VERITAS

Veritas Resiliency Platform

Resiliency and cloud recovery with Veritas NetBackup.

White Paper | November 2021

Contents

Introduction

Executive Summary

Veritas Technologies is a leader in developing application and data resiliency solutions that focus on the protection and management of companies' digital assets critical for their success. 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 across on-premises and the cloud. 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. Resiliency Platform also includes significant integration with Veritas NetBackup™, providing a highly scalable resiliency and cloud-based recovery solution.

Target Audience

This document is for customers, partners and Veritas field personnel interested in learning more about Resiliency Platform's integration with NetBackup and how the two platforms work together to enable a near-zero recovery time objective (RTO) for VMware workloads as well as a cloud recovery solution using backup images created with on-premises systems stored in cloud-based object storage in an optimized format. Although there are multiple publically available cloud-based object storage options on the market, this document will focus on the Resiliency Platform solution with Amazon Web Services (AWS).

Scope

The purpose of this document is to provide technical details to assist in understanding the solution components of Veritas Resiliency Platform, NetBackup and AWS as well as the process and configuration that enables the overall resiliency and cloud recovery solution. It includes hardware and software such as VMware vSphere and its associated components as well as the NetBackup integration and AWS infrastructure that is part of the overall solution.

Although this document provides some deployment examples, we recommend you refer to product documentation for installation, configuration and administration. 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 Resiliency Platform's setup, configuration and operational process.

Table 1. Component Descriptions

Component	Description
VMware vCenter Server 	A centralized management application that allows users to manage VMware virtual machines (VMs) and ESXi hosts centrally. You can use vCenter Server to install the Resiliency Platform appliances by using the 'Deploy OVF Template' option for the Resiliency Platform appliance OVA files.
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 splitter that relays data from the VMs to the local Resiliency Platform Replication Gateway.

Component	Description
VMware High Availability (HA) Cluster 	The vSphere configuration option that provides 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 vCenter Server. HA protects against scenarios such as: host failures, host isolation and application crashes. The Resiliency Platform Replication Gateway is a Virtual Software Appliance (VSA) that installs in an ESXi host that is part of an HA cluster.
Resiliency Platform Resiliency Manager (RM) 	The Resiliency Platform component that provides the services required for protecting assets (for example, 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 VSA.
Resiliency Platform Infrastructure Management Server (IMS) 	The Resiliency Platform component that discovers and monitors assets within a data center and enables management operations on assets such as starting or stopping a VM. The IMS scales horizontally and is deployed as a VSA.
Resiliency Platform Replication Gateway (RG) 	The Resiliency Platform component that manages replication across sites and across hypervisors. The RG scales horizontally and is deployed as a VSA. The RG is also referred to as the Resiliency Platform Data Mover (DM). The RG isn't used as part of the Resiliency Platform-NetBackup integration because the data replication in this scenario is managed by NetBackup.
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 lists the internal databases that contain information about NetBackup backups and configuration. The Resiliency Platform IMS 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.
NetBackup Appliance 	An option that integrates NetBackup enterprise backup software into an appliance form factor with expandable storage and intelligent end-to-end deduplication for physical and virtual environments. NetBackup appliances are available as hardware appliances and as virtual software appliances. The NetBackup Instant Access feature that enables instant access to VM backup data can be orchestrated by Resiliency Platform and requires a NetBackup appliance.
NetBackup Media Server 	A NetBackup component that manages incoming data streams from NetBackup clients and the on-site or cloud-based storage being used by NetBackup as a target for backup images.
NetBackup Client	A system protected by NetBackup is known as a NetBackup client. Data is sent from the client to the NetBackup Media Server, which creates a backup image for that client's data and writes it to a NetBackup managed storage target.
NetBackup CloudCatalyst 	NetBackup CloudCatalyst, also known as a CloudCatalyst storage server, is a software-defined data optimization option that enables NetBackup Media Servers to directly target cloud object storage with deduplicated data without consuming space on the Media Servers. You can deploy CloudCatalyst using a NetBackup appliance or a NetBackup Linux Media Server. You can find additional information in this link.
NetBackup Cloud Recovery Sever (CRS) 	The NetBackup component that is deployed as an EC_2 instance in an AWS Virtual Private Cloud (VPC) environment that manages the recovery of images stored in AWS S_3 storage into systems running in an AWS VPC. The Cloud Recovery Server (CRS) can be installed and configured in AWS using a CFT available in the AWS Marketplace.

Component	Description
Amazon CloudFormation 	The option within AWS that enables the creation of templates for provisioning services or applications within AWS. You can use a CloudFormation Template (CFT) to easily deploy the Resiliency Platform components within an AWS environment.
Amazon EC_2 	A virtual computer system (known as an instance) that is provided by Amazon on which users run their computer applications. You can use EC_2 instances to run the Resiliency Platform components, the Cloud Recovery Server and any backup images that are restored using the Resiliency Platform Cloud Recovery feature described in this document.
Amazon EBS 	A durable, block-level storage device that is attached to an EC_2 instance. EBS volumes can be provisioned using SSD-backed storage and HDD-backed storage. The Resiliency Platform components within AWS use EBS volumes for local storage.
Amazon S_3 	The object storage provided by AWS that is optionally used by Resiliency Platform as a target for storing replicated block-level data from on-site VMware systems. You can also use S_3 for replication in the reverse direction, where it can store block-level data from cloud-based systems being replicated to an on-site VMware environment. NetBackup CloudCatalyst also uses S_3 to store space-optimized backup images that are restored as EC_2 instances in AWS with the cloud recovery feature in Resiliency Platform.

Table 2. Component Requirements

Component	Source Data Center	Target Data Center (NetBackup)	Target Data Center (AWS)
VMware vCenter Server	●	●	
VMware ESXi Server	●	●	
Resiliency Platform Resiliency Manager	o	●	●
Resiliency Platform Infrastructure Management Server	●	●	●
NetBackup Appliance[1]	o	o	
NetBackup Master Server	●	●	
NetBackup Media Server	●	●	
NetBackup CloudCatalyst[2]	o		
NetBackup Cloud Recovery Server			●
AWS S_3			●
AWS EC_2			●
AWS EBS			●

● Required o Optional

Deployment Options

The Resiliency Platform solution is deployed within a virtualized environment in an on-premises data center or in a Virtual Private Cloud (VPC) to support workloads running in AWS. The NetBackup infrastructure is deployed in an on-premises data center and is not required in the AWS environment to enable the cloud recovery solution. For more information on the NetBackup deployment process and requirements, please refer to the NetBackup installation guide in this link.

Resiliency Platform's deployment consists of components that run in both the on-site VMware environment and in the AWS environment. Some components are not applicable or required within both environments. Table 3 describes the deployment options available for the Resiliency Platform components.

Table 3. Resiliency Platform Deployment Options

Option	VMware On-Site (NetBackup Integration)	AWS
OVA File Import	OVA files are used to install all the Resiliency Platform components: Resiliency Manager, Infrastructure Management Server and Replication Gateway. You can import them into VMware using the process described in this link.	N/A
Amazon Machine Image (AMI)	N/A	AMIs are available for all the Resiliency Platform components that you can use to deploy Resiliency Manager, Infrastructure Manager (IMS) and Replication Gateway in AWS.
Express Install	An option that bundles the Resiliency Platform Infrastructure Management Server and Replication Gateway appliances into a single package (vApp) that can be installed using a single process.	This is a CloudFormation Template available in the AWS Marketplace that you can use to quickly deploy the full Resiliency Platform component stack within AWS. The process is described in this link.
Replication Gateway Install	You can install Replication Gateway in a VMware environment by importing the corresponding OVA file and configuring it within the Resiliency Platform Domain. At least one Replication Gateway is required in the VMware environment to replicate data to the AWS environment.	This is a CloudFormation Template available in the AWS Marketplace to install a Replication Gateway only. This option assumes you have already provisioned the Express Install option or the required Resiliency Platform AMIs within the AWS environment.
Cloud Recovery Server (CRS)	N/A	The Cloud Recovery Server is installed and configured in AWS using a Red Hat Enterprise Linux AMI with 200 GB of attached general-purpose disk (EBS). The CRS is also available as a CloudFormation Template in the AWS Marketplace.

Licensing

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

The Resiliency Platform stack available in the AWS Marketplace is provided as a Bring Your Own License (BYOL) model. Please read the product overview sheet and pricing information prior to deploying Resiliency Platform in an AWS environment.

NetBackup licensing may be needed to enable functionality required for the Resiliency Platform integrated solution. See Table 5 for a list of NetBackup objects used by Resiliency Platform.

How It Works

Using Resiliency Platform's NetBackup integration allows users to automate and orchestrate DR, resiliency and system migration using backup images. There are three main configuration options available as part of the overall NetBackup integration and each option provides different benefits that are suited to certain usage scenarios, as described in Table 4.

Table 4. NetBackup Integration Options

Option	Recovery Time Objective (RTO)	Usage Scenario
NetBackup Standard Restore	The RTO when using the NetBackup standard restore option is typically defined in hours. The RTO is variable depending on the size of the backup images selected for restore orchestration within Resiliency Platform. From a data availability perspective, Resiliency Platform will discover backup images that were created up to twice 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 restore is ideally used with systems that do not need to be online quickly in the event of a failure or service disruption. Because it's possible to have multiple systems within a Resiliency Platform Resiliency Group that use NetBackup for DR and resiliency between sites, users can automate and simplify the process of bringing multiple systems online from backup images without having to perform individual restores.
NetBackup Instant Access Restore	The RTO when using NetBackup Instant Access is defined in minutes, regardless of the systems being targeted for Instant Access restore. The restore can happen within seconds, depending on system resource utilization when initiating the restore.	As with the NetBackup standard restore option, you can have multiple systems within a Resiliency Group that use NetBackup as the mechanism for data replication. The Instant Access feature is typically used for systems that need to be online very quickly in the event of a failure, but where the acceptable RPO is the same as when using the NetBackup standard restore option.
Cloud Recovery in AWS	The RTO for cloud recovery is defined in hours and is similar to the RTO available using the NetBackup standard restore. Restore times can vary depending on the size of the systems being restored.	The Cloud Recovery feature is best suited for users currently using CloudCatalyst to write backup data to the cloud and who also want to use the cloud for DR or system migration without having to manage a full NetBackup deployment in the cloud.

The method for replicating data between sites when using NetBackup as the data mover is called Automatic Image Replication (AIR), which is an option within NetBackup that provides optimized data movement between two or more NetBackup domains.

In the case of cloud recovery in AWS, the data movement between sites is handled as a two-part process:

1. Data from systems defined within a backup policy is copied by NetBackup into a CloudCatalyst storage server that then sends the data in optimized format to AWS S3 object storage to be stored as an optimized backup image.

2. When a cloud recovery is initiated, Resiliency Platform uses the API for the CRS to initiate a restore for systems in the Resiliency Group being recovered in AWS. Because the backup images being used for recovery are already in AWS S3 storage, no transfer or replication of data from the source site (on-premises) is required.

Replication of data using AIR and writing backup images to CloudCatalyst for recovery in AWS S3 are mutually exclusive, and you should consider each process based on individual resiliency and data protection requirements.

NetBackup Restore

Users can configure Resiliency Platform to orchestrate restores of NetBackup images by integrating an existing NetBackup deployment into Resiliency Platform, where NetBackup images are replicated between sites (NetBackup domains) using NetBackup AIR.

You can find detailed information on the requirements and deployment process for using Resiliency Platform with NetBackup in this link.

Prerequisites

There are some prerequisites required to effectively use the NetBackup integration with Resiliency Platform. Ensure the following configuration items are in place:

- Every asset being configured in a Resiliency Group should also be included in a NetBackup policy.
- The NetBackup Master Server in the production and recovery data centers should be online.
- The vCenter/ESX servers hosting assets to be protected should be configured in the NetBackup Master Server.
- Have at least one backup schedule that meets the RPO defined in the Resiliency Platform service objective.
- Make at least one backup image available for each VM being protected.
- Ensure the datastore at the recovery data center has enough storage capacity for system restores.

Resiliency Platform also requires that certain objects within NetBackup are configured so they can be leveraged by Resiliency Platform workflows. Table 5 outlines the NetBackup objects used by Resiliency Platform.

Table 5. NetBackup Objects used by Resiliency Platform

NetBackup Object	Description
Backup Policy	A policy defines the backup criteria for one or more NetBackup clients that have similar backup requirements. A policy is required for any scheduled backup job.
Policy Schedule	A schedule controls when backups can occur in addition to other aspects of the backup, such as the type of backup (full or incremental) and how long NetBackup retains the image.
Storage Unit (STU)	The storage device where NetBackup stores files. It can be a set of drives in a robot or consist of one or more single tape drives that connect to the same host.
Storage Lifecycle Policy (SLP)	A storage plan for a set of backups that provides additional staging locations, including all supported disk types, VTL and tape. An SLP also provides additional retention and classification of backup data.
Backup Image	The collection of data NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories and catalog information associated with the backup or archive.

There are two options available in Resiliency Platform that can be used for resiliency orchestration with NetBackup:

1. Standard restore, which uses AIR and traditional NetBackup restores.
2. Instant Access for VMware, which enables the restore process to complete almost instantly, providing a near-zero RTO for system restore.

Standard Restore

The direct integration between Resiliency Platform and NetBackup provides users with an option to orchestrate DR and resiliency workflows while leveraging infrastructure already in place for data protection. (See Figure 4.) This option is a benefit for workloads with less-demanding recovery point and recovery time objectives (RPOs and RTOs) because it eliminates the need to provision other tools to manage data consistency between sites.

Configuration Overview

The process for configuring the integrated NetBackup and Resiliency Platform solution involves some steps that are performed on each platform. Table 6 outlines the process required to configure the Resiliency Platform-NetBackup integration.

Table 6. Configuration Process

Step	Description	NetBackup	Resiliency Platform
1	Add NetBackup Master Servers as copy managers in the Resiliency Platform user interface.		●
2	Add the Resiliency Platform IMS to the Master Server at each site.	●	
3	Create SLPs to replicate the images corresponding to the systems you want protect in Resiliency Groups.	●	
4	Add VMware vCenter servers at each site into Resiliency Platform.		●
5	Activate the copy service objective for NetBackup Recovery.		●
6	Protect assets by applying the service objective to the VMs you want to protect.		●
7	Select Instant Access for VM restore and rehearsal operation.		o
8	Execute Resiliency Platform operations on the Resiliency Groups configured to restore VMs from backups.		●

● Required o Optional

Advantages of NetBackup Integration

There are several benefits to integrating Resiliency Platform and NetBackup. By leveraging the NetBackup integration, backup images can then be used for resiliency and DR as part of an automated workflow that can be customized as required, resulting in a single solution for both data protection and resiliency. Here are some of the main advantages:

- NetBackup integration lets you use backup data for DR and resiliency with minimal configuration and complexity.
- You can orchestrate bulk restores of multiple backup images as a single process.
- Systems within Resiliency Groups that are recovered at a target site are automatically protected by NetBackup Intelligent

You can find additional information on integrating NetBackup with Resiliency Platform in this link.

Instant Access for VMware

The Instant Access for VMware feature available with NetBackup works by mounting a VM snapshot directly on the backup storage device, which lets your ESXi host or cluster treat the snapshot as a normal VM. The VM is available almost instantaneously, achieving a near-zero RTO. To do a full system recovery, you can move the Instant Access VMs to the production vSphere datastore using Storage vMotion with no downtime. (See Figure 5.)

The Instant Access VM recovery can be orchestrated with Resiliency Platform by choosing the Instant Access option as part of the Resiliency Group configuration process, where the user is given a choice of using Instant Access based on the type of storage used for backup images. You can also select the option to do a traditional restore if Instant Access is not available.

Solution Overview

Figure 1 illustrates the Instant Access components and dataflow for vSphere VMs being protected within a NetBackup environment. This dataflow is orchestrated by Resiliency Platform for assets with backup images stored on NetBackup appliances.

The Instant Access for VMware feature adds to the overall integration between Resiliency Platform and NetBackup by offering an additional solution to use backup images for DR and resiliency for systems that have a high uptime requirement and need to be brought back online quickly in the event of a failure or servicedisruption. The Instant Access option includes all the advantages of the standard NetBackup integration plus some additional benefits:

- Near-zero RTO for protected systems.
- Almost-zero storage overhead is needed.
- Instantly provision rehearsals for multi-tier applications using a virtual business service (VBS).
- Automated bulk restores enable multiple systems to be brought online almost instantly with no manual user input.

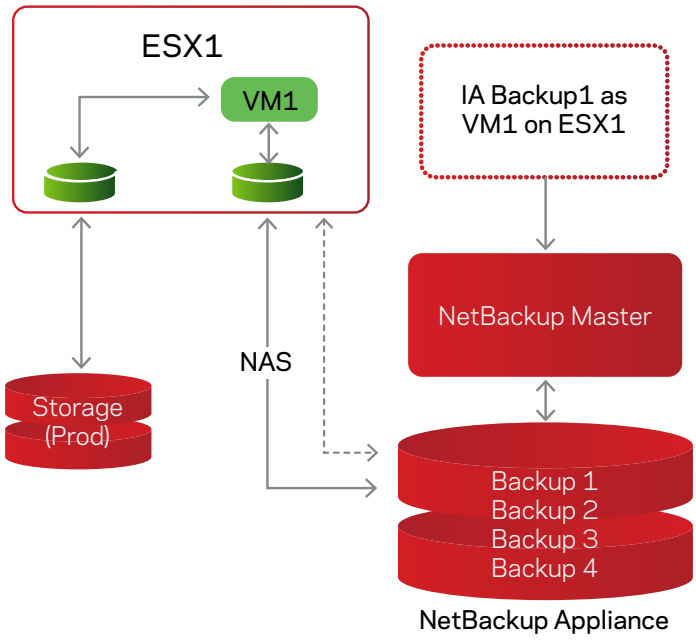

Figure 1. Instant Access for VMware overview.

When using the Instant Access option, data replication between sites is still managed using NetBackup AIR, which is the standard Resiliency Platform workflow for the NetBackup integration. The RPO for systems in a Resiliency Group configured to use NetBackup as the data mover with the Instant Access option enabled is based on the backup schedule set for those systems within the NetBackup policy.

NetBackup Cloud Recovery

The NetBackup Cloud Recovery solution enables Resiliency Platform to manage the restore of NetBackup images written to AWS S3 storage using CloudCatalyst into an AWS VPC without having to deploy NetBackup infrastructure in the AWS environment. This approach offers some key advantages over a traditional on-premises restore scenario:

- You can provision infrastructure needed for system restores on-demand as required in the cloud.
- In addition to cloud restores, you can use backups for rehearsals, providing an additional use for captive data.
- You can migrate to a cloud environment using backups without affecting production systems.

Cloud recovery of backup images enables a hybrid resiliency strategy while providing the flexibility of cloud-based infrastructure that can be provisioned on-demand and used only when needed.

Solution Overview

The Cloud Recovery solution consists of a process where both Resiliency Platform and NetBackup work in parallel to provision new systems in AWS using backup images from on-premises systems that are copied in optimized format into S3 storage.

- A NetBackup CloudCatalyst server is configured on-premises to send deduplicated backup data to an AWS S3 bucket.
  - CloudCatalyst will not be used for restores, thereby avoiding data egress from the cloud.
  - The CloudCatalyst server may also not be available in the event of an on-premises outage.

- The Cloud Recovery Server (CRS) is deployed in the cloud environment to manage the recovery of NetBackup CloudCatalyst images from S3 storage into cloud-based systems.
  - The CRS is pre-bundled with all the NetBackup components required for the AWS Cloud Recovery process.
  - The CRS can be deployed manually, or as a CloudFormation Template in the AWS Marketplace.
- The NetBackup catalog required to restore a NetBackup image will be rebuilt by the CRS as required based on the systems configured in Resiliency Groups and their associated backup images.

Workflow

The high-level workflow for the cloud recovery solution (see Figure 2) is as follows:

1. The NetBackup catalog is rebuilt in the CRS by traversing the backup images available in the S3 bucket corresponding to systems being managed in Resiliency Groups.

2. To execute the system restore, Resiliency Platform calls APIs on the CRS, which then creates a restore image for the systems configured in the Resiliency Group being restored in the cloud.
   - The restored images will be in AMI format and used to provision EC2 instances.
   - The Resiliency Platform cloud data center must be in the same AWS region as the S3 bucket used to store the NetBackup CloudCatalyst backup images.

3. Resiliency Platform provisions EC2 instances and applies compute customization (instance type), storage customization (volume type, IOPS, etc.) and also network/IP customization as requested by the user.

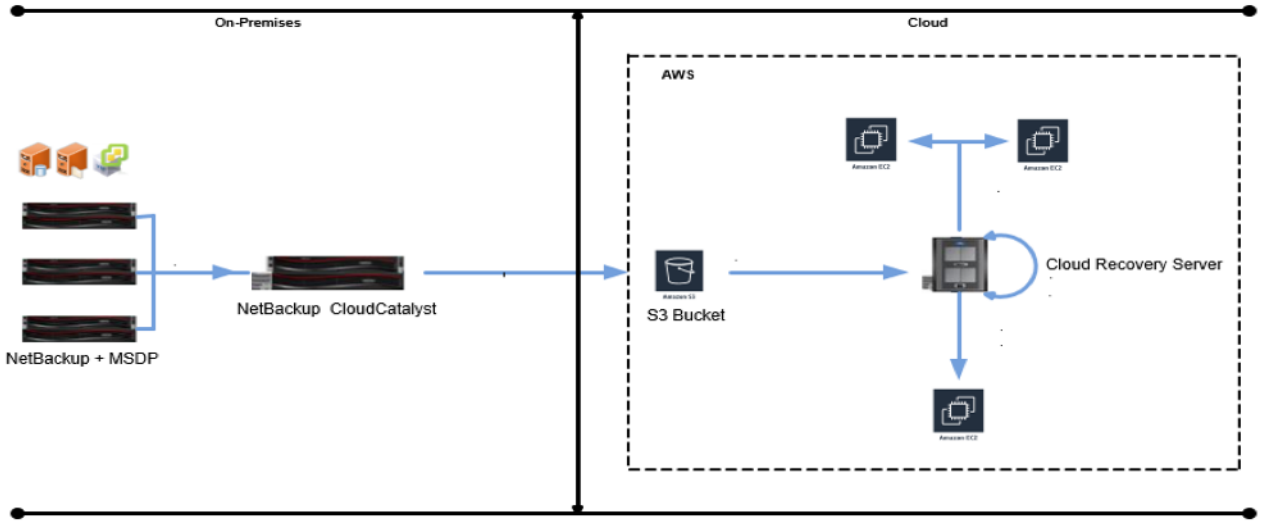

Figure 2. NetBackup Cloud Recovery overview.

Support Guidelines

There are some points to note regarding Resiliency Platform technical support that may be applicable depending on the usage scenario and features being deployed. The following guidelines outline the scope of support when using the Resiliency Platform-NetBackup integrated solution:

- The Resiliency Platform integration with NetBackup currently supports NetBackup VMware policies.
- For hardware and software compatibility details, please refer to this link.
- Data replication using the Resiliency Platform-NetBackup integration is only available using NetBackup Targeted AIR.
- The Cloud Recovery feature is only available for NetBackup images created by a CloudCatalyst storage server and requires NetBackup version 8.2 or greater.

Using components or services that fall outside these guidelines may result in a Resiliency Platform deployment where the NetBackup integration features are not supported by Veritas; however other Resiliency Platform features and functionality are not necessarily subject to the same support guidelines.

Sizing Guidance

The following system resources are required for the Resiliency Platform appliances. System resources used may vary based on factors such as 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. The Resiliency Manager is optional for the on-site data center. It is only required for providing failover orchestration from the AWS environment to 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. As such, 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.

AWS system requirements

- **Resiliency Platform Resiliency Manager:** AWS instance type m4.2xlarge or better. Minimum system requirements of 8 vCPUs and 32 GB RAM. Minimum of 60 GB disk space.
- **Resiliency Platform Infrastructure Management Server:** AWS instance type m4.xlarge or better. Minimum system requirements of 8 vCPUs and 16 GB RAM. Minimum of 60 GB disk space.
- **Cloud Recovery Server: AWS instance type m5a.2xlarge or better.** Minimum system requirements of 8 vCPUs and 32 GB RAM. Minimum of 60 GB disk space.
- **S3 storage:** For information on setting up NetBackup CloudCatalyst in AWS, refer to this link.

NetBackup system requirements

NetBackup supports several platforms and the system requirements can vary depending on the platform you choose for deployment. For detailed information on system requirements and supported configurations, please see the Installation and Upgrade Checklist on the Veritas Services and Operations Readiness Tools (SORT) website at this link.

You can also find current Resiliency Platform product user guides and documentation on the SORT website at this link.

Solution Architecture

Cloud Recovery In AWS

When managed by Resiliency Platform, the recovery of on-premises systems into an AWS cloud environment using NetBackup images can be done with no NetBackup infrastructure deployed in the cloud, using a guided process that minimizes user input. Figure 3 outlines the solution architecture and provides a visual representation of the components required as well as the data flow between the on-premises vSphere environment and AWS. There are two recommended deployment options for the Resiliency Platform components in AWS:

1. Express Install using AWS CFT with AWS Data Gateway option.5

2. Express Install using AWS CFT.

This deployment architecture represents option 2, where Resiliency Platform is deployed in AWS using the Marketplace Express Install option.

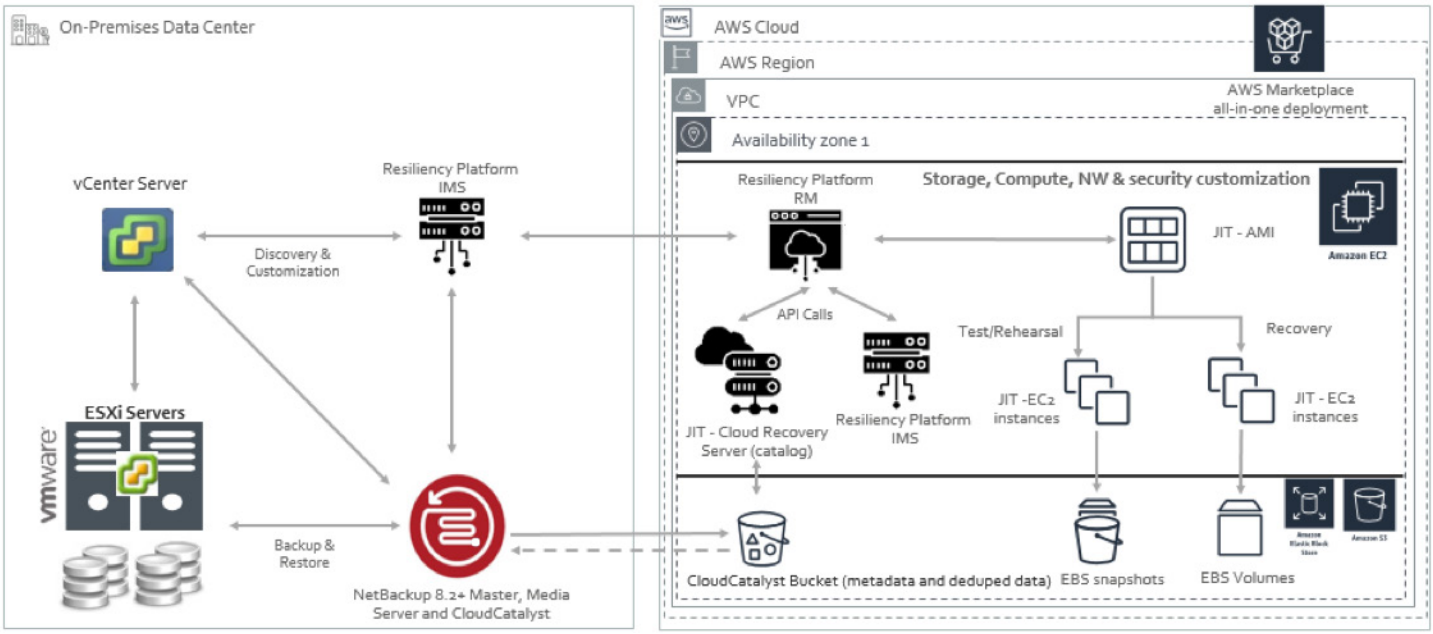

Figure 3. The solution architecture overview.

NetBackup Standard Restore

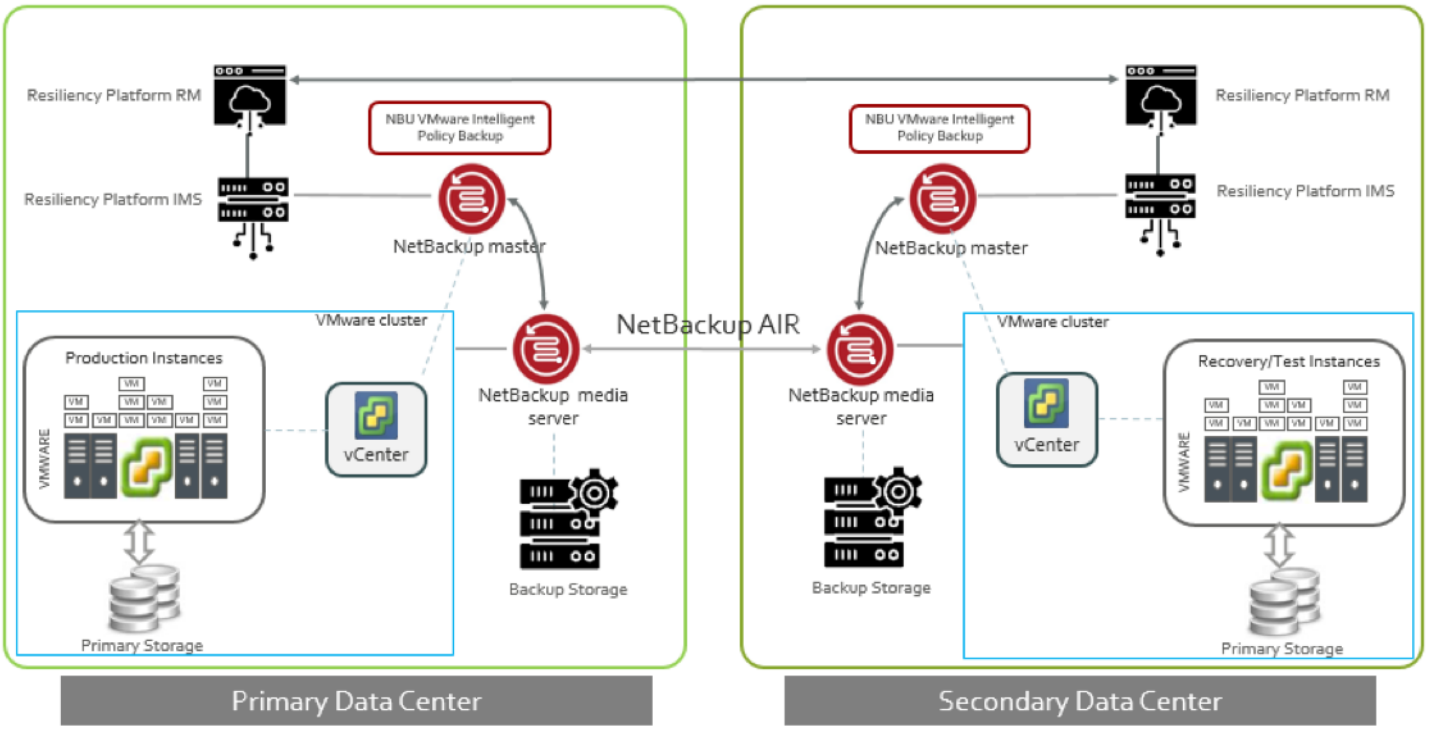

Figure 4. The NetBackup standard restore process.

NetBackup Instant Access Restore

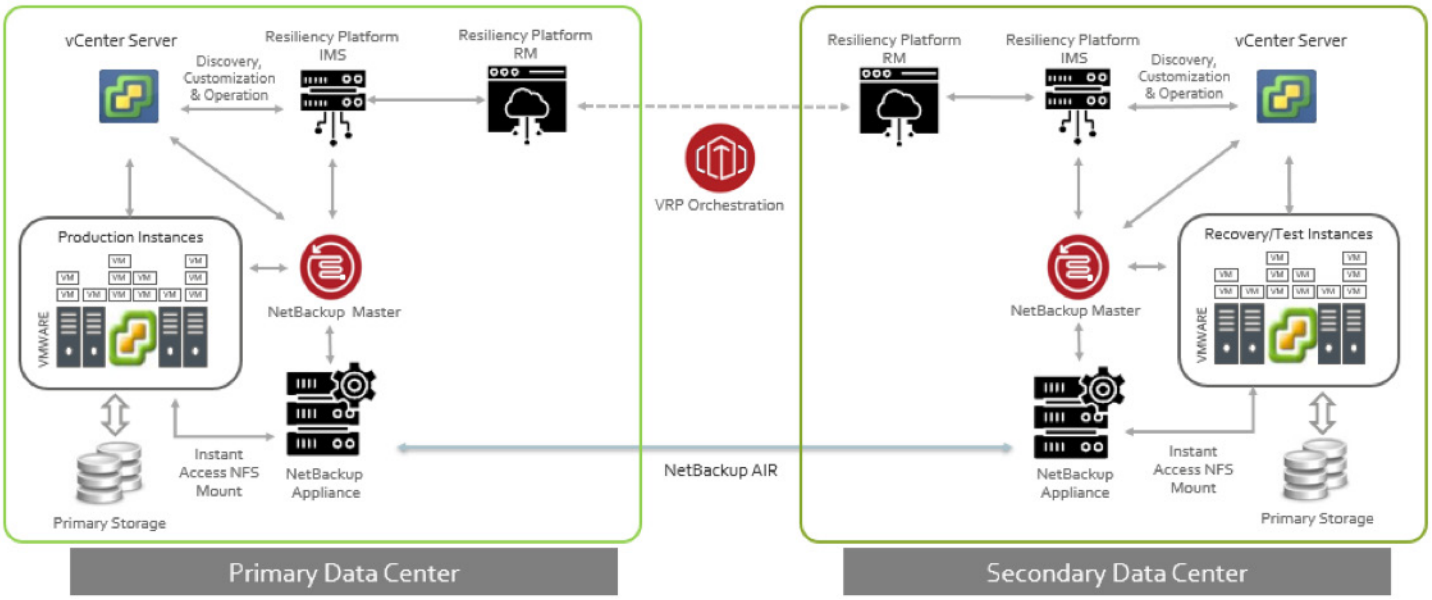

Figure 5. The NetBackup Instant Access restore process.

Solution Value

Creating a resiliency strategy that incorporates backup infrastructure and public cloud services has several benefits, including a lower RTO for protected systems as well as providing enterprise-class availability and service-level objectives (SLOs) by integrating with highly available and reliable cloud services. In many situations, you can do this integration by simply leveraging existing NetBackup infrastructure, which maximizes an investment in NetBackup as a data protection solution. Resiliency Platform complements NetBackup by using the data created as part of the backup process to provide both DR and resiliency for your IT services, which adds to the overall return on investment (ROI) in your NetBackup data protection solution. By integrating with NetBackup to enable resiliency and recovery of backup images in the cloud, Resiliency Platform provides several key benefits.

Cloud Recovery

The option to recover backup images from on-premises systems in the cloud gives you the flexibility to use backup infrastructure for other purposes:

- **Development and testing**—Use backup images and cloud services to build a highly scalable development and test environment using existing data with no impact on production systems. Systems recovered in the cloud can be created and removed on-demand to reduce costs and management complexity for your non-production infrastructure.
- **System migration**—Use NetBackup images as a source for migrating workloads into the cloud. Using the rehearsal feature, you can test systems targeted for migration in the cloud environment before going live. Once the workload is online in the cloud, you can delete that system's corresponding backup images to reduce storage costs.
- **Analytics**—Provision systems in the cloud and leverage advanced cloud-native analytics services with no up-front infrastructure required. Resiliency Platform lets you choose which backup images are recovered and which can be particularly useful for analytics against a wide range of data—all without having to deploy any recovery infrastructure in the cloud.

NetBackup Recovery

The NetBackup integration with Resiliency Platform gives you the ability to incorporate backup data into a full DR and resiliency solution that provides options beyond the typical limits of data protection solutions. Benefits include:

- **Automation**—Save time and effort by using Resiliency Platform to orchestrate the bulk restore of multiple systems simultaneously. Managing multiple individual restore operations can be very time-consuming and requires user oversight. Using a Resiliency Platform virtual business service (VBS), you can restore an entire business service with a single automated process.

- **Simplicity**—Having a single solution to manage resiliency in an environment where multiple SLOs are required keeps things simple. When using the NetBackup integration to provide resiliency for systems with lower SLOs in parallel with workloads that have higher SLOs, you can protect your entire environment based on business requirements with a single platform that unifies the overall resiliency experience.
- **Return on investment (ROI)**—Maximize your investment in NetBackup by using the Resiliency Platform integration to provide additional features and workflows that complement your existing data protection solution.

NetBackup Instant Access Recovery

One common issue with using backup images as a source for DR and resiliency is the recovery time required to bring systems back online in the event of a failure or service disruption. Resiliency Platform solves this problem by incorporating the NetBackup Instant Access feature into the resiliency workflow. Using the Instant Access option, systems can be brought back online very quickly, which has several key advantages:

- **Near-zero RTO**—With NetBackup Instant Access, systems can be brought online nearly instantly using the advanced file system management capability built into the NetBackup appliance family. Once online, you can move systems onto production datastores with no downtime using vSphere Storage vMotion.
- **Rehearsals**—By using the Instant Access option for rehearsals, you can save considerable time by not doing a full system restore to validate system integrity prior to a failover event. The near-instant startup of test workloads on an isolated network maximizes the efficiency of the rehearsal process. Take this one step further by promoting the rehearsal environment to production once system integrity has been verified, with no downtime required.
- **Reduced operating costs**—Almost no additional storage is required for the Instant Access restore process, whether it's used in a failover scenario or a rehearsal. This process improves application resiliency because it achieves a near-zero RTO with no requirement for additional infrastructure.

Best Practices And Recommendations

AWS reserved instances for Resiliency Platform infrastructure. Using Reserved Instances in AWS will result in a significant discount compared to EC2 On-Demand instance pricing. Reserved Instances also provide a capacity reservation, which is ideal for Resiliency Platform and provides additional confidence in your ability to launch instances when needed.

Deploy Resiliency Platform in AWS using Express Install. To do so, go to the AWS Marketplace and find the CloudFormation Template that has been created for the Express Install. The AWS Marketplace deployment offers a more automated process compared to using AMIs and deploying manually. This option also eliminates the need to manually provide bootstrap inputs for the Resiliency Platform appliances.

Use load balancing for NetBackup CloudCatalyst storage servers. Configuring push- or pull-optimized duplication for CloudCatalyst can result in a faster and more efficient backup workflow by maximizing the usage of the media servers for the NetBackup-optimized duplication process. You can find information on how this process works in this link.

Follow the NetBackup for VMware best practices to optimize the data protection process leveraged by the Resiliency Platform-NetBackup integration to provide resiliency and cloud recovery using backup data. You can find best practices information for NetBackup in a VMware environment in this link.

Use the Resiliency Platform Data Gateway option when using the Resiliency Platform data mover to manage resiliency for low-RPO workloads not protected using the NetBackup integration. The Data Gateway adds additional resiliency and scale to the replication process when Resiliency Platform is used as the data mover for systems with a low-RPO requirement that are not good candidates for resiliency using backup images. This approach provides additional resiliency by ensuring data is not lost in the event of a failure or service interruption with the Resiliency Platform Replication Gateway appliance.

Conclusion

Resiliency Platform has been designed to integrate with an evolving IT landscape in a way that helps you achieve resiliency for your IT systems and services while maximizing the investment in your existing NetBackup data protection solution. You can realize some key benefits when using the Resiliency Platform-NetBackup integration to enable resiliency and cloud recovery:

- **Scalability**—The NetBackup integration offers excellent scalability by leveraging the industry-leading scale provided by NetBackup, which can dynamically manage data protection workflows with little or no impact on production applications.
- **Simplified management**—Reduce the need for manual processes that are time-consuming and error-prone. The Resiliency Platform virtual business services (VBS) feature simplifies management by logically representing complex, multi-tier applications as a single entity that can be migrated between sites with a single click. Resiliency Platform automates the tedious manual restoration of NetBackup images by enabling the restore of hundreds of VMs instantly as part of an automated process.
- **Increased visibility and control**—Resiliency Platform provides a visual representation and single management console for the entire resiliency domain. Backup image status and information is incorporated into the resiliency console and can be included in reports used for auditing purposes and to prove compliance with corporate standards. This approach helps eliminate complexity and increases confidence in situations that are often unpredictable.
- **Increased confidence**—You can provision integrated non-disruptive resiliency rehearsals using backup images almost instantly and help preserve production uptime. Rehearsals help increase your confidence in rolling out new technology by providing a sandbox environment where you can test applications with no impact on production. The NetBackup integration also enables system recovery to multiple points in time based on business requirements, giving you additional protection against data corruption and ransomware.

Meeting uptime SLOs with multiple point tools can be complicated and costly. By integrating with NetBackup, Resiliency Platform maximizes the usefulness of backup data, proactively managing workload resiliency and recovery for systems that have less-demanding RPOs. With Resiliency Platform, you have a unified solution that provides flexibility and automation for the overall resiliency process.

Disclaimer

1. NetBackup appliance required for Instant Access restore
2. Required for NetBackup cloud recovery
3. NetBackup appliance required for Instant Access feature. The Instant Access restore option will not appear if backup images are stored on any other storage server type.
4. Instant Access is not possible if the ESX server has reached its maximum allowed number of NFS datastores.
5. Requires an AWS region with FIFO queue support. The Data Gateway is not used as part of the cloud recovery process.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

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

For global contact information visit:
veritas.com/company/contact

V0955 11/21