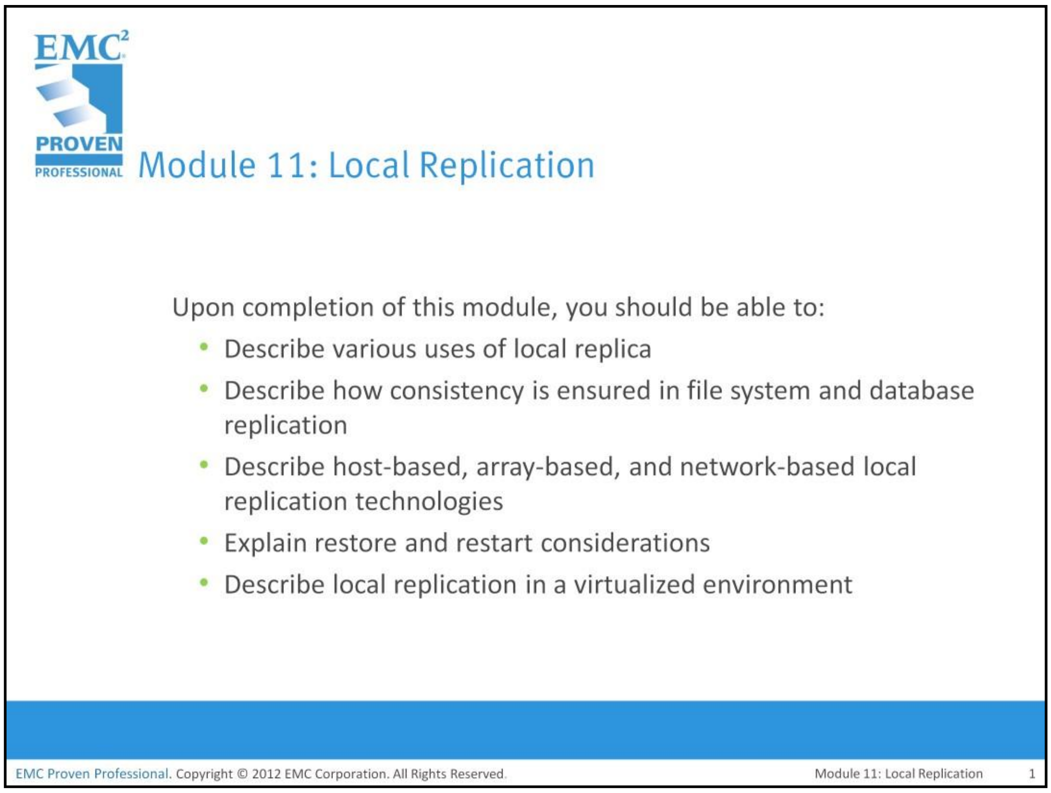
Module – 11
Local Replication



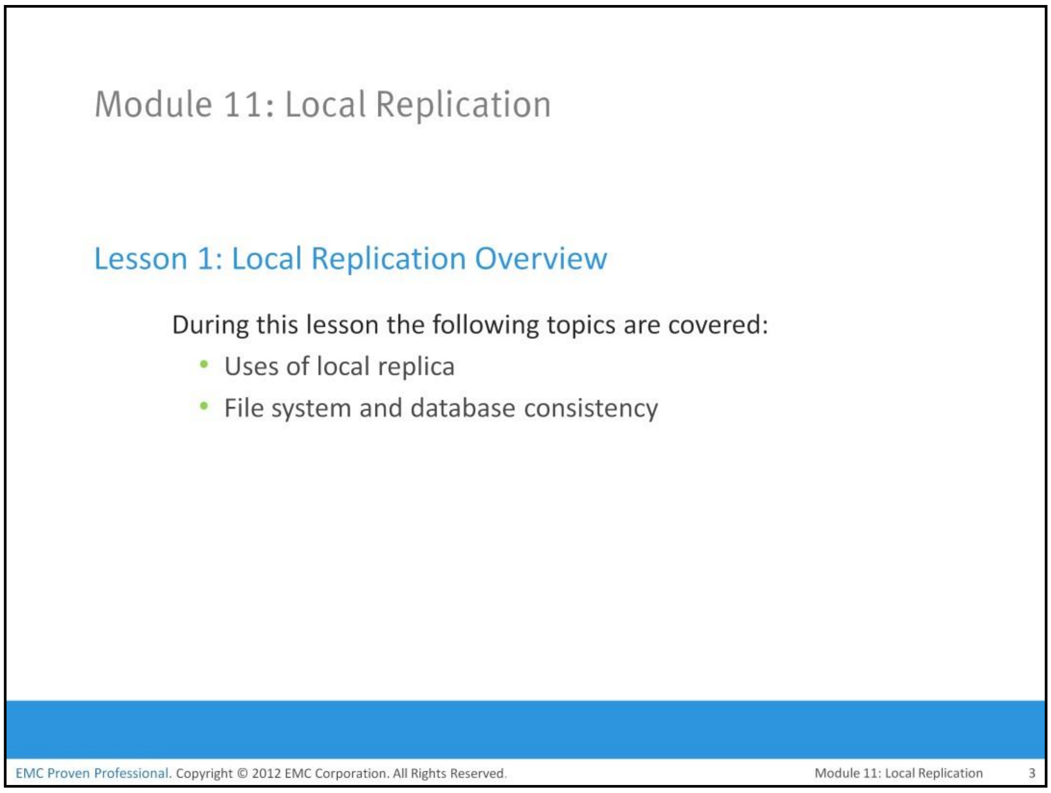
Module 11: Local Replication

Upon completion of this module, you should be able to:

- Describe various uses of local replica
- Describe how consistency is ensured in file system and database replication
- Describe host-based, array-based, and network-based local replication technologies
- Explain restore and restart considerations
- Describe local replication in a virtualized environment

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 1

This module focuses on various uses of local replica along with file system and database consistency in replication. This module also focuses on various host-based, storage-based, and network-based local replication technologies. Further, this module focuses on restore and restart considerations. Additionally, this module details local replication in a virtualized environment.



Module 11: Local Replication

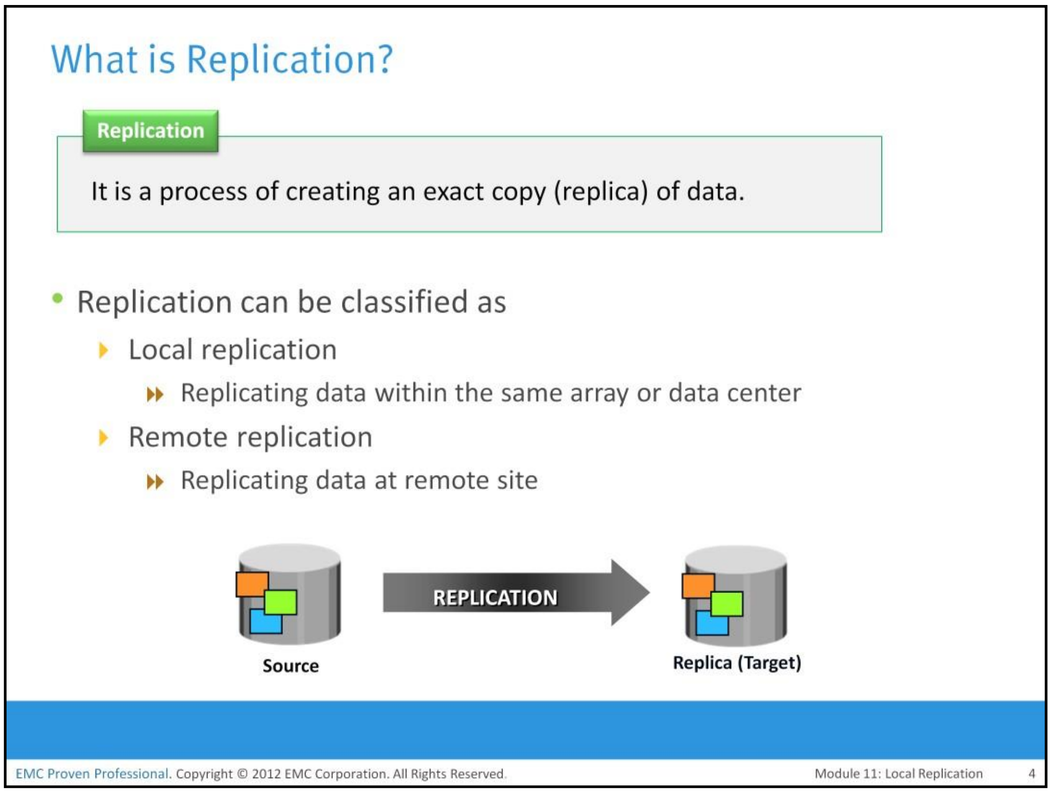
Lesson 1: Local Replication Overview

During this lesson the following topics are covered:

- Uses of local replica
- File system and database consistency

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 3

This lesson covers various uses of local replica and also covers how consistency is ensured in file system and database replication.

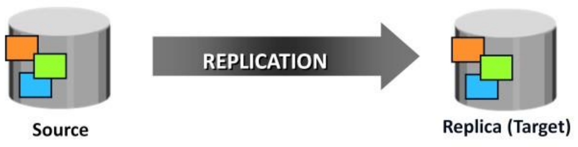


What is Replication?

Replication

It is a process of creating an exact copy (replica) of data.

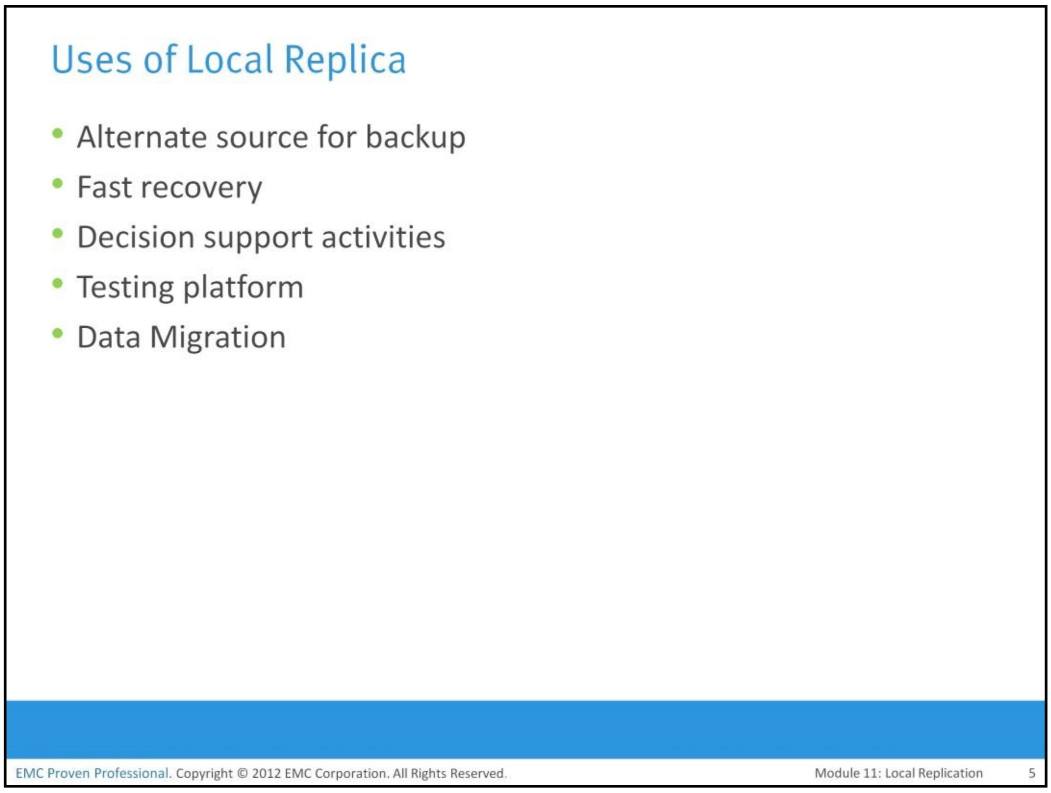
- Replication can be classified as
  - Local replication
    - Replicating data within the same array or data center
  - Remote replication
    - Replicating data at remote site



EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 4

In today’s business environment, it is imperative for an organization to protect mission-critical data and minimize the risk of business disruption. If a local outage or disaster occurs, fast data restore and restart is essential to ensure business continuity (BC). Replication is one of the ways to ensure BC. It is the process to create an exact copy (replica) of data. These replica copies are used for restore and restart operations if data loss occurs. These replicas can also be assigned to other hosts to perform various business operations, such as backup, reporting, and testing.

Replication can be classified into two major categories: local and remote. Local replication refers to replicating data within the same array or the same data center. Remote replication refers to replicating data at a remote site. Remote replication is discussed in the next module.



Uses of Local Replica

- Alternate source for backup
- Fast recovery
- Decision support activities
- Testing platform
- Data Migration

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 5

One or more local replicas of the source data may be created for various purposes, including the following:

Alternative source for backup: Under normal backup operations, data is read from the production volumes (LUNs) and written to the backup device. This places an additional burden on the production infrastructure because production LUNs are simultaneously involved in production operations and servicing data for backup operations. 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.

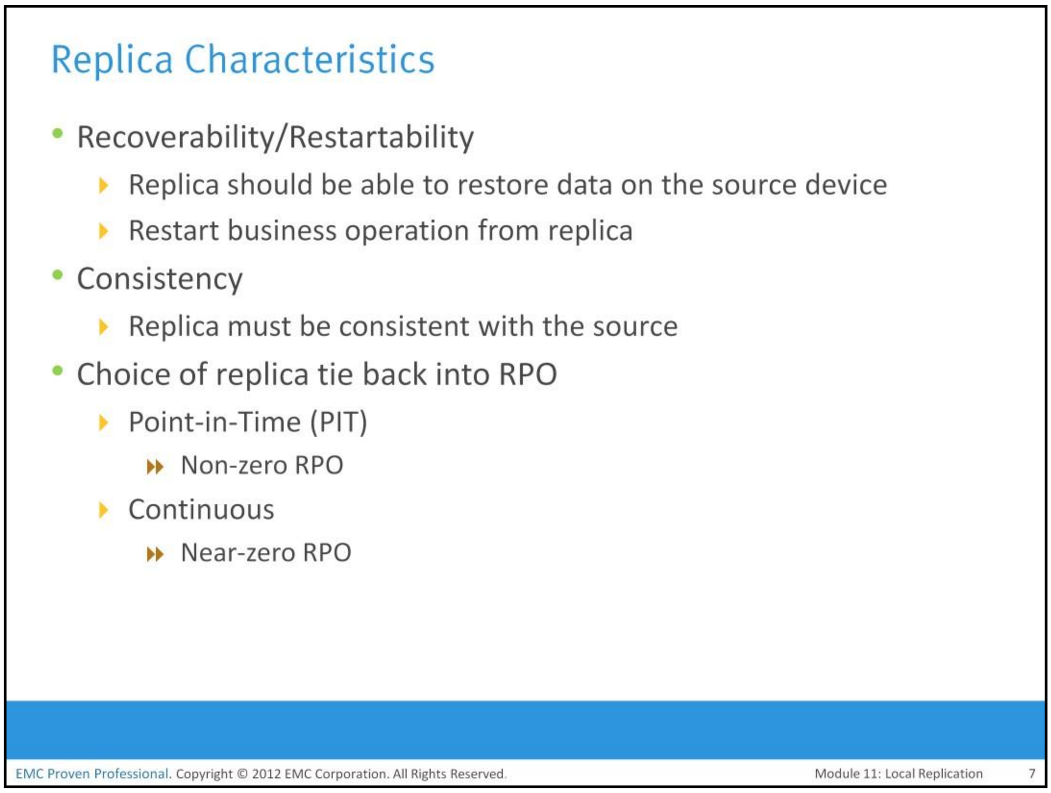
Fast recovery: If data loss or data corruption occurs on the source, a local replica might be used to recover the lost or corrupted data. If a complete failure of the source occurs, some replication solutions enable replica to be used to restore data on to a different set of source devices or production can be restarted on the replica. In either case, this method provides faster recovery and minimal RTO compared to traditional recovery from tape backups.

Cont..

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. Local replicas are also used for data-warehousing applications. 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. For example, an organization may use the replica to test the production application upgrade; if the test is successful, the upgrade may be implemented on the production environment.

Data migration: Another use for a local replica is 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.


Replica Characteristics

- Recoverability/Restartability
  - Replica should be able to restore data on the source device
  - Restart business operation from replica
- Consistency
  - Replica must be consistent with the source
- Choice of replica tie back into RPO
  - Point-in-Time (PIT)
    - Non-zero RPO
  - Continuous
    - Near-zero RPO

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 7

A replica should have following characteristics:

Recoverability: Enables restoration of data from the replicas to the source if data loss or corruption occurs.

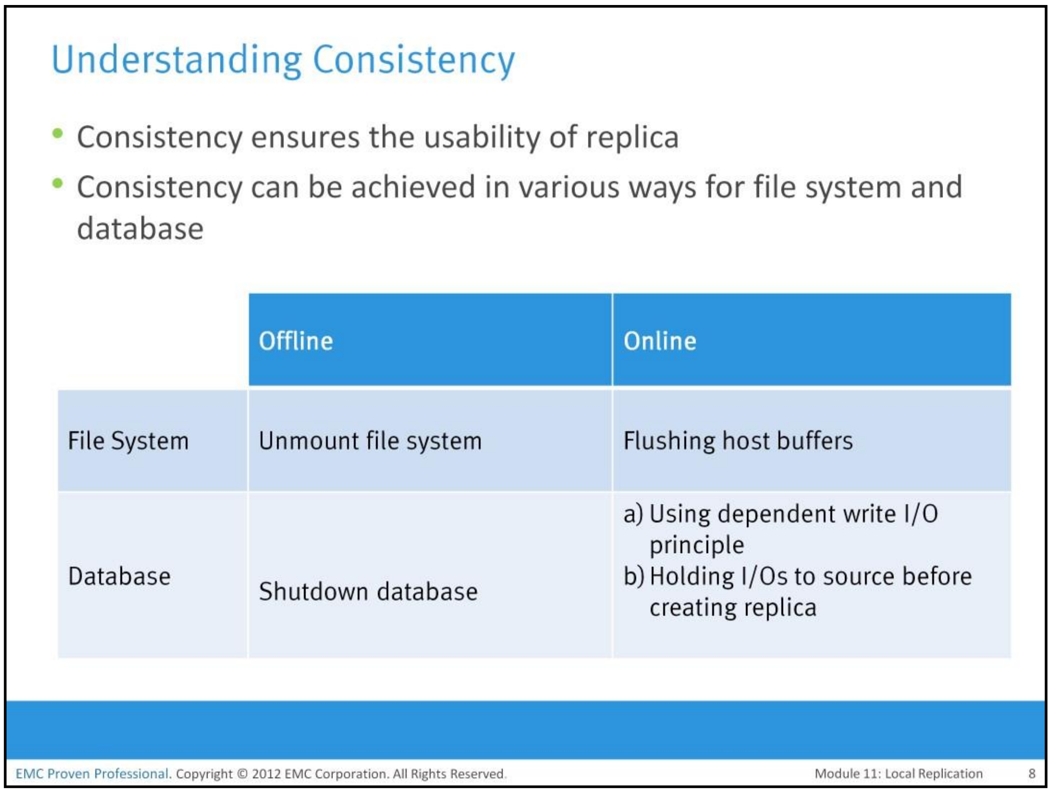
Restartability: Enables restarting business operations using the replicas.

Consistency: Replica must be consistent with the source so that it is usable for both recovery and restart operations. Ensuring consistency is the primary requirement for all the replication technologies.

Replicas can either be point-in-time (PIT) or continuous:

Point-in-Time: The data on the replica is an identical image of the production at some specific timestamp. For example, a replica of a file system is created at 4:00 PM on Monday. This replica would then be referred to as the Monday 4:00 PM PIT copy. The RPO will map to the time when the PIT was created to the time when any kind of failure on the production occurred. If there is a failure on the production at 8:00 PM and there is a 4:00 PM PIT available, the RPO would be 4 hours (8 – 4 = 4). To minimize RPO, take periodic PITs.

Continuous replica: The data on the replica is in-sync with the production data at all times. The objective with any continuous replication is to reduce the RPO to zero or near-zero.

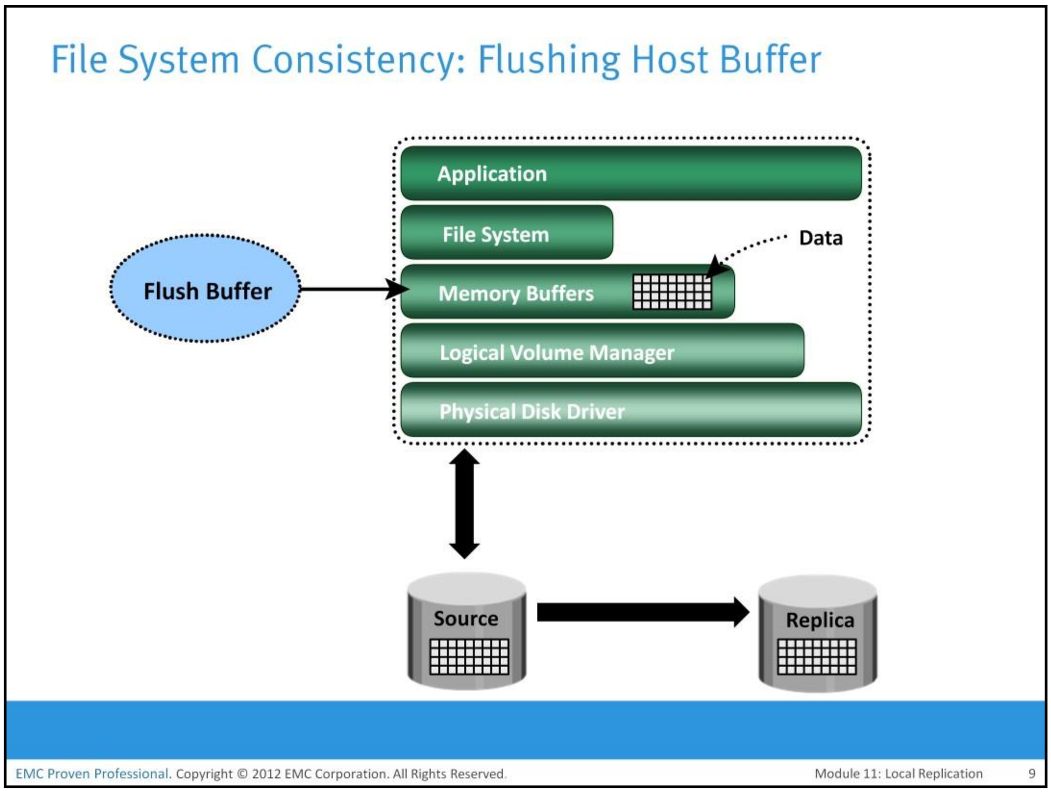


Understanding Consistency

- Consistency ensures the usability of replica
- Consistency can be achieved in various ways for file system and database

	Offline	Online
File System	Unmount file system	Flushing host buffers
Database	Shutdown database	a) Using dependent write I/O principle b) Holding I/Os to source before creating replica

Consistency is a primary requirement to ensure the usability of replica device. In case of file systems, consistency can be achieved either by taking FS offline i.e. by un-mounting FS or by keeping FS online by flushing host buffers before creating replica. Similarly in case of databases, consistency can be achieved either by taking database offline for creating consistent replica or by keeping online. Consistent replica of online database can be created by using dependent write I/O principle or by holding I/Os before creating replica.

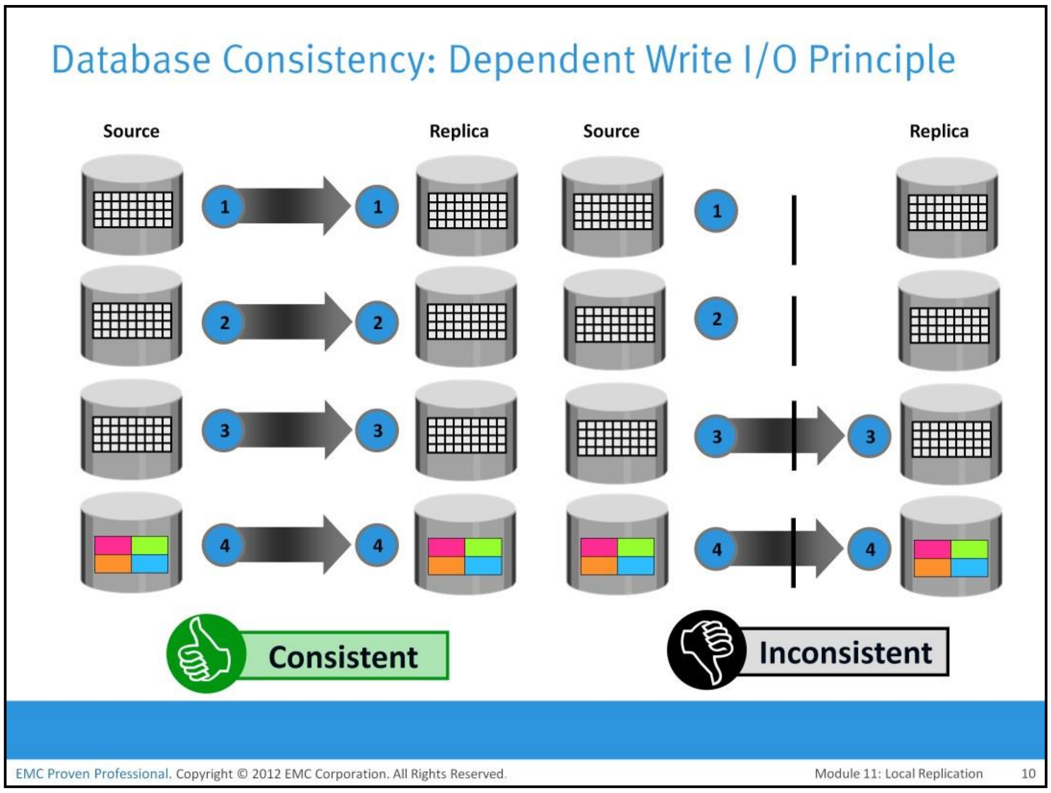


File System Consistency: Flushing Host Buffer

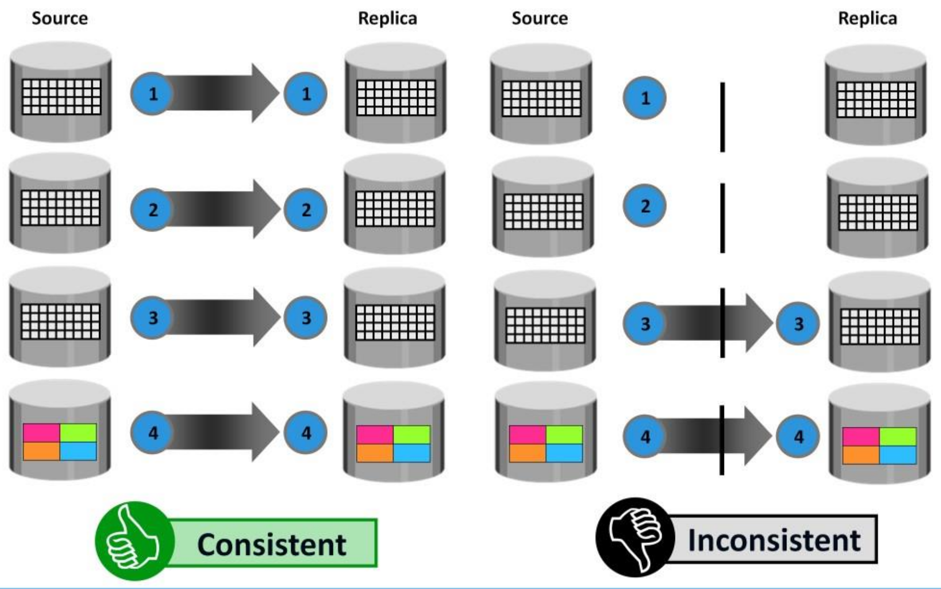
Module 11: Local Replication 9

File systems buffer the data in the host memory to improve the application response time. The buffered data is periodically written to the disk. In UNIX operating systems, *sync daemon* is the process that flushes the buffers to the disk at set intervals. In some cases, the replica is created between the set intervals, which might result in the creation of an inconsistent replica. Therefore, host memory buffers must be flushed to ensure data consistency on the replica, prior to its creation. If the host memory buffers are not flushed, the data on the replica will not contain the information that was buffered in the host. If the file system is unmounted before creating the replica, the buffers will be automatically flushed and the data will be consistent on the replica.

If a mounted file system is replicated, some level of recovery, such as *fsck* or *log replay*, is required on the replicated file system. When the file system replication and check process are completed, the replica file system can be mounted for operational use.



Database Consistency: Dependent Write I/O Principle



EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 10

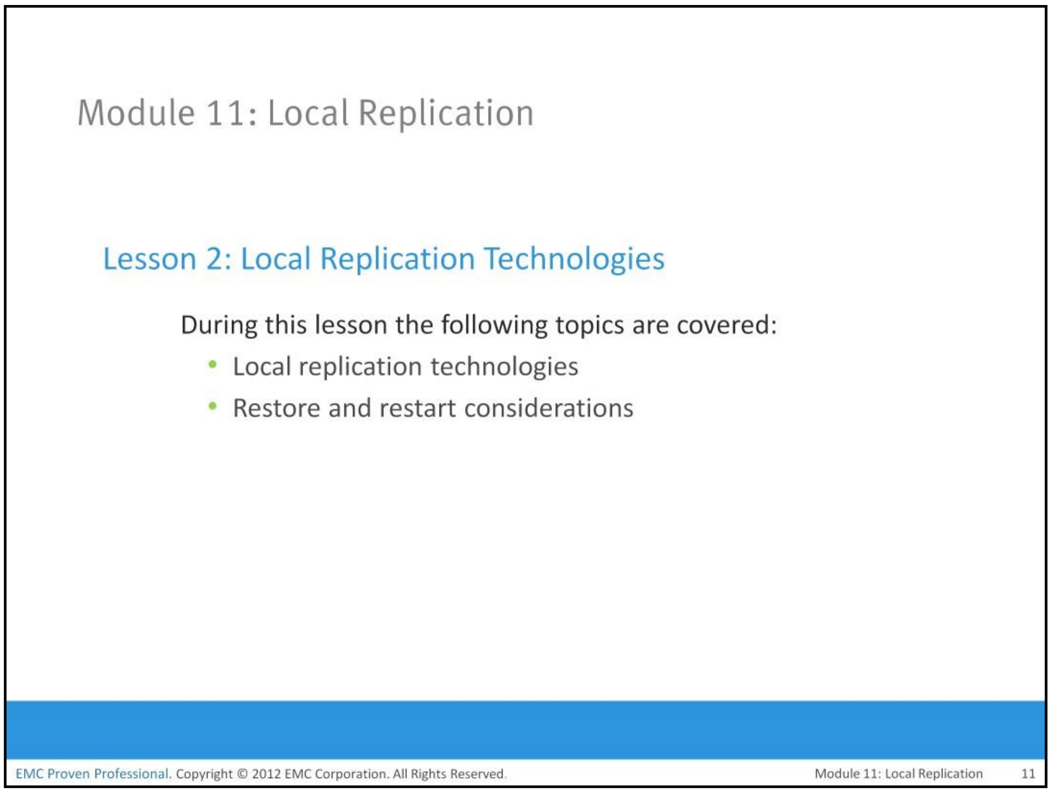
If the database is online, it is available for I/O operations, and transactions to the database update the data continuously. When a database is replicated while it is online, changes made to the database at this time must be applied to the replica to make it consistent. A consistent replica of an online database is created by using the dependent write I/O principle or by holding I/Os momentarily to the source before creating the replica.

A *dependent write I/O* principle is inherent in many applications and database management systems (DBMS) to ensure consistency. According to this principle, a write I/O is not issued by an application until a prior related write I/O has completed. For example, a data write is dependent on the successful completion of the prior log write.

For a transaction to be deemed complete, databases require a series of writes to have occurred in a particular order. These writes will be recorded on the various devices/file systems.

When the replica is created, all the writes to the source devices must be captured on the replica devices to ensure data consistency. Figure on the slide illustrates the process of replication from the source to the replica. The I/O transactions 1 to 4 must be carried out for the data to be consistent on the replica. It is possible that I/O transactions 3 and 4 were copied to the replica devices, but I/O transactions 1 and 2 were not copied. Figure on the slide also shows this situation. In this case, the data on the replica is inconsistent with the data on the source. If a restart were to be performed on the replica devices, I/O 4, which is available on the replica, might indicate that a particular transaction is complete, but all the data associated with the transaction will be unavailable on the replica, making the replica inconsistent.

Another way to ensure consistency is to make sure that the write I/O to all source devices is held for the duration of creating the replica. This creates a consistent image on the replica. However, databases and applications might time out if the I/O is held for too long.



Module 11: Local Replication

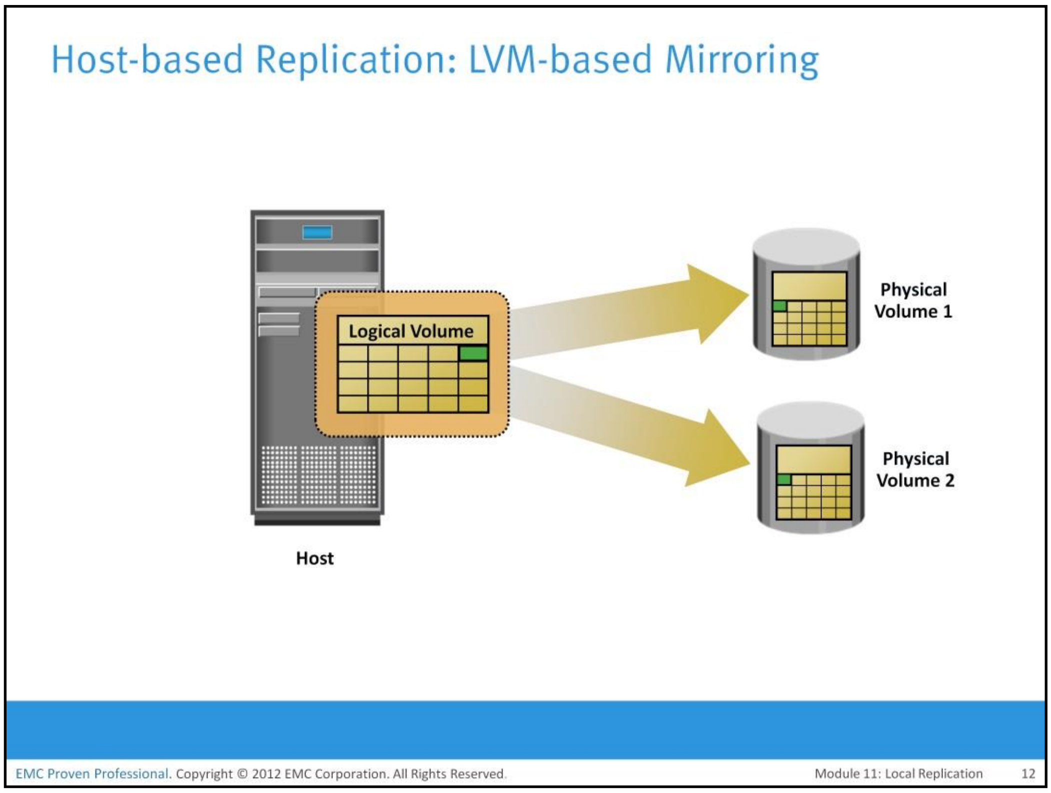
Lesson 2: Local Replication Technologies

During this lesson the following topics are covered:

- Local replication technologies
- Restore and restart considerations

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 11

This lesson covers various host-based, network-based and storage array-based local replication technologies and also covers restore and restart considerations.



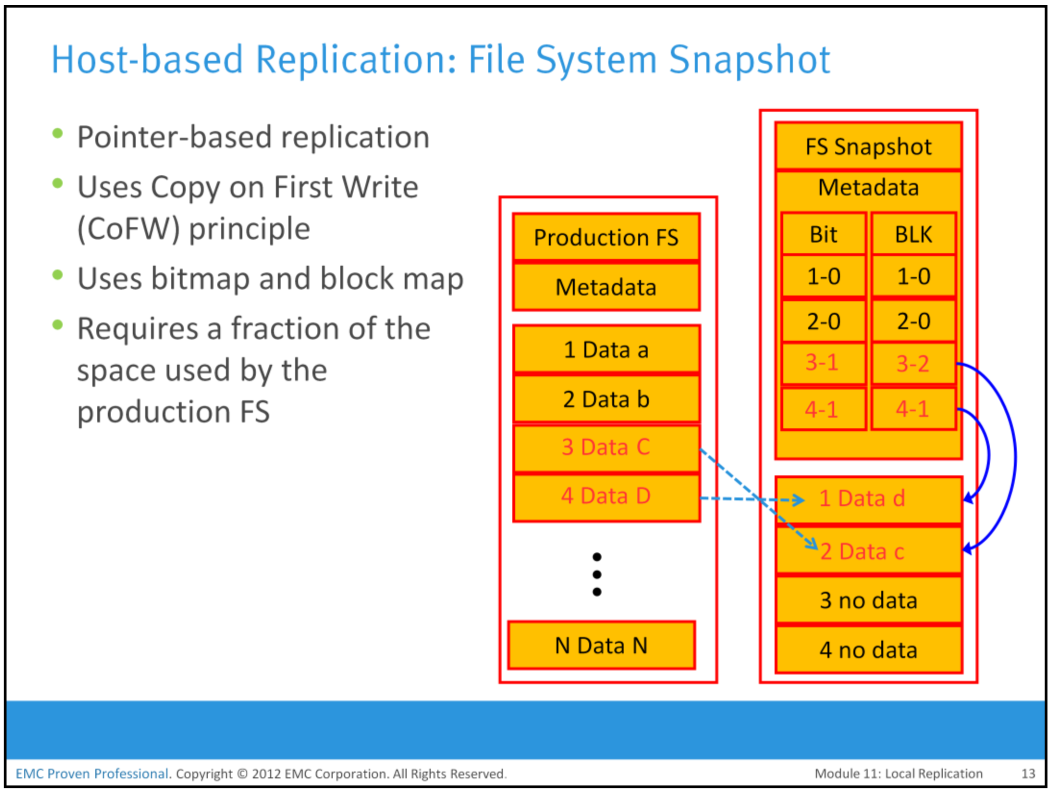
Host-based Replication: LVM-based Mirroring

Module 11: Local Replication 12

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. A volume group can have multiple logical volumes. In LVM-based replication, each *logical block* in a logical volume is mapped to two physical blocks on two different physical volumes, as shown in figure on the slide. 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*. Mirrors can be split, and the data contained therein can be independently accessed.

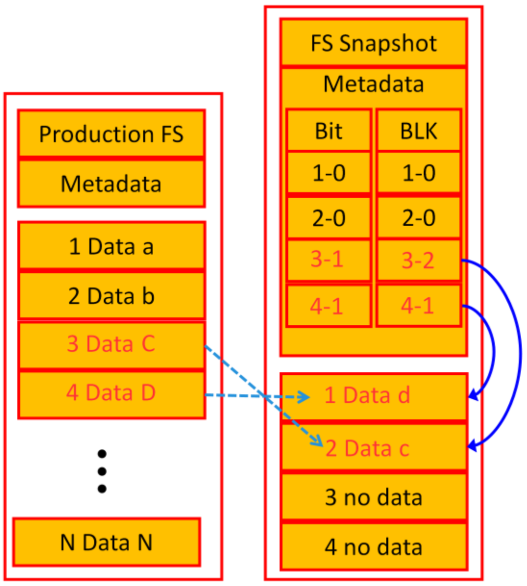
Advantages: The LVM-based replication technology is not dependent on a vendor-specific storage system. Typically, LVM is part of the operating system, and no additional license is required to deploy LVM mirroring.

Limitations: 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. Presenting an LVM-based local replica to another host is usually not possible because the replica will still be part of the volume group, which is usually accessed by one host at any given time. If the devices are already protected by some level of RAID on the array, then the additional protection that the LVM mirroring provides is unnecessary. This solution does not scale to provide replicas of federated databases and applications. Both the replica and source are stored within the same volume group. Therefore, the replica might become unavailable if there is an error in the volume group. If the server fails, both the source and replica are unavailable until the server is brought back online.



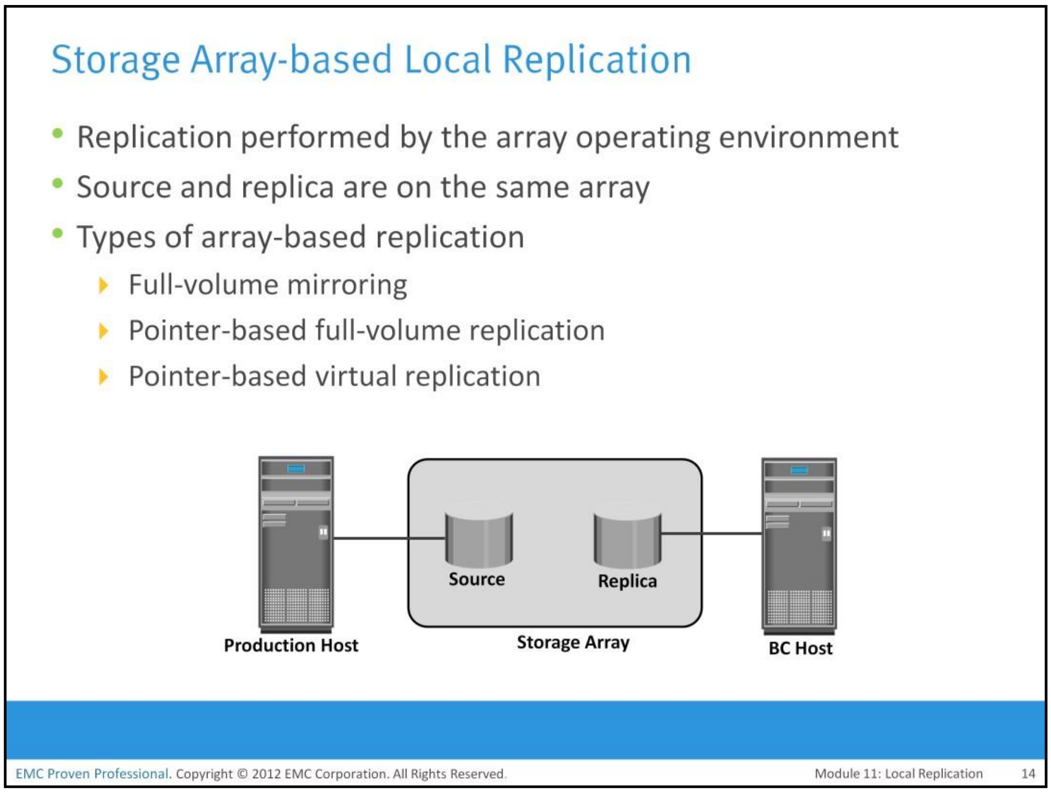
Host-based Replication: File System Snapshot

- Pointer-based replication
- Uses Copy on First Write (CoFW) principle
- Uses bitmap and block map
- Requires a fraction of the space used by the production FS



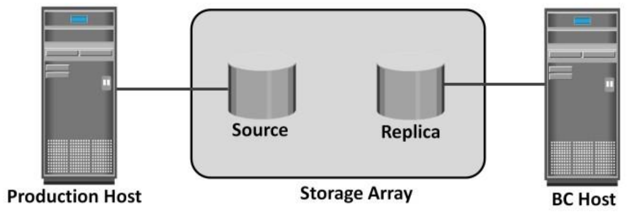
EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 13

File system (FS) snapshot is a pointer-based replica that requires a fraction of the space used by the production FS. It uses the Copy on First Write (CoFW) principle to create snapshots. When a snapshot is created, a bitmap and blockmap are 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 blockmap is used to indicate the exact address from which the data is to be read when the data is accessed from the Snap FS. Immediately after the creation of the FS Snapshot, all reads from the snapshot are actually served by reading the production FS. 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. Subsequent writes to the same location will not initiate the CoFW activity. 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 blockmap and the data is read from that address on the snap FS. Read requests from the production FS work as normal.



Storage Array-based Local Replication

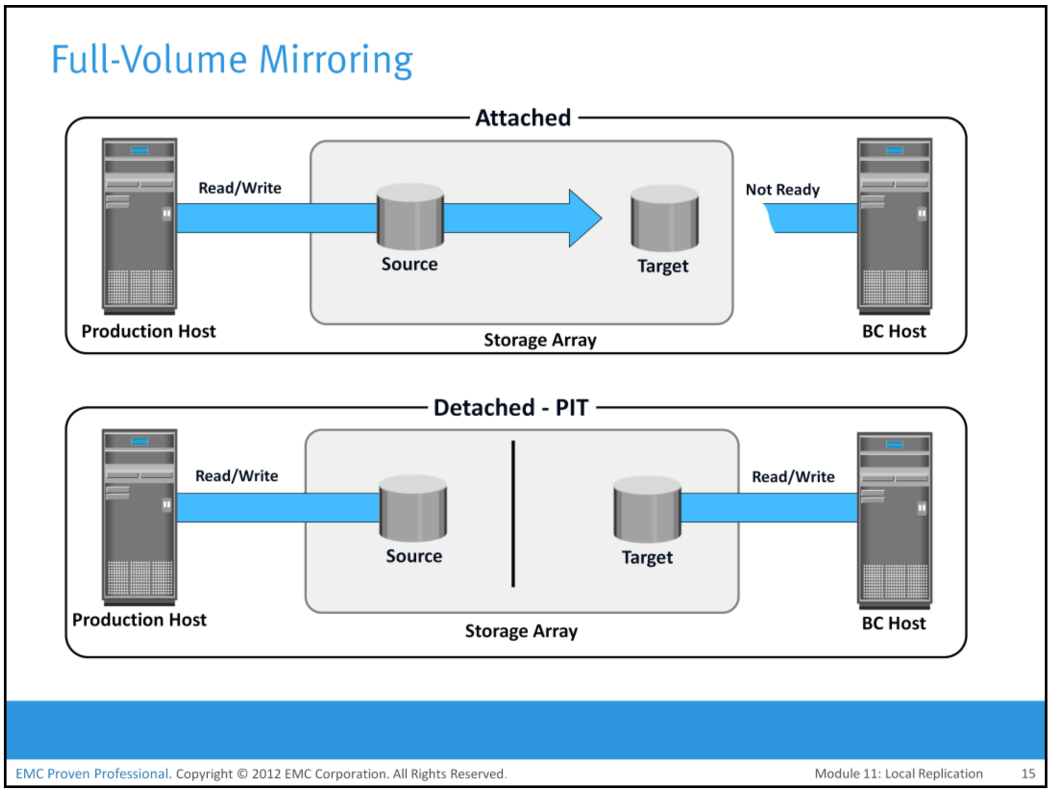
- Replication performed by the array operating environment
- Source and replica are on the same array
- Types of array-based replication
  - Full-volume mirroring
  - Pointer-based full-volume replication
  - Pointer-based virtual replication



Module 11: Local Replication 14

In *storage array-based local replication*, 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. Consequently, the host is not burdened by the replication operations. The replica can be accessed by an alternate host for other business operations.

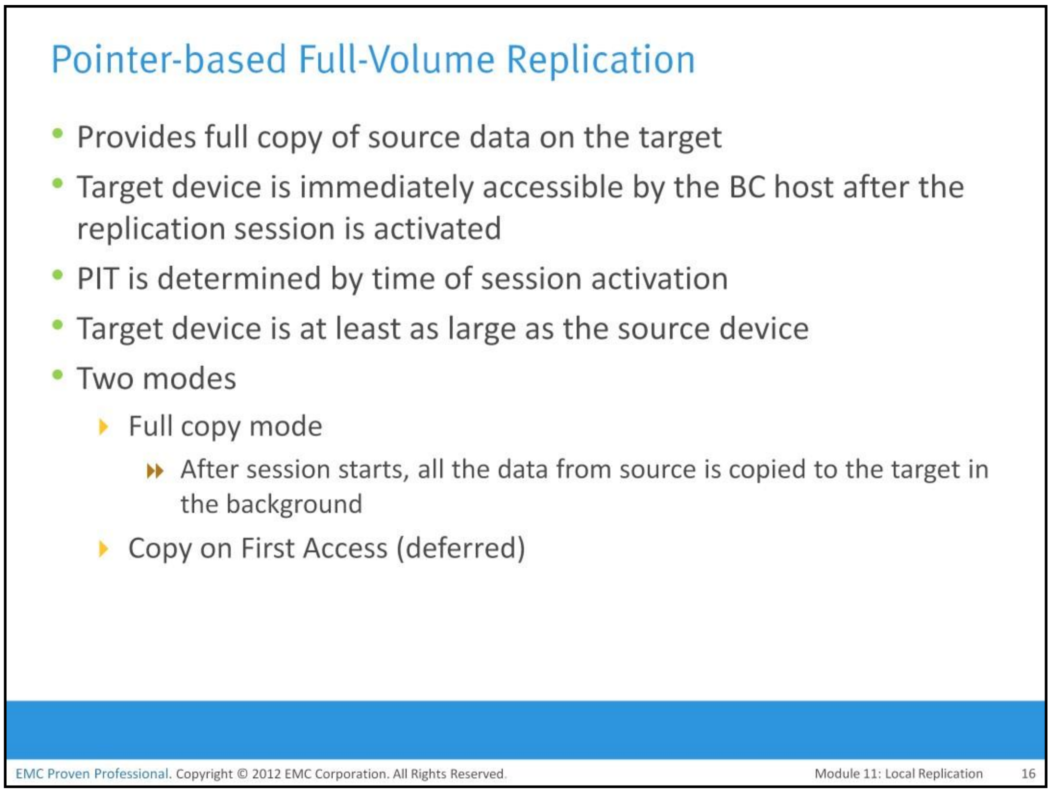
In this replication, the required number of replica devices should be selected on the same array and then data should be replicated between the source-replica pairs. Figure on the slide shows a storage array-based local replication, where the source and target (replica) are in the same array and accessed by different hosts. Storage array-based local replication is commonly implemented in three ways full-volume mirroring, pointer-based full-volume replication, and 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. The data on the source is copied to the target. New updates to the source are also updated on the target. After all the data is copied and both the source and the target contain identical data, the target can be considered as a mirror of the source. While the target is attached to the source it remains unavailable to any other host. However, the production host continues to access the source.

After the synchronization is complete, the target can be detached from the source and made available for other business operations. Both the source and the target can be accessed for read and write operations by the production and business continuity hosts respectively. After detaching from the source, the target becomes a point-in-time (PIT) copy of the source. The PIT of a replica is determined by the time when the target is detached from the source. For example, if the time of detachment is 4:00 pm., the PIT for the target is 4:00 pm. After detachment, changes made to both the source and replica can be tracked at some predefined granularity. This enables incremental resynchronization (source to target) or incremental restore (target to source). The granularity of the data change can range from 512 byte blocks to 64 KB blocks or higher.


Pointer-based Full-Volume Replication

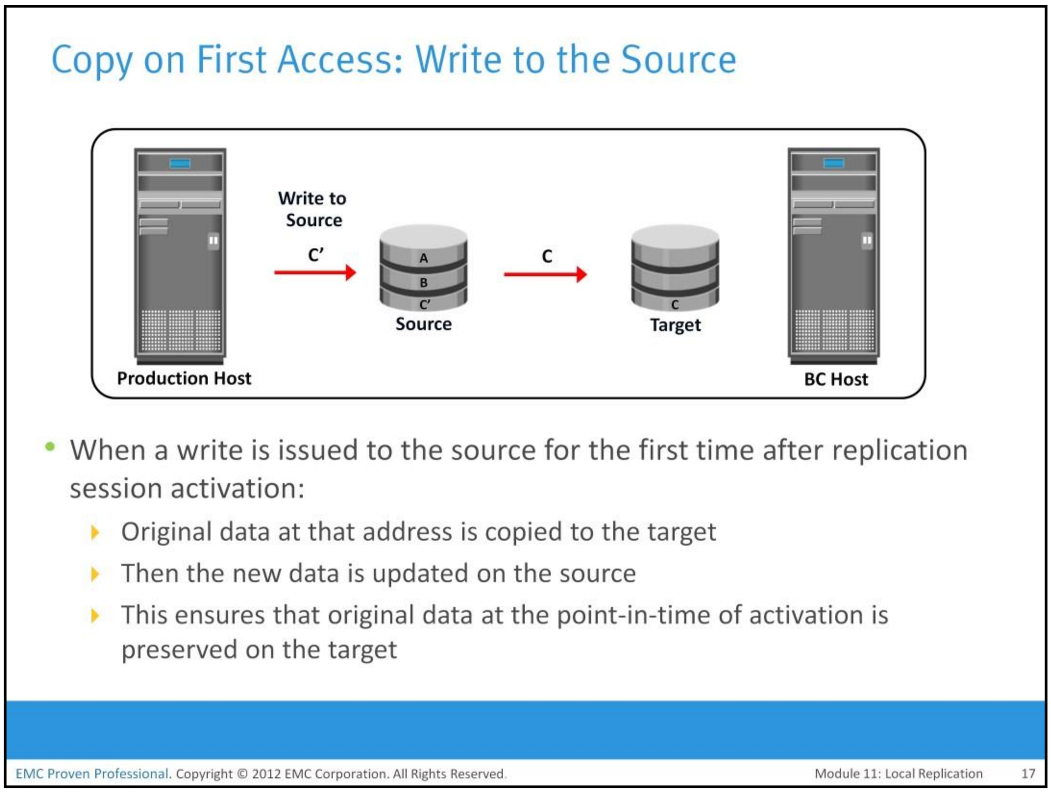
- Provides full copy of source data on the target
- Target device is immediately accessible by the BC host after the replication session is activated
- PIT is determined by time of session activation
- Target device is at least as large as the source device
- Two modes
  - Full copy mode
    - After session starts, all the data from source is copied to the target in the background
  - Copy on First Access (deferred)

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 16

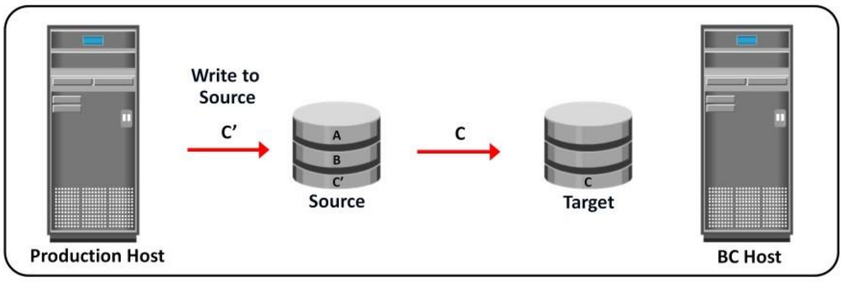
Another method of array-based local replication is *pointer-based full-volume replication*. Similar to full-volume mirroring, this technology can provide full copies of the source data on the targets. Unlike full-volume mirroring, the target is immediately accessible by the BC host after the replication session is activated. Therefore, data synchronization and detachment of the target is not required to access it. Here, the time of replication session activation defines the PIT copy of the source.

Pointer-based, full-volume replication can be activated in either Copy on First Access (CoFA) mode or 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. The data is then copied from the source to the target based on the mode of activation.

In a Full Copy mode, all data from the source is copied to the target in the background. Data is copied regardless of access. If access to a block that has not yet been copied to the target is required, this block is preferentially copied to the target. In a complete cycle of the Full Copy mode, all data from the source is copied to the target. If the replication session is terminated now, 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 restore or other business continuity operations.



Copy on First Access: Write to the Source



- When a write is issued to the source for the first time after replication session activation:
  - Original data at that address is copied to the target
  - Then the new data is updated on the source
  - This ensures that original data at the point-in-time of activation is preserved on the target

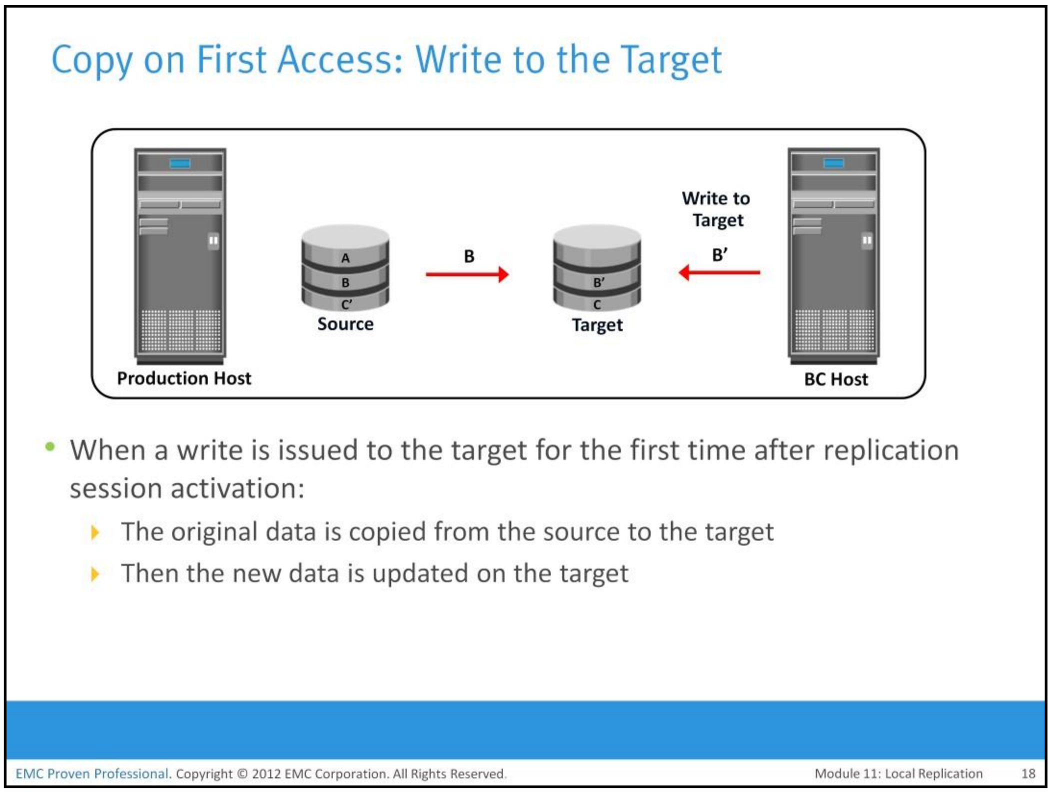
Module 11: Local Replication 17

In CoFA, after the replication session is initiated, the data is copied from the source to the target only when the following condition occurs:

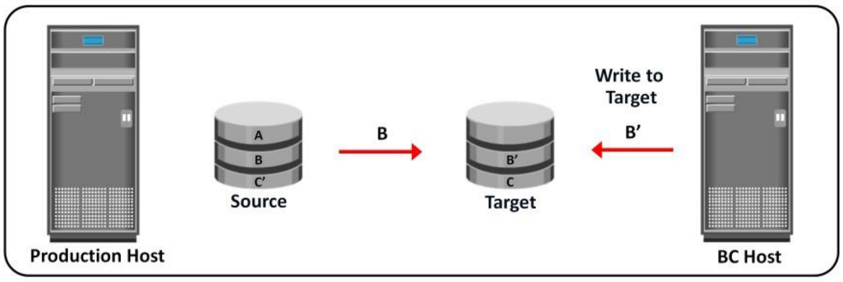
• A write I/O is issued to a specific address on the source for the first time.

• 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.



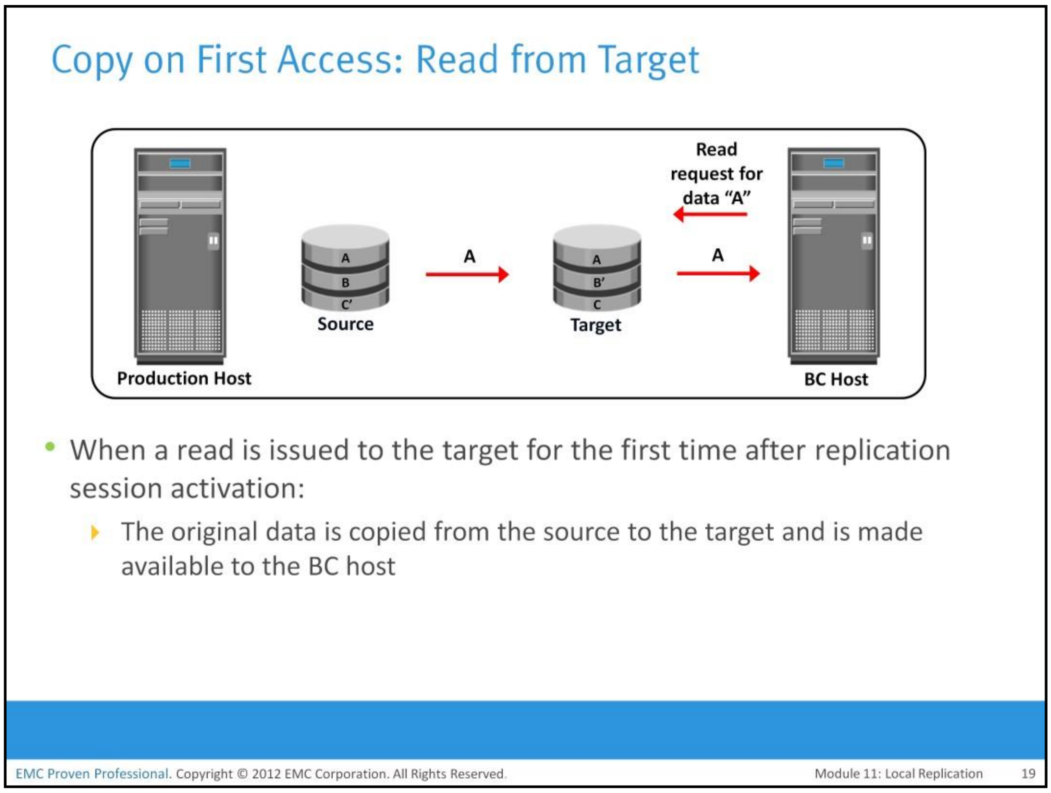
Copy on First Access: Write to the Target



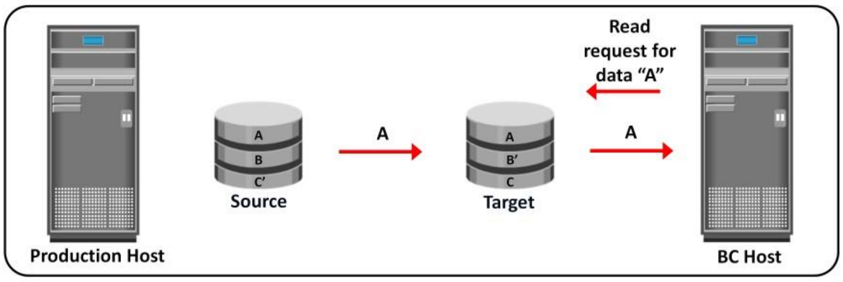
- When a write is issued to the target for the first time after replication session activation:
  - The original data is copied from the source to the target
  - Then the new data is updated on the target

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 18

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 on the slide).



Copy on First Access: Read from Target



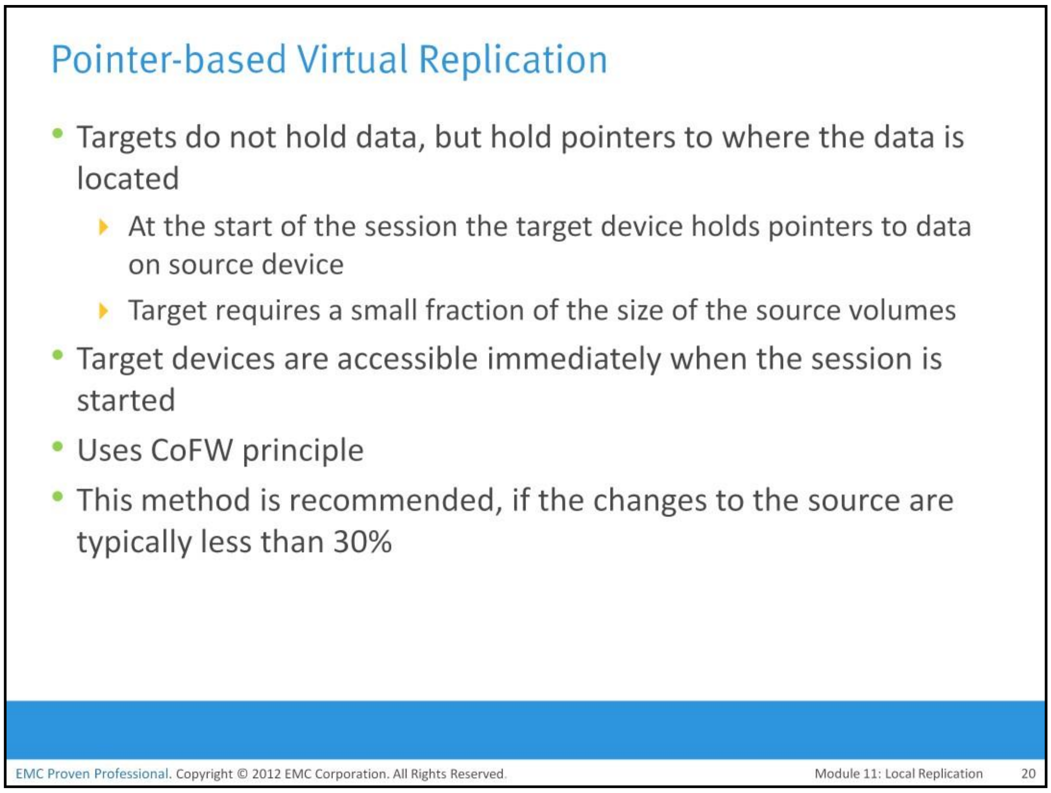
- When a read is issued to the target for the first time after replication session activation:
  - The original data is copied from the source to the target and is made available to the BC host

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 19

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.

In all cases, the protection bit for the data block on the source 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 the reads or writes to the same data blocks on the target, do not trigger a copy operation, therefore this method is termed "Copy on First Access."

If the replication session is terminated, then the target device has only the data that was accessed until the termination, not the entire contents of the source at the point-in-time. In this case, the data on the target cannot be used for restore because it is not a full replica of the source.

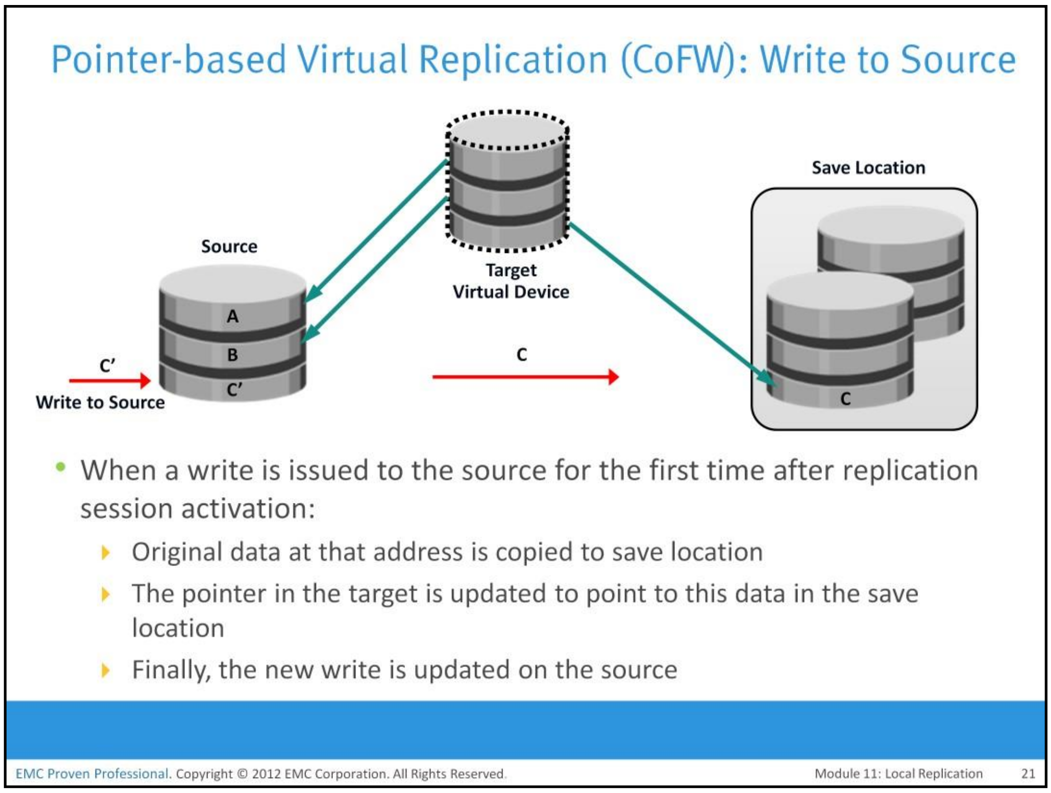


Pointer-based Virtual Replication

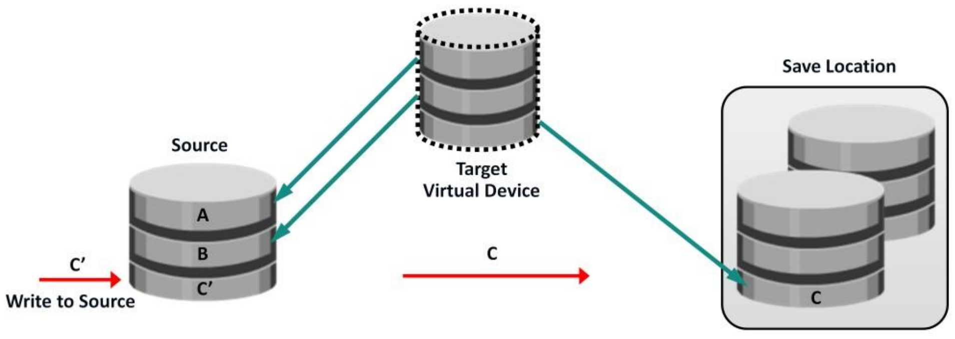
- Targets do not hold data, but hold pointers to where the data is located
  - At the start of the session the target device holds pointers to data on source device
  - Target requires a small fraction of the size of the source volumes
- Target devices are accessible immediately when the session is started
- Uses CoFW principle
- This method is recommended, if the changes to the source are typically less than 30%

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 20

In *pointer-based virtual replication*, at the time of the replication session activation, the target contains pointers to the location of the data on the source. The target does not contain data at any time. Therefore, the target is known as a *virtual replica*. Similar to pointer-based full-volume replication, the target is immediately accessible after the replication session activation. This replication method uses CoFW technology and typically recommended when the changes to the source are less than 30%.

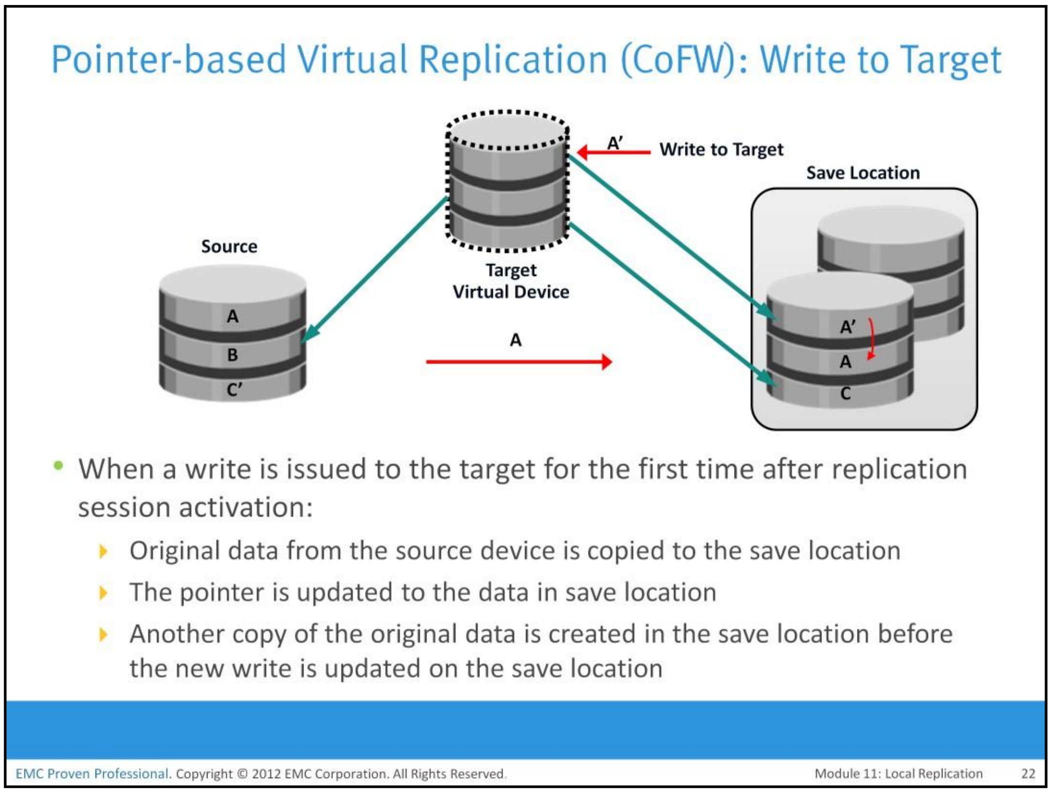


Pointer-based Virtual Replication (CoFW): Write to Source

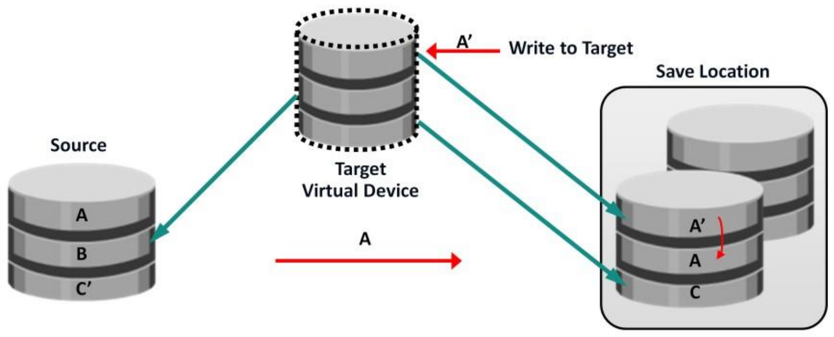


- When a write is issued to the source for the first time after replication session activation:
  - Original data at that address is copied to save location
  - The pointer in the target is updated to point to this data in the save location
  - Finally, the new write is updated on the source

When a write is issued to the source for the first time after the replication session activation, the original data at that address is copied to a predefined area in the array. This area is generally known as the *save location*. The pointer in the target is updated to point to this data in the save location. After this, the new write is updated on the source.



Pointer-based Virtual Replication (CoFW): Write to Target



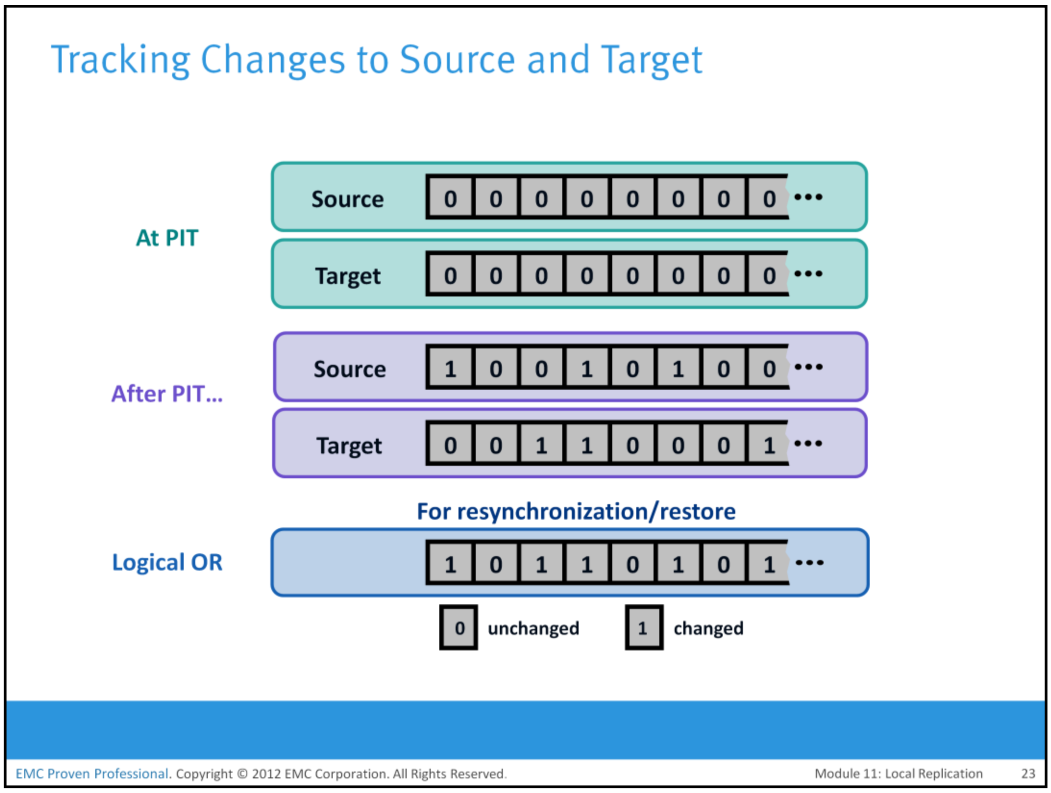
- When a write is issued to the target for the first time after replication session activation:
  - Original data from the source device is copied to the save location
  - The pointer is updated to the data in save location
  - Another copy of the original data is created in the save location before the new write is updated on the save location

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 22

When a write is issued to the target for the first time after replication session activation, the data is copied from the source to the save location, and the pointer is updated to the data in the save location. Another copy of the original data is created in the save location before the new write is updated on the save location. Subsequent writes to the same data block on the source or target do not trigger a copy operation.

When reads are issued to the target, unchanged data blocks since the session activation are read from the source, whereas data blocks that have changed are read from the save location.

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. The target contains only pointers to the data, and therefore, 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 the expected data change.



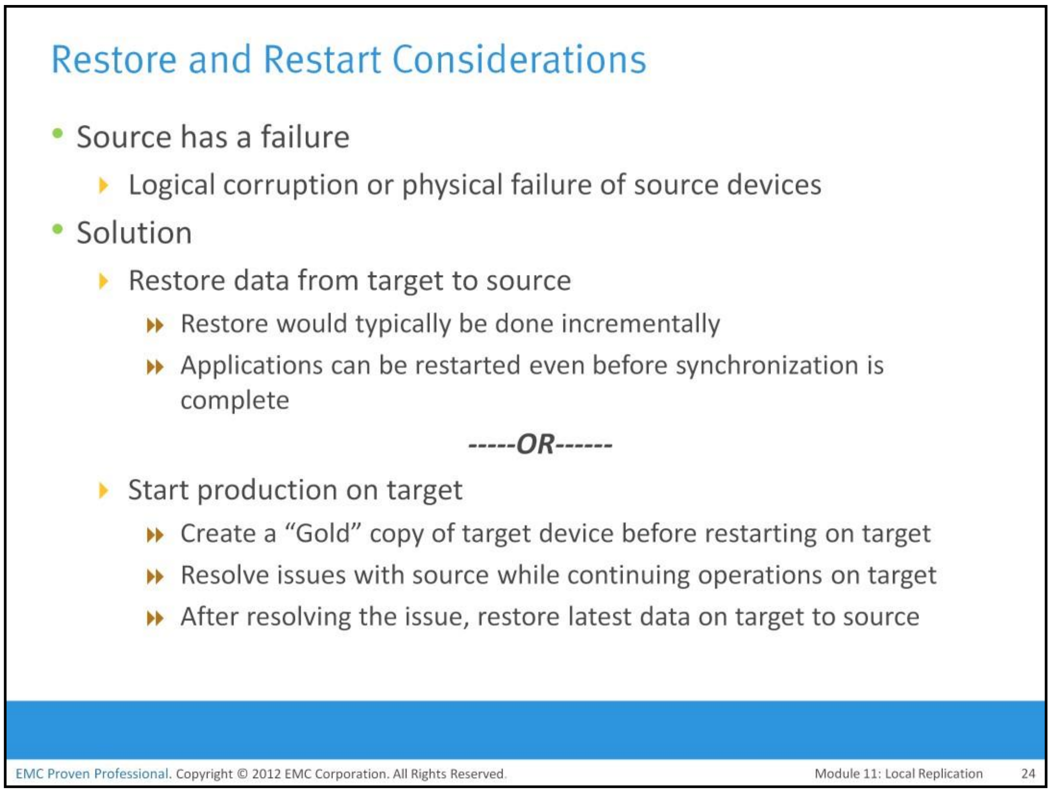
Tracking Changes to Source and Target

At PIT
Source 0 0 0 0 0 0 0 0 •••
Target 0 0 0 0 0 0 0 0 •••
After PIT…
Source 1 0 0 1 0 1 0 0 •••
Target 0 0 1 1 0 0 0 1 •••
For resynchronization/restore
Logical OR
1 0 1 1 0 1 0 1 •••
0 unchanged
1 changed

Module 11: Local Replication 23

Updates can occur on the source device after the creation of point-in-time local replicas. If the primary purpose of local replication is to have a viable point-in-time copy for data recovery or restore operations, then the replica devices should not be modified. Changes can occur on the replica device if it is used for other business operations. To enable incremental resynchronization or restore operations, changes to both the source and replica devices after the point-in-time should be tracked. This is typically done using bitmaps, where each bit represents a block of data. The data block sizes can range from 512 bytes to 64 KB or greater. For example, if the block size is 32 KB, then a 1 GB device would require 32,768 bits (1GB divided by 32KB). The size of the bitmap would be 4 KB. If the data in any 32 KB block is changed, the corresponding bit in the bitmap is flagged. If the block size is reduced for tracking purposes, then the bitmap size increases correspondingly.

The bits in the source and target bitmaps are all set to 0 (zero) when the replica is created. Any changes to the source or replica are then flagged by setting the appropriate bits to 1 in the bitmap. When resynchronization or restore is required, a *logical OR* operation between the source bitmap and the target bitmap is performed. The bitmap resulting from this operation references all blocks that have been modified in either the source or replica. This enables an optimized resynchronization or a restore operation, because it eliminates the need to copy all the blocks between the source and the replica. The direction of data movement depends on whether a resynchronization or a restore operation is performed. If resynchronization is required, changes to the replica are overwritten with the corresponding blocks from the source. If a restore is required, changes to the source are overwritten with the corresponding blocks from the replica. In either case, changes to both the source and the target cannot be simultaneously preserved.


Restore and Restart Considerations

- Source has a failure
  - Logical corruption or physical failure of source devices
- Solution
  - Restore data from target to source
    - Restore would typically be done incrementally
    - Applications can be restarted even before synchronization is complete

-----*OR*------

  - Start production on target
    - Create a "Gold" copy of target device before restarting on target
    - Resolve issues with source while continuing operations on target
    - After resolving the issue, restore latest data on target to source

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 24

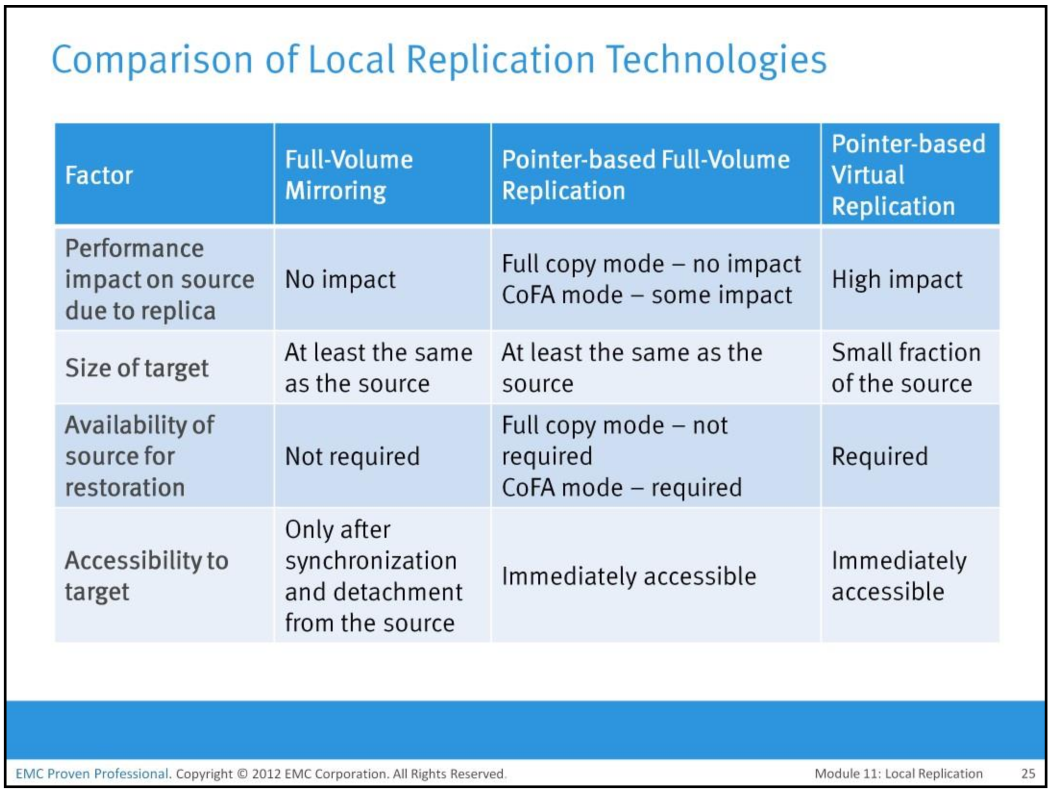
Local replicas are used to restore data to production devices. Alternatively, applications can be restarted using the consistent point-in-time replicas.

Replicas are used to restore data to the production devices if logical corruption of data on production devices occurs—that is, the devices are available but the data on them is invalid. Examples of logical corruption include accidental deletion of data (tables or entries in a database), incorrect data entry, and incorrect data updates. Restore operations from a replica are incremental and provide a small RTO. In some instances, the applications can be resumed on the production devices prior to the completion of the data copy. Prior to the restore operation, access to production and replica devices should be stopped.

Production devices might also become unavailable due to physical failures, such as production server or physical drive failure. In this case, applications can be restarted using the data on the latest replica. As a protection against further failures, a "Gold Copy" (another copy of replica device) of the replica device should be created to preserve a copy of data in the event of failure or corruption of the replica devices. After the issue has been resolved, the data from the replica devices can be restored back to the production devices.

Full-volume replicas (both full-volume mirrors and pointer-based in Full Copy mode) can be restored to the original source devices or to a new set of source devices. Restores to the original source devices can be incremental, but restores to a new set of devices are full-volume copy operations.

In pointer-based virtual and pointer-based full-volume replication in CoFA mode, access to data on the replica is dependent on the health and accessibility of the source volumes. If the source volume is inaccessible for any reason, these replicas cannot be used for a restore or a restart operation.



Comparison of Local Replication Technologies

Factor	Full-Volume Mirroring	Pointer-based Full-Volume Replication	Pointer-based Virtual Replication
Performance impact on source due to replica	No impact	Full copy mode – no impact CoFA mode – some impact	High impact
Size of target	At least the same as the source	At least the same as the source	Small fraction of the source
Availability of source for restoration	Not required	Full copy mode – not required CoFA mode – required	Required
Accessibility to target	Only after synchronization and detachment from the source	Immediately accessible	Immediately accessible

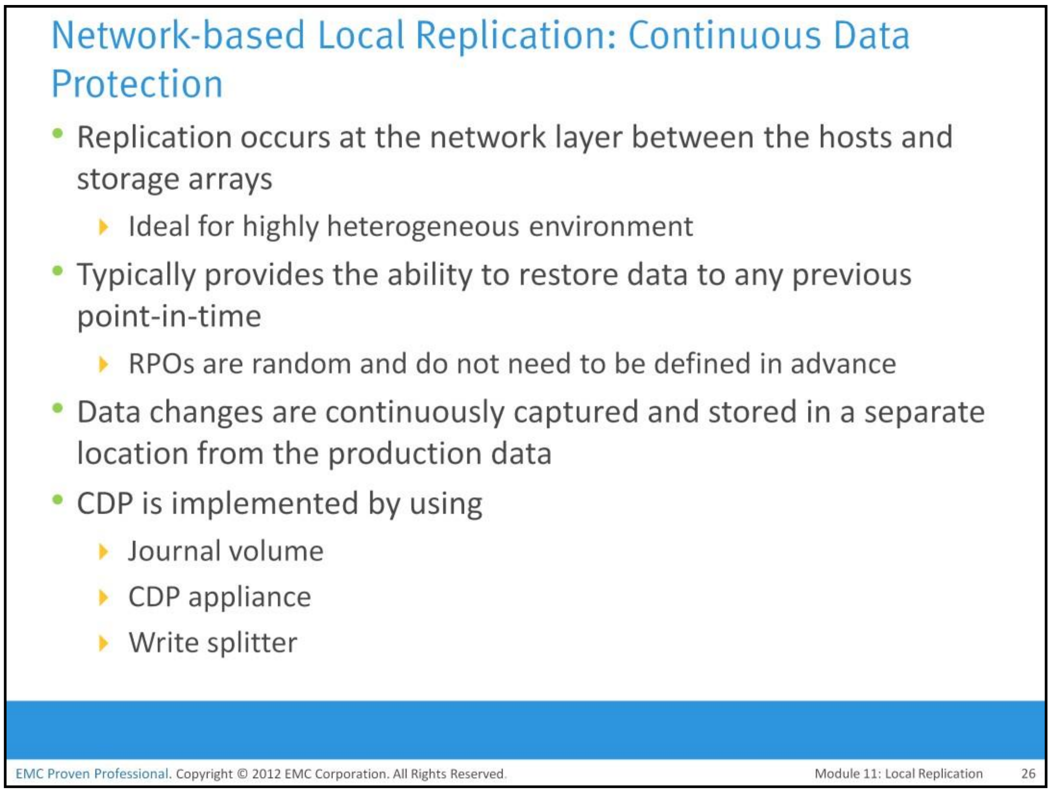
Module 11: Local Replication 25

This table summarizes the comparison between full-volume mirroring, pointer-based full-volume, and pointer-based virtual replication technologies.

Note:

Most array based replication technologies allow the source devices to maintain replication relationships with multiple targets.

- More frequentreplicas will reduce the RPO.
- Each PIT could be used for a different BC activity and also as restore points.


Network-based Local Replication: Continuous Data Protection

- Replication occurs at the network layer between the hosts and storage arrays
  - Ideal for highly heterogeneous environment
- Typically provides the ability to restore data to any previous point-in-time
  - RPOs are random and do not need to be defined in advance
- Data changes are continuously captured and stored in a separate location from the production data
- CDP is implemented by using
  - Journal volume
  - CDP appliance
  - Write splitter

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 26

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. CDP for remote replication is detailed in module 12.

In a data center environment, mission-critical applications often require instant and unlimited data recovery points. Traditional data protection technologies offer limited recovery points. If data loss occurs, the system can be rolled back only to the last available recovery point. Mirroring offers continuous replication; however, if logical corruption occurs to the production data, the error might propagate to the mirror, which makes the replica unusable. In normal operation, CDP provides the ability to restore data to any previous PIT. It enables this capability by tracking all the changes to the production devices and maintaining consistent point-in-time images.

In CDP, data changes are continuously captured and stored in a separate location from the primary storage. Moreover, RPOs are random and do not need to be defined in advance. With CDP, recovery from data corruption poses no problem because it allows going back to a PIT image prior to the data corruption incident. CDP uses a *journal volume* to store all data changes on the primary storage. The journal volume contains all the data that has changed from the time the replication session started. The amount of space that is configured for the journal determines how far back the recovery points can go. CDP also uses *CDP appliance* and *write splitter*. CDP implementation may also be host-based in which CDP software is installed on a separate host machine. CDP appliance is an intelligent hardware platform that runs the CDP software and manages local and remote data replications. Write splitters intercept writes to the production volume from the host and split each write into two copies. Write splitting can be performed at the host, fabric, or storage array.

CDP Local Replication Operation

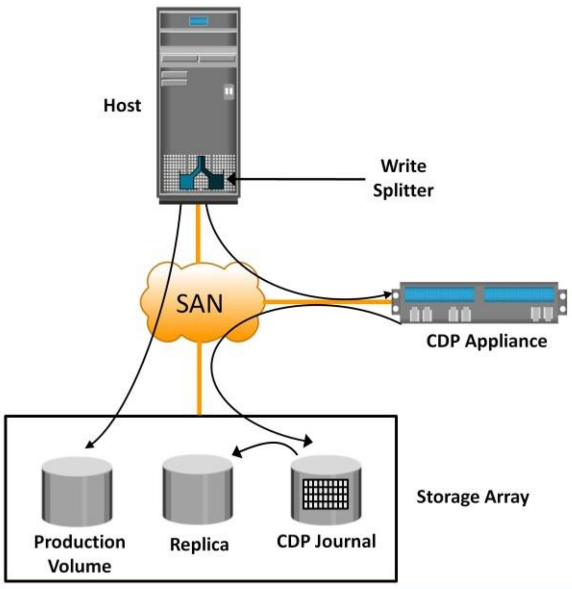
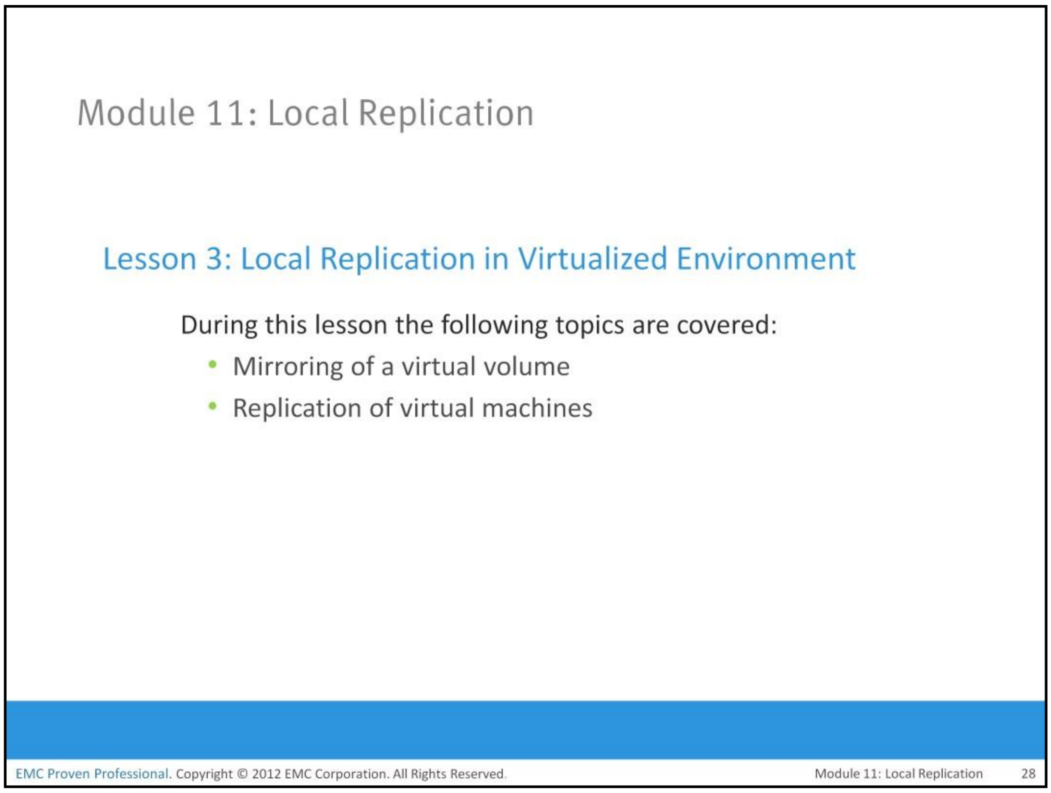


Figure on the slide describes CDP local replication. In this method, before the start of replication, the replica is synchronized with the source and then the replication process starts. After the replication starts, all the writes to the source are split into two copies. One of the copies is sent to the CDP appliance and the other to the production volume. When the CDP appliance receives a copy of a write, it is written to the journal volume along with its timestamp. As a next step, data from the journal volume is sent to the replica at predefined intervals.

While recovering data to the source, the CDP appliance restores the data from the replica and applies journal entries up to the point in time chosen for recovery.


Module 11: Local Replication

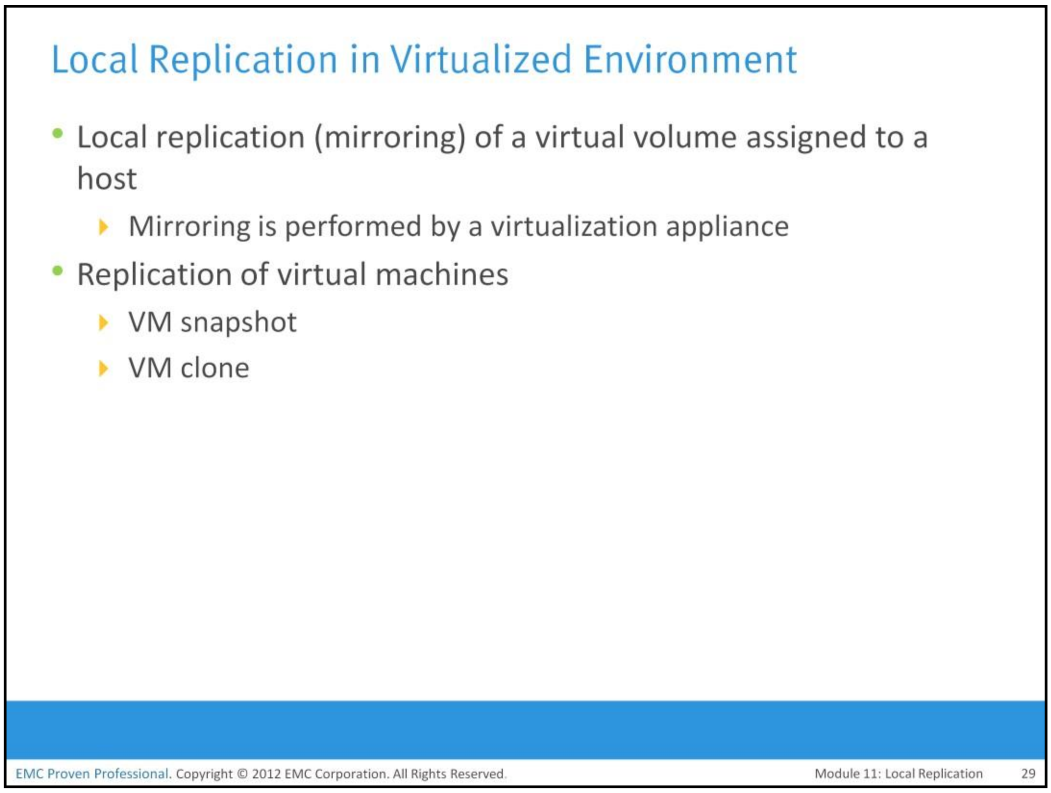
Lesson 3: Local Replication in Virtualized Environment

During this lesson the following topics are covered:

- Mirroring of a virtual volume
- Replication of virtual machines

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 28

This lesson covers mirroring of a virtual volume and also replication of virtual machines.

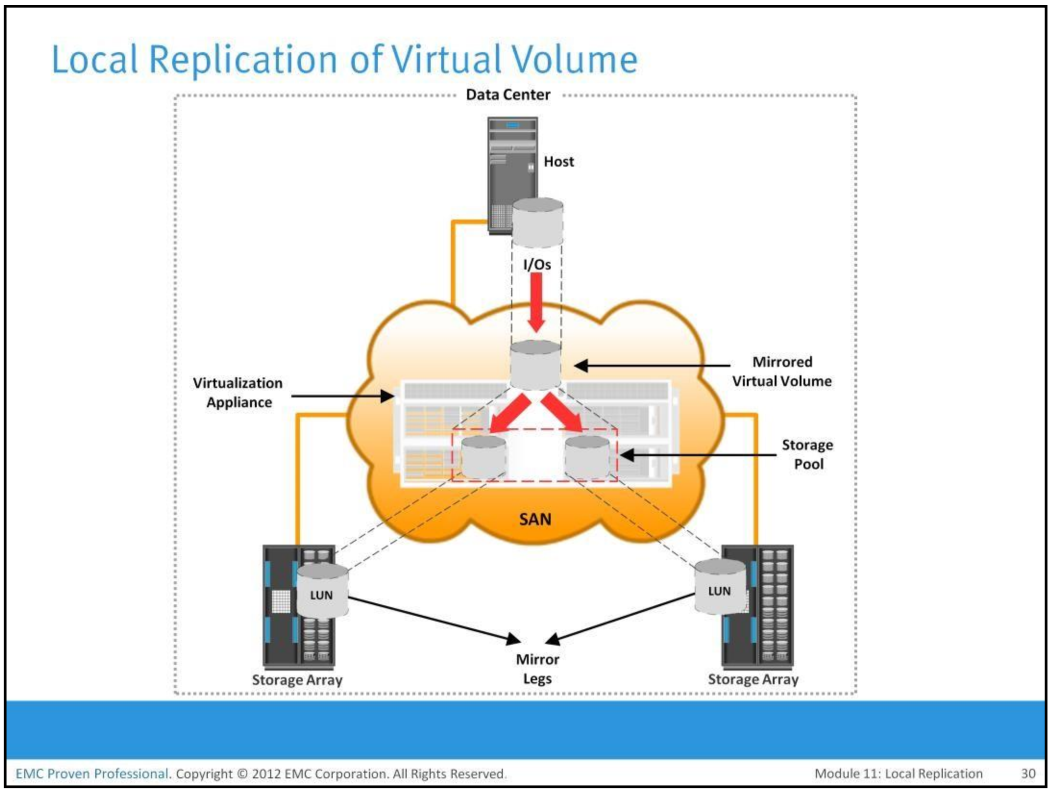


Local Replication in Virtualized Environment

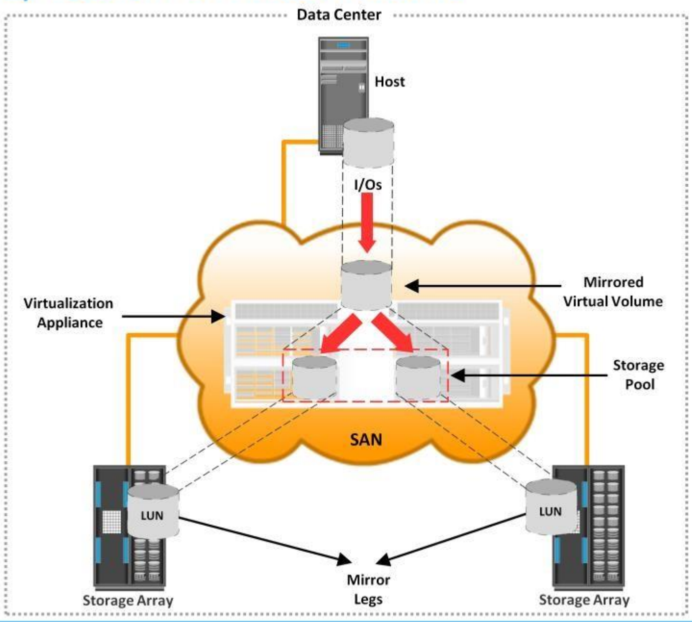
- Local replication (mirroring) of a virtual volume assigned to a host
  - Mirroring is performed by a virtualization appliance
- Replication of virtual machines
  - VM snapshot
  - VM clone

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 29

The discussion so far has focused on local replication in a physical infrastructure environment. In a virtualized environment, along with replicating storage volumes, replication of virtual machine (VM) is performed by the hypervisor. For hypervisor-based local replication, two options are available - VM Snapshot, and VM Clone. However, in a virtualized environment, the data in the virtual volumes can also be replicated with the help of a virtualization layer in a SAN.

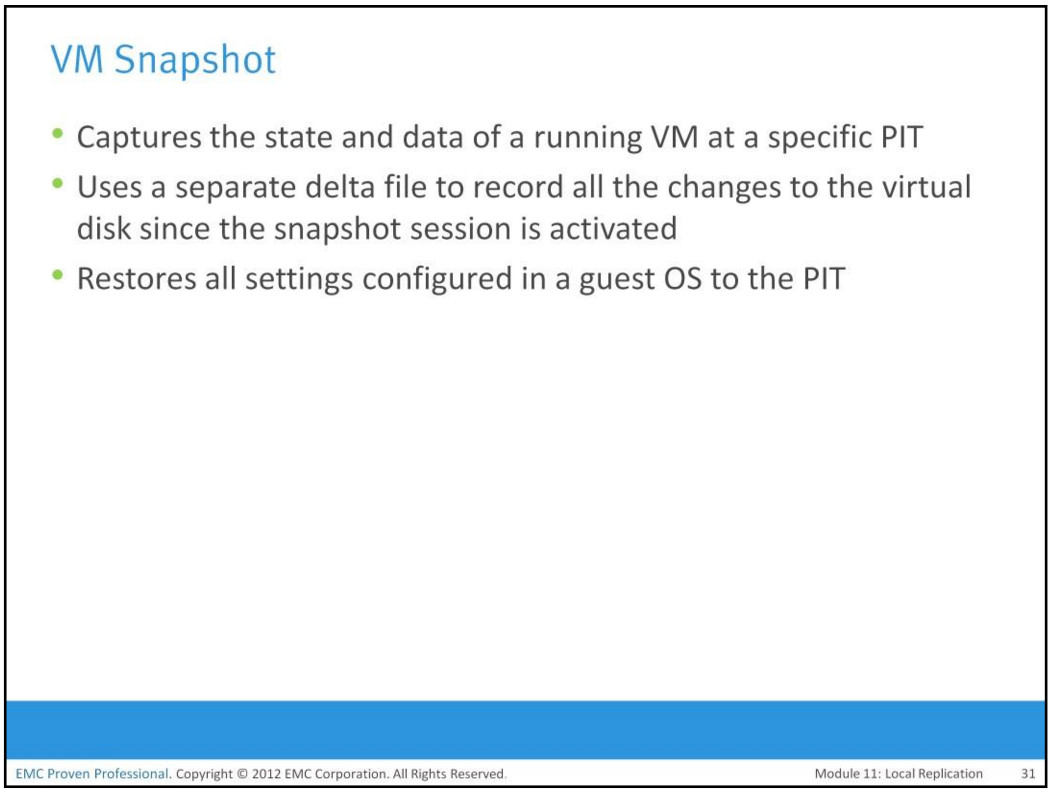


Local Replication of Virtual Volume



EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 30

In a virtualized environment, the virtualization appliance at the SAN abstracts the LUNs and creates virtual volumes. These virtual volumes are presented to the host. The virtualization appliance has the ability to mirror the data of a virtual volume between the LUNs. Figure on the slide provides an illustration of a virtual volume that is mirrored between arrays within a data center. Each I/O to the virtual volume is mirrored to the underlying LUNs on the arrays. If one of the arrays incurs an outage, the virtualization appliance will be able to continue processing I/O on the surviving mirror leg. Upon restoration of the failed storage array, the data from the surviving LUN is resynchronized to the recovered leg.

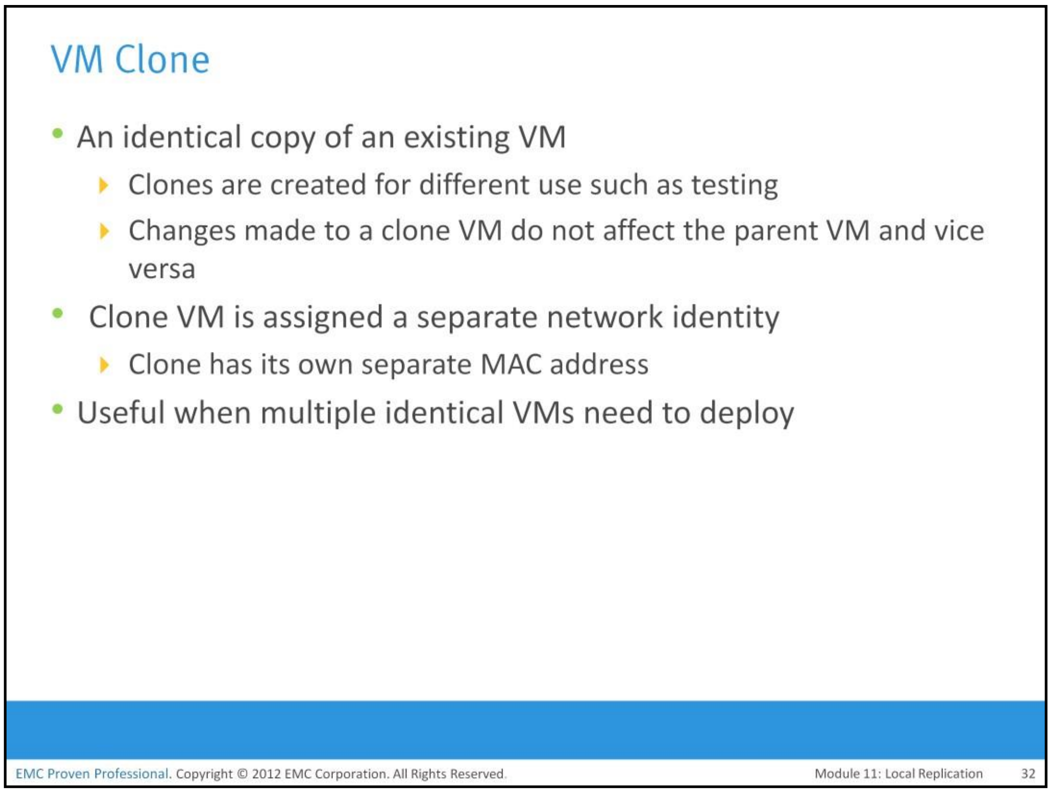


VM Snapshot

- Captures the state and data of a running VM at a specific PIT
- Uses a separate delta file to record all the changes to the virtual disk since the snapshot session is activated
- Restores all settings configured in a guest OS to the PIT

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 31

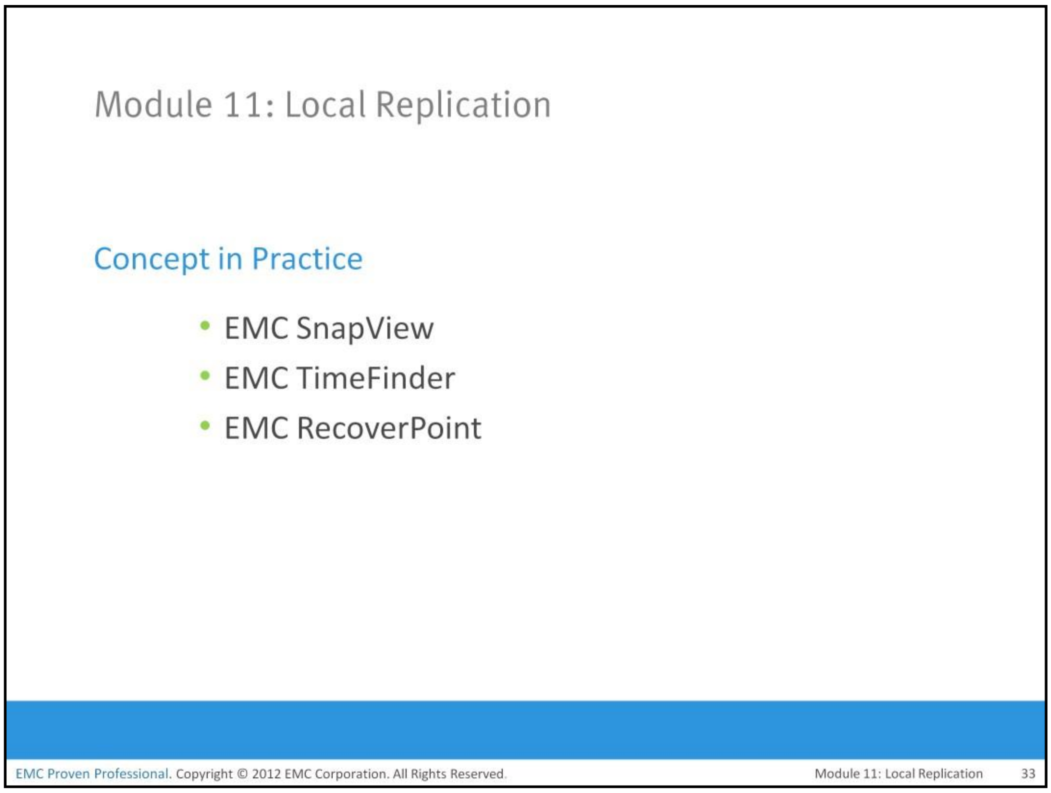
VM Snapshot captures the state and data of a running virtual machine at a specific point in time. The VM state includes VM files, such as BIOS, network configuration, and its power state (powered-on, powered-off, or suspended). The VM data includes all the files that make up the VM, including virtual 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. There are some challenges associated with the VM Snapshot technology. It does not support data replication if a virtual machine accesses the data by using raw disks. Also, using the hypervisor to perform snapshots increases the load on the compute and impacts the compute performance.



VM Clone

- An identical copy of an existing VM
  - Clones are created for different use such as testing
  - Changes made to a clone VM do not affect the parent VM and vice versa
- Clone VM is assigned a separate network identity
  - Clone has its own separate MAC address
- Useful when multiple identical VMs need to deploy

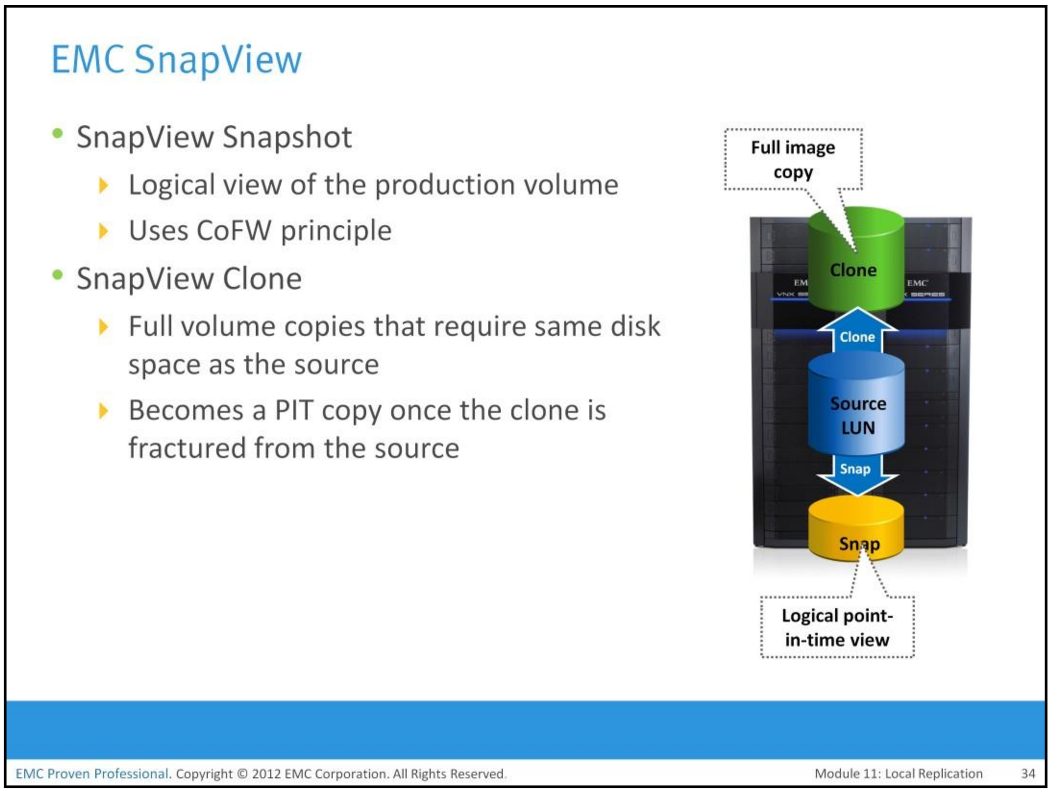
VM Clone is another method that creates an identical copy of a virtual machine. When the cloning operation is complete, the clone becomes a separate VM from its parent VM. The clone has its own MAC address, and changes made to a clone do not affect the parent VM. Similarly, changes made to the parent VM do not appear in the clone. 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.


Module 11: Local Replication

Concept in Practice

- EMC SnapView
- EMC TimeFinder
- EMC RecoverPoint

The concepts in practice section covers various EMC local replication products such as EMC SnapView, EMC TimeFinder, and EMC RecoverPoint.



EMC SnapView

- SnapView Snapshot
  - Logical view of the production volume
  - Uses CoFW principle
- SnapView Clone
  - Full volume copies that require same disk space as the source
  - Becomes a PIT copy once the clone is fractured from the source

Full image copy
Clone
Clone
Source LUN
Snap
Snap
Logical point-in-time view

Module 11: Local Replication 34

SnapView is an EMC VNX array-based local replication software that creates pointer-based virtual copy and full-volume mirror of the source using SnapView snapshot and SnapView clone respectively.

SnapView Snapshot

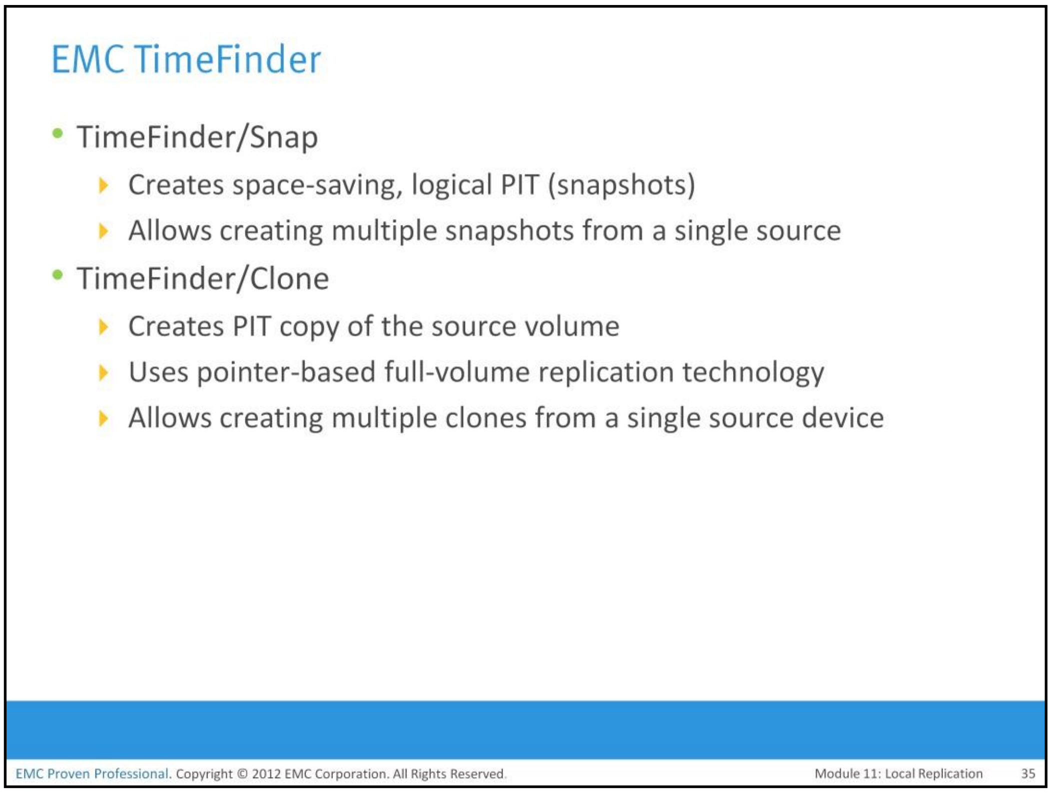
A SnapView snapshot is not a full copy of the production volume; it is a logical view of the production volume based on the time at which the snapshot was created. Snapshots are created in seconds, and can be retired when no longer needed. A snapshot “roll back” feature provides instant restore to the source volume. The key terminologies of SnapView snapshot are as follows:

SnapView session: The SnapView snapshot mechanism is activated when a session starts and deactivated when a session stops. A snapshot appears “offline” until there is an active session. Multiple snapshots can be included in a session.

Reserved LUN pool: This is a private area, also called a save area, used to contain CoFW data. The “Reserved” part of the name refers to the fact that the LUNs are reserved and therefore cannot be assigned to a host.

SnapView Clone

SnapView Clones are full-volume copies that require the same disk space as the source. These PIT copies can be used for other business operations, such as backup and testing. SnapView Clone enables incremental resynchronization between the source and replica. Clone fracture is the process of breaking off a clone from its source. After the clone is fractured, it becomes a PIT copy and available for other business operations.


EMC TimeFinder

- TimeFinder/Snap
  - Creates space-saving, logical PIT (snapshots)
  - Allows creating multiple snapshots from a single source
- TimeFinder/Clone
  - Creates PIT copy of the source volume
  - Uses pointer-based full-volume replication technology
  - Allows creating multiple clones from a single source device

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 35

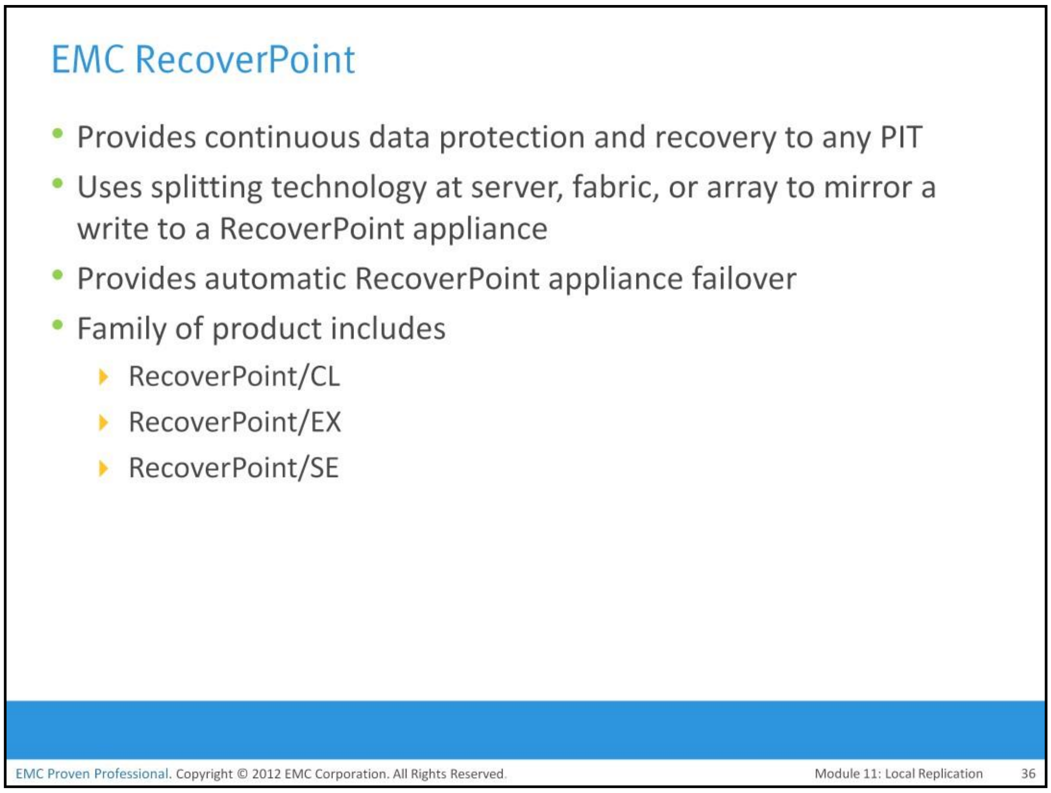
The TimeFinder family of products consists of two base solutions and four add-on solutions. The base solutions are TimeFinder/Clone and TimeFinder/Snap. The add-on solutions are TimeFinder/Clone Emulation, TimeFinder/Consistency Groups, TimeFinder/Exchange Integration Module, and TimeFinder/SQL Integration Module. TimeFinder is available for both open systems and mainframes. The base solutions support the different storage array-based local replication technologies discussed in this module. The add-on solutions are customizations of the replicas for specific application or database environments.

TimeFinder/Snap

TimeFinder/Snap creates space-saving, logical PIT images called snapshots. The snapshots are not full copies, but contain pointers to the source data. The target device used by TimeFinder/Snap is called a virtual device (VDEV). It keeps pointers to the source device or SAVE devices. The SAVE devices keep the point-in-time data that has changed on the source after the start of the replication session. TimeFinder/Snap allows creating multiple snapshots from a single source device.

TimeFinder/Clone

TimeFinder/Clone creates a PIT copy of the source volume that can be used for backups, decision support, or any other process that requires parallel access to production data. TimeFinder/Clone uses pointer-based full- volume replication technology. TimeFinder/Clone allows creating multiple clones from a single production device, and all the clones are available immediately for read and write access.



EMC RecoverPoint

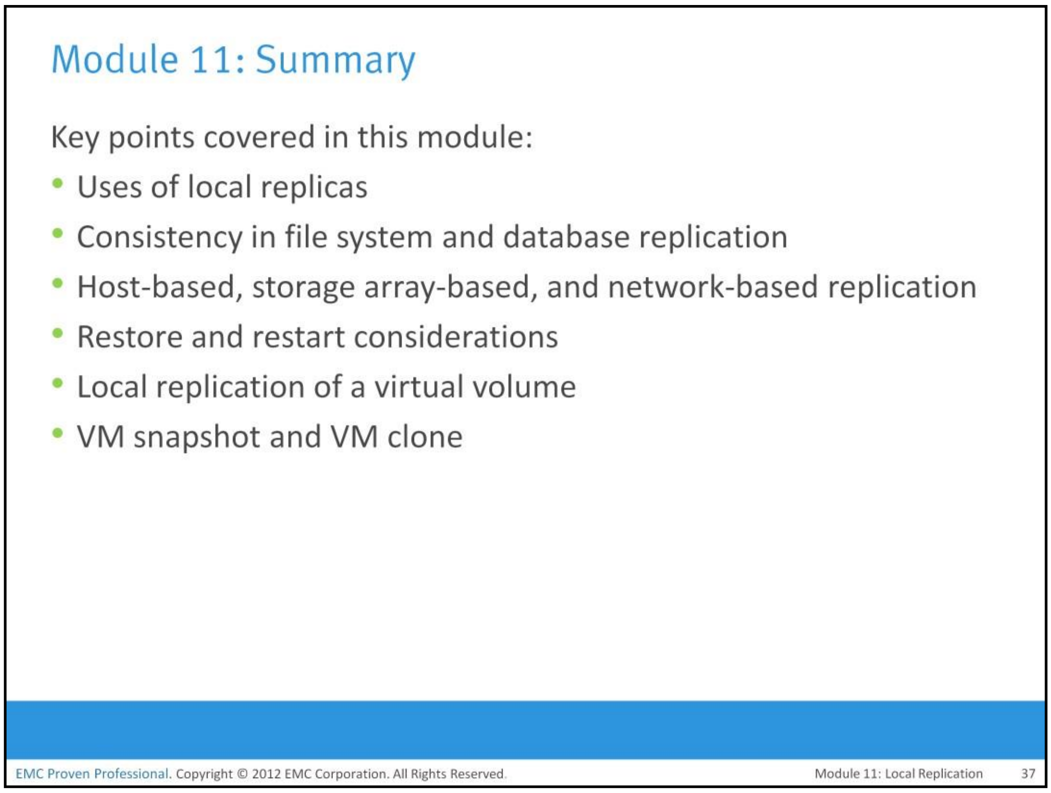
- Provides continuous data protection and recovery to any PIT
- Uses splitting technology at server, fabric, or array to mirror a write to a RecoverPoint appliance
- Provides automatic RecoverPoint appliance failover
- Family of product includes
  - RecoverPoint/CL
  - RecoverPoint/EX
  - RecoverPoint/SE

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 36

RecoverPoint is a high-performance, cost-effective, single product that provides local and remote data protection for both physical and virtual environments. It provides faster recovery and unlimited recovery points. RecoverPoint provides continuous data protection and performs replication between the LUNs. RecoverPoint uses lightweight splitting technology either at the application server, fabric, or arrays to mirror a write to a RecoverPoint appliance. The RecoverPoint family of products include RecoverPoint/CL, RecoverPoint/EX, and RecoverPoint/SE.

RecoverPoint/CL is a replication product for a heterogeneous server and storage environment. It supports both EMC and non-EMC storage arrays. This product supports host-based, fabric-based, and array-based write splitters. *RecoverPoint/EX* supports replication between EMC storage arrays and allows only array-based write splitting.

RecoverPoint/SE is a version of RecoverPoint that is targeted for VNX series arrays and enables only Windows-based host and array-based write splitting.



Module 11: Summary

Key points covered in this module:

- Uses of local replicas
- Consistency in file system and database replication
- Host-based, storage array-based, and network-based replication
- Restore and restart considerations
- Local replication of a virtual volume
- VM snapshot and VM clone

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 37

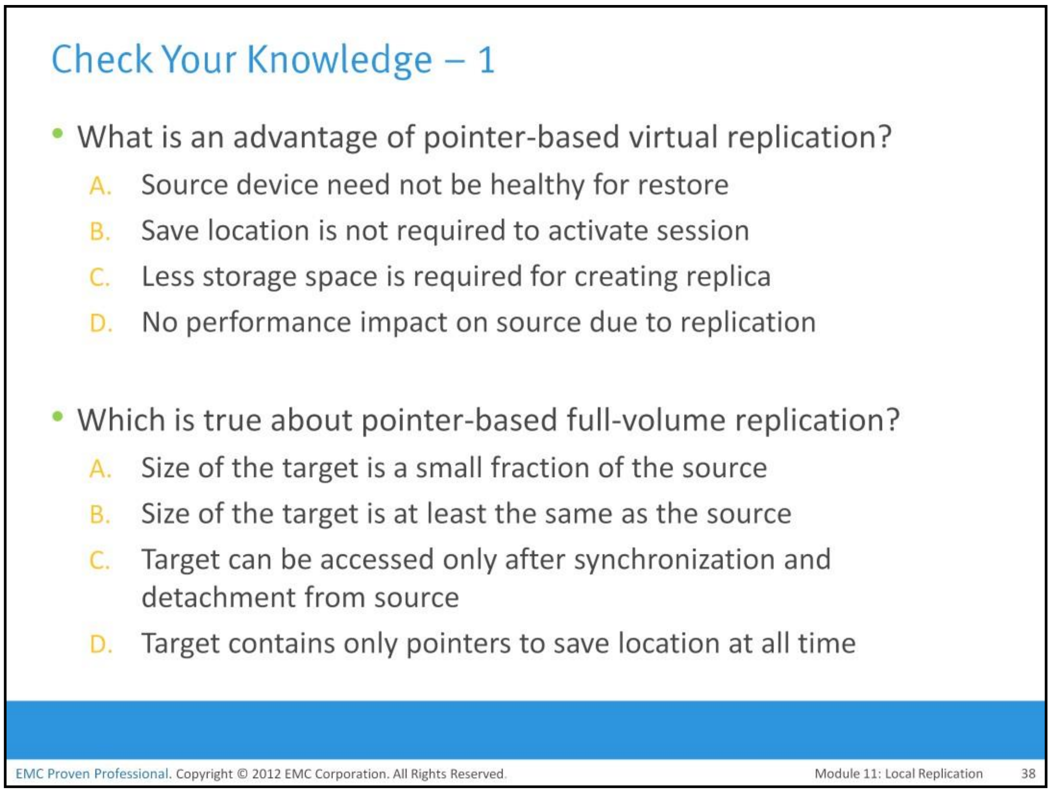
This module covered various uses of local replica along with file system and database consistency in replication. This module also covered various host-based, storage-based, and network-based local replication technologies. Further, this module focused restore and restart considerations for local replica. Finally, this module detailed local replication in virtualized environment.

Local replicas are used for several purposes such as alternate source for backup, fast recovery, decision support, testing platform, and data migration.

Replica must be consistent with the source so that it is usable for both recovery and restart operations. Ensuring consistency is the primary requirement for all the replication technologies.

Host-based, storage array-based, and network-based replications are the major technologies used for local replication. File system replication and LVM-based replication are examples of host-based local replication. Storage array-based replication can be implemented with distinct solutions, namely, full-volume mirroring, pointer-based full-volume replication, and pointer-based virtual replication. Continuous Data Protection (CDP) is an example of network-based replication.

In a virtualized environment, virtual machine (VM) replication is a critical requirement for successful BC process. Typically, local replication of VMs (VM snapshot and VM clone) 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.

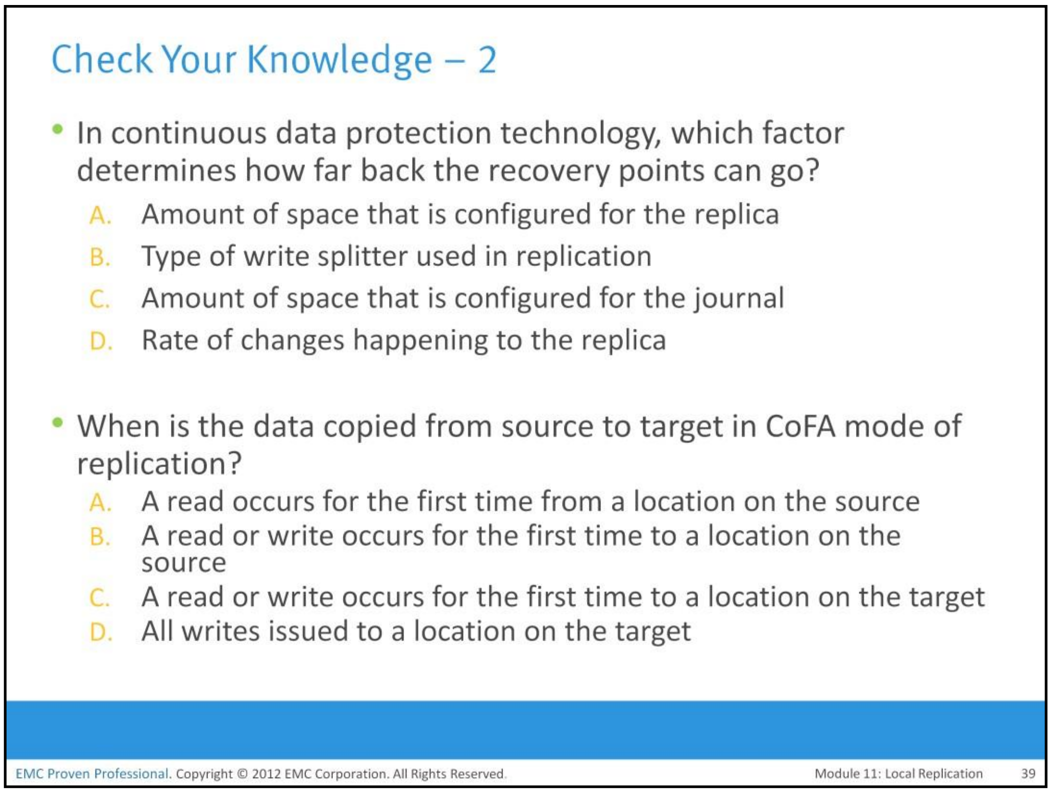


Check Your Knowledge – 1

- What is an advantage of pointer-based virtual replication?
  A. Source device need not be healthy for restore
  B. Save location is not required to activate session
  C. Less storage space is required for creating replica
  D. No performance impact on source due to replication

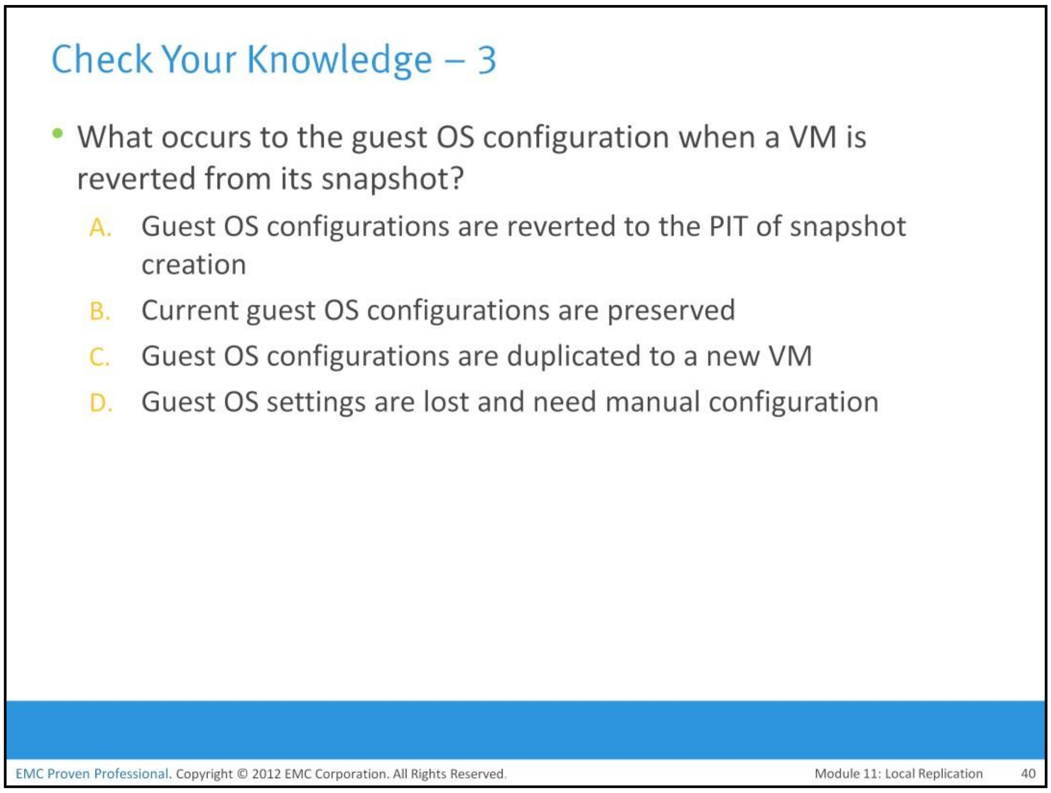
- Which is true about pointer-based full-volume replication?
  A. Size of the target is a small fraction of the source
  B. Size of the target is at least the same as the source
  C. Target can be accessed only after synchronization and detachment from source
  D. Target contains only pointers to save location at all time

Module 11: Local Replication 38


Check Your Knowledge – 2

- In continuous data protection technology, which factor determines how far back the recovery points can go?
  - A. Amount of space that is configured for the replica
  - B. Type of write splitter used in replication
  - C. Amount of space that is configured for the journal
  - D. Rate of changes happening to the replica

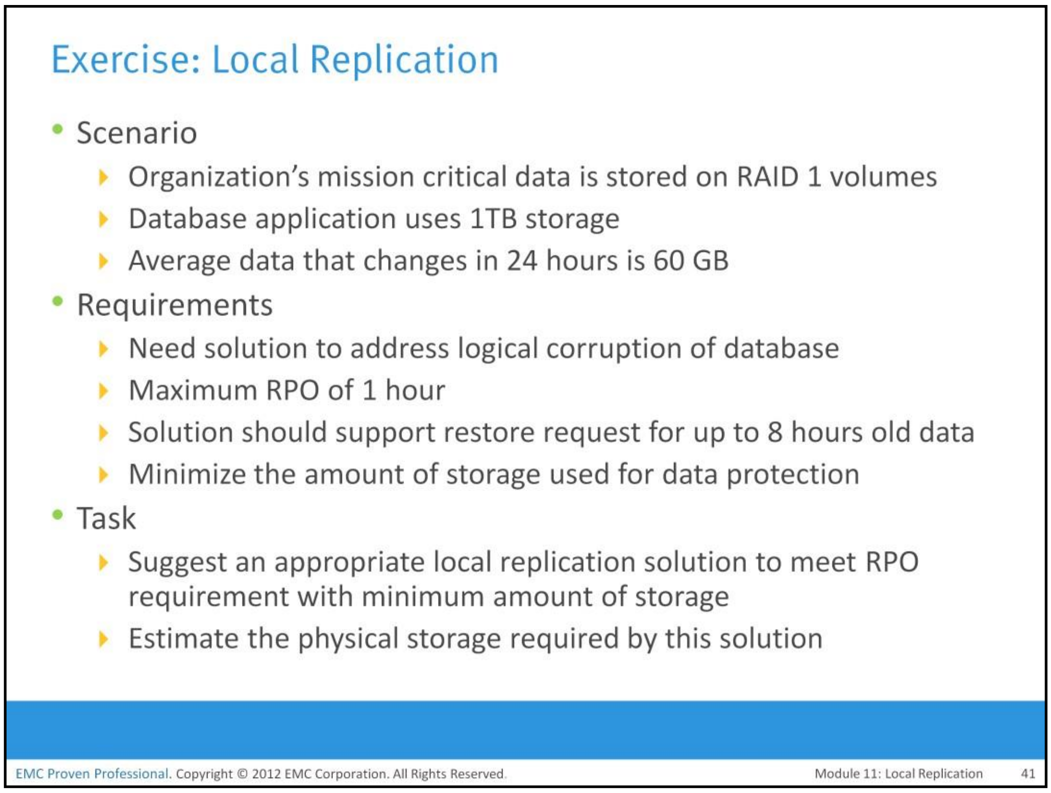
- When is the data copied from source to target in CoFA mode of replication?
  - A. A read occurs for the first time from a location on the source
  - B. A read or write occurs for the first time to a location on the source
  - C. A read or write occurs for the first time to a location on the target
  - D. All writes issued to a location on the target



Check Your Knowledge – 3

- What occurs to the guest OS configuration when a VM is reverted from its snapshot?
  A. Guest OS configurations are reverted to the PIT of snapshot creation
  B. Current guest OS configurations are preserved
  C. Guest OS configurations are duplicated to a new VM
  D. Guest OS settings are lost and need manual configuration

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 40


Exercise: Local Replication

- Scenario
  - Organization's mission critical data is stored on RAID 1 volumes
  - Database application uses 1TB storage
  - Average data that changes in 24 hours is 60 GB
- Requirements
  - Need solution to address logical corruption of database
  - Maximum RPO of 1 hour
  - Solution should support restore request for up to 8 hours old data
  - Minimize the amount of storage used for data protection
- Task
  - Suggest an appropriate local replication solution to meet RPO requirement with minimum amount of storage
  - Estimate the physical storage required by this solution

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 11: Local Replication 41

Scenario:

A manufacturing organization stores data of their mission critical applications on a high end storage array with RAID 1 configuration. The database application has 1 TB of storage and needs 24x7availability. Average data that changes in 24 hours is 60 GB.

Requirements:

Need solution to address logical corruption of database

Maximum RPO of 1 hour

Solution should support restore request for up to 8 hours old data

Minimize the amount of storage used for data protection

Task:

Suggest an appropriate local replication solution to meet RPO requirement with minimum amount of storage. Estimate the physical storage required by this solution.