MODULE - IV

Local Replication

MODULE 4

Local Replication

Module Description

In the previous module, we read about various backup and recovery considerations and the technologies associated with them. This module talks about the replication and data consistency as well as restore and restart techniques. This module provides details about various local replication technologies, along with key steps to plan and design an appropriate local replication solution.

Replication is being used widely by the businesses in order to achieve various business goals, such as fault tolerance, improved performance and backup. It is majorly classified into local and remote replication. In the first chapter, the students will get an insight to the local replication, its benefits and the technologies being used in performing the local replication.

In the second chapter, students will learn about restore and restart techniques. They will also learn to create multiple replicas and will elaborate on various methods of managing an interface.

Chapter 4.1
Replication and Data Consistency

Chapter 4.2
Restore and Restart Techniques

Chapter Table of Contents

Chapter 4.1

Replication and Data Consistency

Aim

To equip the students with the concept of replication and data consistency

Instructional Objectives

After completing this chapter, you should be able to:

- Explain the concept of replication and its uses
- Explain the source and target
- Outline the process of file securing
- Explain data consistency and its types
- Explain the local replication technologies
- Explain the host-based and storage array-based replication

Learning Outcomes

At the end of this chapter, you are expected to:

- Identify the importance of local replication
- Outline the use of local replicas
- Identify the importance of data consistency
- Explain the consistency of replicated file and database
- Illustrate the local replication technologies
- Compare host-based and storage array-based replication

4.1.1 Introduction

The process of creating an exact copy of the data is known as **replication**. This process also entails creating and managing duplicate versions of a database. The process of replication not just creates exact copies of the database data, but it also synchronises a set of replicas in a way that changes made to one replica are reflected in all the other replicas.

The beauty of replication is that it allows multiple users to work on their local copy of the data; however, it keeps the database updated and it appears to the users as if they were working on a single, centralised database. Replication is often the most effective solution when the users are geographically widely distributed and wish to access the database.

This chapter deals with replication and focuses primarily on local replication, where the replication of data takes place locally in the same storage array. In the coming topics, we will discuss and understand the concept of local replication, its benefits and its uses. We will also understand the meaning of source and targets and the process of safeguarding the data and files. Apart from this, we will discuss different local replication technologies and their functioning.

Let us begin with understanding the concepts of replication and local replication.

4.1.2 Local Replication

Creating replicas of the production data is also one of the ways to ensure business continuity. The replication process can turn out to be a boon in the recovery and restart operations and the replicas can be used in the event of data loss.

The main goal of the replication process is to enable users to have the designated data at the correct place and in the correct state to meet the recovery need. Replicas should provide recoverability and restartability.

Recoverability refers to the ability of restoring the data to the point at which the failure occurred. In the event of a data corruption or data loss, recoverability enables the restoration of data from the replicas to the production volumes. The ability to quickly recover from a data loss does not only depends on having the backup copy of the data. It also depends on predefining a plan to recover the backup data on the new hardware. Recoverability must provide minimal Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to ensure quickly resuming the business operations on the production volumes.

Restartability is the ability to start again or anew. Restartability must ensure the consistency of data on the created replicas. This helps in restarting the business operations with the help of replicas.

Replication can be classified into two major categories:

- Local replication
- Remote replication

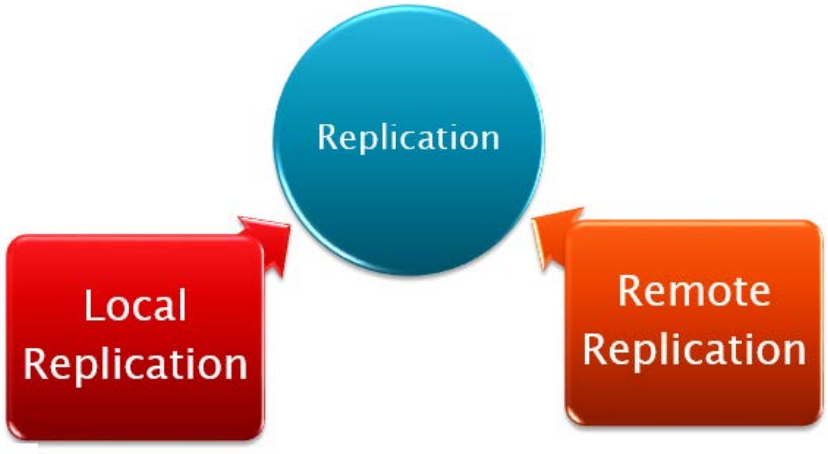

Figure 4.1.1: Replication

Local replication refers to the replication of data locally within the same disk storage array or same data centre. It means that the source and target data volumes are located on the same disk storage array. A disk storage array is a data storage system that consists of a large group of hard disk drives (HDDs) and disk drive trays. It distributes and stores data efficiently using the redundant array of independent disk (RAID) and improves fault tolerance.

Remote replication refers to the process of creating the replicas of information assets at remote locations. It helps the businesses to mitigate the risks associated with the power or other outages that might result from any disaster, natural or man-made.

In a business-critical environment, a strong protection for the valuable data is one of the most critical requirement possessed by the organisation. Local replication helps protect the data in the most efficient way by providing file system snapshot and full-volume mirroring capabilities. With the space-saving file system snapshot copies, the restoration of the files can be easily made, as necessary. With the full-volume mirror data copies, restoration can be performed when a RAID-protected volume fatally fails. We will learn about these capabilities in detail in the coming sections.

Benefits of Local Replication

- Improves RPO and RTO.
- Restore files and roll backs data almost instantaneously.
- Management is simplified; minimal manual intervention is required to perform the data protection.
- Creates point-in-time file system snapshots that consumes a very minimum disk space.
- Creates full-volume mirror copies and minimises data loss.

Did You Know?

A file system is the method and data structure that is used by an operating system to keep a track of files on a disk or partition. It is also used to refer to a partition or disk that stores the files.

Self-assessment Questions

1) Which of the following statements best define replication?
   a) It is the process of creating a copy of data.
   b) It is the process of creating a copy of data within the same disk storage array.
   c) It is the process of creating a copy of data at remote locations.
   d) It is the process of creating an exact copy of data.

2) Which of the following are benefits of local replication? Choose all that apply.
   a) It helps in minimising data loss.
   b) It helps in restoring files.
   c) It improves RPO and RTO.
   d) It provides simplified management in performing backup and recovery operations.

4.1.3 Source and Target

In terms of computer storage, a logical unit number (LUN), refers to a number used to identify a logical unit in a storage system. This logical unit can be either an entire physical disk, or a subset of a larger physical disk or disk volume. The physical disk can be a disk drive. A subset can be a partition of the disk drive or a disk volume from a RAID controller that consists of multiple disk drives aggregated together to ensure large storage capacity and redundancy. A LUN can be associated with any device that supports the read/write operation; however, it is an important factor associated in managing block storage arrays shared over a storage area network (SAN).

A host that accesses data from one or more LUNs on the storage array is referred to as a **production hosts** and the LUNs are known as source LUNs, production LUNs, or simply as **source**.

The LUNs where the data replication takes place are known as target LUNs or simple as **target** or replica. These LUN targets are also accessible by hosts other than the production hosts for performing various operations, such as backup or testing. Although, we have read about hosts in Module 2, Chapter 1, let us quickly recall the definition so that we can easily distinguish between a host and production host. A host is a computer or any other device that enables the running of applications that supports data storage and retrieval.

A host is able to make modifications in the target data without altering the source. This leads to differences in between the target and source data and at some point they might not be the identical copy of each other. To solve this, the target can be incrementally resynchronised, by copying the data that got changed since the last synchronisation, with the source to make them identical.

Self-assessment Questions

3) The LUN where the data replication takes places is known as?

a) Production host
b) Source
c) Production LUN
d) Target

4) Which of the following is the correct expansion for LUN?

a) Logical Usage Number
b) Local Unit Number
c) Local Upgrade Number
d) Logical Unit Number

4.1.4 Uses of Local Replicas

Local replicas can be created to cater several possible purposes, such as:

- **Serves as an alternative source for backup:** In a normal backup operation, the data to be backed up is read from the production volumes or LUNs and then written onto the backup devices. As the production LUNs are also simultaneously busy with the production work, the addition workload of backup activities places an additional burden on the production software.

  The local replicas contain an exact point-in-time file system snapshot of the source data that can be utilised to perform the backup operations. With the help of this, they ease the backup workload on the production volumes. The local replicas also reduce the backup window to zero. A backup window is the time slot when a source is available for performing a backup operation. In some cases, when performing backup from the source, the production operation remains suspended as the data on the production source is locked exclusively for being used by the backup purpose.

- **Provides fast recovery:** Local replicas can be utilised to recover the lost data at times of a partial failure of the source or data corruption. In the unfortunate event of a complete failure of the source, the local replicas can be restored to a different set of source devices. In either of the cases, local replication provides the benefit of fast recovery and minimal RTO as compared to a traditional restore from tape backups. In most of the situations, a business operation can resume and start using the data from the source device before the data is completely copied from the local replica.

- **Provides decision-support activities:** Local replication also provides decision-support activities, such as reporting. You can use the local replicas to create a report that shows the input/output (I/O) workload on the production volume. These reports can be utilised for further analysis and decision-making to reduce the burden on the production volume. Hence, the local replicas can be utilised for minimising the burden on the production volumes.

- **Provides a testing platform:** Local replicas can also be utilised for testing critical business data or application. For example, local replica can be used to test an application upgrade. If the test is successful, it can be restored to the source volumes.

- **Helps in data migration:** Local replication also provides a helping hand in situations of data migration. The migration of data may be performed for several reasons, such as migrating from a small LUN to a larger LUN.

Self-assessment Questions

5) Which of the following describes the best possible time for performing the backup operation?

a) File System
b) Backup window
c) Hot backup
d) Cold backup

6) Local replicas can also be used for generating reports - this statement caters which of the following usages of local replication?

a) Helps in data migration
b) Provides decision-support activities
c) Provides fast recovery
d) Provides a testing platform

4.1.5 Securing Files

While we perform the local data replication technique, the safety and security of files cannot take the back seat. We need to ensure that the files saved locally or even over the network are safe and secure. Prevention is better than cure and hence, although we focus on all sorts of replication technique, we, promptly, need to ensure that the data does not gets destroyed, corrupted, or stolen, at the first place.

Files can be secured over a network using the New Technology File System (NTFS). NTFS is a high-performance system proprietary to Windows that supports securing files. Files can be secured locally by utilising the share permissions, such as read and write. You can assign read, write, or both permissions to the respective users to ensure the accessibility of file within known limits. You can follow the mentioned steps to share a file with other users on your network:

Step 1: Right-click the file you want to share and select **Properties**.

Step 2: Select the **Sharing** tab.

Step 3: In the Sharing tab, choose **Share**.

Step 4: Type the names of the people you want to share the folder with select **Add**.

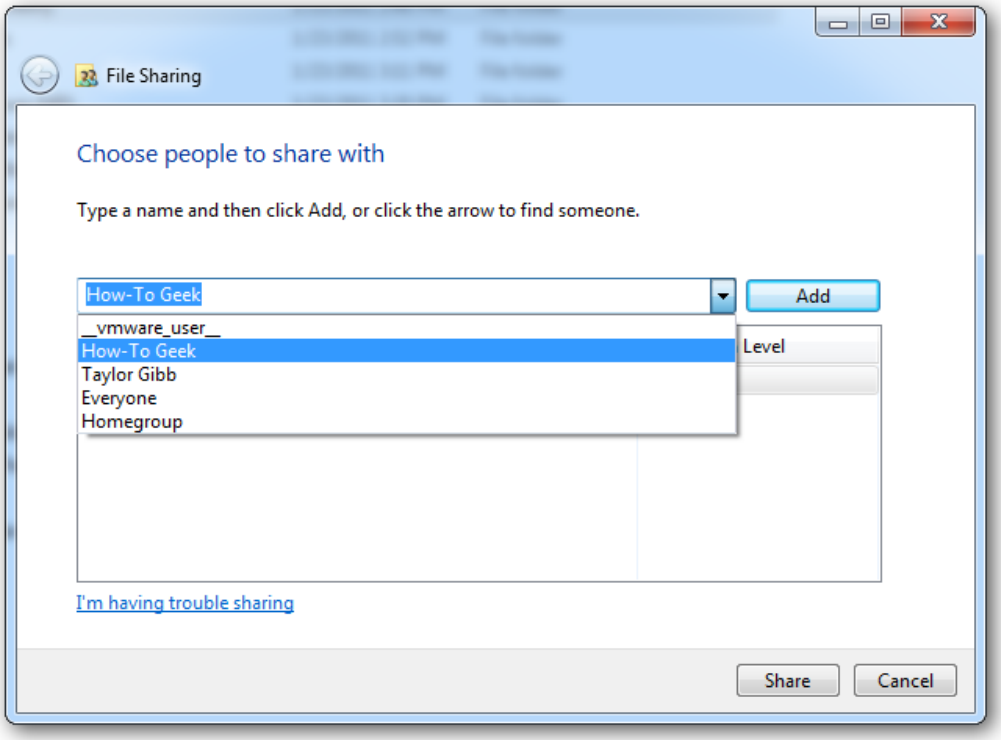

Figure 4.1.2: Adding Users

Step 6: Assign them read/write or both permissions. You can also remove the people from the list if you do not want to share the folder with them.

Step 5: Click **Share**.

You can also set NTFS permissions on a file using the following steps:

Step 1: Right-click the file and select **Properties**.

Step 2: Select the **Security** tab.

Step 3: To edit the NTFS permission for a user or a group, click the **Edit** button.

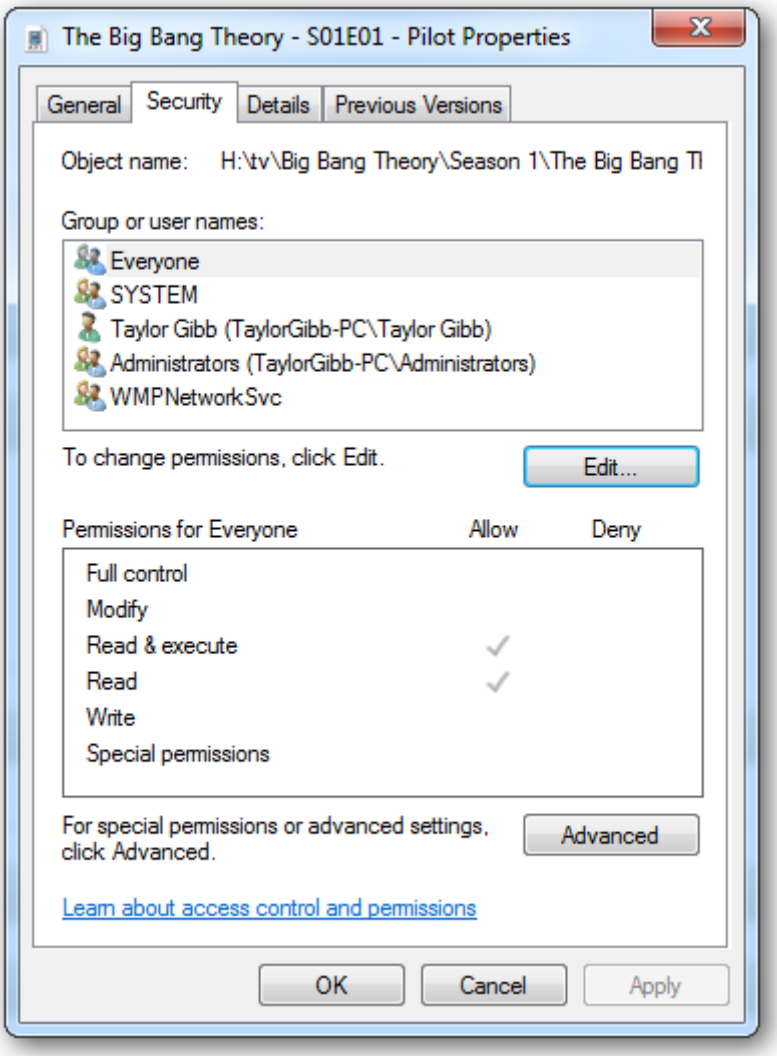

Figure 4.1.3: Editing NTFS Permissions

Step 4: Choose from the given set of permissions, Full control, Modify, Read & Execute, Read and Write and select the checkboxes, **Allow** or **Deny**, to grant or revoke permissions to each user or group.

There are also some more techniques to keep the files safe and secure, such as encryption and decryption, watermarking, etc. Encryption is the process which converts data into a format that cannot be read by another user. Once a user has encrypted a file, it remains encrypted when the file is stored on disk. Decryption is the reverse process whereby data is converted data back from encrypted format to its original format.

Self-assessment Questions

7) Which of the following is the correct expansion for NTFS?

a) New Technique File System
b) New Technology Folder System
c) New Technology File System
d) New Technique File Safety

8) Which of the following is the process of converting data into a format that cannot be read by another user?

a) NTFS
b) Encryption
c) Decryption
d) Read/Write Permissions

4.1.6 Data Consistency

Data consistency refers to the requirement that the data remains constant in time as well as can be used for various transactions without changing their structure.

To ensure that the backup data is usable, it is important to understand and be aware of the backup methodologies that are being used. It is also necessary to understand how the primary data is created and accessed. Apart from that, it is also important to pay attention to the consistency of data after a recovery operation has been complete and the application is ready again for processing.

Before a data is written to a backup disk, most file systems and databases buffer the data into the host. A consistent replica ensures that the data that has been buffered into the host gets properly captured on the disk at the time of replication. For all the replication technologies, the primary requirement is to ensure the consistency in data.

(i) Consistency of a Replicated File System

A file system buffers the data in the memory of the host to improve the response time of the applications. The buffered information then gets written on the disk periodically. The replica can be created in between the set intervals of writing the buffered information to the disk, in some cases.

Therefore, before creation of a replica, the host memory buffers should be flushed to ensure the consistency of data on the replica. In a situation, when the host memory buffers are not flushed, the replicated data might not contain all of the information that was buffered in the host.

If the file system is unmounted before the creation of the replica, the buffers gets automatically flushed out and the data on the replica remains consistent. When the replication takes place on a mounted file system, some level of recovery, such as **fsck** or **CHKDSK**, would be required on the replicated file system. Fsck is a system utility tool that stands for file system consistency check. It is required for checking the consistency of the file system in Unix and Unix-like operating systems, such as Linux. CHKDSK plays the same role in Windows.

After the file system replication process is complete, the replica file system can be mounted for operational use.

Did You Know?

Sync Daemon is the process in Unix that flushes the buffers to disk at set intervals.

(ii) Consistency of a Replicated Database

A database can contain various files, file systems and devices. In the world of Internet, a large number of geographically dispersed users may require querying and updating the same database routinely. In such environment, a centralised database is exposed to various risks; some of them are as follows:

- Degradation in performance due to high server load.
- Risks of data loss due to server crashes.
- Availability issues due to server downtime or lack of network connectivity.

Consistently replicating the database server on a set of peer servers can be one of the most useful solution to such situation.

The replication of the database should happen consistently so that the replica provides the features of restorability and restartability. The process of replication can take place in both the situations of a database being online or offline.

When the database is offline, it means it is in the shutdown state and is unavailable for the I/O operations. As no updates takes place while the database is in the offline mode, the replicas created during that hour are consistent. However, in certain situations, creating an offline replica might not be viable, keeping in mind that some businesses might need to be online 24x7.

When the database is online, it means the database is available for the production work and supports the I/O operations. In such scenario, multiple transactions are received by the database, which, as a result, keeps on updating the database continuously. When the backup process is performed when the database is online, then the changes made in the database must also be applied to the backup copy, in order to maintain consistency.

Performing a backup operation on an online database requires additional procedures to ensure consistency. These procedures can be scripted in order to automate the process. This eases the administrative work and lessens the chances of human error.

Most of the databases today some form of dynamic or hot backup. You have already learnt about the backup methods, hot and cold backups, in Module 3, Chapter 1. Let us quickly recall the definition of a hot backup. A hot backup refers to the backup performed when the database is up and running and the data is actively accessible to users and may currently be in the state of being updated. When the database is in the hot backup mode, then there will be increased logging activities.

In a hot backup mode, first a database checkpoint is issued that flushes the buffers to disk and positions the database in the hot backup mode. The database is taken out of the hot backup mode after the point-in-time snapshot copy is created. The logs collected are then applied to the replica to ensure the consistent restoration of the database.

There is an another approach to ensure data consistency, it is the **dependent write I/O principle**. This principle states that an application cannot issue a write I/O command, until a previous-related I/O command gets completed. ***For example***, in a backup environment, at some point, a log file must be written before the data can be written to the backup media.

To understand this better, let us refer to the Figure 4.1.4 that illustrates the process of flushing the buffer from the host to source. For the transaction to be deemed complete, I/Os 1 to 4 must get completed. Here, each I/O gets completed only after the previous I/O has been successfully completed. I/O 4 is dependent on the completion of I/O 3, which depends on the completion of I/O 2. And I/O 2 can be initiated only when I/O 1 has been successfully completed.

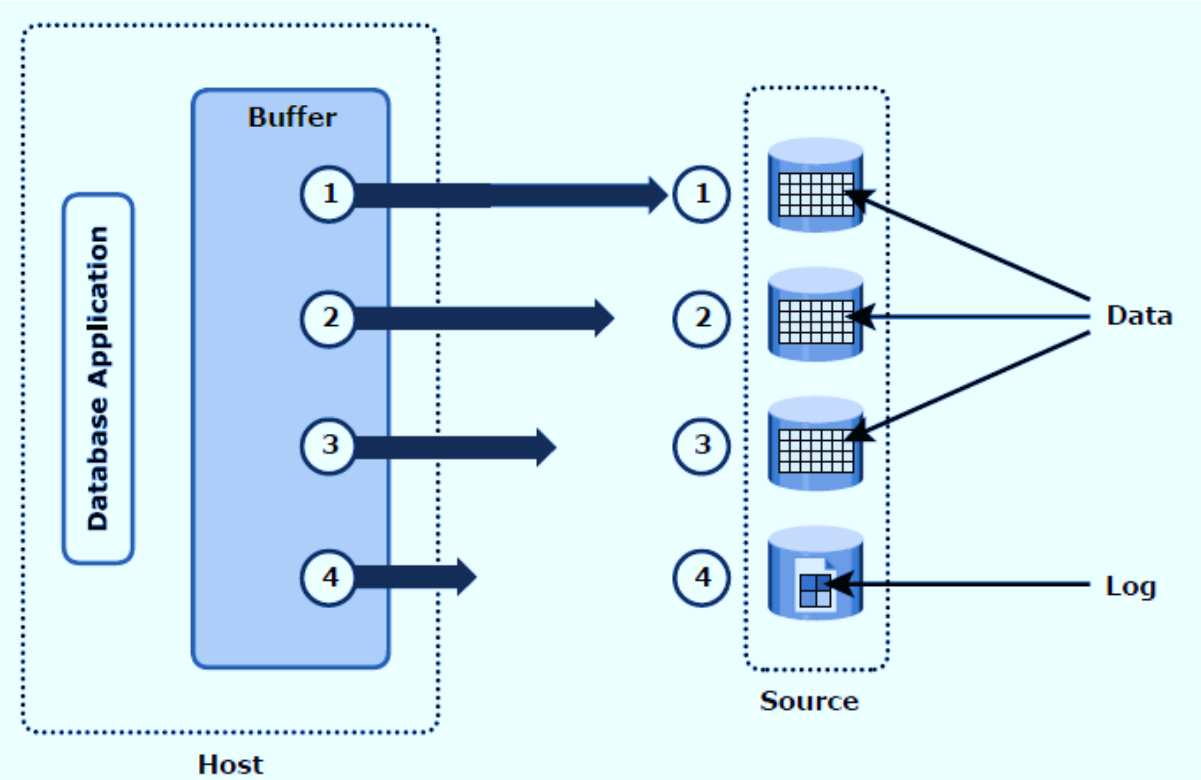

Figure 4.1.4: Dependent Write

Let us refer to the Figure 4.1.5 that shows a comparison between a consistent and inconsistent database using the dependent write I/O principle.

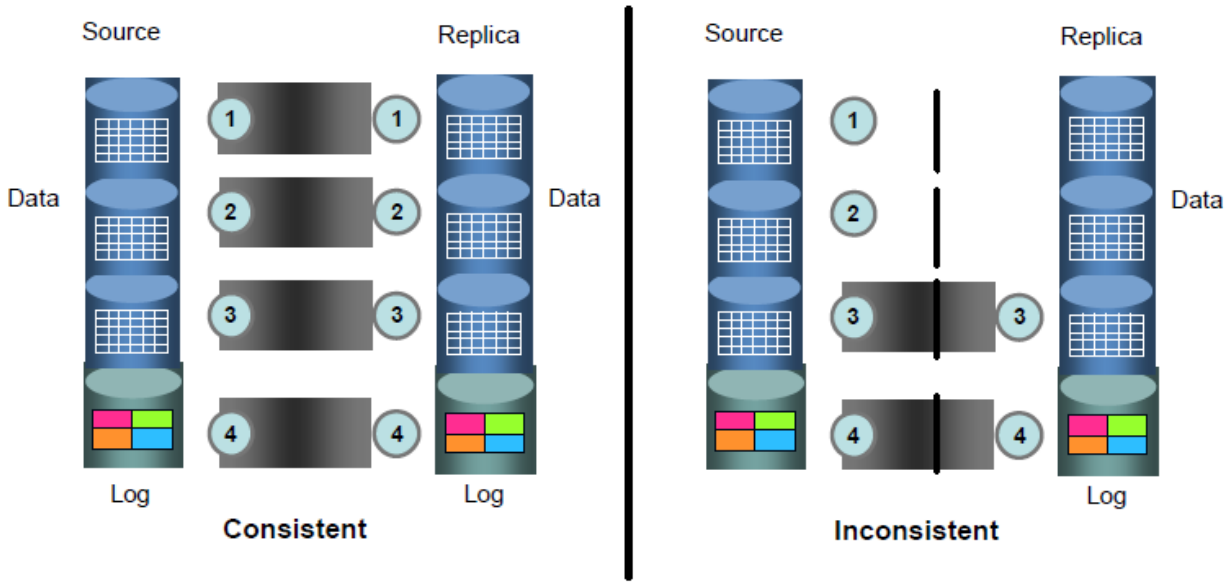

Figure 4.1.5: Database Consistency

When a replica is created, then to ensure consistency, all the writes to the source devices should be captured on the replica devices. Creating a point-in-time copy for multiple devices happens quickly, but it is not an instantaneous process. During the replication, it is possible that all the I/O transactions might not get copied on the replica devices. This can make the replica appear inconsistent with the data available on source. Such situations can be avoided by ensuring that write I/O to all source devices are held for the duration of creating the replica. This will create a consistent image on the replica. One thing that should be considered in this situation is the databases and applications have the tendency to time out if the I/O is held for too long.

Self-assessment Questions

9) Which of the following commands is required for checking the consistency of the file system in Unix?

a) Fsck
b) CHKDSK
c) CHKDISK
d) Fcsk

10) Which of the following states that an application cannot issue a write I/O command, until a previous-related I/O command gets completed?

a) Production host
b) Dependent write I/O
c) Recoverability
d) Restartability

4.1.7 Local Replication Technologies

Replication is being used widely by the businesses in order to achieve various business goals, such as fault tolerance, improved performance and backup. The two major technologies that have been adopted for local replication are host-based and storage array-based replications. Local volume manager (LVM)-based replication and file system replication are the examples of host-based replication technology. Storage array-based replication can be implemented using the distinct solutions, such as full-volume mirroring, pointer-based virtual replication and pointer-based full-volume replication. The decision regarding which technology to use depends on the logical presentation data that is to be replicated.

Let us learn about the two technologies of local replication in detail.

(i) Host-Based Local Replication

Host-based local replication is the technique of copying data from one site to the other using the servers. This process is file-based, asynchronous, designed to work over long distances and generally inexpensive as compared to storage array-based local replication. In this process, a replication agent is installed on the operating systems of the servers that needs to be replicated. This replication agent processes and replicates the I/O traffic present on any storage system to a secondary replication target system.

In host-based local replication, the replication process is performed by the LVMs or the file systems.

Did You Know?

In asynchronous replication, the data is written first to the primary storage and then, depending on the implementation approach, enables data to be replicated to another storage. It allows periodic copying of data at scheduled intervals to replication targets.

LVM-Based Replication

An LVM is a technique for performing logical volume management of the data that includes activities like allocating disks, mirroring and resizing logical volumes. It is an advanced and flexible system of managing logical volumes and is much more than just the traditional method of partitioning a disk and formatting that partition with file systems.

The LVM is divided into three components:

- Physical volume
- Volume groups
- Logical volumes

The physical volume is the physical disk for storing the data. They are the block devices that provide storage space for logical volumes. A volume group is created by grouping one or more physical volumes together. A logical volume corresponds to partitions; these are created within a given volume groups and can span across multiple physical volumes. A volume group can contain multiple logical volumes

In LVM-based local replication, the LVM is responsible for creating, controlling and managing the host-level logical volumes. In this technique of local replication, each logical partitioning in a logical volume is mapped to two different physical partitions based on two different physical volumes. The write I/O to a logical partition gets written to those two physical partitions by the LVM device driver. This process is known as **LVM mirroring**. The mirrors created can also be split and the data contained by each of them can be accessed independently. The LVM mirrors can be added or removed dynamically.

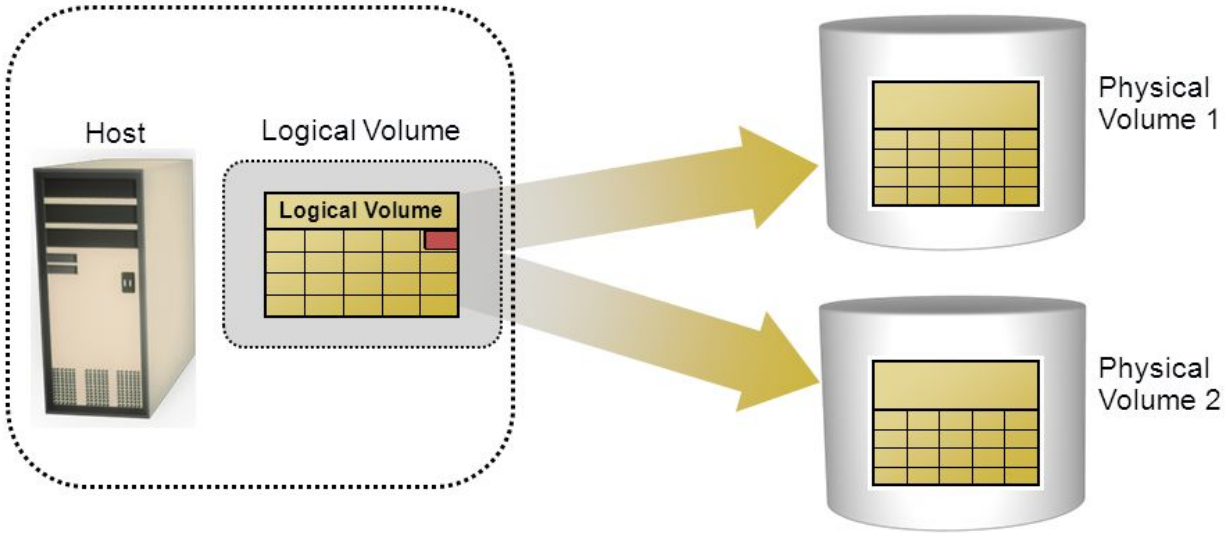

Figure 4.1.6: LVM Mirroring

Advantages of LVM-Based Local Replication

- It is relatively inexpensive than storage array-based replication.
- It is fast; most of the operations with LVM can be done on a fly, while the system is running.
- It is independent of any vendor-specific storage system.
- It provides continuous data protection by enabling to roll back to an earlier version if there is a data corruption on the primary site.
- It is typically a part of the operating system and no additional license is required to deploy LVM mirroring.

Disadvantages of LVM-Based Local Replication

- Since every I/O write generated by the application gets translated into two writes on the disk for mirroring, the host CPU experiences additional burden. This degrades the performance of the applications.
- It is typically not possible to present an LVM-based local replica to a different host at the same time. The replica remains the part of the volume group and that is usually accessed by one host at a time.
- As all the LVMs do not support incremental resynchronisation, tracking changes to the mirrors and performing incremental synchronisation becomes a challenge.
- Since both the replica and the source data are stored on the volume group, at the time of an error in the volume group, there are chances that the replica itself become unavailable.
- In case of a server failure, both the source data and its replica becomes unavailable unless the server is brought back online.

File System Snapshot

A file system snapshot is a pointer-based replica that only requires a fraction of the space consumed by the original file system. When you create a snapshot, then you actually create a new logical volume that acts as a clone of the original logical volume. The snapshot initially does not consume any space; however, with time, as the changes are made to the original logical

volume, the changed blocks, before getting changed, gets copied into the snapshot for being preserved. This means, that the more changes are made to the original volume, the more space will be required by the snapshot.

These snapshots can be implemented by both LVM or the file system itself. The file system snapshot uses the Copy on First Write (CoFW) principle. It is a pointer-based virtual replication method that states that the data should be copied to a predefined area in the array, when a write occurs into the source or target for the very first time.

At the time of creation of a snapshot, a bitmap and blockmap are created into the metadata of the snapshot file system. The bitmap is required to keep a track of the blocks that got changed on the production file system after the creation of the snapshot. The blockmap is required for indicating the exact address from which data is supposed to be read, at the time of data accessing by the snapshot file system.

In order to read from a file system snapshot, the bitmap is consulted. In case the bit is 0, then the read is directed towards the production file system. When the bit is 1, then the block address is fetched from the blockmap and data is read from the mentioned address.

👍 Advantages of File System Snapshot

- Snapshots can be used to get a consistent image of the file system, that can be used for backup without shutting down the system.
- Snapshots can also be used for saving the current state of the system. This can be required when you are apprehensive and may want to return to the previous state of the system if things are messed up.
- Snapshot volumes can be mounted to make changes to it, without altering the original source.

👎 Disadvantage of File System Snapshot

- In case, the snapshot volumes consume all the volume allocated to it, then the snapshot gets broken and is not suitable to be used anymore.

(ii) Storage Array-Based Replication

In this technique, the array operating environment performs the local replication technique by using the built-in software to automatically copy the data from one storage array to the other. The host resources, such as CPU and memory, do not participate in the storage array-based replication process. This enables the host to stay aloof from the replication operations minimising the burden on the host.

In this replication, the required number of replica devices must be chosen on the same array and then the replication of data can take place between the source-replica pairs.

Storage array-based replication can be categorised as:

- Full volume mirroring
- Pointer-based full volume replication
- Pointer-based virtual replication.

Let us learn about each of them in detail.

Full Volume Mirroring

In this technique, the target gets attached to the source and establishes itself as a mirror of the source. Existing data as well as new updates on the source gets copied to the target. After the copying of data is complete, the source and the target becomes identical; the target is then considered as the mirror of the source data. During this process, the target remains unavailable to be accessed by any other host; however, both the target and source can be accessed by the production host. After the synchronisation process gets complete, the target gets detached from the source and is made available for the business continuity operations.

After the target is detached from the source, it acts like a point-in-time copy of the source and the changes made to both source and its replica can be tracked at some predefined granularity. You have already read about backup granularity in Module 3, Chapter 1. Backup granularity describes the level of detail in characterising the backup data.

This enables incremental resynchronisation from source to target or incremental restore from target to source. The granularity of data change is typically tracked using bitmaps, with one bit assigned to one block. It can range from 512 byte blocks to 64 KB block. In case of any update to a particular block, entire block is marked as changed, irrespective of the size of the update.

When the resynchronisation or restore occurs, only the blocks that got changed needs to be copied. This method reduces the time by eliminating the need for a full synchronisation or restore operation.

Did You Know?

The point-in-time of a replica is determined by the time when the source is detached from the target. ***For example***, if the time of detachment is 4:00 pm, the point-in-time for the target is 4:00 pm.

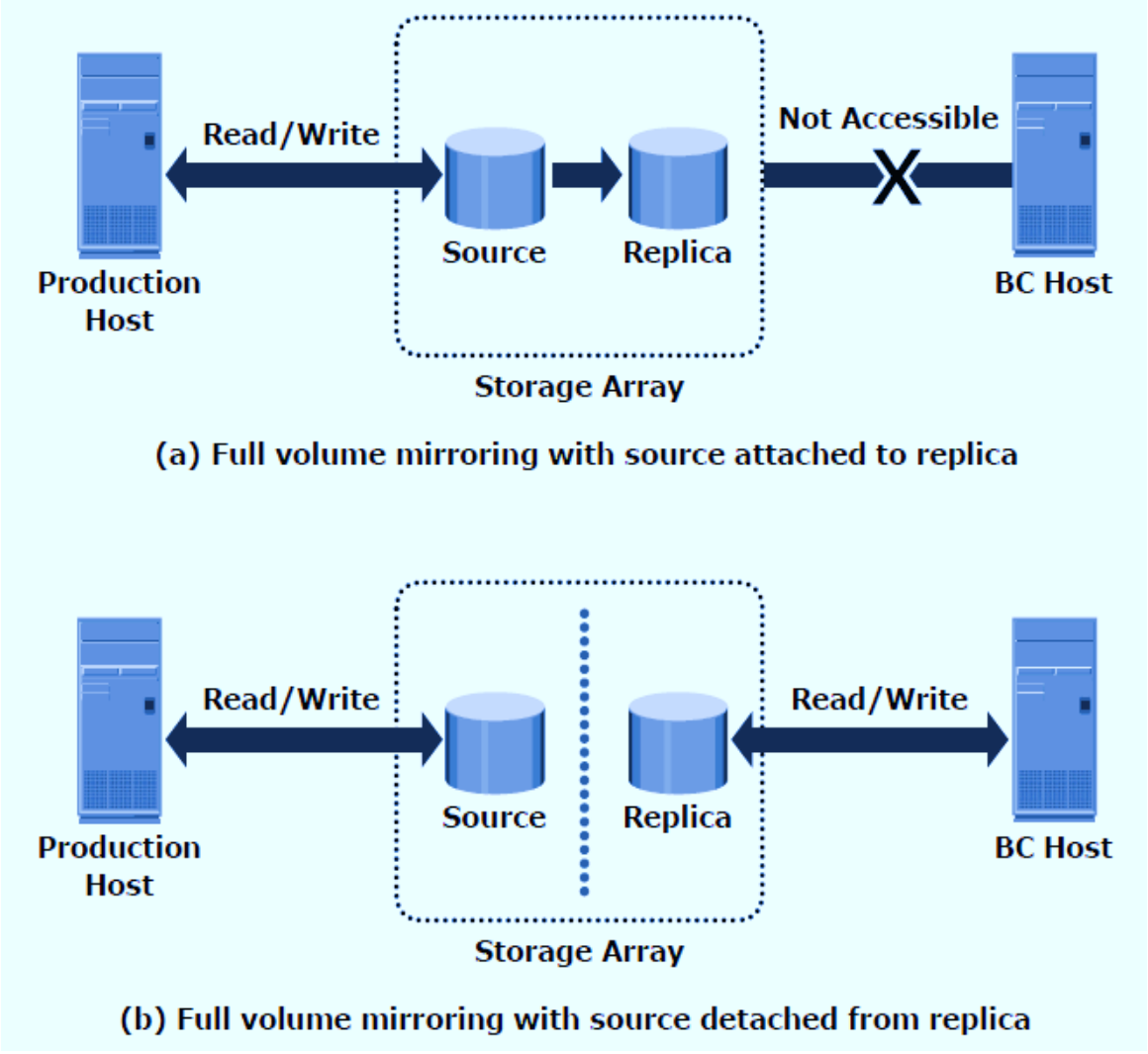

Figure 4.1.7: Full Volume Mirroring

Pointer-Based Full Volume Replication

This technique is similar to full volume mirroring and can provide full copies of the source data on the target. However, unlike full volume mirroring, one does not need to wait for data synchronisation to target and detachment of the target from the source in order to access the target. The target is made immediately accessible when the replication session is activated. The time of activation defines the point-in-time copy of the source.

The pointer-based full volume replication can be activated in either Full copy mode or in the Copy on First Access (CoFA) mode.

In Full copy mode, the copying of data from the source to target takes place in the background and the data gets copied regardless of access. In case, when access to a block that has not yet been copied is required, that block is preferentially copied to the target. In case, the replication session gets terminated in between, the target contains all the original data from the source at the point-in-time of activation. This makes the target a viable copy for restoration, recovery, or any other business continuity operations.

In the CoFA mode, when the replication operation is initiated, the source data gets copied to the target at the trigger of the following:

- When a write operation gets issued to a specific address on the source for the first time.
- When a read or write operation gets issued to a specific address on the target for the first time.

In the first case, when a write operation is issued at the very first time to the source, the original data at that address gets copied to the target and then the source is updated with new data. This is done to ensure that the original data at the point-in-time of activation has been preserved on the target.

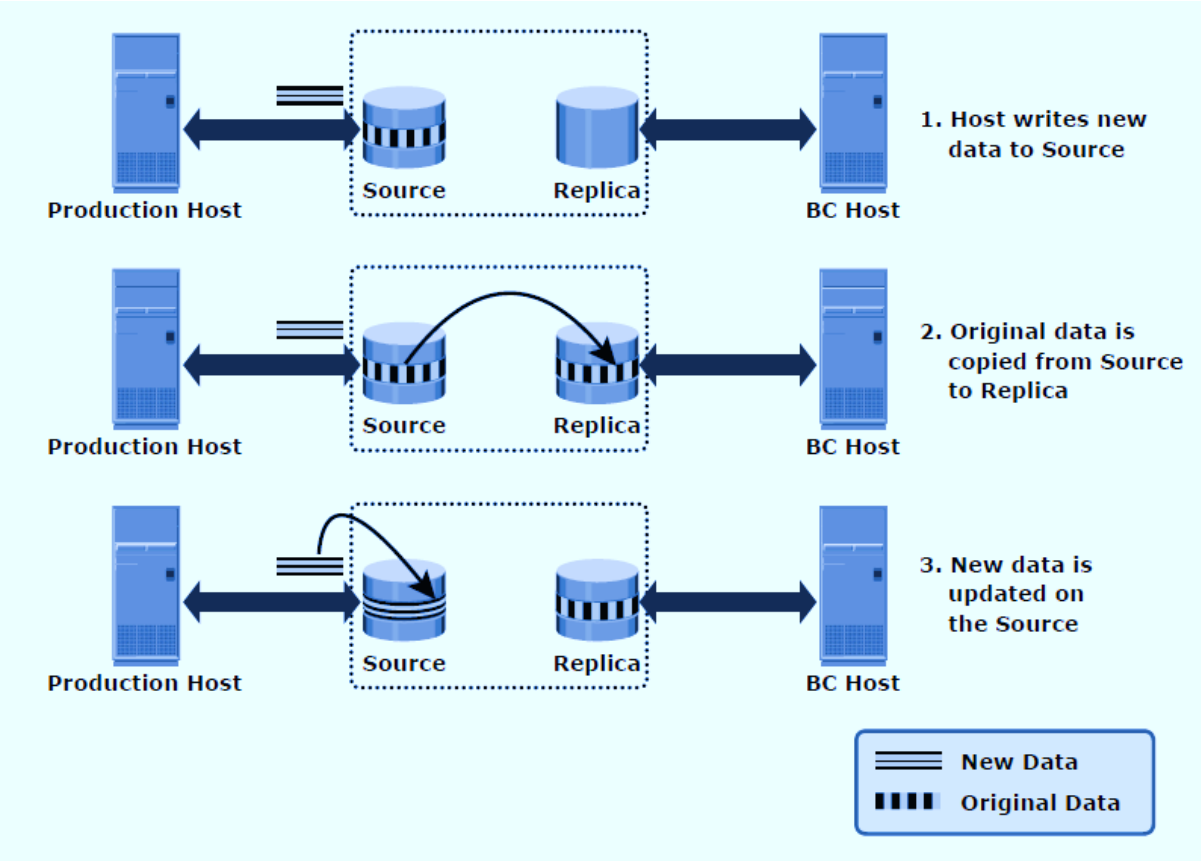

Figure 4.1.8: CoFA – Write to Source

When a read or write operation is issued to the target for the first time after session activation, the original data gets copied from the source to target. However, in case of the read operation, after the copying of data it is made available to the host. In case of the write operation, after the copying of data, new data is updated on the target.

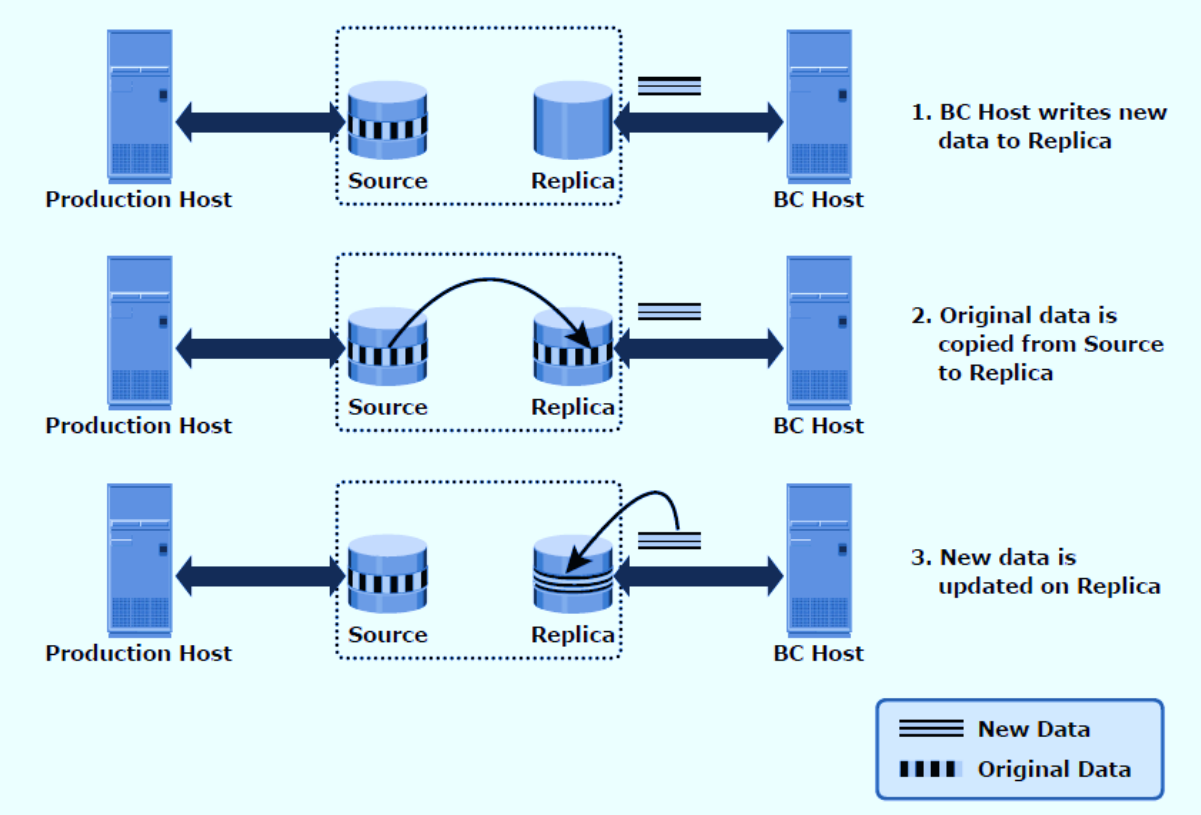

Figure 4.1.9: CoFA – Write to Target

In case the replication session gets terminated in between, then the target only contains the data accessed until the termination and not the entire content of the source at that point-in-time. Hence, in such case, the target cannot be used for recovery or restoration as it is not a complete replica of the source.

In both the full volume mirroring and pointer-based full volume replication, the target device needs to be as large as the source device to store the same amount of data.

Pointer-Based Virtual Replication

In this technique, when the backup session is activated, the target contains the pointers to the location of data on the source. At any time, the target does not contain the actual data but only contains the pointer to the data on the source. Hence, the target is also known as a virtual replica.

Similar to a pointer-based full volume replication, a protection bitmap is created for all the data available on the source device and the target is immediately accessible, unlike full volume mirroring. Similar to a file system snapshot, a pointer-based virtual replication also uses the CoFW technology. Granularity can range from 512 byte blocks to 64 KB blocks or greater.

When a write operation is issued to the source for the first time after the session has been activated, original data from the source is copied to a predefined area in the array known as the **save location**. The pointer in the target then points to the data address in the save location. After this, new data is updated on the source.

When a write operation is issued to the target for the first time after the session has been activated, original data gets copied from the source to the save location. The pointer is updated to point to the address in the save location. Another copy of this data is created in the save location. First copy of the original data is then updated with the new data in the save location.

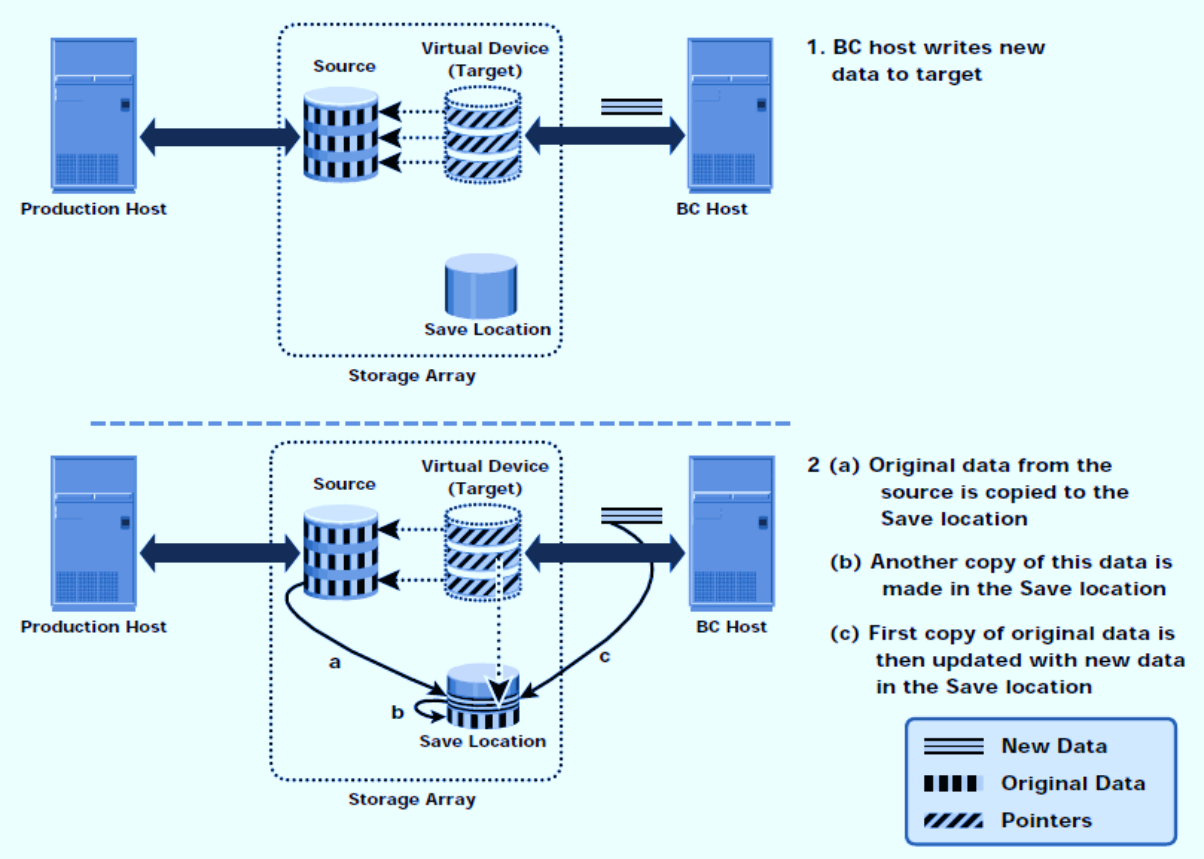

Figure 4.1.10: Pointer-Based Virtual Replication – Write to Target

When a read operation is issued to the target, all the unchanged data blocks since the activation of the session are read from the source and all the original data blocks that have changed are read from the save location.

Data present on the target is a combined view of both the unchanged data on the source and the changed data on the save location. Since the target only contains the pointers to data, it only consumes a fraction of the physical space as compared to the source device. However, the

physical capacity required by the save location is dependent on the amount of the expected change in data.

Self-assessment Questions

11) Which of the following provides incremental resynchronisation? Choose all that apply.

a) File system snapshot
b) Full volume mirroring
c) LVM-based local replication
d) Full Copy Mode

12) Which of the following uses the Copy on First Write (CoFW) technology?

a) Full volume mirroring
b) Pointer-based virtual replication
c) File system snapshot
d) Pointer-based full volume replication

Summary

- Replication is the process of creating an exact copy of the data.
- Local replication refers to the replication of data locally within the same disk storage array or same data centre.
- A host that accesses data from one or more LUNs on the storage array is referred to as a production hosts and the LUNs are known as source LUNs, production LUNs, or simply as source.
- The LUNs where the data replication takes place are known as target LUNs or simple as target or replica.
- Local replicas provide several benefits, such as servers as an alternative backup, provides fast recovery, provides decision-support activities, provides a testing platform and helps in data migration.
- Data consistency refers to the requirement that the data remains constant in time as well as can be used for various transactions without changing their structure.
- Fsck is a system utility tool that stands for file system consistency check. It is required for checking the consistency of the file system in Unix and Unix-like operating systems, such as Linux. CHKDSK plays the same role in Windows.
- The dependent write I/O principle states that an application cannot issue a write I/O command, until a previous-related I/O command gets completed.
- In host-based local replication, the replication process is performed by the LVMs or the file systems.
- LVM mirroring is a process of writing the data to two physical partitions that are mapped by a logical partitioning in a logical volume simultaneously.
- A file system snapshot is a pointer-based replica that only requires a fraction of the space consumed by the original file system.
- Full-volume mirroring and pointer-based full-volume replication in Full Copy mode can provide incremental resynchronisation or restore capability.

- The key difference between pointer-based replica in Full Copy mode and full-volume mirroring is that the target is immediately accessible on session activation in Full Copy mode. In contrast, one has to wait for synchronisation and detachment to access the target in full-volume mirroring.

Terminal Questions

1. Explain the uses of local replication in various business operations.
2. Explain storage array-based replication along with its categories.
3. What is the CoFW principle? Discuss the technologies that follow this principle in the backup and recovery environment.

Answer Keys

Self-assessment Questions	
Question No.	Answer
1	d
2	a, b, c, d
3	d
4	d
5	b
6	b
7	c
8	b
9	a
10	b
11	b, d
12	b, c

Activity

Activity Type: Offline **Duration:** 30 Minutes

Description:

Conduct a debate or discussion on the following topics:

1. Consistency should be ensured in file system and database replication
2. Pros and cons of storage array based replication

Case Study

An administrator configures six pointer based virtual replica of a LUN and creates eight full volume replica of the same LUN. The administrator then creates four pointer based virtual replica for each full volume replica that was created.

a) How many usable replicas are now available?

b) What are the benefits of having replicas?

Bibliography

e-References

- *Host-Based Replication*. (2016). *Enterprisestorageforum.com*. Retrieved from http://www.enterprisestorageforum.com/backup-recovery/host-based-replication-1.html
- Rouse, M. & Hillard, J. (2016). *What is array-based replication? SearchDisasterRecovery*. Retrieved from http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication
- Amir, Y., Danilov, C., Stanton, J., Miskin-Amir, M., & Tutu, C. (2003). *On the Performance of Consistent Wide-Area Database Replication* (1st ed.). Retrieved from http://www.cnds.jhu.edu
- *LVM*. (2016). *Wiki.ubuntu.com*. Retrieved 11 July 2016, from https://wiki.ubuntu.com/Lvm

Image Credits

- Figure 4.1.1: http://www.howtogeek.com/wp-content/uploads/2011/09/656x488xFile-Sharing.png.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic.51X4feiHqb.png
- Figure 4.1.3: http://www.howtogeek.com/wp-content/uploads/2011/09/405x543xNTFS-Dialog.png.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic.6G6Zlk5dRo.png
- Figure 4.1.4: Information Storage and Management: Storing, Managing and Protecting Digital Information
- Figure 4.1.5: www.girtab.ucc.ie/jmcavoy/IS6113/IS6113k%20local%20replication.pdf
- Figure 4.1.6: http://images.slideplayer.com/25/8029985/slides/slide_15.jpg
- Figure 4.1.7: Information Storage and Management: Storing, Managing and Protecting Digital Information
- Figure 4.1.8: Information Storage and Management: Storing, Managing and Protecting Digital Information

- Figure 4.1.9: Information Storage and Management: Storing, Managing and Protecting Digital Information
- Figure 4.1.10: Information Storage and Management: Storing, Managing and Protecting Digital Information

External Resources

- Somasundaram, G. & Shrivastava, A. (2009) *Information storage and management* - Storing, managing and protecting digital information. *Indianapolis, Ind.: Wiley Pub.*
- Dufrasne, B., Eriksson, R., Martinez, L., & Kalabza, W. (2014). *IBM XIV Storage System Architecture and Implementation* (9th ed.). International Business Machines Corporation.

Video Links

Topic	Link
Host-based replication	https://www.youtube.com/watch?v=LIlT3YKNgvI
Replication vs. backup	https://www.youtube.com/watch?v=Fs0XtfLNI8I
Replication techniques	https://www.youtube.com/watch?v=L3WM1p3ErSM

Notes: