Course Title & Code: Big Data Storage and Management (CDS502)

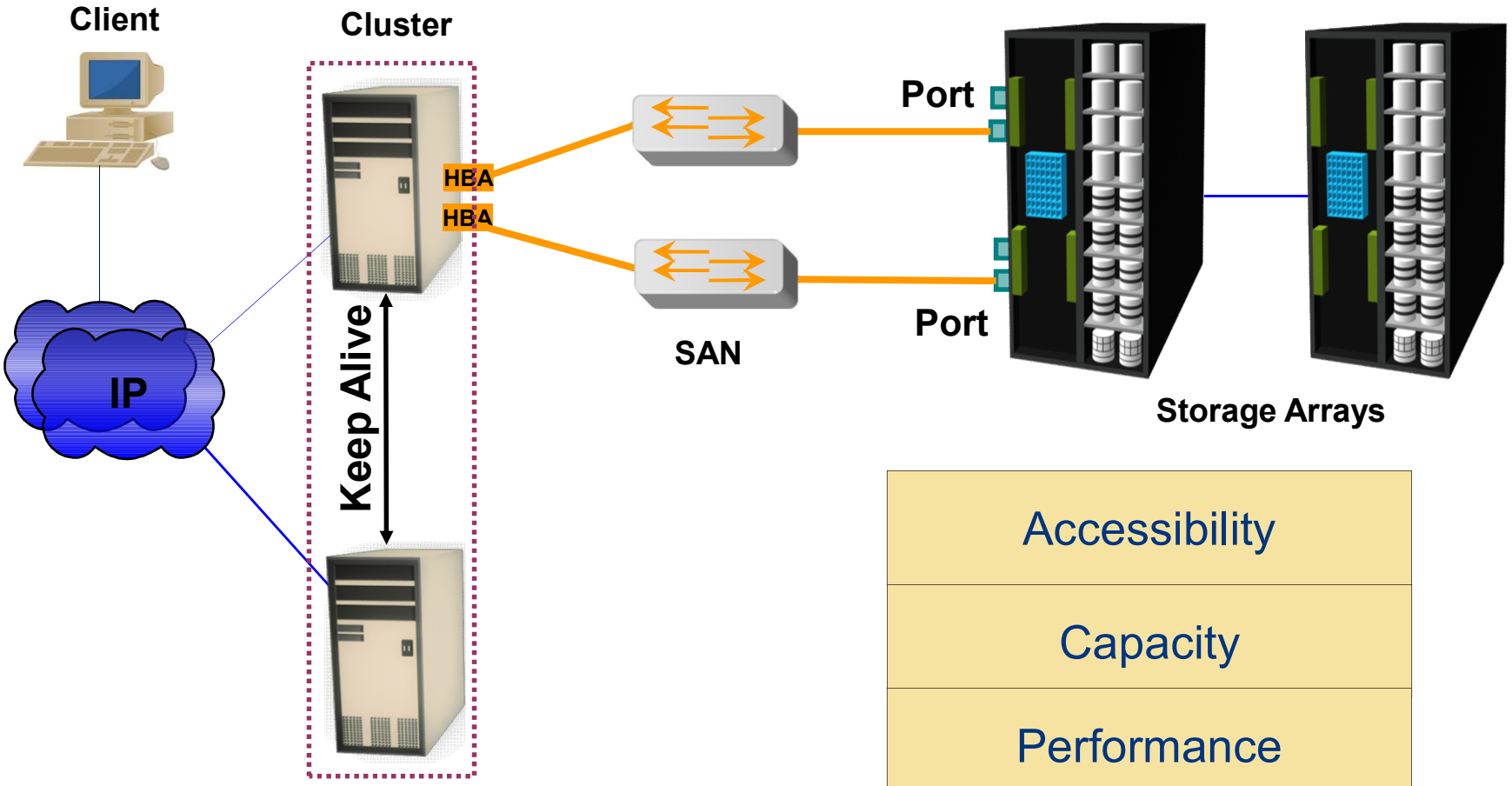
* Big Data Storage Performance Analysis
* Big Data Storage Management

Course Lecturers:
Dr. Mohd. Adib Haji Omar
Dr. Chew XinYing

Storage Infrastructure Management

- Managing storage infrastructure is a key to ensure continuity of business.
- Establishing management processes and implementing appropriate tools is essential to meeting service levels proactively.
- Management activities include **availability**, **capacity**, **performance**, and **security** management.
- **Monitoring** is the most important aspects that forms the basis for storage management.
- Continuous monitoring enables availability and scalability by taking proactive measures.

Monitoring Storage Infrastructure



- Accessibility
- Capacity
- Performance
- Security

Parameters Monitored – Accessibility

- Accessibility refers to the availability of a component to perform a desired operation.
- Why monitor accessibility of different components?
    - Failure of any hardware/software component can lead to outage of a number of different components.
- Monitoring accessibility involves:
    - Checking availability status of the hardware or software components through predefined alerts.

Parameters Monitored – Capacity

- Capacity refers to the amount of storage infrastructure resources available.
- Why monitor capacity?
  - Capacity monitoring prevents outages before they can occur.
    - Inadequate capacity may lead to degraded performance or affect application/service availability.
- More preventive and predictive in nature.
  - Report indicates 90% of all the ports have been utilized in SAN, a new switch must be added if more arrays/servers are to be added.

Parameters Monitored – Performance

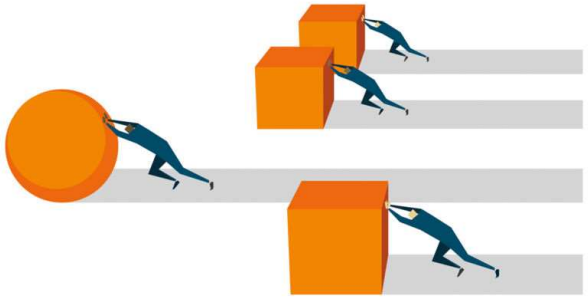
- Performance monitoring evaluates how efficiently different components are performing.

- Why monitor Performance metrics?

  - Want all data center components to work efficiently/optimally.
  - Helps to identify performance bottlenecks.
  - Measures and analyzes the ability to perform at a certain predefined level.

- Examples:

  - Number of I/Os to disks
  - Application response time
  - Network utilization
  - Server CPU utilization



Parameters Monitored – Security

- Monitoring security helps to track and prevent unauthorized access.
- Why monitor security?
  - Need to be protected for confidentiality, integrity and availability.
  - To meet regulatory compliance.
- Examples:
  - Physical security through badge readers, scanners and cameras.

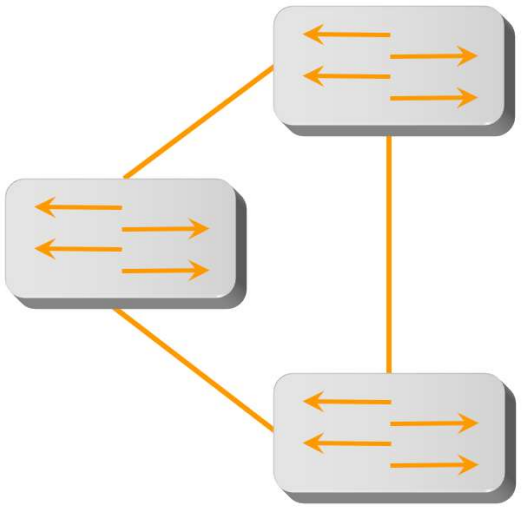
Monitoring Hosts

- Accessibility
  - Hardware components: HBA, NIC, graphic card, internal disk
  - Status of various processes/applications
- Capacity
  - File system utilization
  - Database: Table space/log space utilization
  - User quota
- Performance
  - CPU and memory utilization
  - Transaction response times
- Security
  - Login and authorization
  - Physical security (Data center access)

Host

Monitoring the SAN

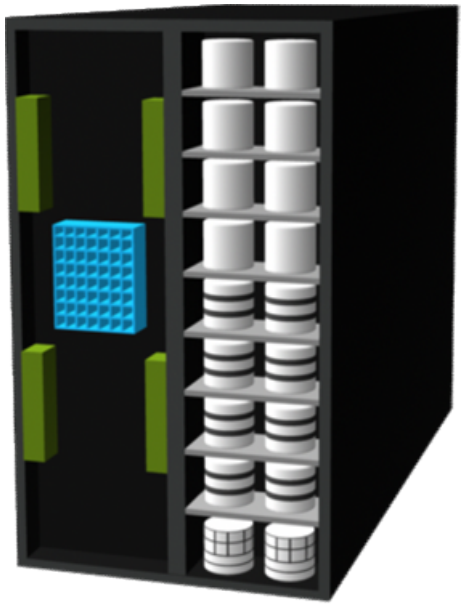
- Accessibility
  - Fabric errors, zoning errors, GBIC failure
  - Device status/attribute change
  - Processor cards, fans, power supplies
- Capacity
  - ISL (inter-switch link) and port utilization
- Performance
  - Connectivity ports
    - Link failures, loss of signal, link utilization
  - Connectivity devices
    - Port statistics
- Security
  - Zoning and LUN Masking
  - Administrative tasks and physical security
    - Authorized access, strict passwords



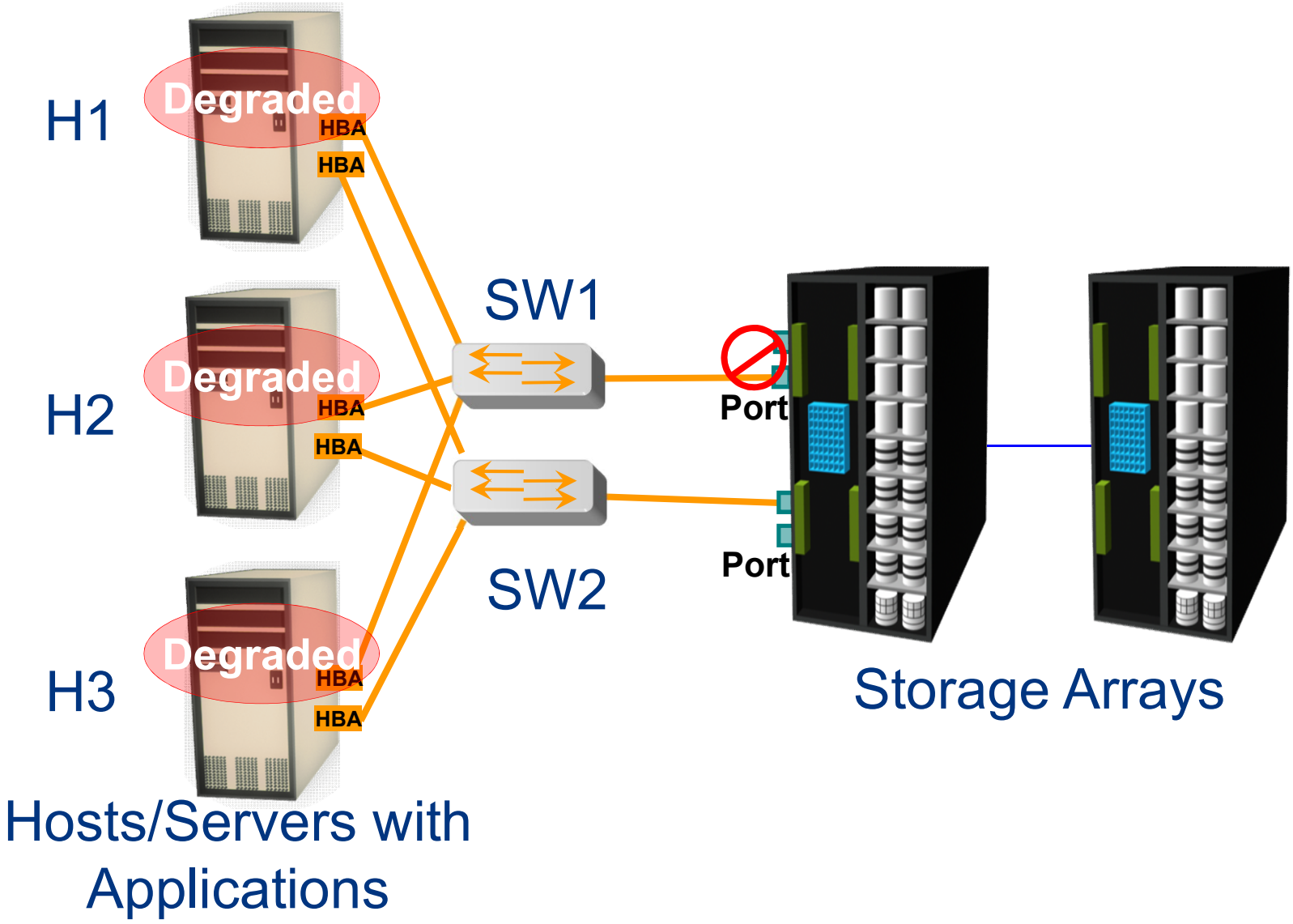
Monitoring Storage Arrays

- Accessibility
  - All Hardware components
  - Array Operating Environment
    - RAID processes
    - Environmental sensors
    - Replication processes
- Capacity
  - Configured/un-configured capacity
  - Allocated/unallocated storage
- Performance
  - FE (front-end) and BE (back-end) utilization/throughput
  - I/O profile, response time, cache metrics
- Security
  - Physical and administrative security

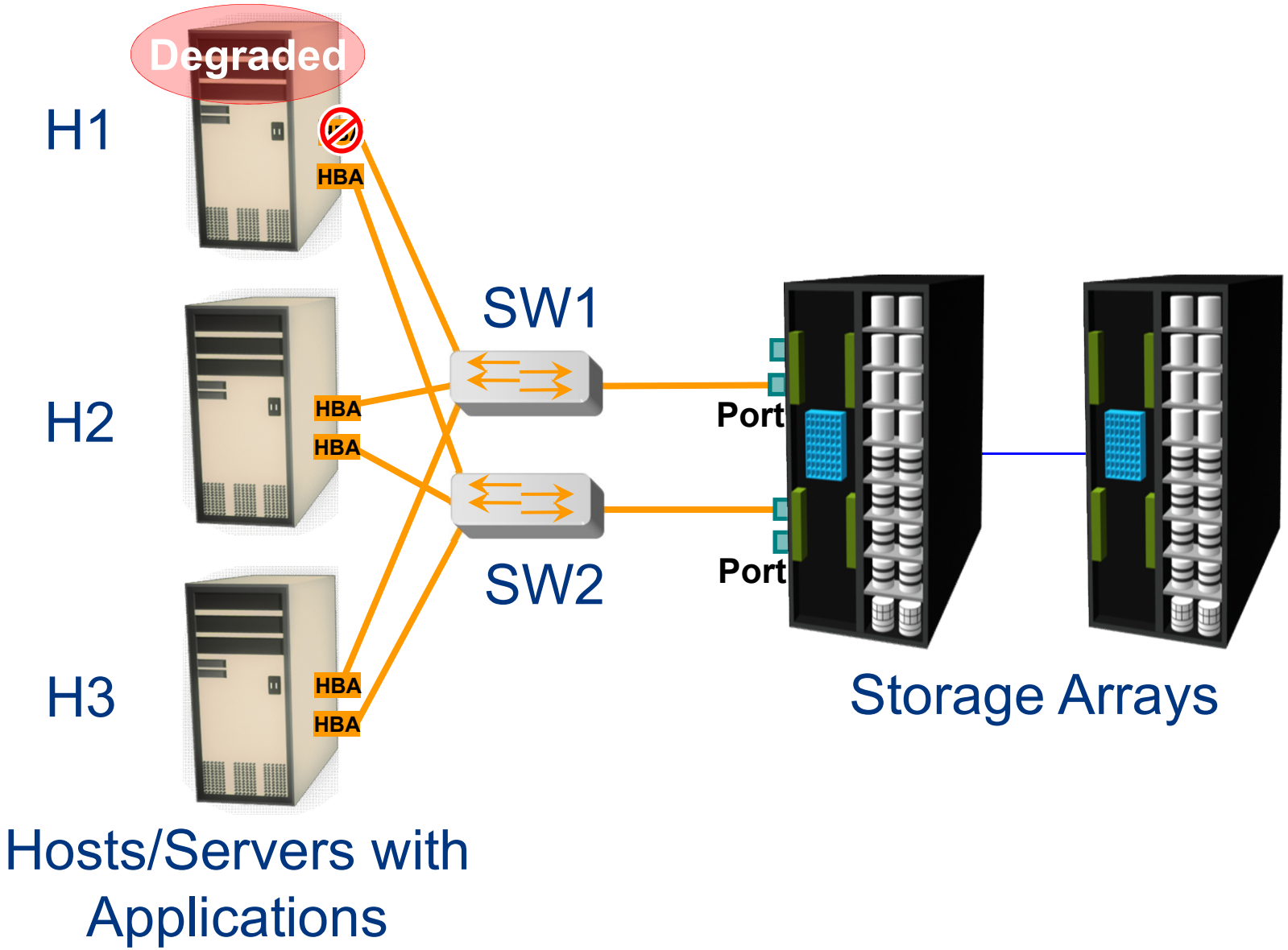
Storage Array



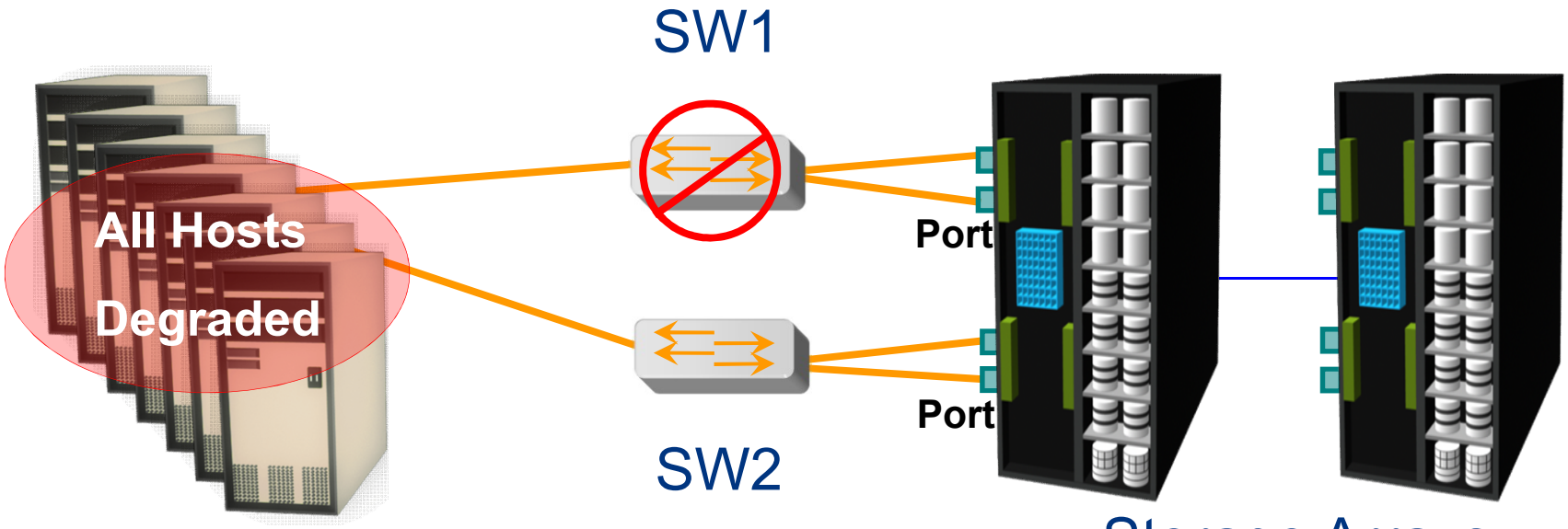
Accessibility Monitoring Example: Array Port Failure



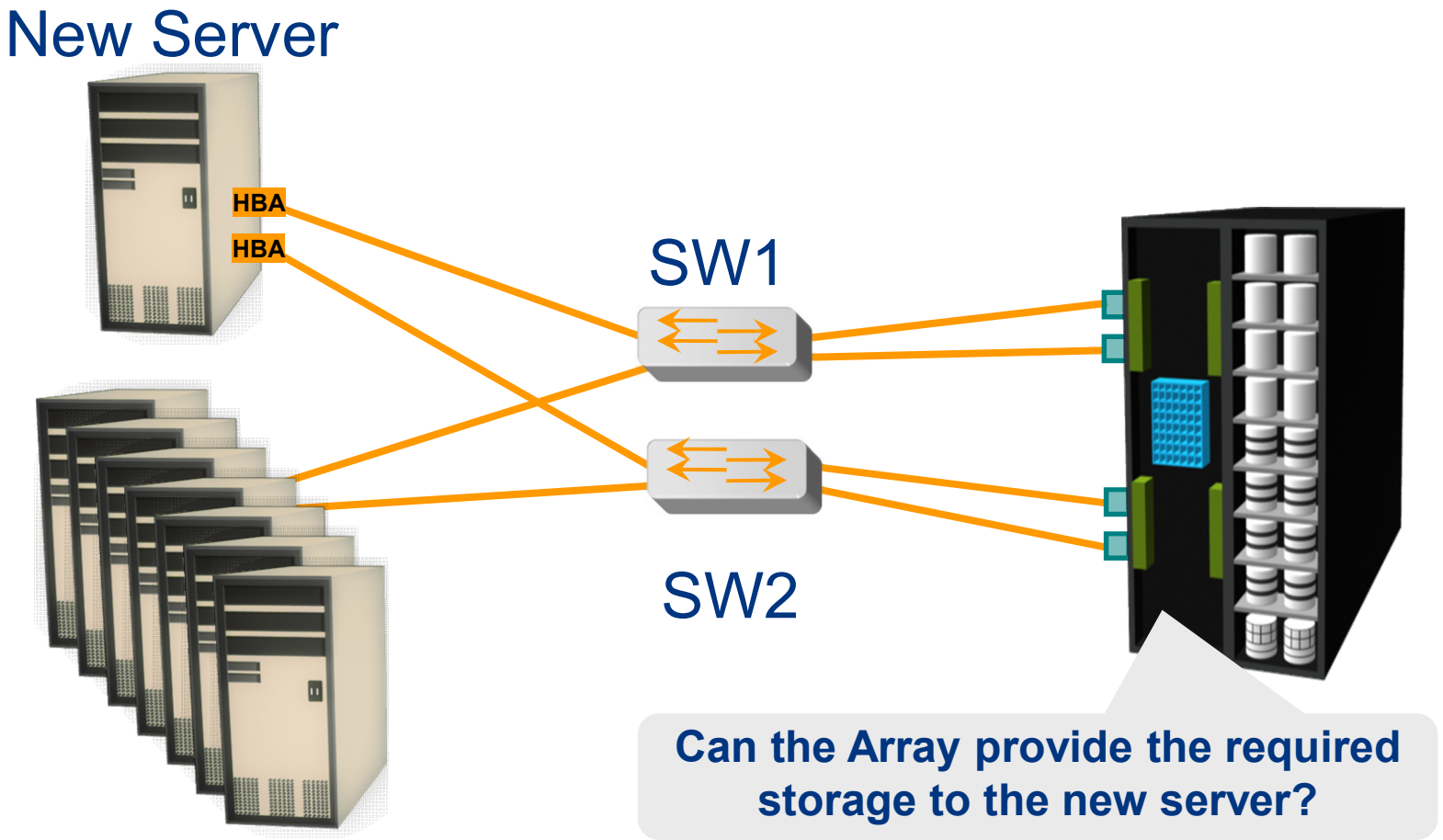
Accessibility Monitoring Example: HBA Failure



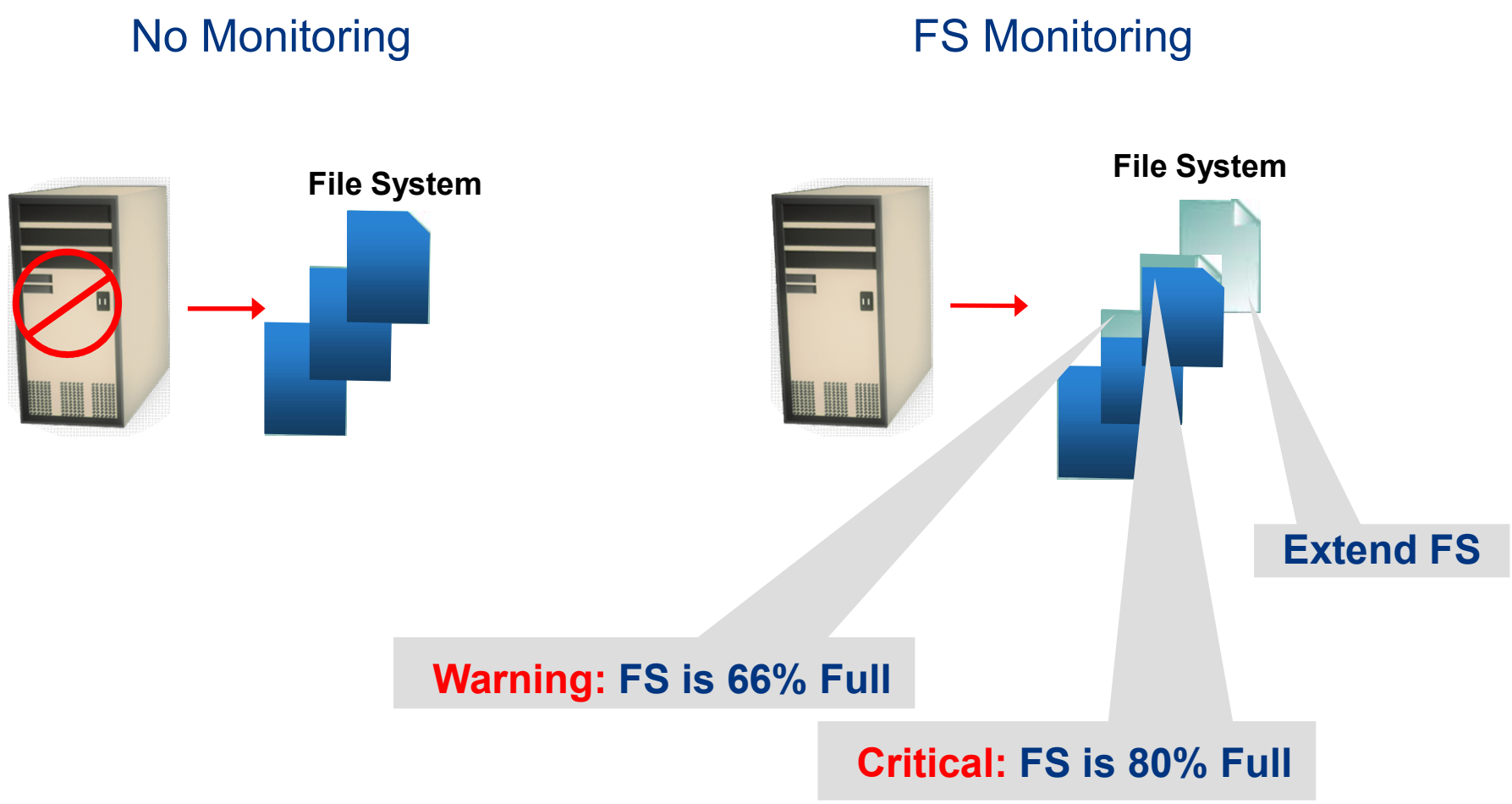
Accessibility Monitoring Example: Switch Failure



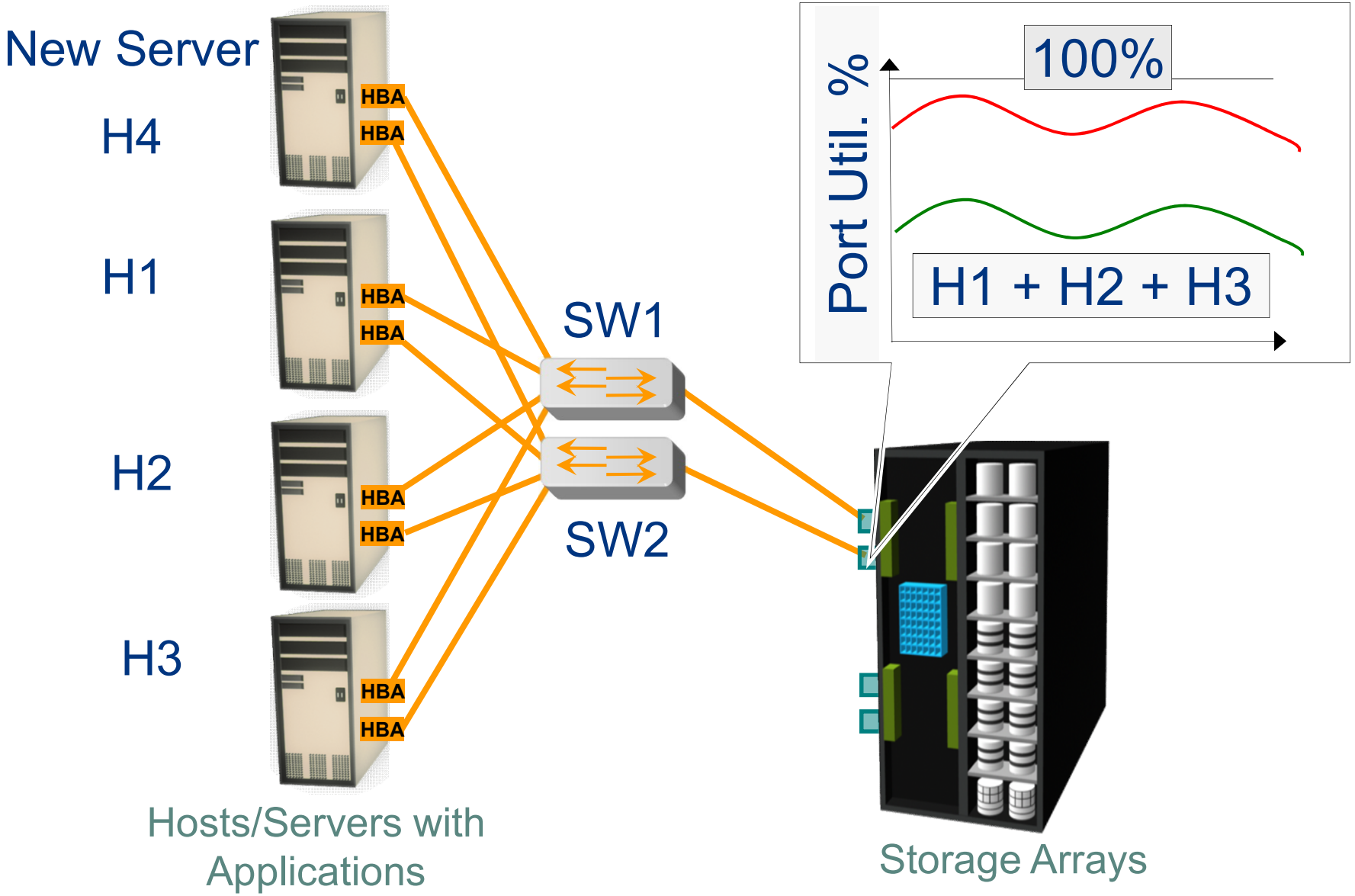
Capacity Monitoring Example: Storage Array



Capacity Monitoring Example: File System Space

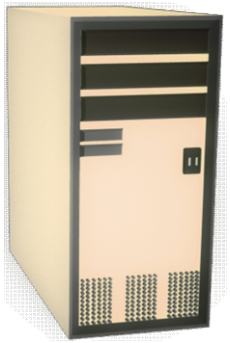


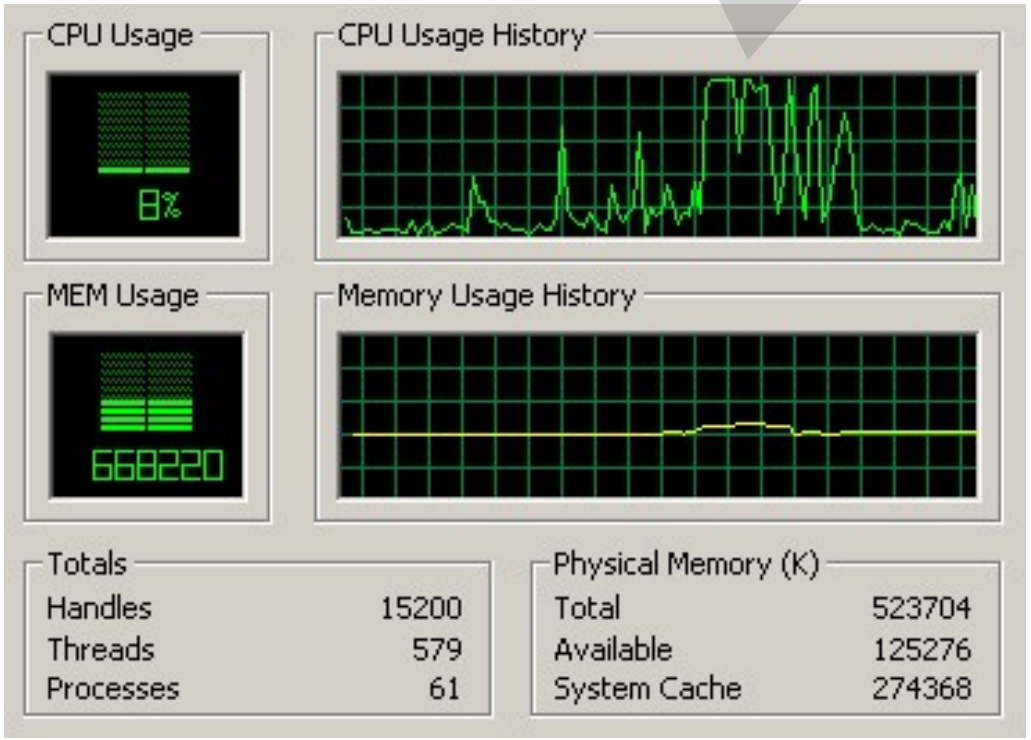
Performance Monitoring Example: Array Port Utilization



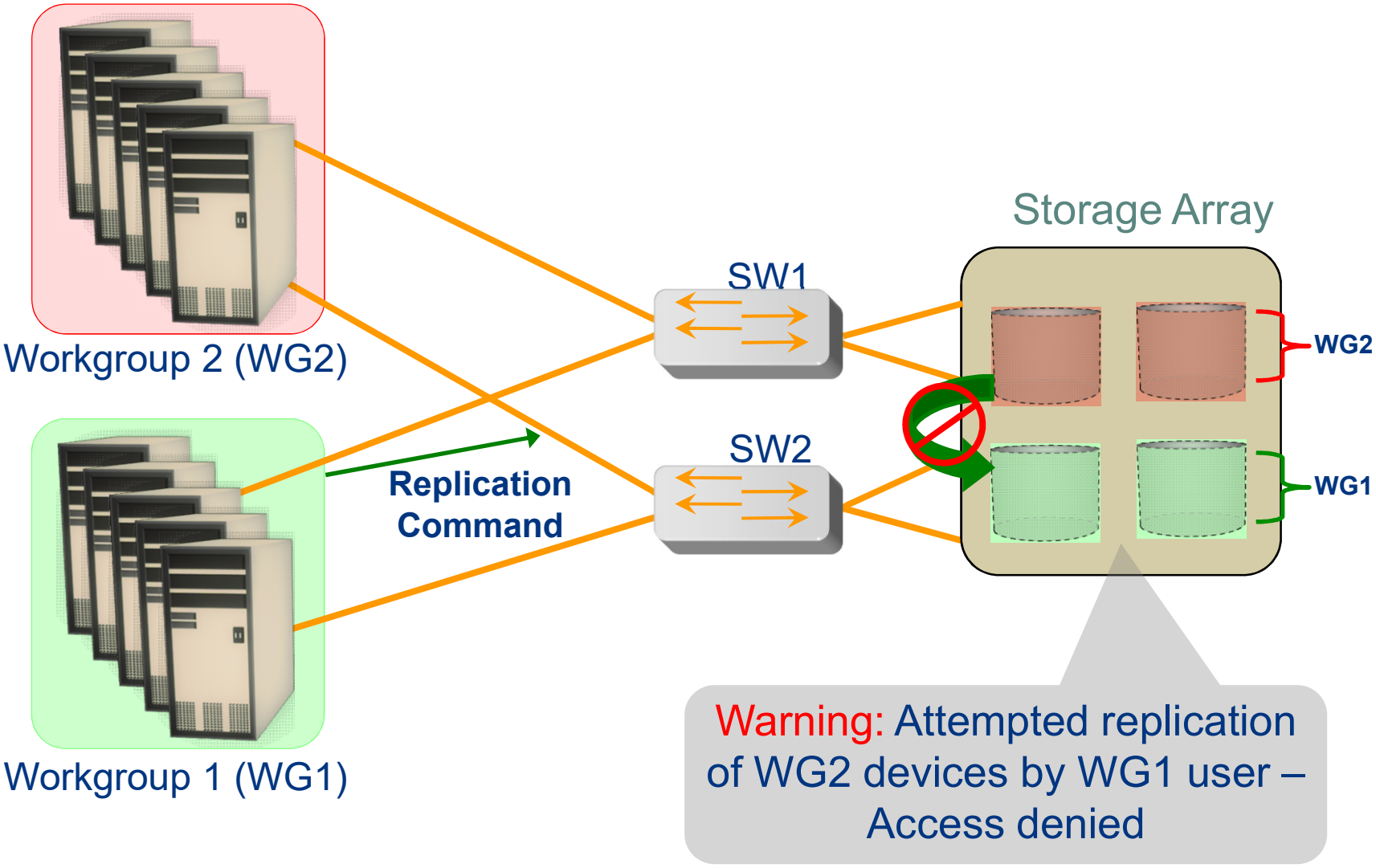
Performance Monitoring Example: Servers CPU Utilization

Critical: CPU Usage above 90% for the last 90 minutes





Security Monitoring Example: Storage Array

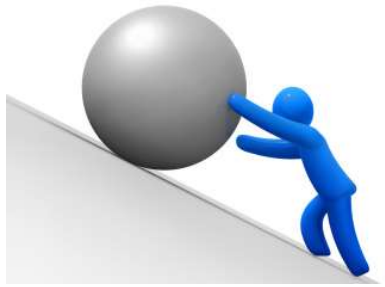


Alerting of Events

- Alerting is an integral part of monitoring
- Monitoring tools enables administrators to assign different severity levels for different events
- Level of alerts based on severity
  - Information alert: Provide useful information and may not require administrator intervention
    - Creation of zone or LUN
  - Warning alerts: Require administrative attention
    - File systems becoming full/Soft media errors
  - Fatal alert: Require immediate administrative attention
    - Power failures/Disk failures/Memory failures/Switch failures

Storage Infrastructure Management Challenges

- Large number and variety of storage arrays, networks, servers, databases and applications.
- Variety of storage devices varying in capacity, performance and protection methodologies.
- Servers with different operating systems: UNIX, LINUX, Windows, mainframe.
- Multiple vendor-specific tools to monitor devices from different vendors.



Backup and Recovery

What is a Backup?

- Backup is an additional copy of data that can be used for restore and recovery purposes.
- The Backup copy is used when the primary copy is lost or corrupted.
- This Backup copy can be created as a:
  - Simple copy (there can be one or more copies)
  - Mirrored copy (the copy is always updated with whatever is written to the primary copy)

Backup and Recovery Strategies

- Several choices are available to get the data to the backup media such as:
  - Copy the data.
  - Mirror (or snapshot) then copy.
  - Remote backup.
  - Copy then duplicate or remote copy.
- Businesses back up their data to enable its recovery in case of potential loss.
- Businesses also back up their data to comply with regulatory requirements.
- Types of backup derivatives:
  - Disaster Recovery
  - Archival
  - Operational

Types of Backup Derivatives

Disaster Recovery addresses the requirement to be able to restore all, or a large part of, an IT infrastructure in the event of a major disaster. (whole system)

Archival is a common requirement used to preserve transaction records, email, and other business work products for regulatory compliance. The regulations could be internal, governmental, or perhaps derived from specific industry requirements.

Operational is typically the collection of data for the eventual purpose of restoring, at some point in the future, data that has become lost or corrupted.
Eventual: occurring or existing at the end of or as a result of a process or period of time. (specific process / individual process)

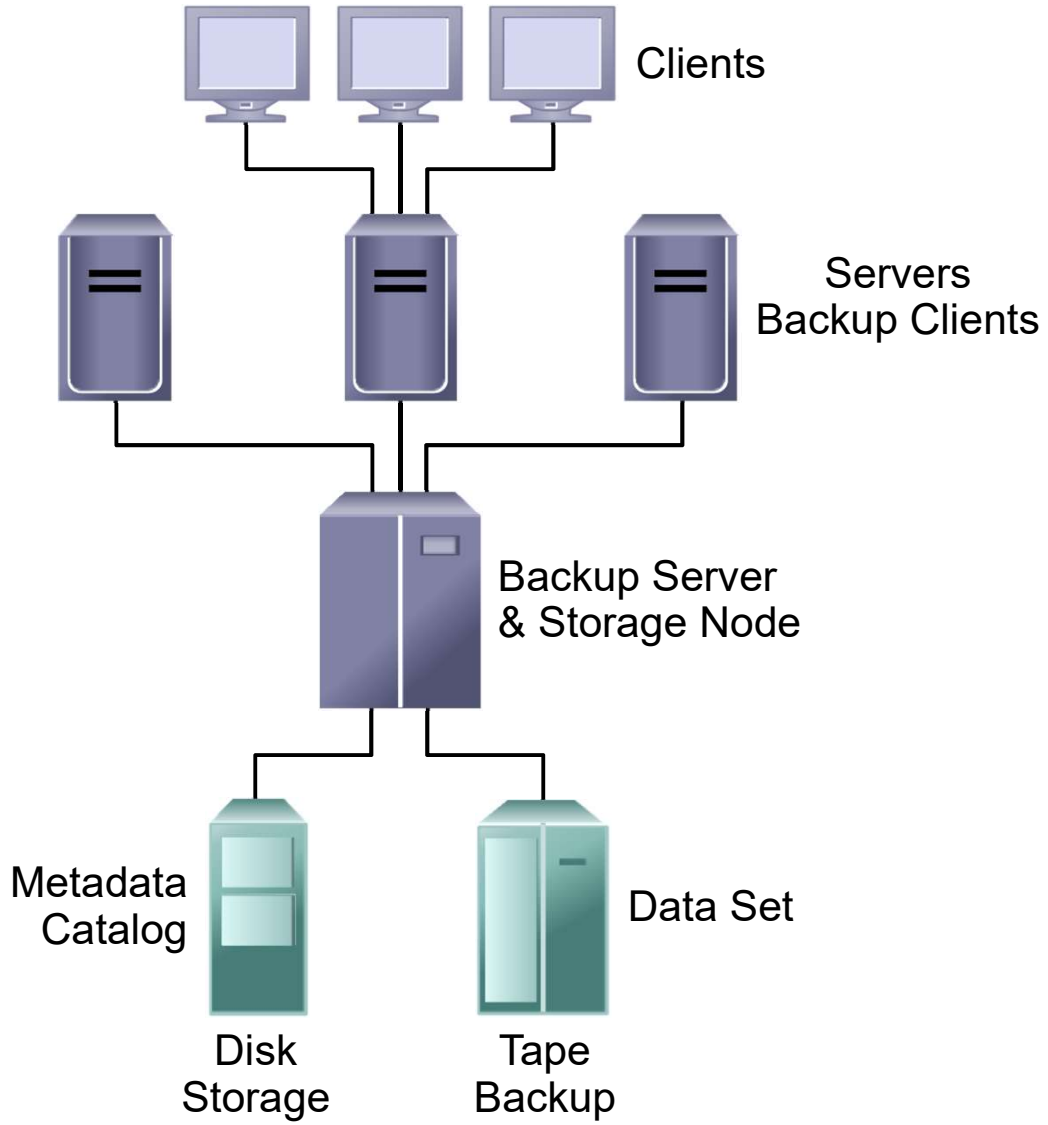
Reasons for a Backup Plan

- **Hardware Failures**
- **Human Factors**
- **Application Failures**
- **Security Breaches**
- **Disasters**

How does Backup Work?

- The basic architecture of a backup system is **client-server**, with a backup server and some number of backup clients or agents.
    - The backup server directs the operations and owns the backup catalog (the information about the backup).
    - The catalog contains the table-of-contents for the data set.
- The backup server depends on the backup client to gather the data to be backed up.
- A backup server receives backup metadata from backup clients to perform its activities.

How does Backup Work



Business Considerations

Some important decisions that need consideration before implementing a Backup/Restore solution include:

- What are the restore requirements – Recovery Time Objective (RTO)?
- Where and when will the restores occur?
- Which data needs to be backed up?
- How frequently should data be backed up?
  - hourly, daily, weekly, monthly
- How long will it take to backup?
- How many copies to create?
- How long to retain backup copies?

Data Considerations: File Characteristics

- **Location**: Many organizations have dozens of heterogeneous platforms that support a complex application. Eg: Consider a data warehouse where data from many sources is fed into the warehouse.

- **Size**: Backing up a large amount of data that consists of a few big files may have less system overhead than backing up a large number of small files. Eg: If a file system contains millions of small files, the very nature of searching the file system structures for changed files can take hours, since the entire file structure is searched.

- **Number**: a file system containing one million files with a ten-percent daily change rate will potentially have to create 100,000 entries in the backup catalog.

Data Considerations: Data Compression

Compressibility depends on the data type, for example:

- Application binaries – do not compress well.
- Text – compresses well.
- JPEG/ZIP files – are already compressed and expand if compressed again.

Data Considerations: Retention Periods

- Operational
  - Data sets on primary media (disk) up to the point where most restore requests are satisfied, then moved to secondary storage (tape).

- Disaster Recovery
  - Driven by the organization's disaster recovery policy
    - Portable media (tapes) sent to an offsite location / vault.
    - Replicated over to an offsite location (disk).
    - Backed up directly to the offsite location (disk, tape or emulated tape).

- Archiving
  - Driven by the organization's policy.
  - Dictated by regulatory requirements.

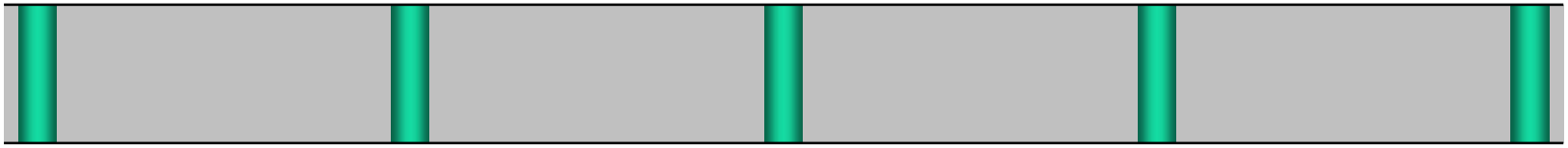
Database Backup Methods

- **Hot Backup**: which means that the application is still up and running, with users accessing it, while backup is taking place, production is not interrupted.
- **Cold Backup**: which means that the application will be shut down for the backup to take place, production is interrupted.
- Most backup applications offer various Backup Agents to do these kinds of operations. **Backup Agents** manage the backup of different data types such as:
  - Structured (such as databases)
  - Semi-structured (such as email)
  - Unstructured (file systems)

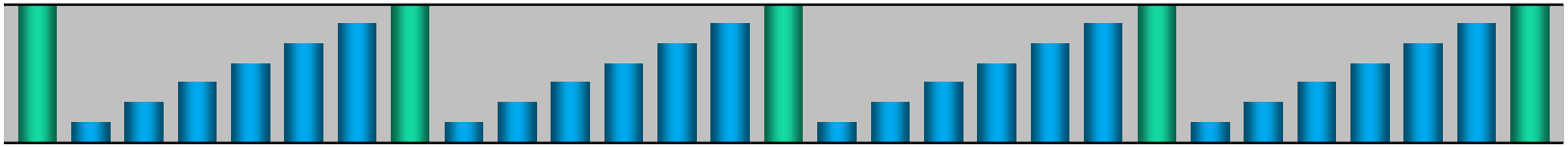
- There will be different agents for different types of data and applications.

Backup Granularity and Levels

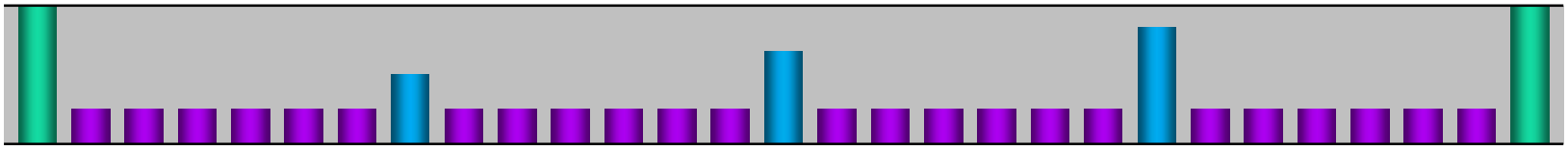
Full Backup is a backup of all data on the target volumes, regardless of any changes made to the data itself.



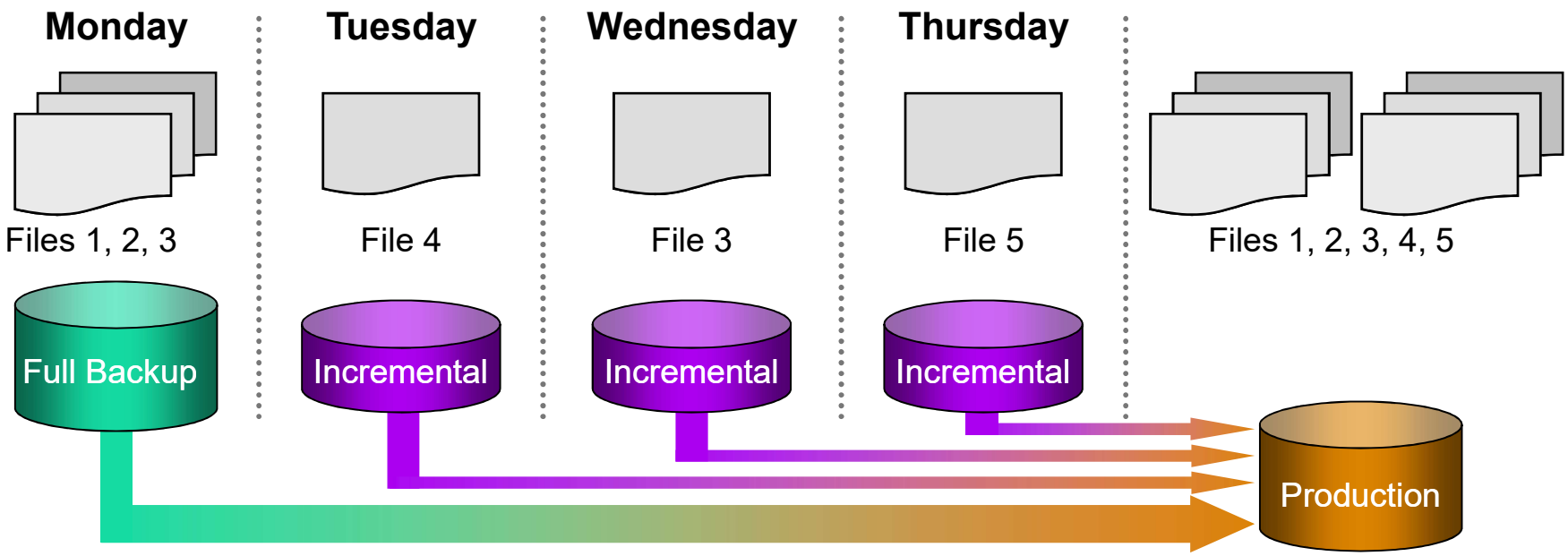
Cumulative (Differential) also known as a Differential backup, is a type of incremental that contains changes made to a file since the last full backup.



Incremental contains the changes since the last backup, of any type, whichever was most recent.



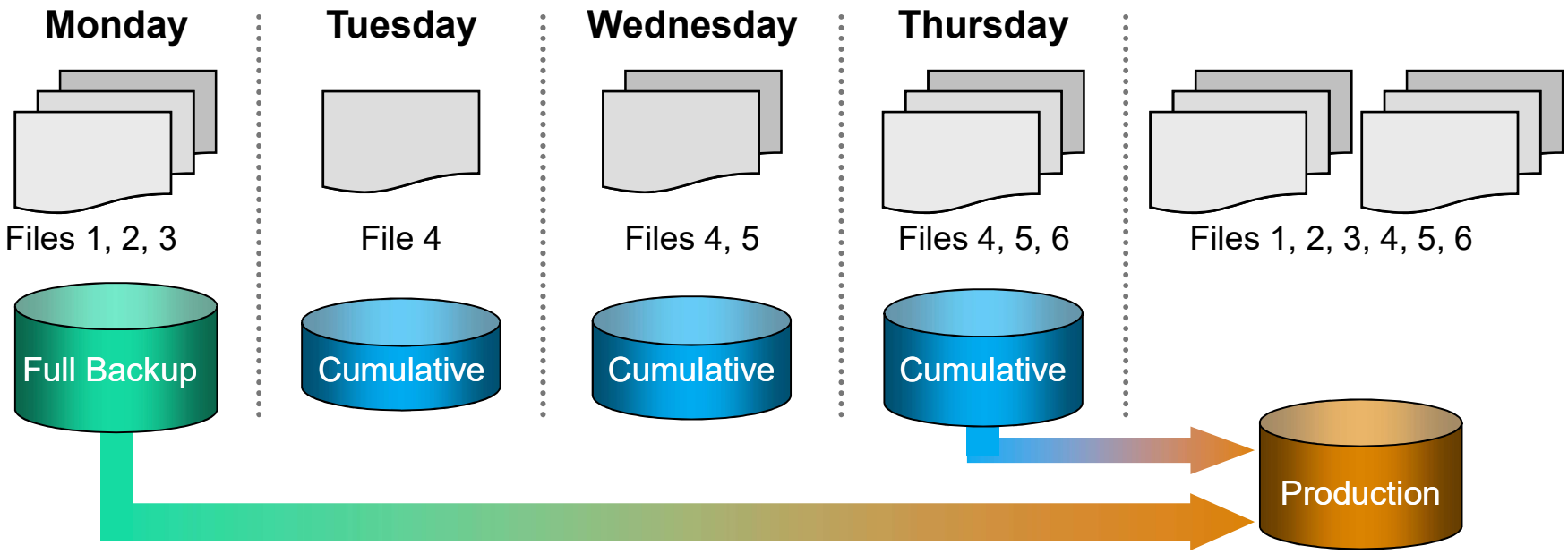
Restoring an Incremental Backup



Key Features:

- Files that have changed since the last full or incremental backup are backed up.
- Fewest amount of files to be backed up, therefore faster backup and less storage space.
- Longer restore because last full and all subsequent incremental backups must be applied.

Restoring a Cumulative Backup



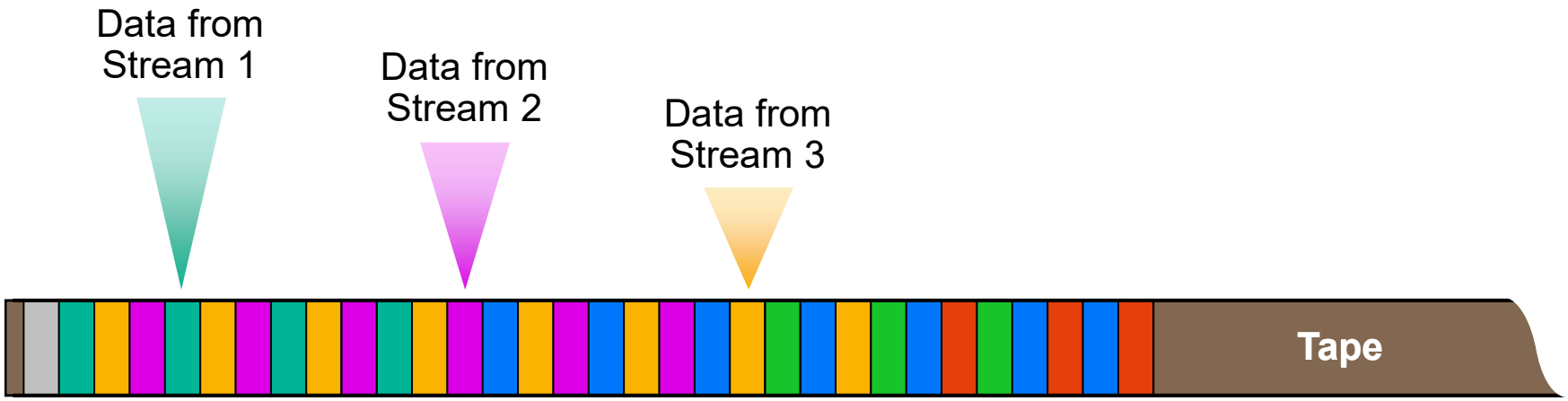
Key Features:

- More files to be backed up, therefore it takes more time to backup and uses more storage space.
- Much faster restore because only the last full and the last cumulative backup must be applied.

Backup Media

- Tape
  - Traditional destination for backups
  - Sequential access
  - No protection
- Disk
  - Random access
  - Protected by the storage array (RAID, hot spare, etc)

Multiple Streams on Tape Media



- Tape drive streaming is recommended from all vendors, in order to keep the drive busy.
- If you do not keep the drive busy during the backup process (writing), performance will suffer.
- Multiple streaming helps to improve performance drastically, but it generates one issue as well: the backup data becomes interleaved, and thus the recovery times are increased.

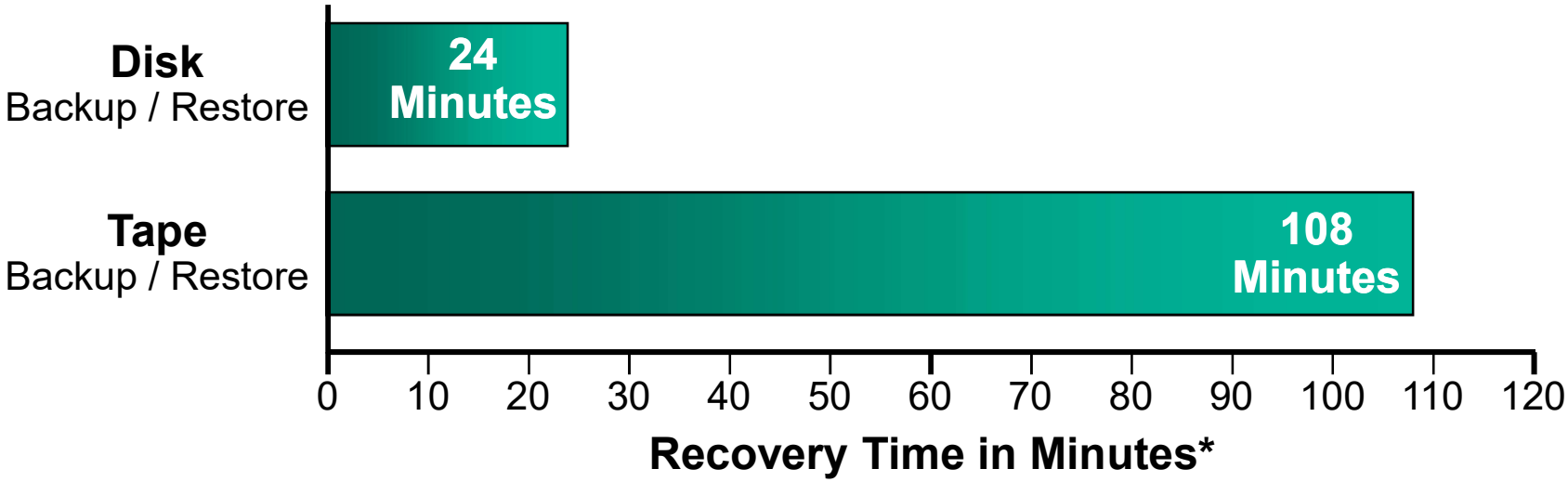
Backup to Disk

- Backup to disk replaces tape and its associated devices, as the primary target for backup, with disk.

- Backup to disk systems offer major advantages over equivalent scale tape systems, in terms of capital costs, operating costs, support costs, and quality of service.

- It can be implemented fully on day 1 or over a phased approach.

Tape versus Disk – Restore Comparaison



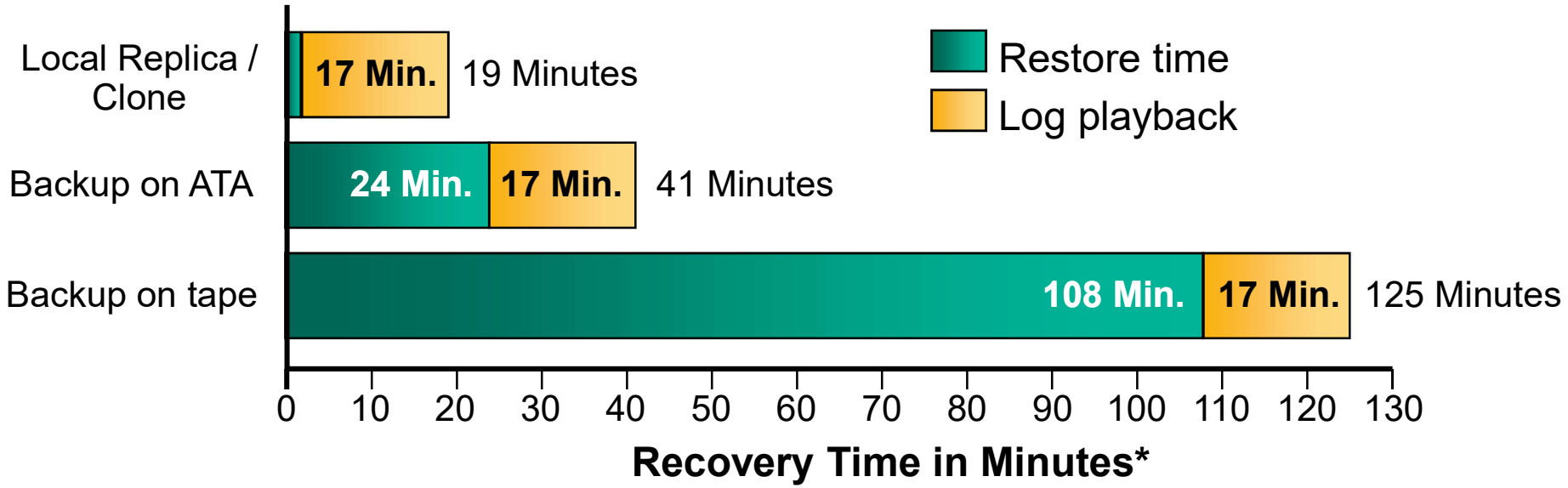
*Total time from point of failure to return of service to e-mail users

This example shows a typical recovery scenario using tape and disk. As you can see, recovery with disk provides much faster recovery than does recovery with tape.

Typical Scenario:

- 800 users, 75 MB mailbox
- 60 GB database

Three Backup / Restore Solutions based on RTO



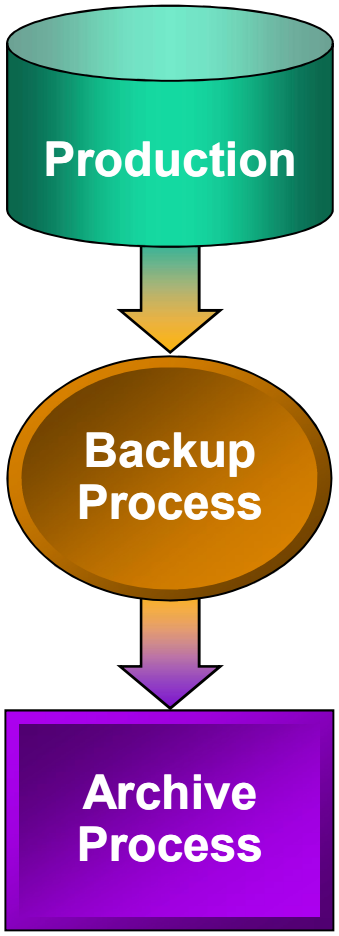
*Total time from point of failure to return of service to e-mail users

Typical Scenario:

- 800 users, 75 MB mailbox
- 60 GB DB – restore time
- 500 MB logs – log playback

- Time of last image dictates the log playback time
- Larger data sets extend the recovery time (ATA and tape)

Traditional Backup, Recovery and Archive Approach

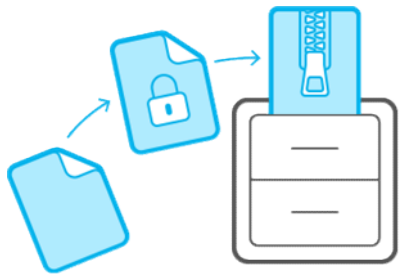


- Production environment grows
  - Requires constant tuning and data placement to maintain performance
  - Need to add more tier-1 storage
- Backup environment grows
  - Backup windows get longer and jobs do not complete
  - Restores take longer
  - Requires more tape drives and silos to keep up with service levels
- Archive environment grows
  - Impact flexibility to retrieve content when requested
  - Requires more media, adding management cost
  - No investment protection for long term retention requirements

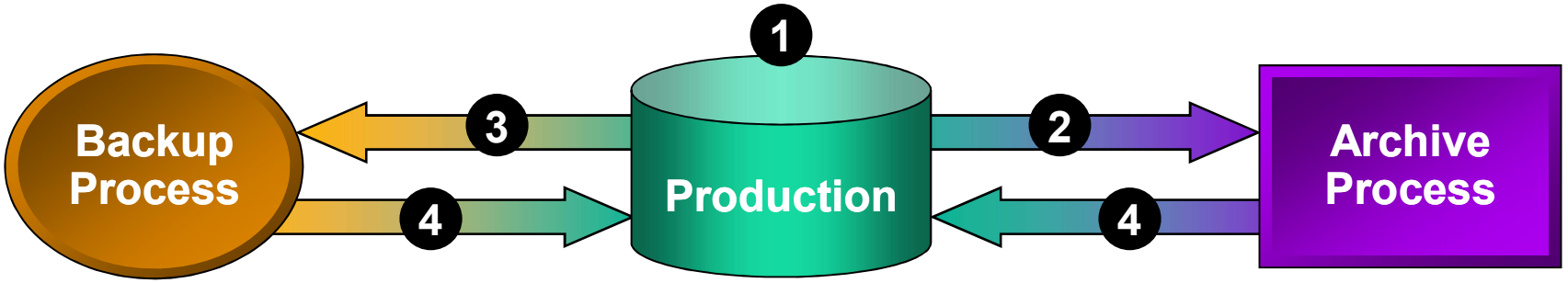
Differences Between Backup / Recovery & Archive

USM
We lead

Backup / Recovery	Archive
A **secondary copy** of information	**Primary copy** of information
Used for **recovery** operations	Available for information **retrieval**
Typically **short-term** (weeks or months)	Typically **long-term** (months, years, or decades)
Data typically **overwritten** on periodic basis (*e.g.*, monthly)	Data typically **maintained** for analysis, value generation, or compliance



New Architecture for Backup, Recovery & Archive



- Understand the environment
- Actively archive valuable information to tiered storage
- Back up active production information to disk
- Retrieve from archive or recover from backup

Managing the Backup Process

USM
We lead

How a Typical Backup Application Works?

- Backup clients are grouped and associated with a Backup schedule that determines when and which backup type will occur.
- Groups are associated with Pools, which determine which backup media will be used.
- Each backup media has a unique label.
- Information about the backup is written to the Backup Catalog during and after it completes. The Catalog shows:
  - when the Backup was performed, and
  - which media was used (label).
- Errors and other information is also written to a log.

Backup Application User Interfaces

We lead

There are typically two types of user interfaces:

- Command Line Interface – CLI
- Graphical User Interfaces – GUI

Managing the Backup and Restore Process

- Running the B/R Application: Backup
  - The backup administrator configures it to be started, most (if not all) of the times, automatically
  - Most backup products offer the ability for the backup client to initiate their own backup (usually disabled)
- Running the B/R Application: Restore

  - There is usually a separate GUI to manage the restore process
  - Information is pulled from the backup catalog when the user is selecting the files to be restored
  - Once the selection is finished, the backup server starts reading from the required backup media, and the files are sent to the backup client

Backup Reports

- Backup softwares also offer reporting features.
- These features rely on the backup catalog and log files.
- Reports are meant to be easy to read and provide important information such as:
  - Amount of data backed up
  - Number of completed backups
  - Number of incomplete backups (failed)
  - Types of errors that may have occurred
- Additional reports may be available, depending on the backup software product used.

Importance of the Backup Catalog

- Backup operations strongly rely on the backup catalog.
- If the catalog is lost, the backup software alone has no means to determine where to find a specific file backed up two months ago.
- It's a good practice to protect the catalog
  - By replicating the file system where it resides to a remote location
  - By backing it up
- Some backup products have built-in mechanisms to protect their catalog (such as automatic backup).

Solution Example: Major Telecom Company

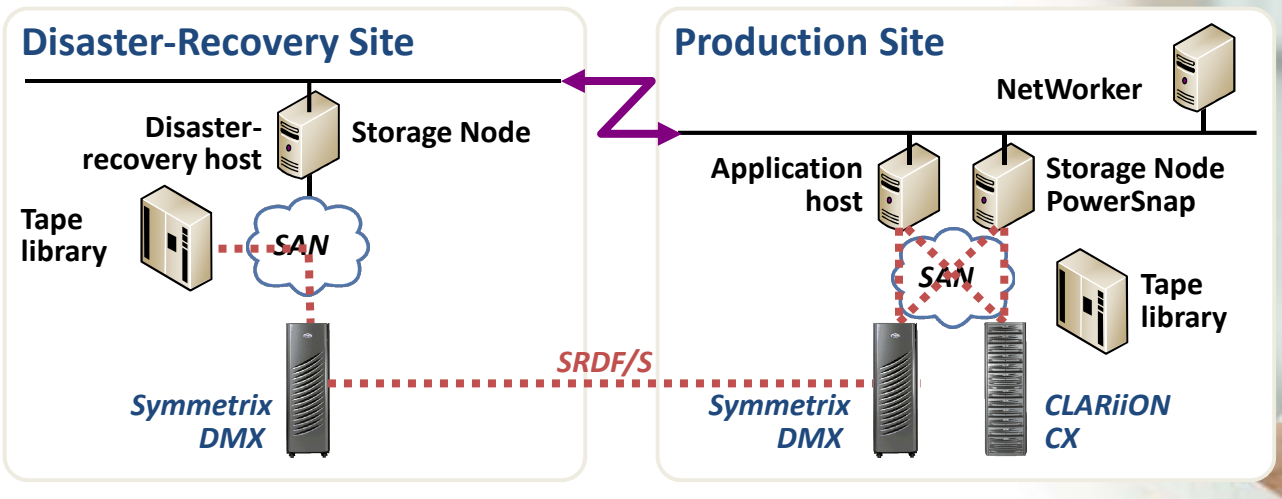
Enterprise-Information Protection

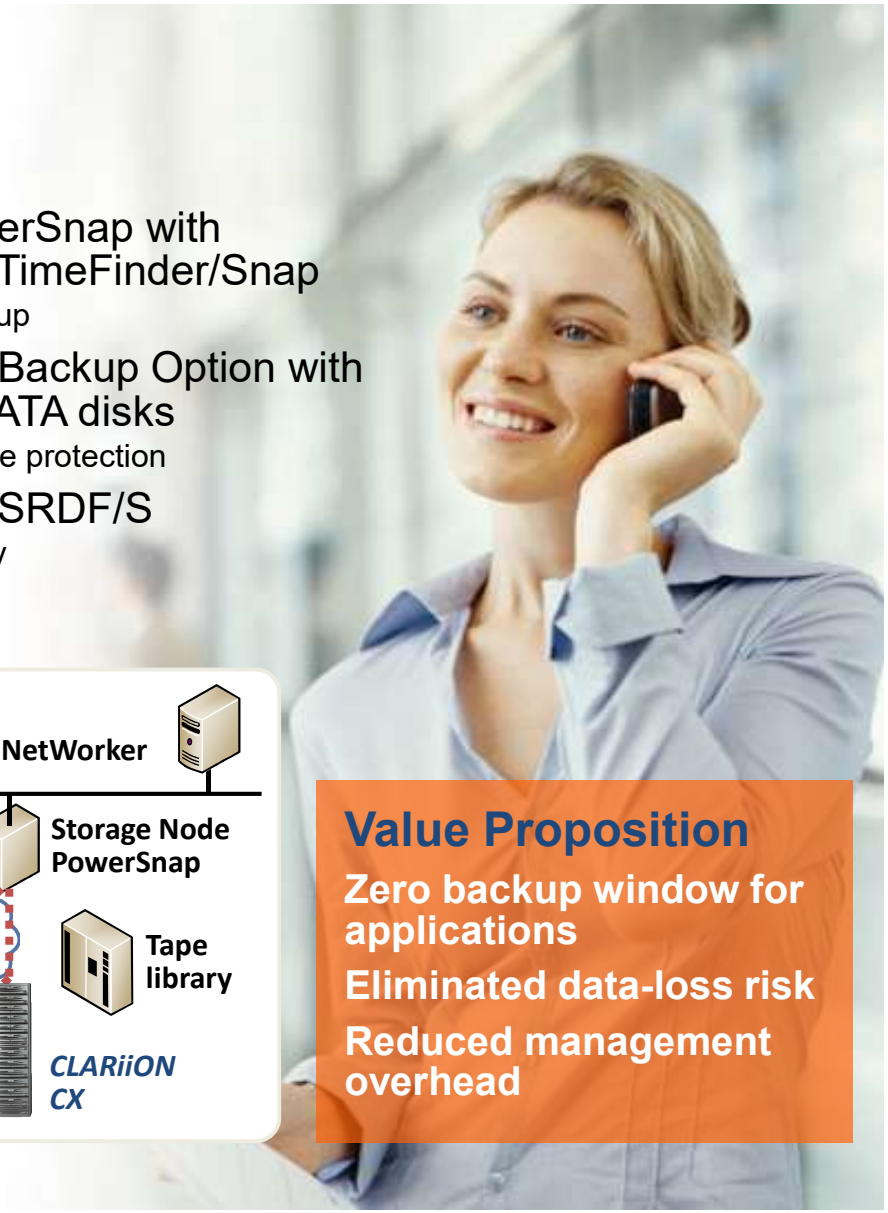
Business Challenge:

- Complex application environment
- No backup window
- Recovery-time objective: Restore 24 TB in two hours

Solution:

- NetWorker PowerSnap with Symmetrix and TimeFinder/Snap
  - Server-free backup
- NetWorker DiskBackup Option with CLARiiON with ATA disks
  - Rapid primary-site protection
- NetWorker and SRDF/S
  - Disaster recovery
  - Offsite protection





Value Proposition

Zero backup window for applications

Eliminated data-loss risk

Reduced management overhead

Thank You

Prepared & Presented by:
Dr. Chew XinYing
School of Computer Sciences