Using Live Sync to Support Disaster Recovery for VMware Virtual Machines
Version 11 Service Pack 6
Tuesday, December 13, 2016
## Contents

- Introduction .......................................................................................................................... 5
  - Audience ............................................................................................................................... 5
  - Architecture .......................................................................................................................... 6

- Using Live Sync to Support Disaster Recovery ..................................................................... 6
  - Basic Live Sync Flow ........................................................................................................... 6
  - Live Sync Flow with DASH Copy ......................................................................................... 7

- Planning and Requirements .................................................................................................. 7
  - Live Sync Requirements ....................................................................................................... 8
  - Scalability and Performance ................................................................................................. 8
  - Incremental Forever .............................................................................................................. 8
  - Selective Copy ...................................................................................................................... 9
  - SAN or HotAdd Deployments ............................................................................................... 9

- Alternative Deployments ....................................................................................................... 9
  - Local Recovery Site .............................................................................................................. 9
  - Backup Copies ..................................................................................................................... 10
  - Remote Disaster Recovery Site ........................................................................................... 11
  - Multiple Disaster Recovery Sites ....................................................................................... 12

- Live Sync Configuration ....................................................................................................... 12
  - Live Sync Schedules ........................................................................................................... 13
  - Storage Policy Copies .......................................................................................................... 15

- Validation ............................................................................................................................... 15

- Monitoring ............................................................................................................................... 16

- Comparison of Different Technologies and Solutions ............................................................ 17
  - Hardware Replication ......................................................................................................... 17
  - Software-Based Virtual Machine Replication .................................................................... 18
  - Backup-Based Recovery with Scheduled Full VM Restores .......................................... 18
  - Specialized Disaster Recovery Software ......................................................................... 19
  - Application-Level Replication ............................................................................................ 19
Recovery Scenarios and Orchestration ................................................................. 20
  Test Boot Virtual Machines ........................................................................ 20
  Planned Failover ....................................................................................... 20
  Unplanned Failover .................................................................................. 20
  Fail Back ................................................................................................. 20

Conclusion .................................................................................................... 21

Glossary of Terms ...................................................................................... 23

Index ........................................................................................................... 25
Introduction

The Live Sync feature enables you to use backup data to create and maintain a warm disaster recovery site for virtual machines (VMs) running critical business applications. Live Sync provides software-based replication for source VMs. By using backup data and performing replication using backup infrastructure, you can minimize the impact on production systems.

Live Sync uses a full or synthetic full backup to create each destination VM and updates destination VMs from subsequent incremental backups of the source VMs. You can configure Live Sync schedules to create multiple Live Sync jobs for each schedule, with each job using its own stream for a subset of virtual machines; this approach dramatically reduces the amount of time required to replicate large numbers of virtual machines.

The recovery time objective (RTO), the time interval between a service interruption and the restoration of services from the recovery site, is the time needed to power on the virtual machines at the recovery site. Automated validation and the ability to specify new network connections and IP addresses at the recovery site ensure that startup time is minimized.

Because Live Sync is based on backups the recovery point objective (RPO), the acceptable time interval within which virtual machine data must be recoverable, is determined by the frequency of backups.

In the event of corrupted data in source VMs, you can recover source VMs from any stable recovery point that is available in backup history, and then use Live Sync to resync VMs from the recovered source VM.

In the event of a disaster, you can power on the destination virtual machines for minimal disruption of vital business applications.

Live Sync provides quick recovery capability for critical applications running on virtual machines. And as always, Commvault data protection enables recovery of less critical virtual machines from backups as needed.

Audience

This white paper is intended for system engineers, disaster recovery planners, and data protection and recovery administrators. You should be familiar with backup technology, the VMware virtualization platform, and disaster recovery concepts.
Architecture

A disaster recovery site includes standby servers with the following components:

- VMware vCenter
- Commvault® CommServe® software
- Virtual Server Agent
- MediaAgent
- Storage

Using Live Sync to Support Disaster Recovery

For quick recovery, a disaster recovery site can be maintained locally using basic Live Sync flow.

For recovery in scenarios where the primary location is unavailable, a disaster recovery site can be maintained in a different location using a Live Sync flow with DASH copy.

With either approach, Live Sync can run immediately after backups or on a scheduled basis (daily, weekly, monthly, or yearly).

Live Sync uses "bucketing" of operations within a single backup schedule to spawn multiple jobs and process Live Sync operations efficiently. Bucketing is enabled by default.

Basic Live Sync Flow

The basic Live Sync configuration duplicates virtual machine data from backups to the disaster recovery site on an ongoing basis. Live Sync also replicates virtual machine changes that are captured during backup operations and overlays those changes on destination virtual machines.
Live Sync Flow with DASH Copy

When used with deduplication, ongoing changes for each incremental backup can be transmitted to a secondary copy of backup data at a remote disaster recovery site, with only changed blocks transmitted to the remote site (DASH copy). The DASH copy approach reduces traffic over the wide area network (WAN) and enables faster replication to the DR site.

Live Sync can be configured to run immediately once changes have been DASH copied to the remote site.

Planning and Requirements

The first and most critical part of planning a disaster recovery site is identifying VMs running the most critical business applications.

In designing the best solution for your environment, consider the following factors:

- The speed with which you can perform backups of virtual machines on production servers.
- The impact of backup and replication processes on production systems and backup infrastructure.
- Network transfer speeds between the production site and the disaster recovery site.

If wide area network (WAN) traffic between the primary site and the disaster recovery site is a concern, you can use an auxiliary copy on the disaster recovery site for Live Sync operations.

Provide a VMware vCenter at the disaster recovery site to host the virtual machines for the disaster recovery site.
Live Sync Requirements

- Commvault® version 11 or version 10, Service Pack 12 or later must be installed.
- Live Sync is supported for virtual machines using hardware version 7 or higher.
- Live Sync can be used to replicate virtual machines from a streaming backup, auxiliary copy, or backup copy. You cannot replicate virtual machines directly from IntelliSnap® backups.
- To add virtual machines to the Live Sync schedule, the virtual machines must have been backed up at least once.
- Live Sync configuration can specify network connections and IP addresses to be used for VMs in the disaster recovery site.

Scalability and Performance

For large disaster sites, use the following guidelines:

- Ensure that critical VMs are backed up and synched first.
- For remote disaster recovery sites, use auxiliary copy with deduplication (DASH Copy).
- Use SAN or HotAdd mode to minimize the time for data movement at the remote site.
- Organize VMs into different subclients and define separate backup schedules to stagger backups and Live Sync operations across the operating schedule.
- Use incremental backups to update destination VMs on an ongoing basis while minimizing data transport times.

Incremental Forever

The best method for scheduling backups of source VMs is to use the "Incremental Forever" approach:

- Perform an initial full or synthetic full backup to create destination VMs using Live Sync.
- After the destination VM is created, run regular incremental backups to keep the destination VM current.
- Run a synthetic full backup on a periodic basis to consolidate incremental backups into full VM backups without the need to touch production VMs. Synthetic full backups trigger a Live Sync operation but only apply changes from any incremental backups that have not yet been replicated.

Note: Do not schedule full backups; a full backup results in syncing the destination VM completely.
Selective Copy

When setting up a remote site, you can use the selective copy feature to ensure that only the latest full or synthetic full backup and subsequent incremental backups are copied to the remote site for use with Live Sync. When using selective copy, you must configure the Live Sync schedule so that the Live Sync operation is triggered by the completion of the selective copy operation rather than the primary backup operation.

SAN or HotAdd Deployments

To further enhance the speed of transfers, you can deploy the Virtual Server Agent and MediaAgent at the remote site on a physical machine (SAN mode) or on a virtual machine (HotAdd mode). You can also deploy one or more VSAs in HotAdd mode with a MediaAgent on a physical machine.

Alternative Deployments

You can deploy Live Sync in different ways depending on your requirements, to maintain a local recovery site or multiple remote sites.

Local Recovery Site

The simplest Live Sync deployment uses streaming backups for critical VMs. Live Sync runs against backups and replicates virtual machines on another server at the same site for quick recovery.
For a local recovery site, the source and destination virtual machines (VMs) are hosted on ESX servers in the same geographic location.

The ESX servers can be standalone servers or part of the same VMware vCenter, or the ESX servers at each end can be part of different vCenters.

A Virtual Server Agent (VSA) proxy and a MediaAgent are installed on a physical or virtual machine between the source and destination servers. The VSA proxy manages backups of VMs and the MediaAgent controls data movement to storage.

The Live Sync operation runs against backups to create and update destination VMs. A full or synthetic full backup is used to create the destination VM. Subsequent incremental backups are used to update the destination VMs with changes from the source VMs. This approach is called "Incremental Forever."

The ESX server that hosts the source VMs is touched only once, for the initial backup.

Backup Copies

Live Sync can also be used in deployments using IntelliSnap® backup copies. IntelliSnap leverages hardware snapshots on storage arrays to capture software snapshots that are used to create streaming backup copies. Backup copies can be used directly by Live Sync, or they can be used to create auxiliary copies for use with Live Sync.

At the source, we can reduce backup time by taking a hardware snapshot of the source VMs.

The snapshot is then mounted on an ESX server (different from the ESX server that hosts the source VMs). A backup copy operation runs against the snapshot to create a streaming backup copy, and the Live Sync operation runs against the backup copy.

The movement of data to the destination is the same as in other scenarios.
Remote Disaster Recovery Site

For larger implementations using a remote disaster recovery site, the optimal solution uses auxiliary copies at the remote site, DASH copy transfers of incremental backup data, and deduplication.

As with a simple deployment, we use an Incremental Forever approach.

You can use the auxiliary copy feature to duplicate streaming backup data to the remote site. The auxiliary copy operation runs on backup infrastructure without any impact on production systems. Live Sync uses the auxiliary copy at the remote site to create and maintain destination VMs.

Deduplication between the local and remote site reduces the amount of network traffic by only transmitting new or changed data blocks to the remote site (DASH copy).

The primary site can use streaming backups or IntelliSnap backup copies.

The destination is a remote Disaster Recovery (DR) site. For example, the primary site could be New York City and the remote site could be Philadelphia. A cloud or wide area network (WAN) is between the primary and DR sites.

Backups are performed at the primary site.

Backup data is transferred to the remote site using an auxiliary copy operation.

A VSA proxy and MediaAgent are deployed at both the primary site and the DR site.

To reduce traffic over the WAN, deduplication is used to identify changed blocks and only transmit the changed blocks. Compression is used to further reduce the size of data packets that are transmitted between the primary and DR sites.

The VSA and MediaAgent at the primary site manage writing backups to storage. The MediaAgents at both ends manage the data transfer to storage at the remote site. The VSA proxy and MediaAgent at the DR site are used to perform the Live Sync operation from the backups that reside on storage at the remote site.
Multiple Disaster Recovery Sites

You can leverage virtual machine backups from a primary site to maintain multiple DR sites. In this scenario, we have one primary site but multiple DR sites (for example, New York to Philadelphia and Los Angeles).

The primary site and each of the remote DR sites has a VSA proxy and MediaAgent.

Data movement from the primary site to each of the DR sites is the same as for a single remote DR site.

Live Sync Configuration

You can create a replication schedule and specify disaster recovery options using basic configuration.
Live Sync Schedules

Configure a Live Sync schedule by adding specific VMs that have previously been backed up.

Determine whether Live Sync operations should run immediately after backups or on a scheduled basis.

Specify exactly where you want to place destination VMs.
Automate destination VM naming conventions, resource pools, network connections, and other options for groups of destination VMs.

Customize the behavior of each Live Sync schedule, including whether to validate the destination VM after each Live Sync to verify that the VM can be powered on successfully.
Storage Policy Copies

To use an auxiliary copy as the source for Live Sync, define a selective storage policy copy, define auxiliary copy job options, and specify the copy to be used for Live Sync.

Validation

You can choose to automatically validate destination VMs after each Live Sync operation by automatically powering the VMs on and off to ensure that they are bootable and ready for use. (Changes resulting from the power on are not preserved.) Any VMs that cannot be validated are queued for resync during the next cycle.

If validation fails, the destination virtual machine reverts to its last valid (bootable) state.
Monitoring

Monitor the status of all the VMs in Live Sync schedules.

View the progress of Live Sync jobs while they are running or as part of job history.

View details about each VM.
Comparison of Different Technologies and Solutions

Different VM replication solutions and products use different technologies and approaches. In each case, the goal is to enable quick and easy recovery of key business applications, but the technology choices can make significant differences in effectiveness and performance, and support different recovery point objectives (RPOs).

Live Sync leverages the best features of different technologies to provide VM replication that is fast, efficient, and reliable.

Hardware Replication

<table>
<thead>
<tr>
<th><strong>Advantages</strong></th>
<th><strong>Disadvantages</strong></th>
<th><strong>Live Sync Comparison</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides fast data replication using storage array hardware snapshot.</td>
<td>Requires identical hardware at DR site.</td>
<td>Can leverage hardware snapshot as source for backup copy.</td>
</tr>
<tr>
<td>Has minimal impact on production systems.</td>
<td>Can be expensive.</td>
<td>Can use backup copy as source for replication.</td>
</tr>
<tr>
<td>Is easy to configure.</td>
<td>Recovery of virtual machines is longer and more complex.</td>
<td>Enables VM-level replication as well as point-in-time VM recovery and file recovery.</td>
</tr>
<tr>
<td>Is available to any host that can access storage array.</td>
<td>File recovery is difficult (might not be supported).</td>
<td>Has minimal impact on production systems.</td>
</tr>
<tr>
<td>Does not require application awareness.</td>
<td>Has large storage requirements.</td>
<td>Provides efficient transfers across wide area network.</td>
</tr>
<tr>
<td>Minimizes data loss.</td>
<td>Requires ongoing monitoring of dedicated storage space.</td>
<td>Works with different storage arrays.</td>
</tr>
</tbody>
</table>
## Software-Based Virtual Machine Replication

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Live Sync Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides direct replication of VM to DR site.</td>
<td>Can replicate bad data from source VM to destination VM.</td>
<td>Includes VM replication from streaming backup, backup copy, or auxiliary copy.</td>
</tr>
<tr>
<td>Works at hypervisor level.</td>
<td>Synchronous replication impacts production systems and increases network latency.</td>
<td>Requires only one touch of the production system.</td>
</tr>
<tr>
<td>Enables quick recovery.</td>
<td>Requires a large amount of storage space to support multiple recovery points.</td>
<td>Provides warm DR capability with automated validation.</td>
</tr>
<tr>
<td>Works with different storage arrays.</td>
<td>Requires multiple touches of the production system.</td>
<td>Is application aware.</td>
</tr>
<tr>
<td>Is cost effective.</td>
<td></td>
<td>Can leverage Changed Block Tracking and compression to minimize network traffic.</td>
</tr>
<tr>
<td>May be application aware.</td>
<td></td>
<td>Uses incremental backups with deduplication to eliminate redundant data transfer.</td>
</tr>
<tr>
<td>Can leverage Changed Block Tracking to minimize network traffic.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Backup-Based Recovery with Scheduled Full VM Restores

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Live Sync Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables point-in-time recovery.</td>
<td>Is time consuming.</td>
<td>Provides VM replication from backup data.</td>
</tr>
<tr>
<td>Includes archiving support.</td>
<td></td>
<td>Offloads replication from production system.</td>
</tr>
<tr>
<td>Enables file-level restores.</td>
<td></td>
<td>Updates destination VM from backups, either immediately or on scheduled basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains warm DR capability for quick recovery and failover.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables point-in-time recovery from backup history aligned with data retention policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides more long term recovery choices compared to traditional replication methods.</td>
</tr>
</tbody>
</table>
## Specialized Disaster Recovery Software

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Live Sync Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides fast return to operation.</td>
<td>Is expensive.</td>
<td>Can automate orchestration with workflows.</td>
</tr>
<tr>
<td>Supports point-in-time cloning and recovery.</td>
<td></td>
<td>Monitor Live Sync status through dashboard.</td>
</tr>
<tr>
<td>Provides application protection.</td>
<td></td>
<td>Includes automatic validation.</td>
</tr>
<tr>
<td>Includes orchestration for failover and failback.</td>
<td></td>
<td>Provides network connection at the DR site.</td>
</tr>
<tr>
<td>Provides validation and failover testing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides failback capability.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Application-Level Replication

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Live Sync Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicates only application data.</td>
<td>Requires OS and updates on destination VM.</td>
<td>Application-aware VM backups create application consistent VMs on the recovery site, without requiring separate operating system installs or updates.</td>
</tr>
<tr>
<td>Supports quick failover of application.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recovery Scenarios and Orchestration

Live Sync supports failover and failback orchestration for the following scenarios. For any of these scenarios, you can specify the sequence in which the scenario is applied to virtual machines.

Test Boot Virtual Machines

To verify that destination virtual machines are ready for use in the event of a disaster, power on virtual machines. To avoid conflicts with the source VM and ensure that the virtual machine is not modified by the test boot, this workflow takes a snapshot of the virtual machine before the test boot, boots destination VMs with network connections disabled, and reverts to the snapshot afterwards.

Planned Failover

You can initiate a planned failover to perform maintenance on your primary site. This workflow powers off source VMs, performs an incremental backup of source VMs to capture the latest data, and then runs Live Sync to update the VMs in the disaster recovery site. After the DR site is up to date, the workflow disables Live Sync and powers on virtual machines in the DR site with appropriate network connections and IP addresses.

Unplanned Failover

In the event that the primary site is unavailable, this workflow disables Live Sync and powers up destination VMs at the DR site with appropriate network connections and IP addresses.
Fail Back

When the primary site becomes available again after a failover, you can sync virtual machines in the primary site by applying changes from the disaster recovery site.

Conclusion

By using backup data to create virtual machines in a disaster recovery site, Live Sync provides the ability to maintain a warm disaster recovery site with minimal impact on production systems.

This solution can take advantage of the capabilities included with storage arrays while offering the flexibility and application consistency of software-based solutions.
Glossary of Terms

A

auxiliary copy

A secondary copy of backup data for the same storage policy, typically using the primary backup as source.

B

backup copy

A copy of backup data that is created by mounting a snapshot that is used as source for a streaming backup.

backup set

An entity that manages backups of data for a specific client computer (hypervisor). Each virtualization client includes a default backup set, and each backup set contains at least one subclient.

C

copy

An instance of a storage policy that defines a particular type of backup. Each copy can specify retention criteria for backup data.

J

Job Details

A dialog box that provides detailed information about an active or completed job (such as a backup or restore operation).

L

Live Sync Monitor

A display that provides information about all of the scheduled Live Sync operations for a virtualization instance, backup set, or subclient.

M

MediaAgent

A software module that transmits data between client computers and storage media and manages data on the storage media.

P

proxy (VSA proxy)

A software module that manages backup and restore operations. A physical or virtual machine with the Virtual Server Agent installed is a VSA proxy.

S

schedule

An object that triggers automatic execution of a job with preset options. A Live Sync schedule can run automatically as soon as backups complete or on a periodic basis, and the schedule includes options for the Live Sync operation (such as the destination, whether to validate the destination VM, and other criteria).

selective copy

An instance of a storage policy that enables a specific copy of backup data to be selected as the source for auxiliary copy operations.

storage policy

A logical entity that associates backup data for one or more subclients with physical storage media.
subclient

A logical entity that identifies targets for backup operations. When created, the default subclient is automatically configured to protect all unprotected virtual machines; you can create user-defined subclients to target specific virtual machines or automatically discover virtual machines based on various criteria (such as host, guest operating system, or storage location).

Virtual Server Agent (VSA)

Software that is installed on a physical or virtual machine to enable the machine to manage backups.
Index

A
Alternative Deployments - 9
Application-Level Replication - 19
Architecture - 6
Audience - 5
auxiliary copy - 23

B
Backup Copies - 10
backup copy - 23
backup set - 23
Backup-Based Recovery with Scheduled Full VM Restores - 18
Basic Live Sync Flow - 6

C
Comparison of Different Technologies and Solutions - 17
Conclusion - 21
copy - 23

F
Fail Back - 21

H
Hardware Replication - 17

I
Incremental Forever - 8
Introduction - 5

J
Job Details - 23

L
Live Sync Configuration - 12
Live Sync Flow with DASH Copy - 7
Live Sync Monitor - 23
Live Sync Requirements - 8
Live Sync Schedules - 13
Local Recovery Site - 9

M
MediaAgent - 23
Monitoring - 16

Multiple Disaster Recovery Sites - 12

P
Planned Failover - 20
Planning and Requirements - 7
proxy (VSA proxy) - 23

R
Recovery Scenarios and Orchestration - 20
Remote Disaster Recovery Site - 11

S
SAN or HotAdd Deployments - 9
Scalability and Performance - 8
schedule - 23
selective copy - 23
Selective Copy - 9
Software-Based Virtual Machine Replication - 18
Specialized Disaster Recovery Software - 19
storage policy - 23
Storage Policy Copies - 15
subclient - 24

T
Test Boot Virtual Machines - 20

U
Unplanned Failover - 20
Using Live Sync to Support Disaster Recovery - 6

V
Validation - 15
Virtual Server Agent (VSA) - 24