Module-3: Backup, Archive, and Replication

Syllabus: Backup, Archive and Replication Introduction to Business Continuity: Information Availability, BC Terminology, BC Planning Lifecycle, Failure Analysis, BC Technology Solutions. Backup and Archive: Backup Methods, Backup Topologies, Backup Targets, Data Deduplication for Backup, Backup in Virtualized Environments, Data Archive. Local Replication: Replication Terminology, Uses of Local Replicas, Local Replication Technologies, Local Replication in a Virtualized Environment. Remote Replication: Remote Replication Technologies, Three-Site Replication, Remote Replication and Migration in a Virtualized Environment.

Chapter 9: Introduction to Business Continuity

Introduction

- Continuous access to information is a must for the smooth functioning of business operations today.
- There are many threats to information availability, such as natural disasters (e.g., flood, fire, earthquake), unplanned occurrences (e.g., cybercrime, human error, network and computer failure), and planned occurrences (e.g., upgrades, backup, restore) that result in the inaccessibility of information.
- ***Business continuity (BC)*** is an integrated and enterprise-wide process that includes all activities (internal and external to IT) that a business must perform to mitigate the impact of planned and unplanned downtime.
- BC entails preparing for, responding to, and recovering from a system outage that adversely affects business operations. It involves proactive measures, such as business impact analysis and risk assessments, data protection, and security, and reactive countermeasures, such as disaster recovery and restart, to be invoked in the event of a failure.
- The **goal of a business continuity solution is to ensure the "information availability"** required to conduct vital business operations.

9.1 Information Availability

Information availability (IA) refers to the ability of the infrastructure to function according to

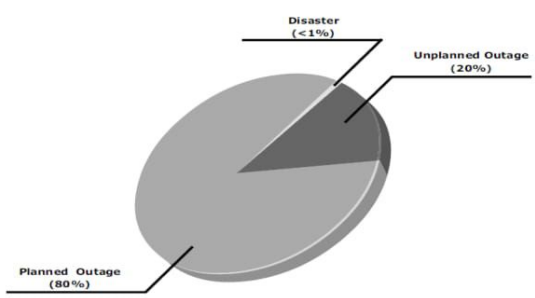
business expectations during its specified time of operation and ensure that people (Employees, customers, partners) can access information whenever they need it. I.A. can be defined with the help of following terms:

- **Accessibility:** This ensures that the required information is accessible at the right place, to the right user.
- **Reliability:** Information should be reliable and correct in all aspects. It is "the same" as what was stored, and there is no alteration or corruption to the information.
- **Timeliness:** Defines the exact moment or the time window (a particular time of the day) during which information must be accessible. For example, if online access to an application is required between 8:00 am and 10:00 pm each day, any disruptions to data availability outside of this time slot are not considered to affect timeliness.

9.1.1 Causes of Information Unavailability

Various planned and unplanned incidents result in data unavailability.

1. ***Planned outages*** include installation/ integration/ maintenance of new hardware, software upgrades or patches, taking backups, application and data restores, facility operations (renovation and construction), and refresh/migration of the testing to the production environment.
2. ***Unplanned outages*** include failure caused by database corruption, component failure, and human errors.
   - Another type of incident that may cause data unavailability is natural or man-made disasters such as flood, fire, earthquake, and contamination.
   - As illustrated in Figure 9-1, the majority of outages are planned. Planned outages are expected and scheduled, but still cause data to be unavailable.
   - Statistically, less than 1 percent is likely to be the result of an unforeseen disaster.



9.1.2 Consequences of Downtime

- Information unavailability or downtime results in loss of productivity, loss of revenue, poor financial performance, and damage to reputation.
- Loss of productivity includes reduced output per unit of labor, equipment, and capital.
- Loss of revenue includes direct loss, compensatory payments, future revenue loss, billing loss, & investment loss. Poor financial performance affects revenue recognition, cash flow, discounts, credit rating, and stock price.
- Damages to reputations may result in a loss of confidence or credibility with customers, suppliers, financial markets, banks, and business partners.

The business impact of downtime is the sum of all losses sustained as a result of a given disruption. An important metric, ***average cost of downtime per hour***, provides a key estimate in determining the appropriate BC solutions.

It is calculated as follows:

Average cost of downtime per hour = Avg productivity loss / hour + Avg revenue loss per hour

Where:

Productivity loss per hour = (total salaries and benefits of all employees per week)/ (average number of working hours per week)

Average revenue loss per hour = (total revenue of an organization per week)/ (average number of hours per week that an organization is open for business)

11.1.2 Measuring Information Availability

- Information availability relies on the availability of the hardware and software components of a data center. Failure of these components might disrupt information availability.
- A failure is the termination of a component's ability to perform a required function. The component's ability can be restored by performing an external corrective action, such as a manual reboot, a repair, or replacement of the failed component(s).
- Repair involves restoring a component to a condition that enables it to perform a required function within a specified time by using procedures and resources.
- Proactive risk analysis performed as part of the BC planning process considers the component failure rate and average repair time, which are measured by MTBF and MTTR:

1. **Mean Time Between Failure (MTBF):** It is the average time available for a system or component to perform its normal operations between failures. It is the measure of system or component reliability and is usually expressed in hours.
2. **Mean Time to Repair (MTTR):** It is the average time required to repair a failed component. While calculating MTTR, it is assumed that the fault responsible for the failure is correctly identified and that the required spares and personnel are available.

   Fault is a physical defect at the component level, which may result in data unavailability. MTTR includes the time required to do the following: detect the fault, mobilize the maintenance team, diagnose the fault, obtain the spare parts, repair, test, and resume normal operations. Figure 9-2 illustrates the various information availability metrics that represent system uptime and downtime.

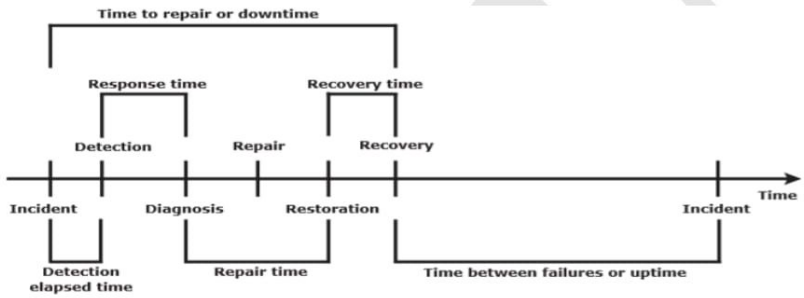


Figure 9-2: Information availability metrics

IA is the ***fraction of a time period*** that a system is in a condition to perform its intended function upon demand. It can be expressed in terms of system uptime and downtime and measured as the amount or percentage of system uptime:

$$IA = \text{system uptime} / (\text{system uptime} + \text{system downtime})$$

In terms of MTBF and MTTR, IA could also be expressed as

$$IA = MTBF / (MTBF + MTTR)$$

Uptime per year is based on the exact timeliness requirements of the service, this calculation leads to the number of "9s" representation for availability metrics.

Table 11-1 lists the approximate amount of downtime allowed for a service to achieve certain levels of 9s availability.

Table 11-1: Availability Percentage and Allowable Downtime

UPTIME (%)	DOWNTIME (%)	DOWNTIME PER YEAR	DOWNTIME PER WEEK
98	2	7.3 days	3 hr 22 minutes
99	1	3.65 days	1 hr 41 minutes
99.8	0.2	17 hr 31 minutes	20 minutes 10 sec
99.9	0.1	8 hr 45 minutes	10 minutes 5 sec
99.99	0.01	52.5 minutes	1 minute
99.999	0.001	5.25 minutes	6 sec
99.9999	0.0001	31.5 sec	0.6 sec

9.2 BC Terminology

This section introduces and defines common terms related to BC operations

1. **Disaster recovery:** This is the coordinated process of restoring systems, data, and the infrastructure required to support ongoing business operations after the disaster occurs.
    - It is the process of restoring a previous copy of the data and applying logs or other necessary processes to that copy to bring it to a known point of consistency.
    - Once all recoveries are completed, the data is validated to ensure that it is correct.
2. **Disaster restart:** This is the process of restarting business operations with mirrored consistent copies of data and applications.
3. **Recovery-Point Objective (RPO):** This is the point in time to which systems and data must be recovered after an outage. It defines the amount of data loss that a business can endure.
    - A large RPO signifies high tolerance to information loss in a business.
    - Based on the RPO, organizations plan for the minimum frequency with which a backup or replica must be made. Example: if the RPO is six hours, backups or replicas must be made at least once in 6 hours.
    - Figure 11-2 shows various RPOs and their corresponding ideal recovery strategies.
    - An organization can plan for an appropriate BC technology solution on the basis of the RPO it sets. For example:

a. **RPO of 24 hours:** This ensures that backups are created on an offsite tape drive every midnight. The corresponding recovery strategy is to restore data from the set of last backup tapes.

b. **RPO of 1 hour:** This ship database logs to the remote site every hour. The corresponding recovery strategy is to recover the database at the point of the last log shipment.

c. **RPO in the order of minutes:** Mirroring data asynchronously to a remote site.

d. **Near zero RPO:** This mirrors data synchronously to a remote site.

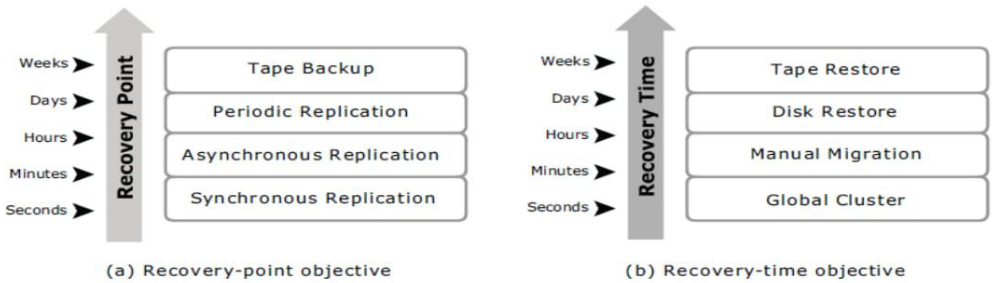


Figure 11-2: Strategies to meet RPO and RTO targets

4. **Recovery-Time Objective (RTO):** The time within which systems, applications, or functions must be recovered after an outage.

   It defines the amount of downtime that a business can endure and survive.

   Businesses can optimize disaster recovery plans after defining the RTO for a given data center or network. For example, if the RTO is two hours, then use a disk backup because it enables a faster restore than a tape backup.

   However, for an RTO of one week, tape backup will likely meet requirements. Some examples of RTOs and the recovery strategies to ensure data availability are listed below (Figure 11-2):

a. **RTO of 72 hours:** Restore from backup tapes at a cold site.

b. **RTO of 12 hours:** Restore from tapes at a hot site.

c. **RTO of 4 hours:** Use a data vault to a hot site.

d. **RTO of 1 hour:** Cluster production servers with controller-based disk mirroring.

e. **RTO of a few seconds:** Cluster production servers with bidirectional mirroring, enabling the applications to run at both sites simultaneously.

Data vault: A repository at a remote site where data can be periodically or continuously copied (either to tape drives or disks) so that there is always a copy at another site

Hot site: A site where an enterprise's operations can be moved in the event of disaster. It is a site with the required hardware, operating system, application, and network support to perform business operations, where the equipment is available and running at all times.

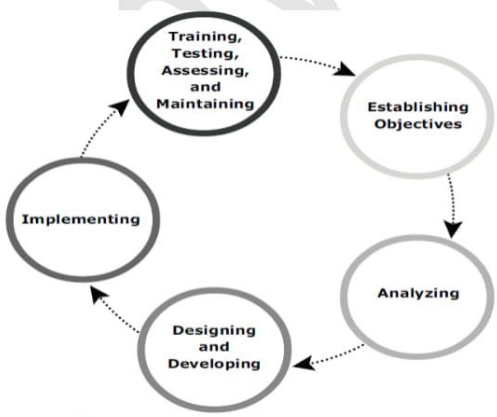
Cold site: A site where an enterprise's operations can be moved in the event of disaster, with minimum IT infrastructure and environmental facilities in place, but not activated

Server Clustering: A group of servers and other necessary resources coupled to operate as a single system. Clusters can ensure high availability and load balancing. Typically, in failover clusters, one server runs an application and updates the data, and another server is kept as standby to take over completely, as required. Server clustering provides load balancing by distributing the application load evenly among multiple servers within the cluster.

11.3 BC Planning Lifecycle

BC planning must follow a disciplined approach like any other planning process. From the conceptualization to the realization of the BC plan, a lifecycle of activities can be defined for the BC process. The BC planning lifecycle includes five stages (see Figure 11-3):

1. Establishing objectives
2. Analyzing
3. Designing and developing
4. Implementing
5. Training, testing, assessing, and maintaining



e 11-3: BC planning lifecycle

Several activities are performed at each stage of the BC planning lifecycle, including the following key activities:

1. ***Establishing objectives***

- Determine BC requirements.
- Estimate the scope and budget to achieve requirements.
- Select a BC team by considering subject matter experts from all areas of the business,

whether internal or external.

- Create BC policies.

2. ***Analyzing***

- Collect information on data profiles, business processes, infrastructure support, dependencies, and frequency of using business infrastructure.
- Identify critical business needs and assign recovery priorities.
- Create a risk analysis for critical functions and mitigation strategies.
- Conduct a Business Impact Analysis (BIA).
- Create a cost and benefit analysis based on the consequences of data unavailability.
- Evaluate options.

3. ***Designing and developing***

- Define the team structure and assign individual roles and responsibilities. For example, different teams are formed for activities such as emergency response, damage assessment, and infrastructure and application recovery.
- Design data protection strategies and develop infrastructure.
- Develop contingency scenarios.
- Develop emergency response procedures.
- Detail recovery and restart procedures.

4. ***Implementing***

- Implement risk management and mitigation procedures that include backup, replication, and management of resources.
- Prepare the disaster recovery sites that can be utilized if a disaster affects the primary data center.
- Implement redundancy for every resource in a data center to avoid single points of failure.

5. ***Training, testing, assessing, and maintaining***

- Train the employees who are responsible for backup and replication of business-critical data on a regular basis or whenever there is a modification in the BC plan.
- Train employees on emergency response procedures when disasters are declared.
- Train the recovery team on recovery procedures based on contingency scenarios.

- Perform damage assessment processes and review recovery plans.
- Test the BC plan regularly to evaluate its performance and identify its limitations.
- Assess the performance reports and identify limitations.
- Update the BC plans and recovery/restart procedures to reflect regular changes within the data center.

9.3 Failure Analysis

Failure analysis involves analyzing the data center to identify systems that are susceptible to a single point of failure and implementing fault-tolerance mechanisms such as redundancy.

9.4.1 Single Point of Failure

- A single point of failure refers to the failure of a component that can terminate the availability of the entire system or IT service.

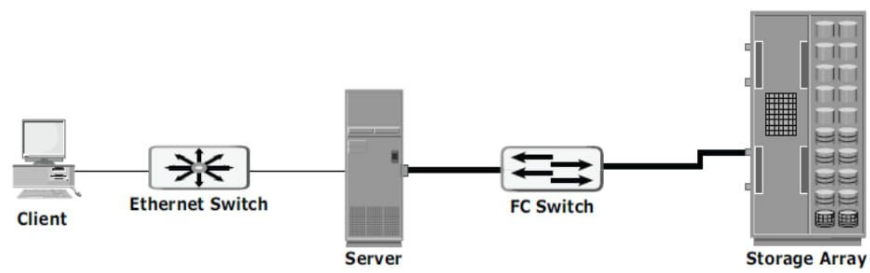


Figure 11-4: Single point of failure

- Figure 11-4 illustrates the possibility of a single point of failure in a system with various components: server, network, switch, and storage array.
- The figure depicts a system setup in which an application running on the server provides an interface to the client and performs I/O operations.
- The client is connected to the server through an IP network, the server is connected to the storage array through a FC connection, an HBA installed at the server sends or receives data to and from a storage array, and an FC switch connects the HBA to the storage port.
- In a setup where each component must function as required to ensure data availability.
- The failure of single component causes the failure of entire data center/application resulting

in disruption of business operations.

- In this example, several single points of failure can be identified. i.e. HBA on the server, the server itself, the IP network, FC switch, the storage array ports, or even storage array can become potential single point of failure.
- To avoid this situation, it is essential to implement fault tolerance mechanism.

9.4.2 Resolving Single Point of Failure: Fault Tolerance

- To overcome single point of failure, systems are designed with redundancy such that system will fail only if all the components in the redundancy group fail.
- This ensures that the failure of a single component does not affect data availability. Figure 11-5 illustrates the fault-tolerant implementation of the system just described (and shown in Figure 11-4).

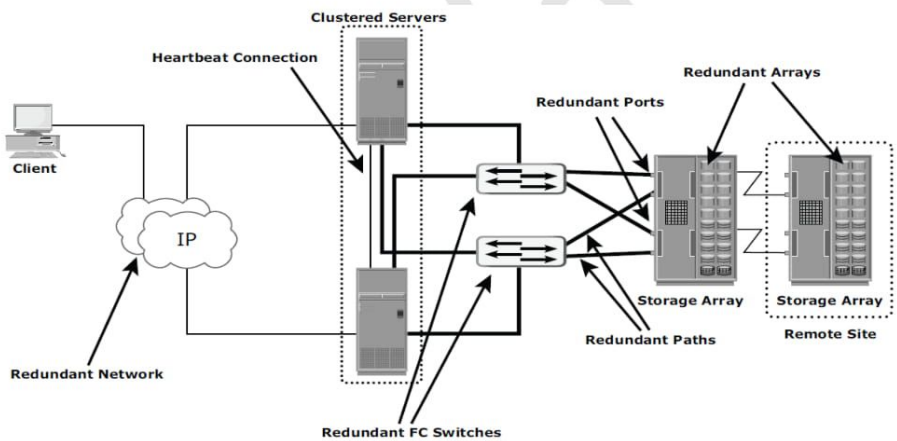


Figure 11-5: Implementation of fault tolerance

- Careful analysis is performed to eliminate every single point of failure, in the example figure below, all enhancements are done in the infrastructures to overcome single points of failure such as

  1. Configuration of multiple HBAs to mitigate single HBA failure.

  2. Configuration of multiple fabrics to account for a switch failure.

  3. Configuration of multiple storage array ports to enhance the storage array's availability.

4. RAID configuration to ensure continuous operation in the event of disk failure.

5. Implementing a storage array at a remote site to mitigate local site failure.

6. Implementing server (host) clustering, a fault-tolerance mechanism whereby two or more servers in a cluster access the same set of volumes. Clustered servers exchange *heartbeats* to inform each other about their health. If one of the servers fails, the other server takes up the complete workload.

9.4.3 Multipathing Software

- Configuring multiple paths increases the data availability through path failover.
- . If servers are configured with one I/O path to the data there will be no access to the data if that path fails. Redundant paths eliminate the path to become single points of failure.
- Multiple paths to data also improve I/O performance through load sharing and maximize server, storage, and data path utilization.

9.5 BC Technology Solutions

After analyzing the business impact of an outage, designing appropriate solutions to recover from a failure is the next important activity. Using one of the strategies data can be recovered and business operations can be restarted using an alternate copy:

o Backup/Restore

Backup to tape has been a predominant method to ensure business continuity

Frequency of backup is depending on RPO/RTO requirements

o Local Replication

Data from the production devices is copied to replica devices within the same array

The replicas can then be used for restore operations in the event of data corruption or other events

o Remote Replication

Data from the production devices is copied to replica devices on a remote array

In the event of a failure, applications can continue to run from the target device

Chapter 10

Backup and Recovery

- *A backup* is a copy of production data, created and retained for the sole purpose of recovering deleted or corrupted data.
- Data archiving is the process of moving data that is no longer actively used, from primary storage to a low-cost secondary storage.
- Backup Purpose
  1. Disaster Recovery
  2. Operational Recovery
  3. Archival

10.1 Backup Methods

There are two methods; cold backup and hot backup. They are based on the state of the application when the backup is performed.

1. **Hot backup**

- In a hot backup, the application is up-and-running with users accessing their data during the backup process. This method is also referred as an **online backup.**
- Hot backup of online data is challenging because data is actively used and changed. If a file is open, it is normally not backed up during the backup process. In such situations, an open file agent is required to back up the open file.
- These agents interact directly with the operating system or application and enable the creation of consistent copies of open files.
- In database environments, the use of open file agents is not enough, because the agent should also support a consistent backup of all the database components.

- Consistent backups of databases can also be done by using a cold backup. This requires the database to remain inactive during the backup.
- Hot backup is used in situations where it is not possible to shut down the database. This is facilitated by ***database backup agents*** that can perform a backup while the database is active.

Disadvantages of a hot backup

- The agents usually affect the overall application performance.

2. Cold backup

- In a cold backup, the application is shut down during the backup process. Hence this method is referred as offline backup.
- Consistent data backup can be done using cold backup due to it requires the database to remain inactive during the backup.
- The **disadvantage** of a cold backup is that the database is inaccessible to users during the backup process.

❖ A ***point-in-time (PIT)*** copy method is deployed in environments where the impact of downtime from a cold backup or the performance resulting from a hot backup is unacceptable. A pointer-based PIT copy consumes only a fraction of the storage space and can be created very quickly. The PIT copy is created from the production volume and used as the source for the backup. This reduces the impact on the production volume.

❖ In a disaster recovery environment, ***bare-metal recovery (BMR)*** refers to a backup in which all metadata, system information, and application configurations are appropriately backed up for a full system recovery.

Backup Architecture and Process

- **Backup client**

  Sends backup data to backup server or storage node

- **Backup server**

  Manages backup operations and maintains backup catalog

- **Storage node**

  Responsible for writing data to backup device

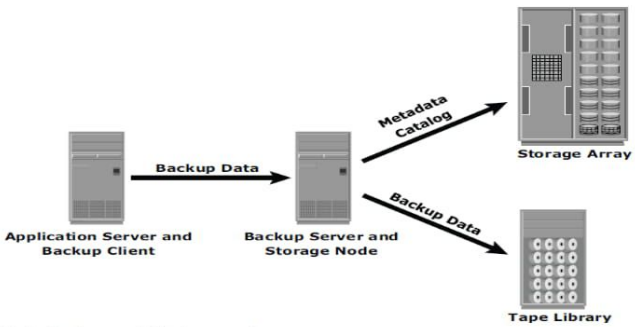


Figure 12-4: Backup architecture and process

Backup and Restore Operations

When a backup process is initiated, significant network communication takes place between the different components of a backup infrastructure. The backup server initiates the backup process for different clients based on the backup schedule configured for them. For example, the backup process for a group of clients may be scheduled to start at 3:00 am every day.

The backup server coordinates the backup process with all the components in a backup configuration (see Figure 12-5). The backup server maintains the information about backup clients to be contacted and storage nodes to be used in a backup operation. The backup server retrieves the backup-related information from the backup catalog and, based on this information, instructs the storage node to load the appropriate backup media into the backup devices. Simultaneously, it instructs the backup clients to start scanning the data, package it, and send it over the network to the assigned storage node. The storage node, in turn, sends metadata to the backup server to keep it updated about the media being used in the backup process. The backup server continuously updates the backup catalog with this information.

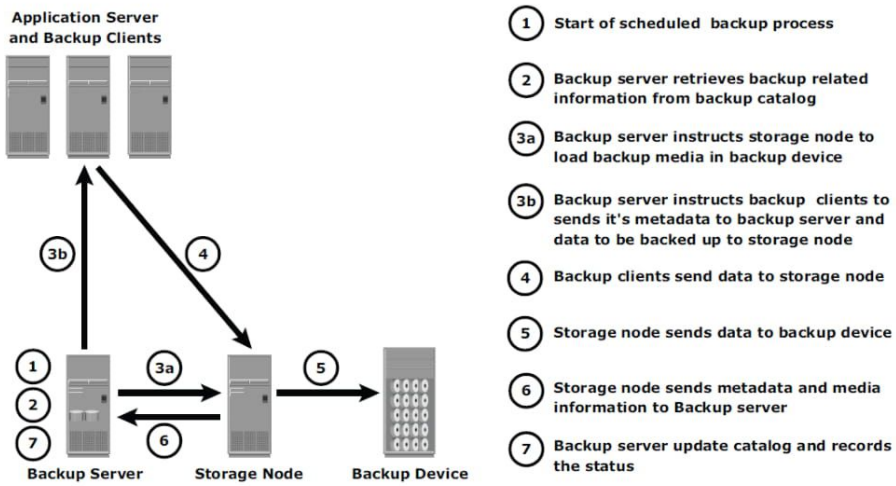


Figure 12-5: Backup operation

After the data is backed up, it can be restored when required. A restore process must be manually initiated. Some backup software has a separate application for restore operations. These restore applications are accessible only to the administrators.

Figure 12-6 depicts a restore process.

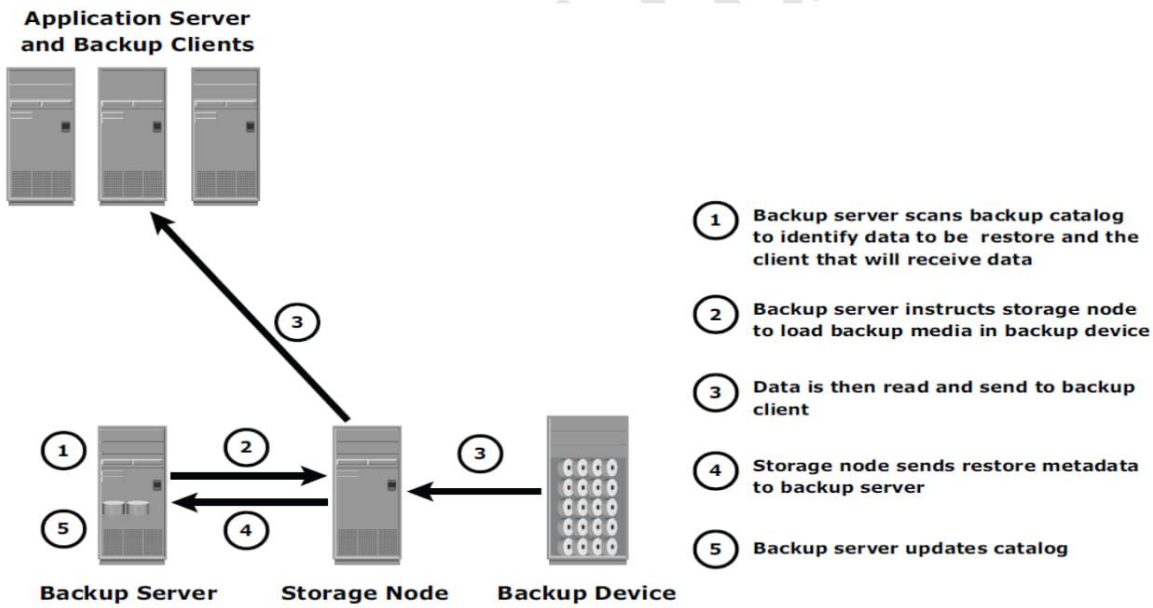


Figure 12-6: Restore operation

Upon receiving a restore request, an administrator opens the restore application to view the list of clients that have been backed up. While selecting the client for which a restore request has been made, the administrator also needs to identify the client that will receive the restored data. Data can be restored on the same client for whom the restore request has been made or on any other client.

The administrator then selects the data to be restored and the specified point in time to which the data has to be restored based on the RPO. Note that because all of this information comes from the backup catalog, the restore application must also communicate to the backup server.
The administrator first selects the data to be restored and initiates the restore process. The backup server, using the appropriate storage node, then identifies the backup media that needs to be mounted on the backup devices. Data is then read and sent to the client that has been identified to receive the restored data.

10.2 Backup Topologies

Three basic topologies are used in a backup environment:

1. Direct attached backup,
2. LAN based backup,
3. SAN based backup.
4. A mixed topology is also used by combining LAN based and SAN based topologies.

1. Direct attached backup

- In a direct-attached backup, the storage node is configured on a backup client, and the backup device is attached directly to the client.
- Only the metadata is sent to the backup server through the LAN.
- This configuration frees the LAN from backup traffic.

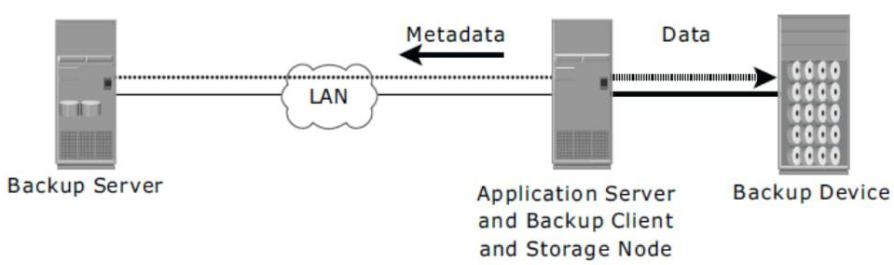


Figure 12-7: Direct-attached backup topology

- Figure 12-7 depicts use of a backup device that is not shared, the backup device is directly attached and dedicated to the backup client.
- As the environment grows, there will be a need for central management of all backup

devices and sharing of backup devices to optimize costs.

- **Disadvantage:** Not possible to share the backup devices among multiple servers.
- Network-based topologies (LAN-based and SAN-based) provide the solution to optimize the utilization of backup devices.

2. LAN Based Backup

- In a LAN-based backup, the clients, backup server, storage node, and backup device are connected to the LAN.
- The data to be backed up is transferred from the backup client (source) to the backup device (destination) over the LAN, which might affect network performance.

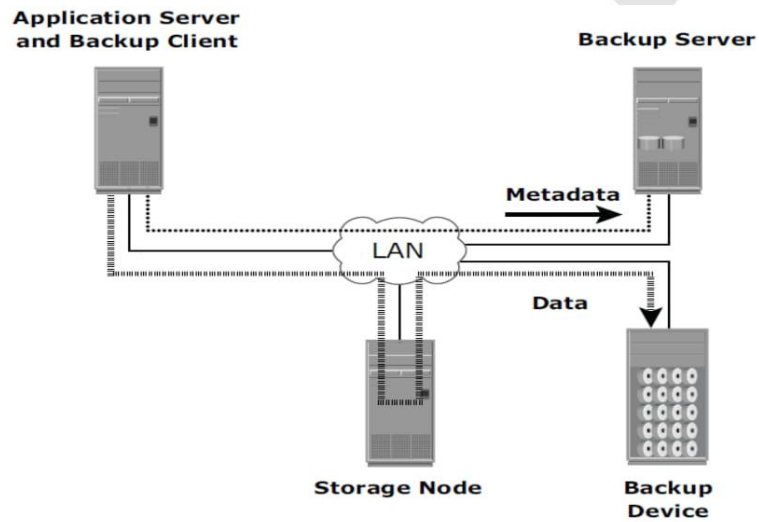


Figure 12-8: LAN-based backup topology

- This impact can be minimized by adopting a number of measures, such as configuring separate networks for backup and installing dedicated storage nodes for some application servers.

3. SAN Based Backup

- A SAN-based backup is also known as a **LAN-free backup.**
- This topology is most appropriate solution when a backup device needs to be shared among the clients. In this case the backup device and clients are attached to the SAN.

- A client sends the data to be backed up to the backup device over the SAN, only the backup metadata is transported over the LAN.
- Figure 10-9 illustrates a SAN-based backup.

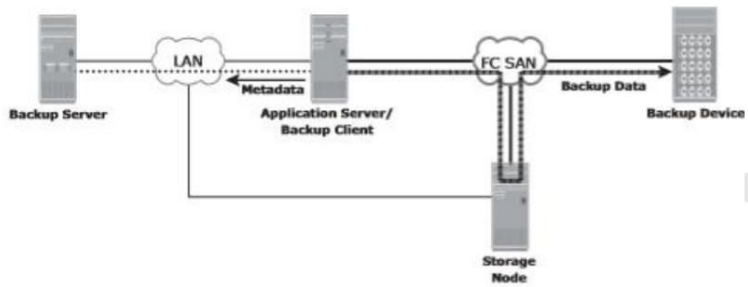
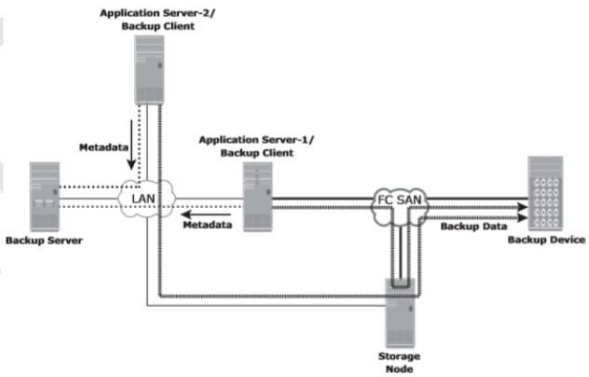


Figure 10-9: SAN-based backup topology

- In this example, a client sends the data to be backed up to the backup device over the SAN. Therefore, the backup data traffic is restricted to the SAN, and only the backup metadata is transported over the LAN. The volume of metadata is insignificant when compared to the production data; the LAN performance is not degraded in this configuration.

4. Mixed topology

- The mixed topology uses both the LAN-based and SAN-based topologies, as shown in Figure



- This topology might be implemented for several reasons, including cost, server location, reduction in administrative overhead, and performance considerations.

10.3 Backup Targets

A wide range of technology solutions are currently available for backup targets. Tape and disk libraries are the two most commonly used backup targets.

10.3.1 Backup to Tape

- ✓ Tapes, a low-cost technology, are used extensively for backup.
- ✓ Tape drives are used to read/write data from/to a tape cartridge. Tape drives are referred to as sequential, or linear, access devices because the data is written or read sequentially.
- ✓ Tape mounting is the process of inserting a tape cartridge into a tape drive. The tape drive has motorized controls to move the magnetic tape around, enabling the head to read or write data.

10.3.1 Physical Tape Library

- o The physical tape library provides housing and power for a large number of tape drives and tape cartridges, along with a robotic arm or picker mechanism.
- o The backup software has intelligence to manage the robotic arm and entire backup process.

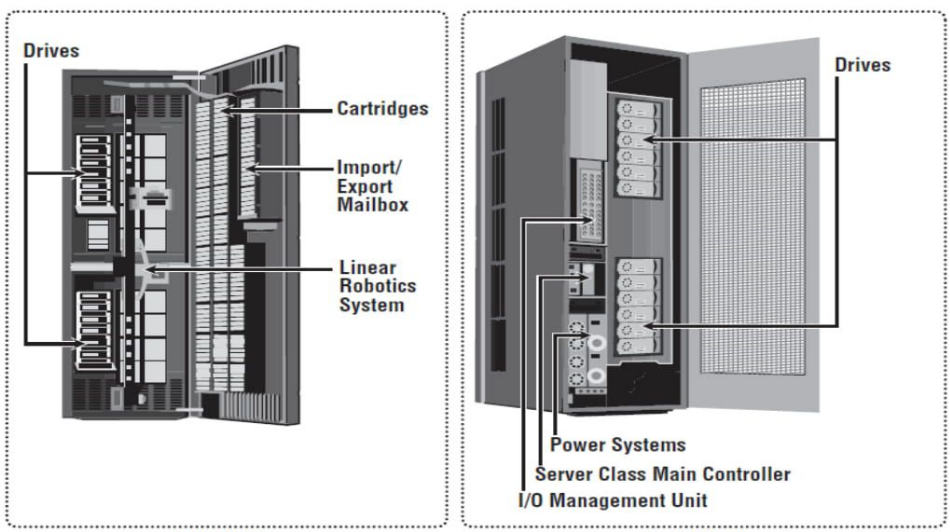


Figure 12-15: Physical tape library

- o Tape drives read and write data from and to a tape. Tape cartridges are placed in the slots when not in use by a tape drive. Robotic arms are used to move tapes between

cartridge slots and tape drives. Mail or import/export slots are used to add or remove tapes from the library without opening the access doors.

- When a backup process starts, the robotic arm is instructed to load a tape to a tape drive. This process adds the delay.
- The time taken to position the heads and validate header information is called load or ready time.
- The tape receives the backup data and stores in its internal buffer as blocks. The speed of the tape drives can also be adjusted to match the data transfer rate.
- To improve performance tape drive using multiple streaming; writes data from multiple streams on a single tape to keep the drive busy.
- Tape drive *streaming* or *multiple streaming* writes data from multiple streams on a single tape to keep the drive busy. Shown in Figure 12-16, multiple streaming improves media performance, but it has an associated disadvantage. The backup data is interleaved because data from multiple streams is written on it. Consequently, the data recovery time is increased.

Figure 12-16: Multiple streams on tape media

Limitations of Tape

- Tapes are primarily used for long-term offsite storage because of their low cost.
- Tapes must be stored in locations with a controlled environment to ensure preservation of the media and prevent data corruption.
- Data access in a tape is sequential, which can slow backup and recovery operations. Physical transportation of the tapes to offsite locations also adds management overhead.

10.3.3 Backup to Disk

Advantage over Backup to tape

- ❖ Disks have now replaced tapes as the primary device for storing backup data because of their performance advantages. Backup-to-disk systems offer ease of implementation, reduced cost, and improved quality of service. Apart from performance benefits in terms of data transfer rates, disks also offer faster recovery when compared to tapes.

- o Backing up to disk storage systems offers clear advantages due to their inherent random access and RAID-protection capabilities.

- o Backup to disk copies the data temporarily before transferring or staging it to tapes, this enhances the performance.

- o Some backup products allow for backup images to remain on the disk for a period of time even after they have been staged. This enables a much faster restore.

- o Recovering from a full backup copy stored on disk and kept onsite provides the fastest recovery solution.

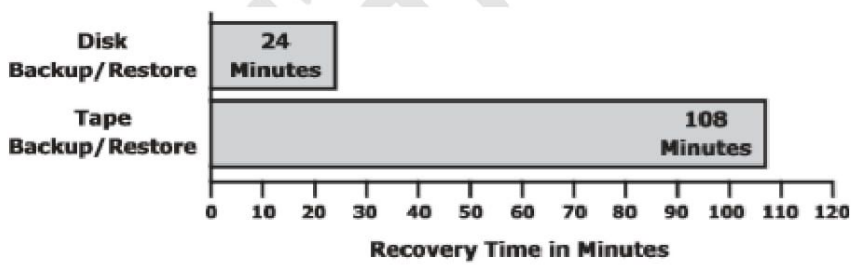


Figure 10-17: Tape versus disk restore

- o The above figure shows the comparison between disks that supports 800 users with a 75 MB mailbox and a 60GB database. It is observed that disk took 24 mins compared to the restore from tape, which took 108 mins for the same environment.

3. Backup to Virtual Tape

Virtual tapes are disk drives emulated and presented as tapes to the backup software. The key benefit of using a virtual tape is that it does not require any additional modules, configuration,

or changes in the legacy backup software. This preserves the investment made in the backup software.

Virtual Tape Library

- Components of Virtual Tape Library (VLT) are same as physical tape drive library, except that the majority of the components are presented as virtual resources.
- Backup software; there is no difference between physical tape library and a virtual tape library.
- Virtual tape libraries use disks as backup media.
- Emulation software has a database with a list of virtual tapes, and each virtual tape is assigned space on a LUN.
- Similar to physical tape library, a robot mount is virtually performed when a backup process starts in a virtual tape library; it does not involve any mechanical delays as in physical tape library. Even the load and ready time is much less than the physical tape library.
- After the virtual tape is mounted and the virtual tape drive is positioned, the virtual tape is ready to be used, and backup data can be written to it. In most cases the data is written immediately.
- Compared to physical tapes, virtual tapes offer better single stream performance, better reliability, and random disk access characteristics.
- Backup and restore operations are online and provide faster backup and recovery.
- The steps to restore data are similar to physical tape library but the restore operation is nearly instantaneous. Even though virtual tapes are based on disks, which provide random access, they still emulate the tape behavior.

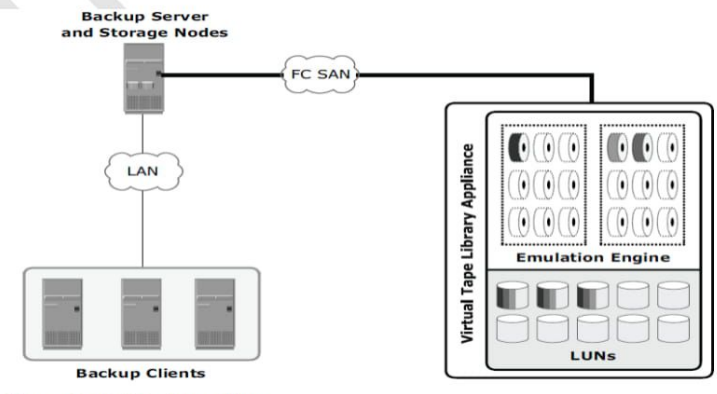


Figure 12-18: Virtual tape library

Advantages

- Using virtual tape offers several advantages over both physical tapes and disks. Compared to physical tape, virtual tape offers better single stream performance, better reliability, and random disk access characteristics.
- Backup and restore operations are sequential by nature, but they benefit from the disk's random-access characteristics because they are always online and ready to be used, improving backup and recovery times.
- Virtual tape does not require the usual maintenance tasks associated with a physical tape drive, such as periodic cleaning and drive calibration.
  - Compared to back up-to-disk devices, virtual tapes offer easy installation and administration and inherent offsite capabilities.

Data Deduplication for Backup

Data deduplication is the process of identifying and eliminating redundant data. Data deduplication helps to reduce the storage requirement for backup, shorten the backup window, and remove the network burden. It also helps to store more backups on the disk and retain the data on the disk for a longer time.

Data Deduplication Methods

There are two methods of deduplication: file level and subfile level.

File-level deduplication (also called ***single-instance storage***)

- It detects and removes redundant copies of identical files.
- It enables storing only one copy of the file; the subsequent copies are replaced with a pointer that points to the original file.
- File-level deduplication is simple and fast but does not address the problem of duplicate content inside the files.

Subfile deduplication

- It breaks the file into smaller chunks and then uses a specialized algorithm to detect

redundant data within and across the file. There are two forms of subfile deduplication:

- The **fixed-length block deduplication** divides the files into fixed length blocks and uses a hash algorithm to find the duplicate data.
- In **variable-length segment deduplication**, if there is a change in the segment, the boundary for only that segment is adjusted, leaving the remaining segments unchanged. This method vastly improves the ability to find duplicate data segments compared to fixed-block.

Data Deduplication Implementation

1. Source based data deduplication

- Source-based data deduplication eliminates redundant data at the source before it transmits to the backup device.
- Source-based data deduplication can dramatically reduce the amount of backup data sent over the network during backup processes.
- It provides the benefits of a shorter backup window and requires less network bandwidth.
- There is also a substantial reduction in the capacity required to store the backup images.
- Source-based deduplication increases the overhead on the backup client, which impacts the performance of the backup and application running on the client.

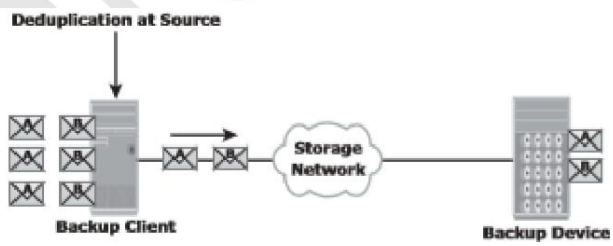


Figure 10-19: Source-based data deduplication

2. Target based data deduplication

- Target-based data deduplication occurs at the backup device, which offloads the backup client from the deduplication process.
- In this case, the backup client sends the data to the backup device and the data is

deduplicated at the backup device, either immediately (inline) or at a scheduled time (post-process).

- Backup data needs to be transferred over the network, which increases network bandwidth requirements.

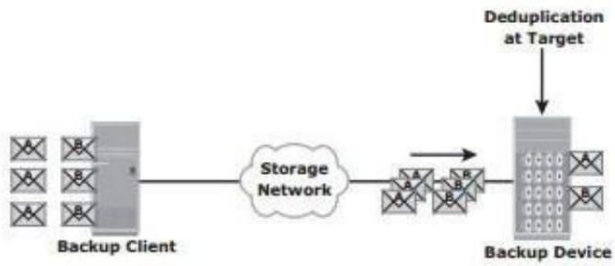


Figure 10-20: Target-based data deduplication

3. Inline deduplication

- It performs deduplication on the backup data before it is stored on the backup device. Hence, this method reduces the storage capacity needed for the backup.
- Inline deduplication introduces overhead in the form of the time required to identify and remove duplication in the data. So, this method is best suited for an environment with a large backup window.

4. Post-process deduplication

- It enables the backup data to be stored or written on the backup device first and then deduplicated later.
- This method is suitable for situations with tighter backup windows.
- Post-process deduplication requires more storage capacity to store the backup images before they are deduplicated.

Backup in Virtualized Environment

In a virtualized environment, it is imperative to back up the virtual machine data (OS, application data, and configuration) to prevent its loss or corruption due to human or technical errors. There are two approaches for performing a backup in a virtualized environment: the traditional backup

approach and the image-based backup approach.

1. Traditional Backup approach

- A backup agent is installed either on the virtual machine (VM) or on the hypervisor.
- If the backup agent is installed on a VM, the VM appears as a physical server to the agent.

Figure 10-21: Traditional VM backup

- The backup agent installed on the VM backs up the VM data to the backup device. The agent does not capture VM files, such as the virtual BIOS file, VM swap file, logs, and configuration files. Therefore, for a VM restore, a user needs to manually re-create the VM and then restore data onto it.
- VM files are backed up by performing a file system backup from a hypervisor. This approach is relatively simple because it requires having the agent just on the hypervisor instead of all the VMs.
- The backup should be performed when the server resources are idle or during a low activity period on the network.

2. Image-based backup approach

- It operates at the hypervisor level and takes the snapshot of the VM. It creates a copy of the guest OS and all the associated with, including the VM state and application configurations.
- The backup is saved as a single file called an 'image' and this image is mounted on the separate physical machine-proxy server, which acts as a backup client.
- Image based backup enables quick restoration of a VM.

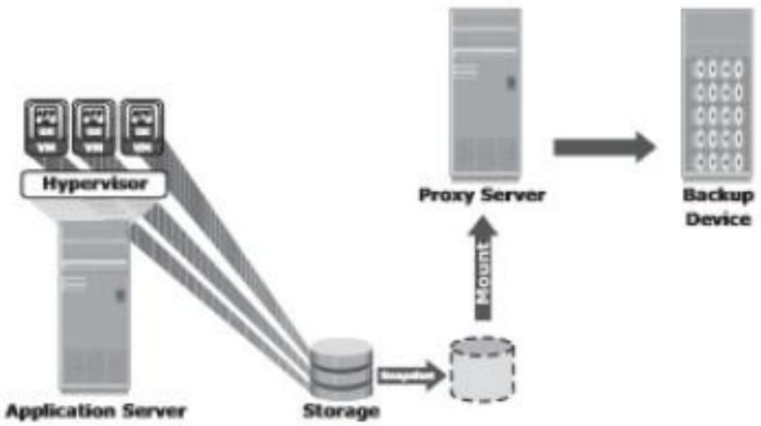


Figure 10-22: Image-based backup

Data Archive

In the life cycle of information, data is actively created, accessed, and changed. As data ages, it is less likely to be changed and eventually becomes "fixed" but continues to be accessed by applications and users. This data is called fixed content. X-rays, e-mails, and multimedia files are examples of fixed content. A repository where fixed content is stored is known as an archive.

An archive can be implemented as an online, nearline, or offline solution:

- **Online archive:** A storage device directly connected to a host that makes the data immediately accessible.
- **Nearline archive:** A storage device connected to a host, but the device where the data is stored must be mounted or loaded to access the data.
- **Offline archive:** A storage device that is not ready to use. Manual intervention is required to connect, mount, or load the storage device before data can be accessed.

Chapter 11

Local Replication

Replication Terminology

The common terms used to represent various entities and operations in a replication environment are listed below:

- **Source:** A host accessing the production data from one or more LUNs on the storage array is called a production host, and these LUNs are known as source LUNs (devices/volumes), production LUNs, or simply the source.
- **Target:** A LUN (or LUNs) on which the production data is replicated, is called the target LUN or simply the target or replica.
- **Point-in-Time (PIT) and continuous replica:** Replicas can be either a PIT or a continuous copy.
    - The PIT replica is an identical image of the source at some specific timestamp.
    - The continuous replica is in-sync with the production data at all times.
- **Recoverability and restart ability:**
    - Recoverability enables restoration of data from the replicas to the source if data loss or corruption occurs.
    - Restart ability enables restarting business operations using the replicas.

Uses of Local Replicas

- **Alternative source for backup:. The** local replica contains an exact point-in-time (PIT) copy of the source data, and therefore can be used as a source to perform backup operations. This alleviates the backup I/O workload on the production volumes. Another benefit of using local replicas for backup is that it reduces the backup window to zero.
- **Fast Recovery:**
    - If data loss or data corruption occurs on the source, a local replica might be used to recover the lost or corrupted data.
    - If a complete failure of the source occurs, some replication solutions enable a replica to be used to restore data onto a different set of source devices, or production can be restarted on the replica.

- In either case, this method provides faster recovery and minimal RTO compared to traditional recovery from tape backups.

- **Decision-support activities, such as reporting or data warehousing:** Running the reports using the data on the replicas greatly reduces the I/O burden placed on the production device. The data-warehouse application may be populated by the data on the replica and thus avoid the impact on the production environment.
- **Testing Platform:** Local replicas are also used for testing new applications or upgrades.
- **Data migration:** Data migrations are performed for various reasons, such as migrating from a smaller capacity LUN to one of a larger capacity for newer versions of the application.

Local Replication Technologies

Host-based, storage array-based and network-based replications are the major technologies used for local replication.

Host-Based Local Replication

LVM-based replication and file system (FS) snapshot are two common methods of host-based local replication.

LVM-Based Replication

- In *LVM-based replication*, the logical volume manager is responsible for creating and controlling the host-level logical volumes.
- An LVM has three components: physical volumes (physical disk), volume groups, and logical volumes.
  - A *volume group* is created by grouping one or more physical volumes.
  - *Logical volumes* are created within a given volume group.
- Each *logical block* in a logical volume is mapped to two physical blocks on two different

physical volumes, as shown in figure

- An application write to a logical volume is written to the two physical volumes by the LVM device driver. This is also known as *LVM mirroring*.

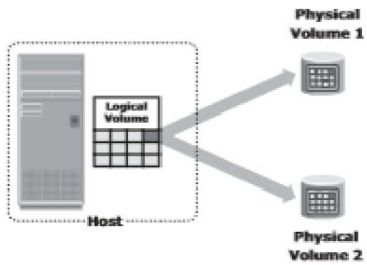


Figure 11-5: LVM-based mirroring

Advantages

- ✓ The LVM-based replication technology is not dependent on a vendor-specific storage system. No additional license is required to deploy LVM mirroring

Limitation

- × Every write generated by an application translates into two writes on the disk, and thus, an additional burden is placed on the host CPU. This can degrade application performance.
- × Tracking changes to the mirrors and performing incremental resynchronization operations is also a challenge because all LVMs do not support incremental resynchronization.

File system snapshot

A file system (FS) snapshot is a pointer-based replica, this snapshot can be implemented by either FS or by LVM. It uses the Copy on First Write (CoFW) principle to create snapshots.

- When a snapshot is created, a bitmap and block map is created in the metadata of the Snap FS. The bitmap is used to keep track of blocks that are changed on the production FS after the snap creation. The bitmap is used to keep track of blocks that are changed on the production FS after the snap creation.

- In a CoFW mechanism, if a write I/O is issued to the production FS for the first time after the creation of a snapshot, the I/O is held and the original data of production FS corresponding to that location is moved to the Snap FS. Then, the write is allowed to the production FS. The bitmap and blockmap are updated accordingly.
- To read from the Snap FS, the bitmap is consulted. If the bit is 0, then the read is directed to the production FS. If the bit is 1, then the block address is obtained from the block map, and the data is read from that address on the Snap FS.
- Figure below illustrates the write operations to the production file system.
- A write data "C" occurs on block 3 at the production FS, which currently holds data "c"' The snapshot application holds the I/O to the production FS and first copies the old data "c" to an available data block on the Snap FS.
- The bitmap and block map values for block 3 in the production FS are changed in the snap metadata.
- The bitmap of block 3 is changed to 1, indicating that this block has changed on the production FS. The blockmap of block 3 is changed and indicates the block number where the data is written in Snap FS, (in this case block 2).
- After this is done, the I/Os to the production FS are allowed to complete.
- Any subsequent writes to block 3 on the production FS occur as normal, and it does not initiate the CoFW operation.
- Similarly, if an I/O is issued to block 4 on the production FS to change the value of data "d" to "D," the snapshot application holds the I/O to the production FS and copies the old data to an available data block on the Snap FS.
- Then it changes the bitmap of block 4 to 1, indicating that the data block has changed on the production FS.

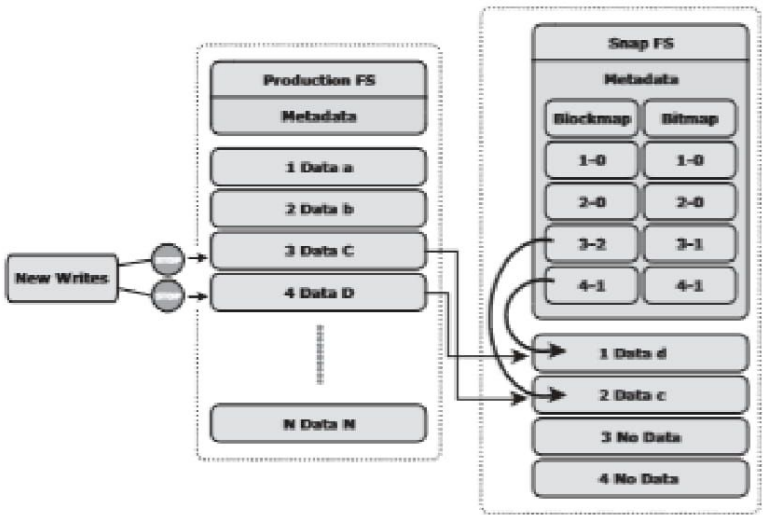


Figure 11-6: Write to production FS

- The blockmap for block 4 indicates the block number where the data can be found on the Snap FS, in this case, data block 1 of the Snap FS
- After this is done, the I/O to the production FS is allowed to complete.

Storage Array-Based Local Replication

• In this, the array-operating environment performs the local replication process. The host resources, such as the CPU and memory are not used in the replication process.

• In this replication process, the required number of replica devices should be selected on the same array and then data should be replicated between the source-replica pairs.

• Below figure shows a storage array-based local replication, where the source and target are in the same array and accessed by different hosts.

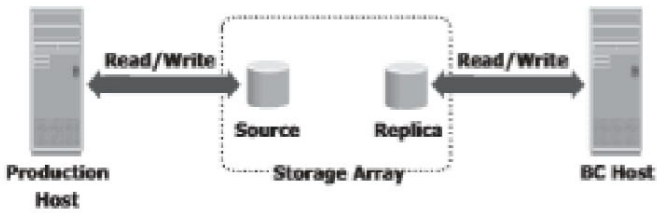
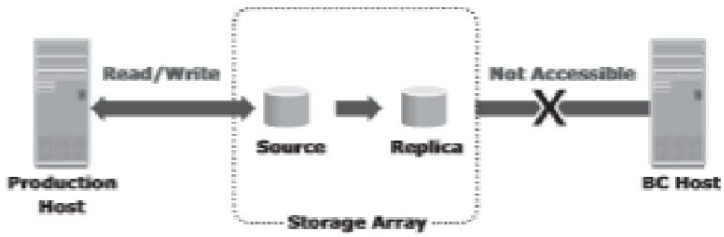


Figure 11-7: Storage array-based local replication

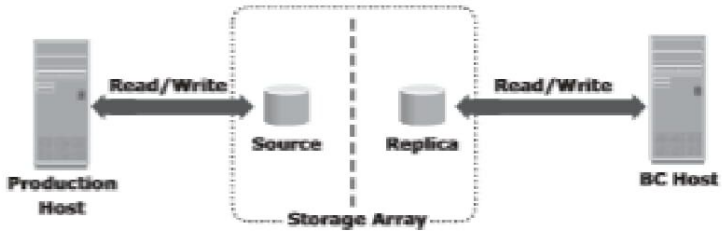
- Storage array-based local replication is implemented in three ways:
  - Full-Volume mirroring
  - Pointer-based full-volume replication
  - Pointer-based virtual replication

Full-Volume Mirroring

- In full-volume mirroring, the target is attached to the source and established as a mirror of the source
- Figure (a) the data is copied to the source to the target. New updates to the source are also updated to the target i.e., both source and target contains identical data, the target can be considered as a mirror of the source.
- Figure (b) shows full-volume mirroring when the target is detached from the source. Both the source and the target can be accessed for read and write operations by the production and business continuity hosts respectively.



(a) Full Volume Mirroring with Source Attached to Replica



(b) Full Volume Mirroring with Source Detached from Replica

Figure 11-8: Full-volume mirroring

Pointer-Based Full-Volume Replication

• Similar to full-volume, this technology can provide full copies of the source data on the targets.

• Unlike full-volume mirroring, the target is immediately accessible by the BC host after the replication session is activated.

• Pointer-based, full-volume replication can be activated in either

1. Copy on First Access (CoFA) mode
2. Full Copy mode.

• In either case, at the time of activation, a protection bitmap is created for all data on the source devices. The protection bitmap keeps track of the changes at the source device.

• The pointers on the target are initialized to map the corresponding data blocks on the source.

• After replication, the data is copied from source to target only when the following condition occurs;

- A write I/O is issued to a specific address on the source for the first time.
- A read or write I/O is issued to a specific address on the target for the first time.

• When a write is issued to the source for the first time after replication session activation, the original data at that address is copied to the target. After this operation, the new data is updated on the source. This ensures that the original data at the point-in-time of activation is preserved on the target (see Figure 11-9).

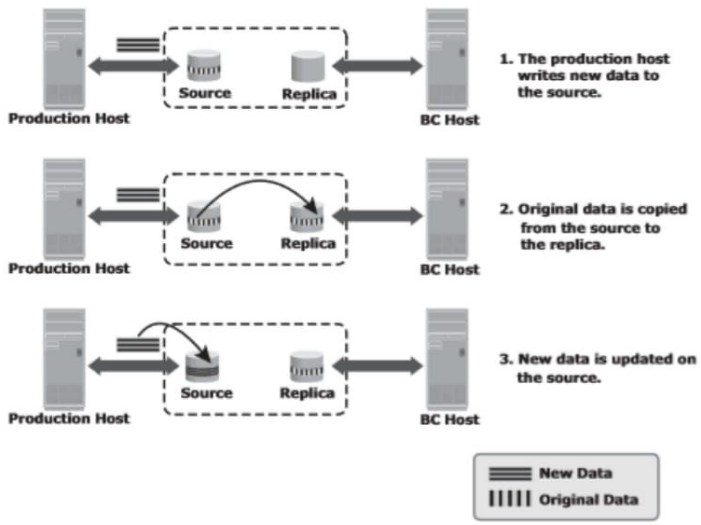


Figure 11-9: Copy on first access (CoFA) – write to source

• When a read is issued to the target for the first time after replication session activation, the original data is copied from the source to the target and is made available to the BC host (see Figure 11-10).

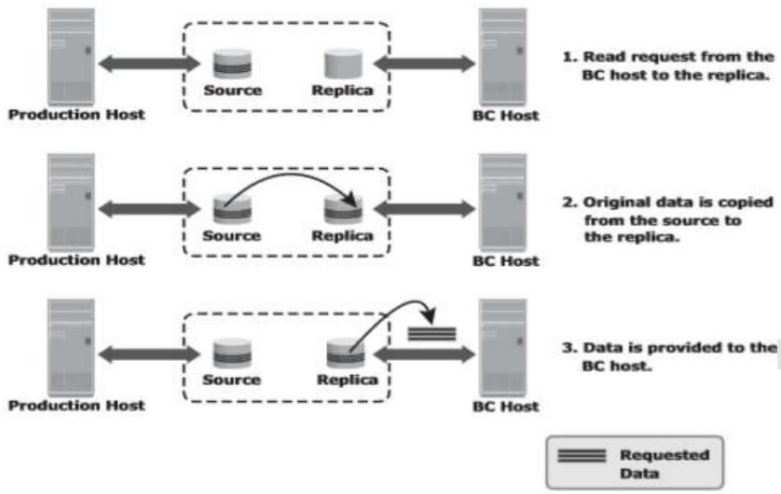


Figure 11-10: Copy on first access (CoFA) – read from target

When a write is issued to the target for the first time after the replication session activation, the original data is copied from the source to the target. After this, the new data is updated on the target (see Figure 11-11).

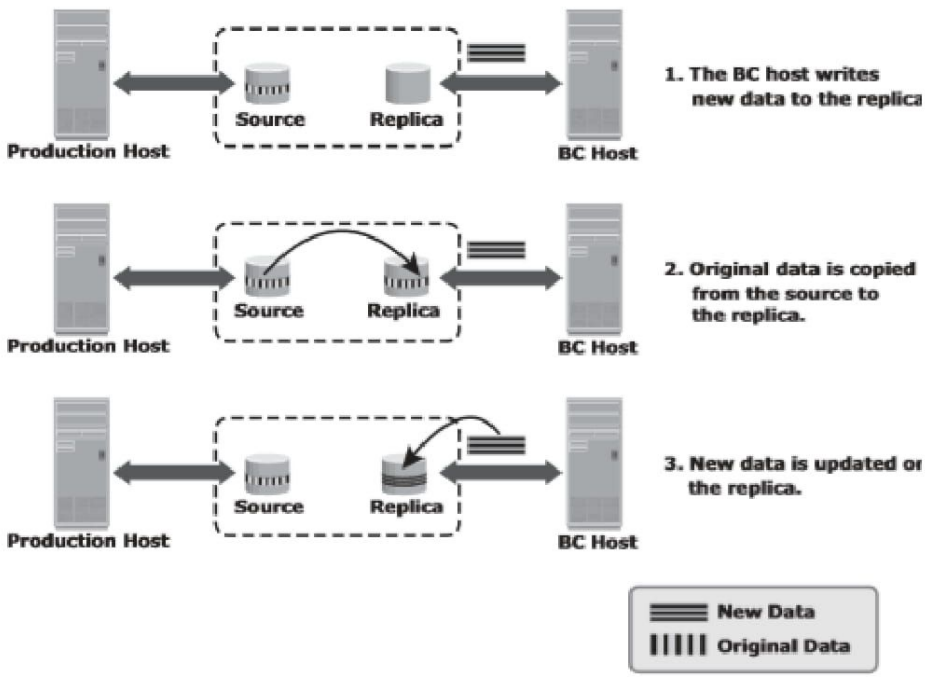


Figure 11-11: Copy on first access (CoFA) – write to target

In all cases, the protection bit for that block is reset to indicate that the original data has been copied over to the target. The pointer to the source data can now be discarded.

Subsequent writes to the same data block on the source, and reads or writes to the same data blocks on the target, do not trigger a copy operation (and hence are termed Copy on First Access).

2. Full Copy Mode

On session start, the entire contents of the Source device are copied to the Target device in the background. If the replication session is terminated, the target will contain all the original data from the source at the PIT of activation. Target can be used for restore and recovery In CoFA mode, the target will only have data was accessed until termination, and therefore it cannot be used for restore and recovery Most vendor implementations provide the ability to track changes:

- Made to the Source or Target
- Enables incremental re-synchronization

Pointer-Based Virtual Replication

- In *pointer-based virtual replication*, at the time of session activation, the target contains pointers to the location of data on the source.
- The target does not contain data, at any time. Hence, the target is known as a *virtual replica*. Similar to pointer-based full-volume replication, a protection bitmap is created for all data on the source device, and the target is immediately accessible. Granularity can range from 512-byte blocks to 64 KB blocks or greater.
- When a write is issued to the source for the first time after session activation, original data at that address is copied to a predefined area in the array. This area is generally termed the *save location*. The pointer in the target is updated to point to this data address in the save location. After this, the new write is updated on the source. This process is illustrated in Figure 13-10.

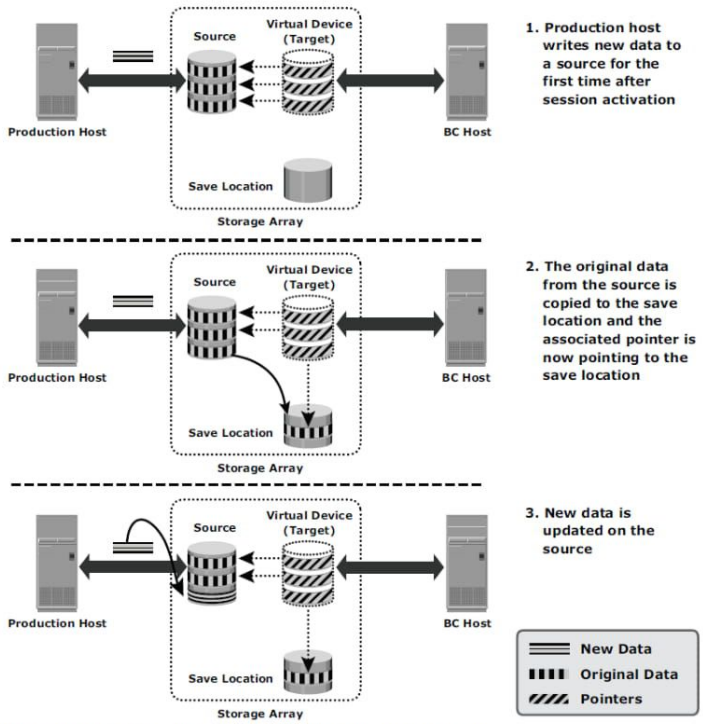


Figure 13-10: Pointer-based virtual replication – write to source

- When a write is issued to the target for the first time after session activation, original data is copied from the source to the save location and similarly the pointer is updated to data in save location. Another copy of the original data is created in the save location before the new write is updated on the save location. This process is illustrated in Figure 13-11.
- When reads are issued to the target, unchanged data blocks since session activation are read from the source. Original data blocks that have changed are read from the save location.
- Pointer-based virtual replication uses CoFW technology. Subsequent writes to the same data block on the source or the target do not trigger a copy operation.
- Data on the target is a combined view of unchanged data on the source and data on the save location. Unavailability of the source device invalidates the data on the target. As the target only contains pointers to data, the physical capacity required for the target is a fraction of the source device. The capacity required for the save location depends on the amount of expected data change.

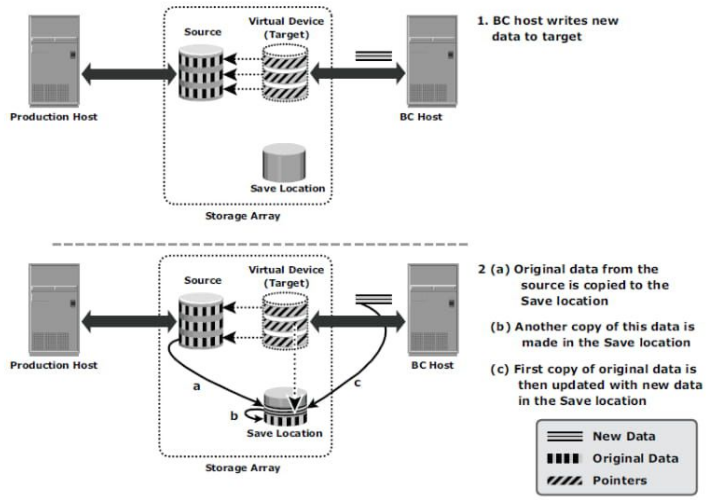


Figure 13-11: Pointer-based virtual replication – write to target

Network-Based Local Replication

- In network-based replication, the replication occurs at the network layer between the hosts and storage arrays.
- Network-based replication combines the benefits of array-based and host-based replications.
- By offloading replication from servers and arrays, network-based replication can work across a large number of server platforms and storage arrays, making it ideal for highly heterogeneous environments. Continuous data protection (CDP) is a technology used for network-based local and remote replications.

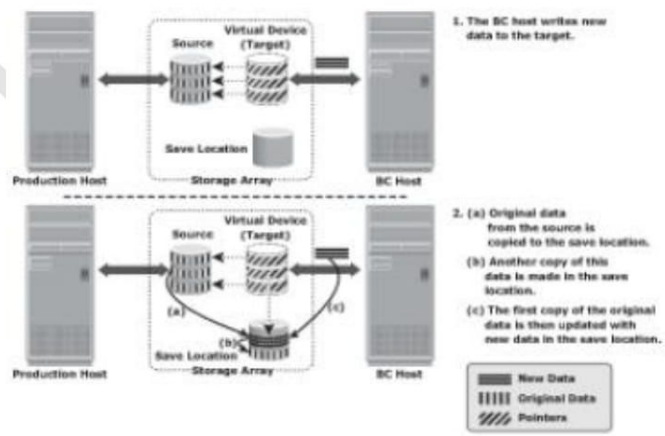


Figure 11-13: Pointer-based virtual replication – write to target

Local Replication in a Virtualized Environment

- Local replication of VMs is performed by the **hypervisor** at the compute level. However, it can also be performed at the **storage level** using **array-based local replication**, similar to the physical environment.
- In the **array-based method**, the LUN on which the VMs reside is replicated to another LUN in the same array.
- For **hypervisor-based** local replication, two options are available: **VM Snapshot and VM Clone.**
- **VM Snapshot** captures the state and data of a running virtual machine at a specific point in time. The VM state includes VM files, such as BIOS, network configuration, and its power state (powered-on, powered-off, or suspended).
- The VM data includes all the fi les that make up the VM, including virtual disks and memory. A VM Snapshot uses a separate delta file to record all the changes to the virtual disk since the snapshot session is activated.
- Snapshots are useful when a VM needs to be reverted to the previous state in the event of logical corruptions.
- Reverting a VM to a previous state causes all settings configured in the guest OS to be reverted to that PIT when that snapshot was created.
- **Challenges:** It does not support data replication if a virtual machine accesses the data by using raw disks.
- Using the hypervisor to perform snapshots increases the load on the compute and impacts the compute performance.
- **VM Clone** is another method that creates an identical copy of a virtual machine. When the cloning operation is complete, the clone becomes a separate VM from its parent VM.
- The clone has its own MAC address, and changes made to a clone do not affect the parent VM. Similarly, changes made to the parent VM do not appear in the clone.
- **Advantages:** VM Clone is a useful method when there is a need to deploy many identical VMs.
- Installing guest OS and applications on multiple VMs is a time-consuming task; VM Clone

helps to simplify this process.

Chapter 12

Remote Replication

Remote replication is the process to create replicas of information assets at remote sites (locations). Remote replication helps organizations mitigate the risks associated with regionally driven outages resulting from natural or human-made disasters

Remote Replication Technologies

Remote replication of data can be handled by the hosts or storage arrays. Other options include specialized network-based appliances to replicate data over the LAN or SAN.

Host-Based Remote Replication

Host-based remote replication uses the host resources to perform and manage the replication operation.

There are two basic approaches to host-based remote replication:

1. Logical volume manager (LVM) based replication
2. Database replication via log shipping.

LVM-Based Remote Replication

- LVM-based remote replication is performed and managed at the volume group level. Writes to the source volumes are transmitted to the remote host by the LVM.
- The LVM on the remote host receives the writes and commits them to the remote volume group. Prior to the start of replication, identical volume groups, logical volumes, and file systems are created at the source and target sites.
- Initial synchronization of data between the source and replica is performed.
- One method to perform initial synchronization is to back up the source data and restore the data to the remote replica.
- Alternatively, it can be performed by replicating over the IP network. Until the completion

of the initial synchronization, production work on the source volumes is typically halted.

- After the initial synchronization, production work can be started on the source volumes and replication of data can be performed over an existing standard IP network (Fig 12-5).

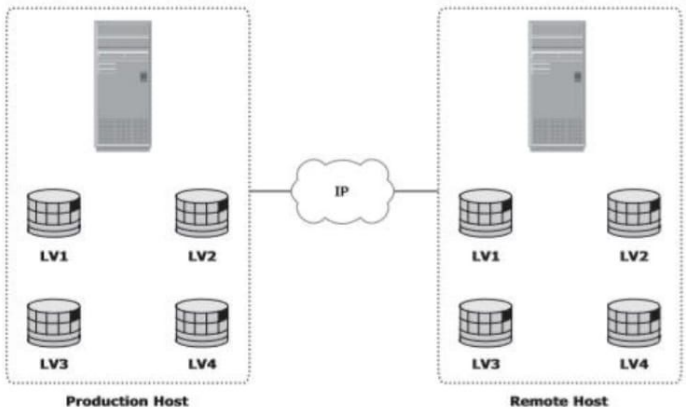


Figure 12-5: LVM-based remote replication

- LVM-based remote replication supports both synchronous and asynchronous modes of replication. If a failure occurs at the source site, applications can be restarted on the remote host, using the data on the remote replicas.
- LVM-based remote replication is independent of the storage arrays and therefore supports replication between heterogeneous storage arrays.
- Systems are shipped with LVMs, so additional licenses and specialized hardware are not typically required.

Host-Based Log Shipping

- Database replication via log shipping is a host-based replication technology supported by most databases.
- Transactions to the source database are captured in logs, which are periodically transmitted by the source host to the remote host (see Figure 12-6).
- The remote host receives the logs and applies them to the remote database.
- Prior to starting production work and replication of log fi les, all relevant components of the source database are replicated to the remote site. This is done while the source database is shut down. After this step, production work is started on the source database.

- The remote database is started in a standby mode. Typically, in standby mode, the database is not available for transactions.
- All DBMSs switch log fi les at preconfigured time intervals or when a log file is full.
- The current log fi le is closed at the time of log switching, and a new log fi le is opened. When a log switch occurs, the closed log fi le is transmitted by the source host to the remote host.

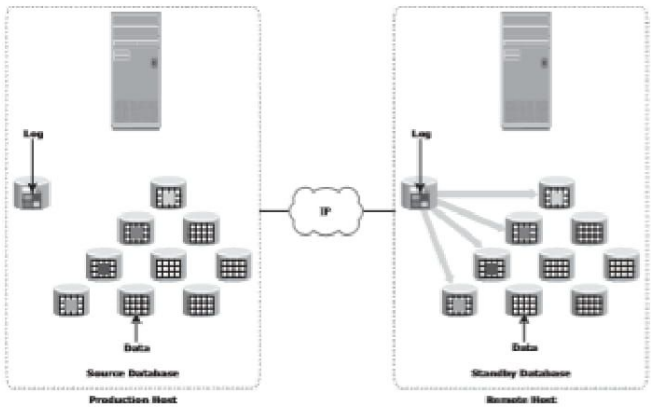


Figure 12-6: Host-based log shipping

- The remote host receives the log and updates the standby database. This process ensures that the standby database is consistent up to the last committed log.
- RPO at the remote site is finite and depends on the size of the log and the frequency of log switching.

Storage Array-Based Remote Replication

- In storage array-based remote replication, the array-operating environment and resources perform and manage data replication. This relieves the burden on the host CPUs, which can be better used for applications running on the host.
- A source and its replica device reside on different storage arrays.
- Data can be transmitted from the source storage array to the target storage array over a shared or a dedicated network.
- Replication between arrays may be performed in **synchronous, asynchronous, or disk-buffered modes.**

1. Synchronous Replication Mode

- In array-based synchronous remote replication, writes must be committed to the source and the target prior to acknowledging "write complete" to the production host.
- Additional writes on that source cannot occur until each preceding write has been completed and acknowledged. Figure 12-7 shows the array-based synchronous remote replication process

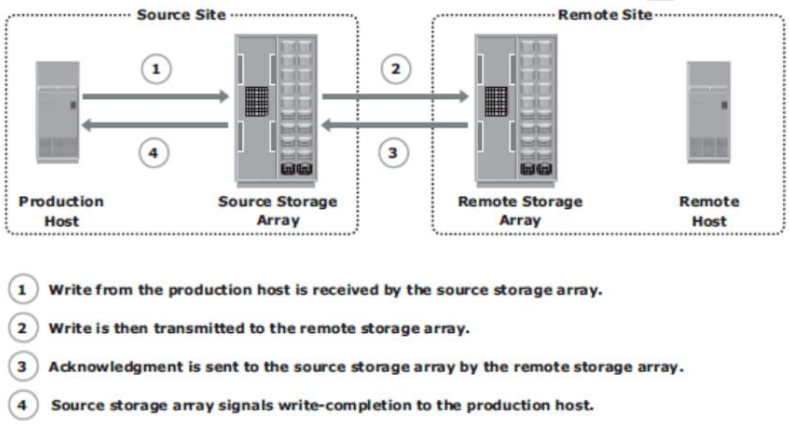
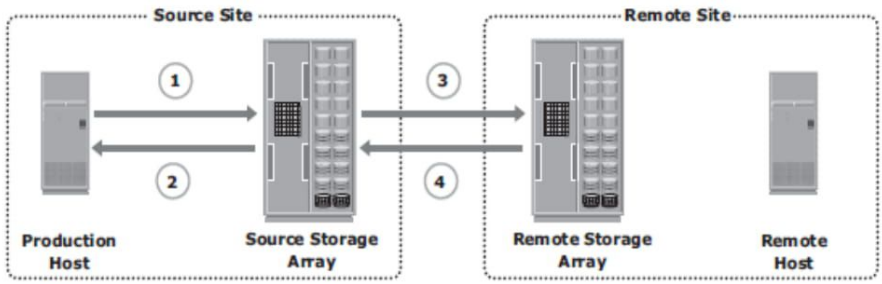


Figure 12-7: Array-based synchronous remote replication

2. Asynchronous Replication Mode

- In array-based asynchronous remote replication mode, as shown in Figure 12-8, a write is committed to the source and immediately acknowledged to the host.
- Data is buffered at the source and transmitted to the remote site later.
- The source and the target devices do not contain identical data at all times.
- The data on the target device is behind that of the source, so the RPO in this case is not zero.



1. The production host writes to the source storage array.
2. The source array immediately acknowledges the production host.
3. These writes are then transmitted to the target array.
4. After the writes are received by the target array, it sends an acknowledgment to the source array.

Figure 12-8: Array-based asynchronous remote replication

3. Disk-Buffered Replication Mode

- Disk-buffered replication is a combination of local and remote replication technologies.
- A consistent PIT local replica of the source device is first created.
- This is then replicated to a remote replica on the target array. Figure 12-9 shows the sequence of operations in a disk-buffered remote replication.
- At the beginning of the cycle, the network links between the two arrays are suspended, and there is no transmission of data.
- While production application runs on the source device, a consistent PIT local replica of the source device is created. The network links are enabled, and data on the local replica in the source array transmits to its remote replica in the target array.
- After synchronization of this pair, the network link is suspended, and the next local replica of the source is created.
- Optionally, a local PIT replica of the remote device on the target array can be created.

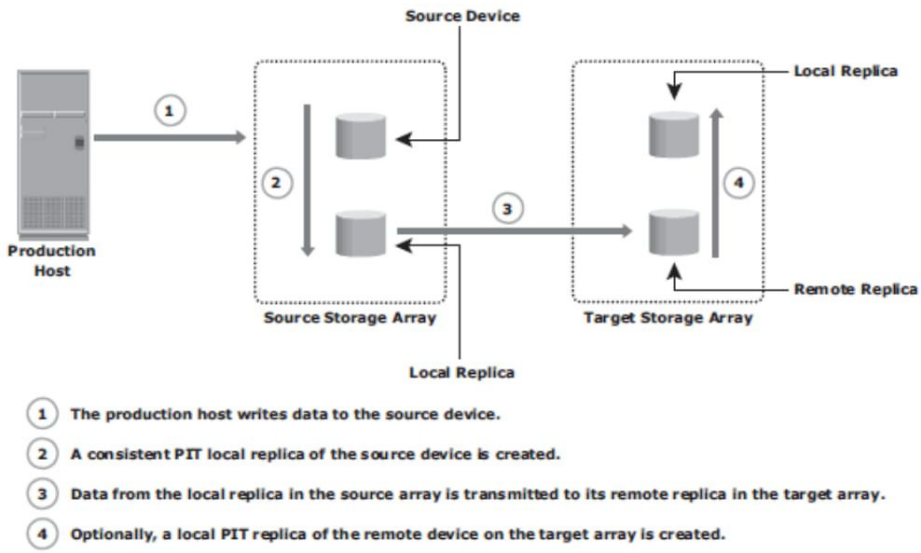
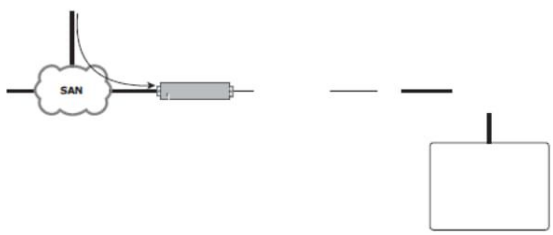


Figure 12-9: Disk-buffered remote replication

Network-Based Remote Replication

In network-based remote replication, the replication occurs at the network layer between the host and storage array.

In normal operation, CDP remote replication provides any-point-in-time recovery capability, which enables the target LUNs to be rolled back to any previous point in time. Similar to CDP local replication, CDP remote replication typically uses a journal volume, CDP appliance, or CDP software installed on a separate host (host-based CDP), and a write splitter to perform replication between sites. The CDP appliance is maintained at both source and remote sites. Figure 12-10 describes CDP remote replication.



- In this method, the replica is synchronized with the source, and then the replication process

starts. After the replication starts, all the writes from the host to the source are split into two copies.

- One of the copies is sent to the local CDP appliance at the source site, and the other copy is sent to the production volume.
- After receiving the write, the appliance at the source site sends it to the appliance at the remote site. Then, the write is applied to the journal volume at the remote site.
- For an asynchronous operation, writes at the source CDP appliance are accumulated, and redundant blocks are eliminated.
- Then, the writes are sequenced and stored with their corresponding timestamp. The data is then compressed, and a checksum is generated. It is then scheduled for delivery across the IP or FC network to the remote CDP appliance.
- After the data is received, the remote appliance verifies the checksum to ensure the integrity of the data. The data is then uncompressed and written to the remote journal volume.
- As a next step, data from the journal volume is sent to the replica at predefined intervals.

Three-Site Replication

- Three-site replication mitigates the risks identified in two-site replication.
- In a three-site replication, data from the source site is replicated to two remote sites.
- Replication can be synchronous to one of the two sites, providing a near zero-RPO solution, and it can be asynchronous or disk buffered to the other remote site, providing a finite RPO.

Three-site remote replication can be implemented as

1. Cascade/multihop
2. Triangle/multitarget solution.

Three-Site Replication — Cascade/Multihop

- In the cascade/multihop three-site replication, data fl ows from the source to the intermediate storage array, known as a bunker, in the first hop, and then from a bunker to

a storage array at a remote site in the second hop.

- Replication between the source and the remote sites can be performed in two ways: **synchronous + asynchronous or synchronous + disk buffered**.
- Replication between the source and bunker occurs synchronously, but replication between the bunker and the remote site can be achieved either as disk-buffered mode or asynchronous mode.

Synchronous + Asynchronous

- This method employs a combination of synchronous and asynchronous remote replication technologies.
- Synchronous replication occurs between the source and the bunker.
- Asynchronous replication occurs between the bunker and the remote site. The remote replica in the bunker acts as the source for asynchronous replication to create a remote replica at the remote site. Figure 12-11 (a) illustrates the synchronous + asynchronous method.

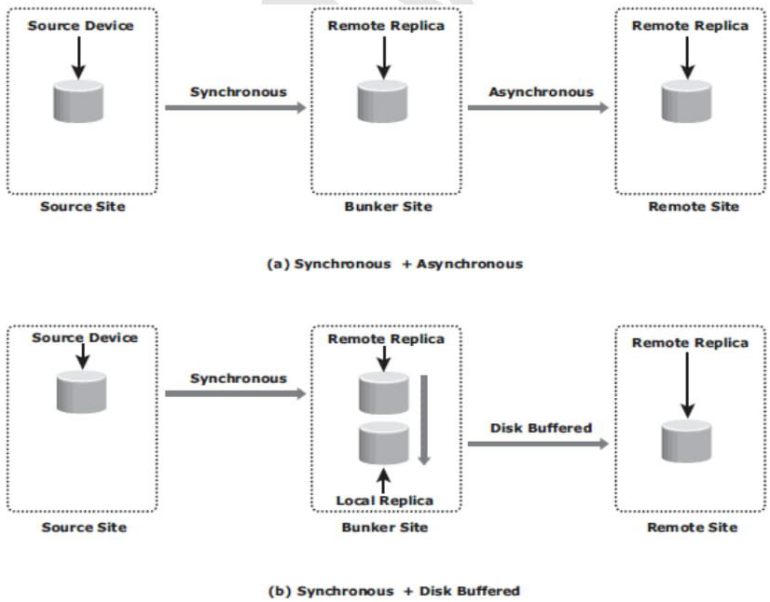


Figure 12-11: Three-site remote replication cascade/multihop

Synchronous + Disk Buffered

- This method employs a combination of local and remote replication technologies.

- Synchronous replication occurs between the source and the bunker: a consistent PIT local replica is created at the bunker.
- Data is transmitted from the local replica at the bunker to the remote replica at the remote site. Optionally, a local replica can be created at the remote site after data is received from the bunker. Figure 12-11 (b) illustrates the synchronous + disk buffered method.
- In this method, a minimum of four storage devices are required (including the source) to replicate one storage device.
- The other three devices are the synchronous remote replica at the bunker, a consistent PIT local replica at the bunker, and the replica at the remote site.
- RPO at the remote site is usually in the order of hours for this implementation.

Three-Site Replication — Triangle/Multitarget

- In three-site triangle/multitarget replication, data at the source storage array is concurrently replicated to two different arrays at two different sites, as shown in Figure 12-12. The source-to-bunker site (target 1) replication is synchronous with a near-zero RPO.
- The source-to-remote site (target 2) replication is asynchronous with an RPO in the order of minutes.
- The distance between the source and the remote sites could be thousands of miles.
- This implementation does not depend on the bunker site for updating data on the remote site because data is asynchronously copied to the remote site directly from the source.
- The triangle/multitarget configuration provides consistent RPO unlike cascade/ multihop solutions in which the failure of the bunker site results in the remote site falling behind and the RPO increasing.

Benefits

- ✓ The ability to failover to either of the two remote sites in the case of source-site failure, with disaster recovery (asynchronous) protection between the bunker and remote sites.
- ✓ Resynchronization between the two surviving target sites is incremental. Disaster recovery protection is always available if any one-site failure occurs.

Remote Replication and Migration in a Virtualized Environment

- Virtual machine migration is another technique used to ensure business continuity in case of hypervisor failure or scheduled maintenance.
- VM migration is the process to move VMs from one hypervisor to another without powering off the virtual machines.
- VM migration also helps in load balancing when multiple virtual machines running on the same hypervisor contend for resources.

Two commonly used techniques for VM migration are

1. **Hypervisor-to-hypervisor**
2. **Array-to-array migration.**

1. **In hypervisor-to-hypervisor VM migration**

   - The entire active state of a VM is moved from one hypervisor to another. Figure 12-14 shows hypervisor-to hypervisor VM migration.
   - This method involves copying the contents of virtual machine memory from the source hypervisor to the target and then transferring the control of the VM's disk fi les to the target hypervisor.

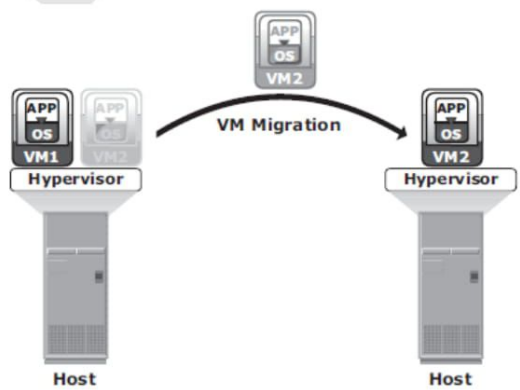


Figure 12-14: Hypervisor-to-hypervisor VM migration

   - Because the virtual disks of the VMs are not migrated, this technique requires both source and target hypervisor access to the same storage.

In array-to-array VM migration

- Virtual disks are moved from the source array to the remote array. This approach enables the administrator to move VMs across dissimilar storage arrays.
- Figure 12-15 shows array-to-array VM migration. Array-to-array migration starts by copying the metadata about the VM from the source array to the target.

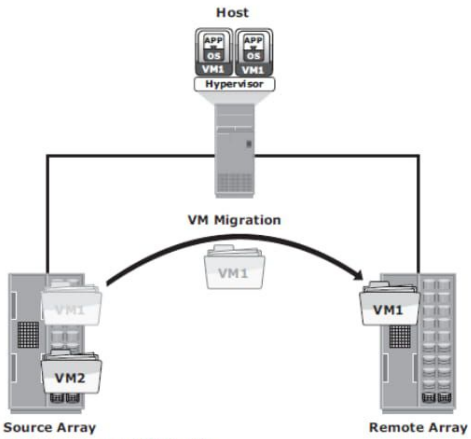


Figure 12-15: Array-to-array VM migration

- The metadata essentially consists of configuration, swap, and log files. After the metadata is copied, the VM disk fi le is replicated to the new location.

Sample Questions

1. Describe the failure analysis in BC. Briefly explain BC technology solution
2. With a neat diagram explain the steps involved in backup and restore operation.
3. What is information availability? Explain how information availability is defined and measured.
4. What is BC. Explain BC planning life cycle with a neat diagram
5. Explain the reasons for which backup is performed
6. What is BC? Explain the BC terminology in detail.
7. What is data deduplication? Explain the implementation of data deduplication.
8. Explain failure analysis.
9. Explain the factors used for measuring information availability.
10. Explain backup method and architecture.
11. Explain backup and restore operations.

12. Explain backup topologies. With a neat diagram
13. Explain backup technologies.
14. Explain backup in virtualized Environment with a neat diagram
15. Explain the different backup targets with comparison.
16. Explain local replication technologies.
17. Compare local replication technologies.
18. Explain modes of remote replication.
19. Briefly explain remote replication technologies.
20. Explain network infrastructure over remote replication.
21. What is local replication. Explain host based local replication technologies
22. Explain array based local replication technologies with a neat diagram
23. Differentiate between pointer based full volume replication and pointer based virtual replication methodology
24. Explain in detail local replication in Virtualized Environment.
25. Define remote replication. Explain remote replication technologies.
26. Explain with a neat diagram storage array based remote replication
27. Explain Synchronous + Asynchronous and Synchronous + Disk Buffered methods of three-site replication with neat diagram.
28. Explain Remote Replication and Migration in a Virtualized Environment.