



vSphere Replication Technical Overview

VMware BC/DR

Table of contents

vSphere Replication Technical Overview	3
Introduction	3
vSphere Replication use cases	3
vSphere Replication features and benefits	3
Architecture Overview	4
Initial Deployment and Configuration	5
Replication Process	6
Retention of Multiple Recovery Points	8
Reporting	9
Recovery Process	10
Summary	12

vSphere Replication Technical Overview

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 host-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 vCenter™ 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 objectives (RPOs) range from 5 minutes to 24 hours and can be configured on a per-virtual machine basis.
- Compatibility is provided with VMware vSAN™, traditional SAN, NAS, and local storage.
- Quick recovery for individual virtual machines minimizes downtime and resource requirements.
- Optional network isolation, replication traffic encryption, 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 the reliability of recovered virtual machines.

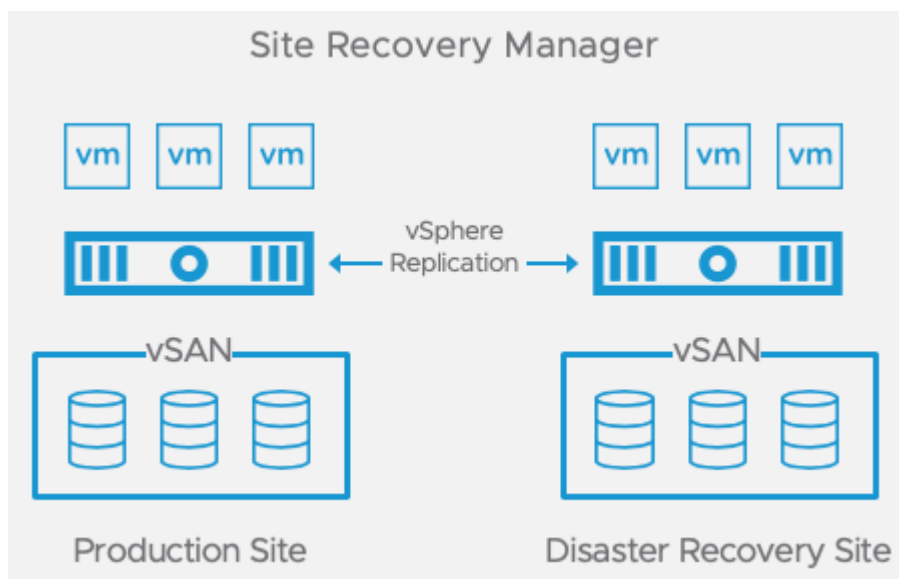
This paper presents an overview of the architecture, deployment, configuration, and management of vSphere Replication.

Architecture Overview

vSphere Replication is deployed as one or more prebuilt, Photon OS-based virtual appliances. A maximum of 10 vSphere Replication appliances can be deployed per vCenter Server.

Because vSphere Replication is host-based replication, it is independent of the underlying storage and it works with a variety of storage types including vSAN, 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, vSAN to DAS, SAN to NAS, and SAN to vSAN. vSphere Replication can, of course, replicate virtual machines between the same types of storage, such as vSAN to vSAN.

vSphere Replication can also serve as the replication engine for VMware Site Recovery Manager. In this scenario, vSphere Replication virtual appliances are deployed at both the source and target locations, as with VMware Site Recovery Manager. Replication is configured on a per-virtual machine basis, enabling fine control and selection of the virtual machines that are included in VMware Site Recovery Manager protection groups and recovery plans. The use of VMware Site Recovery Manager to protect virtual machines running on vSAN requires vSphere Replication.



Initial Deployment and Configuration

A vSphere Replication virtual appliance is deployed from an Open Virtualization Format (OVF) file using the 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 the 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 and VMware Site Recovery Manager. In many cases, this is the only appliance that must be deployed to enable vSphere Replication protection.

vSphere Replication 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. The 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 separate replication traffic and management traffic. vSphere Network I/O Control can be used to control vSphere Replication bandwidth utilization. Traffic encryption can be configured on a per-VM basis to protect traffic from the source host to the target vSphere Replication Appliance.

Replication Process

vSphere HTML5 client configures replication for a virtual machine. Replication for one or more virtual machines can be selected and configured via the same workflow. When configuring replication, an administrator specifies items such as the virtual machine storage policy, RPO, VSS or Linux file system quiescing, network compression and encryption of replication traffic. Virtual machine snapshots are **not used** as part of the replication process unless VSS quiescing is enabled.

The target location for vSphere Replication can be within the same vCenter Server environment or in another vCenter Server environment with vSphere Replication deployed.

Configure Replication - Web05

- 1 VM validation
- 2 Target site**
- 3 Target datastore
- 4 Replication settings
- 5 Protection group
- 6 Ready to complete

Target site

Select the target site where the virtual machine will be replicated.

	Target Site	Status
<input type="radio"/>	vcentersitea.vsanpe.vmware.com	✓ Logged in
<input checked="" type="radio"/>	vcentersiteb.vsanpe.vmware.com	✓ Logged in

2 site(s)

Select the vSphere Replication server that will handle the replication.

- Auto-assign vSphere Replication Server
- Manually select vSphere Replication Server

	Name	Replications
<input type="radio"/>	VRsiteB01 (embedded)	4

1 replication server(s)

[CANCEL](#)
[BACK](#)
[NEXT](#)

The same vSphere Replication deployment can replicate some virtual machines to a local vCenter Server environment and other virtual machines to a remote vCenter or to VMware Site Recovery for VMware Cloud on AWS.

Forward replications

[Learn more](#)

+ NEW

<input type="checkbox"/>	Virtual Machine	Status	Target	Replication Server
<input type="checkbox"/>	> App01	✓ OK	Site B	VRsiteB01
<input type="checkbox"/>	> App02	✓ OK	Site B	VRsiteB01
<input type="checkbox"/>	> App03	✓ OK	Site B	VRsiteB01
<input type="checkbox"/>	> Finance01	✓ OK	Site B	VRsiteB01

NOTE: The same virtual machine cannot be replicated to more than one target.

After replication has been configured for a virtual machine, vSphere Replication begins the initial full synchronization of the source virtual machine to the target location, using TCP port 31031. 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.

A copy of the VMDKs to be replicated can be created and shipped to the target location and used as “seeds,” reducing the time and network bandwidth consumed by the initial full synchronization. When replication begins, 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 issue.

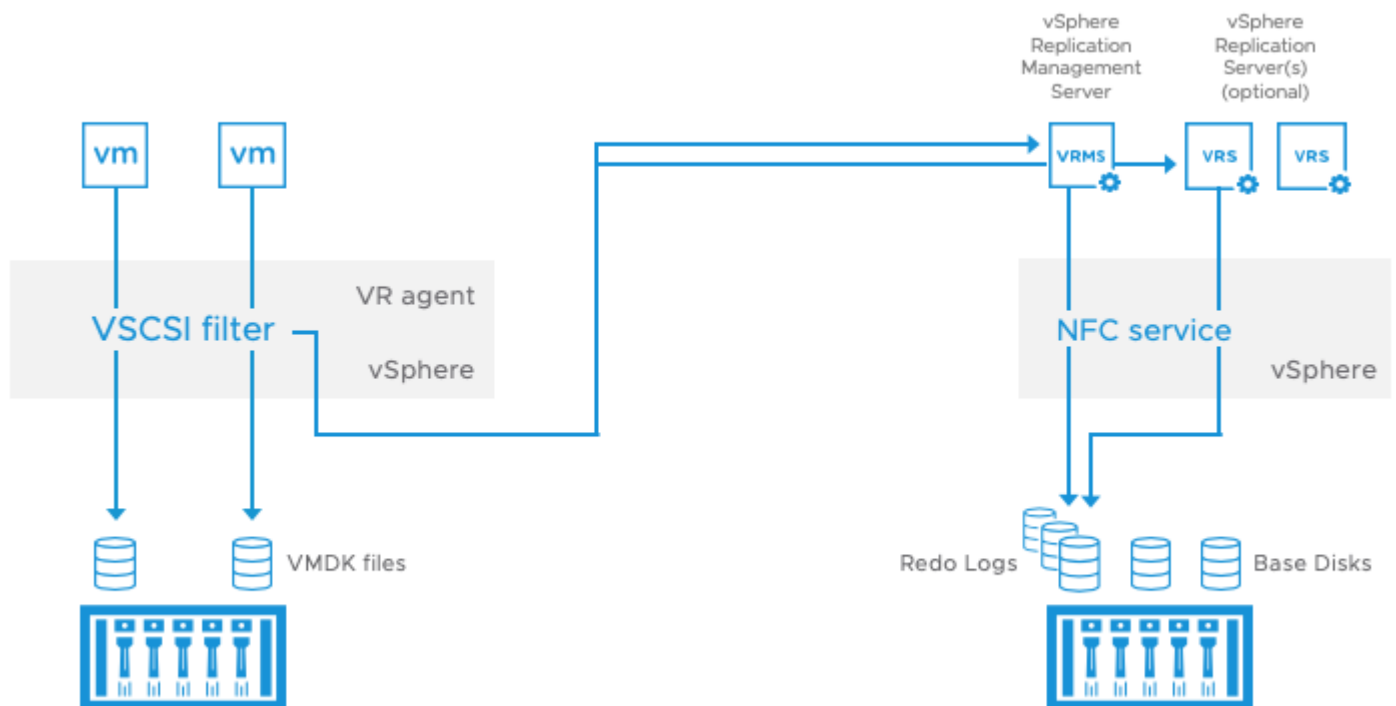
After the initial full synchronization, changes to the protected virtual machine are tracked and replicated on a regular basis. The transmissions of these changes are referred to as “lightweight delta syncs.” Their frequency is determined by the RPO that was configured for the virtual machine. A lower RPO requires more-frequent replication.

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.

App03		✓ OK	Site B	VRsiteB01
Configured disks:	2 of 2	Last instance sync point:	May 9, 2019, 9:26:52 PM	
Managed by:	VR	Last sync duration:	3 minutes and 16 seconds	
Quiescing:	Disabled	Last sync size:	4.34 MB	
Network compression:	Disabled	RPO:	1 hour	
		Points in time:	Enabled (keep 24 instances per day for the last 1 days)	

As mentioned earlier, the components that transmit replicated 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 the changed data to one or more vSphere Replication virtual appliances.

When the target is a vCenter Server environment, data is transmitted from the source vSphere host to either a vSphere Replication management server or vSphere Replication server and is written to storage at the target location. The replication stream can be encrypted. As data is being replicated, the changes are first written to a file called a redo log, which is separate from the base 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 VMware Site Recovery for VMware Cloud on AWS is identical to normal vSphere Replication operation.

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)

Enable point in time instances ⓘ

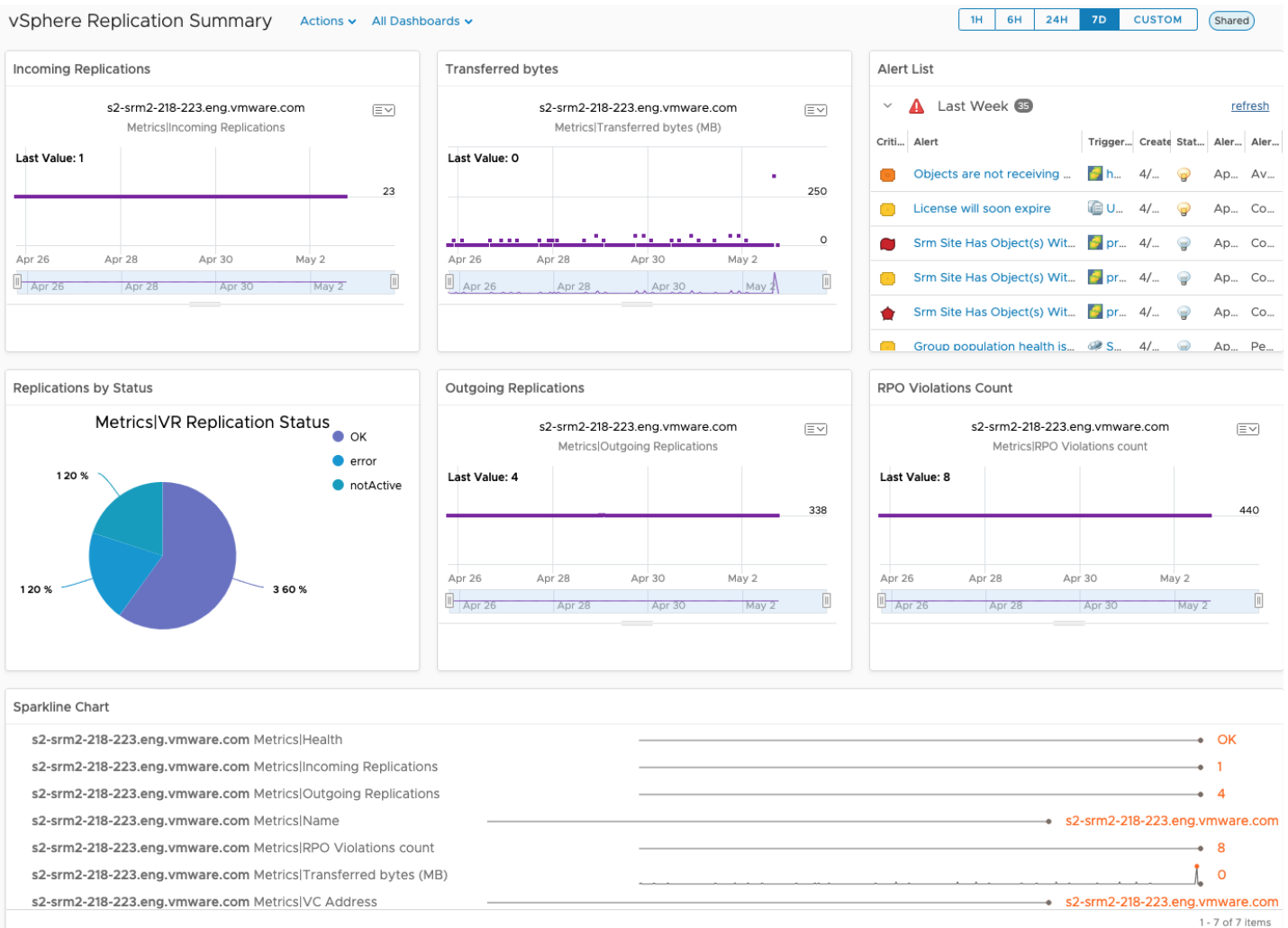
Keep 3 instances per day for the last 5 days

If the RPO period is longer than 8 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.

The number of recovery points that can be retained per day is dependent on the RPO—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

For general reporting, the vSphere Replication interface includes details about replication direction, site target, appliance target, and status. For detailed reporting, there is the vSphere Replication Management pack for vRealize Operations.



There are several vCenter Server alarms 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 the 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.

Recover virtual machine

- 1 Recovery options
- 2 Folder
- 3 Resource
- 4 Ready to complete

Recovery options ✕

- Synchronize recent changes
 Perform synchronization with the latest data from the source machine. Use this option if the source virtual machine is accessible. Requires login to the remote site.
- 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.
- Power on the virtual machine after recovery.
- Points in time recovery
 There are 1 currently retained instances that will be converted to snapshots during recovery.

After selecting a recovery option, an administrator must select the folder and resource where the virtual machine will be recovered. 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.

Manage Snapshots | App03

The screenshot displays a list of snapshots for a virtual machine named 'App03'. The snapshots are listed in chronological order, starting from 2019-05-11 19:48:25 UTC and ending at 2019-05-12 07:00:00 UTC. Each snapshot entry includes a small icon representing a snapshot and a downward arrow indicating it is expanded. Below the list, there are three buttons: 'DELETE ALL', 'DELETE', and 'REVERT TO'. The interface also features a vertical scrollbar on the right and a horizontal scrollbar at the bottom of the list area.

Automation and additional recovery options are available when vSphere Replication is used with vCenter 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 reprotect workloads and replicate them from the recovery location back to the original location with minimal downtime, which is useful in disaster avoidance scenarios. vCenter Site Recovery Manager automates 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 vSAN, 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.

