

VMware vSphere Replication 8.8

Table of Contents

Release Notes	9
vSphere Replication 8.8.0.3 Release Notes.....	9
vSphere Replication 8.8.0.2 Release Notes.....	10
vSphere Replication 8.8.0.1 Release Notes.....	11
VMware vSphere Replication 8.8 Release Notes.....	12
VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 Release Notes.....	27
VMware Aria Operations Management Pack for vSphere Replication 8.8 Release Notes.....	31
Compatibility Matrices for vSphere Replication 8.8.....	33
vSphere Replication Administration	39
About VMware vSphere Replication	39
vSphere Replication Appliance Components.....	40
Local and Remote Sites.....	40
How vSphere Replication Works.....	41
Replication Data Compression.....	45
vSphere Replication System Requirements	45
vSphere Replication Licensing.....	46
Operational Limits of vSphere Replication.....	46
vSphere Replication Compatibility Information.....	47
Bandwidth Requirements for vSphere Replication.....	48
Calculate Bandwidth For vSphere Replication.....	50
Installing and Setting Up vSphere Replication	50
Prepare Your Environment to Install vSphere Replication.....	51
Deploy the vSphere Replication Appliance.....	51
Configure the vSphere Replication Appliance to Connect to a vCenter Server instance.....	53
Concurrent Installations of vSphere Replication in an Enhanced Linked Mode Environment.....	53
Configure the vSphere Replication Appliance to Connect to a vCenter Server.....	54
Understanding the States of vSphere Replication Displayed in the.....	55
Configure vSphere Replication Connections.....	57
Understanding the vSphere Replication Site Connection States.....	57
Reconnect to a Remote Site.....	58
Use the OVF Tool to Deploy vSphere Replication Virtual Appliance.....	59
Uninstall vSphere Replication.....	61
Remove the vSphere Replication Tag from Target Datastores.....	62
Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted.....	63
Clean up the vCenter Lookup Service.....	63
Clean up the vCenter Server Extension Manager.....	64

Participate in the Customer Experience Improvement Program.....	65
Exporting and Importing Replication Configuration Data.....	65
Export Replication Configuration Data.....	66
Use a Properties File to Export vSphere Replication Configuration Data.....	67
Import Replication Configuration Data.....	68
Import Large Numbers of Replications.....	69
Properties for Automated Export and Import of vSphere Replication Configuration Data.....	69
Syntax of the Import/Export Tool.....	70
Isolating the Network Traffic of vSphere Replication.....	72
Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host.....	74
Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host.....	75
Create a VM Network Adapter to Use for Incoming Replication Traffic on the Combined vSphere Replication Appliance.....	75
Create VM Network Adapters to Isolate the Network Traffic of an Additional vSphere Replication Server.....	76
Configure a Static Route on an Additional VM Network Adapter.....	78
Deploying Additional vSphere Replication Servers.....	78
Deploy an Additional vSphere Replication Server.....	78
Register an Additional vSphere Replication Server.....	80
Replication Server Connection States.....	80
Reconfigure vSphere Replication Server Settings.....	80
Unregister and Remove a vSphere Replication Server.....	82
Deactivate the Embedded vSphere Replication Server.....	83
Use the OVF Tool to Deploy an Additional vSphere Replication Server.....	83
Upgrading vSphere Replication.....	85
Order of Upgrading vSphere and vSphere Replication Components.....	85
Upgrade Additional vSphere Replication Servers.....	86
Upgrade vSphere Replication Appliance.....	87
Update the vCenter Server IP Address in the vSphere Replication Management Server.....	87
Reconfiguring the vSphere Replication Appliance.....	88
Reconfigure General vSphere Replication Settings.....	88
Change the Password of the vSphere Replication Appliance.....	90
Change the Keystore Passwords of the vSphere Replication Appliance.....	90
Change the Truststore Passwords of the vSphere Replication Appliance.....	91
Activate or Deactivate SSH Access to the vSphere Replication Appliance.....	92
Change the SSL Certificate of the vSphere Replication Appliance.....	92
How to Activate the Verification of Certificate Validity.....	93
vSphere Replication Certificate Verification.....	93
Requirements When Using a Public Key Certificate with vSphere Replication.....	94
Generate and Download a Certificate Signing Request for the vSphere Replication Appliance.....	94
Configure vSphere Replication Network Settings.....	95

Configure the Time Zone and Time Synchronization Settings for the vSphere Replication Appliance.....	97
Start, Stop, and Restart vSphere Replication Appliance Services.....	97
Forward vSphere Replication Appliance Log Files to Remote Syslog Server.....	97
Enable the SHA-1 Hashing Function.....	98
Activate FIPS on vSphere Replication.....	98
How do I validate that FIPS mode is activated.....	102
vSphere Replication Roles and Permissions.....	102
vSphere Replication Roles Reference.....	102
Assign VRM Replication Viewer Role.....	105
Assign VRM Virtual Machine Replication User Role.....	106
Assign VRM Virtual Machine Recovery User Role and Perform a Recovery Operation.....	106
Clone an Existing VRM Administrator Role and Modify Privileges.....	106
Replicating Virtual Machines.....	107
Recovery Point Objective.....	107
How the Retention Policy Works.....	108
Replicating a Virtual Machine and Enabling Multiple Point in Time Instances.....	109
Using vSphere Replication with vSAN Storage.....	110
Using vSphere Replication with vSphere Storage DRS.....	111
How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration.....	111
How vSphere Replication Synchronizes Data Between the Source and the Target Sites During Incremental Sync.....	113
Replicating Virtual Machines Using Replication Seeds.....	113
Replicating a Virtual Machine in a Single vCenter Server Instance.....	114
Replicating Encrypted Virtual Machines.....	114
Network Encryption of Replication Traffic.....	115
How vSphere Replication Works When Using Guest OS Trim/Unmap Commands.....	115
Use the Unmap Handling Mode of the vSphere Replication Filter Driver.....	116
Best Practices for Using and Configuring vSphere Replication.....	117
Configure a Replication.....	119
Move a Replication to a New vSphere Replication Server.....	121
Stop Replicating a Virtual Machine.....	121
Reconfiguring Replications.....	122
Reconfigure Recovery Point Objectives (RPO) in Replications.....	123
Change the Point in Time Settings of a Replication.....	123
Increasing the Size of Replicated Virtual Disks.....	123
Change the Target Datastore Location of a Replication.....	125
Exclude a Disk from the Replication.....	126
Include a Disk to the Replication.....	127
Changing the Storage Policy of Replica Disks.....	127
Enable VM Encryption for an Already Replicated VM.....	128

Replicate Virtual Machines with DataSets.....	128
Stopping a Virtual Machine Offline Synchronization Task.....	129
Stop a Virtual Machine Offline Synchronization Task by Using an SSH Connection.....	129
Stop a Virtual Machine Offline Synchronization Task by Using the vCenter Server MOB.....	129
Monitoring and Managing Replications in vSphere Replication.....	130
Monitor the Status of a Replication.....	131
View Replication Reports for a Site.....	132
Interpreting Replication Statistics for a Site.....	133
Identifying Replication Problems.....	135
Manage vSphere Replication Connections.....	135
Manage vSphere Replication Servers.....	136
Performing a Recovery with vSphere Replication.....	137
Recover Virtual Machines with vSphere Replication.....	137
Failback of Virtual Machines in vSphere Replication.....	139
Using the vSphere Replication REST API Gateway.....	139
Download the Open API Specification.....	140
List of vSphere Replication REST APIs.....	140
How to Use the REST APIs to Create a Site Pairing.....	147
How to Use the REST APIs to Configure a Replication.....	148
DR REST API Rate Limiter.....	151
Best practices for setting the optimal Rate Limit configuration.....	152
Troubleshooting vSphere Replication.....	152
Generate vSphere Replication Support Bundle.....	153
Increase the Support Volume for Support Bundles.....	153
Manually Access the vSphere Replication Logs.....	154
vSphere Replication Events and Alarms.....	154
List of vSphere Replication Events.....	154
Solutions for Common vSphere Replication Problems.....	157
OVF Package Is Invalid and Cannot Be Deployed.....	157
vSphere Replication Service Fails with Unresolved Host Error.....	157
Error Recovering Virtual Machine in a Single vCenter Server Instance.....	158
vSphere Replication RPO Violations.....	158
vSphere Replication Appliance Extension Cannot Be Deleted.....	159
vSphere Replication Does Not Start After Moving the Host.....	159
Unexpected vSphere Replication Failure Results in a Generic Error.....	160
Reconnecting Sites Fails If One of the vCenter Server Instances Has Changed Its IP Address.....	161
vSphere Replication Server Registration Takes Several Minutes.....	161
Generating Support Bundles Disrupts vSphere Replication Recovery.....	161
vSphere Replication Operations Take a Long Time to Complete.....	162
vSphere Replication Operations Fail with Authentication Error.....	162

vSphere Replication Does Not Display Incoming Replications When the Source Site Is Inaccessible.....	162
vSphere Replication Is Inaccessible After Changing vCenter Server Certificate.....	163
vSphere Replication Cannot Establish a Connection to the Hosts.....	163
Anti-Virus Agent in Firewall Stops Virtual Machine Replication.....	163
Initial Full Synchronization of Virtual Machine Files to VMware vSAN Storage Is Slow.....	163
Update the Child Replica Disks When Changing the Storage Policy for a vSAN Target Datastore.....	164
Configuring Replication Fails Because Another Virtual Machine Has the Same Instance UUID.....	164
vSphere Replication Operations Run Slowly as the Number of Replications Increases.....	165
Unable to Establish an SSH Connection to the vSphere Replication Appliance.....	165
The Replication Pauses When You Add a New Disk to the Source VM.....	166
The vSphere Replication Appliance Root File System Switches to Read-Only Mode and Login Fails.....	166
Configuration of an Encrypted VM Fails with an Error.....	166
Reprotect Failures on Overloaded Datastores.....	167
Reconfigure replication process fails with an error after a long time.....	167
Configuring a replication for a VM with physical mode RDM disk fails with an error.....	167
You cannot use custom defined users and roles with vSphere Replication.....	168
VMs that are located in the target folder are overwritten during recovery with vSphere Replication.....	168
Generating a support bundle fails.....	168
You cannot configure new replications with network encryption.....	168
Replications with network encryption appear in Not Active state.....	169
You cannot use network encryption for vSphere Replication.....	169
VMware Aria Operations Management Pack Alerts and Metrics for vSphere Replication.....	169
VMware vSphere Replication Security Guide.....	172
About VMware vSphere Replication Security Guide.....	172
vSphere Replication Security Reference.....	172
Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses.....	172
vSphere Replication Configuration Files.....	175
vSphere Replication Private Key, Certificate, and Keystore.....	176
vSphere Replication License and EULA File.....	176
vSphere Replication Log Files.....	176
vSphere Replication User Accounts.....	177
Security Updates and Patches for vSphere Replication.....	178
Using the VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8.....	179
Using the vSphere Replication Plug-In.....	179
Automated Operations That VMware Aria Automation Orchestrator Plug-In for vSphere Replication Provides.....	179
Installing the vSphere Replication Plug-In.....	180
Functional Prerequisites.....	180
Installing, Upgrading, and Uninstalling the vSphere Replication Plug-In.....	180
Using the vSphere Replication Plug-In Workflows.....	181

Available Workflows in vSphere Replication Plug-In.....	181
Prerequisites for Using the vSphere Replication Plug-In.....	183
Finding Common Objects in the vSphere Replication Plug-In.....	183
Configure Replication Workflows.....	185
Configure Replication Workflow.....	186
Protect Multiple Virtual Machines Workflow.....	187
Reconfigure Replication Workflow.....	188
Remote Site Management Workflows.....	189
Pair with a vCenter Server Site Workflow.....	190
Reconnect a vCenter Server Site to a vCenter Server Site Pair Workflow.....	190
Configure vSphere Replication Plug-in Connection Settings Workflow.....	191
Log In to a vCenter Server Site Workflow.....	191
Log in to a vCenter Server Site with Credentials Workflow.....	191
Register vCenter Server Site Workflow.....	192
Unregister vCenter Server Site Workflow.....	192
Sync Workflows.....	192
Full Sync Replication to vCenter Server Workflow.....	193
Offline Sync Replication to vCenter Server Workflow.....	193
Sync Replication to vCenter Server Workflow.....	193
Pause Workflows.....	193
Pause Replication to vCenter Server.....	193
Resume Workflows.....	194
Resume Replication to vCenter Server Workflow.....	194
Stop Replication Workflows.....	194
Stop Replication Workflow.....	194
Replication Details Workflows.....	195
Check Replication Status Workflow.....	195
Get Replication Configuration Workflow.....	195
Get Replication List Workflow.....	196
Get Replication Issues Workflow.....	196
Get Replication IDs Workflow.....	197
Get Replication Recovery Solution Workflow.....	197
Get Replication Recovery Point Objective Violation Workflow.....	197
Get Replication Test Bubble Status Workflow.....	198
Troubleshooting the VMware Aria Automation Orchestrator Plug-In for vSphere Replication.....	198
Incorrect remote site object is retrieved when using the vSphere Replication Plug-in through VMware Aria Automation.....	198
Documentation Legal Notice.....	200

Release Notes

Product enhancements, updates, support notices, known and resolved issues for the VMware vSphere Replication 8.8 releases.

vSphere Replication 8.8.0.3 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Installation and Upgrade](#)

Introduction

vSphere Replication 8.8.0.3 | 08 FEB 2024 | Build 23263438 | [Download](#)

Check for additions and updates to these release notes.

VMware vSphere Replication 8.8.0.3 is a minor product patch release that provides bug fixes. The content of the [VMware vSphere Replication 8.8 Release Notes](#) applies to this version as well.

What's New

VMware vSphere Replication 8.8.0.3 Express Patch provides the following new capabilities:

- Updated VMware Postgres to version 14.10
- Updated the Tomcat server to version 9.0

Installation and Upgrade

For the supported upgrade paths for vSphere Replication, select **Upgrade Path** and **VMware vSphere Replication** in the [VMware Product Interoperability Matrices](#).

You use the ISO file and the VRMS Appliance Management Interface to upgrade from vSphere Replication 8.6.x or 8.7.x to vSphere Replication 8.8.0.x.

Important: Before you initiate an upgrade, verify that the vSphere Replication appliance has an OVF environment, or context. See [Checking and Restoring the OVF Context of the vSphere Replication Appliance \(2106709\)](#).

See [Upgrade Additional vSphere Replication Servers](#) and [Upgrade the vSphere Replication Appliance](#) for the procedures on upgrading to vSphere Replication 8.8.0.3.

Notes:

- After upgrading vSphere Replication, the ESXi hosts automatically enter and exit maintenance mode. See [KB 389735](#).
- When you use vSphere Replication with Site Recovery Manager, upgrade vSphere Replication on both of the protected and the recovery sites before you upgrade the Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. For more information, see the *VMware Site Recovery Manager Documentation*.

vSphere Replication 8.8.0.2 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Installation and Upgrade](#)
- [Resolved Issues](#)

Introduction

vSphere Replication 8.8.0.2 | 21 NOV 2023 | Build 22780283

Check for additions and updates to these release notes.

[VMware vSphere Replication 8.8.0.3](#) replaces the previously released VMware vSphere Replication 8.8.0.2. The content of the [VMware vSphere Replication 8.8 Release Notes](#) applies to this version as well.

What's New

- VMware vSphere Replication 8.8.0.2 Express Patch provides security and bug fixes.
- FIPS compliance for Site Recovery user interface and vSphere Client plug-in. For more information, see [How do I activate FIPS on vSphere Replication](#) and [How do I validate that FIPS mode is activated](#).

Installation and Upgrade

For the supported upgrade paths for vSphere Replication, select **Upgrade Path** and **VMware vSphere Replication** in the [VMware Product Interoperability Matrices](#).

You use the ISO file and the VRMS Appliance Management Interface to upgrade from vSphere Replication 8.6.x or 8.7.x to vSphere Replication 8.8.0.x.

Important: Before you initiate an upgrade, verify that the vSphere Replication appliance has an OVF environment, or context. See [Checking and Restoring the OVF Context of the vSphere Replication Appliance \(2106709\)](#).

See [Upgrade Additional vSphere Replication Servers](#) and [Upgrade the vSphere Replication Appliance](#) for the procedures on upgrading to vSphere Replication 8.8.0.2.

Notes:

- After upgrading vSphere Replication, the ESXi hosts automatically enter and exit maintenance mode. See [KB 389735](#).
- When you use vSphere Replication with Site Recovery Manager, upgrade vSphere Replication on both of the protected and the recovery sites before you upgrade the Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. For more information, see the *VMware Site Recovery Manager Documentation*.

Resolved Issues

You are unable to get a list of virtual machines by using the vSphere Replication REST APIs

The vSphere Replication REST API call `/pairings/{pairing_id}/vcenters/{vcenter_id}/vms` fails with an error 404 Not Found.

This issue is fixed in vSphere Replication 8.8.0.2.

You cannot replicate an encrypted VM to a vSphere Storage DRS cluster

When you try to configure a replication for an encrypted VM to a vSphere Storage DRS cluster, the cluster is not available for selection in the Target Datastore wizard page.

This issue is fixed in vSphere Replication 8.8.0.2.

vSphere Replication 8.8.0.1 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Installation and Upgrade](#)
- [Resolved Issues](#)

Introduction

vSphere Replication 8.8.0.1 | 17 OCT 2023 | Build 22602641 | [Download](#)

Check for additions and updates to these release notes.

VMware vSphere Replication 8.8.0.1 is a minor product patch release that provides bug fixes. The content of the [VMware vSphere Replication 8.8 Release Notes](#) applies to this version as well.

What's New

VMware vSphere Replication 8.8.0.1 Express Patch provides bug fixes.

Installation and Upgrade

For the supported upgrade paths for vSphere Replication, select **Upgrade Path** and **VMware vSphere Replication** in the [VMware Product Interoperability Matrices](#).

You use the ISO file and the VRMS Appliance Management Interface to upgrade from vSphere Replication 8.6.x or 8.7.x to vSphere Replication 8.8.0.x.

Important: Before you initiate an upgrade, verify that the vSphere Replication appliance has an OVF environment, or context. See [Checking and Restoring the OVF Context of the vSphere Replication Appliance \(2106709\)](#).

See [Upgrade Additional vSphere Replication Servers](#) and [Upgrade the vSphere Replication Appliance](#) for the procedures on upgrading to vSphere Replication 8.8.0.1.

Notes:

- After upgrading vSphere Replication, the ESXi hosts automatically enter and exit maintenance mode. See [KB 389735](#).
- When you use vSphere Replication with Site Recovery Manager, upgrade vSphere Replication on both of the protected and the recovery sites before you upgrade the Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. For more information, see the *VMware Site Recovery Manager Documentation*.

Resolved Issues

Upgrade to vSphere Replication 8.8 fails with an error

When you attempt to perform a chain upgrade from an earlier version of vSphere Replication, for example from version 8.3 to version 8.8, the upgrade might fail with an error.

Operation Failed: Failed to install update.

The logs located in `/opt/vmware/var/log/vami/updatecli.log` show the following:

Error: Failed to synchronize cache for repo 'VMware Photon Linux 3.0 (x86_64)' from 'https://packages.vmware.com/photon/3.0/photon_release_3.0_x86_64'1. package xml-security-c-1.7.3-4.ph2.x86_64 requires libcrypto.so.1.0.0() (64bit), but none of the providers can be installed.

Alternatively, vSphere Replication might fail to boot, displaying the following error:

```
Loading Linux 4.19.182-2.ph3 ...
error: file '/vmlinuz-4.19.182-2.ph3' not found.
Loading initial ramdisk ...
error: you need to load the kernel first.
```

This issue is fixed in vSphere Replication 8.8.0.1.

VMware vSphere Replication 8.8 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Localization](#)
- [Product Documentation](#)
- [Compatibility](#)
- [Installation](#)
- [Upgrading vSphere Replication](#)
- [Operational Limits of vSphere Replication](#)
- [Open Source Components](#)
- [Caveats and Limitations](#)
- [Known Issues](#)

Introduction

vSphere Replication 8.8 | 21 SEP 2023 | Build 22436165 | [Download](#)
vSphere Replication Configuration Import/Export Tool 8.8 | 21 SEP 2023 | Build 22297628 | [Download](#)
Check for additions and updates to these release notes.

What's New

- VMware vSphere Replication 8.8 adds compatibility with VMware vSphere 8.0 Update 2.
- VMware vSphere Replication 8.8 adds support for VMware vSphere Lifecycle Manager-managed hosts and clusters.
- Expose the DR REST APIs through the VMware Aria Automation Orchestrator plug-in for vSphere Replication 8.8. Introducing the end-to-end support of vSphere Replication REST APIs through the VMware Aria Automation Orchestrator plug-in for vSphere Replication 8.8. Customers can benefit by automating manual workflows to monitor, protect, manage appliances, and run recovery plans. For more information, see [DR REST plug-in for VMware Aria Automation Orchestrator Release notes](#).
- VMware Aria Operations Management Pack for vSphere Replication 8.8. For information about the management pack, see [VMware Aria Operations Management Pack for vSphere Replication 8.8 Release notes](#).
- VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8. For information about the new workflows, see [VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 Release notes](#).

For interoperability with earlier or later releases of VMware vSphere, see the [Compatibility Matrices for vSphere Replication 8.8](#).

For information about the features of vSphere 8.0 Update 2, see the [vSphere 8.0 Update 2 documentation](#).

Localization

VMware vSphere Replication 8.8 is available in the following languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Spanish
- Simplified Chinese
- Traditional Chinese

Product Documentation

In addition to the current release notes, you can use the documentation set for vSphere Replication 8.8 that includes the following deliverables.

- [vSphere Replication 8.8 Documentation Center](#)
- [Compatibility Matrices for vSphere Replication 8.8](#)

Compatibility

vSphere Replication 8.8 is compatible with vSphere 7.0 Update 3 and later, and supports ESXi versions 7.0 Update 3 and later.

For interoperability and product compatibility information, see the [Compatibility Matrices for vSphere Replication 8.8.x](#).

Installation

Download the vSphere Replication **.iso** image and mount it. You can deploy the vSphere Replication appliance by using the Deploy OVF wizard in the vSphere Web Client. Navigate to the *bin* directory in the **.iso** image and use the corresponding OVF file:

1. **vSphere_Replication_OVF10.ovf**: Use this file to install all vSphere Replication components, including the vSphere Replication Management Server and a vSphere Replication Server.
2. **vSphere_Replication_AddOn_OVF10.ovf**: Use this file to install an optional additional vSphere Replication Server.

For more information on the installation, see the section Installing vSphere Replication in the [vSphere Replication Documentation Center](#).

For vCenter Server to vCenter Server replications, the version of the vSphere Replication Management server on the source and the target site can be 8.7 or 8.8.

vSphere Replication 8.8 requires a supported vCenter Server version on both the source site and the target site. For more information, see [VMware Product Interoperability Matrices](#).

Upgrading vSphere Replication

You use the ISO file and the VRMS Appliance Management Interface to upgrade from vSphere Replication 8.6.x or 8.7.x to vSphere Replication 8.8.

You cannot upgrade vSphere Replication from versions earlier than 8.6 to version 8.8 by using the Virtual Appliance Management Interface (VAMI). See the [compatibility matrices](#) for further information on supported versions.

Important: Before you initiate an upgrade, verify that the vSphere Replication appliance has an OVF environment, or context. See [Checking and Restoring the OVF Context of the vSphere Replication Appliance \(2106709\)](#).

Verify that you read the Upgrade and General sections under Known Issues.

See [Upgrade Additional vSphere Replication Servers](#) and [Upgrade the vSphere Replication Appliance](#) for the procedures on upgrading to vSphere Replication 8.8.

Notes:

- After upgrading vSphere Replication, the ESXi hosts automatically enter and exit maintenance mode. See [KB 389735](#).
- When you use vSphere Replication with Site Recovery Manager, upgrade vSphere Replication on both of the protected and the recovery sites before you upgrade the Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. For more information, see the *VMware Site Recovery Manager Documentation*.

Operational Limits of vSphere Replication

The operational limits of vSphere Replication 8.8 are documented in the VMware Knowledge Base. See [Operational Limits for vSphere Replication 8.x \(KB 2102453\)](#).

Note: vSphere Replication requires additional configuration to support more than 500 replications per a vSphere Replication Management server. See [Operational Limits for vSphere Replication 8.x](#) and [Configuring Upgraded vSphere Replication Appliances to Support up to 4000 Replications](#).

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in vSphere Replication 8.8 are available at the [vSphere Replication Open Source Disclosure](#) page.

Caveats and Limitations

To ensure successful virtual machine replication, you must verify that your virtual infrastructure respects certain limits before you start the replication.

- In a federated environment with linked vCenter Server instances, when you log in to the REST API gateway local site this will automatically log you in to the remote site. You do not have to make a POST /remote-session request. It is not possible to log in to the remote site with a different user name.
- The hms-db-max-connections property value is automatically updated from 99 to 149 during the upgrade to vSphere Replication 8.8. To preserve a custom value, you must change it manually after the upgrade.
- vSphere Replication 8.8 does not provide support for Federal Information Processing Standards (FIPS).
- Resizing a replicated disk of a virtual machine by non-multiple of 512 bytes is not supported. If the disk is resized by non-multiple of 512 bytes, the replication fails. To return to the OK state, the disk size must be set to a multiple of 512 bytes.
- vSphere Replication does not support the protection of virtual machines that have persistent memory (PMem) devices or PMem disks. vSphere Replication does not support configuring replication as a source or a target on a PMem datastore.
- vSphere Replication will stop working correctly if you run the vSphere [Prevent Guest Operating System Processes from Sending Configuration Messages to the Host](#) procedure on the vSphere Replication Appliance.
- vSphere Replication does not support single virtual machine protection with two replication technologies. If a virtual machine is protected with VMware Cloud Disaster Recovery, it cannot be protected with vSphere Replication.

- vSphere Replication 8.8 does not provide support bundle management in the VRMS Appliance Management Interface. This includes lists with support bundles and deleting support bundles. To manage the support bundles through SSH, establish an SSH connection to the vSphere Replication Appliance.
- The 5 minute RPO scales to a maximum supported limit of 50 VMs on a provisional vVol datastore.
- vSphere Replication does not support VSS quiescing on Virtual Volumes.
- vSphere Replication cannot replicate virtual machines that share vmdk files.
- vSphere Replication does not support vSphere APIs for IO Filtering on both the source and the target sites. You cannot replicate a virtual machine that is assigned a VM Storage Policy that contains IOFilters, nor can you assign such a policy to the replication target VM. Before configuring a virtual machine for replication, verify that the VM Storage Policy that is assigned to it does not contain IOFilters. Do not assign VM Storage policies with IOFilters to virtual machines that are already configured for replication.
- Deploying more than one vSphere Replication appliance produces a warning during the initial configuration process in the VRMS Appliance Management Interface. This requires user confirmation to proceed with the new appliance. This situation does not occur when deploying more than one vSphere Replication servers.
- Each vSphere Replication Management Server can manage a maximum of 4000 replicated virtual machines. See [Configuring Upgraded vSphere Replication Appliances to Support up to 4000 Replications \(KB 2102463\)](#) and [Requirements to the Environment... \(KB 2107869\)](#).
- vSphere Replication supports a maximum disk size of 62TB. If you attempt to activate replication on a virtual machine with a disk larger than 62TB, the virtual machine will not perform any replication operation and will not power on.
- vSphere Replication tracks larger blocks on disks over 2TB. Replication performance on a disk over 2TB might be different than replication performance on a disk under 2TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.
- vSphere Replication does not support upgrading the VMware Tools package in the vSphere Replication appliance.
- vSphere Replication supports replicating RDMs in Virtual Compatibility Mode. RDMs in Physical Compatibility Mode cannot be configured for replication.
- vSphere Replication does not replicate virtual machine snapshot hierarchy at the target site.
- You can configure virtual machines that are powered off for replication. However, actual replication traffic begins when the virtual machine is powered on.
- When using Storage DRS at a replication site, ensure that you have homogeneous host and datastore connectivity to prevent Storage DRS from performing resource consuming cross-host moves (changing both the host and the datastore) of replica disks.
- vSphere Replication does not support VMware vSphere® Trust Authority™. vSphere Replication supports Standard Key Provider and VMware vSphere® Native Key Provider™.
- When using the TRIM/UNMAP commands to reclaim space, if the UNMAP command is used at the source site, the replication traffic sends the command as a large stream of zeroes, unless compression is used on the replication. The data is stored as zeroes at the target site and space on the replica disks is not reclaimed.

Known Issues

Upgrade

Upgrade to vSphere Replication 8.8 fails with an error

When you attempt to perform a chain upgrade from an earlier version of vSphere Replication, for example from version 8.3 to version 8.8, the upgrade might fail with an error: `Operation Failed: Failed to install update.`

The logs located in `/opt/vmware/var/log/vami/updatecli.log` show the following:

```
Error: Failed to synchronize cache for repo 'VMware Photon Linux 3.0 (x86_64)' from
'https://packages.vmware.com/photon/3.0/photon_release_3.0_x86_64'1. package xml-security-
```

c-1.7.3-4.ph2.x86_64 requires libcrypto.so.1.0.0()(64bit), but none of the providers can be installed.

The previous upgrades from Photon 2.0 to Photon 3.0 did not clean the packages properly causing the error in the upgrade procedure.

Workaround: Before performing the upgrade check whether package `xml-security-c` exist. If the package exists, remove it.

1. Revert the appliance before the update begins.
2. Check if the `xml-security-c` package exist. Run the following command `rpm -qa | grep ph2`.

The output will be similar to this:

```
xml-security-c-1.7.3-4.ph2.x86_64
xerces-c-3.2.1-1.ph2.x86_64
openjre8-1.8.0.232-1.ph2.x86_64
libarchive-3.3.1-5.ph2.x86_64
apache-ant-1.10.1-7.ph2.noarch
libdnet-1.11-5.ph2.x86_64
```

3. To remove the `xml-security-c` package, run the following command `rpm -e xml-security-c-1.7.3-4.ph2.x86_64`.
4. Continue with the upgrade of the appliance.

The vSphere Replication Management service does not start after the upgrade

After you upgrade vSphere Replication, the vSphere Replication Management (VRM) service appears as stopped in the VAMI, and the `/opt/vmware/hms/logs/hms-configtool.log` file in the virtual appliance contains `java.net.ConnectException: Connection refused` error messages.

This problem is observed if the upgrade procedure of the embedded DB schema fails because the vPostgreSQL service was not fully started.

Workaround:

1. In the virtual appliance console, log in as the root user.
2. Run the following command:


```
$ /opt/vmware/hms/bin/hms-configtool -cmd upgrade -configfile /opt/vmware/hms/conf/hms-configuration.xml
```

 The DB schema upgrade starts.
3. Wait for the DB upgrade procedure to complete.
4. In the vSphere Replication VAMI, navigate to the **Configuration** tab, and complete the SSO registration of the appliance.

Missing vSphere Replication permissions after upgrading the vSphere Replication appliance, certificate or IP change

If you upgrade the vSphere Replication appliance, or if for some other reason the certificate or the IP address of the vSphere Replication appliance changes, the permissions that are assigned to the default VRM user roles are deleted. This problem is observed every time the vSphere Replication extension is unregistered and registered with the vCenter Server extension manager.

Workaround: Clone the predefined VRM roles and create your custom roles before upgrading the vSphere Replication appliance, or changing its certificate or IP address. The permissions that are assigned to custom roles are not removed.

General

vSphere Replication alarms are not visible in the alarm definitions

vSphere Replication events might not be visible when adding an alarm definition in vCenter Server 8.0 and vCenter Server 8.0 Update 1.

Workaround: Upgrade your vCenter Server instance to vCenter Server 8.0 Update 2.

DR REST API v.8.8. hits DR server session limit exceeded

A bug in the DR REST API v.8.8 Rate Limiter tier *Session* prevents the DR server session to auto-close after a preconfigured timeout interval. The DR REST API client maintains a high number of DR sessions which results in exhaustion of the maximum possible number of DR server live sessions.

Workaround: Switch off the DR REST API Rate Limiter tier *Session* by performing the following steps.

1. Navigate to `/opt/vmware/dr-rest/webapps/rest/WEB-INF/web.xml` and comment out the following section.

```
<!--
<filter>
  <filter-name>SessionRateLimitFilter</filter-name>
  <filter-class>com.vmware.dr.restapi.infrastructure.rateLimit.SessionRateLimitFilter</filter-class>
  <async-supported>true</async-supported>
</filter>
-->
...
<!--
<filter-mapping>
  <filter-name>SessionRateLimitFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2. To close all live sessions, restart the DR service.
3. Restart the DR REST API service to switch off the DR REST API Rate Limiter tier *Session*.
4. Apply the workaround on all DR REST API instances of the server ecosystem.

After reconfiguring a replication to a vSAN ESA datastore, the replication gets stuck and cannot proceed

Due to changes in ESXi version 8.0 Update 2 that affect the vSphere Replication Appliance 8.8, moving a replication to a target vSAN ESA datastore, regardless of the type of the source datastore, will cause the replication to get stuck as the disk hierarchy at the new location will become read-only. Any further write operations to these disks, coming from the source site of the replication, will fail.

Workaround: Reconfigure the replication back to its original place or move it to a different datastore which is not vSAN ESA.

Planned migration and failover might fail with an error during the power on operation

When performing a planned migration or test failover at 4000 scale, the operation might fail with the following error while powering on the virtual machine: "Unable to write VMX file: /vmfs/volumes/...vmx".

Workaround: Rerun the failed recovery plan.

Changing the storage policy of a replication fails for an encrypted VM when the target datastore is vSAN or vSAN ESA

If a replication uses a storage policy with vSAN storage attributes and virtual machine encryption, and then the replication is reconfigured to a storage policy without the vSAN storage attributes, the replication gets into an error state with the following message: 'Cannot apply policy to vSAN object <id> (status: 'failed'), fault: InvalidArgument, message: Non vSAN Profile'. This might happen in the workflows of configuring a replication with seeds, reversing a replication during a reprotect operation, or changing the storage policy during reconfigure replication.

Workaround: Change the attributes of the new storage policy to use vSAN attributes.

Continuous HBR Agent VIB install errors in the vCenter Server tasks after upgrade

After upgrading vCenter Server, if there are ESXi hosts in the inventory that are not managed by vSphere Lifecycle Manager, you might observe HBR Agent VIB install errors in the vCenter Server tasks view.

Workaround: Reconfigure the vSphere Replication Management Server.

Failover or planned migration might fail due to storage errors

At 4000 scale on the target datastore, the test failover or planned migration might fail with the following error: "Cannot create a failover image for group <GID> on vSphere Replication Server <server>. A problem occurred with the storage on datastore path <path>".

Workaround: None.

Planned migration fails with an error

If you trigger a replication sync, the replication might fail with the following error due to connectivity issues: "VR synchronization failed for VRM group 'VM Name'. A general system error occurred: VM has no replication group". Even though this might be a sporadic issue, the replication might not get back to an OK status automatically.

Workaround: Reconfigure the replication of all the failed virtual machines.

Custom hms-db-max-connections property value is not preserved after vSphere Replication upgrade to version 8.8

hms-db-max-connections property value is automatically updated in hms-configuration.xml during the upgrade to vSphere Replication 8.8. The value is changed from 99 to 149. The previously set custom value for this property is overridden after the upgrade.

Workaround:

If you want to preserve your old hms-db-max-connections property value, you must set it manually:

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Open /opt/vmware/hms/conf/hms-configuration.xml file with any editor, modify the hms-db-max-connections property value and save the changes.
3. Restart the HMS Service in the VRMS Appliance Management Interface or by establishing an SSH connection to the vSphere Replication Appliance and running the `systemctl restart hms` command.

The replication keeps the last error even though the latest status is OK

The replication is in OK status, but the last error message "A replication error occurred at the vSphere Replication Server for replication <replication ID> "No connection to VR Server for virtual machine <vm name> on host <host IP> in cluster <cluster ID> in SDDC-Datacenter: Unknown " still exists on the Site Recovery user interface. This is because the events that provide the information that the replication is OK and that the error must be cleared are sent at the host level. As there are too many events in a short time, they are improperly filtered and therefore lost.

Workaround:

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab > **Advanced Settings** > **Edit Settings**.
3. On the source site, configure a key-value to enable the `config.vpxd.event.burstFilter.whiteList` option. Events that should be included in the allowlist are: `vim.event.UserLoginSessionEvent`; `vim.event.UserLogoutSessionEvent`; `hbr.primary.DeltaCompletedEvent`; `hbr.primary.NoConnectionToHbrServerEvent`; `hbr.primary.ConnectionRestoredToHbrServerEvent`

```
;hbr.primary.FSQuiescedDeltaCompletedEvent;hbr.primary.AppQuiescedDeltaCompletedEvent;
hbr.primary.UnquiescedDeltaCompletedEvent.
```

4. Restart the vmware-vpxd service for all changes to take effect.

Reprotect fails with the Unable to reverse replication for the virtual machine error

During a reverse replication, vSphere Replication prepares the source virtual machine by removing its snapshots and collapsing disks. This task might take longer than expected and vSphere Replication constructs a reverse replication spec using a child disk. The following error appears: `Unable to reverse replication for the virtual machine...`

Workaround: Retry the reprotect operation.

Reprotect from the vSAN datastore fails with an error

In rare cases, the vSphere Replication reprotect operation might fail with the error message `Unable to reverse replication for the virtual machine '<VM_name>'. Permission to perform this operation was denied when attempting to create a seeds directory on a vSAN datastore.`

Workaround:

1. Restart the management services on the designated host and retry the reprotect operations. See [Restarting the Management agents in ESXi \(KB 1003490\)](#).
2. Reboot the host if needed and retry the reprotect operations.
3. Unconfigure and configure replications on the failing virtual machines if needed.

Replication reconfiguration attempts fail with a TaskInProgress fault

You might encounter a situation where a snapshot is created due to the enabled quiescing feature. If a reconfiguration attempt is made, it internally invokes the vim.HbrManager API, which might result in a TaskInProgress exception if a snapshot creation is still in progress.

Workaround: Retry the reconfiguration operation.

Moving seed replica disks from different datastores into one datastore fails

When you try to move seed replica disks with identical names from different datastores into one datastore, the process fails. Seed replica disks with the same names cannot exist in the same location.

Workaround: Rename the seed replica disks before the move.

An unexpected error appears in the Summary tab if you have a second NIC, configured with a static route set

If you have a second NIC and if you configured a static route set for it, the VRMS Appliance Management Interface cannot obtain an IP address from the second NIC. This might result in the following unexpected error in the IP Address for Incoming Storage Traffic field, under the Summary tab:

```
The Storage Traffic IP address <IP_address> must match one of the NIC IP addresses .
```

Workaround: The NIC is correctly configured and you can discard the error. You can verify if the replication traffic uses the correct IP address by running the following command: `cat /etc/vmware/hbrsrv-nic.xml`.

When you modify the VM disks configuration, the replication goes into an Error state

When a VM is part of an ongoing replication, and you modify the VM storage configuration (add, delete, or resize disks), this action starts a replication reconfiguration task. If another reconfiguration operation is already in progress on this replication, the replication might fall into an Error state with an error. For example, `"Invalid configuration spec. Some disks are not specified for replication, nor excluded."` error.

Workaround: Manually reconfigure the replication.

If you reconfigure a replication to assign a new storage policy to replicated virtual disks that are not targeted to a vSAN target datastore, the policy is not applied to the replica disks at the target site

The storage policy is applied to the replica disks at the target site at the time you first configure or recover a replication. If you reconfigure the replication with a new storage policy, and the replicated virtual disks are not targeted to a vSAN target datastore, the change is not automatically reflected in the pair site.

Workaround:

1. Recover the virtual machines with reconfigured replication.
2. By using the vSphere Client, change the storage policy of the recovered virtual machines to the new policy.
3. Unregister the recovered virtual machines from the vCenter Server inventory.
4. Configure replication again by using seeds and with the new storage policy.

A replicated VM becomes unresponsive or cannot serve network requests

During a vSphere Replication sync operation, the VM disk I/O blocks for the duration of the sync. The vSphere Replication filter driver fails the SCSI UNMAP commands during a sync operation, if these commands override the transfer of the current replica disk to the target site.

Workaround: Allow vSphere Replication to accommodate the UNMAP commands.

1. Establish an SSH connection to the source ESXi Server.
2. Run the following command:

```
esxcli system settings advanced set -o /HBR/DemandlogFailCollidingUnmap -i 0
```

The command takes immediate effect and you don't need to perform a system reboot.

Reprotect fails with an error

When you are replicating virtual machines at a large scale, reprotect might fail with the following error:

```
"Unable to reverse replication for the virtual machine A generic error occurred in the vSphere Replication Management Server "java.net.SocketTimeoutException: Read timed out"
```

Workaround:

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Run the following command:

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-default-vlsi-client-timeout=15
```

3. Restart the HMS service.

The replication goes into Error state when you both remove and add disks to the source VM.

Auto include new disks option is activated. If you edit the settings of the VM and both remove one of the disks and add a new disk in a single task, the replication might go into Error state.

Workaround 1: Reconfigure the replication manually in the Site Recovery UI.

Workaround 2: When you modify the VM, add and remove new disks with two separated tasks

Automatic replication does not start when a disk is replaced on the same SCSI device

Auto replication new disks is activated. When in a single step you both remove and add protected disk on the same SCSI device, the replication goes into an Error state:

```
The set of disks on the vSphere Replication Server does not match the source set for replication '<vm name>'.
```

Workaround 1: Replace disk with two separated configuration operations.

Workaround 2: If you replaced the disk on the SCSI device with a single configuration operation, reconfigure the replication.

If you try to run a sync operation after disk resizing, the operation fails.

If you perform disk resizing, depending on the size of the disk, the operation might take up to a few hours. When you try to run a sync operation in the meantime, the operation fails, even if the replication is in OK state.

Workaround: Wait for the disk resizing operation to complete. You can verify the completion by checking the `/var/log/vmware/hbrsrv.log` log file, where you should be able to see this entry:

```
Resizing disk <replicated disk ID>
```

The recovery of a replication of a VM, encrypted with vSphere Native Key Provider, fails

If you remove from the cluster, which is configured with Native Key Provider, all hosts to which the target datastore is attached, the existing replications remain in OK state. However, if you try to perform a recovery, the recovery fails and the replication goes into Error state.

Workaround: Make the datastore accessible in the cluster again. If you did not attempted recovery and the replication is still in OK state, reconfigure the replication and change the target datastore to a datastore, which is accessible in the cluster.

Newly added virtual disk is not replicated upon reprotect operation

If you perform recovery and add a new disk to the recovered VM, the new disk is not replicated upon reprotect operation. The new disk is not automatically replicated if the initial replication was configured to automatically replicate new disks either.

Workaround: Manually include the new disk to the replication.

Recovery operation does not progress

If, within a short period of time, you exclude a virtual disk with a vVOL target datastore from the replication, and then include it again, this might affect a subsequent recovery operation. If you attempt to perform the recovery, it might not progress.

Workaround 1

If you already started the recovery operation:

1. Remove the replication, retaining the replica disks.
2. Configure the replication again, using seeds.
3. Perform recovery.

Workaround 2:

If you have not yet started the recovery operation:

1. Exclude the disk with a vVOL target datastore.
2. Sync the replication.
3. Include the disk again.
4. Perform recovery.

Replication sync does not progress

If, within a short period of time, you exclude a virtual disk with a vVOL target datastore from the replication, and then include it again, this might affect a subsequent replication sync operation. If you attempt to perform a replication sync, it might not progress.

Workaround:

1. Exclude the disk with a vVOL target datastore.
2. Sync the replication.
3. Include the disk again.

When you attempt to configure IPv6 through the VMware VRMS Appliance Management you receive an invalid property - dns error

When you attempt to configure IPv6 through the VMware VRMS Appliance Management and select the 'Obtain IPv6 settings automatically through router advertisement' option with auto assigned dns, the following error occurs invalid property - dns.

Workaround:

SSH to the vSphere Replication Appliance host machine and run `$netmgr ip6_address --set --interface --dhcp 0 --autoconf 1.`

To receive an IP address through DHCP run `$netmgr ip6_address --set --interface --dhcp 1 --autoconf 1.`

You cannot reconfigure the IPv6 settings through the VMware VRMS Appliance Management

If you have configured the IPv6 network with the 'Obtain IPv6 settings automatically through router advertisement' or 'Obtain IPv6 settings automatically through DHCP' option, you are unable to reconfigure the IPv6 settings with only 'Obtain IPv6 settings automatically through DHCP'. Either both options must be selected or none of them.

Workaround:

SSH to the vSphere Replication Appliance host machine and run `$netmgr ip6_address --set --interface --dhcp 0 --autoconf 1.`

To receive an IP address through DHCP run `$netmgr ip6_address --set --interface --dhcp 1 --autoconf 1.`

Reconfiguring a replication fails after removing and then adding the same disk to a different Virtual Device Node on the source VM

If you remove a virtual disk and add a new one with the same VMDK file, and then you try to perform a manual or an automatic (if you activated the Auto include new disks option) reconfiguration of the replication, the process fails with the following error:

```
Cannot reconfigure replication group '<VM_ID>' (managed object ID: 'GID-<group-ID>').
Details: 'Duplicate key (hms.Disk) { dynamicType = null, dynamicProperty = null,
deviceKey = <DEVICE_KEY>, destination = (hms.ExtendedDatastorePath) { dynamicType
= null, dynamicProperty = null, datastore = MoRef: type = Datastore, value =
<DATASTORE>, serverGuid = null, path = <PATH>, fileName = <FILENAME>, dsCluster =
null }, storageProfileId = null, useOfflineCopy = false, virtualDiskType = thin,
skipDiskUuidValidation = true, replicationDiskId = null, contentId = null, capacityInKb =
<CAPACITY> }'. ThrowableProxy.cause The operation is not allowed in the current state.
```

Workaround

1. Stop the replication and preserve the replica disks.
2. Configure the replication again by using the disks as seeds.

Configuring replication fails after switching from vSphere Trust Authority to KMS as an encryption mechanism

If you are using vSphere Trust Authority as an encryption mechanism, but switch back to the old encryption mechanism using KMS servers, and then try to configure a replication, the process might fail. The problem is observed, because the encryption keys might not be properly distributed to the target hosts, after switching the encryption mechanisms.

Workaround: Restart the HMS service.

Test recovery fails with an error

If you configure a replication to a VMFS datastore and then reconfigure any disk of this group to be replicated to a vSAN datastore (while the VM home is still configured to a VMFS datastore), when you try to perform a test recovery, it fails with the following error:

```
Cannot create a test bubble image for group '<group-ID>' on vSphere Replication Server...
```

Workaround 1: Reconfigure all replica disks back to using a VMFS datastore.

Workaround 2: Reconfigure the VM home to be replicated to a vSAN datastore.

When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovery UI is blocked without notification in Mozilla Firefox browser

By default the Site Recovery UI opens in a new tab. When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovery UI is blocked without notification in Mozilla Firefox browser.

Workaround: From the Options menu in Mozilla Firefox, select the Content tab and add the URL of the vCenter Server to the Pop-ups exception list.

Configuring a replication that uses seeds on a vVol target datastore succeeds, but the replication is in Error state

If you configure a replication to use as a seed a VM that has snapshots, the configure operation succeeds, but the replication goes into the **Error** state at the end of the **Initial Full Sync**. An issue with a similar error description appears:

```
A replication error occurred at the vSphere Replication Server for replication 'vmname'.
Details: 'Error for (datastoreUUID: "vvol:9148a6192d0349de-94149524b5f52bc4"), (diskId:
"RDID-fd3ed4de-2356-43c7-a0e2-7bc07a7da012"), (hostId: "host-33"), (pathname: "vmname/
vmname.vmdk"), (flags: retrieable): Class: NFC Code: 10; NFC error: NFC_DISKLIB_ERROR
(Input/output error); Set error flag: retrieable; Can't write (multiEx) to remote disk;
Can't write (multi) to remote disk'.
```

Workaround: Delete the snapshots from the seed VM.

During full synchronization vSphere Replication fails with error: A replication error occurred at the vSphere Replication Server

During full synchronization vSphere Replication might fail with the following error.

```
A replication error occurred at the vSphere Replication Server for replication
<group_name>. Details: 'Error for (datastoreUUID: "..."), (diskId: "..."), (hostId:
"..."), (pathname: "..."), (flags: retrieable, pick-new-host, nfc-no-memory): Class: NFC
Code: 5; NFC error: NFC_NO_MEMORY; Set error flag: nfc-no-memory; Code set to: Host unable
to process request.; Set error flag: retrieable; Set error flag: pick-new-host; Can't write
(single) to remote disk'.
```

Usually, this error is transient and the operation succeeds after some time.

Replacing the SSL certificate of vCenter Server causes certificate validation errors in vSphere Replication

If you replace the SSL certificate on the vCenter Server system, a connection error occurs when vSphere Replication attempts to connect to vCenter Server.

Workaround: For information about how to update vCenter Server certificates and allow solutions such as vSphere Replication to continue to function, see <http://kb.vmware.com/kb/2109074>.

Data synchronization fails and the log file of the source vSphere Replication Management Server contains error `DeltaAbortedException`

If your environment experiences connectivity issues during data synchronization, you might observe the following problems.

- Replication group synchronizations fail and the `hms<n>.log` file in the vSphere Replication Management server at the source site contains the following error message:
`DeltaAbortedException.`
- In Site Recovery Manager, replication group synchronizations fail with the following error message:
`VR synchronization failed for VRM group <group_name>. A generic error occurred in the vSphere Replication Management Server. Exception details: 'com.vmware.hms.replication.sync.DeltaAbortedException'.`

Workaround: Resolve the connectivity issues in your environment before you proceed.

Failover with "Sync latest changes" might fail with `SocketTimeoutException` when multiple replications are recovered concurrently and there is a huge accumulated delta since the latest synchronization

The vSphere Replication Management server might not receive due responses through the vCenter reverse proxy when there is heavy replication traffic at the same network. Some replication management or monitoring operations might fail with the following error message:

```
com.vmware.vim.vmomi.client.exception.ConnectionException:
java.net.SocketTimeoutException: Read timed out
```

Workaround: Configure network traffic isolation for vSphere Replication traffic, so that the management communication between vCenter and the vSphere Replication Management server is not affected by the heavy replication traffic. See [Isolating the Network Traffic of vSphere Replication](#).

Replications appear in Not Active (RPO violation) status after changing the IP address of the vSphere Replication server at the target site

If the IP address of the vSphere Replication server at the target site changes, the status of all replications to this site turns to Not Active (RPO violation). This problem is observed because replications on the source site are not reconfigured automatically when the IP address changes.

Workaround: Reconfigure all replications, so that the source hosts use the new IP address of the target vSphere Replication server.

Transient Error state during the initial full synchronization

During the initial synchronization, you might observe that the state of the synchronization changes temporarily to **Error** and back to normal multiple times. The error state might indicate resource deficiency at the target site. If the IO workload caused by the sync operation is higher than the load that target hosts can handle, the state of the replication will turn to **Error**. When the IO workload decreases, the error disappears.

Workaround: Reduce the value of the host configuration option called **HBR.TransferMaxContExtents** on each ESXi host where replication source VMs are running. The default value is 8, and a lower value decreases the size of data blocks that are sent during one sync update, but increases the duration of the initial full sync. After the initial full sync, change the value back to its default (**8**) to achieve maximum RPO performance. If transient errors continue to appear during delta synchronizations, it might mean that a lot of changed blocks are transferred during each delta, and the hosts at the target site cannot accommodate the incurred IO workload. In such cases, keep the value of the **HBR.TransferMaxContExtents** configuration option low. Alternatively, you can add more hosts to the secondary site.

Users that are assigned the VRM administrator or VRM virtual machine replication role cannot access the Configure Replication wizard

The Configure Replication wizard is not launched if a user that is assigned the predefined VRM administrator or VRM virtual machine replication role logs in the Site Recovery user interface and attempts to configure a replication.

Workaround: Clone the default role to add the **Profile-driven storage -> Profile-driven storage view** privilege to it, and assign the cloned role to the user.

The option to activate quiescing is deactivated in Configure Replication wizard for a powered off replication source VM, though the guest OS supports quiescing

For both Linux and Windows sources, the Enable Quiescing option is activated based on the information about the guest OS. If a virtual machine has never been powered on, ESXi hosts always report no support for quiescing, because the guest OS information is not available.

Workaround: Verify that replication source VMs have been powered on at least once before you configure replications.

vSphere Replication service is inaccessible after vCenter Server certificate changes

If the vCenter Server certificate changes, vSphere Replication becomes inaccessible.

Workaround: See [vSphere Replication is Inaccessible After Changing vCenter Server Certificate](#).

vSphere Replication Management Server (VRMS) might leak a partially recovered virtual machine in the target vCenter Server after a failed recovery

In rare cases VRMS might stop during recovery immediately after registering the recovered virtual machine in the target vCenter Server. The last recovery error in the replication details panel says **VRM Server was unable to complete the operation**. When VRMS restarts, it cleans up the files for the partially recovered virtual machine. In some cases, it fails to unregister the virtual machine from the target vCenter Server. Subsequent recovery attempts show an error in the recovery wizard that the selected virtual machine folder already contains an entity with the same name.

Workaround: Manually remove the virtual machine from the target vCenter Server, but keep its disks as they point to the replica placeholder files.

A virtual machine recovered in vSphere Replication does not power on in vCenter Server

When you use vSphere Replication to run a recovery on a virtual machine, it fails, and the status of the replication is not 'Recovered'. The virtual machine is registered in the vCenter inventory, but when you try to power it on, it fails with error: `File [datastorename] path/vmname.vmx was not found.`

The virtual machine registration as part of the vSphere Replication recovery workflow can succeed in vCenter Server, but the response might not reach the vSphere Replication Management Server due to a transient network error. vSphere Replication reverts the replication image and reports a failed recovery task due to virtual machine registration error. If you initiate another recovery, it fails with a message that a virtual machine with the same name is already registered in vCenter Server.

Workaround: Remove the partially recovered virtual machine from the vCenter Server inventory. Do not delete the files from disk. Try the recovery again.

During replication of multiple virtual machines, a vSphere Replication server might enter a state where it does not accept any further VRMS connections but continues to replicate virtual machines

Workaround: Reboot the vSphere Replication server.

vSphere Replication operations fail with a Not Authenticated error

If you start an operation on one site, for example configuring vSphere Replication on a virtual machine, and then restart vCenter Server and the vSphere Replication appliance on the other site, vSphere Replication operations can fail with the error `VRM Server generic error`. Please check the documentation for any troubleshooting information. The detailed exception is: `'com.vmware.vim.binding.vim.fault.NotAuthenticated'`.

This problem is caused by the fact that the vSphere Replication server retains in its cache the connection session from before you restarted vCenter Server and the vSphere Replication appliance.

Workaround: Clear the vSphere Replication connection cache by logging out of the vSphere Web Client and logging back in again.

Operation in vSphere Replication Management Server fails with error "... UnmarshalException"

When the vSphere Replication Management Server experiences high load or transient network errors, operations can fail with `UnmarshalException` due to errors in the communication layer.

Workaround: Try the failed operation again.

vSphere Replication operations fail when there is heavy replication traffic

vSphere Replication operations might fail with error `java.net.UnknownHostException`. These errors occur because DNS requests are dropped due to network congestion.

Workaround: Configure your network to ensure that management traffic is not dropped, by configuring traffic shaping, quality of service, or DNS on the vSphere Replication appliance. One possible solution is to modify the network address caching policy for the vSphere Replication appliance.

1. Log into the vSphere Replication appliance as root.
2. Open the file `/usr/java/jre-vmware/lib/security/java.security` in an editor.
3. Uncomment the line `networkaddress.cache.ttl` and set its value to at least 86400 seconds (24 hours) or to the longest time that is required for an initial full sync to complete.
4. Save the file and reboot the vSphere Replication appliance.
5. Repeat the procedure for all remaining vSphere Replication appliances.

Replications to vCenter Server

You cannot move a replication to another server

If you run vSphere Replication 8.7 on your local site and vSphere Replication 8.6 on your remote site, and you try to move a replication to a different server, the process fails with the following error:

```
Cannot complete the operation due to an incorrect request to the server
```

Workaround 1: When you are moving the replication, specify a target replication server in reconfigure wizard.

Workaround 2: Upgrade the target site to the same version as the local site.

Configure and reconfigure replication processes fail with an error

When you try to configure or reconfigure a replication with seed disks, a vSAN target datastore and a VM Encryption Policy storage policy, the process fails with an error:

```
A generic error occurred in the vSphere Replication Management Server. Exception details:
Cannot apply policy to vSAN object 'xxx' (status: 'failed', fault: InvalidArgument,
message: Non vSAN Profile)
```

This error occurs because it is not possible to apply storage profiles without at least one vSAN rule to vSAN objects.

Workaround 1: Use a predefined storage policy, for example Management Storage policy - Encryption.

Workaround 2: Create a custom storage policy that contains at least one vSAN rule.

Configuring a replication to a newly registered VM fails with an error

If after performing a successful failover, you remove the recovered VM and then re-register it, when you attempt to configure a replication for this VM, the process fails with the following error:

VM '<VM_ID>' was recovered in optimized reprotect mode in another replication group. To configure new replication for the VM, you must first remove the existing recovered replication.

Workaround: Deactivate vSphere Replication on this VM. See <https://kb.vmware.com/s/article/2106946>.

You cannot encrypt an unencrypted source VM in an active replication

If you try to encrypt an unencrypted virtual machine in an active replication configuration, the encryption fails.

Workaround: Recover the unencrypted virtual machine and configure a new replication with encrypted seed disks.

1. Recover the VM on the remote site, but do not power the VM on.
2. Remove the replication of the source VM.
3. Edit the settings of the VM on the target site and change the VM storage policy to VM Encryption Policy.
4. Edit the settings of the source VM on the source site and change the VM storage policy to VM Encryption Policy.
5. Unregister the recovered virtual machine on the target site, but do not delete the disks.
6. Configure a new replication and select the disks of the recovered VM on the target site as seeds.

A recovered virtual machine with multiple point-in-time instances enabled can lose the attached disks to the latest snapshot when you revert to a previous snapshot and then revert to latest snapshot again

When you recover a virtual machine for which you enabled point-in-time instances and attach a disk for unresolved disks, if any, the disks attach to the latest snapshot. If you revert to a previous snapshot and then revert to the latest one, the attached disks are not available.

Workaround: Edit settings of the virtual machine and add the required disks as existing hard disks.

Recovering a virtual machine with vSphere Replication 8.8 fails to power on the recovered virtual machine

If a replicated virtual machine is attached to a distributed virtual switch and you attempt to perform a recovery in an automated DRS cluster, the recovery operation succeeds but the resulting virtual machine cannot be powered on.

Workaround: Edit the recovered virtual machine settings to attach it to the correct network.

Registering additional vSphere Replication servers takes a long time

If vCenter Server manages several hundred ESXi Server hosts, registering an additional vSphere Replication server with the vSphere Replication appliance can take several minutes. This is because the vSphere Replication server must register with each ESXi Server host.

VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Introduction to the VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8](#)
- [Installation](#)
- [Featured Workflows](#)
- [Caveats and Limitations](#)
- [Known Issues](#)
- [Known Issues from Previous Releases](#)

Introduction

vSphere Replication 8.8 | 21 SEP 2023 | Build 22436165 | [Download](#)

VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 | 21 SEP 2023 | Build 22458997 | [Download](#)

Check for additions and updates to these release notes.

What's New

- The VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 release provides support for VMware Aria Automation Orchestrator 8.12.2.

Introduction to the VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8

The VMware Aria Automation Orchestrator Plug-In for vSphere Replication allows VMware administrators to simplify the management of their vSphere Replication infrastructure by leveraging the robust workflow automation platform of VMware Aria Automation Orchestrator. The VMware Aria Automation Orchestrator Plug-In for vSphere Replication extends automation capabilities for certain vSphere Replication operations by including them in VMware Aria Automation Orchestrator workflows.

The plug-in also delivers pre-built out-of-the-box building blocks and complete workflows that cover certain existing vSphere Replication actions.

The VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 release runs with the latest version of VMware Aria Automation Orchestrator. For more information on interoperability with earlier or later releases of VMware Aria Automation Orchestrator, see the [VMware Product Interoperability Matrices](#).

You can download the VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 from the [download](#) page.

For information about creating workflows by using VMware Aria Automation Orchestrator, see the [VMware Aria Automation Orchestrator documentation](#).

For more information on the supported workflows, see the Featured Workflows section.

For more information on the compatibility between the VMware VMware Aria Automation Orchestrator Plug-In for vSphere Replication and VMware Aria Automation Orchestrator Appliance, see the [compatibility matrix](#).

Installation

The VMware Aria Automation Orchestrator Plug-In for vSphere Replication software requires VMware vRealize Orchestrator 8.12.2, and vSphere Replication 8.8. For information on installing VMware Aria Automation Orchestrator, see the [VMware Aria Automation Orchestrator documentation](#). For information on installing vSphere Replication 8.8, see [Installing and Setting Up vSphere Replication](#) in the VMware vSphere Replication documentation.

The VMware Aria Automation Orchestrator Plug-In for vSphere Replication software is distributed as a VMware Aria Automation Orchestrator application file. Install and configure the plug-in by using the VMware Aria Automation Orchestrator configuration interface.

After you install the VMware Aria Automation Orchestrator Plug-In for vSphere Replication, the plug-in automatically discovers the vSphere Replication instances on all vCenter Servers that are currently registered.

After you install the VMware Aria Automation Orchestrator Plug-In for vSphere Replication, you find the vSphere Replication workflows in the VMware Aria Automation Orchestrator UI:

1. Go to **Library > Workflows**
2. Search for the workflow by name or switch to tree view from the top right icon. In tree view you can find the workflows under **Library > vSphere Replication** folder.

Before you can run vSphere Replication workflows, which interact with remote sites, you must register the remote site, by running the corresponding workflow from **Library > vSphere Replication > Remote Site Management > Register VC Site**.

Note: The VMware Aria Automation Orchestrator user, which is used to register the vCenter Server sites in VMware Aria Automation Orchestrator must have the privilege **Sessions.ValidateSession** and the **VRM Administrator** role (or all the privileges of the VRM Administrator role). The user must have the privileges on all vCenter Server instances in the VMware Aria Automation Orchestrator inventory, otherwise the VMware Aria Automation Orchestrator Plug-In for vSphere Replication does not populate the vSphere Replication inventory objects in VMware Aria Automation Orchestrator.

Even if you want to configure replication to the same site, you must register it by selecting **self pair** in the Site field. Then, you must log in to the remote site by running the **Login to VC Site** workflow. You must run this workflow only once per VMware Aria Automation Orchestrator user.

Note: VMware Aria Automation Orchestrator communicates with the vSphere Replication appliance over port 8043.

Featured Workflows

The VMware Aria Automation Orchestrator plug-in provides out-of-the-box workflows to help customers automate vSphere Replication operations. Below are some of the implemented workflows.

- Remote Site Management workflows:
 - Log in to a vCenter Server site
- Configure Replication workflows:
 - Reconfigure Replication
- Pause Replication workflows
- Resume Replication workflows
- Stop Replication workflows
- Replication Details Workflows
 - Check Replication Status
 - Get Replication Configuration
 - Get Replication List

Caveats and Limitations

- The VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8 supports vRealize Orchestrator 8.10 and 8.11 with certain limitations. For more information, see the [Known Issues from Previous Releases](#) section.

Known Issues

You cannot directly upgrade from VMware Aria Automation Orchestrator Plug-In for vSphere Replication version 8.7 to version 8.8

When you try to upgrade the VMware Aria Automation Orchestrator Plug-In for vSphere Replication from version 8.7 to 8.8 from the configuration page of VMware Aria Automation Orchestrator 8.13.1, the upgrade fails.

Workaround 1: Remove VMware Aria Automation Orchestrator Plug-In for vSphere Replication version 8.7 and then install version 8.8.

Workaround 2: Upgrade VMware Aria Orchestrator to version 8.14.1.

Known Issues from Previous Releases

A NullPointerException appears in the reconfigure replication workflow

In some cases, a `NullPointerException` appears in the VMware Aria Automation Orchestrator user interface when you want to reconfigure replications with multiple disks and all disks are excluded from the replication. As a result, the datastores are not loaded.

Workaround: On the Disks page, select a storage profile from the drop-down menu. The datastores are loaded and you can submit the workflow.

You cannot select the same options twice for Disk format per disk, Storage profile per disk or Target datastore per disk, when running the Configure Replication or Reconfigure Replication workflows with the Per disk configuration option activated

When you run the **Configure Replication** or **Reconfigure Replication** workflows with the **Per disk configuration** option activated and you try to select options for the **Disk format per disk**, **Storage profile per disk** and **Target datastore per disk** arrays, you cannot select the same options twice and you get an error message.

Workaround 1: Use the **Configure Replication** or **Reconfigure Replication** workflows with the **Per disk configuration** options deactivated.

Workaround 2: Use the VMware Aria Automation Orchestrator scripting objects.

When you attempt to register a new vCenter Server instance, you receive an error in the vCenter Server plug-in

When you attempt to register a new vCenter Server instance, the operation fails because of a vmodl mismatch error: `(unusable: (vmodl.fault.InvalidType) { faultCause = null, faultMessage = null, argument = ImageLibraryManager })`. As a result, you are blocked from using the VMware Aria Automation Orchestrator plug-in for vSphere Replication 8.7 as it depends on the vCenter Server registration from the vCenter plug-in. The issue is present with the out-of-the-box vCenter Server plug-in that comes with vRealize Orchestrator versions 8.10.1, 8.10.2, 8.11, 8.11.1, and 8.11.2.

Workaround: Download and install the latest vCenter Server plug-in from the marketplace.

The vSphere Replication site is not shown in the inventory view when a new vCenter instance has been added to VMware Aria Automation Orchestrator.

Workaround: Restart the VMware Aria Automation Orchestrator Server service.

Executing any of the unregister workflows from Library > vSphere Replication > Remote Site Management does not terminate the already established connection to the target site.

Workaround: Restart the VMware Aria Automation Orchestrator Server service.

When registering vCloud Air as a Standalone Org or a Remote Cloud Site and "Ignore certificate warnings" is set to "No", the following warnings appear

1) Untrusted certificate, with certificate info:

```
Validity : [From : Apr 23, 2013 To : Apr 27, 2016]Organizational Unit :Public key :
RSAFingerprint (MD5) : 80 C1 77 2F 78 16 01 EB 9A 4B 88 E5 A3 E3 C0 29Organization :
VMware, Inc.Common Name (6 characters min) : *.vchs.vmware.comCountry : USSerial Number :
1B C3 C0 84Alternative names :[2, [2]*.vchs.vmware.com][2, [2]vchs.vmware.com]
```

2) Wrong site - saying that the certificate is issued to `*.vchs.vmware.com`

Workaround: Verify that the fingerprint is the same as the above, the validity is correct and continue with importing the certificate despite the warnings.

You might see an error in the vSphere Replication inventory of the VMware Aria Automation Orchestrator after replacing a vSphere Replication management server certificate at the local site of a pair

If for some reason you change the certificate of the vSphere Replication management server at the local site of a replication pair, you might not be able to see the pair in the vSphere Replication inventory of the VMware Aria Automation Orchestrator. You see an error similar to:

\Unable to execute 'fetchRelation' for type : Site : com.vmware.vim.vmomi.client.exception.SslException: com.vmware.vim.vmomi.core.exception.CertificateValidationException: Server certificate chain is not trusted and thumbprint doesn't match

Stale certificates in the VMware Aria Automation Orchestrator inventory cause the issue.

Workaround:

1. Restart the VMware Aria Automation Orchestrator server:
 - a. Launch a console to the virtual machine on which the VMware Aria Automation Orchestrator server is installed.
 - b. Log in to the console as root.
 - c. Run the command `service vco-server restart` to restart the VMware Aria Automation Orchestrator server.
2. Restart the VMware Aria Automation Orchestrator client. Wait for the validation to complete. You can monitor validation progress at this url pattern: `https://{your VMware Aria Automation Orchestrator server address}:8283/vco-controlcenter/config/#/control-app/validate`
3. In case the vSphere Replication management server is in a pair with another vSphere Replication management server, you must reconnect the pair.
4. In the VMware Aria Automation Orchestrator inventory, unregister the old server entries and register the new ones.

VMware Aria Operations Management Pack for vSphere Replication 8.8 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [About the VMware Aria Operations Management Pack for vSphere Replication 8.8](#)
- [Installation and Configuration](#)
- [Caveats and Limitations](#)
- [Network Port](#)
- [Known Issues from Previous Releases](#)

Introduction

vSphere Replication 8.8 | 21 SEP 2023 | Build 22436165 | [Download](#)

VMware Aria Operations Management Pack for vSphere Replication 8.8 | 21 SEP 2023 | Build 22458998 | [Download](#)

Check for additions and updates to these release notes.

What's New

The VMware Aria Operations Management Pack for vSphere Replication 8.8 provides the following new features:

- Support for VMware Aria Operations 8.12.1.
- Improvements in the VRMS server's certificate expiration information. When there are less than three days left for the certificate to expire, an alarm is triggered.

About the VMware Aria Operations Management Pack for vSphere Replication 8.8

The VMware Aria Operations Management Pack for vSphere Replication 8.8 allows VMware administrators to monitor the health and current status of their underlying vSphere Replication environment in VMware Aria Operations Manager. By using the VMware Aria Operations Management Pack for vSphere Replication 8.8, you can explore replication details per VM, such as direction of replication, replication status, and Recovery Point Objective (RPO) violations. You can also monitor replication metrics, such as transferred bytes, last instance sync points, last sync duration, and last sync size.

By using the pack, you get visibility on replication settings such as RPO, multiple points in time (MPIT), quiescing, and network compression. In addition, you see alarms when vSphere Replication health or a replication status is in Error state, or if there is an RPO violation. The VMware Aria Operations Management Pack for vSphere Replication 8.8 release runs with VMware Aria Operations 8.12.1. For more information on interoperability with earlier or later releases of VMware Aria Operations Manager, see the [VMware Product Interoperability Matrices](#).

You can download the VMware Aria Operations Management Pack for vSphere Replication 8.8 from the [download](#) page.

Installation and Configuration

The VMware Aria Operations Management Pack for vSphere Replication 8.8 software requires VMware Aria Operations 8.12.1, and vSphere Replication 8.8. For information about VMware Aria Operations 8.12.1, see the [VMware Aria Operations documentation](#). For information on installing vSphere Replication 8.8, see [Installing and Uninstalling vSphere Replication](#) in the VMware vSphere Replication documentation.

The VMware Aria Operations Management Pack for vSphere Replication 8.8 software is distributed as PAK file. You install and configure the management pack by using the VMware Aria Operations Manager interface.

1. Log in to VMware Aria Operations Manager.
2. Select **Data Sources > Integrations > Repository**.
3. Click **Add**.
4. Navigate to the **vrAdapterPak-8.8.pak** file and click **Upload**. When the PAK file is uploaded, click **Next**.
5. Read and agree to the end-user license agreement. Click **Next** to install the management pack.
6. Review the installation progress, and click **Finish** when the installation completes.

After the installation completes you must configure the VMware Aria Operations Management Pack for vSphere Replication 8.8 so that VMware Aria Operations Manager can collect data from the target system. The minimum role required to collect data is the **VRM replication viewer**. For more information on roles and permissions, see [vSphere Replication Roles and Permissions](#).

1. Select **Data Sources > Integrations > Accounts**.
2. Click **Add account**.
3. Select **vSphere Replication Adapter**.
4. Enter the required information and click **Add**.

Note: User name and password are case-sensitive.

Caveats and Limitations

- **Transferred bytes (MB)** metric for Virtual Machines displays data only for outgoing replications. Data for incoming replications is displayed at 0.
Transferred bytes (MB) metric for VRMS Site includes data only for outgoing replications.
- For the **RPO Violations Count**, **Transferred Bytes (per VM)** and **Transferred Bytes (per site)** metrics, the granularity of the statistical data depends on the **rrd-updater-interval** parameter. The parameter is defined in the `/opt/vmware/hms/conf/hms-configuration.xml` configuration file. This parameter controls the interval, at which the statistical data is saved. By default, the value is set to 5 minutes, but it can be changed if needed.

Network Port

VMware Aria Operations Management Pack for vSphere Replication uses port 8043 (protocol HTTPS) to connect to the vSphere Replication Management Server.

Known Issues from Previous Releases

Using the vRealize Operations administration page for upgrade of management packs is not supported

Installing updates from the Software Updates pane of the vRealize Operations administration page is not supported for management pack due to a known issue with not updating the visual elements. The issue is fixed in VMware Aria Operations 8.12.

Workaround: Use the standard vRealize Operations UI to upgrade the management pack.

1. From the left menu click **Data Sources>Integrations**, and then click the Repository tab.
2. On the Repository tab, click **Add/Upgrade**.

The Topology Graph widget does not load

If you are using the vRealize Operations Management pack for vSphere Replication with vRealize Operations 8.2 or later, when you open the dashboard for the vSphere Replication Summary, the Topology Graph widget does not load.

Workaround: This is an issue with the widget in vRealize Operations Manager 8.2 and later. Edit the widget without making any changes. That refreshes the widget and it will start working.

You cannot upgrade from vRealize Operations Management Pack for VMware vSphere Replication 8.2.0.1 or earlier

If you are using vRealize Operations 8.0 or later, the upgrade process from vRealize Operations Management Pack for VMware vSphere Replication 8.2.0.1 or earlier is not supported.

If you are using vRealize Operations 7.6 or earlier, the upgrade process from vRealize Operations Management Pack for VMware vSphere Replication 8.2 or earlier is not supported.

Workaround: Uninstall the vRealize Operations Management Pack for VMware vSphere Replication and install the latest supported version of the vRealize Operations Management Pack for VMware vSphere Replication.

Compatibility Matrices for vSphere Replication 8.8

This document contains the following sections

- [Introduction](#)
- [General Information](#)
- [vSphere Editions](#)
- [Upgrade Path](#)
- [Platform Components](#)
- [Interoperability with VMware Solutions](#)
- [Supported Database Software](#)
- [Guest Operating System Support](#)
- [Guest OS Quiescing Support](#)
- [Linux Quiescing Support](#)
- [Disclaimer](#)

Introduction

Compatibility Matrices for vSphere Replication 8.8

The *Compatibility Matrices for vSphere Replication 8.8* describe the compatibility between vSphere Replication 8.8 and platform components, VMware solutions, database software, and guest operating systems. Interoperability details for vSphere Replication can be found in the *VMware Product Interoperability Matrices*. The present pages describe how to use that tool to find the relevant information. Where the *VMware Product Interoperability Matrices* does not provide information relating to vSphere Replication, this information is listed here.

- [General Information](#)
- [Guest Operating System Support](#)
- [Guest OS Quiescing Support](#)

General Information

- [vSphere Editions](#)
- [Upgrade Path](#)
- [Platform Components](#)
- [Interoperability with VMware Solutions](#)
- [Supported Database Software](#)

vSphere Editions

The license for vSphere Replication 8.8 is included in the following editions of vSphere

vSphere Edition	vSphere Replication 8.8
vSphere Essentials	NO
vSphere Essentials Plus	YES
vSphere Standard	YES
vSphere Enterprise	YES
vSphere Enterprise Plus	YES
vSphere Desktop	YES

NOTE: The protection and recovery of encrypted virtual machines with vSphere Replication requires VMware vSphere 7.0 Update 2c or later for 7.0.x based versions.

Upgrade Path

You can upgrade existing installations of vSphere Replication 8.6.x and vSphere Replication 8.7.x to vSphere Replication 8.8.

For the most up to date supported upgrade paths for vSphere Replication, check the [VMware Product Interoperability Matrices](#).

1. Click **Upgrade Path**.
2. From the **Select a Solution** menu, select **VMware vSphere Replication**.

Platform Components

For the most up to date ESXi and vCenter Server interoperability, for vSphere Replication 8.8, check the [VMware Product Interoperability Matrices](#).

For the supported versions of vSAN, see [KB 2150753](#).

For vCenter Server to vCenter Server replications, the version of the vSphere Replication Management server on the source and the target site can be 8.7 or 8.8.

Interoperability with VMware Solutions

For the most up to date information on the interoperability of vSphere Replication with VMware solutions, check the [VMware Product Interoperability Matrices](#).

Supported Database Software

vSphere Replication 8.8 includes only an embedded vPostgreSQL database. vSphere Replication 8.8 does not support external databases.

Guest Operating System Support

vSphere Replication 8.8 supports the protection and recovery of virtual machines that run all of the guest operating systems that vSphere 7.0 and later versions support.

NOTE: If support for a guest operating system has been added in an update release of ESXi Server and vSphere Replication, to protect virtual machines that run those operating systems you must update ESXi Server to the corresponding update release as well as updating vSphere Replication. You must update ESXi Server on both the source and target sites.

For the full list of guest operating systems that vSphere 7.0 and later versions support, check the online [VMware Compatibility Guide](#).

1. Go to <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software>.
2. Select **Guest OS** from the drop-down menu.
3. For **Product Name** select **ESXi**.
4. For **Product Release Version** select **ESXi *n***, where *n* is a release of ESXi that vSphere 7.0 and above versions support.
5. To see all the supported versions of guest operating systems from an operating system vendor:
 - a. For **OS Family Name**, select **All**.
 - b. For **OS Vendor**, select the operating system vendor. For example, select **Red Hat**.
6. To check which updates of a particular operating system is supported:
 - a. For **OS Family Name**, select the operating system. For example, select **Red Hat Enterprise Linux 3.0**.
 - b. For **OS Vendor**, select **All**.
7. Click **Update and View Results**.

Guest OS Quiescing Support

VSS Quiescing Support

Microsoft Volume Shadow Copy Service (VSS) quiescing is supported for virtual machines running Windows Server 2003, XP, or later versions of Windows. vSphere Replication does not support quiescing for earlier versions of Windows, such as Windows 2000. The quiescing option is unavailable for unsupported operating systems.

NOTE: vSphere Replication 8.8 does not support VSS quiescing on vSphere Virtual Volumes.

When you enable quiescing, vSphere Replication first attempts application level quiescing. If application level quiescing fails, vSphere Replication attempts file-system level quiescing.

Operating System	Application Quiescing	File System Quiescing
Windows Server 2025	YES (ESXi 8.0.1 or later)	YES (ESXi 8.0.1 or later)
Windows 11	NO	NO
Windows 10	NO	YES
Windows 8.1	NO	YES
Windows Server 2022	YES (ESXi 8.0 or later)	YES (ESXi 8.0 or later)
Windows Server 2019	YES (ESXi 7.0.3 or later)	YES (ESXi 7.0.3 or later)
Windows Server 2016	YES	YES
Windows Server 2012 R2	YES*	YES
Windows Server 2012	YES*	YES
Windows 8	NO	YES
Windows 7	NO	YES
Windows Server 2008 R2	YES*	YES
Windows Server 2008	YES*	YES
Windows 7	NO	YES
Windows Vista	NO	YES
Windows Server 2003 R2	YES	YES
Windows Server 2003	YES	YES

* vSphere Replication performs application quiescing on Windows Server 2008, Windows Server 2012 and Windows Server 2016 by creating a snapshot of the virtual machine. See [Working with Microsoft Shadow Copy](#) and [Linux Backup Implementation](#) for Windows Server 2008 and 2012 limitations.

- The virtual machine must be running on a 7 or later host.
- The UUID attribute must be enabled. It is enabled by default for virtual machines created on 4.1 or later. For details on enabling this attribute, see **Enable Virtual Machine Application Consistent Quiescing** in [Working with Microsoft Shadow Copy](#) <https://code.vmware.com/docs/9684/virtual-disk-development-kit-programming-guide-6-7-3/GUID-78D5787C-BEA8-4C9C-86EE-B63C9AAE1F3A.html>.
- The virtual machine must use SCSI disks only and have the same number of free SCSI slots as the number of disks. Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.
- The virtual machine must not use dynamic disks.

Linux Quiescing Support

To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.

NOTE: vSphere Replication 8.8 supports quiescing for Linux guest OS only for virtual machines that run on ESXi 7.0 hosts or later.

Operating System Vendor	Operating System	Application Quiescing	File System Quiescing
Asianux	Asianux 4.0 or later	NO	NO
Asianux	Asianux 3.0	NO	YES
Canonical Ltd	Ubuntu	NO	YES

CentOS	CentOS 9	NO	NO
CentOS	CentOS 6.x, 7x, 8x	NO	YES (ESXi 8.0 or later)
CentOS	CentOS 5.x	NO	YES
CentOS	CentOS 4.9	NO	YES
Debian	Debian GNU/Linux 8.x or later	NO	NO
Debian	Debian GNU/Linux 7.x	NO	YES
Debian	Debian GNU/Linux 6.0	NO	YES
FreeBSD	FreeBSD 11.x or later	NO	NO
FreeBSD	FreeBSD 10.x	NO	YES
FreeBSD	FreeBSD 9.x	NO	YES
FreeBSD	FreeBSD 8.x	NO	YES
FreeBSD	FreeBSD 7.x	NO	YES
Cybertrust Japan Co.,Ltd.	MIRACLE LINUX 9.x	NO	NO
Cybertrust Japan Co.,Ltd.	MIRACLE LINUX 8.x	NO	YES
Oracle	Oracle Linux 6.x or later	NO	NO
Oracle	Oracle Linux 5.x	NO	YES
Oracle	Oracle Linux 4.9	NO	YES
Red Hat	Red Hat Enterprise Linux 9.x	NO	NO
Red Hat	Red Hat Enterprise Linux 8.x	NO	YES (ESXi 8.0 or later)
Red Hat	Red Hat Enterprise Linux 7.x	NO	YES
Red Hat	Red Hat Enterprise Linux 6.x	NO	YES
Red Hat	Red Hat Enterprise Linux 5.x	NO	YES
Red Hat	Red Hat Enterprise Linux 4.x	NO	YES
Rocky Enterprise Software Foundation	Rocky Linux 9.x	NO	NO
Rocky Enterprise Software Foundation	Rocky Linux 8.x	NO	NO
SCO	OpenServer 6	NO	YES
SCO	OpenServer 5	NO	YES
Serenity Systems	eComStation 2	NO	YES
Serenity Systems	eComStation 1	NO	YES
Sun Microsystems	Solaris 11	NO	YES
Sun Microsystems	Solaris 10	NO	YES
Sun Microsystems	Solaris 9	NO	YES
Sun Microsystems	Solaris 8	NO	YES
SUSE	SUSE Linux Enterprise Server 15	NO	YES (ESXi 8.0 or later)
SUSE	SUSE Linux Enterprise Desktop 15	NO	YES (ESXi 8.0 or later)
SUSE	SUSE Linux Enterprise Server 12	NO	YES
SUSE	SUSE Linux Enterprise Desktop 12	NO	YES

SUSE	SUSE Linux Enterprise Server 11	NO	YES
SUSE	SUSE Linux Enterprise Server 10 Service Pack 4	NO	YES
SUSE	SUSE Linux Enterprise Server 9 Service Pack 4	NO	YES

Disclaimer

THIS CONTENT IS PROVIDED "AS-IS," AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE DISCLAIMS ALL OTHER REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, REGARDING THIS CONTENT, INCLUDING THEIR FITNESS FOR A PARTICULAR PURPOSE, THEIR MERCHANTABILITY, OR THEIR NONINFRINGEMENT. VMWARE SHALL NOT BE LIABLE FOR ANY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS CONTENT, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF VMWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

vSphere Replication Administration

Step-by-step instructions on how to install, configure, upgrade, and use VMware vSphere Replication.

About VMware vSphere Replication

VMware vSphere Replication is an extension to VMware vCenter Server that provides a hypervisor-based virtual machine replication and recovery.

vSphere Replication is an alternative to storage-based replication. It protects virtual machines from partial or complete site failures by replicating the virtual machines between the following sites:

- From a source site to a target site
- Within a single site from one cluster to another
- From multiple source sites to a shared remote target site

vSphere Replication provides several benefits as compared to storage-based replication.

- Data protection at a lower cost per virtual machine.
- A replication solution that allows flexibility in the storage vendor selection at the source and target sites.
- Lower overall cost per replication.

vSphere Replication Use and Compatibility

You can use vSphere Replication with the vCenter Server Appliance or with a standard vCenter Server installation. You can have a vCenter Server Appliance on one site and a standard vCenter Server installation on the other.

vSphere Replication is compatible with N-1 version of vSphere Replication on the paired site. For example, if the current version of vSphere Replication is 8.8, the supported versions for the paired site is 8.6 and later.

vSphere Replication Functionalities

With vSphere Replication, you can replicate virtual machines from a source data center to a target site quickly and efficiently.

You can deploy additional vSphere Replication servers to meet your load-balancing needs.

After you set up the replication infrastructure, you can select the virtual machines to be replicated at a different recovery point objective (RPO). You can enable the multi-point-in-time retention policy to store more than one instance of the replicated virtual machine. After recovery, the retained instances are available as snapshots of the recovered virtual machine.

You can use VMware vSAN datastores as target datastores and select destination storage profiles for the replica virtual machine and its disks when configuring replications.

You can configure all vSphere Replication features in the Site Recovery user interface like managing sites, registering additional replication servers monitoring and managing replications.

Site Recovery Client Plug-In

The vSphere Replication appliance adds a plug-in to the vSphere Client. The plug-in is also shared with Site Recovery Manager and is named Site Recovery.

You use the Site Recovery client plug-in to perform all vSphere Replication actions.

- View the vSphere Replication status for all vCenter Server instances that are registered with the same vCenter Single Sign-On.
- Open the Site Recovery user interface.
- View a summary of the replication configuration parameters on the **Summary** tab of virtual machines that are configured for replication.
- Reconfigure the replications of one or more virtual machines by selecting the VMs and using the context menu.

vSphere Replication Appliance Components

The vSphere Replication appliance provides all the components that vSphere Replication requires.

- Site Recovery user interface that provides a full functionality for working with vSphere Replication.
- A plug-in to the vSphere Client that provides a user interface for troubleshooting vSphere Replication health status and links to the Site Recovery standalone user interface.
- A VMware standard embedded vPostgreSQL database that stores the replication configuration and management information. vSphere Replication does not support external databases.
- A vSphere Replication management server:
 - Configures the vSphere Replication server.
 - Enables, manages, and monitors replications.
 - Authenticates users and checks their permissions to perform vSphere Replication operations.
- A vSphere Replication server that provides the core of the vSphere Replication infrastructure.

The vSphere Replication appliance provides a virtual appliance management interface (VRMS Appliance Management Interface.) You can use the VRMS Appliance Management Interface to configure the appliance after deployment. For example, you can use the VRMS Appliance Management Interface to change the appliance security settings or change the network settings. You can deploy additional vSphere Replication Servers using a separate .ovf package.

Related Links

[Local and Remote Sites on page 40](#)

In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.

[How vSphere Replication Works on page 41](#)

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

[Replication Data Compression on page 45](#)

You can configure vSphere Replication to compress the data that it transfers through the network.

Local and Remote Sites

In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.

The local site can be any site where vCenter Server supports a critical business need. The remote site can be in another location, or in the same facility to establish redundancy. The remote site is usually located in a facility that is unlikely to be affected by environmental, infrastructure, or other disturbances that might affect the local site.

vSphere Replication has the following requirements for the vSphere® environments at each site:

- Each site must have at least one data center.
- The remote site must have hardware, network, and storage resources that can support the same virtual machines and workloads as the local site.
- The sites must be connected by a reliable IP network.

- The remote site must have access to networks (public and private) comparable to the ones on the local site, although not necessarily the same range of network addresses.

Connecting Local and Remote Sites

Before you replicate virtual machines between two sites, you must connect the sites. When connecting sites, users at both sites must have the **VRM remote > Manage VRM** privilege assigned.

When you connect sites that are part of the same vCenter Single Sign-On domain, you must select the remote site only, without providing authentication details, because you are already logged in.

When you connect sites that belong to different vCenter Single Sign-On domains, the vSphere Replication Management Server must register with the Platform Services Controller on the remote site. You must provide authentication details for the remote site, including IP or FQDN of the server where Platform Services Controller runs, and user credentials. See [Local and Remote Sites](#) .

After connecting the sites, you can monitor the connectivity state between them in the Site Recovery user interface.

Related Links

[vSphere Replication Appliance Components on page 40](#)

The vSphere Replication appliance provides all the components that vSphere Replication requires.

[How vSphere Replication Works on page 41](#)

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

[Replication Data Compression on page 45](#)

You can configure vSphere Replication to compress the data that it transfers through the network.

How vSphere Replication Works

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

When you configure a virtual machine for replication, the vSphere Replication agent sends changed blocks in the virtual machine disks from the source site to the target site. The changed blocks are applied to the copy of the virtual machine. This process occurs independently of the storage layer. vSphere Replication performs an initial full synchronization of the source virtual machine and its replica copy. You can use replication seeds to reduce the network traffic that data transfer generates during the initial full synchronization.

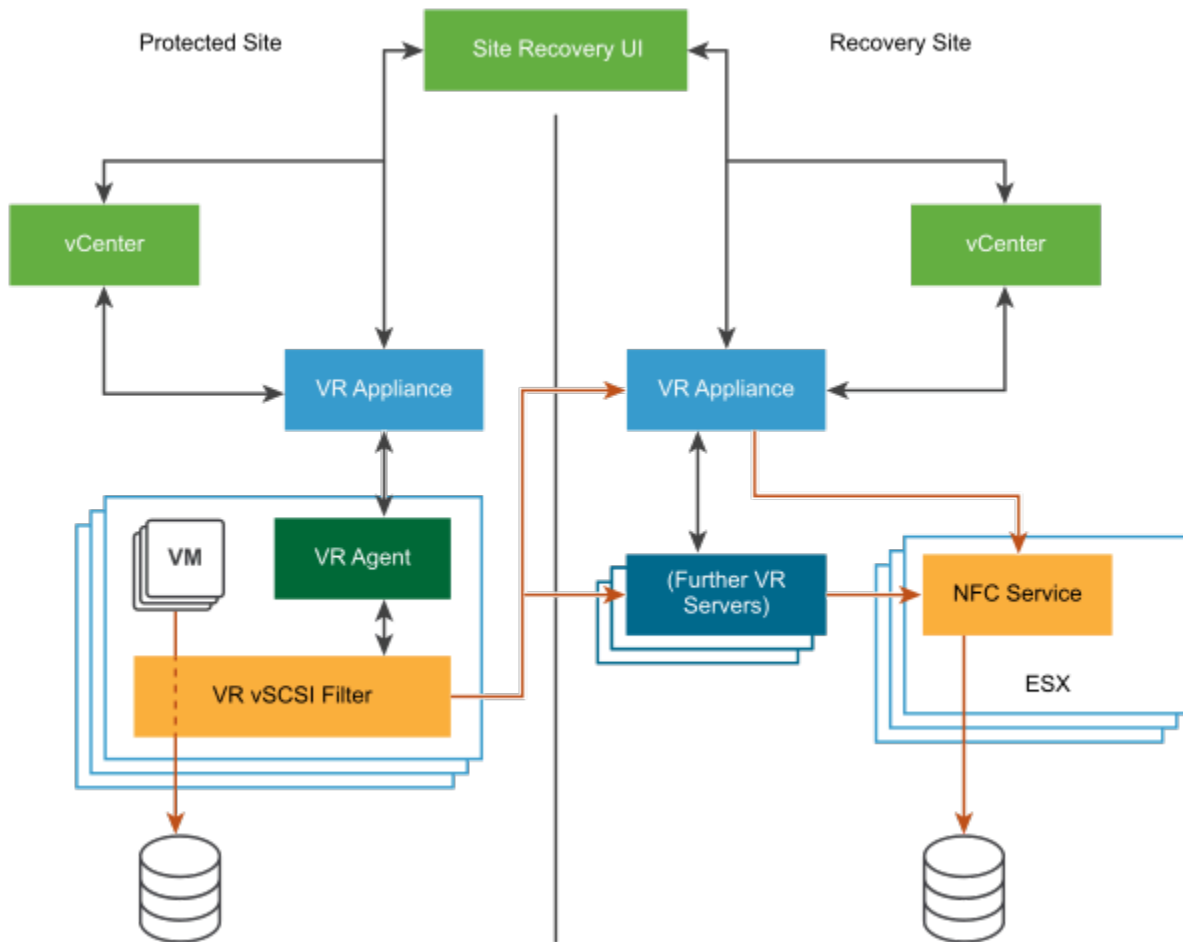
During replication configuration, you can set a recovery point objective (RPO) and enable retention of instances from multiple points in time (MPIT).

As administrator, you can monitor and manage the status of the replication. You can view information for outgoing and incoming replications, local and remote site status, replication issues, and for warnings and errors.

When you manually recover a virtual machine, vSphere Replication creates a copy of the virtual machine connected to the replica disk, but does not connect any of the virtual network cards to port groups. You can review the recovery and status of the replica virtual machine and attach it to the networks. You can recover virtual machines at different points in time, such as the last known consistent state. vSphere Replication presents the retained instances as ordinary virtual machine snapshots to which you can revert the virtual machine.

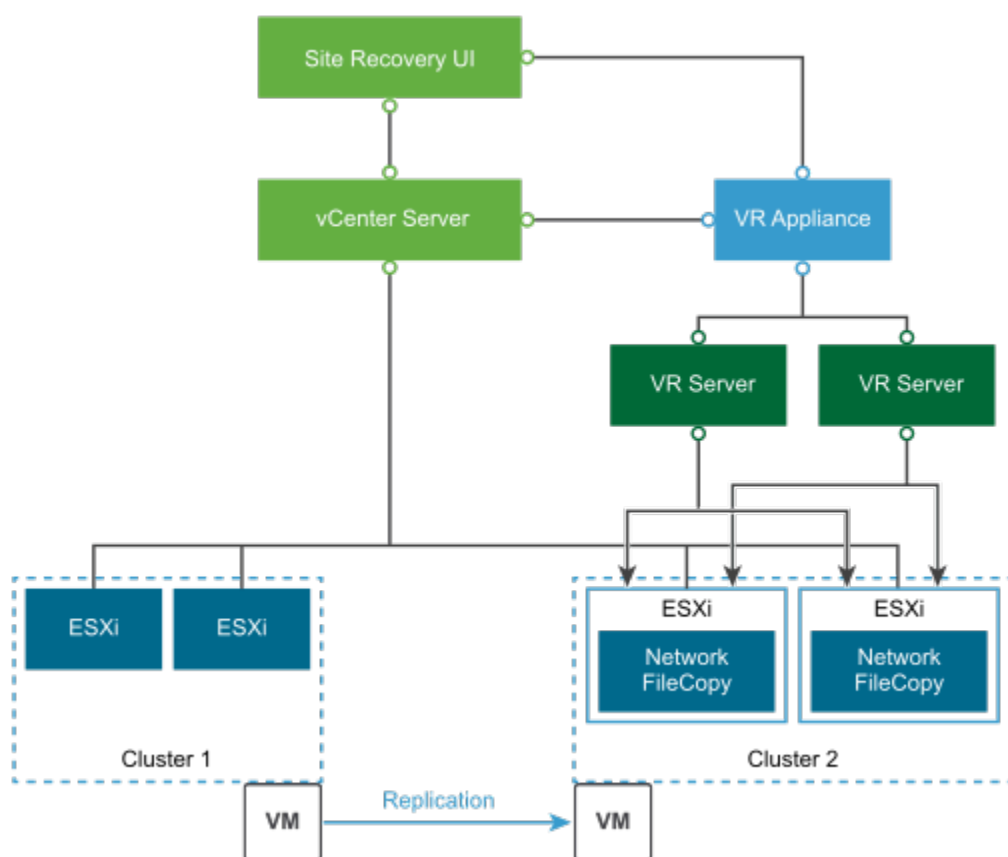
vSphere Replication stores replication configuration data in its embedded database.

You can replicate a virtual machine between two sites. vSphere Replication is installed on both source and target sites. Only one vSphere Replication appliance is deployed on each vCenter Server. You can deploy additional vSphere Replication Servers.

Figure 1: Replication Between Two Sites

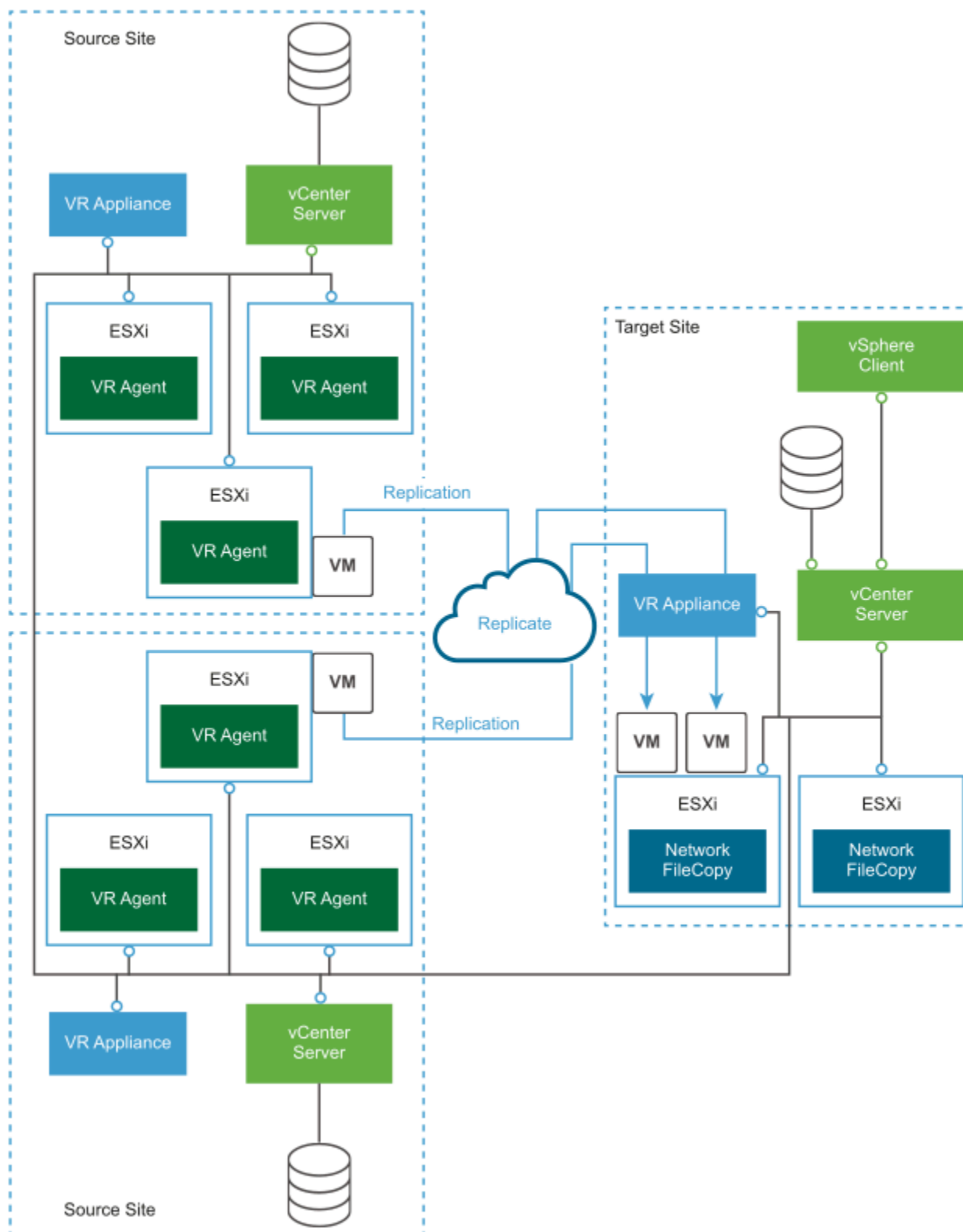
You can also replicate a virtual machine between datastores at the same vCenter Server. In that topology one vCenter Server manages hosts at the source and at the target. Only one vSphere Replication appliance is deployed on the single vCenter Server. You can add multiple Additional vSphere Replication servers in a single vCenter Server to replicate virtual machines to other clusters.

To perform recovery, the vCenter Server managing the target datastore, the vSphere Replication appliance, and any additional vSphere Replication Servers managing the replication must be up and running.

Figure 2: Replication in a Single vCenter Server

You can replicate virtual machines to a shared target site.

Figure 3: Replication to a Shared Target Site



Related Links

[vSphere Replication Appliance Components on page 40](#)

The vSphere Replication appliance provides all the components that vSphere Replication requires.

[Local and Remote Sites on page 40](#)

In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.

[Replication Data Compression on page 45](#)

You can configure vSphere Replication to compress the data that it transfers through the network.

Replication Data Compression

You can configure vSphere Replication to compress the data that it transfers through the network.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

The ESXi host on the source site compresses the data, and the vSphere Replication server on the target site passes off the data to the ESXi host, where the host decompresses the data, and writes it to disk.

Related Links

[vSphere Replication Appliance Components on page 40](#)

The vSphere Replication appliance provides all the components that vSphere Replication requires.

[Local and Remote Sites on page 40](#)

In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.

[How vSphere Replication Works on page 41](#)

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

vSphere Replication System Requirements

The environment in which you run the vSphere Replication virtual appliance must meet certain hardware requirements.

vSphere Replication is distributed as a 64-bit virtual appliance packaged in the `.ovf` format. It is configured to use a dual-core or quad-core CPU, a 16 GB and a 17 GB hard disk, and 8 GB of RAM. Additional vSphere Replication servers require 1 GB of RAM.

You must deploy the virtual appliance in a vCenter Server environment by using the OVF deployment wizard on an ESXi host.

You must deploy vSphere Replication in the same vCenter Server inventory where you replicate virtual machines.

vSphere Replication consumes negligible CPU and memory on the source host ESXi and on the guest OS of the replicated virtual machine.

NOTE

vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

The operation of vSphere Replication depends on certain services, ports, and external interfaces. For more information, see [Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses](#).

vSphere Replication Licensing

You can use vSphere Replication with certain editions of vSphere that include vSphere Replication in the license.

vSphere Replication does not have a separate license as it is a feature of certain vSphere license editions.

- vSphere Essentials Plus
- vSphere Standard
- vSphere Enterprise
- vSphere Enterprise Plus
- vSphere Desktop

If you have the correct vSphere license, there is no limit on the number of virtual machines that you can replicate by using vSphere Replication.

You cannot use vSphere Replication to replicate virtual machines on ESXi hosts that do not have the correct vSphere license. If you install vSphere Replication on an ESXi host that does not have the correct license and try to configure a replication for virtual machines on that host, the replication fails with a licensing error.

If you configure a virtual machine for a replication on a host with the correct vSphere license and move it to a host with an unsupported license, vSphere Replication stops the replication of that virtual machine. You can deactivate vSphere Replication on a configured virtual machine on the unlicensed host.

Operational Limits of vSphere Replication

To ensure a successful virtual machine replication, you must verify that your virtual infrastructure respects certain limits before you start the replication.

The following operational limits apply to vSphere Replication:

- You can only deploy one vSphere Replication appliance on a vCenter Server instance. After you deploy another vSphere Replication appliance, during the initial configuration process in the VRMS Appliance Management Interface, vSphere Replication detects another appliance already deployed and registered as an extension to vCenter Server. To proceed with the new appliance, you must confirm.
- Each newly deployed vSphere Replication appliance can manage a maximum of 400 replications. See <https://kb.vmware.com/kb/2102453> for more information.
- vSphere Replication 8.8 uses only an embedded database and requires additional configuration to enable the support of a maximum of 4000 replications. See <https://kb.vmware.com/kb/2102463>.
- The maximum number of replications with 5 minute RPO can vary, depending on the network bandwidth and the change rates per disk. vSphere Replication 8.8 can accommodate 5 minute RPO for 500 VMs.

Table 1: Replication Maximums for vSphere Replication 8.8

Item	Maximum
vSphere Replication appliances per vCenter Server instance.	1
Maximum number of additional vSphere Replication servers per vSphere Replication.	9
Maximum number of protected virtual machines per vCenter Server instance.	4000

Item	Maximum
Maximum number of protected virtual machines per vSphere Replication appliance (by using the embedded vSphere Replication server.)	400
Maximum number of protected virtual machines per vSphere Replication server.	400
Maximum number of virtual machines configured for one replication at a time.	20
Maximum number of protected virtual machines with 5 minute RPO per vCenter Server instance.	500
Maximum number of protected virtual machines per vSphere Replication appliance on vSAN Express storage.	1000
Maximum number of protected disks per virtual machine on ESXi 8.0 or earlier version.	64
Maximum number of protected disks per virtual machine on ESXi 8.0 Update 1 or later version.	256
Maximum number of protected disks per host.	8192

vSphere Replication Compatibility Information

vSphere Replication is compatible with certain other vSphere management features and other VMware software.

vSphere Replication Compatibility with Other vSphere Features

You can safely use vSphere Replication with certain vSphere features, such as vSphere vMotion. Some other vSphere features, for example, vSphere Distributed Power Management, require a special configuration for use with vSphere Replication.

NOTE

To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

Table 2: Compatibility of vSphere Replication with Other vSphere Features

vSphere Feature	Compatible with vSphere Replication	Description
vSphere vMotion	Yes	You can migrate replicated virtual machines by using vMotion. Replication continues at the defined recovery point objective (RPO) after the migration is finished.
vSphere Storage vMotion	Yes	You can move the disk files of a replicated virtual machine on the source site using Storage vMotion with no impact on the ongoing replication.
vSphere High Availability	Yes	You can protect a replicated virtual machine by using HA. Replication continues at the defined RPO after HA restarts a virtual machine. vSphere Replication does not perform any special HA handling. You can protect the vSphere Replication appliance itself by using HA.
vSphere Fault Tolerance	No	You cannot replicate virtual machines that have Fault Tolerance enabled. You cannot protect the vSphere Replication appliance itself with FT.
vSphere DRS	Yes	Replication continues at the defined RPO after the resource redistribution is finished.

vSphere Feature	Compatible with vSphere Replication	Description
vSphere Storage DRS	Yes	On the source site, Storage DRS can move the disk files of replicated virtual machines with no impact on the ongoing replication. On the target site, you must register the vSphere Replication appliance with the vCenter Single Sign-On service to enable the communication between Storage DRS and the vSphere Replication Management server. See Configure the vSphere Replication Appliance to Connect to a vCenter Server instance .
vSAN datastore	Yes	You can use vSAN datastores as the source and target datastore when configuring replications.
vSAN Express datastore	Yes	You can use vSAN Express datastores as the source and target datastore when configuring replications.
vSphere Distributed Power Management	Yes	vSphere Replication coexists with DPM on the source site. vSphere Replication does not perform any special DPM handling on the source site. You can deactivate DPM on the target site to allow enough hosts as replication targets.
VMware vSphere Flash Read Cache	Yes	You can protect virtual machines that contain disks that use the VMware vSphere Flash Read Cache storage. Since the host to which a virtual machine recovers might not be configured for Flash Read Cache, vSphere Replication deactivates Flash Read Cache on disks when it starts the virtual machines on the recovery site. vSphere Replication sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take note of the virtual machine's cache reservation from the vSphere Client. After the recovery, you can migrate the virtual machine to a host with Flash Read Cache storage and restore the original Flash Read Cache setting on the virtual machine manually.
vSphere Lifecycle Manager	Yes	You can use vSphere Replication and vSphere Lifecycle Manager (vLCM) in the same data center with a manual workaround. For more information, see the VMware vSphere Replication 8.5.0.3 Release Notes .
vCloud APIs	Not applicable	No interaction with vSphere Replication.
vCenter Chargeback	Not applicable	No interaction with vSphere Replication
VMware Data Recovery	Not applicable	No interaction with vSphere Replication.

vSphere Replication Compatibility with Other Software

vSphere Replication is compatible with certain versions of ESXi, vCenter Server, Site Recovery Manager, and Web browsers.

For information about the vSphere Replication compatibility, see the following documents:

- Compatibility Matrices for vSphere Replication 8.8 at <https://docs.vmware.com/en/vSphere-Replication/8.8/rn/compatibility-matrices-for-vsphere-replication-88/index.html>.
- vSphere Replication interoperability with backup software when using VSS at <https://kb.vmware.com/kb/2040754>.
- VMware Compatibility Guide at https://partnerweb.vmware.com/comp_guide2/search.php
- Browser compatibility at vSphere Client and Software Requirements in the *vSphere Installation and Setup* guide.

Bandwidth Requirements for vSphere Replication

To replicate virtual machines efficiently, before configuring a replication you can determine the storage and network bandwidth requirements for vSphere Replication.

Storage and network bandwidth requirements can increase when using vSphere Replication. The following factors play a role in the amount of network bandwidth that vSphere Replication requires for an efficient replication.

Network-Based Storage

Network bandwidth requirements increase if all storage is network-based, because data operations between the host and the storage also use network. When you plan your deployment, be aware of the following levels of traffic:

- Between the host running the replicated virtual machine and the vSphere Replication server.
- Between the vSphere Replication server and a host with access to the replication target datastore.
- Between the host and storage.
- Between storage and the host, during redo log snapshots.

Network-based storage is a concern when you are replicating virtual machines within a single vCenter Server instance, that shares the network for the levels of traffic listed. When you have two sites, each with a vCenter Server instance, the link speed between the two sites is the most important as it can slow down the replication traffic between the two sites.

Dataset Size

vSphere Replication might not replicate every virtual machine or every VMDK file in the replicated virtual machines. To evaluate the dataset size that vSphere Replication replicates, calculate the percentage of the total storage used for virtual machines, then calculate the number of VMDKs within that subset that you have configured for replication.

For example, you might have 2 TB of virtual machines on the datastores and use vSphere Replication to replicate half of these virtual machines. You might only replicate a subset of the VMDKs and the maximum amount of data for replication is 1 TB.

Data Change Rate and Recovery Point Objective

Recovery point objective (RPO) affects the data change rate. To estimate the size of the data transfer for each replication, you must evaluate how many blocks change in a given RPO for a virtual machine. The data change rate within the RPO period provides the total number of blocks that vSphere Replication transfers. This number might vary throughout the day, which alters the traffic that vSphere Replication generates at different times.

vSphere Replication transfers blocks based on the RPO schedule. If you set an RPO of one hour, vSphere Replication transfers any block that has changed in that hour. vSphere Replication only transfers the block once in its current state, at the moment that vSphere Replication creates the bundle of blocks for transfer. vSphere Replication only registers that the block has changed within the RPO period, not how many times it changed. The average daily data change rate provides an estimation of how much data vSphere Replication transfers or how often the transfers occur.

If you use Volume Shadow Copy Service (VSS) to quiesce the virtual machine, replication traffic cannot be spread out in small sets of bundles throughout the RPO period. Instead, vSphere Replication transfers all the changed blocks as one set, when the virtual machine is idle. Without VSS, vSphere Replication can transfer smaller bundles of changed blocks on an ongoing basis as the blocks change, spreading the traffic throughout the RPO period. The traffic changes if you use VSS and vSphere Replication handles the replication schedule differently, leading to varying traffic patterns.

If you change the RPO, vSphere Replication transfers more or less data per replication to meet the new RPO.

Link Speed

If you have to transfer an average replication bundle of 4 GB in a one hour period, you must examine the link speed, to determine if the RPO can be met. If you have a 10Mb link, under ideal conditions on a dedicated link with little overhead, 4GB takes about an hour to transfer. Meeting the RPO saturates a 10Mb WAN connection. The connection is saturated even under ideal conditions, with no overhead or limiting factors such as retransmits, shared traffic, or excessive bursts of data change rates.

You can assume that only about 70% of a link is available for traffic replication. This means that on a 10Mb link you obtain a link speed of about 3GB per hour. On a 100Mb link, you obtain a speed of about 30GB per hour.

To calculate the bandwidth, see [Calculate Bandwidth For vSphere Replication](#).

There is no hard requirement about the minimal latency across the Wide Area Network (WAN) caused by the geographic distance between the data centers. However, when the WAN connecting the two data centers has latency, out-of-order or dropped packets, the replication throughput can be affected resulting in RPO violations.

Calculate Bandwidth For vSphere Replication

To determine the bandwidth that vSphere Replication requires to replicate virtual machines efficiently, you calculate the average data change rate within an RPO period, divided by the link speed.

- Examine how data change rate, traffic rates, and the link speed meet the RPO.
- Look at the aggregate of each group.

If you have groups of virtual machines that have different RPO periods, you can determine the replication time for each group of virtual machines. For example, you might have four groups with RPO of 15 minutes, 1 hour, 4 hours, and 24 hours. If you want to calculate the bandwidth requirements for vSphere Replication, consider the following factors:

- All the different RPOs in the environment.
 - The subset of virtual machines in your environment that is replicated.
 - The change rate of the data within that subset.
 - The number of data changes within each configured RPO.
 - The link speeds in your network.
1. Identify the average data change rate within the RPO by calculating the average change rate over a longer period, then dividing it by the RPO.
 2. Calculate how much traffic this data change rate generates in each RPO period.
 3. Measure the traffic against your link speed.

For example, a data change rate of 100GB requires approximately 200 hours to replicate on a T1 network, 30 hours to replicate on a 10Mbps network, 3 hours on a 100Mbps network.

Installing and Setting Up vSphere Replication

To ensure a successful vSphere Replication deployment, follow the sequence of tasks required.

vSphere Replication uses the replication technologies included in ESXi with the assistance of virtual appliances to replicate virtual machines between source and target sites.

To use vSphere Replication, you must deploy the vSphere Replication appliance on an ESXi host by using the vSphere Client.

NOTE

You must deploy vSphere Replication in the same vCenter Server inventory where you replicate virtual machines.

The vSphere Replication appliance registers as an extension with the corresponding vCenter Server instance. For example, on the source site, the vSphere Replication appliance registers with the vCenter Server instance on the source site. Only one vSphere Replication appliance is allowed per vCenter Server.

The vSphere Replication appliance contains an embedded vSphere Replication server that manages the replication process. To meet the load balancing needs of your environment, you might need to deploy additional vSphere Replication servers at each site. Additional vSphere Replication servers that you deploy are themselves virtual appliances. You must register any additional vSphere Replication server with the vSphere Replication appliance on the corresponding site.

The vSphere Replication appliance automatically installs an encryption agent VIB on all ESXi hosts from the vCenter Server inventory. The encryption agent is used to encrypt the outgoing replicated data of the virtual machines that run on these ESXi hosts.

When using vSphere Replication, all hosts within the vCenter Server inventory are registered automatically. If you want to exclude hosts or hosts under a given cluster or datacenter from registration in vSphere Replication, you can tag them with the `com.vmware.vr.disallowedHost` tag. This is valid for the incoming replications on the target site. The tagged hosts are still used for outgoing replications and the virtual machines on the disallowed hosts can be replicated.

The vSphere Replication appliance provides a virtual appliance management interface (VRMS Appliance Management Interface). You can use the VRMS Appliance Management Interface to perform initial configuration and reconfigure the vSphere Replication database, network settings, public-key certificates, and passwords for the appliances.

Prepare Your Environment to Install vSphere Replication

Before you deploy the vSphere Replication appliance, you must prepare the environment.

Verify that you have vSphere and vSphere Client installations for the source and target sites.

NOTE

vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

1. In the vSphere Client, select the vCenter Server instance on which you are deploying vSphere Replication, click **Configure > Settings > Advanced Settings**, and verify that the `VirtualCenter.FQDN` value is set to a fully qualified domain name or a literal address.
2. If you configure vSphere Replication in an IPv6 network, verify that the IPv6 address of the vSphere Replication appliance, vCenter Server, and the ESXi hosts are mapped to fully qualified domain names on the DNS server. Install the vSphere Replication appliance by using FQDN and post installation, make sure that the **Local Host** text box in the VRMS Appliance Management Interface is set to the FQDN of the vSphere Replication appliance. Do not use a static IPv6 address.

You can deploy the vSphere Replication appliance.

Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance. To deploy vSphere Replication successfully, follow the sequence of instructions.

- Download the vSphere Replication ISO image and mount it on a system in your environment.

You deploy the vSphere Replication appliance by using the standard vSphere OVF deployment wizard.

NOTE

vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Copying or migrating an existing vSphere Replication appliance is not supported. You must do a new deployment.

1. Log in to the vSphere Client on the source site.
If you use the HTML5-based vSphere Client to deploy the OVF virtual appliance, on vSphere version earlier than vSphere 6.7 Update 1, the deployment succeeds, but vSphere Replication fails to start.
2. On the home page, select **Hosts and Clusters**.
3. Right-click a host and select **Deploy OVF template**.
4. Provide the location of the OVF file from which to deploy the vSphere Replication appliance, and click **Next**.
 - Select **URL** and provide the URL to deploy the appliance from an online URL.
 - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_OVF10.ovf`, `vSphere_Replication_OVF10.cert`, `vSphere_Replication_OVF10.mf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files.
5. Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**.
You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.
6. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
7. Review the virtual appliance details and click **Next**.
8. Accept the end-user license agreements (EULA) and click **Next**.
9. Select a destination datastore, disk format for the virtual appliance, and VM storage policy, and click **Next**.
Encrypting the vSphere Replication appliance VM is not necessary to replicate encrypted VMs with vSphere Replication.
10. Select a network from the list of available networks, set the IP protocol and IP allocation, and click **Next**.
vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the VRMS Appliance Management Interface after installation.
11. On the **Customize template** page, enter one or more NTP server host names or IP addresses.
12. Set the password for the root account and enter the hostname or IP address of at least one NTP server.
The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. The username cannot be a part of the password.
13. To check the integrity of the vSphere Replication appliance binary files, select the **File Integrity Flag** check box.
If the vSphere Replication appliance detects changes to the binary files, it sends log traces to the syslog.
14. Optional: You can modify the default Network Properties.

Setting	Action
Host Network IP Address Family	Select the Network IP address family. The options are IPv4 or IPv6.
Host Network Mode	Select the host network mode. The options are static, DHCP, or autoconf. Autoconf is available only for IPv6.
Default Gateway	Enter the default gateway address for this VM.
Domain Name	Enter the domain name of this VM.

Setting	Action
Domain Search Path	Enter the domain search path for this VM. Use comma or space separated domain names.
Domain Name Servers	The domain name server IP Addresses for this VM. Use commas to separate the IP addresses.
Network 1 IP Address	The IP address for the default Ethernet adapter.
Network 1 Netprefix	The prefix for the default Ethernet adapter.

15. Click **Next**.

16. Review the settings and click **Finish**.

The vSphere Replication appliance is deployed.

17. Power on the vSphere Replication appliance. Take a note of the IP address of the appliance and log out of the vSphere Client.

18. To deploy vSphere Replication on the target site, repeat the procedure.

Configure the vSphere Replication Appliance to connect to a vCenter Server.

You can change the number of vCPUs after deploying the vSphere Replication Appliance. Selecting higher number of vCPUs ensures the better performance of the vSphere Replication Management Server, but might slow down the replications that run on ESXi host systems that have 4 or less cores per NUMA node. If you are unsure what the hosts in your environment are, select 2 vCPUs.

Configure the vSphere Replication Appliance to Connect to a vCenter Server instance

To start replicating virtual machines, you must configure the vSphere Replication Appliance to connect to a vCenter Server instance on both the source and the target sites.

[Deploy the vSphere Replication Virtual Appliance](#) and power it on.

Concurrent Installations of vSphere Replication in an Enhanced Linked Mode Environment

In an Enhanced Linked Mode environment, do not install vSphere Replication under more than one vCenter Server at the same time.

A conflict can arise in the creation of the service account that vCenter Server creates at the domain level for vSphere Replication authentication with vCenter Server if the following conditions exist:

- If the installation of one vSphere Replication instance overlaps with the installation of another vSphere Replication Server instance under two different vCenter Server instances.
- Those vCenter Server instances are in Enhanced Linked Mode.

The conflict does not prevent installation, but it does cause one of the vSphere Replication Server instances to fail to start, with the error message `Failed to start service`. The message `Failed to start Authorization Manager` appears in the event log for that vSphere Replication Server instance.

Configure the vSphere Replication Appliance to Connect to a vCenter Server

Configure the vSphere Replication Appliance to connect to a vCenter Server instance on both sites.

1. Log in to the VRMS Appliance Management Interface as admin.
2. Click on **Summary**, then click **Configure Appliance**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register vSphere Replication.
PSC port	Accept the default value of 443, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the Platform Services Controller certificate.
5. On the **vCenter Server** page, select the vCenter Server instance with which to register the vSphere Replication Appliance, and click **Next**.



CAUTION

The drop-down menu includes all the vCenter Server instances that are registered with the Platform Services Controller. In an environment that uses Enhanced Linked Mode, it might also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. After you configure the vSphere Replication Appliance, you cannot select a different vCenter Server instance.

6. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

Menu Item	Description
Site name	A name for this vSphere Replication site, which appears in the vSphere Replication interface. The vCenter Server address is used by default. Use a different name for each vSphere Replication instance in the pair.
Administrator email	The email address of the vSphere Replication administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for vSphere Replication events.

Menu Item	Description
Local host	<p>The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the vSphere Replication Appliance detects is not the interface that you want to use.</p> <p>NOTE To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.</p>
Extension ID	The unique identifier of the vSphere Replication Appliance. The Extension ID is not customizable.
Storage Traffic IP	The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data.

7. On the **Ready to Complete** page, review your settings and click **Finish**.
8. To configure the vSphere Replication Appliance on the target site, repeat the procedure.

Understanding the States of vSphere Replication Displayed in the

You can see the vSphere Replication status on each vCenter Server in your environment and if vSphere Replication does not function properly, you can find the appropriate remediation.

Before you begin using vSphere Replication, you must configure the vSphere Replication Appliance to Connect to a vCenter Server.

After the configuration, in the vSphere Client, when you click **Site Recovery**, you can see the list of vCenter Server instances and the status of vSphere Replication on each vCenter Server instance. If you have Site Recovery Manager deployed in your environment, you can also see the status of Site Recovery Manager. You can change the configuration of each vSphere Replication appliance by clicking the **Configure** icon next to the status icon.

The following table lists the vSphere Replication states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 3: vSphere Replication States on vCenter Server Instances

Status	Description	Remediation
Not installed	The vSphere Replication extension is not registered in the vCenter Server Extension Manager. The vSphere Replication appliance is either not deployed or the vSphere Replication extension has been deleted from the vCenter Server Extension Manager.	If a vSphere Replication appliance is deployed on this vCenter Server, restart the appliance or the vSphere Replication Management service on the appliance. 1. Use a supported browser to log in to the VRMS Appliance Management Interface as the admin user. The URL for the VRMS Appliance Management Interface is <code>https://vr-appliance-address:5480</code> . 2. Click Services , then select hms and click Restart .
Not configured	A configuration error occurred. The configuration of the vSphere Replication Management Server is incorrect and must be updated. You cannot manage existing replications, or configure new replications to this server .	Configure the vSphere Replication appliance. 1. Point to the <code>Enabled (Configuration issue)</code> status. The detailed error message appears in a tooltip. 2. Click the Configure icon. The VRMS Appliance Management Interface opens. 3. Click Summary , then click Reconfigure , and enter the parameters indicated in the error message. 4. Click Restart .
Not compatible	There is a vSphere Replication appliance with earlier version than 8.0, registered in the vCenter Server.	Install vSphere Replication 8.0 or later.
Not accessible	The vSphere Replication Management Server is not accessible. The vSphere Replication extension is registered in the vCenter Server Extension Manager, but the vSphere Replication appliance is missing or powered off, or the vSphere Replication Management service is not running. You cannot manage existing replications, or configure new replications to this server .	<ul style="list-style-type: none"> • Verify that the vSphere Replication appliance exists on the vCenter Server. • Verify that the vSphere Replication appliance is powered on. • Restart the VRM service. <ul style="list-style-type: none"> a. Use a supported browser to log in to the VRMS Appliance Management Interface as the admin user. The URL for the VRMS Appliance Management Interface is <code>https://vr-appliance-address:5480</code>. b. Click Services, then select hms and click Restart.
OK	The vSphere Replication appliance is installed, configured, and functioning properly.	Not needed.

Configure vSphere Replication Connections

To use vSphere Replication between two sites managed by different vCenter Server instances, you must configure a connection between the two vSphere Replication appliances.

- Verify that you have installed vSphere Replication at the local and remote sites.
- If you plan to configure a remote connection, obtain the IP address or FQDN of the PSC server where the remote vSphere Replication Management Server is registered.

If the source and target vCenter Server instances use the same vCenter Single Sign-On domain, the connection is considered local. vSphere Replication uses the vCenter Single Sign-On service on the local site to authenticate with each vCenter Server in the vCenter Single Sign-On domain.

If the source and the target vCenter Server instances use different vCenter Single Sign-On domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller of the remote vCenter Single Sign-On domain.

You can use vSphere Replication to replicate virtual machines between ESXi hosts that the same vCenter Server manages. In this case, you deploy only one vSphere Replication appliance and do not need to connect the local and remote sites.

You can configure a connection on either site on which you have installed a vSphere Replication appliance. If you are using an untrusted certificate, certificate warnings might appear during the process.

You can also set up a connection between two sites while you configure a replication between them.

1. On the home page, click **Site Recovery** and click **Open Site Recovery**.
2. On the Site Recovery home page, click the **New Site Pair** button.
3. Select a local vCenter Server from the list, select a pair type, and click **Next**.
 - Pair with a peer vCenter Server located in a different Single Sign-On domain
 - Pair with a peer vCenter Server located in the same Single Sign-On domain
4. Enter the address of the Platform Services Controller for the vSphere Replication Server on the second site, provide the user name and password, and click **Find vCenter Server Instances**.

The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed vSphere Replication Server on the target site.

IMPORTANT

To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

5. Select the vCenter Server and the services you want to pair, and click **Next**.
6. On the Ready to complete page, review your settings selection, and click **Finish**.



The local and the remote sites are connected. The pair appears under on the home page of the Site Recovery user interface.

Understanding the vSphere Replication Site Connection States

You can view the states of the connections to target sites in the Site Recovery user interface.

The following table lists the states that you can observe, their meanings, and what you can do to change a state back to normal. You can view the states by clicking **View Details** for a site pair in the Site Recovery user interface.

Table 4: Replication Server Connection States

Icon	Status	Description	Remediation
	Connected	The connection between the local and remote vSphere Replication management servers is working properly.	Not needed.
	Not Connected	<ul style="list-style-type: none"> The SSL certificate on the local or remote vSphere Replication Management Server has been changed. The network connection between the local and remote vSphere Replication Management Servers is not functioning properly or one of the servers is offline. The user that is used for authentication with the Lookup Service or the VRMS extension user in the vCenter Single Sign-On might be deactivated or deleted. <p>In this state, configured replications might not be running.</p>	<ul style="list-style-type: none"> To reconnect the site connection, click the Reconnect button in the upper-right corner of the Summary page. In the vSphere Client, navigate to the vCenter Server, select the Monitor tab, and select Events under Tasks and Events to search for events related to vSphere Replication. Verify the status of the remote vSphere Replication appliances in the Site Recovery plug-in for vSphere Client.

Reconnect to a Remote Site

If the state of the connection to a target site is `Not connected`, you must repair the connection to manage existing replications, and to enable the creation of new replications.

Verify that the vCenter Server and the vSphere Replication Management Server on the local site are up and running, and that there is no network problem that can cause the `Not connected` status.

The states of the connections to the target sites appear in the Site Recovery user interface.

If the source and the target vCenter Server instances use different vCenter Single Sign-On domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller of the remote vCenter Single Sign-On domain. To establish a connection to a remote site, you provide the address of the vCenter Server and the Platform Services Controller, and enter the credentials of a user that has the **VRM remote > VRM Server > Manage VRM** privilege assigned. If the Platform Services Controller address changes or there is a change in the certificate, the connection status changes to `Not connected` and you must reconnect the two sites.

NOTE

You cannot use the **Reconnect** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Select **Site Pair > Summary**, and click **Reconnect**.
You can initiate the reconnect from either site, even if you only changed the installation on one of the sites.
5. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**.
If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that vSphere Replication already extends.

The connection status changes to `Connected`.

Use the OVF Tool to Deploy vSphere Replication Virtual Appliance

You can use the VMware OVF tool to deploy the vSphere Replication Virtual Appliance from an OVF template.

- Verify that you have downloaded and mounted the vSphere Replication .iso image.
- Verify that you have downloaded and installed on your computer the VMware OVF tool 4.2 or later.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about `ovftool`, see the [OVF Tool Documentation](#).

1. To deploy the vSphere Replication Virtual Appliance with the VMware OVF Tool, use one of the following command lines.

- If you want to obtain network settings through DHCP:

```
ovftool
--acceptAllEulas
--datastore="DATASTORE NAME"
--name="VIRTUAL MACHINE NAME"
--deploymentOption='standard | light'
--ipAllocationPolicy="dhcpPolicy"
--net:"Network 1"="VC NETWORK TO BE USED FOR VA"
--prop:"varoot-password"="PASSWORD"
--prop:"vaadmin-password"="PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
--prop:network.netmode.vSphere_Replication_Appliance='dhcp'
--prop:network.addrfamily.vSphere_Replication_Appliance='ipv4'
--vService:installation=com.vmware.vim.vsm:extension_vservice
${VSPHERE_REPLICATION_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=${ESX_HOST_NAME}
```

- If you want to obtain network settings through a static IP address:

```
ovftool
--acceptAllEulas
--datastore="DATASTORE NAME"
--name="VIRTUAL MACHINE NAME"
--deploymentOption='standard | light'
--net:"Network 1"="VC NETWORK TO BE USED FOR VA"
--prop:"varoot-password"="PASSWORD"
--prop:"vaadmin-password"="PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
```

```

--prop:"network.ip0.vSphere_Replication_Appliance"="VA IP"
--prop:"network.netprefix0.vSphere_Replication_Appliance"="NETWORK PREFIX"
--prop:"network.gateway.vSphere_Replication_Appliance"="GATEWAY IP"
--prop:"network.DNS.vSphere_Replication_Appliance"="DNS SERVER 1, DNS SERVER 2"
--prop:"network.searchpath.vSphere_Replication_Appliance"="DNS SEARCH PATH - DOMAIN"
--prop:"network.netmode.vSphere_Replication_Appliance"='static'
--ipAllocationPolicy="fixedPolicy"
--prop:network.addrfamily.vSphere_Replication_Appliance='ipv4'
--vService:installation=com.vmware.vim.vsm:extension_vservice
${VSPHERE_REPLICATION_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=${ESX_HOST_NAME}

```

2. Replace the variables in the example with values from your environment.

Variable	Description
<i>DATASTORE NAME</i>	The target datastore name.
<i>VIRTUAL MACHINE NAME</i>	Specify the vSphere Replication Management Server name.
<i>NETWORK 1</i>	The name of the network to which you attach the vSphere Replication Appliance.
<i>PASSWORD</i>	<ul style="list-style-type: none"> The password for the <code>root</code> account. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. The password for the <code>admin</code> account, which you use to log in to the vSphere Replication Management Server. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
<i>NTP SERVER IP OR FQDN</i>	The IP address or FQDN of the NTP server.
<i>VA IP</i>	The IP address of the vSphere Replication Management Server.
<i>NETWORK PREFIX</i>	The network prefix of the vSphere Replication Management Server.
<i>GATEWAY IP</i>	The gateway IP address of the vSphere Replication Management Server.
<i>DNS SERVER</i>	The DNS address of the vSphere Replication Management Server.
<i>DNS SEARCH PATH - DOMAIN</i>	The domain search path for this virtual machine (use a comma or a space to separate the different names.)
<i>VSPHERE_REPLICATION_OVF_FILEPATH</i>	The path to the OVF package. To get access to the vSphere Replication OVF files, navigate to the <code>\bin</code> directory in the ISO image.
<i>VSPHERE_USER</i>	The user name for the target vCenter Server.
<i>VSPHERE_USER_PASSWORD</i>	The password for the target vCenter Server.
<i>VCENTER_SERVER_ADDRESS</i>	The address of the target vCenter Server.
<i>ESX_HOST_NAME</i>	The name of the target ESX host.

Register the vSphere Replication appliance with the vCenter Single Sign-On service.

Uninstall vSphere Replication

Uninstall vSphere Replication from your environment.

- Verify that the vSphere Replication appliance is powered on.
- Stop all existing outgoing or incoming replications to the site.
- Disconnect any connections to other vSphere Replication sites.

NOTE

If a vSphere Replication appliance is deleted before all replications that it manages are stopped, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing. To prevent errors, you must remove the tags from all target datastores that were used for replications by the deleted vSphere Replication appliance. See [Search and Remove the vSphere Replication Tag from Target Datastores](#).

To uninstall vSphere Replication from your environment, you must unregister the appliance from the vCenter Single Sign-On service and from the vCenter Server, and then delete the vSphere Replication appliance.

If you delete the vSphere Replication appliance before unregistering it from the vCenter Single Sign-On server and the vCenter Server, a special procedure must be performed to clean up your environment. See [Clean up the vCenter Server Extension Manager](#).

1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
2. Click on **Summary**, then click **Unregister**.
3. In the vSphere Client, power off and delete the vSphere Replication appliance.
The Site Recovery plug-in is uninstalled automatically.

You removed vSphere Replication from your environment.

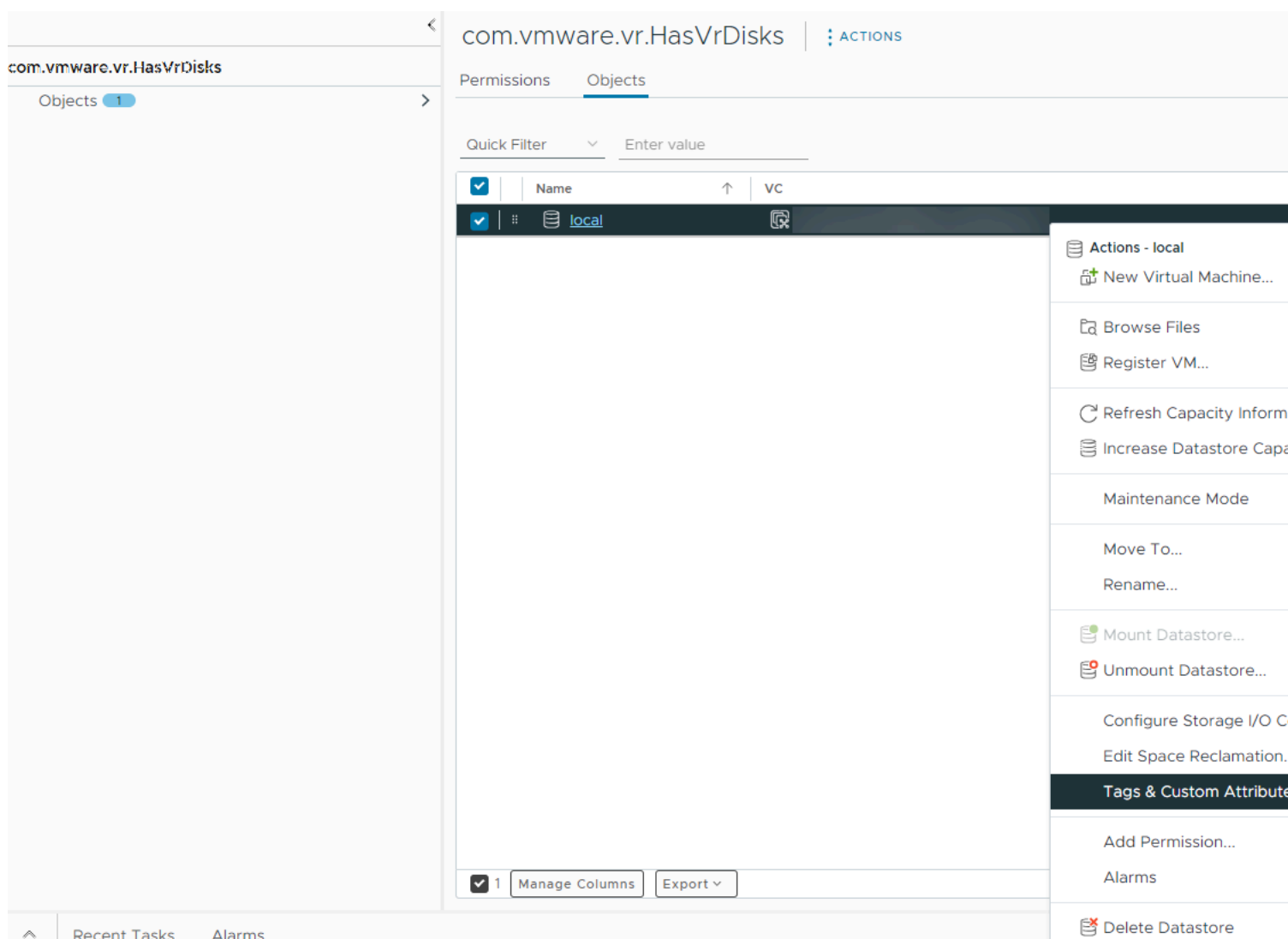
Remove the vSphere Replication Tag from Target Datastores

If you delete the vSphere Replication appliance before stopping all its replications, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. To prevent errors, remove the tags from all target datastores that were used for replications by the deleted vSphere Replication appliance.

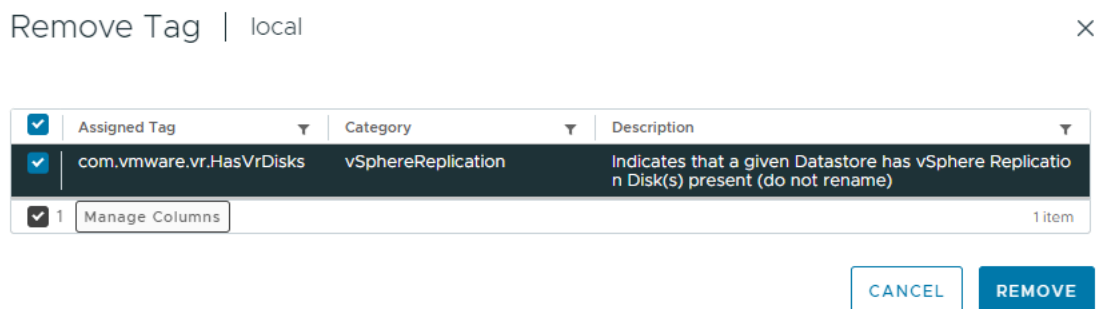
- Verify that the vSphere Replication appliance is deleted.
- Verify that you have the required privilege on the root vCenter Server instance (**Inventory Service > vSphere Tagging > Assign or Unassign vSphere Tag.**)

If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing.

1. Log in to the vSphere Client on the target site.
2. In the search box enter `com.vmware.vr.HasVrDisks`, press enter and click the tag.
3. Click the **Objects** tab.
4. Right-click a datastore and select **Tags & Custom Attributes > Remove Tag.**



- In the Remove Tag dialog box, select the row that contains `com.vmware.vr.HasVrDisks` and click **Remove**.



- Repeat steps 4 and 5 for all datastores that are assigned the `com.vmware.vr.HasVrDisks` tag.

Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted

If you delete the vSphere Replication appliance before unregistering it from the environment, you cannot use the VRMS Appliance Management Interface to unregister vSphere Replication from vCenter Server

Before you deploy a new vSphere Replication Appliance, you must clean up your environment by using the Managed Object Browser (MOB).

Clean up the vCenter Lookup Service

Use the Managed Object Browser (MOB) to clean up the old vSphere Replication registration in Lookup Service after deleting the vSphere Replication Appliance.

Verify that you have the credentials of a vSphere administrator.

If you delete the vSphere Replication Appliance before you unregister it from the environment, you cannot use the VRMS Appliance Management Interface to unregister vSphere Replication from vCenter Server

- Log in with vCenter Server credentials to `https://<vCenter_Server_address>:443/lookupservice/mob/?moid=ServiceRegistration&method=List&vmobl=1`.

NOTE

If you have external Platform Services Controller (PSC), use the PSC address instead of the vCenter Server address.

- To search for the VRMS registrations, replace the value in the **Value** field with the following text and click **Invoke Method**.

```
<filterCriteria>
<siteId></siteId>
<nodeId></nodeId>
<serviceType>
<product></product>
<type>com.vmware.vr.vrms</type>
</serviceType> <endpointType>
<protocol></protocol>
<type></type>
</endpointType>
</filterCriteria>
```

3. Look for the old VRMS registration and copy its **serviceld** value.
4. Navigate to `https://<vCenter_Server_address>:443/lookupservice/mob/?moid=ServiceRegistration&method=Delete`.
5. To delete the service registration, enter the **serviceld** value and click **Invoke Method**.

Clean up the vCenter Server Extension Manager

Use the Managed Object Browser (MOB) to clean up vSphere Replication from vCenter Extension Manager after deleting the vSphere Replication Appliance.

Verify that you have the credentials of a vSphere administrator.

The procedures on removing the permissions for a service account and on removing a service account from the vCenter Single Sign-On domain are documented in the *vSphere 6.5 Security* document. See topics [Remove Permissions](#) and [Delete vCenter Single Sign-On Solution Users](#).

1. Log in to `https://<vCenter_Server_address>/mob/?moid=ExtensionManager` with vCenter Server credentials.
2. In the extensionList property, click the link for the `com.vmware.vcHms` extension key to check the key details.
3. Verify that the displayed data is for a vSphere Replication appliance that is already lost.
4. In ExtensionManager, click **unregisterExtension**.
5. Enter `com.vmware.vcHms` for the extension key value, and click **Invoke Method**.
6. Verify that the result displays `void` and not an error message.
An error message might appear if the specified extension is not registered, or if an unexpected runtime error occurs.
7. Close the window.
8. Refresh the ExtensionManager page and verify that the extensionList entry does not include `com.vmware.vcHms`.
9. Remove the permissions for the HMS service account from all vCenter Server instances in the Single Sign-On domain.
10. Remove the HMS service account from the vCenter Single Sign-On domain.

You can deploy a new vSphere Replication appliance.

NOTE

If a vSphere Replication appliance is deleted before all replications that it manages are stopped, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing. To prevent errors, you must remove the tags from all target datastores that were used for replications by the deleted vSphere Replication appliance. See [Search and Remove the vSphere Replication Tag from Target Datastores](#).

Participate in the Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

- CEIP participation requires connection from the vSphere Replication virtual appliance to `https://vcsa.vmware.com:443`.
- If the system uses a firewall or a proxy to connect to the Internet, you must specify a firewall or a proxy rule allowing outbound traffic through for `https://vcsa.vmware.com:443/ph/api/*`.
- Verify that you are a member of the `Administrators@vsphere.local` group.

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

You can choose to join the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

1. Log in to the vCenter Server instance as a member of `Administrators@vsphere.local` by using the vSphere Client.
2. On the vSphere Client Home page, under Administration, click **Customer Experience Improvement Program**.
3. To activate the CEIP, click **Join**. To deactivate the CEIP, click **Leave**.

Exporting and Importing Replication Configuration Data

You can use the vSphere Replication 8.8 Configuration Import/Export Tool to export and import configuration data about the replications created in vSphere Replication.

If you plan to migrate vSphere Replication to a different host, you can use the tool to export replication settings and the related objects into an XML file. You can then import the configuration data from the previously exported file.

The vSphere Replication 8.8 Configuration Import/Export Tool creates new outgoing and incoming replications and it does not modify any existing replications. For example, if you export 10 outgoing replications and delete 6 of them, the import operation configures only the six deleted replications. It skips processing the four existing replications.

When you deploy the vSphere Replication appliance, the vSphere Replication 8.8 Configuration Import/Export Tool is also deployed with the appliance. The tool is located in the `/opt/vmware/vr-impex-tool` directory.

Requirements for Using the vSphere Replication 8.8 Configuration Import/Export Tool

- You must have Java 1.8.x installed.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=C:\Program Files\Java\jre1.8.0_152` for Windows, or `JAVA_HOME=/usr/java/jre1.8.0_152` for Linux.

Requirements for Exporting and Importing Replication Groups Configuration Data

- Before you can export a configuration, you must have a site pair with vSphere Replication 8.8.x up and running on both the protected and the recovery site.
- Import is supported in a clean vSphere Replication 8.8.x installation, registered to the same vCenter Server instance or to a vCenter Server instance which contains the same inventory.

Input Parameters Required for Import

- Lookup Service host name. The host name of the Platform Services Controller or the vCenter Server host name, if you are using vCenter Server with an Embedded Platform Services Controller.
- vCenter Single Sign-On administrator user name and password for both sites.

Exported Information

The vSphere Replication 8.8 Configuration Import/Export Tool exports the host folder information, compute resources, network and datastore information, datastore paths, RPO settings, multiple points in time (MPIT), quiescing, network compression, and so on.

Network Requirements

You must verify that the following network ports are open.

Default Port	Target	Description
443	On-premises vCenter Server	vCenter Server HTTPS port
443	On-premises Platform Services Controller / Lookup service	Platform Services Controller HTTPS port
8043	On-premises vSphere Replication	vSphere Replication port

Export Replication Configuration Data

You use the vSphere Replication 8.8 Configuration Import/Export Tool to export replication configuration data in an XML file.

- Verify that you have Java 1.8.x installed and environment variables configured.
 - Verify that you have a site pair with vSphere Replication running on both the protected and the recovery sites.
1. Open a command shell, navigate to `/opt/vmware/vr-impex-tool` directory, and run the following command.

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
```

To make the XML file more human-readable, add the `format` option. Adding the `format` option significantly increases the XML file size.

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive --format
```
 2. Enter the host name or the IP address of the Lookup Service.
 3. Enter the port number or press Enter, if you use the default port.
 4. Accept the SHA Thumbprint.
 5. Enter user name and password for the local vCenter Server instance.
 6. Select a paired vSphere Replication instance.
 7. Enter user name and password for the remote vCenter Server instance.

Example for Export of Outgoing Replications

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:
10.92.228.236
Enter port (or press Enter in case you use the default - 443):

Host 10.92.228.236 has untrusted certificate with SHA-1 Thumbprint:
 63:50:89:60:76:5C:78:C9:B0:1A:A6:B6:D0:08:D7:8E:31:46:BF:A7 .
Accept thumbprint? (y/n):
y
Enter username for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
```

```

administrator@vsphere.local
Enter password for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
Establishing connection...
Available HMS servers:
[0] wdc-rdops-vm08-dhcp-221-15.eng.vmware.com
[1] wdc-rdops-vm09-dhcp-228-236.eng.vmware.com

0
One HMS server found: wdc-rdops-vm09-dhcp-228-236.eng.vmware.com
Enter username for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
administrator@vsphere.local
Enter password for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
Collecting data...
Starting export...
2019-09-03 16:28:14,771 DEBUG - Hms inventory export started.
2019-09-03 16:28:14,993 DEBUG - Replication groups export started.
2019-09-03 16:28:15,627 DEBUG - Hms inventory export ended.
2019-09-03 16:28:23,680 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.

```

Use a Properties File to Export vSphere Replication Configuration Data

You can use a properties file to simplify or automate the export of vSphere Replication configuration data.

- Verify that you have Java 1.8.x installed on the vSphere Replication host machine.
- Verify that you have a site pair with vSphere Replication running on both the protected and the recovery site.
- Prepare an `export_vr_configuration.properties` file. See [Properties for Automated Export and Import of vSphere Replication Configuration Data](#).

Open a command shell, navigate to `/opt/vmware/vr-impex-tool` directory, and run the following command.

```

java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
exportProperties=Path_to_properties_file

```

To make the XML file more human-readable, add the `format` option. Adding the `format` option significantly increases the XML file size.

```

java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
exportProperties=Path_to_properties_file

```

Example of Export with Properties File

```

java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --exportProperties=/opt/
vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-impex-tool/
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***

```

```

Initiating using properties file.

```

```

Establishing connection...

```

```

Collecting data...

```

```

Starting export...

```

```

2019-10-28 07:56:52,529 DEBUG - VR inventory export started.

```

```
2019-10-28 07:56:52,632 DEBUG - Replication groups export started.
```

```
2019-10-28 07:56:52,668 DEBUG - VR inventory export ended.
```

```
2019-10-28 07:56:53,329 DEBUG - Replication groups export ended.
```

```
Writing to file started.
```

```
Writing to file finished.
```

```
Export ended successfully.
```

Import Replication Configuration Data

You can use the vSphere Replication 8.8 Configuration Import/Export Tool to import replication configuration data from a previously exported XML file.

- Provide a clean vSphere Replication installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.
1. Open a command shell, navigate to the folder of the `/opt/vmware/vr-impex-tool` directory, and run the following command.


```
java -jar vr-impex-tool-<version>.jar --importInteractive --
path=Path_toexported_XML_file
```
 2. Optional: To automate the import process by using a `sample.properties` file, run the following command instead.


```
java -jar vr-impex-tool-<version>.jar --importProperties=sample.properties --
path=Path_toexported_XML_file
```
 3. Enter the host name or the IP address of the Lookup Service.
 4. Enter the port number or press Enter, if you use the default port.
 5. Accept the SHA Thumbprint.
 6. Enter user name and password for the local vCenter Server instance.
 7. Select a paired vSphere Replication instance.
 8. Enter user name and password for the remote vCenter Server instance.

The vSphere Replication 8.8 Configuration Import/Export Tool creates replications using the exported XML file.

Example of Importing the Configuration by Using a Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --importProperties=/opt/
vmware/vr-impex-tool/sample.properties --path=/opt/vmware/vr-impex-tool/sample.xml
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating using properties file.
Establishing connection...
Collecting data...
2019-08-23 02:13:10,246 INFO - Importing hms data.
Reading file...
Reading file done.
2019-08-23 02:13:10,636 INFO - Import hms configurables started.
2019-08-23 02:13:11,478 DEBUG - Getting profiles for server with guid 'd83b4ce0-4530-4a45-
b493-5f137598d3f2'.
2019-08-23 02:13:11,510 DEBUG - Getting profiles for server with guid '1c0f9490-3ac3-4546-
af4a-10ab4ee634c7'.
```

```

2019-08-23 02:13:11,525 DEBUG - Starting import of replications.
2019-08-23 02:13:11,619 DEBUG - Importing Replication Group for server with guid
'd83b4ce0-4530-4a45-b493-5f137598d3f2' is complete.
2019-08-23 02:13:13,834 DEBUG - Importing Replication Group for server with guid
'1c0f9490-3ac3-4546-af4a-10ab4ee634c7' is complete.
2019-08-23 02:13:13,834 INFO - Import VR configurables ended. Imported : 2 .
Import ended successfully.

```

Import Large Numbers of Replications

You can use the vSphere Replication 8.8 Configuration Import/Export Tool to import the replication configuration data for over 200 replications. You can import the data from a previously exported XML file.

- Verify that you have Java 1.8.x installed and environment variables configured.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=C:\Program Files\Java\jre1.8.0_152` for Windows, or `JAVA_HOME=/usr/java/jre1.8.0_152` for Linux.
- Verify that you have a site pair with vSphere Replication 8.8.x up and running on both the protected and the recovery site.

When you have an environment with over 200 replications, the replications are spread on more than one vSphere Replication server. After you export the replication configuration data, you must change the exported XML file to balance the replication workload.

1. Copy the exported XML file, so that you have two identical files.
For example, `exported_vr_config.xml` and `exported_vr_config.1.xml`.
2. Open `exported_vr_config.xml` in a text editor and change the replication number to 200 or less.
3. Open `exported_vr_config.1.xml` in a text editor and change the replication number to the remaining replications in your environment.
4. Change the target vSphere Replication server name in `targetHbrServerName` to `vrs-<No.>`.
5. Import `exported_vr_config.xml` that contains 200 replication configurations or less.
6. Deploy a second vSphere Replication server on the target site.
7. Import `exported_vr_config.1.xml`.

Properties for Automated Export and Import of vSphere Replication Configuration Data

You use the vSphere Replication 8.8 Configuration Import/Export Tool properties file to automate the export and import of replication configuration data.

The vSphere Replication 8.8 Configuration Import/Export Tool properties file must follow a specific structure.

Table 5: Parameters for the Properties File

Parameter	Description
<code>lookup.service.address</code>	The local Lookup Service address. For a cloud to cloud pairing, use the internal vCenter Server IP address.
<code>port</code>	The port number for the Lookup Service. The default value is 443 . This parameter is optional.
<code>local.vc.address</code>	The local vCenter Server name.
<code>local.auth.credentials.vc.username</code>	The user name of the local vCenter Server.

Parameter	Description
<code>local.auth.credentials.vc.password</code>	The password for the local vCenter Server.
<code>local.vr.name</code>	The name of the local vSphere Replication Management server. NOTE The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI.
<code>remote.vc.address</code>	The remote vCenter Server name.
<code>remote.auth.credentials.vc.username</code>	The user name for the remote vCenter Server. Required if your environment is not federated.
<code>remote.auth.credentials.vc.password</code>	The password for the remote vCenter Server. Required if your environment is not federated.
<code>remote.vr.name</code>	The name of the remote vSphere Replication Management server. NOTE The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI.

Sample Properties File

```
lookup.service.address=10.193.15.152
local.auth.credentials.vc.username=administrator@vsphere.local
local.auth.credentials.vc.password=
remote.auth.credentials.vc.username=administrator@vsphere.local
remote.auth.credentials.vc.password=
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
```

Syntax of the Import/Export Tool

The vSphere Replication 8.8 Configuration Import/Export Tool includes different options that you can use to import or export configuration data.

Table 6: vSphere Replication 8.8 Configuration Import/Export Tool Options

Option	Description
<code>--export</code>	Required when doing an export. Cannot be used together with <code>--import</code> .
<code>--exportProperties</code>	Used to start an export by using a properties file.
<code>--exportInteractive</code>	Used to start an export interactively with prompts for the required information.
<code>--exportPath</code>	Used to specify the directory in which to create the exported file. When the directory is not specified, the file is exported in the location of the import/export tool.
<code>--importInteractive</code>	Used to start an import interactively with prompts for the required information.

Option	Description
<code>--importProperties</code>	Used to start an import by using a properties file.
<code>--path</code>	Used for importing data. Path to the previously exported file.
<code>--lsp</code>	The Platform Services Controller address. Can be an IP address or FQDN. For vSphere Replication, it must match the <code>lookup.service.address</code> property.
<code>--port <[1, 2147483647]></code>	The port number for the Lookup Service. The default value is 443.
<code>--localVrName</code>	The name of the local vSphere Replication Management server. It must match the <code>local.vr.name</code> property.
<code>--remoteVrName</code>	The name of the remote vSphere Replication Management server. It must match the <code>remote.vr.name</code> property.
<code>--localAuthCredsUsername</code>	The user name for the local vCenter Server.
<code>--localAuthCredsPass</code>	The password for the local vCenter Server.
<code>--remoteAuthCredsUsername</code>	The user name for the remote vCenter Server.
<code>--remoteAuthCredsPass</code>	The password for the remote vCenter Server.
<code>--format</code>	Used to make the exported XML file better formatted and human-readable. The <code>--format</code> option significantly increases the file size.

Sample Commands with Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-impex-tool/
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importProperties=/opt/vmware/vr-impex-tool/sample.properties --path=/opt/vmware/vr-impex-tool/sample.xml
```

Sample Properties File

```
lookup.service.address=10.193.15.152
local.auth.credentials.vc.username=administrator@vsphere.local
local.auth.credentials.vc.password=
remote.auth.credentials.vc.username=administrator@vsphere.local
remote.auth.credentials.vc.password=
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
```

Sample Commands in Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importInteractive --path=Path_to_exported_XML_file
```

Sample of Using Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:10.193.15.152
Enter port (or press Enter in case you use the default - 443):
Host sc2-rdops-vm08-dhcp-15-152.eng.vmware.com has untrusted certificate with SHA-1 Thumbprint:
 82:CF:58:F2:E7:C6:A1:4C:
89:FC:7B:05:31:DD:13:00:28:21:DA:F3 .
Accept thumbprint? (y/n):y
```

```

Enter username for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:administrator@vsphere.local
Enter password for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:
Establishing connection...
Available VR servers:
[0] sc-rdops-vm12-dhcp-109-104.eng.vmware.com
[1] sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
0
One VR server found: sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
Enter username for pair site 'sc-rdops-vm12-dhcp-109-104.eng.vmware.com':administrator@vsphere.lo-
cal
Enter password for pair site 'sc-rdops-vm12-dhcp-109-104.eng.vmware.com':
Collecting data...
Starting export...
2019-10-30 04:21:18,464 DEBUG - VR inventory export started.
2019-10-30 04:21:18,548 DEBUG - Replication groups export started.
2019-10-30 04:21:18,585 DEBUG - VR inventory export ended.
2019-10-30 04:21:19,228 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.

```

Sample of Using Commands without Properties File

```

java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --localVrName=sc2-rdops-
vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-rdops-vm12-dhcp-109-104.eng.vmware.com --
lssp=10.193.15.152 --format --exportPath=/opt/vmware/vr-impex-tool/ --localAuthCredsUsername=ad-
ministrator@vsphere.local --remoteAuthCredsUsername=administrator@vsphere.local --localAuth-
CredsPass=***** --remoteAuthCredsPass=*****

```

Sample of Using Commands without Properties File

```

java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --localVrName=sc2-rdops-
vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-rdops-vm12-dhcp-109-104.eng.vmware.com --
lssp=10.193.15.152 --format --exportPath=/opt/vmware/vr-impex-tool/ --localAuthCredsUsername=ad-
ministrator@vsphere.local --remoteAuthCredsUsername=administrator@vsphere.local --localAuth-
CredsPass=Admin!23 --remoteAuthCredsPass=Admin!23
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Establishing connection...
Collecting data...
Starting export...
2019-10-30 04:28:54,426 DEBUG - VR inventory export started.
2019-10-30 04:28:54,508 DEBUG - Replication groups export started.
2019-10-30 04:28:54,543 DEBUG - VR inventory export ended.
2019-10-30 04:28:55,230 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.

```

Isolating the Network Traffic of vSphere Replication

You can isolate the network traffic of vSphere Replication from all other traffic in a data center's network.

Isolating the replication traffic helps you ensure that sensitive information is not routed to the wrong destination. It also helps you enhance the network performance in the data center, because the traffic that vSphere Replication generates does not impact other types of traffic. Traffic isolation also facilitates monitoring and troubleshooting. You isolate the

network traffic to the vSphere Replication Server by dedicating a VMkernel NIC on each ESXi host on the primary site that sends data to the vSphere Replication Server. See [Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host](#).

NOTE

You cannot enable the vSphere Replication traffic on a custom TCP/IP stack on the ESXi host. vSphere Replication uses the default stack on the ESXi host. To isolate the network traffic, you must use a VMkernel adapter tagging or configure static routes.

If you are using a distributed network switch, you can take advantage of the vSphere Network I/O Control feature to set limits or shares for incoming and outgoing replication traffic on each ESXi host. The feature allows you to manage the network resources that vSphere Replication uses.

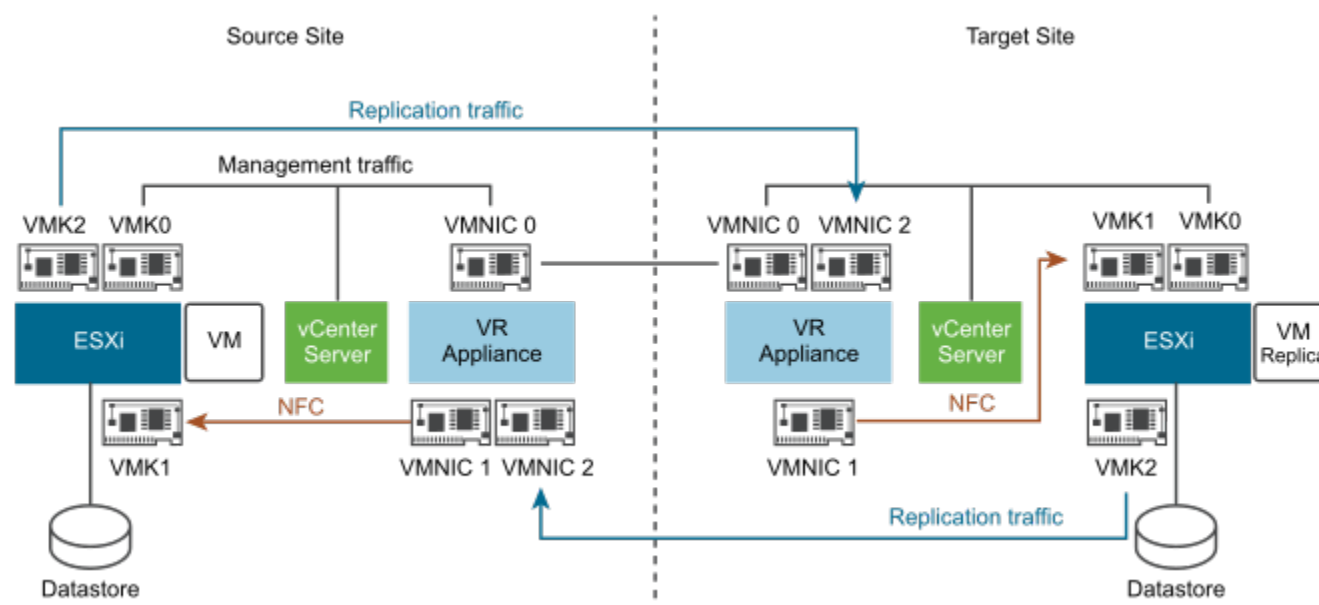
By default, the vSphere Replication appliance has one VM network adapter that is used for various traffic types.

- Management traffic between vSphere Replication Management Server and vSphere Replication Server.
- Replication traffic from the source ESXi hosts to the vSphere Replication Server.
- Traffic between vCenter Server and vSphere Replication Management Server.
- NFC (Network File Copy) traffic, which is the traffic from the vSphere Replication Server appliance at the target site to the destination datastores.

You can add network adapters to the vSphere Replication appliance and use the VRMS Appliance Management Interface to configure a separate IP address to use for each traffic type.

You can isolate the vSphere Replication NFC traffic from the vSphere Replication Server to the target datastore. By default, the NFC traffic is sent to the target ESXi host from the vSphere Replication Server through the management network. You can isolate the NFC traffic from the management traffic by sending it through the replication network. In this case, the vSphere Replication server handles the replication and NFC traffic together, by using the same interface. To isolate the replication and NFC traffic from the management traffic, you must add a second vNIC to separate them. Alternatively, you can add a third vNIC for the NFC traffic only. This option provides security isolation with a dedicated vSphere Replication VLAN for the replication traffic and another one for the NFC traffic, depending on the security requirements in your environment.

Figure 4: vSphere Replication Traffic Isolation



In the vSphere Replication appliance, the IP address that is used for management traffic between the vSphere Replication Management Server and vSphere Replication Server is localhost 127.0.0.1. Therefore, you do not need to add network adapters for this type of traffic.

When the vSphere Replication Management Server and the vSphere Replication Server run on separate appliances, you can specify a non-localhost IP address to be used by the vSphere Replication Management Server.

NOTE

After the IP address of the vSphere Replication server on the target site changes, the replications are automatically reconfigured with the new IP address.

In addition, you must configure the relevant static routes on each ESXi host at the source site to communicate with the target site. For replications to flow in the opposite direction, you must configure reverse routes on the ESXi hosts on the target site. See <https://kb.vmware.com/kb/2001426>. Depending on the complexity of your environment, if you want to isolate the NFC traffic, you must configure the relevant vSphere Replication and NFC vSphere Replication static routes after you configure the VMkernel adapters for vSphere Replication and NFC traffic.

Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host


You create VMkernel adapters to isolate the outgoing replication traffic on source ESXi hosts.

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.
- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

NOTE

To ensure the best possible results, use one VMkernel adapter for one traffic type.

Perform this procedure for every ESXi host that is used as a replication source, and for which you want to isolate the replication traffic.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab and under **Networking**, select **VMkernel adapters**.
3. Click the **Add networking** icon . The **Add Networking** wizard opens.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. On the Select target device page, select a port group or a standard switch and click **Next**.
6. On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

NOTE

vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.

7. Under Available services, select **vSphere Replication** and click **Next**.
8. Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

The VMkernel adapter that you created for outgoing vSphere Replication traffic appears in the list of adapters. The outgoing replication data from the ESXi host is sent to the vSphere Replication server through this adapter.

You can add a vNIC to the vSphere Replication appliance and use the VRMS Appliance Management Interface to configure an IP address to use for incoming replication data.

Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host


You create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts.

- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

NOTE

To ensure the best possible results, use one VMkernel adapter for one traffic type.

Perform this procedure for every ESXi host that is used as a replication target, and for which you want to isolate the replication traffic.

- In the vSphere Client, navigate to the ESXi host.
- Click the **Configure** tab and under **Networking**, select **VMkernel adapters**.
- Click the **Add networking** icon . The **Add Networking** wizard opens.
- On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
- On the Select target device page, select a port group or a standard switch and click **Next**.
- On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

NOTE

vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.

- Under Available services, enable the service for either **vSphere Replication**, **vSphere Replication NFC**, or both on the dedicated vSphere Replication VMkernel adapter.
- Click **Next**.
- Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

The VMkernel adapter that you tagged for NFC traffic appears in the list of adapters. The vSphere Replication Server routes the replication data to the adapter, and the ESXi host saves the data to a datastore.

- Apply the configuration of the VMkernel Adapters for each ESXi host in your environment.
- Configure the relevant static routes on each ESXi host at the source site to communicate with the target site. For replications to flow in the opposite direction, you must configure reverse routes on the ESXi hosts on the target site. See <https://kb.vmware.com/kb/2001426>. Depending on the complexity of your environment, if you want to isolate the NFC traffic, you must configure the relevant vSphere Replication and NFC vSphere Replication static routes after you configure the VMkernel adapters for vSphere Replication and NFC traffic.

Create a VM Network Adapter to Use for Incoming Replication Traffic on the Combined vSphere Replication Appliance

By default, the combined vSphere Replication appliance has one VM network adapter. You can add a second adapter to the appliance, and configure vSphere Replication to use the second adapter only for the incoming replication traffic.

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.
- Make a note of the IP address of the VM network adapter.

The IP address that is used for the vSphere Replication management traffic is localhost 127.0.0.1. The default VM network adapter is used by the vSphere Replication server for the replication traffic, and for managing the add-on replication servers. Use the following procedure to add a second adapter to the vSphere Replication appliance only for the incoming replication traffic.

NOTE

The IP configuration via the VRMS Appliance Management Interface supports only one default gateway on the vSphere Replication appliance. To configure a static route on an additional NIC, see [Configure a Static Route on an Additional VM Network Adapter](#).

1. Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.
 - a) Right-click the VM and select **Edit Settings**.
 - b) From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, click **Network Adapter**.
The new network adapter appears in the list of devices at the right.
 - c) Expand the properties of the new network adapter to verify that **Connect At Power On** is selected.
You can assign a static MAC address or leave the text box empty to obtain a MAC address automatically.
 - d) Click **OK** to close the Edit Setting dialog box.
2. Power on the vSphere Replication appliance.
3. From the **Summary** tab of the vSphere Replication appliance, take a note of the IP address of the new network adapter.
You can click **View all xx IP addresses** to see the IP address of the new NIC.
4. (Optional) If you need to configure a static route on the new NIC, see [Configure a Static Route on an Additional VM Network Adapter](#).
5. Use a supported browser to log in to the VRMS Appliance Management Interface .
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.

NOTE

After powering on the vSphere Replication, the VRMS Appliance Management Interface address might change to the new network adapter's IP address.

6. Click **Networking** and verify that the additional NIC is properly configured as IPv4 or IPv6.
7. Restart the vSphere Replication appliance to change the NIC status to UP in the VRMS Appliance Management Interface.
The new NIC can now obtain and reserve the new IP address.
8. Click **Summary**, then click **Change**.
9. In the **IP Address for Incoming Storage Traffic** text box, enter the IP address of the new network adapter that you added and click **Save**.

The vSphere Replication appliance uses the IP address that you assigned only for the incoming replication traffic.

Create VM Network Adapters to Isolate the Network Traffic of an Additional vSphere Replication Server

By default, the vSphere Replication Server appliance has one VM network adapter. You can add network adapters to the appliance and configure vSphere Replication to use a separate adapter for each traffic type.

- Verify that you have deployed the vSphere Replication Server appliance in your environment and that it is registered as a vSphere Replication Server in the vSphere Client.
- Verify that you have at least one additional vSphere Replication server in your environment.

The default VM network adapter is used by the vSphere Replication Server for management and replication traffic. Use the following procedure to add a second adapter to the vSphere Replication appliance for each traffic type.

NOTE

The IP configuration via the VRMS Appliance Management Interface supports only one default gateway on the vSphere Replication appliance. To configure a static route on an additional NIC, see [Configure a Static Route on an Additional VM Network Adapter](#).

1. Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.
 - a) Right-click the VM and select **Edit Settings**.
 - b) From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, click **Network Adapter**.
The new network adapter appears in the list of devices at the right.
 - c) Optional: If you want to isolate the NFC traffic from the replication traffic, click **Add** again to add another VM NIC to handle the NFC traffic separately.
The first network adapter must be attached to the replication traffic port group and the other network adapter is for the NFC traffic port group.
 - d) To verify that **Connect At Power On** is selected, expand the properties of the new network adapter or adapters, if you want to isolate the NFC from the replication traffic.
You can assign a static MAC address or leave the text box empty to obtain an IP address automatically.
 - e) Click **OK** to close the Edit Setting dialog box.
2. Power on the vSphere Replication appliance.
3. From the **Summary** tab of the vSphere Replication appliance, take note of the IP address of the new network adapters.
You can click **View all xx IP addresses** to see the IP addresses of the new VM NICs.
4. (Optional) If you need to configure a static route on the new NIC, see [Configure a Static Route on an Additional VM Network Adapter](#).
5. Use a supported browser to log in to the VRMS Appliance Management Interface of an additional vSphere Replication server.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
6. Click **Networking** and verify that the additional NIC is properly configured as IPv4 or IPv6.
7. Restart the vSphere Replication appliance to change the NIC status to UP in the VRMS Appliance Management Interface.
The new NIC can now obtain and reserve the new IP address.
8. Click on **Summary**, then click **Change**.
9. Enter the IP addresses of the new VM NICs that you want to use to isolate the network traffic of vSphere Replication.

Option	Description
IP Address for Incoming Storage Traffic	The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data.
IP Address for VRMS Management Traffic	The IP address of a VM NIC to be used by the vSphere Replication Management Server to manage the vSphere Replication Server.

10. Click **Apply Network Settings**.

Separate NICs handle the different types of traffic that vSphere Replication generates.

Configure a Static Route on an Additional VM Network Adapter

To manage replication traffic by using an additional VM NIC, you must configure a static route for the VM NIC.

- Verify that you have added a new VM NIC.
 - Make a note of the number of the new VM NIC.
1. Establish an SSH connection to the vSphere Replication appliance.
 2. To locate the network configuration file, navigate to `/etc/systemd/network`.
 3. Open the `10-eth<NIC_Number>.network` file in a text editor and update it.
 - a) Navigate to the `[Route]` section.
If you are unable to locate this section in the configuration file, you can manually add it.
 - b) Set the `Gateway` parameter to the IP address of the next gateway through which the target network can be reached.
 - c) Set the `Destination` parameter to Classless Inter-Domain Routing (CIDR) notation for the IP range of the target network.
 4. Restart the `systemd-networkd` service by running the `systemctl restart systemd-networkd` command.
 5. Validate the static route by running the `ip r` command for IPv4 or the `ip -6 r` command for IPv6.
 - a) (Optional) If you are not able to validate the route, the network is inaccessible. To force the kernel routing table to accept the network, set the `GatewayOnLink` parameter to `yes` in the `[Route]` section.
 - b) (Optional) Restart the `systemd-networkd` service by running the `systemctl restart systemd-networkd` command.

```
[Route]
Gateway=10.71.239.253
Destination=10.71.232.0/21
```

Deploying Additional vSphere Replication Servers

Depending on replication traffic, you might need to deploy one or more additional vSphere Replication servers.

Deploy an Additional vSphere Replication Server

The vSphere Replication appliance includes a vSphere Replication server. However, you might need to deploy multiple vSphere Replication servers to meet your load-balancing needs.

- Deploy vSphere Replication appliances on the source and target sites.
- Deploy vSphere Replication servers on a network that allows them to communicate with the vSphere Replication appliances on the source and target sites.
- Verify that the vSphere Replication servers can communicate with the ESXi Server instances on the source site that hosts the replicated virtual machines.

You can deploy multiple vSphere Replication servers to route traffic from source hosts to target datastores without traveling between different sites managed by the same vCenter Server. You cannot deploy a second management server on the same vCenter Server.

For information about the loads that a vSphere Replication management server and a vSphere Replication server can support, see <https://kb.vmware.com/s/article/2102453>.

1. Log in to the vSphere Client on the site where you want to deploy the additional vSphere Replication server.
2. On the home page, select **Hosts and Clusters**.
3. Right-click on a data center, host or cluster, and select **Deploy OVF Template**.
4. Provide the location of the OVF file from which to deploy the additional vSphere Replication server, and click **Next**.
 - Select **URL** and provide the URL to deploy the appliance from an online URL.
 - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_AddOn_OVF10.ovf`, `vSphere_Replication_AddOn_OVF10.cert`, `vSphere_Replication_AddOn_OVF10.mf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files. Make sure that you do not select the `vSphere_Replication_OVF10.ovf` file.
5. Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**. You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.
6. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
7. Review the virtual appliance details and click **Next**.
8. Select a destination datastore and disk format for the virtual appliance and click **Next**.

Encrypting the additional vSphere Replication server VM is not necessary to replicate encrypted VMs with vSphere Replication.
9. Set the network properties. Select DHCP or set a static IP address.

You can change network settings after deployment in the VRMS Appliance Management Interface.
10. Enter a password for the appliance.

The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
11. Review your settings and click **Finish**.
12. Power on the vSphere Replication appliance.

When the OVF file has deployed, register the vSphere Replication server with the vSphere Replication appliance.

Register an Additional vSphere Replication Server

After you deploy additional vSphere Replication servers, you must register these servers with the vSphere Replication appliance to enable them as traffic handlers at the recovery site.

- Verify that the vSphere Replication appliance is deployed and configured.
- Verify that an additional vSphere Replication Server is deployed.

NOTE

You can register additional vSphere Replication servers that run within the same vSphere environment.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. On the **Site Pair** tab, select **Configure > Replication Servers**.
5. Click the **Register** icon.
6. From the list, select a virtual machine that is a working vSphere Replication server and click **Select**.

The newly registered vSphere Replication server appears in the list of vSphere Replication servers.



If you want to isolate the network traffic of vSphere Replication, see [Isolating the Network Traffic of vSphere Replication](#).

Replication Server Connection States

You can view the states of the connections with the replication servers and determine if they need a remediation.

The following table lists the states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 7: Replication Server Connection States

Icon	Status	Description	Remediation
	Connected	The connection between the source replication server and the target replication server is working properly.	Not needed.
	Disconnected	<ul style="list-style-type: none"> • The SSL certificate on the remote replication server has been changed. • The network connection between the source site and the target site is not functioning properly, or the remote site is offline. 	<ul style="list-style-type: none"> • Click the Reconnect icon. • Verify that the replication server has network connectivity.

Reconfigure vSphere Replication Server Settings

The vSphere Replication appliance contains a vSphere Replication server. If you deploy additional vSphere Replication servers, the server settings are established during deployment. You can modify the settings after you deploy the server.

Verify that the additional vSphere Replication server is powered on.

A vSphere Replication server does not require additional configuration through the VRMS Appliance Management Interface after deployment. To increase security, you can change the root password of the vSphere Replication server

and install a new certificate. You can use a self-signed certificate, which provides public-key based encryption and authentication, however it does not provide the level of assurance offered when you use a certificate signed by a certificate authority.

You can also reconfigure the network settings for the vSphere Replication server virtual appliance.

NOTE

vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

1. Use a supported browser to log in to the VRMS Appliance Management Interface of the additional vSphere Replication Server that you deployed.

The URL for the VRMS Appliance Management Interface is `https://vr-server-address:5480`.

Use the root password that you set when you deployed the vSphere Replication server.

2. Optional: Click **Certificates**, then click **Change**.
3. Optional: Select a certificate type.

Menu item	Description
Generate a self-signed certificate	<p>Use an automatically generated certificate.</p> <ol style="list-style-type: none"> 1. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2. Accept the default FQDN and IP values. <p>NOTE Using self-signed certificate is not recommended for production environments.</p>
Use a PKCS #12 certificate file	<p>Use a custom certificate.</p> <ol style="list-style-type: none"> 1. Click Browse, navigate to the certificate file, and click Open. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2. Enter the optional private key encryption password.
Use a CA-signed certificate generated from CSR	<p>Use a CA-signed certificate generated from a CSR.</p> <ol style="list-style-type: none"> 1. In the Certificate file row, click Browse, navigate to the certificate file, and click Open. 2. In the CA chain row, click Browse, navigate to the CA chain, and click Open.

4. Optional: Click **Change**.
5. Optional: To change the password for the vSphere Replication server, click **Access** and then **VRMS appliance password > Change**.
6. Optional: To change the network settings, click **Networking**, and then **Edit**.
7. Optional: Configure the DNS settings in the **Hostname and DNS** pane.

Menu Item	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.

Menu Item	Description
Enter DNS settings manually	Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server.

8. Optional: In the **eth0** pane, select the IPv4 or the IPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

Option	Description
Obtain IPv4 settings automatically	Obtains the IP address for the appliance from the network.
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. <ol style="list-style-type: none"> 1. Enter the IPv4 address 2. Enter subnet prefix length. 3. Enter the default IPv4 gateway.

- Configure the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically using DHCP	Assigns IPv6 addresses to the appliance from the network by using DHCP. <p>NOTE To apply this setting, you must restart the vSphere Replication Appliance.</p>
Obtain IPv6 settings automatically using router advertisement	Assigns IPv6 addresses to the appliance from the network by using router advertisement.
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. <ol style="list-style-type: none"> 1. Enter the IPv6 address and the subnet prefix length in the address box. 2. To enter additional IPv6 addresses, click Add. 3. Enter the default IPv6 gateway.

9. Optional: Click **Save**.

10. Optional: To restart the vSphere Replication service, click **Services > hms > Restart**.

11. Optional: To reboot the vSphere Replication server appliance, click **Summary** and click **Restart**.

Unregister and Remove a vSphere Replication Server

If you deployed additional vSphere Replication server instances that you no longer require, you must unregister them from the vSphere Replication appliance before you delete them.

Verify that the vSphere Replication server that you want to unregister does not serve any replications, otherwise the operations fails.

1. On the Site Recovery home page, select a site pair and click **View Details**.
2. On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.

3. Select the server and click the **Unregister** icon.
4. In the **Hosts and Clusters** view of the vSphere Client, power off and delete the vSphere Replication server virtual machine.

Deactivate the Embedded vSphere Replication Server

The vSphere Replication appliance includes an embedded vSphere Replication Server by default. If you want to deactivate the embedded vSphere Replication server, you can do so using SSH.

Verify that no replications are using the embedded server. Stop the replications or move them to a different server.

1. Use SSH into the vSphere Replication appliance and enter:

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-embedded-hbr=false
```

2. Restart the HMS service.

```
# service hms restart
```

3. Unregister the embedded vSphere Replication server from the **Replication Servers** view.

- a) On the Site Recovery home page, select a site pair and click **View Details**.
- b) On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.

- c) Select the server and click the **Unregister** icon.

Rebooting vSphere Replication does not automatically register the embedded server. To restore the default behavior to register automatically the embedded vSphere Replication server, enter:

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-embedded-hbr=true
# service hms restart
```

Use the OVF Tool to Deploy an Additional vSphere Replication Server

You can use the VMware OVF tool to deploy an additional vSphere Replication server from an OVF template.

- Verify that you have downloaded and mounted the vSphere Replication .iso image.
- Verify that you have downloaded and installed on your computer the VMware OVF tool 4.2 or later.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about `ovftool`, see the [OVF Tool Documentation](#).

1. To deploy an additional vSphere Replication server with the VMware OVF Tool, use one of the following command lines.

- If you want to obtain network settings through DHCP:

```
ovftool
-ds="DATASTORE NAME"
-n="VIRTUAL MACHINE NAME"
--net:"Management Network"="NETWORK NAME"
--prop:"varoot-password"="ROOT USER PASSWORD"
--prop:"vaadmin-password"="ADMIN USER PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
${VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=${ESX_HOST_NAME}
```

- If you want to obtain network settings through a static IP address:

```
ovftool
-ds="DATASTORE NAME"
-n="SERVER NAME"
```

```

--net:"Management Network"="NETWORK NAME"
--prop:"varoot-password"="ROOT USER PASSWORD"
--prop:"vaadmin-password"="ADMIN USER PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
--prop:"vami.ip0.vSphere_Replication_Appliance"="IP ADDRESS"
--prop:"vami.netmask0.vSphere_Replication_Appliance"="SUBNET MASK"
--prop:"vami.gateway.vSphere_Replication_Appliance"="GATEWAY IP ADDRESS"
--prop:"vami.DNS.vSphere_Replication_Appliance"="DNS IP ADDRESSES"
--prop:"vami.searchpath.vSphere_Replication_Appliance"="DOMAIN SEARCH PATH"
--ipAllocationPolicy="fixedPolicy"
${VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=${ESX_HOST_NAME}

```

2. Replace the variables in the example with values from your environment.

Variable	Description
<i>DATASTORE NAME</i>	The target datastore name.
<i>VIRTUAL MACHINE NAME</i>	Specify the additional vSphere Replication Server name.
<i>NETWORK NAME</i>	The name of the network to which you attach the additional vSphere Replication server.
<i>ROOT USER PASSWORD</i>	The password for the <code>root</code> account. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
<i>ADMIN USER PASSWORD</i>	The password for the <code>root</code> account, which you use to log in to the vSphere Replication Server. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
<i>NTP SERVER IP OR FQDN</i>	The IP address or FQDN of the NTP server.
<i>SUBNET MASK</i>	The subnet mask address of the additional vSphere Replication Server.
<i>GATEWAY IP ADDRESS</i>	The Gateway address to the additional vSphere Replication Server.
<i>DNS IP ADDRESSES</i>	The DNS address of the additional vSphere Replication Server.
<i>DOMAIN SEARCH PATH</i>	The domain search path for this virtual machine (use a comma or a space to separate the different names.)
<i>VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH</i>	The path to the vSphere Replication Add-On OVF package. To get access to the vSphere Replication OVF files, navigate to the <code>\bin</code> directory in the ISO image.
<i>VSPHERE_USER</i>	The user name for the target vCenter Server.
<i>VSPHERE_USER_PASSWORD</i>	The password for the target vCenter Server.
<i>VCENTER_SERVER_ADDRESS</i>	The address of the target vCenter Server.
<i>ESX_HOST_NAME</i>	The name of the target ESX host.

When the OVF file has deployed, register the vSphere Replication server with the vSphere Replication appliance.

Upgrading vSphere Replication

You upgrade the vSphere Replication appliance and any additional vSphere Replication servers by using a downloaded ISO image and the VRMS Appliance Management Interface.

NOTE

If you uncomment any of the configurations in `/etc/vmware/hbrsrv.xml`, regardless if you change the configuration value, the value remains the same after you upgrade vSphere Replication.

vSphere Replication Upgrade Scenarios

You use the ISO file and the VRMS Appliance Management Interface to upgrade from vSphere Replication 8.6.x or 8.7.x to vSphere Replication 8.8. For the full list of supported upgrade paths, see the *Compatibility Matrices for vSphere Replication 8.8.x* at <https://docs.vmware.com/en/vSphere-Replication/8.8/rn/compatibility-matrices-for-vsphere-replication-88/index.html>.

Order of Upgrading vSphere and vSphere Replication Components

There are alternative strategies for the upgrade of vSphere Replication sites.

You can upgrade all components of one of your sites before upgrading all components on the other site. It is best practice to upgrade the vSphere Replication components before the Platform Services Controller and the vCenter Server components.

An alternative strategy is to upgrade the vSphere Replication components on both sites before upgrading the Platform Services Controller appliances and vCenter Server components.

You can upgrade the ESXi hosts at any time.

IMPORTANT

- In an Enhanced Linked Mode environment, do not upgrade vSphere Replication under more than one vCenter Server instance at the same time.
- To avoid replication failures, you must restart the HMS service after you upgrade the vCenter Server components.

Upgrading vSphere Replication by Sites

By upgrading the protected site first, you can perform a disaster recovery on the recovery site if you encounter problems during the upgrade that render the protected site unusable.

NOTE

To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

1. Upgrade any additional vSphere Replication server deployments on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.
4. (Optional) Upgrade the ESXi host on the protected site
5. Upgrade any additional vSphere Replication server deployments on the recovery site.
6. Upgrade the vSphere Replication appliance on the recovery site.
7. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.
8. (Optional) Upgrade the ESXi host on the recovery site.
9. Verify the connection between the vSphere Replication sites.
10. (Optional) Upgrade the virtual hardware of the virtual machines on the ESXi hosts if there is a specific reason for the upgrade.

Upgrading vSphere Replication by Components

With this strategy, you can decide when to upgrade certain components. For example, you can delay the upgrade of the Platform Services Controller appliances and vCenter Server components or the ESXi hosts. Verify which new functionalities are available with earlier versions of vCenter Server.

NOTE

To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

1. Upgrade any additional vSphere Replication server deployments on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. Upgrade any additional vSphere Replication server deployments on the recovery site.
4. Upgrade the vSphere Replication appliance on the recovery site.
5. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.
6. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.
7. (Optional) Upgrade the ESXi host on the protected site.
8. (Optional) Upgrade the ESXi host on the recovery site.
9. Verify the connection between the vSphere Replication sites.
10. (Optional) Upgrade the virtual hardware of the virtual machines on the ESXi hosts if there is a specific reason for the upgrade.

Upgrade Additional vSphere Replication Servers

If you want to upgrade the additional vSphere Replication servers, you must use a downloadable ISO image. To ensure a successful upgrade, follow the sequence of instructions.

- Download the `VMware-vSphere_Replication-8.8.x.x-build_number.iso` image from the vSphere Downloads page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vSphere Replication.
 - Verify that you are currently running vSphere Replication 8.6.x or later.
1. In the vSphere Client, right-click the vSphere Replication Additional Server virtual machine and select **Edit Settings**.
 2. Required: On the **Virtual Hardware** tab, select **Memory** and increase the memory size to 12 GB.
 3. On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
 4. Navigate to the ISO image in the datastore.
 5. For **File Type**, select **ISO Image** and click **OK**.
 6. Follow the prompts to add the CD/DVD drive to the vSphere Replication Additional Server virtual machine.
 7. In a Web browser, log in to the VRS Appliance Management Interface.
The URL for the VRS Appliance Management Interface is `https://vrs_appliance_address:5480`.
 8. Click the **Update** tab, and click **Edit**.
 9. Select **Use CD-ROM** and click **OK**.
The appliance version appears in the list of available updates.
 10. In the **Available updates** pane, click **Install**.
 11. Accept the End-User License Agreement and click **Install**.
After the update is complete, the appliance restarts.
 12. Login to the VRS Appliance Management Interface as admin and verify that the version is 8.8.0.
- Upgrade the vSphere Replication appliance. See [Upgrade vSphere Replication Appliance](#).

Upgrade vSphere Replication Appliance

If you are using vSphere Replication 8.6.x or later you can directly upgrade to version 8.8.

- Download the `VMware-vSphere_Replication-8.8.x.x-build_number.iso` image from the vSphere Downloads page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vSphere Replication.
 - Verify that you are currently running a version, which allows you to upgrade directly to vSphere Replication 8.8.
 - You can directly upgrade to vSphere Replication 8.8, only if the version of vSphere Replication you currently run is 8.6.x or later.
1. In the vSphere Client, right-click the vSphere Replication virtual machine and select **Edit Settings**.
 2. Required: On the **Virtual Hardware** tab, select **Memory** and increase the memory size to 12 GB.
 3. On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
 4. Navigate to the ISO image in the datastore.
 5. For **File Type**, select **ISO Image** and click **OK**.
 6. Follow the prompts to add the CD/DVD drive to the vSphere Replication virtual machine.
 7. In a Web browser, log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr_appliance_address:5480`.
 8. Click the **Update** tab, and click **Edit**.
 9. Select **Use CD-ROM** and click **OK**.
The appliance version appears in the list of available updates.
 10. In the **Available updates** pane, click **Install**.
 11. Accept the End-User License Agreement and click **Install**.
After the update is complete, the appliance restarts.
 12. Login to the VRMS Appliance Management Interface as admin and verify that the version is 8.8.0.
 13. Click **Reconfigure**.
 14. Follow the prompts, provide the required information, and click **Finish**.
- You might need to re-enable the SSH connections. See [Unable to Establish an SSH Connection to the vSphere Replication Appliance](#).
 - If your infrastructure uses more than one vSphere Replication Server, you must upgrade all vSphere Replication Server instances to version 8.8 on the on-premises site.
 - If you plan to upgrade the vCenter Server next, you must restart the HMS service after you upgrade the vCenter Server components.

Update the vCenter Server IP Address in the vSphere Replication Management Server

If during the upgrade process of vCenter Server and the vSphere Replication appliance you changed the vCenter Server certificate or IP address, you must perform additional steps.

Verify that the vCenter Server and vSphere Replication components are upgraded. For more information, see [Order of Upgrading vSphere and vSphere Replication Components](#).

To update the vCenter Server certificate, see [vSphere Replication Is Inaccessible After Changing vCenter Server Certificate](#).

You must update the IP address in the vSphere Replication Management Server when the vCenter Server uses a DHCP address that changed during the upgrade and the vSphere Replication Management Server is configured to use the vCenter Server IP address and not FQDN.

If vCenter Server uses a static IP address, it preserves the IP address by default after upgrade.

1. Power off the vSphere Replication appliance and power it on to retrieve the OVF environment.
2. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
3. Click **Summary**, and click **Reconfigure**.
4. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.
5. If prompted, click **Connect** to verify the Platform Services Controller certificate.
6. On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.
7. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.
8. On the **Ready to Complete** page, review your settings and click **Finish**.

Reconfiguring the vSphere Replication Appliance

If necessary, you can reconfigure the vSphere Replication appliance settings by using the VRMS Appliance Management Interface.

You provide the settings for the vSphere Replication appliance in the **Deploy OVF** wizard when you deploy the appliance. If you selected automatic configuration of the appliance using an embedded database, you can use the vSphere Replication appliance immediately after deployment. If necessary, you can modify the configuration settings of the vSphere Replication appliance after you deploy it.

Reconfigure General vSphere Replication Settings

You can use vSphere Replication immediately after you deploy the vSphere Replication appliance. If necessary, you can reconfigure the general settings after deployment in the VRMS Appliance Management Interface.

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

The general settings of the vSphere Replication appliance include:

- The name and IP address of the vSphere Replication appliance
- The address and port of the vCenter Server instance to which it connects
- An administrator email address

You can change the general settings from the default values in the VRMS Appliance Management Interface.

For example, you can reconfigure the address of the vSphere Replication appliance if you did not specify a fixed IP address when you deployed the appliance, and DHCP changes the address after deployment. Similarly, you can update the address of the vCenter Server instance if the address changes after deployment.

1. Log in to the VRMS Appliance Management Interface as admin.
2. Click **Summary**, and click **Reconfigure**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register vSphere Replication.
PSC port	Accept the default value of 443, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the Platform Services Controller certificate.
5. On the **vCenter Server** page, click **Next**.
After the initial configuration of the vSphere Replication Appliance, you cannot select a different vCenter Server instance.
6. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

Menu Item	Description
Site name	A name for this vSphere Replication site, which appears in the vSphere Replication interface. The vCenter Server address is used by default. Use a different name for each vSphere Replication instance in the pair.
Administrator email	The email address of the vSphere Replication administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for vSphere Replication events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the vSphere Replication Appliance detects is not the interface that you want to use. NOTE To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

Menu Item	Description
Extension ID	The unique identifier of the vSphere Replication Appliance. The Extension ID is not customizable.
Storage Traffic IP	The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data.

7. On the **Ready to Complete** page, review your settings and click **Finish**.
8. To configure the vSphere Replication Appliance on the target site, repeat the procedure.

You reconfigured the general settings of the vSphere Replication appliance.

Change the Password of the vSphere Replication Appliance

You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the VRMS Appliance Management Interface.

- Verify that the vSphere Replication appliance is powered on.
 - Verify that you have administrator privileges to configure the vSphere Replication appliance.
1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
 2. Enter the admin user name and password for the appliance.
You configured the admin password during the OVF deployment of the vSphere Replication appliance.
 3. Click **Access** and go to **VRMS appliance password > Change**.
 4. Enter the current password in the **Current Password** text box.
 5. Enter the new password in the **New Password** and the **Confirm New Password** text boxes.
The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
 6. Click **Change** to change the password.

Change the Keystore Passwords of the vSphere Replication Appliance

To increase security, you can change the passwords of the vSphere Replication appliance keystore. If you copy the keystores from the appliance to another machine, you must change the passwords before the copy operation.

The keystore passwords might be stored in an access restricted configuration file. vSphere Replication has the following keystores:

- `/opt/vmware/hms/security/hms-keystore.jks`, which contains the vSphere Replication appliance private key and certificate.
 - `/opt/vmware/hms/security/hms-truststore.jks`, which contains additional CA certificates besides the ones that Java already trusts.
1. To change the password for the `hms-keystore.jks` keystore, open the remote console of your vSphere Replication virtual machine and log in as root.
 2. Obtain the current keystore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep keystore
```

Example of the output `hms-keystore-password = old_password`

3. Change the keystore password.

```
# /usr/java/default/bin/keytool -storepasswd -storepass old_password -new new_password -keystore /opt/vmware/hms/security/hms-keystore.jks
```

4. Change the vSphere Replication appliance private key password.

The following command is a long, single command and must be run at once. There are breaks in the command for better visibility. Verify that the command returns a success message.

```
# /usr/java/default/bin/keytool -keypasswd -alias jetty -keypass old_password -new new_password -storepass new_password -keystore /opt/vmware/hms/security/hms-keystore.jks
```

5. Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property 'hms-keystore-password=new_password'
```

6. Update the tomcat server.xml file with the new password.

```
sed -i 's/old_password/new_password/g' /var/opt/apache-tomcat/webapps/dr/WEB-INF/classes/h5dr.properties
```

7. Reboot the appliance for the changes to take effect.

```
# reboot
```

8. Use a supported browser to log in to the VRMS Appliance Management Interface.

The URL for the VRMS Appliance Management Interface is <https://vr-appliance-address:5480>.

9. Click **Configure**, and click **Restart**.

If you want to change the truststore passwords of the vSphere Replication appliance, see [Change the Truststore Passwords of the vSphere Replication Appliance](#).

Change the Truststore Passwords of the vSphere Replication Appliance

To increase security, you can change the passwords of the vSphere Replication appliance truststore.

The truststore passwords might be stored in an access restricted configuration file.

1. To change the password for the hms-truststore.jks keystore, open the remote console of your vSphere Replication virtual machine and log in as root.

2. Obtain the current truststore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep truststore
```

Example of the output: hms-truststore-password = *old_password*

3. Change the truststore password.

The following command is a long, single command and must be run at once. There are breaks in the command for better visibility. Verify that the command returns a success message.

```
# /usr/java/default/bin/keytool -storepasswd -storepass old_password -new new_password -keystore /opt/vmware/hms/security/hms-truststore.jks
```

4. Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property 'hms-truststore-password=new_password'
```

5. Restart the vSphere Replication service.

```
# service hms restart
```

If you want to change the keystore passwords of the vSphere Replication appliance, see [Change the Keystore Passwords of the vSphere Replication Appliance](#).

Activate or Deactivate SSH Access to the vSphere Replication Appliance

You can use the VRMS Appliance Management Interface to edit the appliance SSH access settings.

You can activate or deactivate an SSH access to the appliance only for the `admin` account.

1. Log in to the VRMS Appliance Management Interface as `admin`.
2. Click the **Access** tab.
3. In the **SSH** pane, click **Enable** or **Disable**.

Change the SSL Certificate of the vSphere Replication Appliance

You can change the initial vSphere Replication SSL certificate by generating a new self-signed certificate or uploading an SSL certificate signed by a trusted Certificate Authority.

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

vSphere Replication generates a standard SSL certificate when the appliance first boots and registers with vCenter Server. The vSphere Replication self-signed certificate expires after five years from the first boot of the appliance. When your certificate is due to expire in 30 days, you see a warning under **Issues** on the **Site Pair** tab of vSphere Replication. The default certificate policy uses trust by thumbprint.

You can change the SSL certificate, for example if your company's security policy requires that you use trust by validity and thumbprint or a certificate signed by a certification authority. You change the certificate by using the VRMS Appliance Management Interface of the vSphere Replication appliance. For information about the SSL certificates that vSphere Replication uses, see [vSphere Replication Certificate Verification](#) and [Requirements When Using a Public Key Certificate with vSphere Replication](#).

See [vSphere Replication Certificate Verification](#) for details on how vSphere Replication handles certificates.

1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
2. Enter the admin user name and password for the appliance.
You configured the admin password during the OVF deployment of the vSphere Replication appliance.
3. Click **Certificates**.
4. Optional: To enforce verification of a certificate validity, see [How to Activate the Verification of Certificate Validity](#).
5. Click on **Change**.

Menu item	Description
Generate a self-signed certificate	Use an automatically generated certificate. <ol style="list-style-type: none"> 1. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2. Accept the default FQDN and IP values. <p>NOTE Using a self-signed certificate is only recommended for non-production environments.</p>
Use a PKCS #12 certificate file	Use a custom certificate. <ol style="list-style-type: none"> 1. Click Browse, navigate to the certificate file, and click Open. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2. Enter the optional private key encryption password.

Menu item	Description
Use a CA-signed certificate generated from CSR	Use a CA-signed certificate generated from a CSR. <ol style="list-style-type: none"> 1. In the Certificate file row, click Browse, navigate to the certificate file, and click Open. 2. In the CA chain row, click Browse, navigate to the CA chain, and click Open.

6. Click **Change**.
7. Restart the **vSphere Replication** appliance.

You changed the SSL certificate and optionally changed the security policy to use trust by validity and certificates signed by a certificate authority.

NOTE

If you change a certificate on one of the source or target sites, the connection status to this site changes to *Connection issue*. In the vSphere Client, you can check the list of target sites under **vSphere Replication** on the **Manage** tab, and reconnect the sites.

How to Activate the Verification of Certificate Validity

Activate the verification of the certificate validity by activating vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority.

When you activate vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, vSphere Replication refuses to communicate with a server with an invalid certificate. You cannot use a self-signed certificate if you activate vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority.

NOTE

If you reconfigure vSphere Replication through the VRMS Appliance Management Interface after you activate the verification of certificate validity, the verification gets deactivated and you must activate it again.

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Run the following command: `/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-trust-mode=0`.
3. Restart the HMS Service.

vSphere Replication Certificate Verification

vSphere Replication verifies the certificates of vCenter Server and remote vSphere Replication servers.

All communication between vCenter Server, the local vSphere Replication appliance, and the remote vSphere Replication appliance goes through a vCenter Server proxy at port 80. All SSL traffic is tunneled.

vSphere Replication can trust remote server certificates either by verifying the validity of the certificate and its thumbprint or by verifying the thumbprint only. The default is to verify by thumbprint only. You can activate the verification of the certificate validity. See [How to Activate the Verification of Certificate Validity](#).

Thumbprint Verification

vSphere Replication checks for a thumbprint match. vSphere Replication trusts remote server certificates if it can verify the thumbprints through secure vSphere platform channels or, in some rare cases, after the user confirms them. vSphere Replication only takes certificate thumbprints into account when verifying the certificates and does not check the certificate validity.

Verification of Thumbprint and Certificate Validity

vSphere Replication checks the thumbprint and checks that all server certificates are valid. If you enabled vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, vSphere Replication refuses to

communicate with a server with an invalid certificate. When verifying certificate validity, vSphere Replication checks expiration dates, subject names, and the certificate issuing authorities.

In both modes, vSphere Replication retrieves thumbprints from vCenter Server. vSphere Replication refuses to communicate with a server if the automatically determined thumbprint differs from the actual thumbprint that it detects while communicating with the respective server.

You can mix trust modes between vSphere Replication appliances at different sites. A pair of vSphere Replication appliances can work successfully even if you configure them to use different trust modes.

Requirements When Using a Public Key Certificate with vSphere Replication

If you enforce a verification of certificate validity by enabling vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, some fields of the certificate request must meet certain requirements.

vSphere Replication can only import and use certificates and private keys from a file in the PKCS#12 format. Sometimes these files have a `.pfx` extension.

- The certificate must be issued for the same server name as the value in the **Local Host** setting in the VRMS Appliance Management Interface. Setting the certificate subject name accordingly is sufficient, if you put a host name in the **Local Host** setting or if any of the Subject Alternative Name certificate fields of the certificate matches the **Local Host** setting.
- vSphere Replication checks the issue and expiration dates of the certificate against the current date, to ensure that the certificate is not expired.
- If you use your own certificate authority, for example one that you create and manage with the OpenSSL tools, you must add the fully qualified domain name or IP address to the OpenSSL configuration file.
 - If the fully qualified domain name of the appliance is `VR1.example.com`, add `subjectAltName = DNS: VR1.example.com` to the OpenSSL configuration file.
 - If you use the IP address of the appliance, add `subjectAltName = IP: vr-appliance-ip-address` to the OpenSSL configuration file.
- vSphere Replication requires a trust chain to a well-known root certificate authority. vSphere Replication trusts all the certificate authorities that the Java Virtual Machine trusts. Also, you can manually import additional trusted CA certificates in `/opt/vmware/hms/security/hms-truststore.jks` on the vSphere Replication appliance.
- vSphere Replication accepts SHA2 signatures.
- vSphere Replication does not accept RSA or DSA certificates with 512-bit keys. vSphere Replication requires at least 1024-bit keys. It is a best practice to use 2048-bit public keys.

Generate and Download a Certificate Signing Request for the vSphere Replication Appliance

A certificate signing request (CSR) is an encrypted text file that contains specific information, such as organization name, common name, locality, and country. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.

You generate a CSR and a matching private key. The private key remains on the vSphere Replication Appliance.

ATTENTION

Generating a new private key invalidates any existing CSR configuration.

1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
2. Enter the admin user name and password for the appliance.
You configured the admin password during the OVF deployment of the vSphere Replication appliance.

3. Click **Certificates**, and click **Generate CSR**.
4. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.
5. Accept the default FQDN and IP values and click **Generate and download**.

To submit a certificate request to the CA in accordance with the CA enrollment process, use the contents of the CSR file.

The CA creates a server certificate based on the information in the CSR file, signs it with its private key, and sends you the certificate, which you can then import to the vSphere Replication Appliance.

Configure vSphere Replication Network Settings

You can review your current network settings and change the address and proxy settings for vSphere Replication. If you want to match network configurations, these changes might be necessary.

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

NOTE

vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
2. Enter the admin user name and password for the appliance.
You configured the admin password during the OVF deployment of the vSphere Replication appliance.
3. Click on **Networking**.
4. To configure your network settings, click **Edit**.
5. Configure the DNS settings in the **Hostname and DNS** pane.

Menu Item	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter DNS settings manually	Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server.

6. In the **eth0** pane, select the IPv4 or the IPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

Option	Description
Obtain IPv4 settings automatically	Obtains the IP address for the appliance from the network.
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. <ol style="list-style-type: none"> 1. Enter the IPv4 address 2. Enter subnet prefix length. 3. Enter the default IPv4 gateway.

- Configure the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically using DHCP	Assigns IPv6 addresses to the appliance from the network by using DHCP. <p>NOTE To apply this setting, you must restart the vSphere Replication Appliance.</p>
Obtain IPv6 settings automatically using router advertisement	Assigns IPv6 addresses to the appliance from the network by using router advertisement.
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. <ol style="list-style-type: none"> 1. Enter the IPv6 address and the subnet prefix length in the address box. 2. To enter additional IPv6 addresses, click Add. 3. Enter the default IPv6 gateway.

7. Click **Save**.

If you modified the IP address of the vSphere Replication appliance, you must update and verify certain settings:

- Update the general vSphere Replication settings. See [Reconfigure General vSphere Replication Settings](#).
- Verify that the **IP Address for Incoming Storage Traffic** value is updated with the new IP address.
- Verify that the appliance certificate is valid for the new IP address. You must verify the certificate if you have activated the verification of the certificate validity.

Configure the Time Zone and Time Synchronization Settings for the vSphere Replication Appliance

When you deploy the vSphere Replication, you either use the time settings of the ESXi host on which the appliance is running, or you configure time synchronization with an NTP server. If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

1. Log in to the VRMS Appliance Management Interface as admin.
2. Click the **Time** tab.
3. Configure vSphere Replication Appliance time zone settings.
 - a) On the **Time zone** pane, click **Edit**.
 - b) From the **Time zone** drop-down menu, select a location or a time zone and click **Save**.
4. On the **Time synchronization** pane, click **Edit**.
5. Configure the time synchronization settings and click **Save**.

Mode	Description
Disabled	No time synchronization. Uses the system time zone settings.
Host	Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host.
NTP	Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers.

Start, Stop, and Restart vSphere Replication Appliance Services

If changes in your environment require the restart of certain services, you can use the VRMS Appliance Management Interface to view the state of the services and to start, stop, and restart them.

You can start, stop, and restart the vSphere Replication management server service, the vSphere Replication server service, the embedded database service, and the `tomcat` server service.

1. Log in to the VRMS Appliance Management Interface as admin.
2. In the VRMS Appliance Management Interface, click **Services**.
The Services page displays a table of the installed services that can be sorted by name, startup type, and state.
3. Select a service and click **Start**, **Stop**, or **Restart**.
Restarting some services might lead to functionality becoming temporarily unavailable.
4. Restart the appliance for the changes to take effect.

Forward vSphere Replication Appliance Log Files to Remote Syslog Server

You can forward the vSphere Replication Appliance log files to a remote syslog server to conduct an analysis of your logs.

1. Log in to the VRMS Appliance Management Interface as admin.
2. In the VRMS Appliance Management Interface, select **Syslog Forwarding**.
3. Click **New**, and enter the server address of the destination host in the **New Syslog Forwarding** pane.
4. From the **Protocol** drop-down menu, select the protocol to use.
5. In the **Port** text box, enter the port number to use with the destination host.
The default port number is 514.

6. Click **OK**.
7. Verify that the remote syslog server is receiving messages.
8. In the **Syslog Forwarding** section, click **Send Test Message**.
9. Verify that the test message is received on the remote syslog server.

Enable the SHA-1 Hashing Function

You can install certificates, signed with the SHA-1 hashing function in case your environment requires it.

By default, the vSphere Replication server rejects installation of new certificates, which are signed with the SHA-1 hashing function. To install a certificate, signed with the SHA-1 hashing function, you must enable it in the vSphere Replication appliance.

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Navigate to `/opt/vmware/hms/conf/`.
3. Open `hms-configuration.xml` in a text editor and set the `<hms-allow-legacy-hash-algo>` value to `true`.
4. Restart the vSphere Replication service.

Activate FIPS on vSphere Replication

This topic outlines the necessary task that you must perform to activate Federal Information Processing Standards (FIPS) mode on the vSphere Replication appliance.

Make sure to use trusted certificates when deploying your environment.

NOTE

The certificate file format PKCS#12 is not supported in the Certificates configuration in FIPS mode. The PKCS#12 file format uses non-FIPS compliant algorithms as a standard specification.

1. Start the vSphere Replication Management Server in strict mode.
 - a) Navigate to `/opt/vmware/hms/conf/hms-fips.conf`, open the file and change the following setting.


```
"appl_system_cryptography" : true
```
 - b) Remove any stale BCFKS stores.


```
rm /opt/vmware/hms/security/*.bks
```
 - c) Restart the vSphere Replication Management Server service.


```
systemctl restart hms
```
2. Start vSphere Replication in strict mode.
 - a) Navigate to `/etc/vmware/hbrsrv.xml`, open the file and change the following setting.

```
<Config>
  <vmacore>
    <ssl>
      <fips>true</fips>
    </ssl>
  </vmacore>
</Config>
```

- b) Edit `/usr/lib/vmware/lib/ssl/openssl.cnf`, uncomment the following line `# .include /usr/lib/vmware/lib/ssl/fipsmodule.cnf`, and change the line `default_properties = "fips=no"` to `default_properties = "fips=yes"`.

The file fragment must look like this:

```
# Refer to the OpenSSL security policy for more information.
```

```
# In ESX this will be generated at boot time.
.include /usr/lib/vmware/lib/ssl/fipsmodule.cnf
...
[algorithm_sect]
# Since we use both default and FIPS provider, we need to be specific
# about which algorithm implementation to use as default.
default_properties = "fips=yes"
```

c) Restart the HBR service.

```
systemctl restart hbrsrv
```

3. Start **dr-configurator** service in strict mode.

a) Navigate to `/opt/vmware/dr/conf/drconfig.xml`, open the file and change the following setting.

```
<Config>
  <vmacore>
    <ssl>
      <fips>true</fips>
    </ssl>
  </vmacore>
</Config>
```

b) Edit `/usr/lib/systemd/system/dr-configurator.service`. Uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
# Uncomment to enable FIPS
  Environment=OPENSSL_MODULES=/opt/vmware/dr/lib/openssl-modules
  Environment=OPENSSL_CONF=/opt/vmware/etc/dr/ssl/openssl.cnf
```

c) Restart **dr-configurator** service.

```
systemctl daemon-reload
systemctl restart dr-configurator
```

4. Log in the appliance as **root** user and edit the kernel cmdline.

a) Open `/boot/grub/grub.cfg`.

b) Locate the **menuentry** entry.

c) Append the following at the end of the line in each **menuentry** that starts with **linux**.

```
fips=1
```

d) Save the file.

5. Start the Config UI in strict mode.

a) Edit `/usr/lib/systemd/system/drconfigui.service`. Comment out the existing

`Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
Environment=JRE_HOME=/usr/java/jre-vmware
# Comment when enable FIPS
# Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
# Uncomment to enable FIPS
Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
```

```
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

- b) Uncomment the `<Manager>` tag in the `/opt/vmware/drconfigui/conf/context.xml` file.
The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode.          -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

- c) Optional: Restart the **drconfigui** service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart drconfigui
```

6. Start the UI in strict mode.

- a) Edit `/usr/lib/systemd/system/dr-client.service`. Comment out the existing

```
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
```

and uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
Environment=JRE_HOME=/usr/java/jre-vmware
# Comment when enable FIPS
# Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
# Uncomment to enable FIPS
Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

- b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-client/conf/context.xml` file.
The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode.          -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

- c) Edit the `/opt/vmware/dr-client/lib/h5dr.properties` file and modify parameters to point to BCFKS format keystore and truststore with root CA certificates.

The property must look like this.

```
drTrustStorePass=<same as keyStorePass>
drTrustStoreName=h5dr.truststore.bks
keyStoreName=h5dr.keystore.bks
```

If you choose to use a truststore other than the default one, you must add a link to the truststore in `/opt/vmware/dr-client/lib/` or `/opt/vmware/dr-client/webapps/dr/WEB-INF/classes/`. The keystore format must be BCFKS. To import it from JKS format use the following command.

```
$JAVA_HOME/bin/keytool -importkeystore -srckeystore <path-to-jks-keystore> -srcstoretype JKS -src-
storepass <keystorepass> -destkeystore <path-to-target-bks-keystore> -deststoretype BCFKS -dest-
storepass <keystorepass> -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -provider-
path /opt/vmware/dr-client/lib/ext/bc-fips-1.0.2.3.jar
```

NOTE

The keystore and truststore files you use must have **Others: Read** permission. After reconfiguring the appliance you must reedit the file `/opt/vmware/dr-client/lib/h5dr.properties` according the rules above.

- d) Optional: Restart the **dr-client** service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart dr-client
```

7. Start the UI plugin (dr-client-plugin) in strict mode.

- a) Edit `/usr/lib/systemd/system/dr-client-plugin.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
Environment=JRE_HOME=/usr/java/jre-vmware
# Comment when enable FIPS
# Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
# Uncomment to enable FIPS
Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

- b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-client-plugin/conf/context.xml` file.

The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode. -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

- c) Optional: Restart the dr-client-plugin service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart dr-client-plugin
```

8. Start the REST API service (dr-rest) in strict mode.

- a) Edit `/usr/lib/systemd/system/dr-rest.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
Environment=JRE_HOME=/usr/java/jre-vmware
# Comment when enable FIPS
# Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
# Uncomment to enable FIPS
Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

- b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-rest/conf/context.xml` file.

The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode. -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

- c) Optional: Restart the dr-rest service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart dr-rest
```

9. Reboot the appliance.

Make sure that the `systemctl daemon-reload` command is executed at least once after making the modifications and before rebooting the appliance.

NOTE

SSHD will read that the kernel has enabled FIPS mode and will activate it too. There is no need to edit anything in the sshd configuration.

Validate that FIPS mode is activated.

How do I validate that FIPS mode is activated

This topic outlines the necessary task that you must perform to validate that Federal Information Processing Standards (FIPS) mode is activated on the vSphere Replication appliance.

1. Validate the kernel command line. Run the following command.

```
cat /proc/cmdline
```

2. Validate that the kernel has activated FIPS mode. Run the following command.

```
cat /proc/sys/crypto/fips_enabled
```

3. Validate that the dr-configurator has activated FIPS mode. Run the following command.

```
grep "FIPS" /var/log/vmware/dr/drconfig*
```

4. Validate that hms has activated FIPS mode. Run the following command.

```
grep "FIPS" /opt/vmware/hms/logs/hms.log
```

5. Validate that hbrsrv has activated FIPS mode. Run the following command.

```
grep "FIPS" /var/log/vmware/hbrsrv.log
```

6. Validate UI strict mode.

All UI features must be available and work as expected.

vSphere Replication Roles and Permissions

You can use any predefined roles or clone an existing role, and add or remove privileges from it based on your needs.

vSphere Replication Roles Reference

vSphere Replication includes a set of roles. Each role includes a set of privileges, which enable users with those roles to complete different actions.

For information about how to assign roles, see *Assigning Roles in the vSphere Client* in *vSphere Security*.

NOTE

When assigning permissions with no propagation, make sure that you have at least Read-only permission on all parent objects.

Table 8: vSphere Replication Roles

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM replication viewer	<ul style="list-style-type: none"> View replications. Cannot change replication parameters. 	VRM remote > View VR VRM remote > View VRM VRM datastore mapper > View VRM replication > View replications Virtual machine > vSphere Replication > Monitor replication	vCenter Server root folder with propagation, at the source site (outgoing replications) and the target site (incoming replications). Alternatively, vCenter Server root folder without propagation on both sites and virtual machine without propagation on the source site.
VRM virtual machine replication user	<ul style="list-style-type: none"> View replications. Manage datastores. Configure and unconfigure replications. Manage and monitor replications. View defined storage capabilities and storage profiles. <p>Requires a corresponding user with the same role on the target site and also vSphere Replication target datastore user role on the target data center, or datastore folder or each target datastore.</p>	Datastore > Browse Datastore VRM remote > View VR VRM remote > View VRM VRM replication > View replications VRM datastore mapper > Manage VRM datastore mapper > View Host > vSphere Replication > Manage replication Virtual machine > vSphere Replication > Configure replication Virtual machine > vSphere Replication > Manage replication Virtual machine > vSphere Replication > Monitor replication Profile-driven storage > Profile-driven storage view	vCenter Server root folder with propagation on both sites. Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, source datastores without propagation on the source site.

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM administrator	Incorporates all vSphere Replication privileges.	VRM remote > Manage VR VRM remote > View VR VRM remote > Manage VRM VRM remote > View VRM VRM datastore mapper > Manage VRM datastore mapper > View VRM diagnostics > Manage VRM replication > View replications VRM session > Terminate Datastore > Browse datastore Datastore > Configure datastore Datastore > Low level file operations Host > vSphere Replication > Manage replication Resource > Assign virtual machine to resource pool Virtual machine > Configuration > Add existing disk Virtual machine > Configuration > Add or remove device Virtual machine > Interaction > Power On Virtual machine > Interaction > Device connection Virtual machine > Inventory > Register Virtual machine > Inventory > Unregister Virtual machine > vSphere Replication > Configure replication Virtual machine > vSphere Replication > Manage replication Virtual machine > vSphere Replication > Monitor replication Virtual machine > Snapshot management > Remove snapshot Profile-driven storage > Profile-driven storage view	vCenter Server root folder with propagation on both sites. Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, target datastore, target virtual machine folder with propagation on the target site, target host or cluster with propagation on the target site.
VRM diagnostics	Generate, retrieve, and delete log bundles.	VRM remote > View VR VRM remote > View VRM VRM replication > View replication VRM diagnostics > Manage	vCenter Server root folder on both sites.
VRM target datastore user	Configure and reconfigure replications. Used on the target site in on the VRM virtual machine replication user role on both sites.	Datastore > Browse datastore Datastore > Low level file operations	Datastore objects on the target site, or datastore folder with propagation at the target site, or target data center with propagation.

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM virtual machine recovery user	Recover virtual machines.	Datastore > Browse datastore Datastore > Low level file operations Host > vSphere Replication > Manage replication Virtual machine > Configuration > Add existing disk Virtual machine > Configuration > Add or remove device Virtual machine > Interaction > Power On Virtual machine > Interaction > Device connection Virtual machine > Inventory > Register Virtual machine > Inventory > Unregister Virtual machine > Snapshot management > Remove snapshot Resource > Assign virtual machine to resource pool	Secondary vCenter Server root folder with propagation. Alternatively, secondary vCenter Server root folder without propagation, target datastore without propagation, target virtual machine folder with propagation, target host, or cluster with propagation.

Assign VRM Replication Viewer Role

Assign the VRM Replication View role to a user so that they can view replication sites and the replications configured between them, but cannot perform modifications.

- Verify that you have two sites connected and replication configured between them.
 - Verify that you have another user account for each site.
1. Log in as Administrator on the source site.
 2. Select **vCenter > Permissions** and assign the **VRM replication viewer** role with the propagate option to this user.
 3. Assign the same privilege on the target replication site.
 4. Log in as the user with the assigned VRM replication viewer role.

The user with the VRM replication viewer role cannot perform modifications on the configured replication, nor on the replication sites. The following error message appears when this user tries to run an operation: `Permission to perform this operation was denied.`

Assign VRM Virtual Machine Replication User Role

Create a vSphere Replication user who can only configure a replication between sites and use a specific datastore on the target site.

- Verify that two sites are connected.
 - Verify that you have another user account for each site.
1. Log in as the Administrator user on the source site.
 2. Select **vCenter > Permissions** and assign to this user the **VRM virtual machine replication user** role with the propagate option.
 3. Assign the same privilege on the target replication site.
 4. On the target site, select the datastore to store your replica files, and select **Manage > Permissions**.
 5. Edit the assigned permission and assign the **VRM target datastore user** role.
 6. Log in as that user on the source site, select the virtual machine, and click **Configure Replication** to start the configuration wizard.
 7. Select the target site and enter the same user credentials.
 8. Accept the default selections until **Target Location**.
 9. For the target location, select the datastore to which you granted permission.

Assign VRM Virtual Machine Recovery User Role and Perform a Recovery Operation

You assign specific permissions to a vSphere Replication user, so that they can perform only recovery operations.

- Verify that you have two sites connected and replication configured between them.
 - Verify that you have another user account for the target site apart from the Administrator user.
1. Log in as the Administrator user on the target site.
 2. Select **vCenter > Permissions** and assign to a different user account the **VRM virtual machine recovery user** role with the propagate option.
 3. Log in as that user on the target site.
 4. On the home page, click **Site Recovery** and click **Open Site Recovery**.
 5. On the Site Recovery home page, select a site pair and click **View Details**.
 6. Click the **Replications** tab and select **Incoming**.
 7. Select a replication from the list.
 8. To finish the recovery, click the **Recover** icon and follow the prompts.

Clone an Existing VRM Administrator Role and Modify Privileges

Create a vSphere Replication user who can modify the replication infrastructure, but cannot register additional vSphere Replication servers.

- Verify that you have a replication site.
 - Verify that you have another user account to which you can assign the modified privileges.
1. Log in to the vSphere Client.
 2. On the home page, click **Administration** and click **Roles**.
 3. Select the **VRM Administrator** role and click the **Clone role action** icon.
 4. In the cloned role, deselect the **VRM Remote > VR Server > Manage VR Server** privilege.
 5. Navigate to the vCenter Server instance.
 6. On the **Permissions** tab, click the **Add permission** icon.
 7. Select the user that must have the privileges defined by the selected role.

Replicating Virtual Machines

You can replicate virtual machines from a source site to a target site with vSphere Replication.

To replicate a virtual machine using vSphere Replication, you must deploy the vSphere Replication appliance at the source and target sites. A vSphere Replication infrastructure requires one vSphere Replication appliance at each site.

If you want to configure replications, the source and target sites must be connected. You cannot perform replications if one of the sites is in the `Not Connected` state. See [Understanding the vSphere Replication Site Connection States](#).

You can configure replications for powered-off virtual machines, but the data synchronization begins when the virtual machine is powered on. While the source virtual machine is powered off, the replication appears in the `Not active` status.

You can set a recovery point objective (RPO) to a certain time interval depending on your data protection needs. vSphere Replication applies all changes made to virtual machines configured for a replication at the source site to their replicas at the target site. This process reoccurs periodically to ensure that the replicas at the target site are not older than the RPO interval that you set. See [Recovery Point Objective](#).

vSphere Replication does not support the recovery of multiple virtual machines from the same workflow. Each recovery workflow is for an individual virtual machine.

You cannot use vSphere Replication to replicate virtual machine templates.

Recovery Point Objective

When you set a Recovery Point Objective (RPO) value during replication configuration, you determine the maximum data loss that you can tolerate.

How the Recovery Point Objective Affects Replication Scheduling

The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. For example, when you set the RPO to 15 minutes, you instruct vSphere Replication that you can tolerate losing the data for up to 15 minutes. This does not mean that data is replicated every 15 minutes.

If you set an RPO of x minutes, and the RPO is not violated, the latest available replication instance can never reflect a state that is older than x minutes. A replication instance reflects the state of a virtual machine at the time the synchronization starts.

You set the RPO to 15 minutes. If the synchronization starts at 12:00 and it takes five minutes to transfer to the target site, the instance becomes available on the target site at 12:05, but it reflects the state of the virtual machine at 12:00. The next synchronization can start no later than 12:10. This replication instance is then available at 12:15 when the first replication instance that started at 12:00 expires.

If you set the RPO to 15 minutes and the replication takes 7.5 minutes to transfer an instance, vSphere Replication transfers an instance all the time. If the replication takes more than 7.5 minutes, the replication encounters periodic RPO violations.

If the replication starts at 12:00 and takes 10 minutes to transfer an instance, the replication finishes at 12:10.

You can start another replication immediately, but it finishes at 12:20. During the time interval 12:15-12:20, an RPO violation occurs because the latest available instance started at 12:00 and is too old.

The replication scheduler tries to satisfy these constraints by overlapping replications to optimize bandwidth use and might start replications for some virtual machines earlier than expected.

To determine the replication transfer time, the replication scheduler uses the duration of the last few instances to estimate the next one.

Recovery Point Objective Violations After the Initial Full Synchronization

The initial full synchronization of the virtual machine disks is a time-consuming process. As soon as it is complete, vSphere Replication begins to replicate the changed in the meantime disk blocks (first incremental sync), which might require longer transfer time than the set RPO time.

After the first incremental sync, vSphere Replication detects a staleness of the generated replica instance and starts reporting RPO violations. Since the replication is behind the RPO schedule, the second incremental sync begins as soon as the first one completes.

This process of immediate subsequent incremental syncs continues until vSphere Replication creates a replica instance that satisfies the RPO schedule, and does not report an RPO violation. The replication status becomes OK.

How the 5 Minute Recovery Point Objective Works

If the target and the source sites use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, vVol, or vSAN 6.2 Update 3 storage and later, you can use the 5 minute RPO.

vSphere Replication displays the 5 minute RPO setting when the target and the source site use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, vVol, or vSAN 6.2 Update 3 storage and later.

If you are using different datastore types between the source and the target site, you can use the 5 minute RPO setting .

The 5 minute RPO requires the source host to be 6.5 or later.

The 5 minute RPO can be applied to a maximum of 500 VMs on VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, and vSAN 6.2 Update 3 storage and later. The maximum for vVol datastore is 50 VMs.

NOTE

RPO lower than 15 minutes is not supported when you select the OS quiescing option.

For additional information, see [Best Practices for Using and Configuring vSphere Replication](#) and <https://kb.vmware.com/s/article/2102463>.

How the Retention Policy Works

When you configure a replication, you can enable the retention of up to 24 virtual machine replica instances from Multiple Points in Time (MPIT).

After you recover a replicated virtual machine, the retained replicas appear as snapshots of the virtual machine in the vSphere Client. The list of snapshots includes the retained instances according to the retention policy that you set, and the latest instance. You can use the snapshots to revert to an earlier state of the recovered virtual machine.

You can configure the retention of three instances per day for the last five days. The list of snapshots contains 15 snapshots and the latest saved instance of the virtual machine, or a total of 16 snapshots.

Administrators cannot configure the precise time when replica instances are created, because the retention policy is not directly related to the replication schedule and RPO. As a consequence, replications with the same retention policy might not result in replicas retained at the same time instants.

RPO Without Retention Policy

By default, vSphere Replication is configured to a one-hour RPO, so the latest available replica instance can never reflect a state of the virtual machine that is older than one hour. You can adjust the RPO interval when you configure or reconfigure a replication.

When the age of the latest replication instance approaches the RPO interval, vSphere Replication starts a sync operation to create an instance on the target site. The replication instance reflects the state of the virtual machine at the time the synchronization starts. If no retention policy is configured, when the new instance is created, the previous instance expires and the vSphere Replication Server deletes it.

How RPO and the Retention Policy Combine

To save some of the replica instances that are created during RPO synchronizations, you can configure vSphere Replication to keep up to 24 instances per replication. The exact instances that vSphere Replication keeps are determined by applying a specific algorithm. Using this algorithm, the vSphere Replication Server tries to match each instance to a slot of the retention policy. Instances that do not match any slot expire and are deleted. If a slot contains more than one instance, the instances that do not match the retention criteria are also deleted. vSphere Replication always keeps the latest created instance and it is not included when determining the number of instances to keep.

When the age of the latest instance approaches the RPO interval, vSphere Replication starts creating a replica instance. The start time of the sync operation is the time of the new instance. When the sync operation completes, vSphere Replication assesses the existing replica instances to determine which ones to keep:

1. The granularity of the retention policy is determined based on the replication settings. For example, if you configured vSphere Replication to keep three instances for the last one day, it means that you want to keep three replica instances that are relatively evenly distributed over 24 hours. This equals approximately one instance in an eight-hour interval, or the granularity of this retention policy is 8 hours.
2. The time of the last saved instance is rounded down to the nearest slot time. If the granularity is eight hours, the slot times are 0:00, 8:00, and 16:00.
3. The instances that are between the nearest slot time and the last saved instance are traversed. Let us assume that the time of the last saved instance is 10:55. Following our example, the nearest slot time is 8:00 o'clock. Let us also assume that the RPO is 1 hour, and each sync operation takes 5 minutes to complete. Between 8:00 o'clock and 10:55, the slot contains an 8:55 instance, and a 9:55 instance.
4. The earliest instance that is newer than the nearest slot time is saved, and the rest of the instances in this slot are deleted, except for the latest created instance that vSphere Replication always keeps. Following our example, the 8:55 instance is saved, and the 9:55 instance is deleted. The 10:55 instance is the latest created instance, so it is also saved.
5. The granularity of the retention policy decrements the slot time and a check is performed for the earliest instance between the beginning of the current slot and the beginning of the previous slot. If the slot contains expiring instances, they are deleted.
6. The number of slots that contain saved instances is analyzed. If the number of slots with saved instances is higher than the number of slots determined by the retention policy, the oldest saved instance expires and is deleted. The last saved instance is not included in this count. In our example, if we had an instance saved for the interval 8:00 - 16:00 o'clock of the previous day, that instance would be deleted.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, but also requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not verify whether the RPO settings creates enough instances to keep, and does not display a warning message if the instances are not enough, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep six replication instances per day, the RPO period must not exceed four hours, so that vSphere Replication can create six instances in 24 hours.

Replicating a Virtual Machine and Enabling Multiple Point in Time Instances

You can recover virtual machines at specific points in time (PIT), such as the last known consistent state.

When you configure a replication, you can enable multiple point in time (MPIT) instances in the recovery settings. vSphere Replication keeps several snapshot instances of the virtual machine on the target site, based on the retention policy that you specify. vSphere Replication supports a maximum of 24 snapshot instances. After you recover a virtual machine, you can revert it to a specific snapshot.

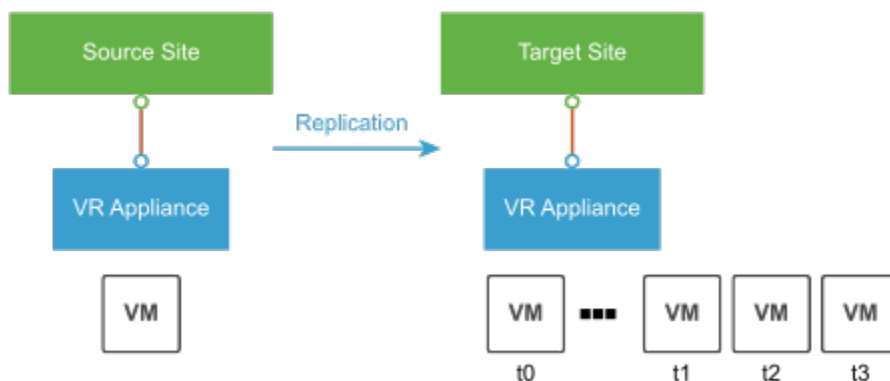
During the replication process, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine has a virus or a corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot in its uncorrupted state.

You can also use the PIT instances to recover the last known good state of a database.

NOTE

vSphere Replication does not replicate virtual machine snapshots.

Figure 5: Recovering a Virtual Machine at Points in Time



Using vSphere Replication with vSAN Storage

When configuring replications, you can use VMware vSAN datastores as target datastores. Follow the guidelines when using vSphere Replication with vSAN storage.

User-friendly names of directories on vSAN datastores might change and cause errors during replication or recovery operations. Because of this reason, vSphere Replication automatically replaces the user-friendly name of a directory with its UUID, which is constant. As a result you may see the UUID displayed in the Site Recovery user interface instead of a human-readable name.

Limits of Using vSphere Replication with vSAN Storage

Because of load and I/O latency, vSAN storage has limits for the numbers of hosts that you can include in a vSAN cluster and the number of VMs that you can run on each host. See the Limits section in the *VMware vSAN Design Guide* at <https://core.vmware.com/resource/vmware-vsant-design-guide>.

Using vSphere Replication adds to the load on the storage. Every virtual machine generates regular read and write operations. Configuring replications on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O latency on the storage. The precise number of virtual machines that you can replicate to vSAN storage by using vSphere Replication depends on your infrastructure. If you notice slower response times when you configure replications for virtual machines in vSAN storage, monitor the I/O latency of the vSAN infrastructure. Potentially, reduce the number of virtual machines that you replicate in the vSAN datastore.

Retaining Point-in-Time Snapshots When Using vSAN Storage

vSAN storage stores virtual machine disk files as a set of objects and components. Each disk object in vSAN storage has mirror and witness objects. In the default vSAN storage policy, a disk object has two mirrors and one witness. The number of mirror components is determined by the size of the virtual machine disk and the number of failures to tolerate that you set in your vSAN storage policy. A mirror object is divided into components of a maximum size of 256 GB each.

- If a virtual machine has one 256 GB disk and you use the default vSAN storage policy, the disk object has two mirror components of 256 GB each and one witness - a total of three components.
- If a virtual machine has one 512 GB disk and you use the default vSAN storage policy, the disk object has four mirror components of 256 GB each and one witness - a total of five components.

See the *VMware vSAN Design Guide* at <https://core.vmware.com/resource/vmware-vsant-design-guide> for explanations of objects, components, mirrors, witnesses, and vSAN storage policies.

If you enable multiple point-in-time (MPIT) snapshots, you must make allowances for the additional components that each snapshot creates in the vSAN storage. You must consider the number of disks per virtual machine, the size of the disks, the number of PIT snapshots to retain, and the number of failures to tolerate. When retaining PIT snapshots and using vSAN storage, you must calculate the number of extra components that you require for each virtual machine:

Number of disks × *number of PIT snapshots* × *number of mirror and witness components*

Examples of using this formula demonstrate that retaining PIT snapshots rapidly increases the number of components in the vSAN storage for every virtual machine that you configure for vSphere Replication:

- You have a virtual machine with two 256 GB disks for which you retain 10 MPIT snapshots, and you set the default vSAN storage policy:
 - 2 (number of disks) × 10 (number of PIT snapshots) × 3 (two mirror components + 1 witness) = 60 components for this one virtual machine.
- You have a virtual machine with two 512 GB disks for which you retain 10 PIT snapshots, and you set the default vSAN storage policy:
 - 2 (number of disks) × 10 (number of PIT snapshots) × 5 (four mirror components of 256 GB each + 1 witness) = 100 components for this one virtual machine.

The number of PIT snapshots that you retain can increase I/O latency on the vSAN storage.

Using vSphere Replication with vSphere Storage DRS

vSphere Replication can operate with target sites that have VMware vSphere® Storage DRS™ enabled.

Storage DRS (SDRS) can detect the data that vSphere Replication copies on the target site and can move replications without affecting the replication process. SDRS on the source site does not impact the replication process.

If there is SDRS enabled on the target site and the target datastore is included in a datastore cluster with SDRS enabled, SDRS communicates with vSphere Replication and does not automatically move the replica files from one datastore to another. vSphere Replication triggers a reconfigure replication that moves the replication data to the new datastore in the cluster. Initially, the replica files might be on one datastore and then they might split to several datastores or to a different datastore.

vSphere Replication manages all SDRS operations.

How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration

When you configure a virtual machine for replication, vSphere Replication starts an initial configuration task. During this task a replica virtual machine is created on the target site, and data synchronization occurs between the source and the target vCenter Server sites.

The speed of data synchronization depends on the availability of information about the block allocation of the VMDK files. vSphere Replication uses this information to find empty regions of the disks and accelerate the sync operations by

skipping these regions. The speed of data synchronization also depends on the site for which block allocation information is available.

- If the allocation information is available at both sites, data synchronization occurs at the highest possible speed.
- If the allocation information is available only at the source or the target site, vSphere Replication skips the empty regions on the VMDK disks at that site, but processes the entire disk at the site where the allocation information is not available. Therefore, data synchronization is slower.
- If the allocation information is not available at either site, data synchronization is done by comparing all blocks between the source site and the target site, even if many of the blocks are not allocated on the disk by the guest OS. This is the slowest method for data synchronization.

NOTE

The availability of block allocation information has little effect on the speed of data synchronization for VMDK disks that are almost full.

Factors That Affect the Availability of Block Allocation Information

The availability of allocation information and the degree to which vSphere Replication can use it to accelerate data synchronization depend on:

- The ESXi versions.
- The vSphere Replication Management server versions.
- The type of VMDK disks, and the type of volumes on which the disks reside.

Version Support

Table 9: Product Versions at the Source and the Target Site

Source Site		Target Site		Result
ESXi Host	vSphere Replication Management Server	ESXi Host	vSphere Replication Management Server	
6.x or later	6.x or later	6.x or later	6.x or later	The acceleration of initial synchronization is supported.
6.x or later	6.x or later	Earlier than 6.x	Earlier than 6.x	The allocation information is available only on the source site.
6.x or later	6.x or later	Earlier than 6.x	6.x or later	
6.x or later	6.x or later	6.x or later	Earlier than 6.x	

The Type of the Datastore

Disks on VMFS or vSAN datastores provide full allocation information.

NFS datastores cannot provide allocation information for the disks that are located on them.

Replication disks on the source and the target site can be on different datastore types. The acceleration of the initial synchronization depends on whether both sites can provide allocation information, or only one site. If none of the sites can provide allocation information, no acceleration occurs.

The Type of Virtual Disk

Lazy zeroed thick disks, thin disks, and vSAN sparse disks, Space-Efficient sparse disks, and VMDK sparse snapshots provide allocation information.

Eager zeroed thick disks do not provide allocation information.

Virtual disks that are based on vVols are native to the volume. vSphere Replication 8.8.x can get allocation information from them only when they are on the target site. For this reason, the acceleration of the initial synchronization is partial.

How vSphere Replication Synchronizes Data Between the Source and the Target Sites During Incremental Sync

After the initial full synchronization is complete, vSphere Replication starts to track the changed blocks on the source site and periodically transfers them to the target site. This process is called an incremental sync. As a result of the incremental sync completion, vSphere Replication creates a new replica instance on the target site. The following removal of the old instance is a time-consuming process.

During the old instance removal process, vSphere Replication might start transferring new changed blocks to the target site. This activity further increases the storage consumption on the target site. When the old instance removal is complete, vSphere Replication frees the storage space occupied by the old instance. If the source disk has a high data change rate, while the old replica instance is being removed, the storage consumption on the target site might temporarily exceed several times the size of the source disk.

NOTE

If due to the temporary spikes in the storage consumption on the target site the space is not enough, you might observe "Insufficient storage space" errors in the Site Recovery user interface. vSphere Replication might start reporting recovery point objective (RPO) violations.

Replicating Virtual Machines Using Replication Seeds

Reduce the amount of network traffic and time during the initial full synchronization. You can copy the virtual disk files in the target datastore and using them as replication seeds.

When you configure a replication for the first time, vSphere Replication performs an initial full synchronization of the virtual machine's disk. This operation is network and time intensive.

vSphere Replication compares the differences on the source and target site, and replicates only the changed blocks.

NOTE

To effectively reduce the amount of network traffic and time during the initial full synchronization, and to replicate only the changed blocks, you must upgrade both sites to vSphere Replication version 8.8 and ESXi host version 8.0. If one of the sites (the source or the target) runs vSphere Replication version 8.8 and ESXi host version 8.0, and the other site operates with previous versions of vSphere Replication and the ESXi host, all disk blocks will be replicated, and not only those that were changed.

When, during replication configuration, you select a target datastore for the virtual machine or a specific disk, vSphere Replication looks for disks with the same filename in the target datastore. If a file with the same name exists, a warning appears in the wizard. You can review and configure the replication seeds or choose not to use any replication seeds. If you choose not to use the discovered seeds, then replica files are placed in a new directory with a unique name. If you choose to configure seeds by selecting the **Select seeds** check box, then a new page appears in the wizard where you can configure seeds for each disk on each virtual machine.

NOTE

If you plan to copy files from the source to the target datastore, the source virtual machine must be powered off before downloading the VMDK files that will be used as seeds for the replication.

Using vSphere CLI for Storage Operations

To create a copy of a virtual disk, you can use the vSphere CLI to manage VMFS volumes, `vmkfstools`.

To prevent performance and data management issues on ESXi hosts, avoid using standard Linux commands for storage operations.

For more information, see [GUID-01D3CF47-A84A-4988-8103-A0487D6441AA.html](https://www.vmware.com/docs/guides/GUID-01D3CF47-A84A-4988-8103-A0487D6441AA.html).

Replicating a Virtual Machine in a Single vCenter Server Instance

You can use vSphere Replication to replicate a virtual machine in a single vCenter Server even if the vCenter Server instance has only one host in its inventory.

When you configure a replication in a single vCenter Server instance, you can select the source site as the target site for the replication. You then configure a replication in the same way as for an infrastructure with a source and a target site. For example, you can replicate a virtual machine to a different datastore attached to the same host or another host. vSphere Replication prevents you from using the source or replicated virtual machine's VMDK files as the target of the replication.

The virtual machine name must be unique and in the same folder in the vCenter Server inventory. In the recovery wizard, vSphere Replication does not allow you to select a folder if there is already a virtual machine with the same name registered to it. During recovery if there is a virtual machine with the same name, you might see an error message. See [Error Recovering Virtual Machine in a Single vCenter Server Instance](#) for more information.

Replicating Encrypted Virtual Machines

You can improve security and protection of your data by replicating encrypted virtual machines.

WARNING

vSphere Replication 8.8 does not support vSphere 7.0 Update 2 if virtual machine encryption is switched on. To use virtual machine encryption with vSphere Replication 8.8, you must use vSphere 7.0 Update 2c or later.

You can replicate virtual machines if you are running vSphere 6.7 Update 1 or later. Ensure that you either use a common Key Management Server (KMS) or that the Key Management Server clusters at both sites use common encryption keys. Ensure that the KMS server is registered with the same name both at the source and target sites. For information about how to set up a Key Management Server cluster, see the *VMware vSphere ESXi and vCenter Server 6.7 documentation*.

An encrypted virtual machine can have both encrypted and unencrypted disks and you must follow different policies for each type.

When you specify the VM Storage Policy for target disks in a replication, you must set a storage policy with VM Encryption enabled at the target if the source disks are encrypted. For unencrypted source disks, you must set a storage policy without VM Encryption enabled at the target.

If you use replication seeds, target disks for encrypted source disks must be encrypted and target disks for unencrypted source disks must be unencrypted. Replica disks can have different encryption keys from the source disks.

If you do not use seed disks, replica disks are encrypted with the same encryption key as the source VM disks.

When you configure a replication of an encrypted VM, encryption of the transferred data is automatically switched on to enhance data security and you cannot switch it off.

For more information on VM encryption, see [Virtual Machine Encryption](#) in the *vSphere Security* documentation.

For information about enabling virtual machine encryption for an already replicated VM, see [Enable VM Encryption for an Already Replicated VM](#).

vSphere Native Key Provider

VMware vSphere® Native Key Provider™ enables encryption-related functionality without requiring an external key server (KMS). Initially, vCenter Server is not configured with a vSphere Native Key Provider. You must manually configure a vSphere Native Key Provider. See [Configuring and Managing vSphere Native Key Provider](#) in the *VMware vSphere Product Documentation*.

Requirements for using vSphere Native Key Provider for encrypting virtual machines and virtual disks:

- You need vSphere 7.0 Update 2c or later.
- You must purchase the vSphere Enterprise+ edition.

You must configure a vSphere Native Key Provider on both the local and remote sites. The vSphere Native Key Provider ID of the encrypted VM on the local site must match the vSphere Native Key Provider ID on the remote site.

To use encryption with a vSphere Native Key Provider for replicated virtual machines, the replica disks must be located on datastores, which are accessible through at least one host, which is a part of a vCenter cluster.

For more information, see *Configuring and Managing vSphere Native Key Provider* in the VMware vSphere 7.0 Product Documentation.

Network Encryption of Replication Traffic

You can activate the network encryption of the replication traffic data for new and existing replications to enhance the security of data transfer.

You can activate encryption of replication traffic flows from the source ESXi host to the datastore at the target site.

The vSphere Replication appliance automatically installs an encryption agent on the source ESXi hosts. For ESXi hosts that are part of the vSphere Lifecycle Managed clusters or standalone ESXi hosts managed by vSphere Lifecycle Manager, the encryption agent is added as part of the desired state of the ESXi image. vSphere Lifecycle Manager takes care of installing the encryption agent on the hosts. For ESXi hosts that are not managed by vSphere Lifecycle Manager, the encryption agent is installed by vSphere Replication Management Server through the Patch Manager.

The network encryption uses secure transport protocol TLSv1.2.

The encrypted replication traffic uses mutual certificate-based authentication between the source ESXi host and target site vSphere Replication server.

When configuring or reconfiguring a replication, the vSphere Replication Management Server (VRMS) updates the source virtual machine configuration with a thumbprint of the target vSphere Replication server certificate. VRMS registers each vSphere Replication server at the target site with the certificates of all ESXi hosts from the source site. The registration is done separately for each paired vSphere Replication site.

VRMS exchanges data for the leaf certificates of the endpoints of the encrypted replication traffic, regardless of the certificate authorities for the source ESXi host and the target vSphere Replication server.

You can run the shell command `esxcli software vib list` on the source ESXi host and look for the `vmware-hbr-agent` VIB to make sure the agent is available in your system.

When the network encryption feature is switched on, the agent encrypts the replication data on the source ESXi host and sends it to the vSphere Replication appliance on the target site. The vSphere Replication server decrypts the data and sends it to the target datastore.

Unencrypted traffic goes through port 31031 on the source ESXi hosts and the vSphere Replication appliance on the target site.

Encrypted traffic goes through port 32032 on the source ESXi hosts and the vSphere Replication appliance on the target site.

If you configure a replication of an encrypted VM, the network encryption is automatically turned on and cannot be deactivated.

How vSphere Replication Works When Using Guest OS Trim/Unmap Commands

Storage and network bandwidth requirements might increase when using the trim/unmap Guest OS commands with vSphere Replication. You might also observe RPO violations.

Incremental Sync After Using Guest OS Trim/Unmap Commands

Calling the trim/unmap commands might increase the storage consumption on the target site.

After using the trim/unmap commands on the source site disk, the free space available on the disk is added to the data blocks that vSphere Replication transfers to the target site during the next RPO cycle. As a result, when the source site disk is less full, the size of the changed blocks that are transferred to the target site is larger.

For example, if the source site disk is 10 TB, and only 1 TB is allocated, calling the trim/unmap commands results in a transfer of at least 9 TB to the target site. If the source site disk is 10 TB, 9 TB of which are allocated, and if you delete 2 TB of data, calling the trim/unmap commands results in a transfer of at least 3 TB of data to the target site.

Because of the incremental sync and depending on the RAID configuration defined by the VM storage policy at the target site, the storage consumption by the replicated VM can be more than two times as high as the consumption by the source VM.

NOTE

If you use the trim/unmap commands at the source site, it is a best practice to configure the replication with an activated network compression to reduce the network bandwidth. See: [Replication Data Compression](#) and [Configure a Replication](#).

NOTE

If you use the trim/unmap commands, and the target datastore is vSAN, to reduce the actual physical storage space consumption at the target site, you must activate deduplication and compression of vSAN. If you do not use deduplication and compression, no storage space is reclaimed at the target site. Even after deduplication and compression, you might still see storage consumption spikes at the target location, but after the sync and the reconciliation, the storage space is freed. For more information about deduplication and compression, see [Using Deduplication and Compression](#).

You can't see the storage consumption by the replicated VM at the target site. You can only see the overall consumption of the entire vSAN datastore. So, you can't track the reclaimed storage space at the VM disk level, but you can track it by looking at the overall free space left on the vSAN datastore.

Recovery Point Objective Violations After Using the Trim/Unmap Commands on the Source Virtual Machine

You can call the trim/unmap commands manually or they can be called by the guest OS at certain intervals of time. In both cases, the synchronization after the command might take a significant amount of time.

The usage of the trim/unmap commands to reclaim the unused space on the source virtual machine might generate a large number of changed disk blocks. The synchronization of these changes might take longer than the configured RPO, and vSphere Replication starts reporting RPO violations.

Since the replication is behind the RPO schedule, to synchronize the changed disk blocks, a new incremental sync begins as soon as the synchronization of the previous instance completes. This process of immediate subsequent incremental syncs continues until vSphere Replication creates a replica instance that satisfies the RPO schedule, and does not report an RPO violation. The replication status becomes OK.

Use the Unmap Handling Mode of the vSphere Replication Filter Driver

On ESXi 7.0 Update 3 or later, by default, the vSphere Replication filter driver fails the SCSI Unmap commands during a sync operation, if these commands override the content that is transferred to the target site. The guest OS will retry the

command later without impacting the applications that run in the virtual machine. Some guest OS do not like this behavior of the filter driver and might get unresponsive while the sync operation is in progress.

- On ESXi 7.0 Update 3 or later, you can return to the previous behavior by using the ESXi advanced setting

On ESXi 7.0 Update 2 or earlier, there is a different Unmap handling mode of the `hbr_filter` where the Unmap commands are accommodated by preserving the content that is transferred. Some guest OS behave better in this mode even though the method has some disadvantages:

- Additional read and write operations for preserving the overlapping regions which on a slow storage might result in unexpected delays. These delays can cause some guest OS to issue device resets during the sync operation.
- Temporarily increased storage space consumption by the preserved disk content.

1. To allow trim/unmap during sync operations, use the following command running on the ESXi host where the virtual machine is working:

```
$ esxcli system settings advanced set -o /HBR/DemandlogFailCollidingUnmap -i 0
```

2. To disallow trim/unmap during sync operations, use the following command running on the ESXi host where the virtual machine is working:

```
$ esxcli system settings advanced set -o /HBR/DemandlogFailCollidingUnmap -i 1
```

Best Practices for Using and Configuring vSphere Replication

Best practices for using and configuring vSphere Replication can prevent your environment from possible issues during replication.

IMPORTANT

You mustn't change the source VM hardware while you are in the process of configuring a replication. For example, don't add or remove hard disk to the source VM before you finish configuring the replication.

Setting the Optimal Recovering Point Objective (RPO) Time

The replication of several thousand virtual machines is a bandwidth consuming process. One of the many factors that influence bandwidth requirements for vSphere Replication is the RPO configuration for each replicated virtual machine.

You can set the RPO to 5 minutes, but you must estimate the optimal RPO time to save bandwidth for the replication, and to cover your business requirements for the protection of your VMs.

For instance, if a block changes only once per day, it is replicated only once regardless of the RPO configuration. However, if a block changes many times during the day, and the RPO is set to a low number such as 30 minutes, the block might be replicated as many as 48 times in one day.

vSphere Replication tracks larger blocks on disks over 2 TB. Replication performance on a disk over 2 TB might be different than replication performance on a disk under 2 TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.

A network with the appropriate bandwidth available to transfer the system's data ingest rate is required to support the desired replication interval.

For example, if you have a dataset of 1 TB with a daily change rate of 2 GB per hour and RPO set to one hour, this means vSphere Replication must transfer 2 GB in 1 hour or 4.7 Mbps. This is the minimum theoretical bandwidth required to complete the vSphere Replication transfer.

The data change rate is not uniform throughout the day even though the above example assumes it. Use the peak data change rate in your scenario to calculate the minimum bandwidth requirement

See [Calculate Bandwidth For vSphere Replication](#) for details.

Using Multiple Point in Time (MPIT) Recovery

Each point in time snapshot consumes storage. The amount consumed depends on the data change rate in the VM. When you set multiple point in time instances for replication of a VM between two vCenter Server sites, vSphere Replication presents the retained instances as standard snapshots after recovery. The time required to consolidate snapshots after recovery, increases with the number of snapshots.

For example, if you configure a replication with 10 recovery points, then the storage consumption on the target site might increase to 11 times the original size of the source disk.

Although vSphere Replication supports up to 24 recovery points, you must set the MPIT to the lowest number of recovery points that meets your business requirements. For example, if the business requirement is for 10 recovery points, you must set up vSphere Replication to save only 10 snapshots. You can set up two recovery points per day for the last five days. As a result, the consumed storage and the time needed to consolidate the snapshots after recovery are less than if you use the maximum number of recovery points.

Configuring Quiescing

For VMs with high levels of storage I/O, quiescing of the file system and applications can take several minutes and impact the performance of the VM. When quiescing a file system and applications for Windows VMs, vSphere Replication requires a regular VM snapshot before replication. When you estimate the RPO time, consider the time and resource consumption for the quiescing and for the consolidation of the snapshots. For example, if you configure a replication of a Windows VM with an RPO of 15 minutes and quiescing is enabled, vSphere Replication generates a VM snapshot and consolidates it every 15 minutes.

Quiescing options are available only for virtual machines that support quiescing. For more information on which operating systems are supported, see the Guest OS Quiescing Support section in [Compatibility Matrices for vSphere Replication 8.8.x](#).

NOTE

Quiescing for vSphere Replication and backup operations for the same virtual machine is not supported.

Configuring Replication Seeds

You can copy virtual disk files of source VMs to the target location and use these files as replication seeds. By using replication seeds, vSphere Replication reduces the amount of time and network bandwidth required for the initial full sync process. The UUID of the source and target VMDK files must match for the replication to be successful and to prevent unintentional overwrites of disk files that belong to other VMs at the target location.

Monitoring a Datastore on the Target Site

vSphere Replication requires enough disk space at the target site to replicate a VM. If the available space is not enough to save the replication files, the replication might fail. You can create an alarm that alerts you about insufficient storage capacity at the target site.

Configure a Replication

vSphere Replication can protect one or more virtual machines and their virtual disks by replicating them from one vCenter Server instance to another. Configure the replications with your desired settings by using the following procedure.

- Verify that the vSphere Replication appliance is deployed at the source and the target sites.
- To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.
- If you want to replicate an encrypted VM or to activate the network encryption of a replication, verify that your environment meets the requirements. See [Replicating Encrypted Virtual Machines](#).

When you configure a replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of one hour seeks to ensure that a virtual machine loses the data for no more than one hour during the recovery. For smaller RPO values, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date. The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. See [Recovery Point Objective](#).

vSphere Replication guarantees crash consistency among all the disks that belong to a virtual machine. If you use quiescing, you might obtain a higher level of consistency. The available quiescing types are determined by the operating system of the virtual machine. See [Compatibility Matrices for vSphere Replication 8.8.x](#) for Windows and Linux virtual machines.

You can configure virtual machines to replicate from and to vSAN datastores. See [Using vSphere Replication with vSAN Storage](#) for the limitations when using vSphere Replication with vSAN.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab, select **Outgoing** or **Incoming**, and click the **Create new replication** icon.
5. Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site and click **Next**.
6. On the **Virtual machines** page of the **Configure Replication** wizard, select the virtual machines you want to replicate and click **Next**.
7. On the **Target datastore** page, select a datastore or a datastore cluster on which to replicate files.

When replicating multiple virtual machines, you can configure a different target datastore for each virtual machine. You can also use different target datastores for the various disks.

NOTE

All datastores that are selected as the target of the replicated disks must be read and write accessible by at least one host on the target site.

If after configuring the replication the read and write access gets broken, the replication will get into an unrecoverable state.

8. Optional: Select the **Select seeds** check box.
Replication seeds can reduce the network traffic during the initial full synchronization, but unintended use of replication seeds might lead to data loss.
9. Optional: Select or deselect the **Auto-include new disks in replication** check box.
Keep the check box selected to automatically include new disks in the replication, with the same replication configuration as the source virtual machine. Disk format for the automatically included disks is determined the following way: If all replicated disks use the **Same as source** format, the **Same as source** format is applied to the automatically included disks. If that is not the case, but all replicated disks use the same format, for example **Thin**

provision, the same format (**Thin provision**) is applied to the automatically included disks. If all replicated disks use different formats, the **Same as source** format is applied to the automatically included disks.

If **Auto-include new disk** is deactivated, adding a new disk will cause the replication to enter an Error state until the new disk is either included or excluded from the list of the replicated disks through the **Reconfigure Replication** wizard. You must avoid virtual machine disk changes until the replication is in OK state.

10. Optional: Activate or deactivate the **Configure datastore per disk** view.

If you activate the **Configure datastore per disk** view, you can specify a different datastore for each disk. You can also include or exclude existing disks from replication, and you can also activate or deactivate the automatic replication of new disks. To include or exclude a new or existing disk from being replicated, select or deselect the respective disk.

11. Click **Next**.

12. Optional: On the **Select seed** page, review the suggested replication seeds and change them if necessary.

You can select seed files for each virtual machine disk and search for seeds by using the drop-down menu and clicking **Browse**.

The replica files for the disk are written in the seeds file directory.

13. Select the **The selected seeds are correct** check box and click **Next**.

14. On the **Replication settings** page, use the RPO slider to set the acceptable period for which data can be lost if a site failure occurs.

The available RPO range is from 5 minutes to 24 hours.

15. Optional: To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable point in time instances** and adjust the number of instances to keep.

NOTE

You can keep up to 24 instances for a virtual machine. For example, if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is four days.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, but also requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not verify whether the RPO settings creates enough instances to keep, and does not display a warning message if the instances are not enough, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep six replication instances per day, the RPO period must not exceed four hours, so that vSphere Replication can create six instances in 24 hours.

16. Optional: Activate quiescing for the guest operating system of the source virtual machine.

NOTE

Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on vVOL.

17. Optional: Select **Enable network compression for VR data**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

18. Optional: Activate the network encryption of the replication traffic.

If you configure a replication of an encrypted VM, this option is automatically turned on and cannot be deactivated.

19. On the Ready to complete page, review the replication settings, and click **Finish**.

vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

Move a Replication to a New vSphere Replication Server

After configuring vSphere Replication, you can move replications to other vSphere Replication Server instances. You might do this to complete maintenance tasks on existing servers or to balance the load on the servers if one server becomes overloaded with replications.

You must have an additional vSphere Replication Server deployed and registered, apart from the embedded vSphere Replication Server.

1. Log in to the vSphere Client on the source site.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. On the **Target site** page of the **Reconfigure Replication** wizard, select **Manually select vSphere Replication Server**.
7. Select a different vSphere Replication Server instance from the list and click **Next** until you finish the wizard.

NOTE

You can see the list of replications handled by each vSphere Replication Server and if some load balancing is needed, the replications can switch to a less loaded vSphere Replication Server.

If you use the **Auto-assign vSphere Replication Server** option, the vSphere Replication Server will not be changed and the load balancing will not be autotriggered.

The newly assigned server is updated in the **Replication Server** column.

Stop Replicating a Virtual Machine

If you do not need to replicate a virtual machine, you can stop that replication by removing it.

Verify that you are logged in the vSphere Client as a VRM virtual machine replication user or a VRM administrator user. See [vSphere Replication Roles Reference](#).

Take a note of the target datastore and the name of the replication that you are about to stop. You need this information to clean up your environment after you stop the replication.

If you delete the source VM of a configured replication, the replication enters Error state. The replica files remain on the target site. You can recover the VM using the latest available data from the target site. If you don't want to use the replica files, you can stop the replication and clear all replica data.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Remove** icon.

vSphere Replication asks you if you want to stop permanently the replication for the selected virtual machine.

NOTE

The connection between the vSphere Replication sites must be working to stop a replication on both sites. Alternatively, you can force stop the replication on the local site by selecting **Force stop replication**. If the remote site is available, you must also use the Site Recovery user interface to force stop the corresponding

replication on the remote site. If you force stop an outgoing replication, the replication can still be recovered by using the Site Recovery user interface on the remote site.

6. To confirm that you want to stop replicating this virtual machine, click **Remove** .
If you want to retain your replica disks, select the **Retain replica disks** check box.
7. Inspect the target datastore for any leftover replica disks and files. Delete them if you do not plan to use them as seeds in the future.

The virtual machine does not replicate to the target site.

When you stop a replication, the following operations are performed at the replication target site:

- If you selected **Retain replica disks** check box, all files are retained.
- If you deselected the **Retain replica disks** check box, all replica files and seed disks are deleted, even if you previously configured the replication with seed disks.

Reconfiguring Replications

You can reconfigure a replication to modify its settings.

For example, you can reconfigure the replication to activate or deactivate a virtual machine disk file for replication, modify replication options, such as RPO, MPIT retention policy, or quiescing method. You can also specify a different target datastore for replica configuration and disk files.

IMPORTANT

You mustn't change the source VM hardware while you are in the process of reconfiguring a replication. For example, don't add or remove hard disk to the source VM before you finish the reconfiguration of the replication.

Reconfigure Recovery Point Objective in Replications

You can modify the settings for already configured replications to specify different recovery point objective (RPOs).

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** until you reach the **Replication settings** page of the **Reconfigure Replication** wizard.
7. Modify the RPO settings for this replication and click **Next**.
8. Click **Finish** to save your changes.

Change the Point in Time Settings of a Replication

You can reconfigure a replication to activate or deactivate the saving of point in time instances, or to change the number of instances that vSphere Replication keeps.

vSphere Replication can save replication instances that can be used as snapshots after recovery or planned migration operations. You can save up to 24 point in time instances per VM.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** until you reach the **Replication settings** page of the **Reconfigure Replication** wizard.
7. In the **Point in time instances** pane, make the changes that you want to apply and click **Next**.

Action	Procedure
Enable the saving of point in time instances	Select the Enable point in time instances check box.
Disable the saving of point in time instances	Deselect the Enable point in time instances check box.
Adjust the number of instances to keep and for how long to keep them	Use the spin-boxes to adjust the number of instances (no more than 24 per virtual machine) to keep per day and the number of past days for which you want to keep replication instances.

8. Click **Finish** to save your changes.

If you selected to deactivate the saving of point in time instances, the instances that exist on the target site are deleted when the next replication instance appears on the target site. The moment when a new replication instance is saved on the target site depends on the RPO setting.

Increasing the Size of Replicated Virtual Disks

If you run out of disk space, you can seamlessly increase the virtual disks of virtual machines that are configured for replication without triggering an initial full synchronization.

You can resize the virtual disk of a replicated virtual machine while the virtual machine is powered on or powered off.

IMPORTANT

As a best practice, resize the virtual disk of a replicated virtual machine while the virtual machine is powered on. If you increase the disk size of a virtual machine that is powered off, full synchronization is performed the next time you power on the replicated virtual machine.

After you increase the virtual disk on the source site, the virtual disk on the target site automatically resizes and the ongoing replication enters `Resizing disk` state, until the task completes.

NOTE

After you resize the virtual disk, vSphere Replication clears all available multiple points in time. You can modify this behavior by changing the virtual disk resizing configuration options.

When the target datastore for a replication is NFS and you want to increase a thick-provisioned virtual disk, if the available storage space on the target datastore is not enough for the new size, then the resized replica disk is of a thin type.

To use this feature, you need vSphere 7.0 or later on the source site and vSphere 6.5 or later on the target site.

For more information about disk resizing, see *Change the Virtual Disk Configuration in the VMware Host Client* in the vSphere Product Documentation.

Configure the Virtual Disk Resizing

You can determine the behavior of vSphere Replication during disk resizing, by choosing one of the three configuration options. To activate your preferred option, you must change the value of three different parameters in the `/etc/vmware/hbrsrv.xml` configuration file.

- vSphere Replication can follow two approaches to perform the disk resizing on the target site. To configure the way the server handles the resizing, change the value of the `extendDiskPITHierarchyPolicy` parameter.

Table 10: extendDiskPITHierarchyPolicy Parameter Values

Value	Description
<code>extendDiskPITHierarchyPolicy = auto</code>	vSphere Replication selects <code>preserve</code> or <code>collapse</code> , depending on the current datastore storage consumption and the requested new virtual disk size. This is the default value of the parameter.
<code>extendDiskPITHierarchyPolicy = collapse</code>	vSphere Replication collapses the disk hierarchy of the replica disk and extends the resulting base disk. All PITs created before the start of the virtual disk resizing are lost. You cannot perform recovery until you create a PIT after resizing the virtual disk.
<code>extendDiskPITHierarchyPolicy = preserve</code>	vSphere Replication creates a new base disk, which is a full clone of the latest PIT. vSphere Replication extends the new disk to the new size. The original base disk still exists. The extra consumed storage is freed, after vSphere Replication removes all PITs, which contain the original disk. Then the vSphere Replication removes the original replica base disk.

- To adjust the behavior when the `extendDiskPITHierarchyPolicy` is set to `auto`, you can use the `extendDiskPITHierarchyPolicyAutoThreshold` parameter. You can change the property value to a number between 0 and 1 (the default value is 0.9). This way you set a limit to the datastore capacity. vSphere Replication calculates this limit by multiplying the size of the datastore capacity by the `extendDiskPITHierarchyPolicyAutoThreshold` parameter value.

For example, if the datastore capacity is 5 TB and the `extendDiskPITHierarchyPolicyAutoThreshold` parameter is set to 0.8, then the datastore capacity limit is 4 TB.

vSphere Replication calculates what is the final storage consumption, if the `preserve` mode is active. If the storage consumption is below the threshold, vSphere Replication uses the `preserve` mode and if it is above the threshold, it uses the `collapse` mode.

- To reduce the period of extended storage consumption, when `extendDiskPITHierarchyPolicy` is set to `preserve` mode, change the value of the `removeMPITsBeforeBaseDisks` parameter.

Table 11: `removeMPITsBeforeBaseDisks` Parameter Values

Value	Description
<code>removeMPITsBeforeBaseDisks = true</code>	The vSphere Replication server drops all PITs, which are based on the original disk size, after a new PIT which is based on the extended disk appears.
<code>removeMPITsBeforeBaseDisks = false</code>	The retention policy of the PITs determines the expiration of the older PITs. The storage consumption drops, after all PITs, which refer to the original disk, are expired.

Change the Target Datastore Location of a Replication

You can reconfigure a replication to change the datastore or datastore cluster where replicated data is saved.

To change the target datastore, the old target datastore from which you want to move the replication data must be online. If the old datastore or datastore cluster is inaccessible, the reconfiguration task fails. To change the target datastore when the old datastore is inaccessible, you must stop the replication to the old datastore and configure another replication to the new datastore or datastore cluster.

NOTE

You cannot change the target datastore, while you are performing a test recovery. To change the target datastore, you must wait for the test cleanup to be complete.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** to reach the **Target datastore** page of the **Reconfigure Replication** wizard.
7. Select a new datastore or a datastore cluster.

NOTE

All datastores that are selected as the target of the replicated disks must be read and write accessible by at least one host on the target site.

If after reconfiguring the replication the read and write access gets broken, the replication will get into an unrecoverable state.

8. Click **Next** until you reach the **Ready to complete** page and click **Finish** to save your settings.

vSphere Replication moves all replicated instances and configuration files to the new target datastore according to your settings.

Exclude a Disk from the Replication

You can reconfigure a replication to exclude some of the disks from the replication. You can also retain the replica disk when excluding a disk from the replication.

When you exclude a disk from a replication, you can retain the replica file on the target site and it is not deleted. If you want to include the disk to the replication again, you can use the retained disk as a seed disk.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** to reach the **Target datastore** page of the **Reconfigure Replication** wizard.
7. To exclude a disk, deselect it from the list.
The disk is marked as **Not replicated**.
8. Optional: To retain the replica disks, select the **Retain replica for excluded disks** check box.

Reconfigure Replication - VM_3

- 1 Target site
- 2 Target datastore
- 3 Replication settings
- 4 Ready to complete

Target datastore

Select a datastore for the replicated files.

Name	Disk Format	Disk Controller	Storage Policy	Datastore
<input type="checkbox"/> VM home ⓘ	N/A	N/A	Datastore Default	local CHANGE
<input type="checkbox"/> Hard disk 1 ⓘ	N/A	SCSI controller 0	N/A	Not replicated
<input checked="" type="checkbox"/> New Hard disk	Thick provision lazy ...	N/A	Same as VM home	Same as VM home ⓘ

Retain replica for excluded disks

CANCEL
BACK
NEXT

9. Click **Next** until you reach the **Ready to complete** page and click **Finish** to save your settings.

NOTE

If you exclude a disk and then you want to include it back before the next recovery point objective (RPO), you have to sync the replication. The synchronization will only work if there is no multiple point in time (MPIT) enabled. If you enable the MPIT, the older points in time that contain the disk must expire before adding it again to the replication.

Include a Disk to the Replication

You can add a new disk to the replication after you configure the replication.

If you add a new disk to the source virtual machine of the replication, you can include it to the list of replicated disks. If a disk is previously excluded from the list of replicated disks, you can include it back.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** to reach the **Target datastore** page of the **Reconfigure Replication** wizard.
7. To include a disk, select it from the list.
8. Optional: Specify a seed disk from the target site.
9. Optional: Click **Change** to change the storage policy and the target datastore or datastore cluster.
10. Click **Next** until you reach the **Ready to complete** page and click **Finish** to save your settings.

Changing the Storage Policy of Replica Disks

The storage policy is applied to the replica disks at the target site at the time you first configure a replication. During the vSphere Replication Management Server recovery process, it is applied to the virtual machine and its disks.

If the target datastore is vSAN, you can reconfigure a replication with a new storage policy. The replica base disks are resynced with the new storage policy.

NOTE

If the target datastore is vSAN, the replica child disks are not resynced with the new storage policy.

If the target datastore is not vSAN and you reconfigure a replication to assign a new storage policy to replicated virtual disks, it is not immediately reflected to the replica disks at the target site. The storage policy is applied only after a recovery process.

Change the Storage Policy

You can change the storage policy of replica disks to the target site to a non-vSAN datastore.

1. Recover the virtual machines with the reconfigured replication.
2. To change the storage policy of the recovered virtual machines to the new policy, use the vSphere Client.
3. Unregister the recovered virtual machines from the vCenter Server inventory.
4. Configure the replication again by using the new storage policy and seeds.

Enable VM Encryption for an Already Replicated VM

You can enable the virtual machine encryption for an already replicated VM to protect the virtual machine disks.

1. Recover the virtual machine.
2. Stop the replication.
3. Encrypt the disk on the source site.
4. Encrypt the disk of the recovered virtual machine on the target site.
5. Unregister the recovered virtual machine on the target site without deleting the disks.
6. Configure a replication by using the disks of the recovered virtual machine as seeds.

Replicate Virtual Machines with DataSets

You can replicate the VM DataSets files along with the standard VM configuration files.

Verify that your environment meets the following requirements on both the source and the target sites:

- vSphere Replication 8.6 or later.
- vCenter Server 8.0 or later.
- ESXi host 8.0 or later.
- Virtual machines must be of hardware version 20.

Review the [Configure a Replication](#) or [Reconfiguring Replications](#) procedure.

The DataSets files contain configuration information and provide a way to share data between the vSphere Client and a virtual machine guest operating system. The DataSets are stored together with the other VM configuration files in the VM directory. There are two types of DataSets files:

- .dsv - VM mode DataSets file. This file is not preserved during a snapshot and clone operations.
- .dsd - Disk mode DataSets file. This file is preserved during snapshots and clone operations.

For more information about the DataSets feature, see [Sharing Data Between the vSphere Client and a Virtual Machine Guest Operating System with DataSets](#) in vSphere 8.0 product documentation.

NOTE

vSphere Replication does not automatically replicate the DataSets files of the VMs, which were configured for replication prior to the system upgrade to vSphere Replication 8.6 or later, vCenter Server 8.0 or later, and ESXi host 8.0 or later. By default, after a system upgrade, the Enable DataSets replication setting is deactivated for

all VMs. You must reconfigure the VMs for a replication and activate the configuration option for DataSets files replication.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** > **Open Site Recovery**.
3. On the **Site Recovery** home page, select a site pair and click **View Details**.
4. Click the **Replications** tab, and select **Outgoing** or **Incoming**.
5. Depending on your needs, click either the **Create new replication** icon or the **Reconfigure** icon, and follow the prompts of the wizard.
6. On the **Replication Settings** screen, select **Enable DataSets replication** check box.
7. Finish the configuration or the reconfiguration of the VM.

NOTE

If you have a protected virtual machine with enabled DataSets and turn off the replication of the DataSets files, the recovered virtual machine might still get DataSets enabled after recovery. This might happen if the DataSets files are added to the replica folder or the DataSets files existed in the replica folder before recovery.

If you want to recover a VM with DataSets files, follow the standard process for recovering a virtual machine. See [Recover Virtual Machines with vSphere Replication](#). vSphere Replication recovers the DataSets files in the existing replica file location with the other replicated VM configuration files.

Stopping a Virtual Machine Offline Synchronization Task

You can stop an ongoing offline synchronization task for a powered off virtual machine by using two different methods: by establishing an SSH connection to the ESXi host of the source VM or by using the vCenter Server Managed Object Browser (MOB).

Stop a Virtual Machine Offline Synchronization Task by Using an SSH Connection

1. Establish an SSH connection to the ESXi host that hosts the source virtual machine.
2. To get the list of all VMs, and to find the ID of the VM whose offline sync you want to stop, run the following command:
`vim-cmd vmsvc/getallvms`.
3. To check the progress of the sync task, run the following command: `vim-cmd hbrsvc/vmreplica.queryReplicationState <vmid>`.
4. To stop the offline sync task, run the following command: `vim-cmd hbrsvc/vmreplica.stopOfflineInstance <vmid>`.

Stop a Virtual Machine Offline Synchronization Task by Using the vCenter Server MOB

Verify that you have the credentials of a vSphere administrator.

1. To get the Managed Object ID (MOID) of the source VM:
 - a) Log in to the vSphere Client on the source site.
 - b) Navigate to the source VM.
 - c) Copy the `vm-...` value from the URL.
2. Log in to `https://<vc_ip>/mob/?moid=hbrManager&method=stopOfflineInstance&vmodl=1` with vCenter Server credentials.
3. In the **Value** text box, replace the MOID text with the MOID of the VM, and click **Invoke Method**.
4. To check the state of the `stopOfflineInstance` task:
 - a) In the **Value** text box of the **Method Invocation Result: ManagedObjectReference** panel, click the displayed task session.
 - b) On the **Managed Object Type: vim.Task** window, click the **Info** value.
 - c) Optional: Refresh the page.

Monitoring and Managing Replications in vSphere Replication

vSphere Replication provides a management interface where you can monitor and manage virtual machine replication and connectivity states for local and remote sites.

On the home page of the Site Recovery user interface, you can see all vSphere Replication site connections and the number of outgoing and incoming replications between the sites.

To see details about the status of a connection, replication problems, and to manage and monitor replications between a site pair, click the **View Details** button.

Monitor the Status of a Replication

You can monitor the status of your replications, view information about the virtual machines configured for replication, or get a remediation plan for some replication states.

- Verify that vSphere Replication is running.
- Verify that the virtual machines are configured for replication.

For more information about how to identify replication errors, see [Identifying Replication Problems](#).

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. To see details of the virtual machines replicated from this site, select the **Replications** tab and click **Outgoing** or **Incoming**.

Table 12: Replication Statuses

Status	Description	Remediation
OK	The replication is running.	Not needed.
Not Active	<p>The replication is not running at the moment.</p> <ul style="list-style-type: none"> • The source virtual machine is powered off. • A communication problem might have occurred between the source ESXi host and the target site. • At target site, the vSphere Replication server cannot access the datastore using an ESXi host. 	<ul style="list-style-type: none"> • Power on the source virtual machine. • Check the network connectivity between source and target site.

Status	Description	Remediation
Paused	The replication is not running at the moment. A vSphere Replication user has paused the replication.	From the list of replications, select the paused replication and click the Resume icon.
Error	The replication is not running at the moment. <ul style="list-style-type: none"> A configuration error occurred. A replication error occurred. For example, the target site infrastructure is not accessible. 	<ul style="list-style-type: none"> Reconfigure the replication. Verify whether some problem occurred on the virtual machine by clicking the Site Pair tab and clicking Issues.
Status (RPO violation)	<p>For replication status <code>OK</code>, <code>Sync</code>, or <code>Full Sync</code>, the replication is running, but the RPO that is set for the replication is not met and is violated.</p> <p>For replication status <code>Not Active</code> or <code>Error</code>, the replication is not running, and the RPO that is set for the replication is violated.</p> <ul style="list-style-type: none"> The network connection between the source and the target site is dropping intermittently. The bandwidth of the connection between the source and the target site is too low. The replication is not running, so data cannot be replicated on the target site. 	<ul style="list-style-type: none"> Improve the network connection between the source and target site. Increase the RPO period. For replication status <code>Not Active</code> or <code>Error</code>, address the cause for the status and wait for the next sync.

NOTE

If a replication is in the `Not Active` replication state, you might have connected the source and target sites using network address translation (NAT). vSphere Replication does not support NAT. Use credential-based authentication and network routing without NAT when connecting the sites. Another cause for a `Not Active` replication state might be that the source virtual machine is powered off. Automatic replication works only on virtual machines that are powered on.

View Replication Reports for a Site

If you observe frequent RPO violations, want to learn more about the network usage of vSphere Replication, or verify the status of your outgoing replications, you can view replication statistics for source and target vCenter Server sites.

Verify that vSphere Replication is running.

You can view statistics for the replications for a certain time period. The transferred bytes statistics do not include the transferred data for the initial full synchronization, only the data transferred after the initial synchronization is complete. The update of the information in the statistics might occur in the end of the selected RPO period. For example, if you configure a replication with the default RPO of 1 hour, you might not see any transferred data for this VM in the statistics for up to 1 hour.

The granularity of the statistical data depends on the `rrd-updater-interval` parameter. The parameter is defined in the `the/opt/vmware/hms/conf/hms-configuration.xml` configuration file. This parameter controls the interval, at which the statistical data is saved. By default, the value is set to 5 minutes, but it can be changed if needed.

NOTE

Data is collected in 10 minute intervals and the graphs represent aggregated data for each interval. Therefore, you cannot see the exact moment when a peak value occurred and there might be an additional delay of up to 10 minutes before the Transferred Bytes statistics display the data. The displayed data combines all site pairs.

- Transferred Bytes - total bytes transferred for all outgoing replications, excluding the data from the initial full synchronization.
- Replications Count - number of outgoing replications.
- RPO Violation Count - number of RPO violations.
- Target Sites Count - number of vSphere Replication site connections.
- VR Sites Count - number of registered replication servers.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Site Pair** tab and click **vSphere Replication reports**.

The **Reports** page displays historic data for vSphere Replication for a certain time period.

- You can use the drop-down menu above the reports to change the time range of the reports.
- You can zoom in the data.
- Export any chart as a CSV file.

Interpreting Replication Statistics for a Site

You can use the reports that vSphere Replication compiles to optimize your environment for replication, identify problems in your environment, and reveal their most probable cause.

As an administrator, you can get the necessary information to diagnose various replication issues by using the server and site connectivity, number of RPO violations, and other metrics.

The following sections contain examples of interpreting the data displayed under **vSphere Replication reports** on the **Site Pair** tab of vSphere Replication.

RPO Violations

The large number of RPO violations can occur due to by various problems in the environment, on both the protected and the recovery site. With more details on historical replication jobs, you can make educated decisions on how to manage the replication environment.

Table 13: Analyzing RPO Violations

Probable Cause	Solution
<ul style="list-style-type: none"> • The network bandwidth cannot accommodate all replications. • The replication traffic might have increased. • The initial full sync for a large virtual machine is taking longer than the configured RPO for the virtual machine. 	<ul style="list-style-type: none"> • To allow the lower change rate virtual machines to meet their RPO objectives, deactivate the replication on some virtual machines with a high change rate. • Increase the network bandwidth for the selected host. • Check if the replication traffic has increased. If the traffic has increased, investigate possible causes, for example the usage of an application might have changed without you being informed. • Check the historical data for average of transferred bytes for a notable and sustained increase. If an increase exists, contact application owners to identify recent events that might be related to this increase. • Adjust to a less aggressive RPO or look at other ways to increase bandwidth to accommodate the current RPO requirements.
<ul style="list-style-type: none"> • A connectivity problem exists between the protected and the recovery site. • An infrastructure change might have occurred on the recovery site. 	<ul style="list-style-type: none"> • To verify the connection between the protected and recovery site, check the site connectivity data. • Check if the infrastructure on the recovery site has changed or is experiencing problems that prevent vSphere Replication from writing on the recovery datastores. For example, storage bandwidth management changes made to recovery hosts might result in storage delays during the replication process. • Check on the vSphere Replication Management Server appliance and the vSphere Replication Server appliance. Someone might have shut down the appliance or it might have lost connection.

Transferred Bytes

Correlating the total number of transferred bytes and the number of RPO violations can help you decide on how much bandwidth might be required to meet RPO objectives.

Table 14: Analyzing the Rate of Transferred Bytes and RPO Violations

Graph Values	Probable Cause	Solution
<ul style="list-style-type: none"> High rate of transferred bytes and high number of RPO violations Low rate of transferred bytes and high number of RPO violations 	The network bandwidth might be insufficient to accommodate all replications.	<ul style="list-style-type: none"> Check the transferred bytes graph and use the drop-down menus to filter the data by virtual machine and time period. To let virtual machines with a lower change rate meet their RPO objectives, you can deactivate the replication on some virtual machines with a high change rate. Increase the network bandwidth for the selected host.
<ul style="list-style-type: none"> High rate of transferred bytes and a few or no RPO violations Low rate of transferred bytes and a few or no RPO violations 	The environment operates as expected.	N/A

Identifying Replication Problems

You can view and troubleshoot possible vSphere Replication problems that might occur during replication.

Under **Issues** on the **Site Pair** tab of vSphere Replication, you can view and identify possible replication problems.

Table 15: Possible Replication Problems

Problem	Cause	Solution
Not Active	The replication is not active because the virtual machine is powered off and a warning icon appears. Replication is not running for that virtual machine.	Power on the virtual machine to resume the replication.
Paused	If you paused the replication, a warning icon appears.	Resume the paused replication from the Issues tab.
Error	If you added a disk on a virtual machine which is already configured for replication with deactivated automatic replication for new disks, the replication pauses and goes to an error state.	Reconfigure the replication and activate or deactivate the newly added disk.
Error	While configuring replication, the replication fails with the incorrect UUID. For example, the replication seed found and intended for use has a different UUID from the original hard disk.	Reconfigure the replication.
RPO Violation	A replication contains an RPO violation.	See Reconfigure Recovery Point Objective in Replications .

Manage vSphere Replication Connections

You can reconnect a site pair or break the connections between vSphere Replication sites.

Verify that you have paired your protected site with at least one recovery site. To create a connection to a new recovery site, see [Configure vSphere Replication Connections](#).

If you have problems with an existing site pair, you can attempt to reconnect the site pair with the **Reconnect** action. When you provide the required credentials, the reconnection operation attempts to repair the existing site pair.

With the **Break Site Pair** action, you can disconnect vSphere Replication sites.

NOTE

You cannot use the **Reconnect** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Site Pair** tab and click **Summary**.
5. Manage the site pair.

Option	Description
Reconnect	<ol style="list-style-type: none"> 1. Select Site Pair > Summary, and click Reconnect. 2. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click Reconnect.
Break a site pair	<ol style="list-style-type: none"> 1. Click Break Site Pair. 2. Select the services you want to disconnect. 3. Click Disconnect.

Manage vSphere Replication Servers

You can view, configure, reconnect, and unregister vSphere Replication Server instances that are registered in your environment.

Verify that vSphere Replication is running.

1. Log in to the vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Site Pair** tab, click **Replication Servers**, and select a server from the list.
5. To manage the vSphere Replication servers, select an option.

Option	Description
Register a virtual machine as vSphere Replication Server.	Click to register a virtual machine as a vSphere Replication Server. See Register an Additional vSphere Replication Server .
Unregister the selected vSphere Replication Server.	Click to unregister the vSphere Replication Server that you selected from the list. See Unregister and Remove a vSphere Replication Server .
Reconnect the selected vSphere Replication Server.	Click if the status of the vSphere Replication Server that you selected from the list is Disconnected .
Configure the selected vSphere Replication Server.	Click to access the VRMS Appliance Management Interface of the vSphere Replication Server that you selected from the list.

Performing a Recovery with vSphere Replication

With vSphere Replication, you can recover virtual machines that were successfully replicated at the target site.

vSphere Replication performs a sequence of steps to recover replicated virtual machines.

- vSphere Replication prepares for the recovery operation.
 - If you perform a synchronization of the latest changes, vSphere Replication checks that the source site is available and source virtual machine is powered off before recovering the virtual machine on the target site. Then vSphere Replication synchronizes the changes from the source to the target site.
 - If you skip the synchronization and recover with the latest data available, for example, if the source site is not available, vSphere Replication uses the latest available data at the target site.
- vSphere Replication rebuilds the replicated `.vmdk` files.
- vSphere Replication reconfigures the newly replicated virtual machine with the correct disk paths.
- vSphere Replication registers the virtual machine with vCenter Server at the target site.

You can recover one virtual machine at a time in **Incoming** replications on the **Replications** tab at the target site. Optionally, you can power on the recovered virtual machine. The network devices of the recovered virtual machine are disconnected. You might need to configure the recovered virtual machine to render it fully operational.

If you enabled the saving of point in time instances, those instances are converted to snapshots of the recovered virtual machine. You can use the vSphere Client to revert to a snapshot from the list.

Recover Virtual Machines with vSphere Replication

With vSphere Replication, you can recover virtual machines that were successfully replicated at the target site. You can recover one virtual machine at a time.

Verify that the virtual machine at the source site is powered off. If the virtual machine is powered on, an error message reminds you to power it off.

NOTE

- If you have replications, configured to automatically replicate newly added disks, then you perform a recovery, and add a new disk to the recovered VM, this disk will not be replicated upon reprotect operation. You must include the new disk to the replication manually.
- In case you delete the source VM of a configured replication, the replication enters Error state. The replica files remain on the target site. You can recover the VM using the latest available data from the target site. If you don't want to use the replica files, you can stop the replication and clear all replica data.

1. Log in to the target site by using the .
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Incoming**.
5. Click the **Recover** icon.
6. Select whether to recover the virtual machine with all the latest data, or to recover the virtual machine with the most recent data available on the target site.

Option	Description
Synchronize recent changes	Performs a full synchronization of the virtual machine from the source site to the target site before recovering the virtual machine. Selecting this option avoids data loss, but it is only available if the data of the source virtual machine is accessible. You can only select this option if the virtual machine is powered off.

Option	Description
Use latest available data	Recovers the virtual machine by using the data from the most recent replication on the target site, without performing synchronization. Selecting this option results in the loss of any data that has changed since the most recent replication. Select this option if the source virtual machine is inaccessible or if its disks are corrupted.

7. Optional: Select the **Power on the virtual machine after recovery** check box.

8. Click **Next**.

9. Select the recovery folder and click **Next**.

10. Select the target compute resource and click **Next**.

The selected host must have read and write access to all datastores that are used as targets for the replica disks.

11. Optional: If the virtual machine contains hard disks for which you have not activated replication, select a target destination to attach an existing disk or detach the disk, and click **Next**.

This page only appears if the virtual machine contains hard disks for which you have not activated replication.

- To select a target destination, click **Browse** and navigate to a folder on a datastore in which disk file is placed.
- To detach the disk and exclude disk files from the recovery, click **Detach**.

12. Click **Finish**.

vSphere Replication validates the provided input and recovers the virtual machine. If successful, the virtual machine status changes to *Recovered*. The virtual machine appears in the inventory of the target site.

If you activated multiple point in time instances when you configured replication for the virtual machine, vSphere Replication presents the retained instances as standard snapshots after a successful recovery. You can select one of these snapshots to revert the virtual machine. vSphere Replication does not preserve the memory state when you revert to a snapshot.

If the recovery fails, the replication of the virtual machines reverts to the replication state before the attempted recovery. For more information about the failed recovery attempt, check the last recovery error message in the replication details pane or check vCenter Server tasks.

The recovery might also fail if you use the same name for the virtual machine in a scenario where you use vSphere Replication to replicate a virtual machine in a single vCenter Server and the vCenter Server instance has only one host in its inventory. See [Error Recovering Virtual Machine in a Single vCenter Server Instance](#) for more information.

After a successful recovery, vSphere Replication deactivates the virtual machine for replication if the source site is still available. When the virtual machine is powered on again, it does not send replication data to the recovery site. To unconfigure the replication, click the **Remove** icon.

When the source virtual machine is no longer in the vCenter Server inventory, the replication is removed from the **Outgoing** tab, but it can still be found in the **Incoming** tab on the target site.

If a replicated virtual machine is attached to a distributed virtual switch and you attempt to perform a recovery in an automated DRS cluster, the recovery operation succeeds but the resulting virtual machine cannot be powered on. To attach it to the correct network, edit the recovered virtual machine settings.

vSphere Replication disconnects virtual machine network adapters to prevent damage in the production network. After recovery, you must connect the virtual network adapters to the correct network. A target host or cluster might lose access to the DVS the virtual machine was configured with at the source site. In this case, manually connect the virtual machine to a network or other DVS to successfully power on the virtual machine.

Failback of Virtual Machines in vSphere Replication

Failback of virtual machines between vCenter Server sites is a manual task in vSphere Replication. Automated failback is not available.

After performing a successful recovery on the target vCenter Server site, you can perform failback. Click **Incoming** and manually configure a new replication in the reverse direction, from the target site to the source site. The disks on the source site are used as replication seeds, so that vSphere Replication only synchronizes the changes made to the disk files on the target site. For more information on replication seeds, see [Replicating Virtual Machines Using Replication Seeds](#).

Before you configure an incoming replication, you must unregister the virtual machine from the inventory on the source site.

Using the vSphere Replication REST API Gateway

VMware vSphere Replication REST API Gateway provides an API access to the vSphere Replication functionality and allows you to programmatically perform various vSphere Replication tasks without the use of the Site Recovery user interface.

System Requirements to use the vSphere Replication REST API Gateway

To use the public REST APIs, you must have an installation of vSphere Replication 8.6 or later.

Before you run any REST APIs to or from a target site, verify that you have created a session to the desired vCenter Server site by using the vSphere Replication REST API Gateway.

NOTE

In a federated environment with linked vCenter Server instances, when you log in to the REST API gateway local site this will automatically log you in to the remote site. You do not have to make a `POST /remote-session` request. It is not possible to log in to the remote site with a different user name.

vSphere Replication REST API Gateway Documentation

The vSphere Replication REST APIs introduce an end-to-end automation for vSphere Replication:

- Endpoints for Configure and Reconfigure replications.
- Ability to manage replications, such as start, stop, pause, resume, or delete, with the option to retain replica disks.
- Ability to monitor replications, site pairs, or vSphere Replication servers and their respective states.
- Ability to create, delete, or reconnect vSphere Replication site pairs.
- Endpoints for Register, Unregister, or Reconnect additional vSphere Replication servers.
- Full set of REST APIs to configure and manage the vSphere Replication appliance.

You can access the vSphere Replication REST APIs documentation and guidelines at <https://developer.broadcom.com/xapis/>.

- To access the vSphere Replication REST API Gateway, see <https://developer.broadcom.com/xapis/vsphere-replication-api/latest/>.
- To access the vSphere Replication Management Server (VRMS) Configuration REST APIs, see <https://developer.broadcom.com/xapis/vrms-appliance-config-api/latest/>.
- To access the vSphere Replication Server (VRS) Configuration REST APIs, see <https://developer.broadcom.com/xapis/vrs-appliance-config-api/latest/>.

Download the Open API Specification

You can explore the vSphere Replication REST APIs and download the Open API specifications from the REST API Explorer.

1. Navigate to the vSphere Replication Appliance home page.
2. Click **Explore REST API**.
3. From the **Select product** drop-down menu, select an API, and click **DOWNLOAD OPEN API SPEC**.

Option	Description
configure	Downloads the vSphere Replication Appliance configuration REST APIs.
vr	Downloads the vSphere Replication Server REST APIs.

4. Optional: To discover the available REST API versions, make a GET request.

```
GET <VR-APPLIANCE-FQDN>/api/rest/supported-versions
```

5. Optional: To retrieve the open api specifications, use the following endpoints:

- GET <VR-APPLIANCE-FQDN>/api/rest/configure/<VERSION>/open-api.yaml
- GET <VR-APPLIANCE-FQDN>/api/rest/configure/<VERSION>/open-api.json
- GET <VR-APPLIANCE-FQDN>/api/rest/vr/<VERSION>/open-api.yaml
- GET <VR-APPLIANCE-FQDN>/api/rest/vr/<VERSION>/open-api.json

List of vSphere Replication REST APIs

The following REST APIs are available with vSphere Replication 8.8.

Table 16: vSphere Replication Configuration and Management REST APIs

Category	Operation Type	REST API Name	Description
Authentication	GET	Get Current Session	Returns information about the current session, if any.
Authentication	POST	Login	Logs in and returns the session ID. In the subsequent requests, include the 'x-dr-session' header with the returned session ID value.
Authentication	DELETE	Logout	Logs out if the session is authenticated.
Pairing	POST	Create Remote Session	Returns information about the current session to the remote vSphere Replication Management Server (VRMS).
Pairing	POST	Create Remote Session	Returns information about the current session to the remote vSphere Replication Management Server.
Pairing	DELETE	Delete VR Pairing	Delete the existing pairing with the remote vSphere Replication Management Server.

Category	Operation Type	REST API Name	Description
Pairing	GET	Get All VR Details In Pairing	Get information about vSphere Replication servers that are paired.
Pairing	GET	Get All VR Servers In Pairing	Get all registered replication servers for vSphere Replication in a pairing.
Pairing	GET	Get Remote Session	Returns information about the current session to the remote vSphere Replication Management Server, if any.
Pairing	GET	Get VR Info In Pairing	Get information about specific vSphere Replication in a pairing.
Pairing	GET	Get VR Pairing	Get information about the pairing.
Pairing	GET	Get VR Pairing Issues	Get all issues for the pairing.
Pairing	GET	Get VR Pairings	Get a list of all existing pairings.
Pairing	GET	Get VR Server In Pairing	Get information about a registered vSphere Replication server for a vSphere Replication Management Server, which is part of a pairing.
Pairing	POST	Pair VR	Pair to the remote vSphere Replication Management Server.
Pairing	POST	Reconnect VR Pairing	Reconnect the existing pairing to the remote vSphere Replication Management Server.
Pairing	POST	Reconnect VR Server In Pairing	Update the connection information for this vSphere Replication Server and reset any current connection for vSphere Replication in a pairing.
Pairing	POST	Register VR Server In Pairing	Register a replication Server for vSphere Replication in a pairing.
Pairing	DELETE	Unregister VR Server In Pairing	Unregister a vSphere Replication Server for vSphere Replication in a pairing.
Replication	POST	Browse Datastore	Browse the datastore that is defined in the URL by its ID. This API returns files that reside on the given datastore. These files are filtered based on the given search criteria.
Replication	POST	Check Storage Policy Compliance	Check datastores for compliance against a given storage policy.
Replication	POST	Configure Replication	Configure replication for a virtual machine from a source site to a target vCenter Server site.

Category	Operation Type	REST API Name	Description
Replication	DELETE	Destroy Replication	Delete replication of a VM. The operation deletes the replication only on the local site. Remove the replication configuration first.
Replication	GET	Get All Replications	Get a list of all the incoming or outgoing replications from a vCenter Server.
Replication	GET	Get Local VM Disks	Retrieve information about the disks of a VM.
Replication	GET	Get Local VMS	Get a list of all VMs on the vCenter Server specified by a vCenter Server ID in the URL.
Replication	GET	Get Replicated VM Disks	Retrieve information about the disks of a replicated VM.
Replication	GET	Get Replication Info	Get information about the replication.
Replication	GET	Get Replications Count	Get the total number of replications - both incoming and outgoing.
Replication	GET	Get Replications Issues	Get a list of all the current issues for all incoming or outgoing replications.
Replication	POST	Get Seeds For Disks	Retrieve information about possible seeds for a given set of disks.
Replication	GET	Get VC Storage Policies	Retrieve vCenter Server storage policies.
Replication	GET	Get VM Capability	Retrieve vSphere Replication capability information about a specific VM.
Replication	GET	Get VR Capable Target Datastores	Retrieve vSphere Replication supported datastores.
Replication	POST	Pause Replication	Pause the replication for a virtual machine from the source site to a remote vCenter Server site.
Replication	POST	Reconfigure Replication	Change the settings of a replication, including reconfiguring a replication on new virtual hard disks and enabling the default seed disk to use a replica disk in the VM folder.
Replication	POST	Resume Replication	Resume a paused replication to the target vCenter Server site.
Replication	POST	Sync Replication	Sync the latest changes for a virtual machine with a configured replication to the target vCenter Server site.

Category	Operation Type	REST API Name	Description
Replication	POST	Unconfigure Replication	Gracefully remove the replication configuration of a VM. If the remote site is not available, use DELETE / replications/{replication_id} to delete the replication from the local site.
Server	GET	Get All VR Servers	Get all registered replication servers.
Server	GET	Get VR Info	vSphere Replication Management Server information.
Server	GET	Get VR Server	Get information about a registered vSphere Replication Server.
Server	POST	Reconnect VR Server	Update the connection information for this vSphere Replication Server and reset any current connection.
Server	POST	Register VR Server	Register a replication server.
Server	DELETE	Unregister VR Server	Unregister a vSphere Replication Server.
Tasks	GET	Get Recent Tasks Info	Retrieve all recent tasks.
Tasks	GET	Get Task Info	Retrieve task information.

Table 17: vSphere Replication Management Server (VRMS) Appliance Configuration REST APIs

Category	Operation Type	REST API Name	Description
Appliance	GET	Get Appliance Disks	Get information about the virtual appliance's disks.
Appliance	GET	Get Appliance Info	Get information about the virtual appliance.
Appliance	POST	Restart Appliance	Restart the virtual appliance.
Appliance	POST	Shutdown Appliance	Shut down the virtual appliance.
Appliance Settings	GET	Get Syslog Servers	Get a list of all configured syslog servers.
Appliance Settings	GET	Get Time Settings	Get information about the current time settings.
Appliance Settings	GET	Get Time Zones	Get information about the supported time zones.
Appliance Settings	POST	Send Syslog Test Message	Send a test message to all syslog servers.
Appliance Settings	POST	Update Appliance Password	Update the appliance password.
Appliance Settings	PUT	Update Syslog Servers	Update the configured syslog servers.
Appliance Settings	PUT	Update Time Settings	Update the current time settings.

Category	Operation Type	REST API Name	Description
Authentication	GET	Get Current Session	Get information about the current session, if any.
Authentication	POST	Login	Logs in and returns the session ID. In the subsequent requests, include the 'x-dr-session' header with the returned session ID value.
Authentication	DELETE	Logout	Logs out if the session is authenticated.
Certificates	POST	Add CA Certificates	Add certificate authorities (CA) certificates.
Certificates	POST	Delete CA Certificates	Delete certificate authorities (CA) certificates.
Certificates	POST	Generate CSR	Generate a new key and a certificate signing request (CSR), and return it for signing.
Certificates	GET	Get Appliance CA Certificates	Get the installed certificate authorities (CA) certificates that are used to validate the other certificates of the server.
Certificates	GET	Get Appliance Certificate	Get the appliance certificate information.
Certificates	POST	Probe SSL	Check if the appliance can establish a successful SSL connection to the specified endpoint.
Certificates	POST	Update Appliance Certificate	Update the appliance certificate.
Configuration	POST	Check Extension Key	Check if a given extension key is already registered in SSO, lookup service and as a vCenter Server extension.
Configuration	POST	Delete Configuration	Remove the current configuration.
Configuration	GET	Get Configuration	Get the appliance configuration information.
Configuration	GET	Get vSphere Replication Server Settings	Get the vSphere Replication Server settings.
Configuration	GET	Get Reconfigure Required	Check if a reconfigure operation is required after an upgrade.
Configuration	POST	List VC Services	List all vCenter Serverservices in the Platform Services Controller (PSC).
Configuration	PUT	Update Configuration	Update the appliance configuration.
Configuration	PUT	Update vSphere Replication Server Settings	Update the vSphere Replication Server settings.
Configuration	POST	Validate Connection	Validate the connections to the vSphere infrastructure.

Category	Operation Type	REST API Name	Description
Network Settings	GET	Get All Network Interfaces Settings	Get all network interface settings.
Network Settings	GET	Get All Network Settings	Get the current appliance network settings.
Network Settings	GET	Get Network DNS Settings	Get the DNS settings.
Network Settings	GET	Get Network Interface Settings	Get the network interface settings.
Network Settings	PUT	Update Network DNS Settings	Update the DNS settings.
Network Settings	POST	Update Network Interface Settings	Update the network interface settings.
Services	GET	Get All Services	Get information about all services.
Services	GET	Get Service	Get information about a specific service.
Services	POST	Restart Service	Restart the service.
Services	POST	Start Service	Start the service.
Services	POST	Stop Service	Stop the service.
Support Bundles	GET	Get Support Bundles	Get all support bundles available on the server.
Support Bundles	GET	Download Support Bundle	Download the support bundle information from the server.
Support Bundles	POST	Generate Support Bundle	Generate a support bundle.
Support Bundles	DELETE	Delete Support Bundle	Delete the existing support bundle on the server.
Tasks	GET	Get All Tasks Info	Retrieve all configuration-related tasks.
Tasks	GET	Get Task Info	Retrieve task information.
Updates	PUT	Change Updates Repository	Change the current updates repository.
Updates	POST	Get Updates	Get all available updates in the repository.
Updates	GET	Get Updates Repository	Get information about the current updates repository.
Updates	POST	Install Update	Install the update.

Table 18: vSphere Replication Server (VRS) Appliance Configuration REST APIs

Category	Operation Type	REST API Name	Description
Appliance	GET	Get Appliance Disks	Get information about the virtual appliance's disks.
Appliance	GET	Get Appliance Info	Get information about the virtual appliance.
Appliance	POST	Restart Appliance	Restart the virtual appliance.
Appliance	POST	Shutdown Appliance	Shut down the virtual appliance.

Category	Operation Type	REST API Name	Description
Appliance Settings	GET	Get Syslog Servers	Get a list of all configured syslog servers.
Appliance Settings	GET	Get Time Settings	Get information about the current time settings.
Appliance Settings	GET	Get Time Zones	Get information about the supported time zones.
Appliance Settings	POST	Send Syslog Test Message	Send a test message to all syslog servers.
Appliance Settings	POST	Update Appliance Password	Update the appliance password.
Appliance Settings	PUT	Update Syslog Servers	Update the configured syslog servers.
Appliance Settings	PUT	Update Time Settings	Update the current time settings.
Authentication	GET	Get Current Session	Get information about the current session, if any.
Authentication	POST	Login	Logs in and returns the session ID. In the subsequent requests, include the 'x-dr-session' header with the returned session ID value.
Authentication	DELETE	Logout	Logs out if the session is authenticated.
Certificates	POST	Add CA Certificates	Add certificate authorities (CA) certificates.
Certificates	POST	Delete CA Certificates	Delete certificate authorities (CA) certificates.
Certificates	POST	Generate CSR	Generate a new key and a certificate signing request (CSR), and return it for signing.
Certificates	GET	Get Appliance CA Certificates	Get the installed certificate authorities (CA) certificates that are used to validate the other certificates of the server.
Certificates	GET	Get Appliance Certificate	Get the appliance certificate information.
Certificates	POST	Update Appliance Certificate	Update the appliance certificate.
Configuration	GET	Get vSphere Replication Server Settings	Get the vSphere Replication Server settings.
Configuration	PUT	Update vSphere Replication Server Settings	Update the vSphere Replication Server settings.
Network Settings	GET	Get All Network Interfaces Settings	Get all network interface settings.
Network Settings	GET	Get All Network Settings	Get the current appliance network settings.
Network Settings	GET	Get Network DNS Settings	Get the DNS settings.
Network Settings	GET	Get Network Interface Settings	Get the network interface settings.
Network Settings	PUT	Update Network DNS Settings	Update the DNS settings.

Category	Operation Type	REST API Name	Description
Network Settings	POST	Update Network Interface Settings	Update the network interface settings.
Services	GET	Get All Services	Get information about all services.
Services	GET	Get Service	Get information about a specific service.
Services	POST	Restart Service	Restart the service.
Services	POST	Start Service	Start the service.
Services	POST	Stop Service	Stop the service.
Support Bundles	GET	Get Support Bundles	Get all support bundles available on the server.
Support Bundles	GET	Download Support Bundle	Download the support bundle information from the server.
Support Bundles	POST	Generate Support Bundle	Generate a support bundle.
Support Bundles	DELETE	Delete Support Bundle	Delete the existing support bundle on the server.
Tasks	GET	Get All Tasks Info	Retrieve all configuration-related tasks.
Tasks	GET	Get Task Info	Retrieve task information.
Updates	PUT	Change Updates Repository	Change the current updates repository.
Updates	POST	Get Updates	Get all available updates in the repository.
Updates	GET	Get Updates Repository	Get information about the current updates repository.
Updates	POST	Install Update	Install the update.

How to Use the REST APIs to Create a Site Pairing

You use the vSphere Replication REST APIs to connect your source site and your target site.

To create a site pairing, you must register your vSphere Replication to the Platform Services Controller (PSC) by using the VRMS Appliance Management Interface or the VRMS Appliance Configuration REST API Gateway.

1. To login to the source site, make a POST request.

```
POST BASE_URL/api/rest/vr/API_VERSION/session
```

2. To create a site pairing, make a POST request.

```
POST BASE_URL/api/rest/vr/API_VERSION/pairings/
```

Example request body:

```
{
  "pair_vc_id": "775043e3-5ef7-440f-bb1f-6c071050c92d",
  "pair_psc_info": {
    "url": "vc-colo-2.mycorp.com",
    "port": "443",
    "thumbprint": "7C:42:1E:D9:54:8A:AD:CF:5C:8C:82:E9:DC:55:97:4F:DA:42:1D:73",
    "username": "administrator@mycorp.local",
    "password": "secure_password"
  }
}
```

```
}
}
```

How to Use the REST APIs to Configure a Replication

You can configure virtual machines replication from a source site to a target site by using the vSphere Replication REST APIs.

To configure a virtual machine replication:

- You must register your vSphere Replication to the Platform Services Controller (PSC) by using the VRMS Appliance Management Interface or the VRMS Appliance Configuration REST API Gateway.
- You must have a site pair between the source and the target sites.

1. To login to the source site, make a POST request.

```
POST BASE_URL/api/rest/vr/API_VERSION/session
```

Enter your user name and password in the Authorization HTTP header. Use the returned session ID as a value for **x-dr-session** HTTP header for all subsequent calls to the REST API.

2. To get the pairing ID and the local vCenter Server ID, make a GET request.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/
```

Example response:

```
{
  "pairing_id": "e41c183f-bc55-319b-bf76-8ec83d335074", <----- Pairing ID
  "local_vc_server": {
    "id": "0a98c22d-a553-47e4-bd56-2844f45d8ef6", <----- VC ID
    "url": "https://s2-srm2-219-12.eng.vmware.com:443/sdk",
    "name": "s2-srm2-219-12.eng.vmware.com",
    "server_status": "OK",
    // Other fields are not relevant in this example
  }
}
```

Save the pairing ID and the local vCenter Server ID.

3. To get the virtual machines IDs per site pair, make a GET request.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vcenters/VC_GUID/vms
```

Save the ID of the VM for which you want to configure the replication.

4. To get the target vSphere Replication Server ID:

- a) Make a POST request to login to the target site.

```
POST BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/remote-session
```

Enter your user name and password in the Authorization HTTP header. Ensure the **x-dr-session** HTTP header is still present.

- b) Make a GET request to obtain all vSphere Replication Management Server instances in pairing.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vrs
```

Save the ID of the target vSphere Replication Management Server.

- c) Make a GET request to obtain all vSphere Replication Servers registered to the target vSphere Replication Management Server.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vrs/VR_ID/replication-servers
```

Replace the *PAIRING_ID* value with the ID of the pairing, and the *VR_ID* value with the target vSphere Replication Management Server ID from Step 4.b.

Save the target vSphere Replication Server ID from the result.

5. To get the target datastore, make a GET request.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vcenters/VC_ID/datastores
```

Replace the *VC_ID* value with the ID of the target vCenter Server, and save the response.

6. To get the preferred storage policy ID, make a GET request.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vcenters/VC_ID/storage-policies
```

Replace the *VC_ID* value with the ID of the target vCenter Server, and save the preferred target storage policy ID.

7. To get information about the disks of a VM, make a GET request.

```
GET BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/vcenters/VC_ID/vms/VM_ID/disks
```

Replace the *VC_ID* value with the ID of the source vCenter Server, replace the *VM_ID* value with the ID of the VM which you got in Step 3., and save the response.

8. To configure the replication, make a POST request.

```
POST BASE_URL/api/rest/vr/API_VERSION/pairings/PAIRING_ID/replications
```

Example Configure Replication request body:

```
[
  {
    "auto_replicate_new_disks": true,
    "rpo": 60,
    "lwd_encryption_enabled": false,
    "mpit_days": 0,
    "mpit_enabled": false,
    "mpit_instances": 0,
    "network_compression_enabled": false,
    "quiesce_enabled": false,
    // You get this from Step 3.
    "vm_id": "VirtualMachine:vm-38:fa655d23-b8ac-4eb1-8351-129954807e2c",
    //You get this from Step 4.
    "target_replication_server_id": "HmsRemoteHbrServer:HBRsrv-26c6bd13-1fac-4d04-ad-
cb-2700a258025c:b41aa649-bd9b-45e0-9d41-a7a16c0b0946",
    "target_vc_id": "54d0e5ab-3e9d-4372-9f27-036cf1c24639"
    "disks": [
      {
        // You get this from Step 5.
        "destination_datastore_id": "Datastore:datastore-18:54d0e5ab-3e9d-4372-9f27-036cf1c24639",
```

```

// Options for destination_disk_format parameter: SAME_AS_SOURCE, SAME_AS_PRIMARY, AS_DE-
FINED_IN_PROFILE, FLAT, THICK, NATIVE_THICK, THIN, RDM.
"destination_disk_format": "SAME_AS_SOURCE",
"enabled_for_replication": true,
"use_seeds": false,
"destination_path": "target_folder/test-vm-1",
// You get this from Step 6.
"destination_storage_policy_id": "4b97756b-3c50-481a-a105-d6a7b1507f9a",
// You got this from Step 7.
"vm_disk" : {
  "vm_id": "VirtualMachine:vm-38:fa655d23-b8ac-4eb1-8351-129954807e2c",
  "device_key": 2000,
  "is_vm_home": false,
  "encrypted": false,
  "capacity": 524288,
  "source_disk_format": "THIN",
  "source_path": {
    "datastore_id": "Datastore:datastore-17:fa655d23-b8ac-4eb1-8351-129954807e2c",
    "datastore_name": "local",
    "path": "test-vm-1",
    "filename": "test-vm-1.vmdk"
  },
  "source_storage_policy_name": "Datastore Default",
  "source_storage_policy_id": null,
  "label": "Hard disk 1",
  "controller_key": 1000,
  "controller_label": "SCSI controller 0",
  "supported_for_replication": true
}
},
{
// You get this from Step 5.
"destination_datastore_id": "Datastore:datastore-18:54d0e5ab-3e9d-4372-9f27-036cf1c24639",
"destination_disk_format": "SAME_AS_SOURCE",
"enabled_for_replication": true,
"use_seeds": false,
"destination_path": "target_folder/test-vm-1",
// You get this from Step 6.
"destination_storage_policy_id": "4b97756b-3c50-481a-a105-d6a7b1507f9a",
// You get this from Step 7.
"vm_disk" : {
  "vm_id": "VirtualMachine:vm-38:fa655d23-b8ac-4eb1-8351-129954807e2c",
  "device_key": 0,
  "is_vm_home": true,
  "encrypted": false,
  "capacity": 0,
  "source_disk_format": null,
  "source_path": {
    "datastore_id": "Datastore:datastore-17:fa655d23-b8ac-4eb1-8351-129954807e2c",
    "datastore_name": "local",
    "path": "test-vm-1",
    "filename": "test-vm-1.vmx"
  },
}
},

```

```

    "source_storage_policy_name": "Datastore Default",
    "source_storage_policy_id": null,
    "label": "VM home",
    "controller_key": 0,
    "controller_label": null,
    "supported_for_replication": false
  }
}
]
}
]

```

DR REST API Rate Limiter

The DR REST API Rate Limiter is a mechanism to manage the risks of API resource exhaustion and brute force attacks.

The rate limiter is available in the DR REST API of Site Recovery Manager 8.8 and later and vSphere Replication 8.8 and later. The DR REST API Rate Limiter is a trade off between security and performance.

Table 19: DR REST API Request Rate Limit Tiers

Tier	Description	Configuration	Default Value
IP address	Considers requests per IP address.	<i>ipRateLimitQuota</i>	100
		<i>ipRateLimitWindow</i>	60 000 in ms (1 min)
Service	Considers requests per DR REST API service name. In DR REST API there are three service names: <i>srm</i> , <i>vr</i> , and <i>configure</i> . The 'srm v1' and 'srm v2' have the same service name of 'srm'.	<i>serviceRateLimitQuota</i>	1000
		<i>serviceRateLimitWindow</i>	60 000 in ms (1 min)
Session	Considers requests per session.	<i>sessionRateLimitQuota</i>	50
		<i>sessionRateLimitWindow</i>	60000 in ms (1 min)
n/a	Periodic clean of obsolete request rate limiter data structures to reduce the runtime memory fingerprint. Value of 0 (zero) means no cleanup is performed at all.	<i>rateLimitLogPurgeInterval</i>	7 200 000 in ms (2h)

DR REST API Rate Limiter consists of three tiers which work in a chain to rate limit the incoming requests against the tier's criteria. In case the tier's criteria is met a request response is returned immediately thus skipping the rest of the tier chain. DR REST API Rate Limiter tier chain is IP address, Service, Session in that particular order.

You change the DR REST API Rate Limiter configuration by adding or updating the values of the specified properties in the `dr-rest-api.properties` file. The file is located in the `/opt/vmware/dr-rest/lib/` folder. If a Rate Limiter property is not explicitly defined in the DR REST API `dr-rest-api.properties` configuration file, the Rate Limiter uses the default value. To predefine a configuration value, add the corresponding configuration if missing, and set the required value. The updated values become effective when a new rate limit window begins.

Example of `dr-rest-api.properties` file

```
...
ipRateLimitQuota=100
ipRateLimitWindow=60000
serviceRateLimitQuota=1000
serviceRateLimitWindow=60000
sessionRateLimitQuota=50
sessionRateLimitWindow=60000
rateLimitLogPurgeInterval=0
...
```

HTTP Response

Every DR REST API request response has the following headers.

- *RateLimit-Limit* - the server's quota for requests by the client in the time window.
- *RateLimit-Remaining* - the remaining quota in the current window.
- *RateLimit-Reset* - the time remaining in the current window, specified in milliseconds.

ATTENTION

When an HTTP request is rate limited, the response error code is `429 Too Many Requests` and header *RateLimit-Remaining* is 0 (zero). DR REST API responses contain Rate Limit headers from the last rate limit tier which processed the client request.

Best practices for setting the optimal Rate Limit configuration

Setting up the optimal Rate Limit configuration requires taking into consideration various factors.

- Begin with the default values of the Rate Limiter configurations.
 - *ipRateLimitQuota*, *ipRateLimitWindow*, *serviceRateLimitQuota*, *serviceRateLimitWindow*, *sessionRateLimitQuota*, *sessionRateLimitWindow*
 - *rateLimitLogPurgeInterval*
- Listen for request responses with error code `429 Too Many Requests` and take actions accordingly.
 - Wait for the next rate limit window and repeat the requests which were rate limited.
 - Decrease the request intensity at the client side.
 - Update the Rate Limit configurations - increase the related configuration *RateLimitQuota* and or decrease the related configuration *RateLimitWindow*.
- Analyze the response headers *RateLimit-Limit*, *RateLimit-Remaining*, and *RateLimit-Reset* and takes actions accordingly.
 - Change the request intensity at the client side in the required direction.
 - Update the Rate Limit configurations in the required direction.

Troubleshooting vSphere Replication

Known troubleshooting information can help you diagnose and correct problems that occur while replicating and recovering virtual machines with vSphere Replication.

If you have problems with deploying vSphere Replication, replicating or recovering virtual machines, or connecting to databases, you can troubleshoot them. To help identify the problem, you might need to collect and review vSphere Replication logs and send them to VMware Support.

See [Monitoring and Managing Replications in vSphere Replication](#) to learn about replication states and how to identify replication issues.

You can also search for solutions to problems in the VMware knowledge base at <http://kb.vmware.com>.

Generate vSphere Replication Support Bundle

If you need a vSphere Replication support bundle for system monitoring and troubleshooting, you can use the vSphere Replication VRMS Appliance Management Interface to generate one. A VMware support engineer might request the bundle during a support call.

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

To access and download the vSphere Replication logs, you need access to the vSphere Replication VRMS Appliance Management Interface. vSphere Replication rotates its logs when the log file reaches 50 MB and keeps 50 compressed log files at most. For more options on how to collect automatically vSphere Replication logs, see <https://kb.vmware.com/s/article/2013091>.

NOTE

You can save up to three support bundles at any time. If you generate three support bundles and you try to create a new one, the oldest support bundle is deleted. To save more than one support bundle on large environments, you might need to manually enlarge the support disk on the vSphere Replication Management Server VM. See [Increase the Support Volume for Support Bundles](#).

1. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
2. Click **Summary**, and then click **Download Support Bundle** to generate a .zip package of the current vSphere Replication logs.
A link to the package containing the replication and system logs appears. Log files from the vSphere Replication appliance and all connected Additional vSphere Replication Servers are included in the same package.
3. Click **Download** to download the package.

Increase the Support Volume for Support Bundles

To save more than one support bundle on large environments, you might need to manually increase the support disk on the vSphere Replication Management Server VM.

You can save up to three support bundles at any time. If you generate three support bundles and you try to create a new one, vSphere Replication deletes the oldest one.

If you want to save more than one support bundle on large environments, you might need to manually increase the support disk on the vSphere Replication Management Server VM. On environments with nine additional vSphere Replication servers, each support bundle can be over 1 GB in size, but the support volume for the support bundles is 2 GB.

1. Edit the settings of the vSphere Replication Management Server VM and increase the size of the second virtual disk with 3 GB, from 17 GB to 20 GB.
2. Establish an SSH connection to the vSphere Replication Appliance.
3. Verify that the size of the `/dev/sdb` partition is increased by running the following command:
`fdisk -l`
4. Reboot the vSphere Replication Management Server VM.
5. Once the OS detects the disk size change, increase the physical volume of the disk by running the following command:
`pvresize /dev/sdb`

6. Verify the new volume by running the following command:

```
pvs
```

PSize must be 20 GB and PFree must be 3 GB.
7. Optional: If the sizes are not updated, rescan the physical volume and volume groups by running the following commands:

```
pvscan
```

```
vgscan
```
8. Optional: To verify the size of the `support_vg` volume group, run the following command:

```
vgs
```
9. Increase the size of the support volume by running the following command:

```
lvextend -l +100%FREE -r /dev/support_vg/support
```
10. Verify that the logical volume is created by running the following command:

```
lvscan
```

Verify that `/dev/support_vg/ support` volume is `ACTIVE` and verify its disk size.
11. Optional: To see more information about the new logical volume, run the following command:

```
lvdisplay
```

Manually Access the vSphere Replication Logs

You can copy and use the vSphere Replication logs for system monitoring and troubleshooting. A VMware support engineer might request these logs during a support call.

Use SCP or Win SCP to copy log folders and files from the vSphere Replication appliance and all Additional vSphere Replication Servers.

- `/opt/vmware/hms/logs/`
- `/opt/vmware/var/log/lighttpd/`
- `/var/log/vmware/`
- `/var/log/boot.msg`
- `/var/opt/apache-tomcat/logs/dr.log`

vSphere Replication Events and Alarms

vSphere Replication supports event logging. You can define alarms for each event that can trigger if the event occurs. This feature provides a way to monitor the health of your system and to resolve potential problems, ensuring reliable virtual machine replication.

You can define and edit alarms to alert you when a specific vSphere Replication event occurs, such as after you configure a virtual machine for replication. See the vSphere Client documentation.

List of vSphere Replication Events

vSphere Replication monitors replications and the underlying replication infrastructure, and generates different types of events. The events can be informative, they can give you a warning or notify you there is an error in your environment.

Table 20: vSphere Replication Events

Event Name	Event Description	Event Type	Category	Event Target
vSphere Replication configured	Virtual machine is configured for vSphere Replication	com.vmware.vcHms.replicationConfigured	Configuration	Virtual Machine
vSphere Replication unconfigured	Virtual machine was unconfigured for vSphere Replication	com.vmware.vcHms.replicationUnconfigured	Configuration	Virtual Machine
Host configured for vSphere Replication	Host is configured for vSphere Replication	com.vmware.vcHms.hostConfigured	Configuration	Host System
Host unconfigured for vSphere Replication	Host with managed object id <Host Moid> was unconfigured for vSphere Replication	com.vmware.vcHms.hostUnconfigured	Configuration	Host System
Virtual machine is not configured for vSphere Replication	Virtual machine is experiencing problems with vSphere Replication and must be reconfigured	com.vmware.vcHms.vmMissingReplication	Configuration	Virtual Machine
VM cleaned up from vSphere Replication	Virtual machine cleaned up from vSphere Replication configuration	com.vmware.vcHms.vmReplicationCleanedUp	Configuration	Virtual Machine
RPO violated	Virtual machine vSphere Replication RPO is violated by <x> minutes	com.vmware.vcHms.rpoViolated	Configuration	Virtual Machine
RPO restored	Virtual machine vSphere Replication RPO is not longer violated	com.vmware.vcHms.rpoRestored	Configuration	Virtual Machine
Remote vSphere Replication site is disconnected	Connection to the remote vSphere Replication site <siteName> is down	com.vmware.vcHms.remoteSiteDown	Configuration	Folder
Remote vSphere Replication site is connected	Connection to the remote vSphere Replication site <siteName> is established	com.vmware.vcHms.remoteSiteUp	Configuration	Folder
VR Server disconnected	vSphere Replication server <VR Server> disconnected	com.vmware.vcHms.hbrDisconnected	Configuration	Folder
VR Server reconnected	vSphere Replication server <VR Server> reconnected	com.vmware.vcHms.hbrReconnected	Configuration	Folder

Event Name	Event Description	Event Type	Category	Event Target
Invalid vSphere Replication cleaned up	Virtual machine <VM name> was removed from vCenter Server and its vSphere Replication state was cleaned up	com.vmware.vcHms.replicationCleanedUp	Info	Virtual Machine
Virtual machine recovered from replica	Recovered virtual machine <VM Name> from vSphere Replication image	com.vmware.vcHms.vmRecovered	Info	Virtual Machine
vSphere Replication cannot access datastore	Datastore is not accessible for vSphere Replication Server	com.vmware.vcHms.datastoreInaccessible	Warning	Datastore
vSphere Replication handled a disk addition on a virtual machine	vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name>	com.vmware.vcHms.handledVmDiskAddition	Info	Virtual Machine
vSphere Replication handled a disk removal on a virtual machine	vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name>	com.vmware.vcHms.handledVmDiskRemoval	Info	Virtual Machine
Failed to resolve storage policy	Failed to resolve a specific storage policy for the provided storage profile ID <profile ID> and datastore with managed object ID <Moid>	com.vmware.vcHms.failedToResolveStoragePolicy	Warning	Storage Policy
vSphere Replication paused	vSphere Replication was paused as a result of a configuration change, such as a disk being added or reverting to a snapshot where disk states are different	hbr.primary.SystemPauseEvent	Info	Virtual Machine
Invalid vSphere Replication configuration	Invalid vSphere Replication configuration	hbr.primary.InvalidVmReplicationConfiguration	Warning	Virtual Machine
Sync started	Sync started	hbr.primary.DeltaStartedEvent	Info	Virtual Machine
Application consistent sync completed	Application consistent sync completed	hbr.primary.AppQuiescedDeltaCompletedEvent	Info	Virtual Machine
File-system consistent sync completed	File-system consistent sync completed	hbr.primary.FSQiescedDeltaCompletedEvent	Info	Virtual Machine

Event Name	Event Description	Event Type	Category	Event Target
Unquiesced crash consistent sync completed	Quiescing failed or the virtual machine is powered off. Unquiesced crash consistent sync completed.	hbr.primary.UnquiescedDeltaCompleted	Warning	Virtual Machine
Crash consistent sync completed	Crash consistent sync completed	hbr.primary.DeltaCompleted	Info	Virtual Machine
Sync failed to start	Sync failed to start	hbr.primary.FailedToStartDelta	Error	Virtual Machine
Full-sync started	Full-sync started	hbr.primary.SyncStarted	Info	Virtual Machine
Full-sync completed	Full-sync completed	hbr.primary.SyncCompleted	Info	Virtual Machine
Full-sync failed to start	Full-sync failed to start	hbr.primary.FailedToStartSync	Error	Virtual Machine
Sync aborted	Sync aborted	hbr.primary.DeltaAborted	Warning	Virtual Machine
No connection to VR Server	No connection to vSphere Replication Server	hbr.primary.NoConnectionToVRServer	Warning	Virtual Machine
Connection to VR Server restored	Connection to VR Server has been restored	hbr.primary.ConnectionRestoredToVRServer	Info	Virtual Machine
vSphere Replication configuration changed	vSphere Replication configuration has been changed	hbr.primary.VmReplicationConfigurationChanged	Info	Virtual Machine

Solutions for Common vSphere Replication Problems

Known troubleshooting information can help you diagnose and correct problems with vSphere Replication.

OVF Package Is Invalid and Cannot Be Deployed

When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

The error `OVF package is invalid and cannot be deployed` might appear while you attempt to deploy the vSphere Replication appliance.

This problem is due to the vCenter Server port being changed from the default of 80.

If possible, change the vCenter Server port back to 80.

vSphere Replication Service Fails with Unresolved Host Error

If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.

The vSphere Replication service stops running or does not start after a reboot. The error `unable to resolve host: non-fully-qualified-name` appears in the vSphere Replication logs.

1. In the vSphere Client, select the vCenter Server instance and click the **Configure** tab.
2. Under **Settings**, click **Advanced Settings** and verify that the `VirtualCenter.FQDN` key is set to either a fully qualified domain name or to a literal address.
3. Use a supported browser to log in to the VRMS Appliance Management Interface.
The URL for the VRMS Appliance Management Interface is `https://vr-appliance-address:5480`.
4. Optional: Review and confirm the browser security exception to proceed to the login page.
5. Enter the admin user name and password for the appliance.
You configured the admin password during the OVF deployment of the vSphere Replication appliance.
6. Click **Summary**, and click **Reconfigure**.
7. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.
8. If prompted, click **Connect** to verify the Platform Services Controller certificate.
9. On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.
10. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.
11. On the **Ready to Complete** page, review your settings and click **Finish**.

Error Recovering Virtual Machine in a Single vCenter Server Instance

You might receive an error message when you are recovering a virtual machine with the same name in a single vCenter Server instance.

```
Unable to register the recovered virtual machine VM_name with configuration
file <path_to_vmx_config_file>.
```

You cannot recover virtual machines with the same name in the same source and destination folder in the vCenter Server inventory.

Recover the virtual machine in a different `VMs` and `Templates` folder in the same data center. Optionally, after successful recovery, you can remove the old virtual machine from the vCenter inventory and drag the recovered virtual machine to the required virtual machine folder.

vSphere Replication RPO Violations

You might encounter RPO violations even if vSphere Replication is running successfully at the recovery site.

When you replicate virtual machines, you encounter RPO violations.

RPO violations might occur for one of the following reasons:

- Network connectivity problems between source hosts and vSphere Replication servers at the target site.
- As a result of changing the IP address, the vSphere Replication server has a different IP address.
- The vSphere Replication server cannot access the target datastore.

- Slow bandwidth between the source hosts and the vSphere Replication servers.
To calculate bandwidth requirements, see [Calculate Bandwidth For vSphere Replication](#).
- Search the `vmkernel.log` at the source host for the vSphere Replication server IP address to see any network connectivity problems.
- Verify that the vSphere Replication server IP address is the same. If it is different, reconfigure all the replications, so that the source hosts use the new IP address.
- Check `/var/log/vmware/*hbrsrv*` at the vSphere Replication appliance at the target site for problems with the server accessing a target datastore.
- Verify that you have sufficient bandwidth.

vSphere Replication Appliance Extension Cannot Be Deleted

If you delete the vSphere Replication appliance virtual machine, the VRMS Appliance Management Interface is not available to delete the appliance extension that still exists in vCenter Server.

Deleting the vSphere Replication appliance does not remove the vSphere Replication extension from vCenter Server.

1. Use the Managed Object Browser (MOB) to delete the vSphere Replication extension manually.
2. Redeploy the appliance and reconfigure the replications.

For more information, see [Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted](#).

vSphere Replication Does Not Start After Moving the Host

If you move the ESXi Server on which the vSphere Replication appliance runs to the inventory of another vCenter Server instance, vSphere Replication operations are not available. If you reinstall vCenter Server, vSphere Replication operations are also unavailable.

If the ESXi Server instance on which vSphere Replication runs is disconnected from vCenter Server and is connected to another vCenter Server instance, you cannot access vSphere Replication functions. If you try to restart vSphere Replication, the service does not start.

The OVF environment for the vSphere Replication appliance is stored in the vCenter Server database. When the ESXi host is removed from the vCenter Server inventory, the OVF environment for the vSphere Replication appliance is lost. This action deactivates the mechanisms that the vSphere Replication appliance uses to authenticate with vCenter Server.

1. Optional: If possible, redeploy the vSphere Replication appliance and configure all replications and if possible, reuse the existing .vmdk files as initial copies.
 - a) Power off the old vSphere Replication appliances.
 - b) Remove any temporary `hbr*` files from the target datastore folders.
 - c) Deploy new vSphere Replication appliances and connect the sites.
 - d) Configure all replications, reusing the existing replica .vmdk files as initial copies.
2. Optional: If you cannot redeploy the vSphere Replication appliance, use the VRMS Appliance Management Interface to connect vSphere Replication to the original vCenter Server instance.
 - a) Reconnect the ESXi host to vCenter Server.
 - b) Connect to the VRMS Appliance Management Interface of the vSphere Replication server at `https://vr-server-address:5480`.
3. Click **Summary**, and click **Reconfigure**.
4. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.
5. If prompted, click **Connect** to verify the Platform Services Controller certificate.
6. On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.
7. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.
8. On the **Ready to Complete** page, review your settings and click **Finish**.
9. If you use the VRMS Appliance Management Interface solution, you must repeat the steps each time that you change the vSphere Replication certificate.

Unexpected vSphere Replication Failure Results in a Generic Error

vSphere Replication includes a generic error message in the logs when certain unexpected failures occur.

Certain unexpected vSphere Replication failures result in the error message

```
A generic error occurred in the vSphere Replication Management Server.
```

In addition to the generic error, the message provides more detailed information about the problem, similar to the following examples.

- A generic error occurred in the vSphere Replication Management Server.
Exception details: 'org.apache.http.conn.HttpHostConnectException: Connection to `https://vCenter_Server_address` refused'. This error relates to problems connecting to vCenter Server.
- Synchronization monitoring has stopped. Please verify replication traffic connectivity between the source host and the target vSphere Replication Server. Synchronization monitoring will resume when connectivity issues are resolved. This problem relates to a synchronization operation error.

vSphere Replication sends this message when it encounters configuration or infrastructure errors. For example, network issues, or host overload.

Check the `Exception details` message for information about the problem. Depending on the details of the message, you can choose to retry the failed operation, restart vSphere Replication, or correct the infrastructure.

Reconnecting Sites Fails If One of the vCenter Server Instances Has Changed Its IP Address

When the vCenter Server address of one site changes, the connection status between two sites is displayed as `Not connected` and you cannot reconnect the sites.

If you have two connected sites, and the vCenter Server address of either site changes, the connection status `Not connected` appears and you cannot reconnect the sites.

1. Log in the VRMS Appliance Management Interface for the vSphere Replication appliance that is registered to the vCenter Server whose address has changed.
2. Reconfigure the vSphere Replication appliance with the new vCenter Server address. See [Configure the vSphere Replication Appliance to Connect to a vCenter Server instance](#).
3. In the vSphere Replication user interface, from the list of target sites, select the connection that indicates the `Not connected` status.
4. Select **Site Pair > Summary**, and click **Reconnect**.
5. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**.
If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that vSphere Replication already extends.
6. Verify that the connection between the two sites is successfully restored and the status is `Connected`.

vSphere Replication Server Registration Takes Several Minutes

vSphere Replication server registration might take a long time depending on the number of hosts in the vCenter Server inventory.

If the vCenter Server inventory contains a few hundred or more hosts, the Register VR Server task takes more than a few minutes to complete.

vSphere Replication updates the SSL thumbprint registry of each host. The vCenter Server Events pane displays `Host is configured for vSphere Replication` for each host as the vSphere Replication server registration task progresses.

1. Wait for the registration task to complete.
After it finishes, you can use vSphere Replication for incoming replication traffic.
2. Alternatively, edit `/opt/vmware/hms/conf/hms-configuration.xml` and change the `hms-config-host-at-hbr-threadpool-size` parameter to a higher value to enable parallel processing of more hosts at a time and restart the vSphere Replication management server `/etc/init.d/hms restart`

Generating Support Bundles Disrupts vSphere Replication Recovery

If you generate a vSphere Replication log bundle and at the same time attempt to run a recovery, the recovery might fail.

In heavily loaded environments, generating log bundles can cause vSphere Replication connection problems during recovery operations. Recovery fails with the error

```
A generic error occurred in the vSphere Replication Management Server. Exception details:
'Failed write-locking object: object_ID'.
```

vSphere Replication server is blocked when the log bundle is generated. This situation occurs if the storage for the vSphere Replication virtual machine is overloaded.

Rerun the recovery. If the recovery still fails, reevaluate the storage bandwidth requirements of the cluster on which vSphere Replication is running, and the network bandwidth if the storage is NAS.

vSphere Replication Operations Take a Long Time to Complete

Some vSphere Replication operations might take a long time to complete during a heavy load.

Operations such as recovering virtual machines fail with the following error:

```
Object object_GUID is locked by another ongoing operation in vSphere Replication Management Server. Try again later.
```

When running under heavy load, some vSphere Replication operations might take a longer time to complete and other operations can fail with this error because a background update operation on the replication group is slow and holds a lock on the replication for a long time.

Retry the failed operation after a few minutes.

vSphere Replication Operations Fail with Authentication Error

An error message appears when you try to configure a replication between two sites, though the sites are paired.

If two sites are paired, and, while the vSphere Client is open on the source site, you restart the vCenter Server and the vSphere Replication Management Server on the target site, when you try to configure a replication from the source to the target site, the configuration task fails with the following error message:

```
Cannot verify login credentials. The authentication service infrastructure is not responding..
```

The following error message appears in the HMS log file on the restarted target site:

```
The VMOMI call does not contain an HMS session ID.
```

The following error message appears in the HMS log file on the source site:

```
Cannot check login credentials. Authentication service infrastructure failed.
```

When you establish a connection between two sites, the connection is cached in the user session on both sites. When you restart the vCenter Server and the vSphere Replication Management Server on the target site, the information about user sessions is discarded. Because the vSphere Client is open and connected to the source site, the login data remains cached in the vSphere Replication Management Server. When you configure a replication, the source site tries to connect to the target site using the cached login data. The target site interprets that data as stale and stops the reconnecting thread.

- Refresh the Site Recovery user interface.
- Log out the Site Recovery user interface and log back in.

vSphere Replication Does Not Display Incoming Replications When the Source Site Is Inaccessible

The list of incoming replications between two remote sites fails to populate when the connection to the local site is refused.

When you refresh the incoming replications list on a remote site soon after the connection to the local site has become unavailable, the replications do not display due to a communication error between the two sites.

Refresh the Site Recovery user interface. Alternatively, log out and log in again.

vSphere Replication Is Inaccessible After Changing vCenter Server Certificate

If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.

vSphere Replication uses a certificate-based authentication to connect to vCenter Server. If you change the vCenter Server certificate, vSphere Replication is inaccessible.

The vSphere Replication database contains the old vCenter Server certificate.

1. Log into the VRMS Appliance Management Interface of the vSphere Replication appliance and click **Summary > Reconfigure**.
2. Follow all prompts of the reconfiguration wizard without changing any configuration information. vSphere Replication restarts with the new vCenter Server certificate.
3. Log in to the vSphere Client.
4. On the home page, click **Site Recovery** and click **Open Site Recovery**.
5. On the Site Recovery home page, select a site pair and click **View Details**.
6. Select **Site Pair > Summary**, and click **Reconnect**.
7. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**.
If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that vSphere Replication already extends.
8. Repeat steps 3 to 7 for all available pairings.

vSphere Replication Cannot Establish a Connection to the Hosts

Replications fail because vSphere Replication cannot connect to the hosts.

vSphere Replication needs access to port 80. You might see forbidden HTTP connections in the vSphere Replication logs.

Make sure the vSphere Replication appliance has access to port 80 on the storage hosts.

For a list of ports that must be open for vSphere Replication, see [Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses](#).

Anti-Virus Agent in Firewall Stops Virtual Machine Replication

If a virtual machine contains virus information, an anti-virus agent in the firewall might detect the virus data and stop the connection during replication.

When you reconfigure the replication and start a full sync, the replication stops in the same data block with the virus information in it unless the virus data has moved on the disk. Clones of the disk fail, but other virtual machines of the same size and configuration from the same host replicating to the same destination datastore replicate successfully.

Remove the virus information from the replicated guest to avoid replicating virus information.

Make an exception in the anti-virus rules in the firewall to allow the replication to proceed.

Initial Full Synchronization of Virtual Machine Files to VMware vSAN Storage Is Slow

When using VMware vSAN storage and configuring vSphere Replication on multiple virtual machines, the initial full synchronization takes a long time to complete.

Configuring vSphere Replication on a large number of virtual machines simultaneously when using vSphere Replication with vSAN storage causes the initial full synchronization of the virtual machine files to run very slowly.

Initial full synchronization operations generate heavy I/O traffic. Configuring too many replications at the same time can overload the vSAN storage.

Configure vSphere Replication in batches of a maximum of 20 virtual machines at a time.

Update the Child Replica Disks When Changing the Storage Policy for a vSAN Target Datastore

When you change a target storage policy and the target datastore is vSAN, the base disk storage policy is updated, but the child disk storage policy still refers to the previous storage policy.

1. Reconfigure the replication to exclude the disk from the replication by retaining the replica files.
2. Deactivate the MPIT, if activated.
3. Perform a manual synchronization and verify that the `hbrdisk.*` file is removed. Verify this by checking the vSAN cluster monitoring user interface.
4. Reconfigure the replication to include the previously excluded disk by using the retained disk as a seed.
5. Reconfigure the replication to select the desired storage policy.
6. Activate the MPIT, if deactivated.

Configuring Replication Fails Because Another Virtual Machine Has the Same Instance UUID

You cannot configure a replication because another virtual machine already exists at the target site.

You might see the following error message:

```
Unable to configure replication for virtual machine VM_name because group group_name cannot be created.
Another virtual machine configured_VM_name}' that has the same instance UUID instance_UUID already exists on
protection site source_site_name.
```

This error message might appear on the following occasions.

- If, due to a connectivity issue or some other problem, an orphaned replication remains on one of the sites while it is deleted from the other site, the orphaned replication prevents you from configuring a new replication for the same virtual machine.
- If you have paired two sites and reinstall the vSphere Replication Management server appliance, the other site contains information about the old appliance and database, and prevents you from configuring new replications.
- If you have not reinstalled the vSphere Replication Management server, an orphaned replication exists in your environment. You can force stop this replication to delete it.
 - a) Log in to the vSphere Client.
 - b) On the home page, click **Site Recovery** and click **Open Site Recovery**.
 - c) On the Site Recovery home page, select the site pair which contains the protected site, mentioned in the error message that you received.
 - d) Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
 - e) Click the **Remove** icon and select **Force stop replication(s)**.
- Alternatively, you can use the Managed Object Browser (MOB) of the vSphere Replication Management server to delete the replication.
 - a) Navigate to `https://vrms_address:8043/mob/?vmodl=1`
Where `vrms_address` is the IP address of the vSphere Replication Management server.

- b) Click the **content** value.
- c) Select the replicaManager or replicationManager value, depending on the type of replication you want to delete.
 - For an outgoing replication, click **replication-manager > getOutgoingReplications**.
 - For an incoming replication, click **replica-manager > getIncomingReplications**.
- d) Set the relevant **start**, **count**, **sorters**, and **filter** values.

NOTE

You must set the **start** value to 0 and delete the **sorters** and **filter** values, to invoke the first page of maximum 50 listed replications. For more than 50 replications, you can use paging and make additional calls for the next pages of replications or use the **sorters** and **filter** values.

- e) Click **Invoke Method**.
- f) Locate the replication and click the GID link under **replication** value.
- g) Invoke the **destroy** method to remove the replication.
- If the vSphere Replication Management server on one of the sites was reinstalled or otherwise reset:
 - a) Reinstall the vSphere Replication Management server at the other site or reset its database.
 - b) Connect the sites and register any additional vSphere Replication server appliances.
 - c) Remove any temporary `hbr*` files left over from the target datastore folders.
 - d) Configure all replications, reusing the existing replica `.vmdk` files as replication seeds.

vSphere Replication Operations Run Slowly as the Number of Replications Increases

As you increase the number of virtual machines that you replicate, vSphere Replication operations can run more slowly.

Response times for vSphere Replication operations can increase as you replicate more virtual machines. You possibly experience recovery operation timeouts or failures for a few virtual machines, and RPO violations.

Every virtual machine in a datastore generates regular read and write operations. Configuring vSphere Replication on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O load on the storage. The performance of vSphere Replication depends on the I/O load of the virtual machines that you replicate and on the capabilities of the storage hardware. If the load generated by the virtual machines, combined with the extra I/O operations that vSphere Replication introduces, exceeds the capabilities of your storage hardware, you might experience slow response times.

When running vSphere Replication, if response times are greater than 30 ms, reduce the number of virtual machines that you replicate to the datastore. Alternatively, increase the capabilities of your hardware. If you suspect that the I/O load on the storage is an issue and you are using VMware vSAN storage, monitor the I/O latency by using the monitoring tool in the vSAN interface.

Unable to Establish an SSH Connection to the vSphere Replication Appliance

SSH connections to the vSphere Replication appliance are deactivated.

To apply custom settings to vSphere Replication, you must establish an SSH connection to the vSphere Replication appliance, and modify certain configuration files.

To transfer files from and to the vSphere Replication appliance, you use SCP or SFTP protocol.

Because the SSH connections are deactivated, you cannot apply the changes that you need, and you cannot transfer files.

By default, SSH connections to the vSphere Replication appliance are deactivated to strengthen the security in your environment.

The script configures the vSphere Replication appliance to activate SSH connections.

The Replication Pauses When You Add a New Disk to the Source VM

The replication pauses when you add a new disk to the source virtual machine.

When you add a new disk to the source VM and you have deactivated the automatic replication of new disks, the replication pauses.

vSphere Replication detects the addition of a disk to a VM and generates an event such as `vSphere Replication handled a disk addition on a virtual machine`.

Include or exclude the new disk in the replication.

You can set up and view an alarm for the event by using the vSphere Client. See the *vSphere Administration with the vSphere Client* documentation for details.

The vSphere Replication Appliance Root File System Switches to Read-Only Mode and Login Fails

The vSphere Replication appliance root file system switches to read-only mode, and you cannot log in.

vSphere Replication server cannot update its database and becomes unresponsive. Log in through VRMS Appliance Management Interface, SSH, or console fails. Attempts to use the appliance console to log in result in the following error message:

```
Read-only file system.
```

To prevent data corruption the vSphere Replication appliance is configured to put its root file system in read-only mode when it detects a problem with the underlying storage.

1. Resolve the storage problem or use Storage vMotion to migrate the vSphere Replication appliance to another storage.
2. Reboot the vSphere Replication appliance.
3. Verify that you can log in by using the VRMS Appliance Management Interface and the appliance console.

Configuration of an Encrypted VM Fails with an Error

When you try to configure a replication for an encrypted virtual machine, the process fails with an error.

The message that you see is: `"The replication of encrypted virtual machines requires Secure LWD support. Secure LWD is not available for this VM."`.

By default, when you power on the vSphere Replication appliance, a vSphere Installation Bundle (VIB) is installed on all supported ESXi hosts in the vCenter Server inventory where you deployed the appliance. The automatic installation of the VIB file might fail due to different reasons.

To configure a replication for the encrypted VM, you must verify that the VIB file is installed and running on the ESXi host of the source virtual machine. If not, you must manually install it.

Verify the VIB File Installation

1. Run the shell command `esxcli software vib list` on the source ESXi host.
2. In the results, look for the `vmware-hbr-agent VIB` file.

If the VIB file is not available on the source ESXi host, you must install it manually. See [Manually Install the VIB](#).

Manually Install the VIBFile

1. Temporarily deactivate the firewall on the ESXi host.
2. Establish an SSH connection to the ESXi Server.
3. Run the following command: `$ esxcli software vib install -v https://VR_APPLIANCE_IP:8043/vib/vmware-hbr-agent.vib`
4. Enable the firewall on the ESXi host.

Reprotect Failures on Overloaded Datastores

Reversing replications at large scale during the reprotect operation might fail due to issues caused by an overloaded datastore.

When the OSFS module of a vSAN datastore is overloaded, it might fail with the "Invalid datastore path ..." error even though the path is valid.

Running the vSphere Replication operations at large scale at the same time involves increased number of calls to the datastore which on overloaded datastores might lead to unresponsiveness or fault responses from the datastore.

Decrease the number of concurrent reverse replication tasks in `hms-configuration.xml` from 20 to 15.

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Run the following command:
`/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property throttle-remote-reverse=15`
3. Restart the HMS service.

Reconfigure replication process fails with an error after a long time

Reconfiguring a replication with a target ESXi host that has a disallowed tag, fails with an error.

When you try to reconfigure a replication with a target ESXi host that is tagged with the `vSphereReplication.disallowedHost` tag, the process starts but remains at 0 %. After a long time, it fails with an error:

```
Reconfigure virtual machine replication
...
Unable to complete the reconfiguration task at remote site for replication group 'vm-name' (managed object ID:
'GID-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX'): task 'HTID-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX'. Details: 'No
host can be used to access datastore path '[esxi-host] vm-name.vmdk'. Cause: No host can be used to access
datastore path '[esxi-host] vm-name.vmdk'.
...
```

Remove the `vSphereReplication.disallowedHost` tag from the target ESXi host and reconfigure the replication.

Configuring a replication for a VM with physical mode RDM disk fails with an error

You cannot configure a replication for a virtual machine with physical mode RDM disk even if the disk is excluded from replication .

If you configure a replication for a virtual machine with physical mode, you might see the following error:

```
VRM Server generic error. Check the documentation for any troubleshooting information.
The detailed exception is: HMS can not set disk UUID for disks of VM : MoRef: type =
VirtualMachine, value = , serverGuid = null'.
```

None.

You cannot use custom defined users and roles with vSphere Replication

You cannot configure a replication with a custom user, even if the custom user is assigned all required VRM privileges on both sites.

The error message `Permission to perform this operation is denied` appears on the Target Location page in the Configure Replication wizard.

None. All vSphere Replication operations must be performed with the SSO administrator user on both sites.

VMs that are located in the target folder are overwritten during recovery with vSphere Replication

If the target folder contains a registered virtual machine with the same name as the replicated virtual machine, the registered virtual machine is overwritten during the recovery.

When you start the Recovery wizard, vSphere Replication checks the target folder and displays a dialog box for you to confirm the overwrite operation. On rare occasions, after the target check is complete, and while the wizard is still open, a virtual machine might be registered to the target folder. On these occasions, the virtual machine that was copied to the target folder will be overwritten without further notice.

None.

Generating a support bundle fails

If you try to generate a vSphere Replication support bundle, the process fails.

If the vSphere Replication appliance is not configured and you try to generate a support bundle, the process fails. You must manually generate the support bundles for the vSphere Replication appliance and the embedded vSphere Replication server. The generated files are `/tmp/hms-bundle.tar.gz` and `/tmp/embedded-hbr-bundle.tgz`.

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Run the following commands:


```
/bin/tar --force-local --ignore-failed-read -chvpf /tmp/hms-bundle.tar /opt/vmware/hms/logs /opt/vmware/var/log
/opt/vmware/support/logs/dr /opt/vmware/support/logs/drconfigui
/opt/vmware/support/logs/envoy
/usr/bin/gzip --no-name --quiet --stdout /tmp/hms-bundle.tar > /tmp/hms-bundle.tar.gz
/urs/bin/rm /tmp/hms-bundle.tar
/usr/bin/sudo -u root /usr/bin/hbrsrv-support-bundle.sh -f /tmp/embedded-hbr-bundle.tgz
```
3. Navigate to the VRMS Appliance Management Interface for the respective embedded vSphere Replication server and generate the support bundle.

You cannot configure new replications with network encryption

When you try to configure new replications with network encryption, the network encryption option is not active.

By default, when you power on the vSphere Replication appliance, a vSphere Installation Bundle (VIB) is installed on all supported ESXi hosts in the vCenter Server inventory where the appliance is deployed. The automatic installation of the

VIB file might fail due to different reasons. You must install the vSphere Replication VIB file on each ESXi instance that hosts replication source VM.

1. Temporarily deactivate the firewall on the ESXi host.
2. Establish an SSH connection to the ESXi Server.
3. Run the following command: `$ esxcli software vib install -v https://VR_APPLIANCE_IP:8043/vib/vmware-hbr-agent.vib`.
4. Activate the firewall on the ESXi host.

Replications with network encryption appear in Not Active state

Existing replications that were configured with network encryption enter Not Active state.

By default, when you power on the vSphere Replication appliance, a vSphere Installation Bundle (VIB) is installed on all supported ESXi hosts in the vCenter Server inventory where the appliance is deployed. The automatic installation of the VIB file might fail due to different reasons. You must install the vSphere Replication VIB file on each ESXi instance that hosts replication source VM.

1. Temporarily deactivate the firewall on the ESXi host.
2. Establish an SSH connection to the ESXi Server.
3. Run the following command: `$ esxcli software vib install -v https://VR_APPLIANCE_IP:8043/vib/vmware-hbr-agent.vib`.
4. Activate the firewall on the ESXi host.

You cannot use network encryption for vSphere Replication

When you try to configure network encryption for a replication, the option in the **Configure replication** wizard is inactive.

If you are using an older ESXi version, the `hbr-agent.vib` may not be automatically installed on the ESXi hosts and you cannot configure network encryption for these replications.

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Run the following command: `/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-auto-install-hbragent-vib=false`.
3. Restart the HMS service.
4. Download and install the `hbr-agent.vib` on the ESXi hosts. See [KB 2110304](#).

VMware Aria Operations Management Pack Alerts and Metrics for vSphere Replication

The VMware Aria Operations Management Pack for vSphere Replication lets administrators monitor the health and current status of their underlying vSphere Replication environment in VMware Aria Operations manager.

By using the VMware Aria Operations Management Pack for vSphere Replication 8.8, you can see alarms when a problem occurs with a replication or a virtual machine or when there is an RPO violation. VMware Aria Operations Management Pack for vSphere Replication allows you to also explore various vSphere Replication-related metrics. For example, you can view replication details per VM, such as direction of replication, replication status, and Recovery Point Objective (RPO) violations. You can also monitor replication settings and metrics, such as transferred bytes, last instance sync points, last sync duration, and last sync size.

vSphere Replication Alerts Tracked With VMware Aria Operations Management Pack

You can track the following alerts with the VMware Aria Operations Management Pack for vSphere Replication:

- RPO violations count is greater than 0.
- Virtual machine is in error state.
- Replication is in error state.

vSphere Replication Metrics Tracked With VMware Aria Operations Management Pack

- vSphere Replication site metrics:
 - Is paired
 - Is pair site connected
 - Local vCenter Server name
 - Local vCenter Server address
 - Transferred bytes
 - Incoming replications
 - Outgoing replications
 - Replication within the same vCenter Server instance
 - RPO violations count
 - Health status
 - Are there issues present on the site
 - All issues
- vSphere Replication server metrics:
 - LWD replication network traffic: Total network transfer errors encountered so far
 - LWD replication network traffic: Total number of bytes of incoming network traffic
 - LWD replication network traffic: Throughput (bytes per second) of incoming network traffic
 - LWD replication network traffic: Total number of bytes of outgoing network traffic
 - LWD replication network traffic: Throughput (bytes per second) of outgoing network traffic
 - NFC replication network traffic: Total network transfer errors encountered so far
 - NFC replication network traffic: Total number of bytes of incoming network traffic
 - NFC replication network traffic: Throughput (bytes per second) of incoming network traffic
 - NFC replication network traffic: Total number of bytes of outgoing network traffic
 - NFC replication network traffic: Throughput (bytes per second) of outgoing network traffic
 - Total number of disks currently configured for replication for this server
 - Total number of replication groups (VMs) currently protected by this vSphere Replication server
 - Total number of groups added to this server since the daemon started
 - Total number of groups removed from this server since the daemon started
 - List of user tags
- Virtual machine metrics:
 - Name
 - Direction
 - Status
 - Test recovery state
 - vSphere Replication server name
 - Current RPO violation
 - Is peer healthy
 - Transferred bytes
 - Time spent in RPO violation (%) in the context of the current collection interval

- Replication metrics:
 - vSphere Replication server name
 - vSphere Replication status
 - Name
 - vSphere Replication replication status
 - Target site name
 - RPO
 - Quiescing
 - Network compression
 - Encryption
 - MPIT
 - Last sync duration
 - Last sync size
 - Direction
 - Lag time
 - Auto-replicate new disks

VMware vSphere Replication Security Guide

Provides a concise reference to the security features of vSphere Replication.

About VMware vSphere Replication Security Guide

The *VMware vSphere Replication Security Guide* provides a concise reference to the security features of vSphere Replication.

To help you protect your vSphere Replication installation, this guide describes security features built into vSphere Replication and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of vSphere Replication
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information about obtaining the latest security patches

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of vSphere Replication.

vSphere Replication Security Reference

You can use the Security Reference to learn about the security features of vSphere Replication and the measures that you can take to safeguard your environment from attack.

Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses

The operation of vSphere Replication depends on certain services, ports, and external interfaces.

vSphere Replication Services

The operation of vSphere Replication depends on several services that run on the vSphere Replication virtual appliance.

Table 21: vSphere Replication Services

Service Name	Startup Type	Description
hms	Automatic for the vSphere Replication appliance. Deactivated for the vSphere Replication add-on appliance.	vSphere Replication Management Service
hbrsrv	Automatic	vSphere Replication Service
sshd	Deactivated by default.	SSH Service

Service Name	Startup Type	Description
ntpd	Automatic	Time service for syncing-up with Internet Time Server through Network Time Protocol. NOTE After you install or upgrade a vSphere Replication virtual appliance, you must synchronize the appliance with a time server.
vaos	Automatic	Guest OS initialization that drives network settings, host name settings, ssh keys creation, EULA acceptance, boot scripts execution, and VRMS Appliance Management Interface initialization.
rsyslog	Automatic	The rocket-fast system for log processing.
dr-client	Automatic	Provides Site Recovery Manager Client (Tomcat, HTML5 user interface) functionality.
hms-vpostgres	Automatic	The vPostgres server for the vSphere Replication embedded database.
telegraf	Manual	Plugin-driven server agent for collecting and sending metrics and events. The service is stopped by default.
dr-iperf3	Manual	Tool for active measurements of the maximum achievable bandwidth on IP networks. The service is stopped by default.
auditd	Manual	Component responsible for writing audit records to the disk. The service is stopped by default.
dr-rest	Automatic	Provides vSphere Replication REST API functionality.
dr-client-plugin	Automatic	Provides vSphere Replication plug-in functionality.

Communication Ports

vSphere Replication uses several communication ports and protocols.

The vSphere Replication appliance requires certain ports to be open.

NOTE

vSphere Replication servers must have NFC traffic access to target ESXi hosts.

Table 22: Ports Used by the vSphere Replication Appliance

Source	Target	Port	Protocol	Description
vSphere Replication appliance	Local vCenter Server	80	TCP	Used for initial installation of the HBR agent VIB in hosts that are not managed by vSphere Lifecycle Manager. After the initial VIB deployment, you can close port 80.
vSphere Replication appliance	Remote Lookup Service	443	TCP	All calls to the remote Lookup Service.
Site Recovery HTML 5 user interface	vSphere Replication appliance	443	HTTPS	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.

Source	Target	Port	Protocol	Description
Site Recovery HTML 5 user interface	Local and remote vCenter Server or all vCenter Server instances in Enhanced Linked Mode with a registered vSphere Replication.	443	HTTPS	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.
Site Recovery HTML 5 user interface	Local and remote Platform Services Controller instances or all Platform Services Controller instances in Enhanced Linked Mode with a registered vSphere Replication.	443	HTTPS	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.
Site Recovery HTML 5 user interface	Remote Site Recovery Manager appliance	443	TCP	TCP port 443 must be open when you access the Site Recovery HTML 5 user interface from the vSphere Replication appliance.
vSphere Replication server in the vSphere Replication appliance	Local ESXi host (intra-site)	443	HTTP	Traffic between the vSphere Replication server and the ESXi hosts on the same site.
Local ESXi host (intra-site)	vSphere Replication server in the vSphere Replication appliance	443	HTTP	Traffic between the ESXi hosts and the vSphere Replication server on the same site.
vSphere Replication appliance	Local and remote vCenter Server	443	TCP	All management traffic to the vCenter Server.
vSphere Replication appliance	https://vcsa.vmware.com	443	TCP	Customer Experience Improvement Program (CEIP) for vSphere Replication.
vSphere Replication appliance	Local vCenter Server	9084	HTTP	Used for uploading the HBR agent VIB to vCenter Server during the installation of the VIB file to the source ESXi hosts.
vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site only) on target site	902	TCP and UDP	Traffic between the vSphere Replication server and the ESXi hosts on the same site. Specifically the traffic of the NFC service to the destination ESXi servers.
Browser	vSphere Replication appliance	5480	HTTPS	VRMS Appliance Management Interface.
vSphere Replication appliance	vSphere Replication appliance	8043	SOAP	Inter-site communication from the vSphere Replication Management servers of the source and the target site.
vCenter Server	vSphere Replication appliance	8043	SOAP	Intra-site communication used for SDRS.
vSphere Replication appliance	vSphere Replication server	8123	SOAP	Intra-site management traffic from the vSphere Replication Management server to additional vSphere Replication server in the environment.
ESXi host on the source site	vSphere Replication server at the target site	31031	TCP	Initial and outgoing replication traffic from the ESXi host on the source site to the vSphere Replication appliance or vSphere Replication server at the target site for replication traffic without network encryption.

Source	Target	Port	Protocol	Description
ESXi host on the source site	vSphere Replication server at the target site	32032	TCP	Initial and outgoing replication traffic from the ESXi host on the source site to the vSphere Replication appliance or vSphere Replication server at the target site for replication traffic with network encryption.

If you deploy additional vSphere Replication servers, you must open the ports that vSphere Replication requires on those servers.

Table 23: Ports Used by the vSphere Replication Server

Source	Target	Port	Protocol	Description
vSphere Replication server	ESXi host (intra-site only) on target site	902	TCP and UDP	Traffic between the vSphere Replication server and the ESXi hosts on the same site. Specifically the traffic of the NFC service to the destination ESXi servers.
Browser	vSphere Replication server	5480	HTTPS	VRMS Appliance Management Interface.
vSphere Replication Management server	vSphere Replication server	8123	SOAP	Intra-site management traffic from the vSphere Replication Management server to the vSphere Replication server.
ESXi host on the source site	vSphere Replication server at the target site	31031	TCP	Initial and outgoing replication traffic from the ESXi host on the source site to the vSphere Replication server at the target site for replication traffic without network encryption.
ESXi host on the source site	vSphere Replication server at the target site	32032	TCP	Initial and outgoing replication traffic from the ESXi host on the source site to the vSphere Replication server at the target site for replication traffic with network encryption.

Open Source and Third-Party Components

For the complete text of the open-source licenses, a list of all open-source and third-party components, and the open-source code used in vSphere Replication, you can go to http://www.vmware.com/download/open_source.html and see the *VMware vSphere Replication Open Source and Licenses* section under the *VMware vSphere Open Source* link. If a certain open-source license requires it, the vSphere Replication Open Source Disclosure Package (ODP) contains text files with instructions how to build and replace the software libraries.

vSphere Replication Configuration Files

Some configuration files contain settings that affect the security of vSphere Replication.

NOTE

All security-related resources are protected with the correct permissions and ownership. Do not change the ownership or permissions of these files.

File Location	Description
/opt/vmware/hms/conf/hms-configuration.xml	The default system configuration of the vSphere Replication Management server.
/opt/vmware/hms/conf/embedded_db.cfg	The configuration file for the embedded database .

vSphere Replication Private Key, Certificate, and Keystore

The private key, the certificate, and the keystore of vSphere Replication are located on the vSphere Replication virtual appliance.

NOTE

All security-related resources are protected with the correct permissions and ownership. Do not change the ownership or permissions of these files.

- /etc/vmware/ssl/hbrsrv.crt
- /etc/vmware/ssl/hbrsrv.key
- /opt/vmware/hms/security/hms-keystore.jks
- /opt/vmware/hms/security/hms-truststore.jks

vSphere Replication License and EULA File

The end-user license agreement (EULA) and open source license files are located in the vSphere Replication virtual appliance.

File	Location
Open Source License	/usr/share/doc/vmware-vspherereplication/open_source_licenses.txt
VMware Postgres License	/usr/share/doc/vmware-vspherereplication/VMware_Postgres_11.17.0_open_source_licenses.txt
End-user license agreement	/opt/vmware/etc/isv/EULA/language_code/0

vSphere Replication Log Files

The files that contain system messages are located in the vSphere Replication virtual appliance.

File Location	Description
/opt/vmware/hms/logs/hms-configtool.log	Used to log errors that occurred during the VRMS Appliance Management Interface configuration.
/opt/vmware/hms/logs/hms.n.log.gz	Used to track the runtime information of vSphere Replication Management server. The most recent log file is labeled hms.log, and hms.n.log.gz files contain older log messages. The file with the highest n value contains the most recent messages.
/var/log/vmware/	The folder contains the vSphere Replication server log files. Used to track replication problems.
/opt/vmware/support/logs/dr-client/dr.log	Site Recovery user interface logs.
/opt/vmware/hms/logs/hms-audit.log	vSphere Replication audit logs.

Log Messages Related to Security

The /opt/vmware/hms/logs/hms.log file contains login and logout event messages, authorization error messages, and certificate verification error messages in the following format.

- Login message


```
2015-03-23 15:54:05.558 DEBUG jvsl.security.authentication.sessionmap
[tcweb-5] (..security.authentication.SessionMap) operationID=087657ec-
ef0f-494c-9739-a4af62a5c049-HMS-1033 | Adding new session to the session
map:com.vmware.hms.security.authentication.HmsUserSession@234f4bed:[
com.vmware.vim.binding.hms.UserSession:
key = site_...1b034,
userName = root,
fullName = root ,
loginTime = ...,
lastActiveTime = ...,
hmsServers = null,
locale = en,
messageLocale = en
]
```

- **Logout message**

```
15-03-23 15:54:05.585 INFO jvsl.security.authorization [tcweb-8]
(..security.authorization.SessionAuthorizer) |
HmsSessionManager.HmsSessionManagerLogout called on session-manager by
root@/10.26.233.124:50776 with opId 43263a64-1681-4459-a921-1d9406308dc8-HMS-1036
```

- **Authorization message**

```
2015-06-25 16:10:35.994 INFO jvsl.security.authorization [tcweb-5]
(..security.authorization.SessionAuthorizer) | Authorization for method
"HmsRemoteSiteManager.HmsRemoteSiteManagerFindHmsServer" failed.
(vim.fault.NoPermission) {
faultCause = null,
faultMessage = null,
object = MoRef: type = HmsRemoteSiteManager, value = site-manager, serverGuid =
18327b1a-dac2-44d9-972e-fa9dd99f4e47,
privilegeId = HmsRemote.com.vmware.vcHms.Hms.View
}
```

- **Certificate verification error message**

```
2015-06-25 16:19:13.794 WARN jvsl.sessions [hms-main-thread-1]
(..hms.net.ServerRegistryHms) | Can not start HMS connection to remote site 'some-
address.com'
java.util.concurrent.ExecutionException:
com.vmware.vim.vmomi.client.exception.SslException:
javax.net.ssl.SSLHandshakeException:
com.vmware.vim.vmomi.client.exception.VlsiCertificateException: Server certificate
chain is not trusted and thumbprint doesn't match
```

vSphere Replication User Accounts

You must set up a root and admin accounts for vSphere Replication. The admin account is used to access both the virtual appliance console and the VRMS Appliance Management Interface.

vSphere Replication currently uses the admin account as the administrator of the VRMS Appliance Management Interface. No other user is created.

When you deploy the vSphere Replication virtual appliance, you set the password for the root and admin accounts in the OVF Deployment wizard.

The root and admin passwords must be at least 8 characters long.

Privileges Assigned to Default User Roles

vSphere Replication includes a set of roles. Each role includes a set of privileges, which allow users with those roles to complete different actions.

See the topic vSphere Replication Roles and Permissions in the *VMware vSphere Replication Installation and Configuration Guide*.

Security Updates and Patches for vSphere Replication

The vSphere Replication virtual appliance uses VMware Photon OS 4.0 as the guest operating system.

You can apply the latest security update or patch by using the corresponding ISO file.

Before you apply an update or patch to the guest operating system, take into account the dependencies. See [Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses](#).

To receive the latest security announcements, you can subscribe to the [VMware Security Announcements mailing list](#).

Using the VMware Aria Automation Orchestrator Plug-In for vSphere Replication 8.8

Provides information and instructions about configuring and using the Automation Orchestrator plug-in for vSphere Replication.

Using the vSphere Replication Plug-In

Using vSphere Replication Plug-In provides information and instructions about configuring and using the VMware®VMware Aria Automation Orchestrator plug-in for VMware vSphere Replication.

Intended Audience

The information in *Using vSphere Replication Plug-In* is intended for experienced administrators who want to automate replication and configuration tasks on a vSphere environment using the vSphere Replication plug-in. The information is written for experienced users who are familiar with virtual machine technology, with VMware Aria Automation Orchestrator workflow development, and with VMware vSphere Replication.

For more information about VMware Aria Automation Orchestrator, see the *VMware Aria Automation Orchestrator Documentation*.

For more information about vSphere Replication, see the *VMware vSphere Replication Documentation*.

Automated Operations That VMware Aria Automation Orchestrator Plug-In for vSphere Replication Provides

The VMware Aria Automation Orchestrator plug-in for vSphere Replication extends automation capabilities for certain vSphere Replication operations.

The vSphere Replication plug-in includes VMware Aria Automation Orchestrator actions, workflows, and scripting objects to expose selected elements of the vSphere Replication API to workflows. With the plug-in you can automate the configuration of replication for virtual machines, manage local and remote site, and synchronize virtual machine data.

The plug-in provides actions and workflows to configure and manage replications:

- Configure a forward replication for virtual machines from a source to a target vCenter Server site.
- Configure a forward replication for virtual machines from a target to a source vCenter Server site.
- Pause, resume, or stop a forward replication for virtual machines from a source to a target vCenter Server site.
- Pause, resume, or stop a reverse replication for virtual machines from a target to a source vCenter Server site.

The plug-in provides actions and workflows to manage remote sites:

- Pair the local site with a target vCenter Server site.
- Register a vCenter Server site.
- Unregister a vCenter Server site.

The plug-in provides actions and workflows to synchronize virtual machine data:

- Full synchronization to a target vCenter Server site.
- Offline synchronization to a target vCenter Server site.
- Synchronize a replication to a target vCenter Server site.

The plug-in provides actions and workflows to retrieve information about the status or configuration details of replications. You can use the results of the workflows as parameters in other workflows:

- Retrieve the status of a replication.
- Retrieves the configuration details of a replication.
- Retrieves a list of all the incoming or outgoing replications from a vCenter Server.
- Get replication IDs, issues, RPO violations, recovery solutions, and test bubble status.

Installing the vSphere Replication Plug-In

To create and run workflows on the local vSphere Replication site, you must install and configure the vSphere Replication plug-in in VMware Aria Automation Orchestrator.

Functional Prerequisites

To install and use the vSphere Replication plug-in, your system must meet certain functional prerequisites.

vSphere Replication

Your vSphere Replication plug-in version works only with the corresponding vSphere Replication version.

For information about setting up vSphere Replication, see the *vSphere Replication Installation and Configuration* documentation.

VMware Aria Automation Orchestrator

Verify that you have a running instance of VMware Aria Automation Orchestrator and its version is compatible with the versions of your vSphere Replication and vSphere Replication plug-in.

For information about the compatibility between vSphere Replication and VMware Aria Automation Orchestrator, see the *vSphere Replication 8.8 Release Notes* and the *Compatibility matrices for vSphere Replication* documentation.

For information about setting up VMware Aria Automation Orchestrator, logging in the VMware Aria Automation Orchestrator client, and available authentication methods, see the *Installing and Configuring VMware VMware Aria Automation Orchestrator* documentation.

Other Prerequisites

- Verify the compatibility between the vCenter Server plug-in for VMware Aria Automation Orchestrator and the vCenter Server. See the *VMware Aria Automation Orchestrator 8.8 Release Notes*.
- Verify that you have added all vCenter Server instances that you want to use for replications, and all peer sites, by using the Add vCenter Server workflow. For more information, see the *Configure the Connection to a vCenter Server Instance* topic in the VMware Aria Automation Orchestrator documentation.

Installing, Upgrading, and Uninstalling the vSphere Replication Plug-In

You can use the vSphere Replication plug-in after you install it in an VMware Aria Automation Orchestrator instance. The version of vSphere Replication plug-in must be compatible with your vSphere Replication and VMware Aria Automation Orchestrator.

Installing the vSphere Replication Plug-In

You can install the vSphere Replication plug-in if your VMware Aria Automation Orchestrator instance is configured to work with your vSphere environment.

You must configure VMware Aria Automation Orchestrator to use the vSphere environment. For information about how to configure your VMware Aria Automation Orchestrator to work with a vSphere environment, see the *Configuring VMware Aria Automation Orchestrator* section in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

You can download the vSphere Replication plug-in installation `.vmoapp` file from the download page of vSphere Replication.

You can install the vSphere Replication 8.8 plug-in in VMware Aria Automation Orchestrator 8.x by using the `https://your_orchestrator_host/vco-controlcenter/config/#/` configuration interface, click **Manage Plug-Ins** and upload the file. For more information about how to manage the VMware Aria Automation Orchestrator plug-ins, see the *Manage the Orchestrator Plug-Ins* topic in the *Installing and Configuring VMware Realize Orchestrator* documentation.

Upgrading the vSphere Replication Plug-In

You can upgrade your vSphere Replication plug-in by uninstalling the previous version and installing the new version.

NOTE

After you upgrade the vSphere Replication plug-in, you cannot revert to a previous version without doing a reinstallation.

Uninstalling the vSphere Replication Plug-In

You can uninstall your vSphere Replication plug-in by using the `http://your_orchestrator_host/vco-controlcenter/config/#/` configuration interface. For more information about uninstalling the vSphere Replication plug-in, see the *Uninstall a Plug-in* topic in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

Using the vSphere Replication Plug-In Workflows

The vSphere Replication plug-in workflow library contains workflows that you can use to automate vSphere Replication tasks. With the predefined workflows you configure and control replications for virtual machines, add, pair, or remove remote sites. You can use the predefined workflows and the scripting API of the plug-in to create custom workflows.

Available Workflows in vSphere Replication Plug-In

vSphere Replication plug-in provides Remote Site Management and Synchronization workflows, Configure, Reconfigure, Pause, Resume and Stop Replication workflows, and Replication Details workflows.

Table 24: Configure Replication Workflows

Workflow	Description of operation
Configure Replication	Configure a replication for a virtual machine from a local site to a target vCenter Server site.
Protect Multiple VMs	Configure a replication for multiple virtual machines to a vCenter Server site.
Reconfigure Replication	Change the settings of a replication, including reconfiguring a replication on new virtual hard disks and enabling the default seed to use a replica disk in the VM folder.

Table 25: Remote Site Management Workflows

Workflow	Description of operation
Pair with a VC Site	Connect and pair a local site to a remote vCenter Server site.
Reconnect a VC to VC pair	Reconfigures the pairing between two vCenter Server sites.
Configure VR plugin Connection Settings	Configure the vSphere Replication plug-in connection settings.
Login to VC Site	Login to a selected vCenter Server site.
Login to VC Site with credentials	Login with credentials to a selected vCenter Server site paired with a local vCenter Server site.
Register VC site	Register login credentials for a paired vCenter Server site.
Unregister VC Site	Delete stored login credentials for a paired vCenter Server site.

Table 26: Replication Actions Workflows

Workflow	Description of operation
Full Sync Replication to VC	Run an initial full synchronization for a replicated virtual machine to a remote vCenter Server site.
Offline Sync Replication to VC	Run an offline synchronization for a replicated virtual machine to a remote vCenter Server site.
Pause Replication to VC	Pause a replication for a virtual machine from a local site to a remote vCenter Server site.
Resume Replication to VC	Resume a replication for a virtual machine from a local site to a remote vCenter Server site.
Stop Replication	Stop a replication for a virtual machine from a local site to a remote vCenter Server site.
Sync Replication to VC	Run a delta synchronization for a replicated virtual machine to a remote vCenter Server site.

Table 27: Replication Details Workflows

Workflow	Description of operation
Check Replication Status	Retrieves the status of a replication. You can use the returned value as a parameter in another workflow.
Get Replication Configuration	Retrieves the configuration details of a replication. You can use the returned value as a parameter in another workflow.
Get Replication IDs	Retrieves a list of the internal values (IDs) of all outgoing replications, or for the replications which match the provided full or partial replication name.
Get Replication Issues	Retrieves a list of all the current issues for all incoming or outgoing replications.
Get Replication List	Retrieves a list of all the incoming or outgoing replications from a vCenter Server. You can use the returned value as a parameter in another workflow.
Get Replication Recovery Solution	Retrieves the replication recovery solution or an error message from the vSphere Replication Management Server.
Get Replication RPO Violation	Retrieves a list of all recovery point objective (RPO) violations.

Workflow	Description of operation
Get Replication Test Bubble Status	Returns a string indicating whether the replication has a test bubble or not. Requires credentials for the target vCenter Server.

Prerequisites for Using the vSphere Replication Plug-In

To use vSphere Replication plug-in, your environment must meet certain requirements.

- Before managing the objects in your vSphere inventory by using VMware Aria Automation Orchestrator and running workflows on the objects, you must configure the vCenter Server plug-in and define the connection parameters between VMware Aria Automation Orchestrator and the vCenter Server you want to orchestrate. For information about how to configure your VMware Aria Automation Orchestrator to work with a vSphere environment, see the *Configuring VMware Aria Automation Orchestrator* section in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.
- Before running workflows to or from a target site, verify that you have created a session to the desired vCenter Server site, by using the *Login to vCenter Server Site with Credentials* workflow.
- Before running workflows to or from a target site, verify that you have added the vCenter Server by running the *Add a vCenter Server Instance* workflow. For more information, see the *VMware Aria Automation Orchestrator Product Documentation*.

Finding Common Objects in the vSphere Replication Plug-In

You can expand the basic workflows and actions in the VMware Aria Automation Orchestrator client, by combining them with other workflows.

You do this by populating the input fields in the basic workflows with the correct objects. You can find some of the most common objects by running the following scripts.

See *Developing Workflows with VMware Aria Automation Orchestrator* in the VMware Aria Automation Orchestrator Documentation.

Table 28: All Primary Sites in the Inventory

Description	Script
The second parameter in the script is optional and it can be a partial name of the site. The script returns an array of site objects (<code>com.vmware.hms.o11n.model.Site</code>).	<code>Server.findAllForType('VR:Site','')</code>

Table 29: A Specific Primary Site

Description	Script
The second parameter in the script is required and it must be the FQDN of the site. The script returns a site object (<code>com.vmware.hms.o11n.model.Site</code>).	<code>Server.findForType('VR:Site', 'PRIMARY_SITE_FQDN');</code>

Table 35: All Storage Profiles for the Remote Site

Description	Script
Find all storage profiles for the remote site as an array of <code>VRStorageProfile</code> objects. You must be logged in the remote site.	<code>selectedRemoteSite.getStorageProfiles();</code>

Table 36: VMs That Match a Criteria

Description	Script
Find VMs that match a particular condition, for example all VMs, which contain the string <code>accounting</code> .	<code>Server.findAllForType('VC:VirtualMachine', 'SEARCH_CRITERIA');</code>

Table 37: All Supported Disk Formats as an Array

Description	Script
Find all supported disk formats as an array of <code>VRDisktype</code> objects. The relevant fields are Name and ID.	<code>VRPluginConfig.getSupportedDiskFormats()</code>

Configure Replication Workflows

With **Configure Replication** workflows in vSphere Replication plug-in, you can configure replication for virtual machines between the local site and remote vCenter Server sites.

When you configure a virtual machine for replication, vSphere Replication starts an initial configuration task during which the data of the virtual machine is sent to the target site. When you recover the replication, this creates the replica of the virtual machine and data synchronization occurs between the source and the target site. You can set multiple point in time (MPIT) instances in the recovery settings of the selected workflow. vSphere Replication retains a maximum of 24 of snapshot instances of the virtual machine on the target site.

You can configure replications for powered-off virtual machines, but the data synchronization begins when the virtual machine is powered on. When the source virtual machine is powered off, the replication appears in `Not active` status.

NOTE

Each vSphere Replication local and remote site pair (A -> B) has four different possible relations. The regular site relations are A -> B and B -> A and the relations within the same vCenter Server are A -> A and B -> B. When you select a remote site in a workflow, it has the same name regardless if it is A -> B (regular local site - remote site pair) or B -> B (pair within the same vCenter Server). Make sure you select the correct site by checking `vcRemoteSite.uri` to get the source site address and `vcRemoteSite.localSiteUri` to get the target site address.

Configure Replication Workflow

The workflow configures replication for a virtual machine from the local site to another vCenter Server site.

- Verify that the vSphere Replication appliance is deployed at the source and the target sites.
 - To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.
1. Log in to VMware Aria Automation Orchestrator client as an administrator.
 2. Navigate to **Library > Workflows**.
 3. In the **Filter** box, enter `Configure Replication` and press **Enter**.
 4. Click the workflow and click **Run**.
 5. Enter the input parameters that the workflow requires, and click **Run**.

Table 38: Configure Replication Workflow Inputs

Input		Description	
Source Site	Site	Local vCenter Server site.	
Source VM	Source VM	Virtual machine to be replicated.	
Target Site	Site	Remote vCenter Server site.	
Target Datastore	Per disk configuration		Configure the storage policy and datastore per virtual disk. The elements in the array must correspond to each other in order. For example, the first element from Disk format per disk must correspond to the first element in VM disks for replication and so on.
	Per disk configuration enabled	VM disks for replication	Array of disks to be replicated to the remote site.
		VM disks excluded from replication	Array of disks to be excluded from the replication to the remote site.
		Disk format per disk	Virtual disk format and provisioning type per virtual disk. The array size must be the same as the array size in VM disks for replication .
		Storage profile per disk	Virtual machine storage policy profile per virtual disk. The array size must be the same as the array size in VM disks for replication .
		Target datastore per disk	Remote datastore to replicate to, per virtual disk. The array size must be the same as the array size in VM disks for replication .
	Per disk configuration disabled	Disk format	Virtual disk format and provisioning type.
		Storage profile	Virtual machine storage policy profile.
		Target Datastore	Remote datastore to replicate to.
		Use Default Replication Seed	Use the default virtual machine disk files for an initial synchronization.
	Auto replicate new disks	Automatically include new disks in the replication.	

Input		Description
Details	RPO in minutes	Recovery point objective in minutes (default value is 240).
	Guest OS quiescing	Enabling OS quiescing improves data consistency, but limits RPO time.
	Network compression	Enabling replication data compression reduces the network bandwidth, but increases the CPU use.
	Point in time instances	Maximum supported number of snapshots per virtual machine is 24.
	Enable encryption for VR data	Enabling vSphere Replication data encryption.
MPIT (If Points in time instances is enabled)	Instances per day (multiplied by number of days should not exceed 24)	Number of snapshots taken per day.
	Number of days	Number of days for which snapshots are kept.

Protect Multiple Virtual Machines Workflow

The workflow configures replication for multiple virtual machines from the local site to the remote vSphere site.

- Verify that you have configured the connection between your local site and the remote vCenter Server site. For more information, see [Pair with a vCenter Server Site Workflow](#).
- Verify that you have registered the login credentials for the remote vCenter Server site, that you want to use. See [Register vCenter Server Site Workflow](#).

If one or all the selected virtual machines are not powered on, replication is configured but full initial synchronization is completed upon powering on the virtual machines. You can run the workflow with a replicated virtual machine included in the VM array, however the workflow does not reconfigure the replication for that virtual machine. The rest of the virtual machines included in the VM array which are not already replicated are configured for replication.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Protect multiple VMs` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 39: Protect Multiple Virtual Machines Workflow Inputs

Input		Description
Source Site	Site	Local vCenter Server site.
Source VM	Source VMs	Array of virtual machines to be replicated to the remote site.
Target Site	VC site to be used as replication target	Select an available vCenter Server site to be used as a replication target.
Target Datastore	Disk type	Virtual disk format and provisioning type.
	Storage profile	Virtual machine storage policy profile.
	Target datastore	Datastore to replicate to, if the target is vCenter Server site.
	Use replication seeds	Use the default virtual machine disk files for an initial synchronization.

Input		Description
	Auto replicate new disks	Automatically include new disks in the replication.
Details	RPO in minutes	Recovery point objective in minutes (default value is 240).
	Guest OS quiescing	Enabling OS quiescing improves data consistency but limits RPO time.
	Network compression	Enabling replication data compression reduces the network bandwidth, but increases the CPU use.
	Point in time instances	Maximum supported number of snapshots per virtual machine is 24.
	Enable encryption for VR data	Enabling vSphere Replication data encryption.
Replication Settings (Points in time instances enabled)	Instances per day (multiplied by number of days should not exceed 24).	Number of snapshots taken per day.
	Number of days	Number of days for which snapshots are kept.

Reconfigure Replication Workflow

With this workflow, you can change the settings of a replication, including reconfiguring a replication on new virtual hard disks and enabling the default seed to use a replica disk in the VM folder.

- Verify that the vSphere Replication appliance is deployed at the source and the target sites.
- To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Reconfigure Replication` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 40: Reconfigure Replication Workflow Inputs

Input		Description	
Source	Replication	The replication you want to reconfigure.	
Disks	Per disk configuration		
	Configure the storage policy and datastore per virtual disk. The elements in the array must correspond to each other in order. For example, the first element from Disk format per disk must correspond to the first element in VM disks for replication and so on.		
	Per disk configuration enabled	Enabled Disks for Replication	Array of disks to be replicated to the remote site.
		Excluded Disks From Replication	Array of disks to be excluded from the replication to the remote site.
Disk format per disk		Virtual disk format and provisioning type per virtual disk. The array size must be the same as the array size in VM disks for replication .	

Input		Description	
		Storage profile per disk	Virtual machine storage policy profile per virtual disk. The array size must be the same as the array size in VM disks for replication .
		Target datastore per disk	Remote datastore to replicate to, per virtual disk. The array size must be the same as the array size in VM disks for replication .
	Per disk configuration disabled	Disk format	Virtual disk format and provisioning type.
		Storage profile	Virtual machine storage policy profile.
		Target Datastore For All Enabled Disks	Remote datastore to replicate to. When you change this datastore, all disks move to the new target datastore.
	Use default replication seeds		Use the default virtual machine disk files for an initial synchronization.
	Auto replicate new disks		Automatically include new disks in the replication.
Details	RPO in minutes		RPO in minutes
	Guest OS quiescing		Enabling OS quiescing improves data consistency, but limits RPO time.
	Network compression		Enabling replication data compression reduces the network bandwidth, but increases the CPU use.
	Enable encryption for VR data		Enabling vSphere Replication data encryption.
	Point in time instances		Maximum supported number of snapshots per virtual machine is 24.
MPIT (If Points in time instances is enabled)	Instances per day (multiplied by number of days should not exceed 24)		Number of snapshots taken per day.
	Number of days		Number of days for which snapshots are kept.

Remote Site Management Workflows

With **Remote Site Management** workflows, you can configure the connection between the local site and the remote site managed by a different vCenter Server. Before you configure replication tasks to the remote sites, you must pair the local and the remote sites.

Pair with a vCenter Server Site Workflow

The workflow configures the connection between the local site and a remote vCenter Server site.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Pair with a VC Site` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 41: Pair with a vCenter Server Site Workflow Inputs

Input		Description
Local site	Local site	Local vCenter Server site.
	Local site Lookup Service address	IP address or domain name of the server where the Lookup Service runs.
Remote site	Remote site Lookup Service address	IP address or domain name of the server where the Platform Services Controller of the remote vCenter Single Sign-On domain runs.
	Remote username	Remote vCenter Single Sign-On user.
	Password	Password for the remote vCenter Single Sign-On user.
	Ignore certificate warnings	When you select it, the certificate is accepted silently and added to the trusted store.

Reconnect a vCenter Server Site to a vCenter Server Site Pair Workflow

This workflow reconfigures the pairing between two vCenter Server sites.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Reconnect a VC to VC pair` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 42: Reconnect a vCenter Server Site to a vCenter Server Site Pair Workflow Inputs

Input		Description
Local site	Local site	Local vCenter Server site.

Input	Description	
	Local site Lookup Service address	IP address or domain name of the server where the Lookup Service runs.
Remote site	Remote site Lookup Service address	IP address or domain name of the server where the Platform Services Controller of the remote vCenter Single Sign-On domain runs.
	Remote username	Remote vCenter Single Sign-On user.
	Password	Password for the remote vCenter Single Sign-On user.
	Ignore certificate warnings	When you select it, the certificate is accepted silently and added to the trusted store.

Configure vSphere Replication Plug-in Connection Settings Workflow

The workflow configures the vSphere Replication plug-in connection settings.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Configure VR plugin Connection Settings` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the maximum number of connections and the connection timeout, and click **Run**.

You can view the workflow status in the **Value** column of the **Variables** tab of the workflow. You can use the value as a parameter in another workflow.

Log In to a vCenter Server Site Workflow

The workflow performs a login to a selected vCenter Server site for replications within a single vCenter Server instance.

1. Configure the connection to a vCenter Server instance, by running the `Add a vCenter Server Instance` workflow. For more information, see the *VMware Aria Automation Orchestrator Product Documentation*.
2. Register the target site by running the `Register VC Site` workflow.
 1. Log in to VMware Aria Automation Orchestrator client as an administrator.
 2. Navigate to **Library > Workflows**.
 3. In the **Filter** box, enter `Login to VC Site` and press **Enter**.
 4. Click the workflow and click **Run**.
 5. Select a vCenter Server site and click **Run**.

Log in to a vCenter Server Site with Credentials Workflow

The workflow performs a login with credentials to a selected vCenter Server site that is paired with a local vCenter Server site.

Configure the connection to a vCenter Server instance, by running the `Add a vCenter Server Instance` workflow. For more information, see the *VMware Aria Automation Orchestrator Product Documentation*.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Workflows > Library**.
3. In the **Filter** box, enter `Login to VC Site with credentials` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 43: Log in to a vCenter Server Site with Credentials Workflow Inputs

Input	Description
Remote vSphere Site	Remote vCenter Server site.
User name	User name for the remote vCenter Server site.
Password	Password for the remote vCenter Server.

Register vCenter Server Site Workflow

The workflow registers the login credentials for a remote vCenter Server site.

Verify that the local site is paired with a vCenter Server site. See [Pair with a vCenter Server Site Workflow](#).

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Register VC Site` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the paired remote vCenter Server site address.
6. Select whether to ignore the certificates warnings and click **Run**.
If you select it, the certificate is accepted silently and added to the trusted store.

Unregister vCenter Server Site Workflow

The workflow removes the stored credentials for a vCenter Server site paired with the local site. The workflow does not break the pairing.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Unregister VC Site` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the vCenter Server site that you want to unregister and click **Run**.

Sync Workflows

With synchronization workflows you can replicate data for virtual machines with configured replication between the local site and a remote vCenter Server site.

Full Sync Replication to vCenter Server Workflow

The workflow runs a full synchronization for a virtual machine with a configured outgoing replication from the local site to the target vCenter Server site.

Verify that the virtual machine for which you want to run a full synchronization is powered on.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Full Sync Replication to VC` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication that you want to sync and click **Run**.

Offline Sync Replication to vCenter Server Workflow

The workflow runs an offline synchronization for a virtual machine with a configured outgoing replication to the target vCenter Server site.

Verify that the source virtual machine is powered off.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Offline Sync Replication to VC` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication that you want to sync and click **Run**.

Sync Replication to vCenter Server Workflow

The workflow runs a delta synchronization for a virtual machine with a configured outgoing replication to the target vCenter Server site.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Sync Replication to VC` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication that you want to sync and click **Run**.

Pause Workflows

With **Pause** workflows, you can pause replications for virtual machines between the source and the target sites. When a replication is paused, all synchronization calls are blocked and no data is synchronized between the source and the target sites. The replication is not unconfigured and can be resumed.

Pause Replication to vCenter Server

The workflow pauses the replication for a virtual machine from the local site to a remote vCenter Server site.

Verify that you have a configured replication from the local site to a remote vCenter Server site. See [Configure Replication Workflow](#) or [Protect Multiple Virtual Machines Workflow](#).

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the search box, enter `Pause Replication to VC` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication that you want to pause and click **Run**.

Resume Workflows

With **Resume** workflows, you can resume paused replications configured between the local site and remote vCenter Server sites.

Resume Replication to vCenter Server Workflow

The workflow resumes a paused forward replication to the target vCenter Server site.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Resume Replication to VC` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication that you want to resume and click **Run**.

Stop Replication Workflows

With **Stop Replication** workflows, you can stop replications for virtual machines configured between the local and remote vCenter Server sites. When you stop a replication, the replication is unconfigured. If you did not select the **Leave replica disks** option, the replicated data at the target location is removed.

Stop Replication Workflow

The workflow stops a forward replication for a virtual machine to a target vCenter Server site.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Stop Replication` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 44: Stop Replication Workflow Inputs

Input	Description
Site	Remote vCenter Server site.
Replication	Virtual machine for which replication is stopped.
Leave replica disks	Leave the replicated disks intact when you stop a replication.

Replication Details Workflows

With the **Replication Details** workflows, you can retrieve information about the status or configuration details of replications. You can retrieve a list of all incoming or outgoing replications from a source vCenter Server. You can use the results of the workflows as parameters in other workflows.

Check Replication Status Workflow

The workflow retrieves the status of a replication.

Verify that you have a configured replication.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Check Replication Status` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select a replication for which you want to run a verification of the status and click **Run**.

You can view the replication status in the **Value** column of the **Variables** tab of the workflow. You can use the value as a parameter in another workflow.

Get Replication Configuration Workflow

The workflow retrieves the configuration details of a replication.

Verify that you have a configured a replication.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Get Replication Configuration` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication for which you want to retrieve the configuration information and click **Run**.

You can view the replication configuration information in the **Value** column of the **Variables** tab of the finished workflow. You can use the value as a parameter in another workflow.

Get Replication List Workflow

The workflow retrieves a list of all the incoming or outgoing replications from a vCenter Server.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter the `Get Replication List` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 45: Get Replication List Workflow Inputs

Input	Description
Source Site	Source vCenter Server Site.
Replication direction	Direction of the replication that you want to retrieve.
Remote Site	Remote vCenter Server Site.

You can view the list of replications in the **Value** column of the **Variables** tab of the finished workflow. You can use the value as a parameter in another workflow.

Get Replication Issues Workflow

This workflow retrieves a list of all the current issues for all incoming or outgoing replications.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter the `Get Replication Issues` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 46: Get Replication Issues Workflow Inputs

Input	Description
Local Site	Local vCenter Server site.
Outgoing	Select to display issues for outgoing replications. Deselect to display issues for incoming replications.
Remote Site (optional)	Add a particular remote vCenter Server site if more than a single pair of sites is connected.

Get Replication IDs Workflow

This workflow retrieves a list of the internal values (IDs) of all outgoing replications, or for the replications which match the provided full or partial replication name.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter the `Get Replication Ids` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 47: Get Replication IDs Workflow Inputs

Input	Description
Source Site	Local vCenter Server site.
Replication name (Optional)	Full or partial name of the replications whose IDs you want to retrieve. The workflow displays the IDs of the first 100 replications, which contain the Replication name value in their name.

Get Replication Recovery Solution Workflow

The workflow retrieves the replication recovery solution or an error message from the vSphere Replication Management Server.

Verify that you have the credentials for the target vCenter Server.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Get Replication Recovery Solution` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication for which you want to retrieve a replication recovery solution.
6. Enter the target vCenter Server credentials and click **Run**.

You can view the workflow run information in the **Value** column of the **Variables** tab of the finished workflow. You can use the value as a parameter in another workflow.

Get Replication Recovery Point Objective Violation Workflow

The workflow retrieves a list of all recovery point objective (RPO) violations.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Get Replication RPO Violation` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication for which you want to get the list with the RPO violations and click **Run**.

You can view the workflow run information in the **Value** column of the **Variables** tab of the finished workflow. You can use the value as a parameter in another workflow.

Get Replication Test Bubble Status Workflow

The workflow returns a string indicating whether the replication has a test bubble or not.

1. Log in to VMware Aria Automation Orchestrator client as an administrator.
2. Navigate to **Library > Workflows**.
3. In the **Filter** box, enter `Get Replication Test Bubble Status` and press **Enter**.
4. Click the workflow and click **Run**.
5. Select the replication for which you want to get a test bubble status.
6. Enter the target vCenter Server credentials and click **Run**.

You can view the workflow run information in the **Value** column of the **Variables** tab of the finished workflow. You can use the value as a parameter in another workflow.

Troubleshooting the VMware Aria Automation Orchestrator Plug-In for vSphere Replication

Known troubleshooting information can help you diagnose and correct problems that occur while using the VMware Aria Automation Orchestrator Plug-In for vSphere Replication.

Incorrect remote site object is retrieved when using the vSphere Replication Plug-in through VMware Aria Automation

When using the vSphere Replication Plug-in through VMware Aria Automation with a combination of configuration elements, you cannot retrieve the correct remote site object.

You cannot retrieve the virtual machine, because the incorrect remote site object (`VR:VcRemoteSite`) was selected, after being stored in a configuration element. The process fails with the following error:

```
The object '<VM_ID>' has already been deleted or has not been completely created
```

This problem can occur, because the source and remote sites are internally presented as a map within a map. For each pair of source and remote site, there are four relations, which represent each possible direction of a replication:

- Source site – Source site (a relation within the respective site)
- Source site – Remote site (direction of the replication between sites)
- Remote site – Remote site (a relation within the respective site)
- Remote site – Source site (direction of the replication between sites)

There is one map containing the Source and Remote objects for the local sites. Each of these elements contains another map of the Source and Remote objects for the remote sites. There is a total of four elements for remote sites, but only two of them have unique IDs. The VMware Aria Automation configuration element keeps information only for the ID of the stored object and not the ID of its parent, which can lead to retrieving the incorrect remote site object.

Select the parent of the remote site and select the correct remote site by using the following script:

```
for each(var el in localSites) {
    if (el.name == 'SOURCE_SITE_NAME') {
        var remotesites = el.getVcRemoteSites()
        for each( var rsite in remotesites){
            if (rsite.name == 'REMOTE_SITE_NAME') {
                remoteSiteSelected = rsite;
            }
        }
    }
}
```

}

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

