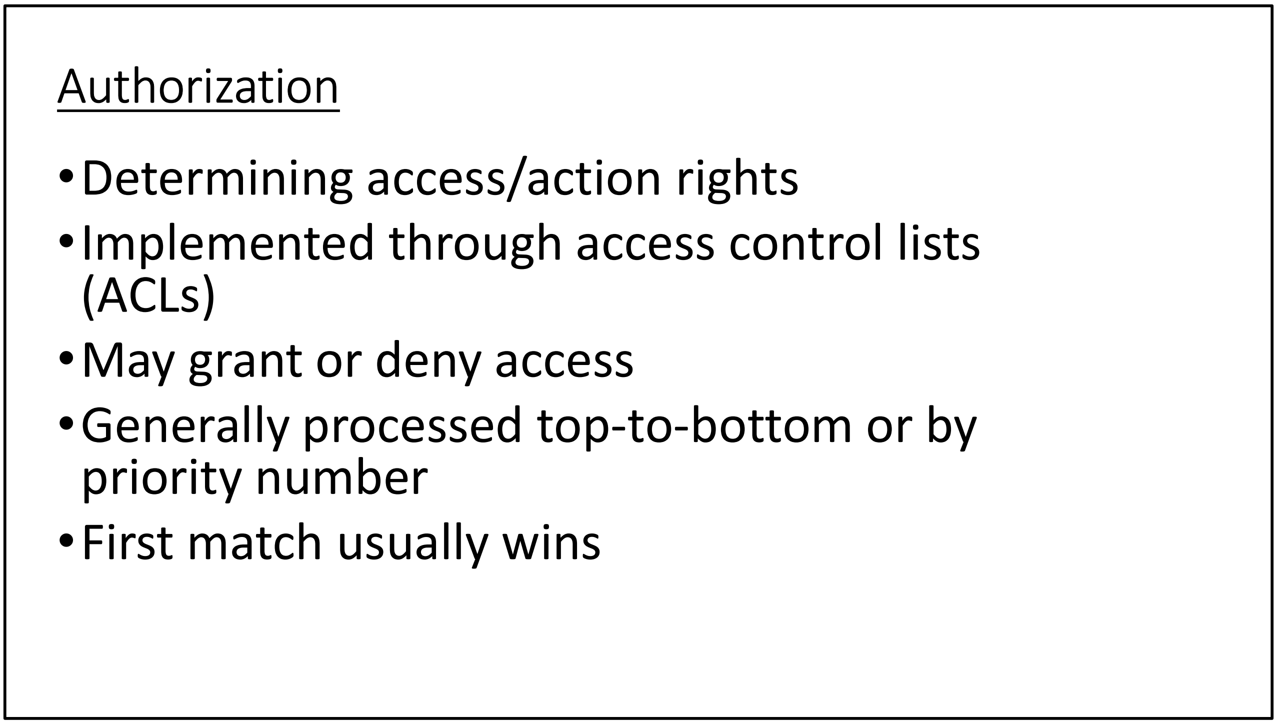
3.07 Storage Security (Lab)

CH03: Cloud Storage



Authentication

- User
  - Validating user identity
    - Password-based
    - Token-based
    - Certificate-based
- Host
  - Validating device identity
    - Password-based
    - Certificate-based
- Multi-factor authentication

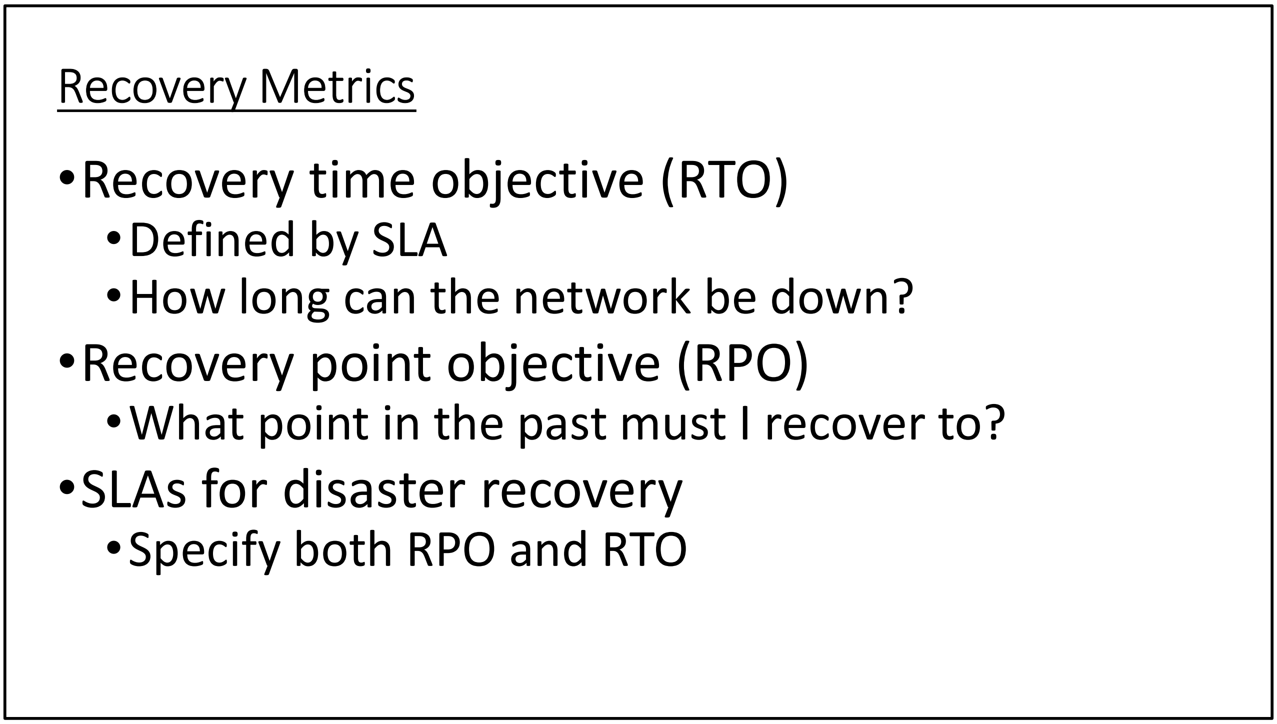


Authorization

- Determining access/action rights
- Implemented through access control lists (ACLs)
- May grant or deny access
- Generally processed top-to-bottom or by priority number
- First match usually wins

3.08 Disaster Recovery Capabilities (Demo)

CH03: Cloud Storage

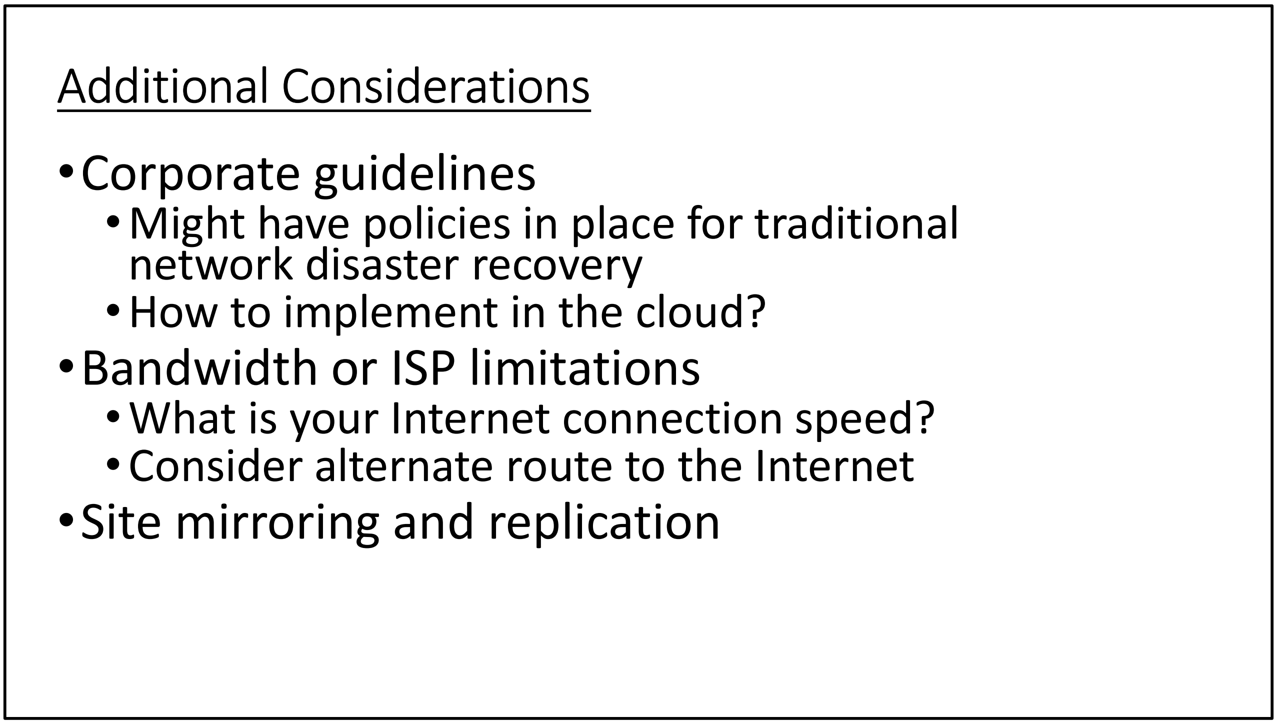


Recovery Metrics

- Recovery time objective (RTO)
  - Defined by SLA
  - How long can the network be down?
- Recovery point objective (RPO)
  - What point in the past must I recover to?
- SLAs for disaster recovery
  - Specify both RPO and RTO

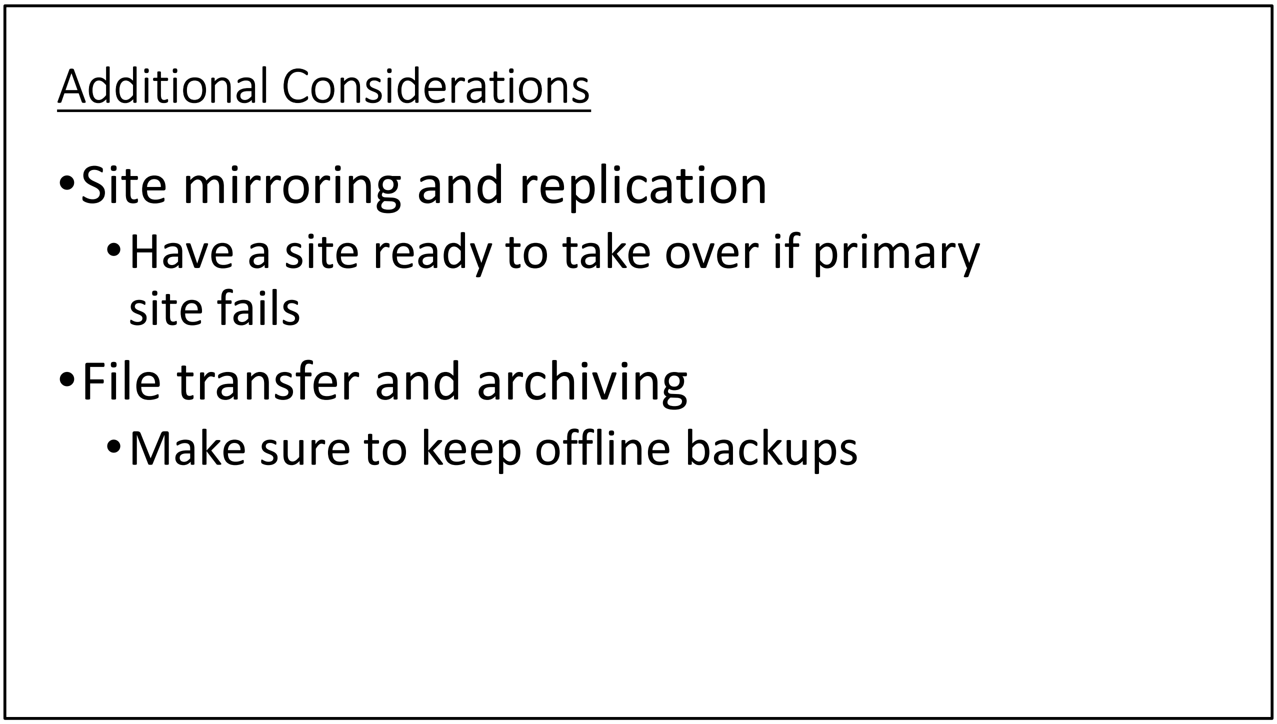
03.09 Disaster Recovery Considerations

CH03: Cloud Storage



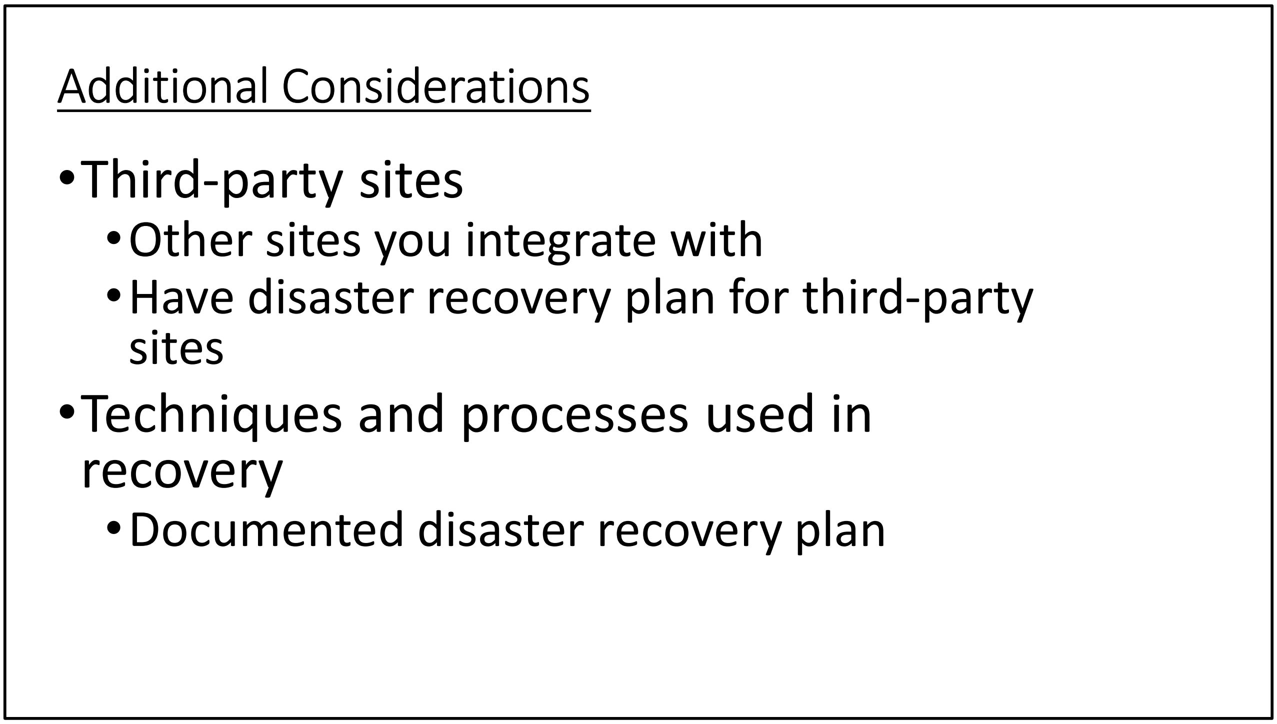
Additional Considerations

- Corporate guidelines
  - Might have policies in place for traditional network disaster recovery
  - How to implement in the cloud?
- Bandwidth or ISP limitations
  - What is your Internet connection speed?
  - Consider alternate route to the Internet
- Site mirroring and replication



Additional Considerations

- Site mirroring and replication
  - Have a site ready to take over if primary site fails
- File transfer and archiving
  - Make sure to keep offline backups



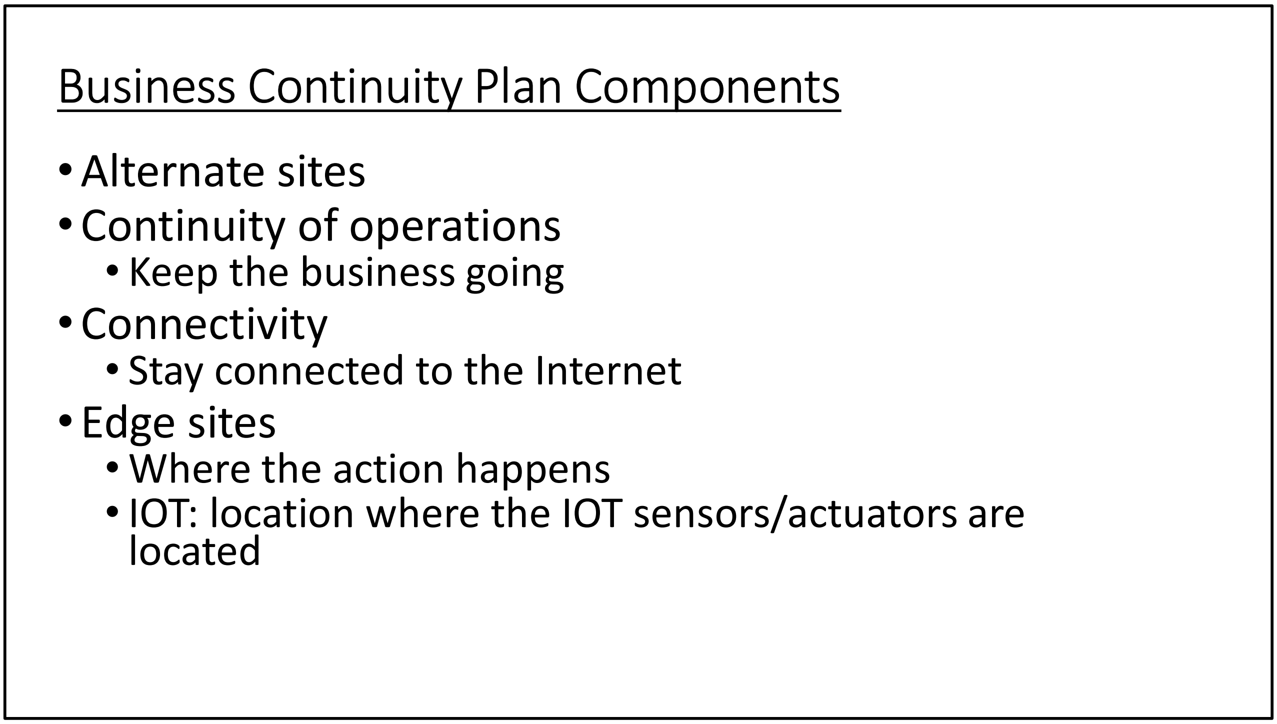
Additional Considerations

- Third-party sites
  - Other sites you integrate with
  - Have disaster recovery plan for third-party sites
- Techniques and processes used in recovery
  - Documented disaster recovery plan

Flesh this out and split into 2

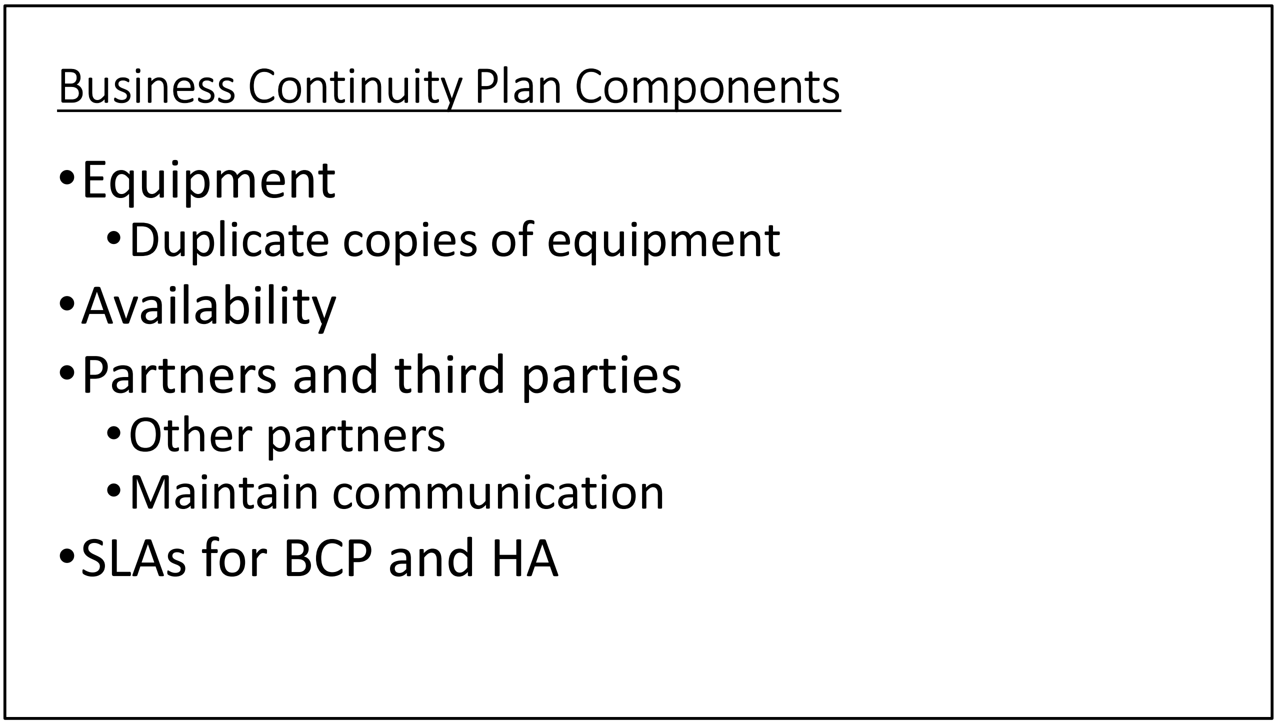
03.10 Business Continuity Plan (Lab)

CH03: Cloud Storage



Business Continuity Plan Components

- Alternate sites
- Continuity of operations
  - Keep the business going
- Connectivity
  - Stay connected to the Internet
- Edge sites
  - Where the action happens
  - IOT: location where the IOT sensors/actuators are located



Business Continuity Plan Components

- Equipment
  - Duplicate copies of equipment
- Availability
- Partners and third parties
  - Other partners
  - Maintain communication
- SLAs for BCP and HA