VMware vSphere Replication 6.1

Technical Overview

Revised August 3, 2015
Contents
Introduction.................................................................................................................................................. 3
vSphere Replication use cases.................................................................................................................. 3
vSphere Replication features and benefits............................................................................................... 3
Architecture.................................................................................................................................................. 3
Initial Deployment and Configuration ...................................................................................................... 5
Replication Process.................................................................................................................................... 6
  Storage Policy-Based Management........................................................................................................ 8
  Recovery Point Objective...................................................................................................................... 8
  Guest Operating System and Application Quiescing............................................................................ 9
  Network Compression............................................................................................................................ 9
  Retention of Multiple Recovery Points............................................................................................ 9
Reporting..................................................................................................................................................... 10
Recovery Process....................................................................................................................................... 11
Summary.................................................................................................................................................... 13
About the Author......................................................................................................................................... 13
Introduction
VMware vSphere® Replication™ is a virtual machine data protection and disaster recovery solution. It is fully integrated with VMware vCenter Server™ and VMware vSphere Web Client, providing hypervisor-based, asynchronous replication of virtual machines. vSphere Replication is a proprietary replication engine developed by VMware that is included with VMware vSphere Essentials Plus Kit and higher editions of VMware vSphere, VMware vSphere with Operations Management™ editions, and VMware vCloud® Suite editions.

vSphere Replication use cases
- Data protection and disaster recovery within the same site and across sites
- Data center migration
- Replication engine for VMware Site Recovery Manager Air™ and VMware vCloud Air™ Disaster Recovery
- Replication engine for VMware Site Recovery Manager™

vSphere Replication features and benefits
- Simple virtual appliance deployment minimizes cost and complexity.
- Integration with vSphere Web Client eases administration and monitoring.
- Protect nearly any virtual machine regardless of operating system (OS) and applications.
- Only changes are replicated, which improves efficiency and reduces network utilization.
- Recovery point objective (RPO) configurable from 5 minutes to 24 hours on a per-virtual machine basis.
- Compatibility with VMware Virtual SAN™, VMware Virtual Volumes™, SAN, NAS, and local storage.
- Quick recovery for individual virtual machines minimizes downtime and resource requirements.
- Optional network isolation and compression help secure replicated data and further reduce network bandwidth consumption.
- Support for Microsoft Volume Shadow Copy Service (VSS) and Linux file system quiescing improves reliability of recovered virtual machines.

This paper presents an overview of the architecture, deployment, configuration, and management of vSphere Replication.

Architecture
vSphere Replication requires vCenter Server, either the Windows implementation or the Linux-based VMware vCenter Server Appliance™. VMware vCenter Single Sign-On™ is also required. If using vSphere Replication with Site Recovery Manager, the versions of the two must be the same. For example, vSphere Replication 6.1 is the only version of vSphere Replication supported with Site Recovery Manager 6.1. For complete details on VMware feature and product interoperability, consult the VMware Compatibility Guides.

vSphere Replication is deployed as one or more prebuilt, Linux-based virtual appliances. A maximum of 10 vSphere Replication appliances can be deployed per vCenter Server. Each appliance is deployed with 4GB of memory and either two virtual CPUs or four virtual CPUs. A vSphere Replication virtual appliance is configured with two virtual machine disk (VMDK) files totaling approximately 18GB in size.
Because vSphere Replication is a hypervisor-based replication solution, it is independent of the underlying storage and it works with a variety of storage types including Virtual SAN, traditional SAN, NAS, and direct-attached storage (DAS). Unlike many array replication solutions, vSphere Replication enables virtual machine replication between heterogeneous storage types. For example, Virtual SAN to DAS, SAN to NAS, and SAN to Virtual SAN. vSphere Replication can, of course, replicate virtual machines between the same types of storage, such as Virtual SAN to Virtual SAN.

vSphere Replication supports Site Recovery Manager Air, a software-as-a-service solution that offers cloud-based recovery plan management and orchestration for the vCloud Air Disaster Recovery service. Deployment consists of a single vSphere Replication virtual appliance on site. Replication is configured per-virtual machine and protected using a Secure Sockets Layer (SSL) connection between the vSphere Replication virtual appliance and vCloud Air. The Web-based Site Recovery Manager Air user interface is used to orchestrate migration of replicated virtual machines for simple, fast, and reliable recovery.

For disaster recovery between sites, vSphere Replication can be used as a replication engine for Site Recovery Manager. vSphere Replication virtual appliances are deployed at the source and target locations. Since replication is configured per-virtual machine, finer control of RPOs and selection of virtual machines included in Site Recovery Manager protection groups and recovery plans are possible. Use of Site Recovery Manager to protect virtual machines running on Virtual SAN requires vSphere Replication.
Initial Deployment and Configuration

A vSphere Replication virtual appliance is deployed from an Open Virtualization Format (OVF) file using vSphere Web Client. After the appliance has been deployed and powered on, a Web browser is used to access the virtual appliance management interface (VAMI) to finalize configuration.

The components that transmit replicated data are built into vSphere. There is no need to install or configure these components, further simplifying vSphere Replication deployment. The first virtual appliance deployed is referred to as the vSphere Replication management server. It contains the necessary components to receive replicated data, manage authentication, maintain mappings between the source virtual machines and the replicas at the target location, and provide support for vCloud Air Disaster Recovery, Site Recovery Manager Air, and Site Recovery Manager. In many cases, this is the only virtual appliance that must be deployed to enable vSphere Replication protection.

![vSphere Replication Deployment Example](image)

Additional vSphere Replication virtual appliances can be deployed to support larger-scale deployments and topologies with multiple target locations. These additional virtual appliances are referred to as vSphere Replication servers. They do not contain the management components found in the vSphere Replication management server and are used only to receive replicated data. In addition to the vSphere Replication management server, as many as nine vSphere Replication servers can be deployed to a vCenter Server environment, for a maximum of 10 deployed vSphere Replication virtual appliances.

Network traffic isolation for vSphere Replication can be configured to improve performance and security. Configuration consists of dedicating a network connection to vSphere Replication on the source and destination hosts as well as adding one or more virtual network interface cards to each vSphere Replication virtual appliance to segregate replication traffic and management traffic. vSphere Network I/O Control can be used to manage vSphere Replication network bandwidth utilization.
Replication Process

vSphere Web Client is used to configure replication for a virtual machine. Replication for one or more virtual machines can be selected and configured in the same workflow. When configuring replication, an administrator specifies items such as the target location, storage policy, RPO, VSS or Linux file system quiescing, network compression of replication traffic, and multiple recovery points. The target location for replicated virtual machines can be within the same vCenter Server environment, in another vCenter Server environment with vSphere Replication deployed, or a cloud provider such as vCloud Air. However, a virtual machine can only be replicated to a single target. For example, it is not possible to replicate the same virtual machine to multiple vCenter Server environments.
Once replication has been configured for a virtual machine, vSphere Replication begins the initial full synchronization of the source virtual machine to the target location. The time required to complete this initial synchronization can vary considerably and depends primarily on how much data must be replicated and how much network bandwidth is available. After the initial full synchronization, only changed data is transmitted in each replication cycle, which helps minimize network bandwidth consumption.

As mentioned earlier, the components that track and transmit data – the vSphere Replication agent and a vSCSI filter – are built into vSphere. They provide the plug-in interfaces for configuring and managing replication, track the changes to VMDKs, automatically schedule replication to achieve the RPO for each protected virtual machine, and transmit changed data to one or more vSphere Replication virtual appliances.

In environments where a large amount of data needs to be replicated initially and/or network bandwidth is considerably limited, copies of the VMDK files to be replicated can be created, shipped to the target location, and used as “seeds.” This method can greatly reduce the time required and network bandwidth consumed by the initial full synchronization versus replicating all of the data across the network. vSphere Replication will compare the source and target “seed” files and transmit only the differences.

NOTE: When replication begins and “seeds” are used, vSphere Replication compares the universally unique identifiers (UUIDs) of the source virtual disks and the target “seed” copies. If the UUIDs of the source and target do not match, vSphere Replication produces an error message and replication will not occur. This is by design to help prevent inadvertent overwriting of other VMDKs at the target location. VMware Knowledge Base article 2041657 contains more information on this topic.

When the target is a vCenter Server environment, data is transmitted from the source vSphere host to a vSphere Replication virtual appliance. The vSphere NFC protocol is used to transmit data received by a vSphere Replication virtual appliance to a vSphere host at the target location where it is written to storage.

The replicated data is first written to a file called a redo log, which is separate from the base target disk. After all changes for the current replication cycle have been received and written to the redo log, the data in the redo log is consolidated into the base disk. This process helps ensure the consistency of each base disk so virtual machines can be recovered at any time, even if replication is in progress or network connectivity is lost during transmission.

The process of replicating to a cloud provider such as vCloud Air is somewhat different. Data is sent from the source vSphere hosts to the on-premises vSphere Replication management server, where it is encrypted and sent to the cloud provider. Replication from the vSphere Replication management server to a cloud provider utilizes TCP port 443.
Storage Policy-Based Management

vSphere Replication supports the use of storage policies. When configuring replication, a storage policy can be selected to provide a list of target datastores that are compatible with the storage policy. When the virtual machine is recovered at the target location, the storage policy is automatically assigned to the recovered virtual machine.

![Select Target Location](image)

**Figure 7. Selecting a Storage Policy and Compatible Datastore When Configuring Replication**

Recovery Point Objective

A recovery point objective (RPO) defines the maximum acceptable age of data recovered from a backup or replicated copy as a result of an IT service or data loss issue. For example, if a virtual machine is deleted and the RPO for the virtual machine is 24 hours, a recovered copy of the virtual machine should contain all data except for any changes that occurred in the last 24 hours.

When replicating to and/or from VMFS and NFS datastores, vSphere Replication supports an RPO of 15 minutes to 24 hours. RPO is configured on a per-virtual machines basis. As an example, a virtual machine named “VM01” can be configured with an RPO of eight hours while “VM02” is configured with an RPO of 30 minutes regardless of which host and datastore they reside on.

Replicating between Virtual SAN datastores enables the configuration of RPOs as low as five minutes. It is important to note that the 5-minute RPO is supported only when replicating from a Virtual SAN datastore to a Virtual SAN datastore.

![Recovery Point Objective (RPO)](image)

**Figure 8. RPO of Five Minutes When Replicating Between Virtual SAN Datastores**
Guest Operating System and Application Quiescing

vSphere Replication offers the option to quiesce some guest operating systems and applications using Microsoft Volume Shadow Copy Service (VSS) for Windows virtual machines and file system quiescing for Linux virtual machines. Quiescing a virtual machine just before replication helps improve the reliability of recovering the virtual machine and its application(s). However, any solution, including vSphere Replication, that quiesces an operating system and/or application might impact performance. This is especially true in virtual machines that produce higher levels of I/O and where quiescing occurs often. For example, a very busy database server replicated with an RPO of 15 minutes. It is recommended to enable quiescing in vSphere Replication only for workloads that truly need it and benefit from it.

Network Compression

After vSphere Replication has completed the initial full synchronization of a virtual machine from the source to the target location, only the changes to the virtual machine are subsequently tracked and replicated to minimize network bandwidth utilization. Network compression can optionally be enabled on a per-virtual machine basis to further reduce the amount of data transmitted. However, this comes at the expense of an incremental increase in CPU utilization at the source and target locations. vSphere Replication uses the FastLZ compression library to provide an optimal balance of compression with low overhead.

Retention of Multiple Recovery Points

When configuring replication for a virtual machine, an administrator has the option to enable the retention of multiple recovery points (point-in-time instances). This can be useful when an issue is discovered several hours, or even a few days, after it occurred. For example, a replicated virtual machine with a 4-hour RPO contracts a virus, but the virus is not discovered until 6 hours after infestation. As a result, the virus has been replicated to the target location. With multiple recovery points, the virtual machine can be recovered and then reverted to a recovery point retained before the virus issue occurred.

The maximum number of recovery points that can be retained is 24. The following are some examples:

- Three recovery points per day over the last 5 days (15 recovery points)
- Five recovery points per day over the last 2 days (10 recovery points)
- Four recovery points over the last 6 days (24 recovery points)
Point in time instances

Retained replication instances are converted to snapshots during recovery. Replication of existing VM snapshots is not supported.

- Enable

Keep 4 instances per day for the last 6 days (24 total)

Figure 10. Configuring Point-in-Time Instances

The number of recovery points that can be retained per day is dependent on the RPO configured – more specifically, on the number of replication cycles that occur during the day. For example, it is not possible to retain eight recovery points per day if the RPO is set to 4 hours, with six replication cycles per day.

Retaining multiple recovery points consumes additional storage at the target location and must be planned for accordingly. The additional storage requirements depend on the number of recovery points retained and the data change rates in the source virtual machines.

Reporting

The vSphere Replication user interface provides information such as status, last synchronization duration and size, configured RPO, and which vSphere Replication server is receiving the replicated data.

Figure 11. Replication Details

Various reporting graphs are available to provide administrators with information such as number of replicated virtual machines per host, amount of data transferred, number of RPO violations, replication count, and number of sites successfully connected. These reports can be expanded for more details, and the date range can be modified.
Several vCenter Server alarms are also included with vSphere Replication to alert administrators of various events in the environment. The following are some examples:

- vSphere Replication server is disconnected
- Remote vSphere Replication site is disconnected
- Replication configuration changed
- RPO violation
- Virtual machine recovered from replica

The vSphere Replication documentation contains a complete list of the available triggers for vSphere Replication monitoring and alerting.

**Recovery Process**

Virtual machines are recovered one at a time in the vSphere Replication user interface. There are two recovery options:

**Synchronize recent changes** – To use this option, the source machine must be accessible and powered off. vSphere Replication replicates the latest changes from the source to the target location before recovering the virtual machine. Although this option likely increases recovery time, it helps ensure no loss of data.

**Use latest available data** – The latest replication data is used to recover the virtual machine. There is no final synchronization before recovery. This option is useful in cases where the source virtual machine is no longer accessible, such as when it has been deleted or after a disaster. As is typically found with asynchronous replication solutions, there is a potential for some data loss. The amount of loss depends on the rate of data change in the source virtual machine, the RPO configured in vSphere Replication, and the most recent replication occurrence.
Recovery options
Select the option to use during recovery.

- **Synchronize recent changes**
  Perform synchronization with the latest data from the source machine. Use this option if the source virtual machine is accessible.

- **Use latest available data**
  Skip data synchronization and use latest replication data on the target site. Use this option if the source site is not available or the disks of the source virtual machine are corrupted.

After selecting a recovery option, an administrator must select the folder and resource where the virtual machine will be re-covered. The virtual machine’s network device(s) will be disconnected when the virtual machine is recovered. An administrator must manually connect the virtual machine to the appropriate network(s) after recovery. Optionally, the virtual machine can be powered on as part of the recovery process.

A virtual machine is always recovered to the most recent recovery point. If replication has been configured with multiple recovery points enabled, an administrator can revert the recovered virtual machine to a previous recovery point after the vSphere Replication recovery process has completed. These recovery points are retained as virtual machine snapshots, which are managed using VMware vSphere Web Client Snapshot Manager, a component of vSphere Web Client. The snapshots are labeled with the date and time of the recovery point. An administrator has the option to revert to a snapshot, delete a snapshot, or delete all snapshots for the recovered virtual machine.
Automation and additional recovery options are available when vSphere Replication is used with Site Recovery Manager and vCloud Air Disaster Recovery. For example, an administrator can easily test the recovery of virtual machines without stopping replication or disrupting production systems. It is also possible after a failover or migration to re-protect workloads and replicate them from the recovery location back to the original location with minimal downtime, which is useful in disaster avoidance scenarios. Site Recovery Manager and Site Recovery Manager Air automate the process of connecting recovered virtual machines to one or more networks at the recovery location and changing IP addresses if needed.

Summary
VMware vSphere Replication provides an efficient solution for protecting a VMware virtual machine infrastructure. It is compatible with VMware Virtual SAN, traditional storage area networks (SANs), network-attached storage (NAS), and direct-attached storage (DAS). vSphere Replication is simple to deploy and consumes minimal network resources through the use of compression and by sending only changed data from the source to the target location. Recovery point objectives range from 5 minutes to 24 hours and can be configured on a per-virtual machine basis. Multiple recovery points can be retained for increased protection. Configuration and recovery are easily enabled using VMware vSphere Web Client. vSphere Replication can be used as a standalone product or with VMware Site Recovery Manager, which provides robust testing, migration, and failover orchestration. vSphere Replication also powers VMware vCloud Air Disaster Recovery, delivering a true hybrid cloud disaster recovery solution.

About the Author
Jeff Hunter is a senior technical marketing architect at VMware with a focus on business continuity and disaster recovery solutions. He has been with VMware for more than 8 years, prior to which he spent several years implementing and administering VMware virtual infrastructures at two Fortune 500 companies.

Follow Jeff on Twitter: @jhuntervmware