Veritas Resiliency Platform

IT Resiliency for the Digital Enterprise

VERITAS™

The truth in information.

Contents

REVISION HISTORY

Version	Date	Changes	Author
1.00	2-7-2019	Initial Version	Joann Starke
1.02			

INTRODUCTION

EXECUTIVE SUMMARY

How do you view disaster recovery (DR)? If you're like many of your peers, DR is viewed as a sunk cost that your organization sees little to no payback. Traditionally, DR meant creating and maintaining a second data center or it meant subscribing with an outside vendor to privately host your DR environment. Costs for both of these approaches were high which meant only the largest enterprise organizations were capable of paying for this level of data protection. Organizations of lesser size and tighter budgets relied on a roll of the dice in hopes that disruption happened to "the other guy" while they resigned themselves to the fact that any recovery could be long, difficult and impact business KPIs.

Cloud has changed the economics of DR. It allows organizations of all sizes to eliminate the building and maintaining of a second data center dedicated solely to DR. It also came with self-service business models and the ability to choose the type of infrastructure used for recovery environments delivering cost and operational efficiency. But with opportunity comes new sources of disruption. Today's digital business needs to protect itself from human error, malware, ransomware and under-provisioned instances in the cloud.

Think you're protected when the cloud is your recovery environment? Think again. When disruption occurs, many organizations are surprised to discover that backup, recovery and data security were the organization's responsibility not the cloud service provider. In many cases, this has led to data loss and damage to reputations.[1]

All this change has led to disruption. Discrete tasks such as backup, disaster recovery and replication have evolved from individual disciplines into a continuum of availability[2] requiring organizations to view recovery through the lens of application and data availability. This larger view has produced a new dialogue around business and IT resilience which is defined as:

- Business resilience is a cooperative effort between IT and business units with the goal of avoiding disruption of any kind.
- IT resilience is serving all the requirements of the business by maintaining uninterrupted application availability.[2]

SCOPE

The purpose of this document is to provide a high-level technical overview of Veritas Resiliency Platform and how it delivers IT resilience to any organization. It is designed for customers, partners and Veritas field personnel interested in learning how Resiliency Platform delivers end-to-end IT resilience across multiple traditional and cloud platforms.

For greater detail on deployment examples, please consult product documentation available for installation, configuration and administration from this link.

IT RESILIENCE

IDC defines IT resilience as the ability to protect data during planned disruptive events, effectively react to unplanned events and accelerate data-oriented business initiatives.[4] In a recent survey, IDC discovered that 93 percent of enterprise organizations have experienced tech-related business disruption in the past two years. The two most common business impacts were employee overtime and loss of productivity. However, 20 percent of participants experienced major reputational damage and permanent loss of customers.

Digital businesses run on data. Organizations rely on IT infrastructure to be reliable, available, resilient and able to avoid disruption. Veritas believes IT resilience requires:

- Automation and orchestration to manage and mitigate risk before data is lost or corrupted
- The ability to measure risk, both real-time and future, to support smarter more certain business decisions
- Business level reporting that validates service level compliance, exposes complexity that slows down business and proves the solution's value to business teams

[1] Truth in Cloud Report, 2017
[2] IDC Market Perspective, 2018
[3] IDC White Paper, 2018
[4] IDC White Paper, 2018

SOLUTION OVERVIEW

Resiliency Platform was designed to transform your organization from DR to automated IT resilience. It is the only multi-cloud platform that recovers entire data centers, applications and virtual machines across different hypervisors, operating systems, storage arrays and cloud platforms. It reduces tool fragmentation by replacing multiple solutions with a single product that supports physical and virtual infrastructure. It removes fear of the unknown— freeing teams to innovate with confidence.

Resiliency Platform was designed to meet the needs of two types of customers:

- Large and Public Sector Enterprises that need to protect:
  - More than 250+ virtual machines.
  - Have 2,500+ employees.
- Service providers upscaling their service offering using VMware vCloud Director for DR-as-a-Service.

The use cases supported by the current release are detailed in Figure 1 below.

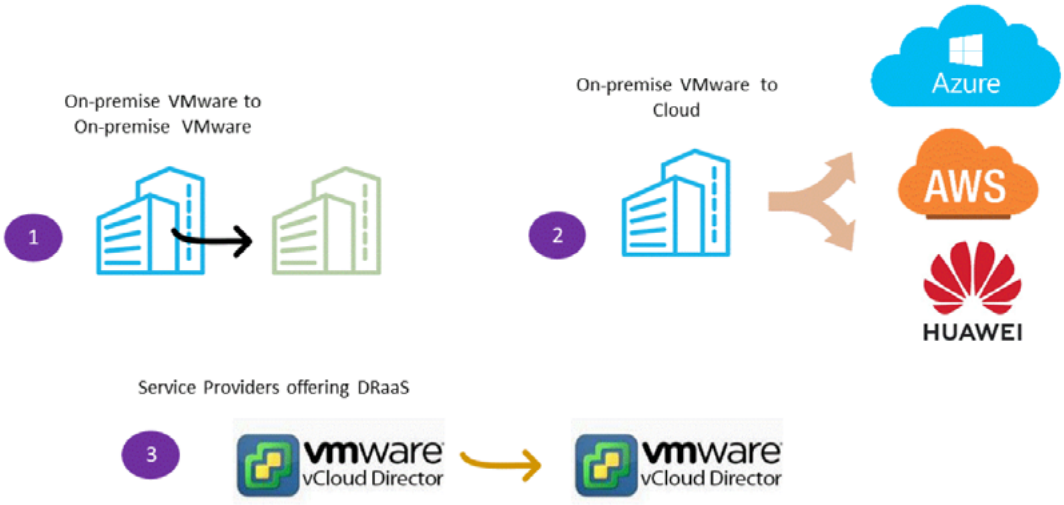
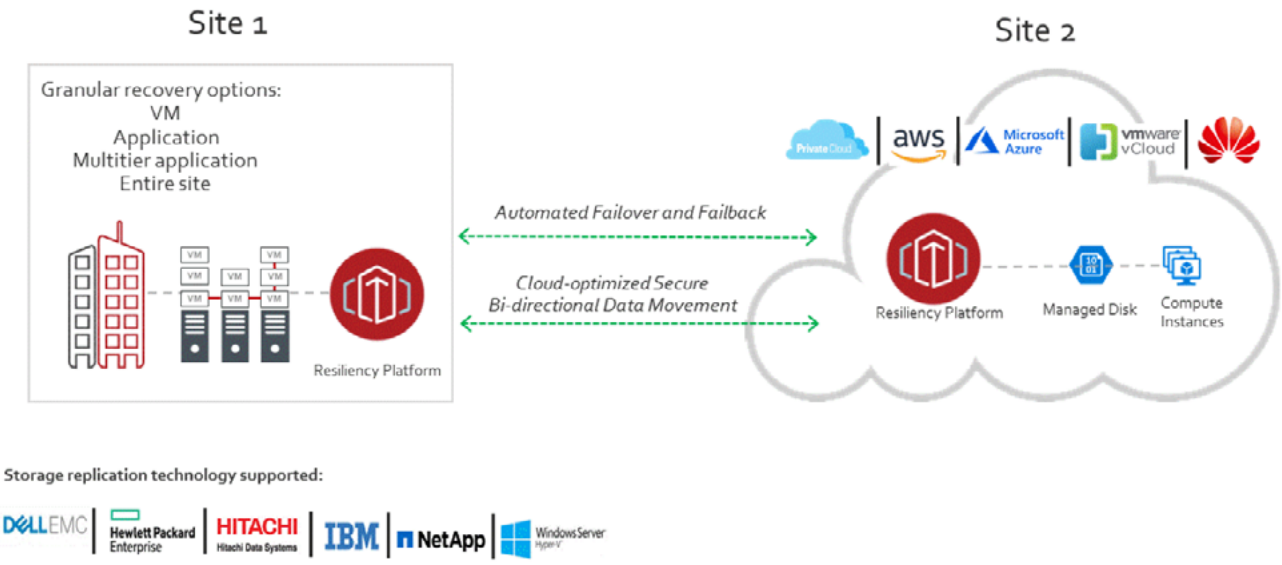


Figure 1 Resiliency Platform Use Cases

SOLUTION ARCHITECTURE

IT resilience is all about maintaining application availability through any planned or unplanned disruption. It is complex, but Resiliency Platform manages it all with:

- Single-click sequential shut down, migration and start-up of complete business services so applications get back on line sooner.
- Built-in task automation and orchestration designed to automate resilience, migration and takeover plans. Rehearse and evacuate multiple resiliency groups and virtual business services.
- Optimized performance of data movement between on-site and cloud services by eliminating data format conversion.
- Bi-directional data movement between sites using built-in compression, deduplication and encrypted connectivity between source and target environments.
- Integration with existing DNS servers to protect existing IP management and security services.
- Automated rehearsals that test links and processes at every functional level on isolated, non-production networks ensuring systems are working properly prior to any full failover event.
- Centralized management across data centers, resiliency groups, virtual machines and rehearsals. Create, manage and launch resiliency and takeover activities.
- Business-level reports prove compliance and service objectives while delivering confidence to business leaders on the resilient state of their business.



Resiliency Platform Architecture

HOW IT WORKS

CENTRALIZED CONSOLE

Resiliency Platform provides a visual representation and single management console across your entire estate that eliminates complexity and increases confidence in often-unpredictable situations. As shown in Figure 2, this console provides quick status for:

- Resiliency groups, virtual business services, rehearsal and migration runtimes.
- Identifies risk as errors, which means something has failed— and warnings which identify when assets are outside of a pre-defined service level. It also identifies potential risks that may impact business in the future.
- Allocation of assets by platform, OS, service objective, risks, application times and replication time.

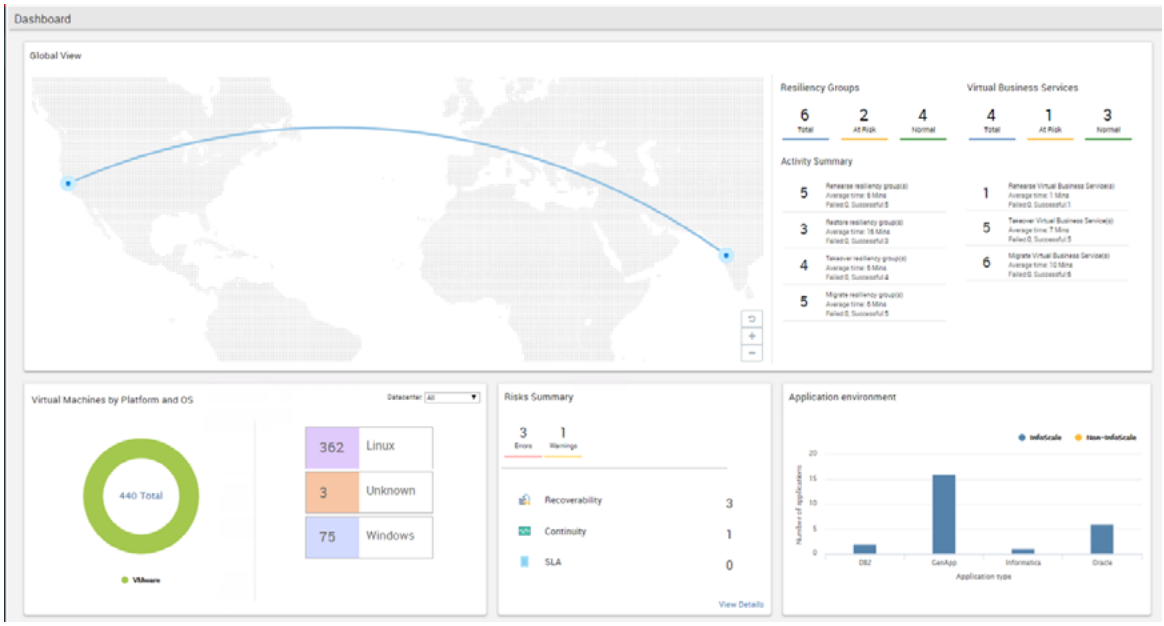


Figure 2 Graphical representation and centralized management of multi cloud environments

INFRASTRUCTURE VIEW

The infrastructure view provides a deeper segmentation of all assets across multi cloud environments. As shown in Figure 3, detailed information is provided for both the source and target environment. Some of the components include:

- Resiliency Manager which holds and transmits user information, larger site information and consistent UI settings across all sites.
- Infrastructure Manager which holds and orchestrates the data around site specific workloads like virtual machines, databases and other applications.
- Access Profile is responsible for storing and maintaining network settings.
- Application Cluster allows administrators to start, stop and orchestrate Veritas InfoScale Availability clusters.
- Data Mover holds and utilizes multiple data movers such as the native data mover, NetBackup AIR, storage and hypervisor replication technologies.
- Hosts is a repository for application settings and replication configurations.
- Storage handles filer level replication.
- Virtualization and Private Cloud holds orchestration configurations for VMware ESX and Microsoft Hyper-V hosts.

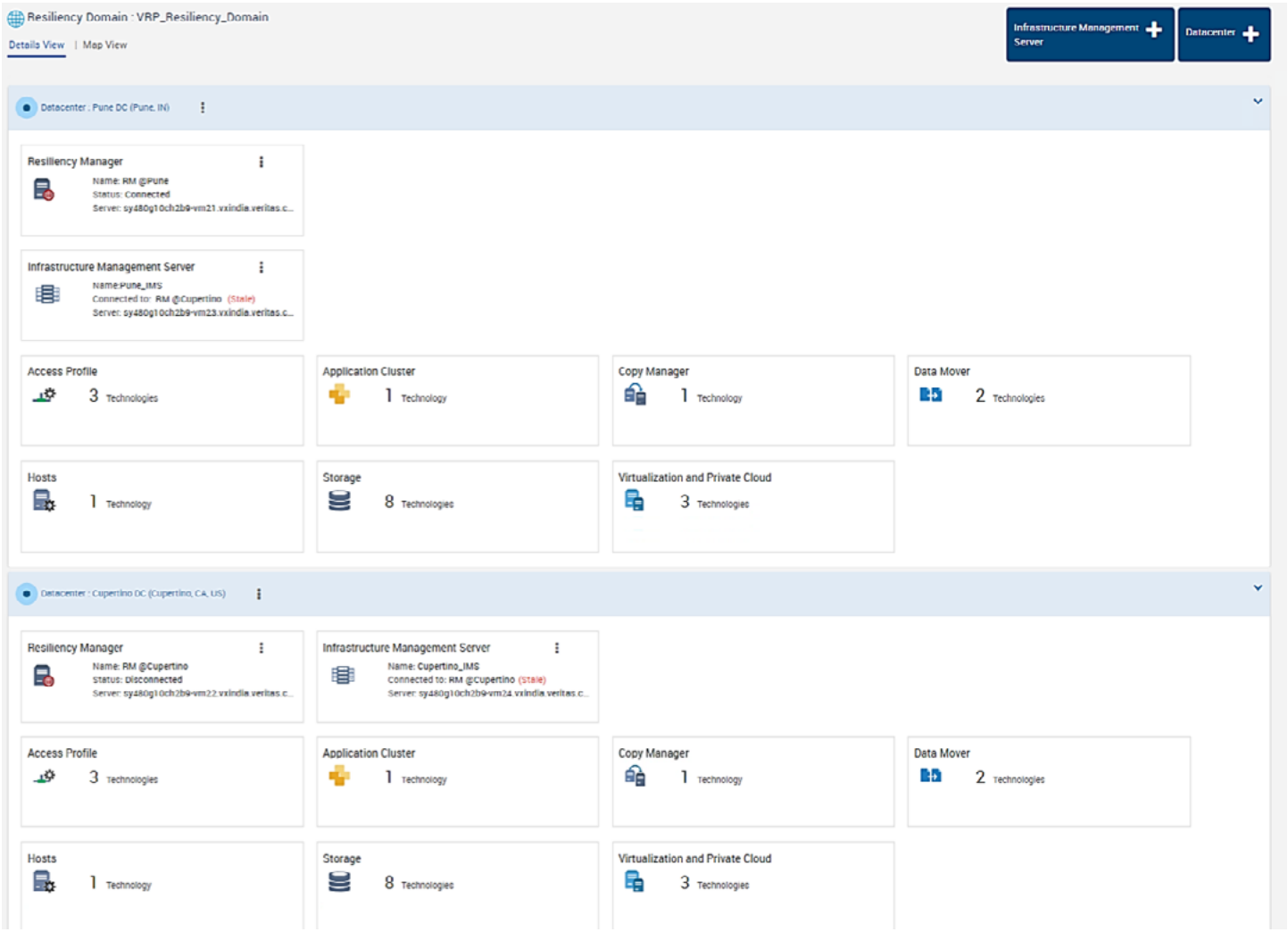


Figure 3 Infrastructure View provides configuration information on Resiliency Platform key components

SERVICE OBJECTIVES

This area is where you will assign service level objectives. Based on the data mover being utilized, this view offers pre-defined templates, as shown in Figure 5, as well as a deep level of granularity on orchestration and the speed which assets come back online.

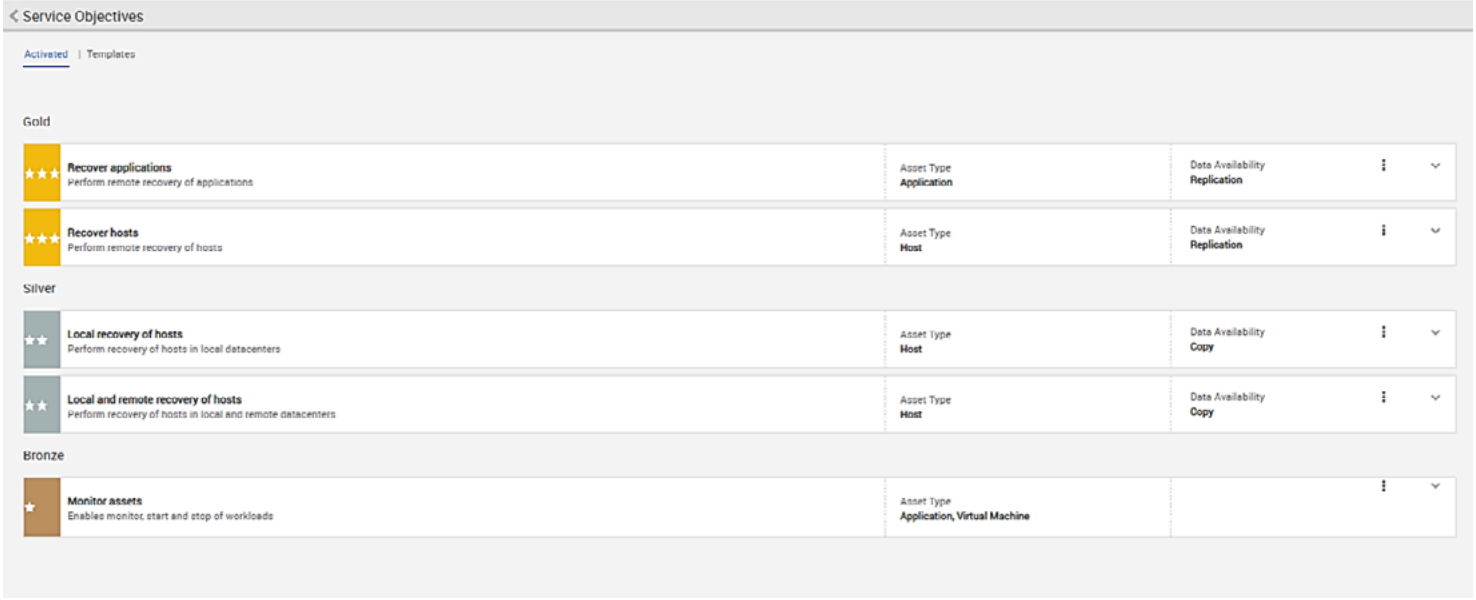


Figure 4 Resiliency Platform service objectives currently activated

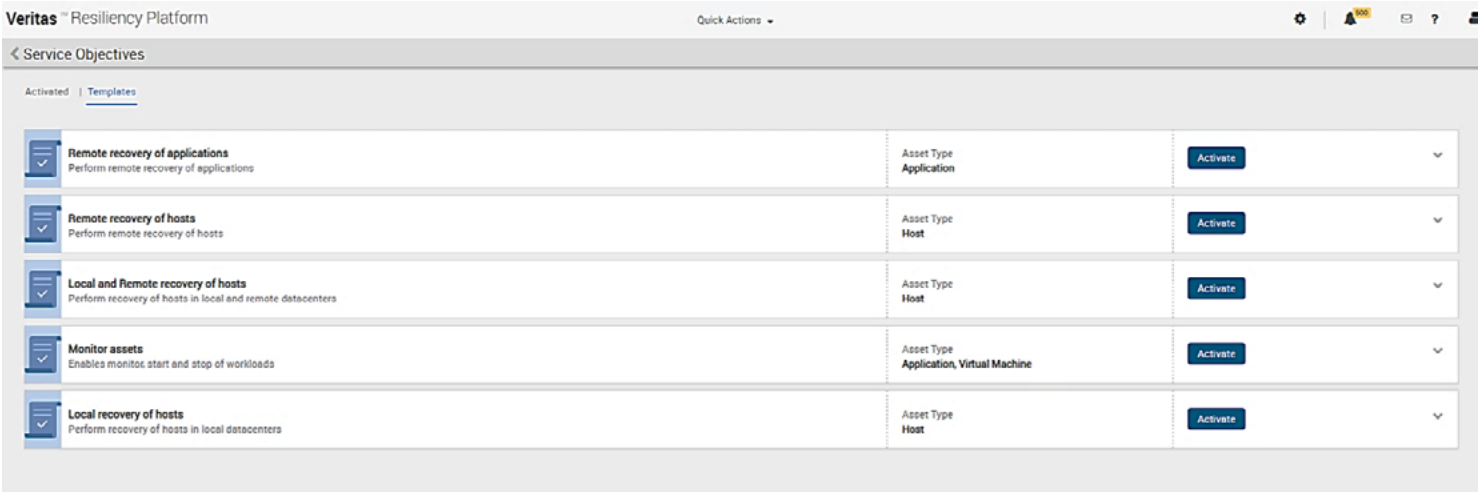


Figure 5 Pre-defined service objective templates

ASSET VIEW

As shown in Figure 6, the asset view provides an overview of the entire estate, breaks assets down by unprotected, protected resiliency groups and virtual business services. These are defined as:

- Assets in the unprotected category are not under management by Resiliency Platform. Resiliency Platform may be used to start, stop and manage these assets on the source environment.
- Resiliency groups are assets that have been configured into specified groups and protected as a single entity. Resiliency groups can be configured for basic monitoring (i.e., start or stop virtual machines) or remote recovery.

- Virtual business services group application tiers together to represent an entire business service. In the event of a failover or rehearsal, Resiliency Platform sequentially shuts down, migrates and starts up the application in the correct sequencing, establishing dependencies and connections making the service available to customers as quickly as possible.

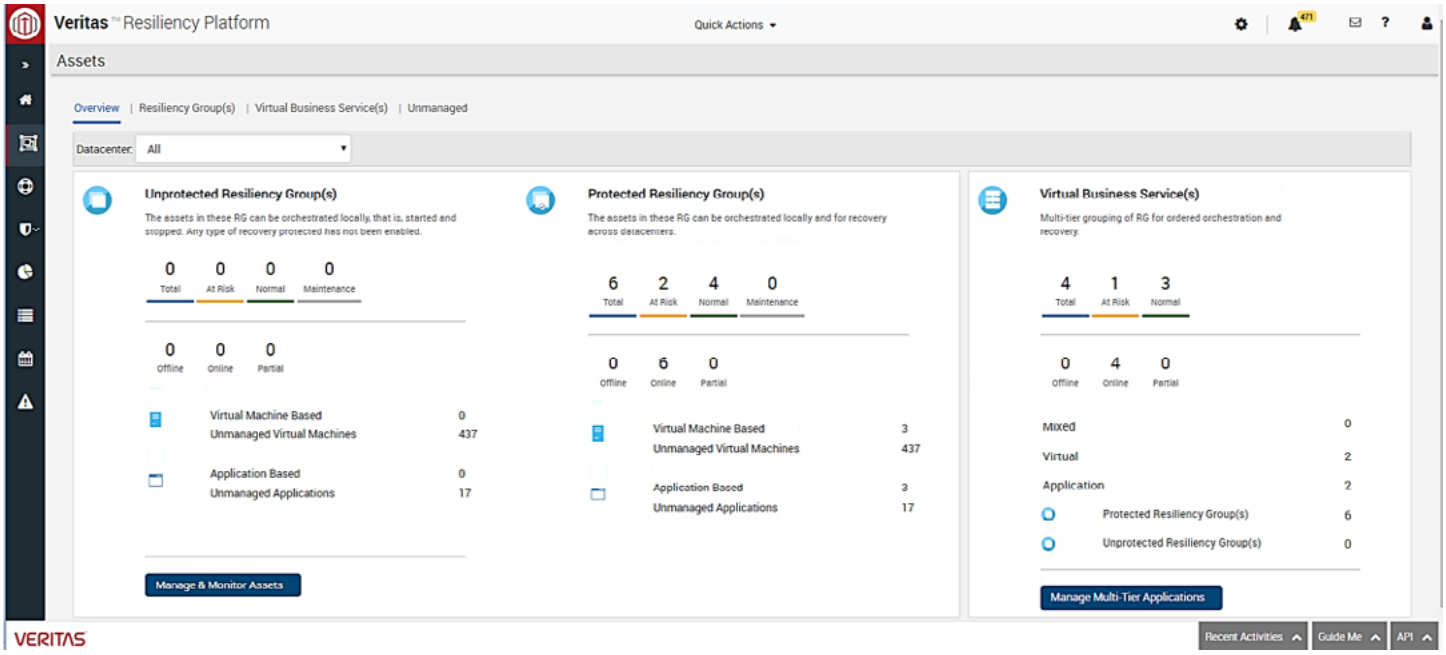


Figure 6 Asset overview and summary

Creating a resiliency group is completed by a "drag and drop" process of all the virtual machines desired in a single resiliency group.
Virtual business services are created in the same manner with the difference being resiliency groups being placed into assigned recovery tiers, see Figure 7.

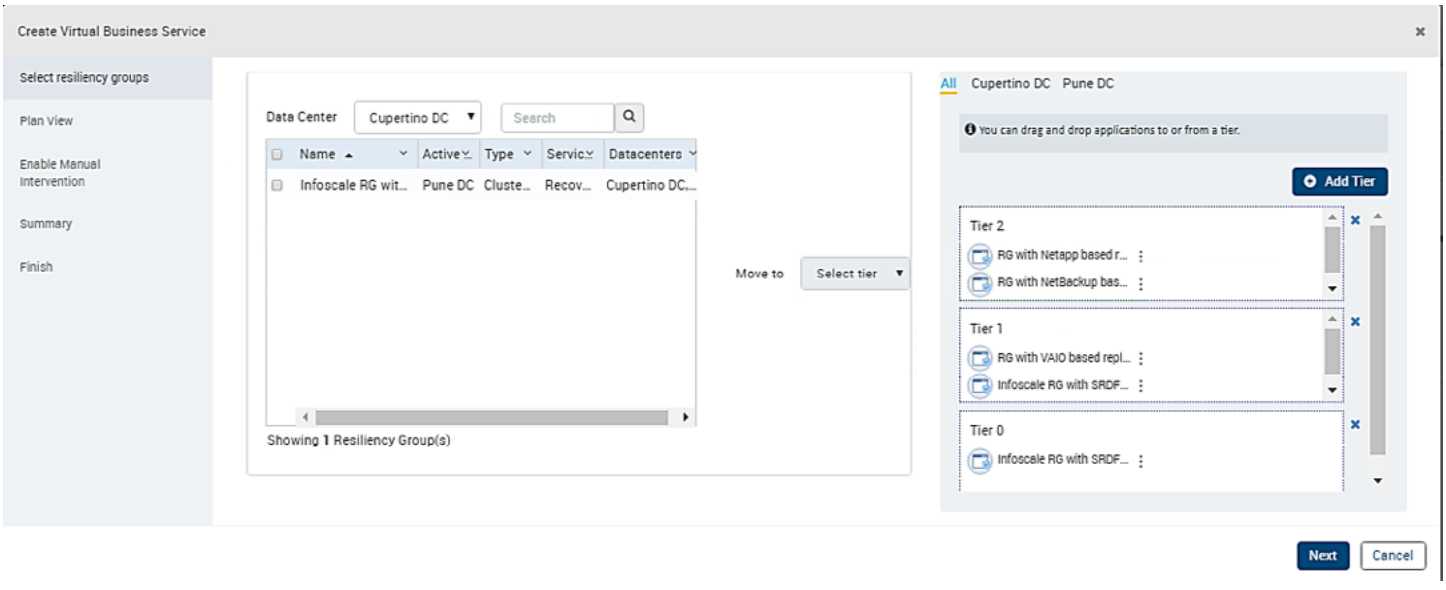


Figure 7 Drag 'n Drop Resiliency Groups to create Virtual Business Services

AUTOMATION PLANS

With the all the individual components defined, Resiliency Platform makes it easy to bring it all together into an automated recovery or rehearsal plan. The automation tab is where customers can find granular information on automation plans. In the example below, we have a primary data center in London and a recovery data center in New York.

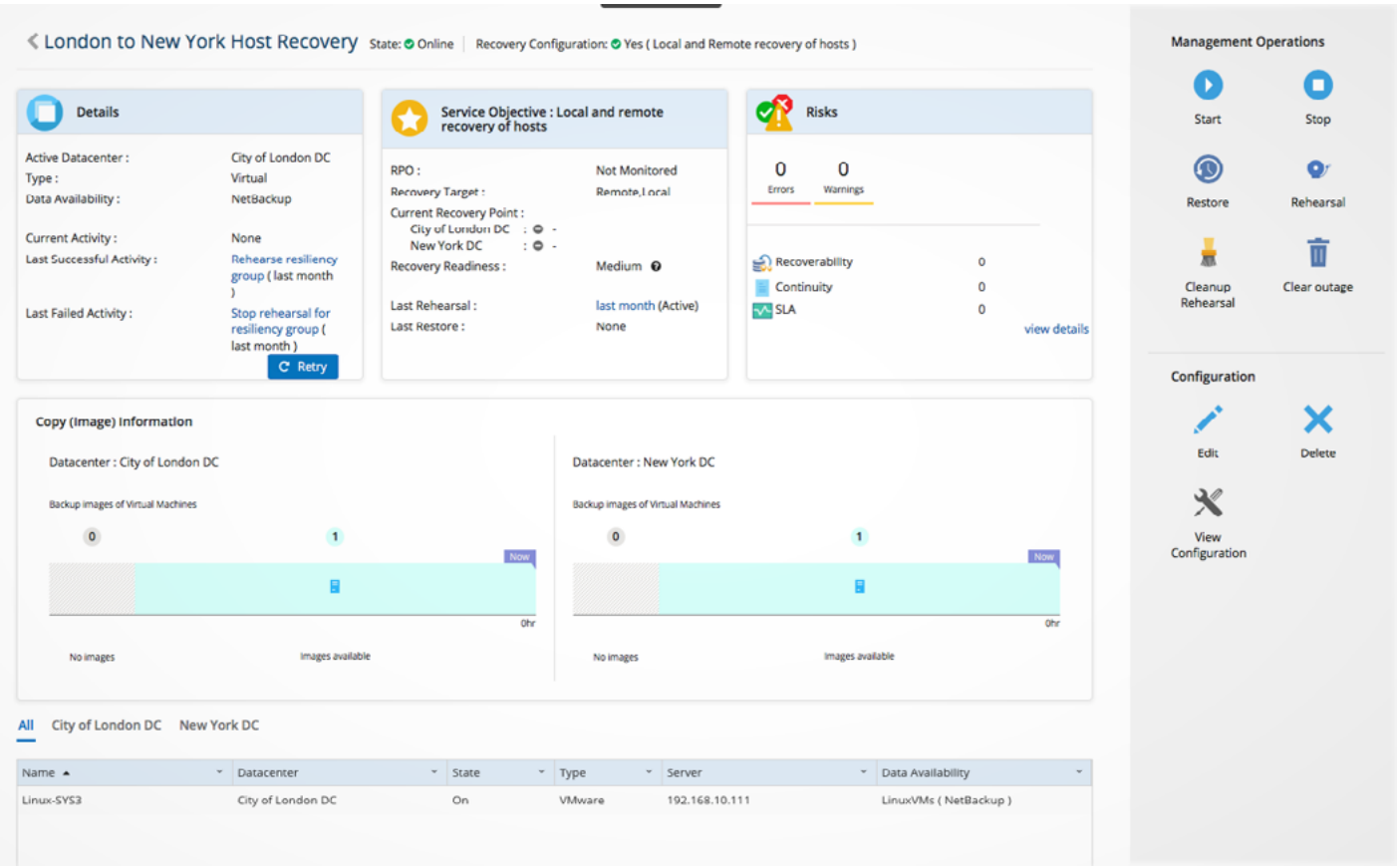


Figure 8 Configuration Detail for Automated Plans

Here we see we are protecting 1 virtual machine that is currently located in the London data center. At the top, we can see more details on where things are being protected as well as the recovery point and recovery time objectives.

To the right of the screen, we see management options that can be added to this automation plan. Start, stop and restore buttons make it simple to start a migration from data center to data center, stop it in mid-progress or restore the image back to the original data center. Customers can also run rehearsals that enable running of the plan in a walled-off environment that looks and behaves just like the production data center. When testing is complete, a simple click initiates an automated clean-up process removing all traces of testing.

COMBINING RESILIENCY GROUPS AND VIRTUAL BUSINESS SERVICES

Recovering business services in the correct sequence can also be configured within Resiliency Platform. Below is an example of a virtual business service recovery plan showing the recovery of an application from London to New York.

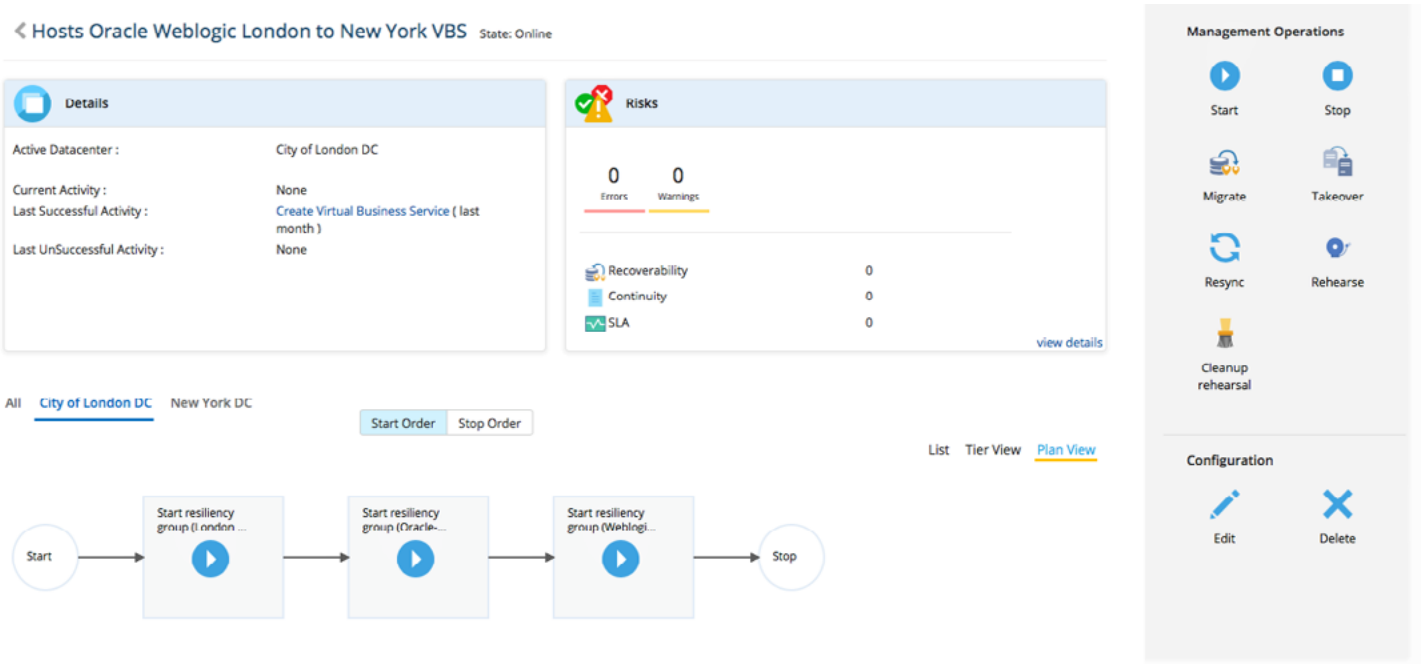


Figure 9 Recovery of application in a tiered and orchestration manner

On the right side of the user interface are recovery operations that can be configured into an automation plan. Migrate involves graceful shut down and start up of applications from a source to a target data center or cloud platform. Takeover is a less graceful way of migrating applications from a source to a target. For example, if the source data center loses power, this is the nuclear option that moves applications to a second data center or cloud platform.

BRINGING IT ALL TOGETHER

Resiliency Platform can tie together resiliency groups, virtual business services, rehearsals, manual tasks and custom scripts. Manual tasks allow the plan to be stopped for a time to complete human driven action and/or custom scripts. Custom scripts allow the user to tie together bash, python, powershell and other automated script options. The figure below details the robust nature of customization available through Resiliency Platform.

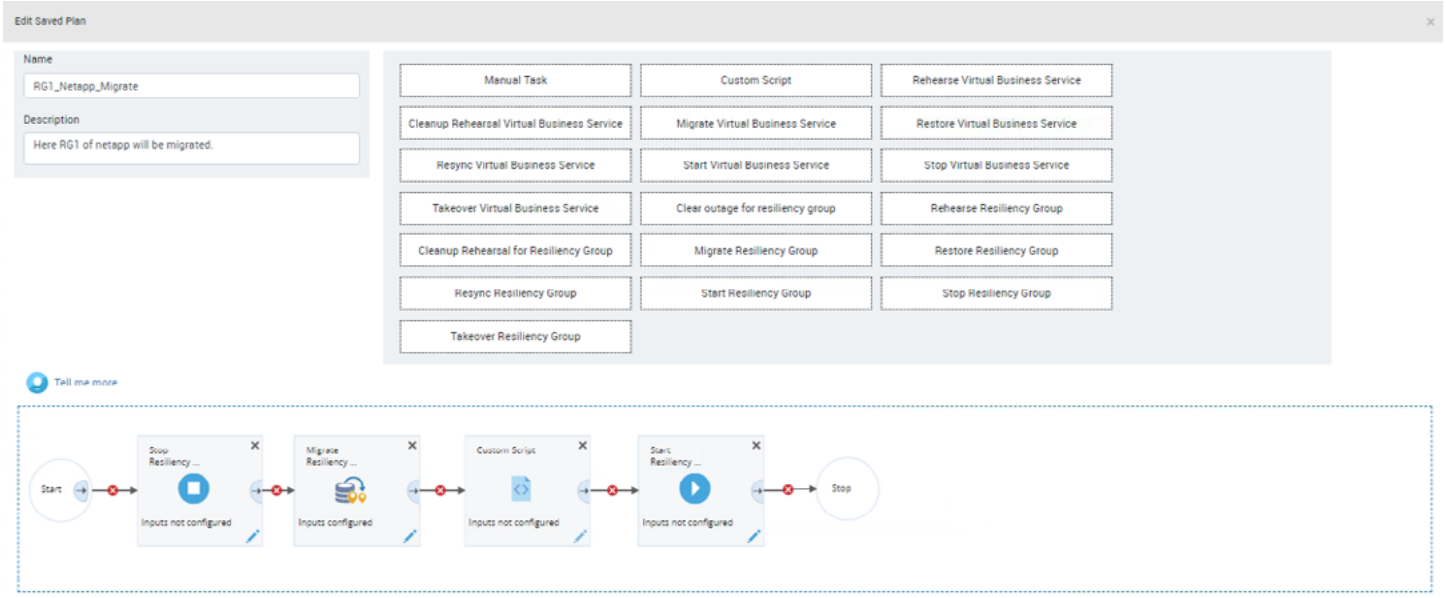


Figure 10 Customizing and Bringing Together Resiliency Groups into HA/DR Plans

GETTING STARTED

Getting started with Resiliency Platform requires installation of three virtual software appliances into any onsite data center. Table 1 details the functionality of each component.

VMware vCenter Server	A centralized management application that allows users to manage VMware virtual machines and ESXi hosts centrally. vCenter Server can be used to install the Resiliency Platform components by using the "Deploy OVF Template" option for the Resiliency Platform OVA files.
VMware ESXi Server (provided by user)	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. For situations where VAIO is not available, Resiliency Platform installs a managed host package on the virtual machine guests running on the ESXi hosts. The managed host package is an I/O tap that relays data from the virtual machines to the local Resiliency Platform Replication Gateway.
Resiliency Manager (RM)	The resiliency manager provides services required to protect assets identified by the user to come under the control of Resiliency Platform. Once identified, this creates what is known as a Resiliency Domain. The Resiliency Manager works in tandem with the Infrastructure Management Server to discover and manage information about assets in each Resiliency Domain.
Infrastructure Management Server (IMS)	The Infrastructure Manager Server (IMS) discovers and monitors assets within a data center and allows management operations on assets in each resiliency domain, for example: starting and stopping a virtual machine. This component scales horizontally to allow Resiliency Platform to scale with the environment.
Replication Gateway (RG)	The replication gateway manages replication across sites and hypervisors. Replication across on-site VMware environments and AWS occurs without format conversion increasing transfer rates and lowers recovery point objectives making applications available sooner. The replication gateway also scales horizontally to meet application scaling.

Table 1 Resiliency Platform components

REPLICATION

Resiliency Platform supports native replication, Veritas NetBackup and third-party storage replication. Please consult the Resiliency Platform for VMware vSphere for more details. (Read the tech brief)

LICENSING

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

When configuring Resiliency Platform to use NetBackup for data replication, a NetBackup license that enables AIR is required.

When using storage replication, licensing for the storage system may be required to enable replication functionality.

SIZING GUIDANCE

System resources may vary based on factors such as environment size, performance requirements and usage patterns. The most current user guides and documentation can be found on the Veritas Services and Operations Readiness Tools (SORT) website at this link.

CONCLUSION

IT resilience must be held as a premium to elevate a business' value. Disruptions are uncontrollable, unpredictable and full of consequences. They range from large-scale events to more frequent errors and malfunctions. Application availability is a growing need to provide 24/7 support to digital business and customer-facing services.

Resiliency Platform was designed to integrate with your evolving IT landscape to deliver IT resilience across hypervisors, operating systems, storage and cloud platforms. It maximizes your existing investment in third party storage arrays and NetBackup—allowing your organization to experience:

- Scalability with cluster level replication that makes it easy to scale VMware environments. Utilization of third party storage integration allowing organizations to dynamically scale and manage data volumes with little or no application downtime.
- Simplified Management that replaces manual processes with automation and orchestration that decreases human error and frees up staff to focus on new innovation. Virtual Business Services further simplifies management by logically representing multi-tier application stacks as single entities that can be migrated and rehearsed with a single click.
- Increased visibility and control with visual representation and a single management console across all environments that eliminates complexity and increases confidence.
- Innovate with confidence with non-disruptive rehearsals that preserve production uptime, keeps business teams informed of the resilience state of the business and allows teams to make smarter, more certain business decisions.

Go deeper with Resiliency Platform at: www.veritas.com/resiliency

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.

V0854 03/19