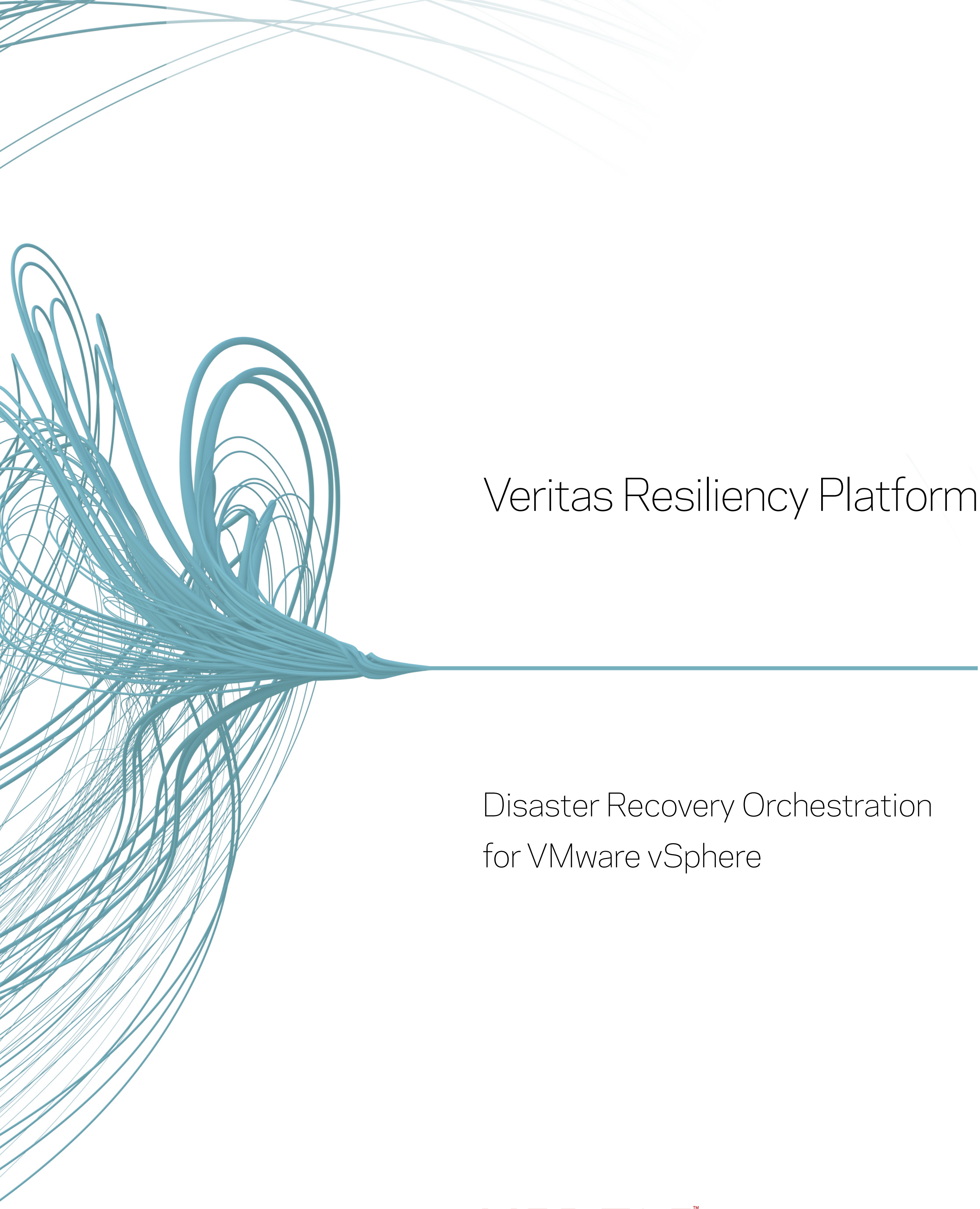


Veritas Resiliency Platform

Disaster Recovery Orchestration for VMware vSphere

VERITAS™

The truth in information.

Contents

REVISION HISTORY

Version	Date	Changes	Author
1.00	2019-Jan	Initial Version	Ryan Behiel
1.01	2019-Feb	Feedback, updates	Ryan Behiel
1.02			

INTRODUCTION

EXECUTIVE SUMMARY

Veritas Technologies is a leader in developing data resiliency solutions that focus on protection and management of digital assets critical for a company's success and business continuity. One of our flagship products, Veritas Resiliency Platform, is designed to enable high availability and disaster recovery (HA/DR) for data centers, hybrid and multi-cloud environments. Adding to the Veritas portfolio and legacy of creating stable solutions customers have trusted and relied on, Resiliency Platform is an enterprise-class solution designed to address the HA/DR needs of organizations using multiple platforms, including VMware vSphere. Resiliency Platform acts as an orchestration engine that can manage a wide range of data center workloads and enable failover, failback, migration and testing of workloads, as required.

TARGET AUDIENCE

This document is for customers, partners and Veritas field personnel interested in learning more about using Resiliency Platform as a solution to provide HA/DR for VMware vSphere data center infrastructure.

SCOPE

The purpose of this document is to provide technical details to assist in understanding Resiliency Platform as a solution for HA/DR in VMware vSphere environments. It describes the components of this solution, its value, sizing guidance and some best practices. This document will also describe native Resiliency Platform integration with third-party storage systems as well as with Veritas NetBackup™. Both integrations can be configured as additional options for DR orchestration in a vSphere environment. Although this document provides some deployment examples, we advise you to refer to the product documentation for installation, configuration and administration information. We update this documentation periodically, and you can download the latest version from this link.

SOLUTION COMPONENTS

The following tables will outline the name and description of the components involved in the Resiliency Platform setup, configuration and operational process. Also included are the NetBackup components required for integration with Resiliency Platform.

Component	Description
NetBackup Master Server 🟦	The NetBackup component that manages backups, archives and restores. The Master Server is responsible for media and device selection for NetBackup. The Master Server typically contains the NetBackup catalog, which is the internal database that contains information about NetBackup backups and configuration. The Resiliency Platform Infrastructure Management Server is added to NetBackup as an additional server within the NetBackup management console. NetBackup VMware policies are required for systems configured within Resiliency Platform to use NetBackup replication.
Resiliency Platform Resiliency Manager 🟥	The Resiliency Platform component that provides the services required for protecting assets such as virtual machines (VMs) within the logical scope of a Resiliency Platform deployment (known as a Resiliency domain). The Resiliency Manager discovers and manages information about data center assets from the Infrastructure Management Server. The Resiliency Manager is deployed as a virtual software appliance.
Resiliency Platform Infrastructure Management Server 🟨	The Resiliency Platform component that discovers and monitors assets within a data center and enables management operations on assets (i.e., starting or stopping a VM). The Infrastructure Management Server scales horizontally and is deployed as a virtual software appliance.
Resiliency Platform Replication Gateway 🟩	The Resiliency Platform component that manages replication across sites and across hypervisors. The Replication Gateway scales horizontally and is deployed as a virtual software appliance. The Replication Gateway is also referred to as the Resiliency Platform Data Mover. You can install multiple Replication Gateway appliances within the same VMware HA cluster, and you can pair a Replication Gateway with more than one other Replication Gateway.
Resiliency Platform Discovery Host 🟪	A role assigned to a Windows or Linux host to discover the storage arrays in the data center. The Infrastructure Management Server is a Discovery Host by default. In addition to the Infrastructure Management Server, you can configure additional Discovery Hosts to offload the discovery and monitoring of multiple enclosures rather than discovering all of them from a single Infrastructure Management Server. A Discovery Host is also required if the Infrastructure Management Server does not have direct connectivity with the enclosures. You only use the Discovery Host component when using Resiliency Platform to manage replication of third-party storage arrays, and you configure it in the Resiliency Platform user interface.
Resiliency Platform Managed Host Package	The Resiliency Platform component that is installed on systems (assets) managed by Resiliency Platform that is used for communication and to enable actions associated with Resiliency Platform operations (such as starting and shutting down a VM). You can also use the Managed Host Package to enable data filtering for the purpose of replication, depending on the infrastructure Resiliency Platform is managing.

VMware ESXi Server	A purpose-built bare-metal hypervisor that installs directly onto a physical server. Resiliency Platform uses the VMware VAIO API to filter I/O at the ESXi level, which is then sent to the Resiliency Platform Replication Gateway and used for replication to another site. In certain situations where VAIO is not available, Resiliency Platform installs a Managed Host Package on the VM guests running on the ESXi hosts. The Managed Host Package acts as an I/O tap that relays data from the VMs to the local Resiliency Platform Replication Gateway.
VMware Data Filter (VAIO) 🟥	The vSphere's APIs for I/O filtering. A framework that enables VMware partners to develop filters that run in ESXi and can intercept I/O requests from a guest operating system to a virtual disk. Resiliency Platform uses VAIO to filter data for the purpose of replication to another site. The I/O filter plug-in is installed by Resiliency Platform on the ESXi hosts and is called vtstap.
VMware High Availability Cluster □	The vSphere configuration option that provides high availability (HA) for VMs by pooling them and the hosts they reside on into a cluster. A cluster is a grouping of ESXi hosts administered collectively by the vCenter Server. HA protects against scenarios such as host failures, host isolation and application crashes. The Resiliency Platform Data Mover is a virtual software appliance that installs in an ESXi host that is part of an HA cluster.
VMware vCenter Server	A centralized management application that allows you to centrally manage VMware VMs and ESXi hosts. You can use the vCenter Server to install Resiliency Platform components by using the 'Deploy OVF Template' option for the Resiliency Platform appliance OVA files.

Table 1. Component Descriptions

DEPLOYMENT OPTIONS

As listed in Table 2, the Resiliency Platform solution consists of different components that are configured based on the chosen replication type. Some components are not required or applicable to all use cases. Table 3 describes the deployment options available for the Resiliency Platform solution. Table 4 provides additional details on the replication options available to help you understand which Resiliency Platform components might be best suited for different usage requirements.

Component	Resiliency Platform Replication	Storage Replication	NetBackup Replication
NetBackup Master Server			🟥
Resiliency Platform Resiliency Manager	🟥	🟥	🟥
Resiliency Platform Infrastructure Management Server	🟥	🟥	🟥
Resiliency Platform Replication Gateway	🟥		
Resiliency Platform Discovery Host		▪	
VMware vCenter Server	🟥	🟥	🟥
VMware High Availability Cluster	🟥	▪	
VMware Backup Policy (NetBackup)			🟥
VMware VAIO Data Filter (vtstap)	🟥		

Table 2. Component Requirements

🟥 Required
▪ Optional

	Express Install	Custom Install
Overview	The deployment option that bundles the Resiliency Platform appliances into a single package (vApp) that you can install using a single process at each site. The Express Install option is for Proof of Concept deployments and is not intended for the deployment of production environments. You can find additional details at this link. The Express Install requires DHCP, preconfigured DNS entries for the Resiliency Platform appliances and access to an NTP server. The Resiliency Platform appliances are bootstrapped and added to the Resiliency Manager as part of the Express Install process.	The Resiliency Platform appliances are available as OVA files that are imported into the VMware environment at each site. The Custom Install option is intended for production environments. You can import the Resiliency Platform appliance OVAs into VMware using the process described in this link. The Custom Install option is described in a Quick Reference Card available as part of the trialware download process in this link.
Resiliency Platform Data Mover	The source site vApp includes the Infrastructure Management Server and Replication Gateway. The target site vApp includes Resiliency Manager, Infrastructure Management Server and Replication Gateway.	Requires three appliances for each site: Resiliency Manager, Infrastructure Management Server and Replication Gateway.

Storage Replication	N/A	Requires two appliances for each site: Resiliency Manager and Infrastructure Management Server. Resiliency Platform Discovery Host: Configure within the Resiliency Platform console after installation of the Resiliency Platform appliances as described in this link.
NetBackup Replication	N/A	Requires two appliances for each site: Resiliency Manager and Infrastructure Management Server. NetBackup requirements: Refer to the section "Recovering VMware virtual machines using NetBackup" in the Resiliency Platform User Guide at this link.
Resiliency Platform Replication Gateway Appliance	N/A	You can install the Replication Gateway and add it to an existing Resiliency Platform domain by importing the corresponding OVA file and configuring it within the Resiliency Platform domain. Requires at least one Replication Gateway per site for replication between sites.
Resiliency Platform Infrastructure Management Server Appliance	N/A	You can install the Infrastructure Management Server and add it to an existing Resiliency Platform domain by importing the corresponding OVA file and configuring it within the Resiliency Platform domain. Typically, a single Infrastructure Management Server can manage one site. For larger sites, you can install additional Infrastructure Management Server appliances for load balancing or to distribute management based on the asset type.

Table 3. Resiliency Platform Deployment Options

LICENSING NOTES

Resiliency Platform installs with an embedded 60-day trial license. Once this trial expires, the product will no longer function.

When configuring Resiliency Platform to use NetBackup for data replication, you'll need a NetBackup license that enables Automatic Image Replication (AIR).

When using storage replication, you may be required to obtain a license for the storage system to enable replication functionality.

Replication Type	Recovery Point Objective (RPO)	Usage Scenario
Resiliency Platform Data Mover	Supports an RPO of roughly 5 minutes. The Resiliency Platform Data Mover creates update sets from the incoming data that are replicated every 2 minutes or every 500mb, whichever is sooner. These parameters are configurable.	The Resiliency Platform Data Mover is typically used in enterprise VMware environments with high application uptime requirements. The Resiliency Platform Data Mover supports any type of storage supported by VMware and requires no installation/footprint inside VMs.
Storage Replication	Supports a near-zero RPO. This figure can vary depending on the type of storage replication used, the features available within the storage system and the network bandwidth available for data replication between the storage systems.	Storage-based replication is best suited for systems with a high uptime requirement that may benefit from features provided by the storage system (e.g., application awareness, volume scaling without application disruption and synchronous replication).
NetBackup Replication	Supports RPO typically defined in days or months. The RPO is based on a user's backup schedule and will vary depending on the backup requirements for individual systems. Resiliency Platform will discover backup images that were created up to 2 times the defined RPO; for example, for a defined RPO of 1 day, Resiliency Platform will discover NetBackup images created within the past 2 days.	NetBackup replication is ideally used with systems that don't need to be online quickly in a DR scenario. Because it's possible to have multiple systems within a Resiliency Platform Resiliency Group that use NetBackup for data movement between sites, you can automate and simplify the process of bringing multiple systems online from backup images without having to perform individual restores.

Table 4. Resiliency Platform Data Replication Options

SOLUTION VALUE

Creating an HA/DR solution for multi-site VMware vSphere environments introduces some challenges that in most cases cannot be completely resolved with native vSphere tools. Resiliency Platform is designed to integrate with VMware vSphere to address these challenges by providing additional functionality and automation of the DR process.

VMware DR Options

The following options are available as part of the vSphere framework and are commonly used to achieve DR capability between two or more VMware environments.

- **vSphere Replication**—This is a hypervisor-based, asynchronous replication solution for vSphere VMs. vSphere replication is configured at the VM level and can be enabled between VMware environments running on any of the storage types supported by vSphere. The vSphere replication option is a solution for data movement only and does not manage any other aspects of the DR process. You can integrate vSphere replication with VMware Site Recovery Manager to provide additional functionality.

- **VMware Site Recovery Manager**—This option provides DR management for VMware environments. Site Recovery Manager provides additional functionality compared to vSphere replication, including automated failover and non-disruptive DR testing. Site Recovery Manager operates as an extension of vCenter Server and is available as an additional licensing option. Site Recovery Manager supports site recovery for VMware environments only, including VMware Cloud on Amazon Web Services (AWS).

Resiliency Platform Managed DR for VMware Environments

The native VMware solutions described above require some degree of configuration and user intervention to successfully recover applications in a DR scenario. Here's how Resiliency Platform can help simplify and improve the DR process for VMware environments and reduce the need for manual user intervention:

- **Resiliency Platform Data Mover**—In addition to providing hypervisor-level replication between sites, Resiliency Platform goes beyond simple moving of data between sites to include automation of DNS updates, management of network mappings between sites and application startup at the recovery site in the event of a failover—all with a single click. Resiliency Platform enables you to group systems by application or Resiliency Group and lets you manage based on application-level requirements.

- **Storage Integration**—In some cases, you can experience significant benefits when using native storage replication technology to move data between sites. Resiliency Platform integrates with industry-leading storage replication technologies so you can move data between sites using your existing storage software while experiencing a near-zero Recovery Time Objective (RTO). Storage-based replication also provides scalability because the storage systems hosting the data can be scaled to meet the needs of evolving application workloads without any need for application reconfiguration or downtime.

- **NetBackup Integration**—Resiliency Platform can integrate with NetBackup to leverage VMware backup images for DR purposes between sites using NetBackup Automatic Image Replication (AIR). This ability is useful when you need to restore several systems in a single process and eliminates the time-consuming process of restoring multiple individual restores.

- **Cloud Integration**–Resiliency Platform can natively manage DR operations between an on-site VMware data center and a private cloud platform such as VMware vCloud Director. Resiliency Platform can also manage DR operations from an on-site VMware data center to public cloud services such as AWS and Microsoft Azure without requiring any data format conversions, optimizing the performance of data movement into the cloud. Resiliency Platform supports bidirectional operations, making it easy to move data from a cloud platform back to VMware infrastructure in an on-site data center.

- **DR Rehearsal**—Resiliency Platform can manage and run a DR rehearsal on an isolated, non-production network segment to ensure systems at the DR site are working properly prior to a full DR failover event. You can run DR rehearsals using snapshots of production data that are then attached to temporarily provisioned systems used for testing purposes. Resiliency Platform also manages the cleanup of the rehearsal environment when it's no longer needed.

An integrated option within Resiliency Platform, known as Virtual Business Service (VBS), can group application tiers together simplifying DR orchestration by recovering a business service in the correct priority and order sequence. A VBS represents a multi-tier application as a single, consolidated entity and can build on the HA/DR provided for the individual tiers by integrating with products such as Veritas Cluster Server and Veritas ApplicationHA.

Additional orchestration options are available with Resiliency Platform:

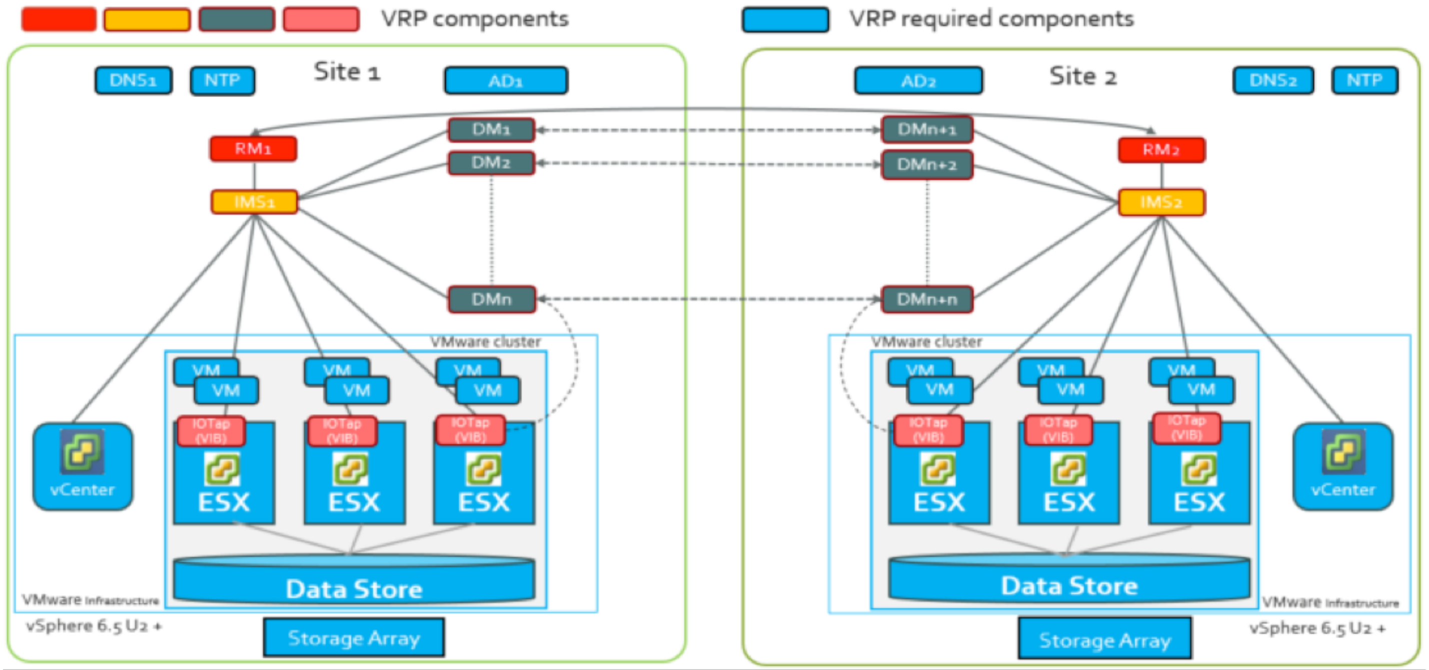
- **Resiliency Plans**—Provide the ability to create a custom automated workflow consisting of a specific set of tasks. This workflow can include tasks such as starting, stopping, migrating and taking over a Resiliency Group or VBS. You can also include DR rehearsals as part of a resiliency plan.

- **Evacuation Plans**—Provide the ability to takeover a Resiliency Group or VBS from one data center (either on-site or in the cloud) in the event of a site evacuation.

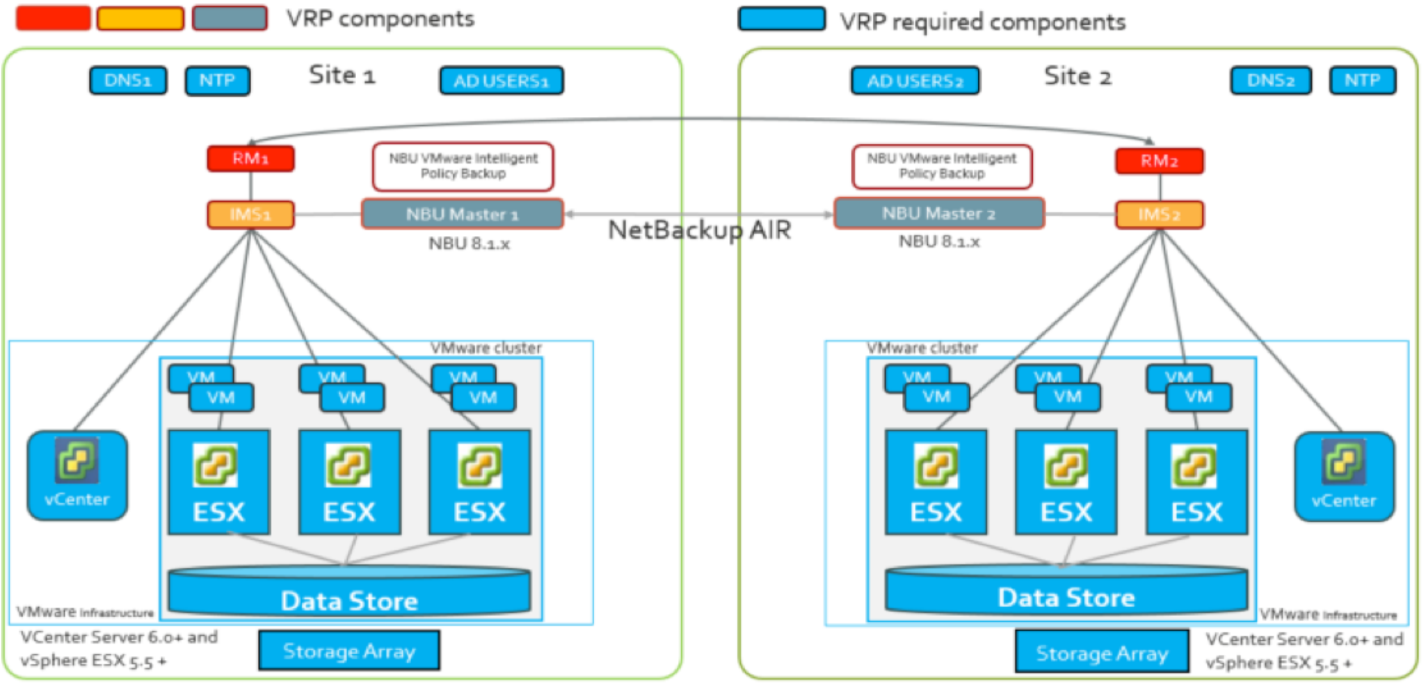
Resiliency Platform also simplifies management by providing a modern and intuitive user interface that lets you manage all the components required to fully orchestrate the DR process. The Resiliency Platform user interface provides a clear view into all operations and can proactively notify administrators of potential risks (i.e., replication lag or backup image status) that may exist within the environment and potentially impact the successful execution of a DR plan.

SOLUTION ARCHITECTURE

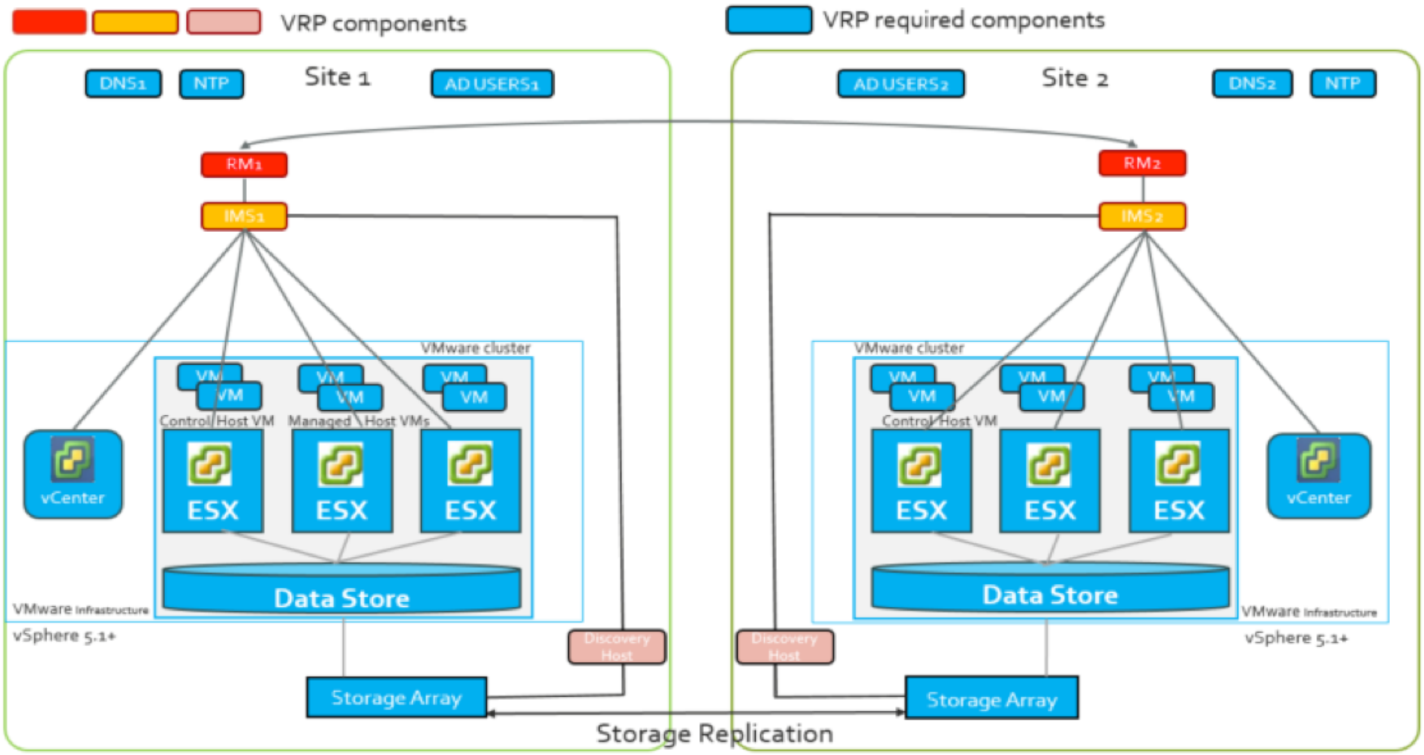
RESILIENCY PLATFORM REPLICATION



NETBACKUP REPLICATION



STORAGE REPLICATION



SIZING GUIDANCE

The following system resources are required for the Resiliency Platform appliances. System resource use may vary based on factors such as your organization's environment size, performance requirements and usage patterns.

VMware vSphere system requirements:

- Resiliency Platform Resiliency Manager—8 vCPUs and 32 GB RAM. Minimum of 60 GB disk space. Resiliency Manager is optional for the on-site data center because its sole purpose is to execute a takeover of the AWS environment from the on-site VMware environment.

- Resiliency Platform Infrastructure Management Server—8 vCPUs and 16 GB RAM. Minimum of 60 GB disk space.

- Resiliency Platform Replication Gateway—8 vCPUs and 16 GB RAM. Minimum of 40 GB disk space. An additional (thick) data disk with a minimum of 50 GB is required, and each protected VM has a disk space requirement that will vary depending on the configuration of the update set parameters; therefore, the data disk may need more than 50 GB, depending on the number of protected VMs. You can find additional capacity planning information for the Replication Gateway here.

- Resiliency Platform Discovery Host—Dual CPU and 4 GB RAM. Minimum of 15 GB disk space. When using the Infrastructure Management Server as a Discovery Host, you must ensure these system requirements are available in addition to the system requirements for the Infrastructure Management Server.

You can find current Resiliency Platform User Guides and product documentation on the Veritas Services and Operations Readiness Tools (SORT) website at this link.

BEST PRACTICES AND RECOMMENDATIONS

- **Use the Resiliency Platform Replication Gateway data mover for tier 1 workloads.** The Replication Gateway data mover appliance supports an RPO of as little as 5 minutes and simplifies the overall installation and deployment of Resiliency Platform within a VMware environment. The Replication Gateway uses a data replication process that is certified by VMware.

- **Use redundant Resiliency Managers to ensure maximum Resiliency Platform operational uptime**. When deployed in a redundant configuration, Resiliency Manager automatically manages the replication of configuration data between Resiliency Managers within a defined Resiliency Platform domain.

- **Use NetBackup integration for applicable workloads with a higher RPO/RTO.** Using NetBackup lets you leverage existing data copies (backup images), reducing the need to create new data sets to manage DR operations.

- **Use a standalone Discovery Host in larger environments when using storage replication.** This approach will reduce the discovery load on the Infrastructure Management Server and provide better scalability as the environment grows.

- **Use an Infrastructure Management Server for each asset type in larger environments.** Doing so allows you to spread the workload and simplify operations when managing more than one asset type within a Resiliency Platform domain. As a guideline, a single Infrastructure Management Server can typically manage roughly 1,000 VMs.

- **Configure the Replication Gateway update sets for optimal performance.** In situations where network connectivity and throughput between paired Replication Gateways is high, the size of the update set can be fairly small (e.g., 500bm). In situations where network connectivity and bandwidth is low, increase the size of the update set to improve data optimization. Smaller update sets typically result in faster data replication. Larger update sets may require more time for data replication, but will be more optimally compressed and deduplicated due to the larger data footprint of the update set.

CONCLUSION

Resiliency Platform has been designed to integrate with an evolving IT landscape in a way that helps you achieve resiliency for VMware vSphere environments while maximizing your investment in existing infrastructure such as third-party storage arrays and Veritas NetBackup. You can realize some key benefits when using Resiliency Platform to provide an HA/DR orchestration solution for vSphere environments:

- **Scalability**—The Resiliency Platform Replication Gateway data mover appliance works at the cluster level, making it easy to scale as the VMware environment grows. Third-party storage integration provides additional scalability by using the storage platform's integrated capability to dynamically manage data volumes with little or no application downtime.

- **Simplified management**—Resiliency Platform replaces manual processes with automation and orchestration, decreasing human error and freeing up staff to focus on innovation. Virtual Business Services further simplify management by logically representing complex, multi-tier applications as a single entity that you can migrate between sites with a single click. Replace lengthy, manual restoration of NetBackup images with one-click restoration of hundreds or thousands of VMs.

- **Increased visibility and control**—Resiliency Platform provides a visual representation and single management console for the entire HA/DR domain that helps eliminate complexity and increases your confidence in often-unpredictable situations.

- **Increased confidence**—Integrated, non-disruptive DR rehearsals preserve production uptime and increase your confidence in rolling out new technology. NetBackup integration enables system recovery to multiple points in time based on business requirements.

Meeting uptime service-level objectives for VMware vSphere environments with multiple point tools can be complicated and costly. Resiliency Platform helps you proactively ensure application resiliency across constantly evolving virtualized environments with a single solution.

GLOSSARY

- **API**: Application Programming Interface. A set of routines, protocols and tools for building software applications.

- **AIR**: Automatic Image Replication. This is a NetBackup option that lets you replicate NetBackup backup images generated in a source domain to storage in one or more target NetBackup domains.

- **ApplicationHA**: Veritas software that provides high availability for business-critical applications through application visibility and control across virtual environments.

- **DHCP**: Dynamic Host Configuration Protocol. A client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- **DNS**: Domain Name System. A naming system for computers, services or other resources connected to the Internet or to a private network that translates domain names to numerical IP addresses.
- **NetBackup**: The Veritas enterprise data protection solution that provides cross-platform backup functionality for a large variety of Windows, UNIX and Linux operating systems.
- **NTP**: Network Time Protocol. A networking protocol for clock synchronization between computer systems.
- **OVA**: Open Virtual Appliance. This is a preconfigured VM image ready to run on a hypervisor.
- **Resiliency Platform asset**: A system managed by Resiliency Platform is referred to as an asset. Assets include physical hosts, VMs and applications.
- **Resiliency Platform domain**: A term that describes the logical scope of a Resiliency Platform deployment. A domain can extend across multiple data centers and regions.
- **RPO**: Recovery Point Objective. This is the maximum targeted period in which data (transactions) might be lost from an IT system or service due to an outage.
- **RTO**: Recovery Time Objective. This is the targeted duration of time in which a business process must be restored after an outage to avoid unacceptable consequences associated with a break in service.
- **Update set**: A set of workload I/Os collected over a period of time by the I/O tap drivers in the systems being managed by Resiliency Platform.
- **VAIO**: vSphere APIs for I/O filtering. VAIO is a framework that enables VMware partners to develop filters that run in ESXi and can intercept any I/O requests from a guest operating system to a virtual disk. Resiliency Platform uses VAIO to filter data for replication to another site.

DISCLAIMER
This publication is provided "as is" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Veritas technologies llc shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this publication. The information contained herein is subject to change without notice.
No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at www.veritas.com or follow us on Twitter at @veritastechllc.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054 USA
+1 (866) 837 4827
veritas.com

For specific country offices and contact numbers,
please visit our website.
veritas.com/about/contact

VERITAS™
The truth in information.

V06847 02/19