# UNMATCHED AVAILABILITY SOLUTION FOR VXRAIL
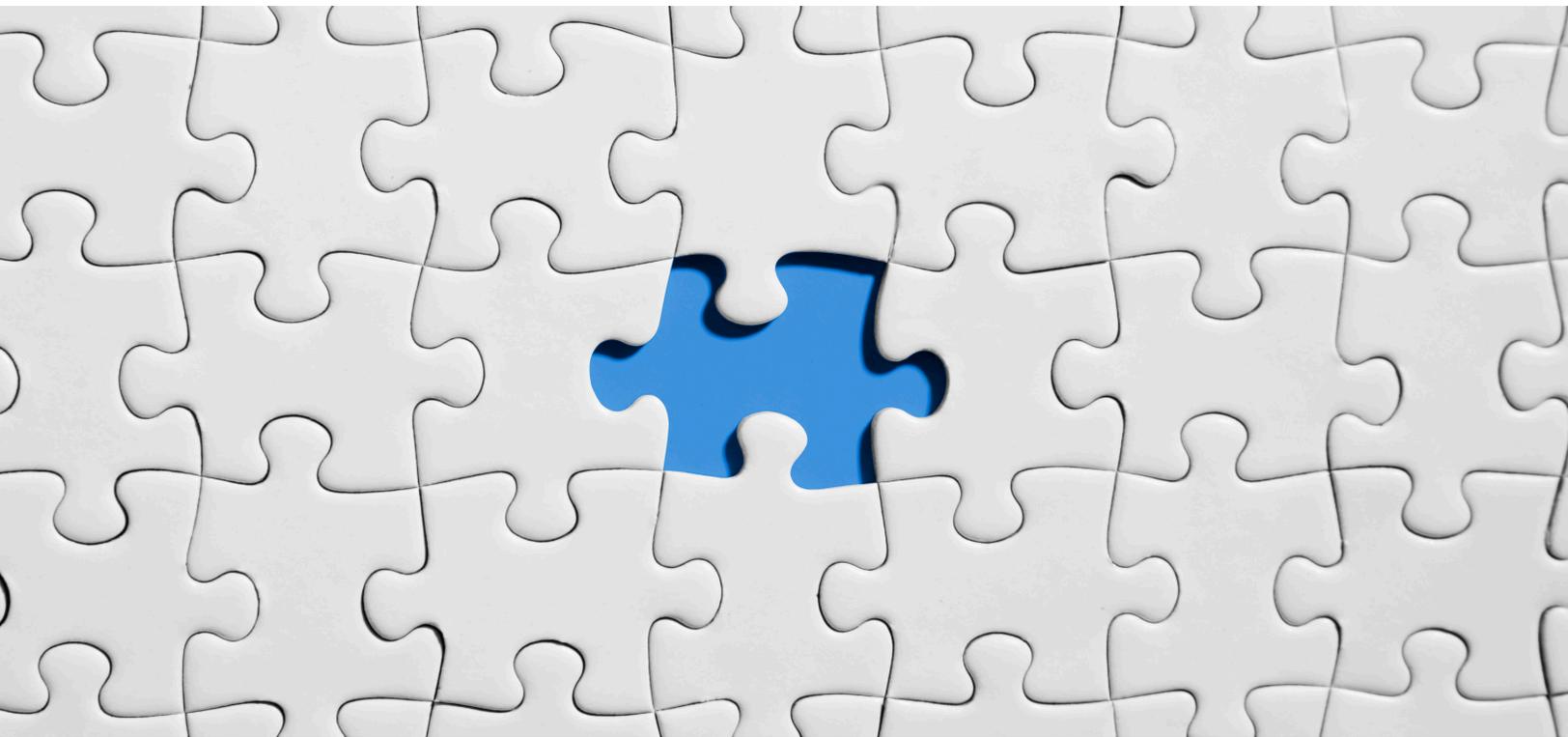
Victor Wu

Senior Solution Expert, Business Consultation

BoardWare Information System Limited

victor.wu@boardware.com.mo

Samson Tu

Senior Service Engineer, Professional Services

BoardWare Information System Limited

samson.tu@boardware.com.mo

Table of Contents

Table of Figures

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Preface

In the digital economy, applications are both the face and the backbone of the modern enterprise. For the digital customer, the user experience is very important. Customer-facing applications must be available anytime, anywhere and on any device, and must provide real-time updates and intelligent interactions. Traditional IT teams are faced with a massive amount of complexity when building, configuring, maintaining and scaling applications. The customers need to successfully deploy and operate an environment that takes full advantage of the innovation taking place across the industry – without the complexity of configuration and supporting a wide range of tools.

One of the first steps a business can take in their transformation journey is to simplify infrastructure deployment and management by introducing hyper-converged infrastructure (HCI) into the environment. HCI systems essentially collapse the traditional three-tier server, network, and storage model so that the infrastructure itself is much easier to manage.

Introduction

This Knowledge Sharing article provides information on availability solutions for VxRail Appliances – i.e. Active-Active (AA) Infrastructure, Active-Active-Passive (AAP) Infrastructure and Point-in-time Recovery (PITR) Solution.

Dell EMC VxRail Appliances

Developed by Dell EMC and VMware, VxRail Appliances are the only fully integrated, preconfigured, and tested HCI appliance powered by VMware vSAN technology for software-defined storage (SDS). VxRail Appliance uses VMware vSphere features such as vMotion, Distributed Resource Scheduler (DRS) and High Availability (HA) for avoiding planned and unplanned downtime and site maintenance of your virtual environment. Additionally, vSAN features Failure to Tolerate (FTT) and Fault Domains (FD) provides site level protection against disk, host, connectivity, power, and rack failure.

VxRail Appliance is configured as a cluster including of a minimum of three server nodes, each node containing the internal storage drives, e.g. SSD, SAS and SATA. VxRail systems come with the software loaded, and it includes VxRail Manager, VMware vCenter Server Appliance, VMware vCenter Server Platform Services Controller (PSC) and VMware vRealize Log Insight. Internal and external connectivity of VxRail Appliance is 10GB Ethernet, 25GB with 1GB Ethernet connectivity also available. VxRail Appliances are built-in with the newest 14th generation Dell EMC PowerEdge server platform.

VxRail Manager presents a simple dashboard interface for infrastructure monitoring and automation of lifecycle management tasks such as software upgrades and hardware replacement. Since VxRail nodes function as ESXi hosts, vCenter Server is used for virtual machines management, automation, monitoring, and security.

VxRail Manager provides out-of-the-box automation and orchestration for day 1 to day 2 appliance-based operational tasks. It can provide lifecycle management, automation, and operational simplicity. For the firmware upgrade of the VxRail Appliance, we just upload a single software package into VxRail dashboard and can complete the upgrade process with a single click. The operation is simple and automated. We no longer need to verify hardware compatibility lists, because the software upgrade package is pre-tested and validated by Dell EMC and VMware.

VxRail Appliance consists of five models to meet the requirements of a wide set of use cases, e.g. smaller workloads, performance optimized, VDI optimized, etc. Table 1 shows the range of platforms designed to support multiple use cases.

Table 1 - VxRail based on 14th generation Dell EMC PowerEdge Servers

Series	G Series Nodes	E Series Nodes	P Series Nodes	V Series Nodes	S Series Nodes
Workload	Compute densely	Smaller Workload	Performance optimized	VDI optimized	Storage densely
Model Type	G560/G560F	E560/E560F	P570/P570F	V570/V570F	S570

Environment

Before we discuss the availability solutions for VxRail Appliances, let us have an overview of the sample environment in this scenario (three sections in this article). This environment consists of:

- Four VxRail E560 Appliances installed on each site (primary, secondary and witness host).
- Two 10GB network switches installed on each site, and each switch is used for the networks of vSAN Cluster, vSphere Management, vMotion and virtual machines.
- One 1GB network switch installed on site, with each switch used for remote management (iDRAC) on each VxRail Appliance.
- One vSAN witness virtual machine installed at the third site, used to monitor the data node at the primary and secondary site.
- One vCenter Server Appliance 6.5 manages the vSAN stretched cluster, the other vCenter Server Appliance 6.5 manages the VxRail cluster installed at the remote site.

- VxRail 4.5 software package installed on each VxRail E560.
- VMware Site Recovery Manager 8 installed at the protected site and recovery site.
- VMware vSphere Replication 8 installed at the protected site and recovery site.
- Dell EMC RecoverPoint for VMs 5.2 installed at the primary site and secondary site provides point-in-time data protection.

Active-Active (AA) Infrastructure

Overview

VxRail Appliance is powered by VMware vSAN software, which is fully integrated with the kernel of vSphere and provides full-featured and cost-effective software-defined storage (SDS). The vSAN stretched cluster feature creates a stretched cluster between two geographically separate sites (primary and secondary site), and synchronously replicates data between sites. This feature allows an entire site failure to be tolerated. It extends the concept of fault domains to data center awareness domains.

The vSAN stretched cluster must build on between two separate sites. Each stretched cluster includes two data sites and one witness host. The witness host deploys a third site that contains the witness components of virtual machine (VM) objects. The witness host is a decision maker that monitors the availability of datastore components when the network connection between the two data sites is lost. The witness host can be a virtual machine or physical machine.

Stretched clusters use fault domain technology to provide redundancy and failure protection across sites. A stretched cluster requires three fault domains: the preferred site, the secondary site, and a witness host. In Figure 1, we see two fault domains and each domain includes two nodes. The minimum number of nodes is dependent on the VxRail version and stretched cluster configuration. Table 2 shows the VxRail version and the minimum number of nodes per site.
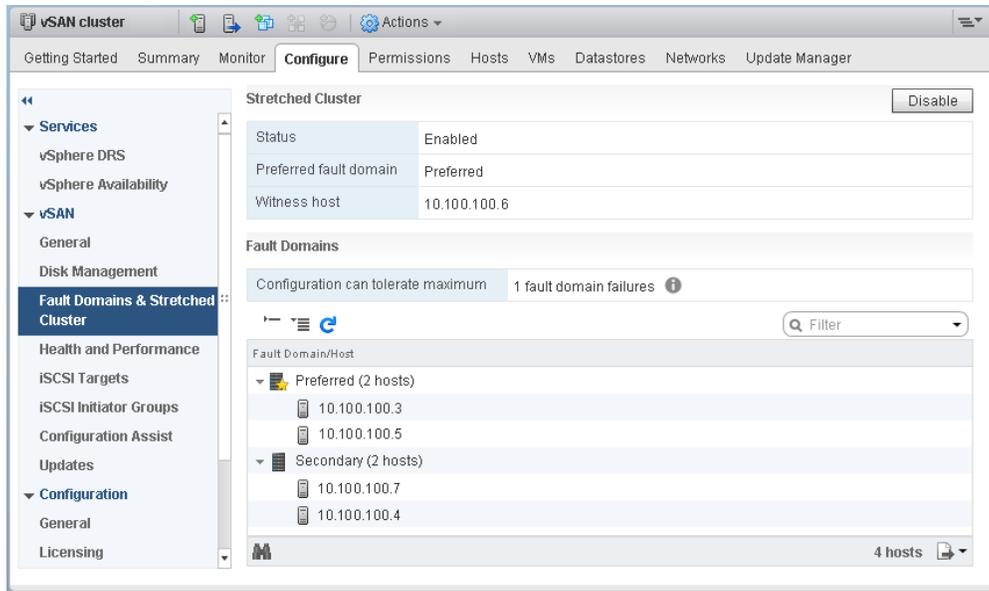
Figure 1 - Configuration of Fault Domains & Stretched Cluster

Table 2 - VxRail version and minimum number of nodes per site

VxRail Version		Minimum Nodes: Preferred Site + Secondary Site + Witness host
VxRail 4.5.070 and later releases NOTE: Erasure Coding can only be enabled on All-Flash vSAN cluster.	PFTT = 1; SFTT=1; Failure Tolerance Method=RAID-1 (Mirroring)	3 + 3 + 1
	PFTT = 1; SFTT=2; Failure Tolerance Method=RAID-1 (Mirroring)	5 + 5 + 1
	PFTT = 1; SFTT=3; Failure Tolerance Method=RAID-1 (Mirroring)	7 + 7 + 1
	PFTT = 1; SFTT=1; Failure Tolerance Method=RAID-5/6 (Erasure Coding)	4 + 4 + 1
	PFTT = 1; SFTT=2; Failure Tolerance Method=RAID-5/6 (Erasure Coding)	4 + 4 + 1

PFTT = Primary level of failures to tolerate, SFTT = Secondary level of failures to tolerate

Architecture

Figure 2 shows a high-level overview of the sample Active-Active infrastructure environment in this scenario.
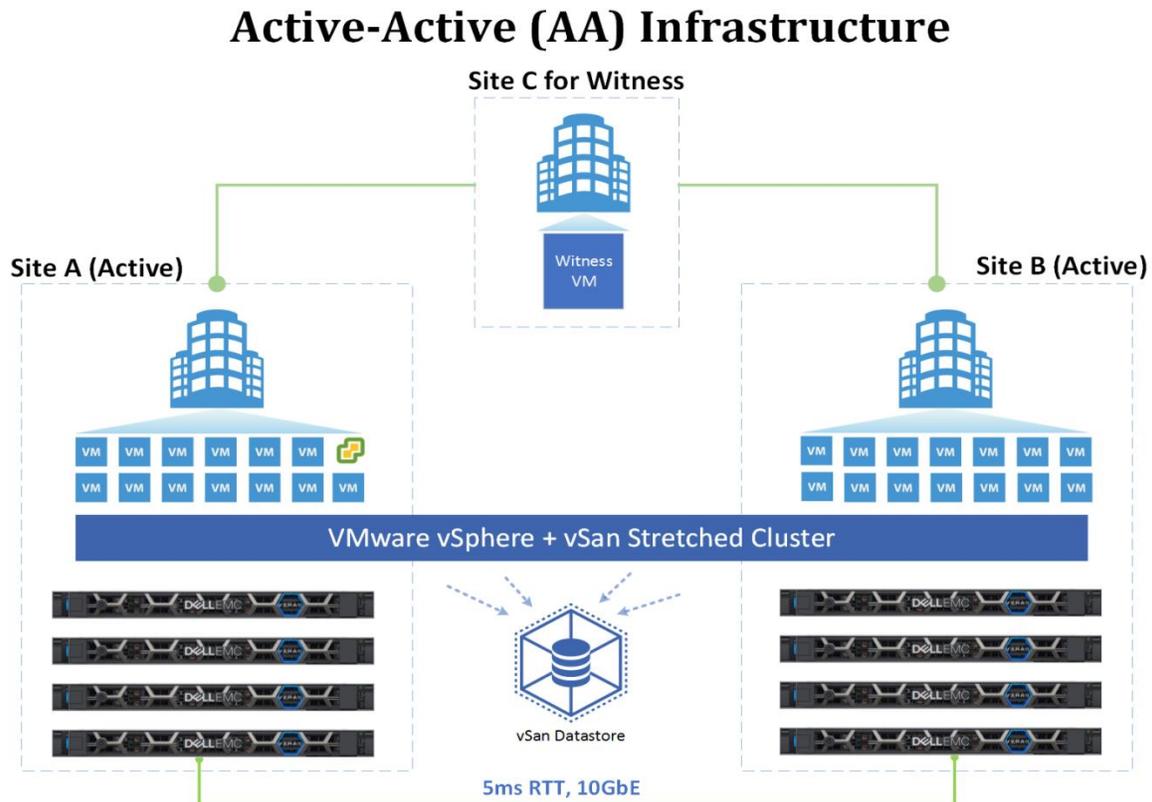
Figure 2 – Architecture Diagram of VMware vSAN Stretched Cluster

The Active-Active infrastructure environment consists of the following:

In site A and B

- Four VxRail E560 appliances are running as data node at site A.
- Four VxRail E560 appliances are running as data node at site B.
- A vSAN stretched cluster (4+4+1) is deployed across site A and B.
- A vCenter server appliance that is installed outside of VxRail cluster manages the vSAN stretched cluster.
- VxRail Manager 4.5 manages and monitors all VxRail E560 across site A and B.

In site C

- A vSAN witness virtual machine is deployed that monitors all vSAN data nodes across site A and B.

Requirements

This section describes the requirements to deploy VMware vSAN stretched clusters in a VxRail Cluster.

VxRail Cluster Requirements

The VxRail Cluster **must** be deployed across two sites in an Active-Active configuration. Table 3 shows the configuration of each VxRail appliance in vSAN stretched cluster. The witness host **must** be installed on a third site that has independent paths to each data site. Table 4 shows the compatibility for VxRail and Witness host. The maximum supported configuration of vSAN stretched cluster is 15+15+1 (30 nodes + 1 witness). Failure Tolerance Method (FTM) of RAID-5/6 is available starting with VxRail 4.5.070 and vSAN 6.6 and must be in the configuration of vSAN All-Flash.

Table 3 - The configuration of each VxRail appliance in vSAN Stretched Cluster

Sites	Server	Fault Domain
A	VxRail E560	Fault Domain 1 (Preferred site) – Active
B	VxRail E560	Fault Domain 2 (Secondary site) – Active
C	Witness VM	Fault Domain 3 (Witness host)

Table 4 – The support matrix with VxRail and Witness Host

| VxRail Version	Witness Host Version
VxRail 3.5	Witness VM host 6.2
VxRail 4.0.x	Witness VM host 6.2
VxRail 4.5.x	Witness VM host 6.5

vCenter Server Requirements

Starting with VxRail 4.5.200, either an embedded vCenter server appliance with VxRail or an external vCenter Server can be supported for vSAN stretched clusters. The external vCenter Server **cannot** be hosted on and manage the VxRail Cluster that is also in its own stretched cluster. The external vCenter Server version **must** be identical to the VxRail vCenter Server version. Choosing the external vCenter server, requires the following:

- The Fully Qualified Domain Name (FQDN) of the external vCenter Server is required.
- If the PSC is non-embedded, the FQDN of external PSC is required.
- Make sure the customer Domain Name System (DNS) server can resolve all VxRail ESXi hostnames before deployment.
- Create a datacenter on the external vCenter Server for joining the VxRail Cluster.

- Create a "VxRail management" user in Single Sign-On (SSO) that has no role assigned. VxRail will make a new role and assign it to the user.

Network Requirements

A stretched cluster in VxRail requires Layer 2 connectivity between two data sites (Site A and B). The connectivity between the data sites and the witness **must** be in Layer 3. Figure 3 shows a high-level supported configuration of the sample supported network topology. The network latency between two data sites should not be higher than 5 msec. The network latency of data site to the witness depends on the number of objects in the vSAN stretched cluster. It must be less than or equal to 100 msec.

Mgmt VLAN = 103
VSAN VLAN = 104

Witness Host

Site 3 (Witness Host)

Static routes VSAN Network
Site 1 VLAN 102 to Site 3 VLAN 104
Site 2 VLAN 102 to Site 3 VLAN 104
Site 3 VLAN 104 to Site 1 VLAN 102
Site 3 VLAN 104 to Site 2 VLAN 102

Switch 3

Router 2

Mgmt VLAN = 101
VSAN VLAN = 102

Mgmt VLAN = 101
VSAN VLAN = 102

Router 1

Stretched Layer 2 Network

Switch 1

Switch 2

Site 1 (Active)

Site 2 (Active)
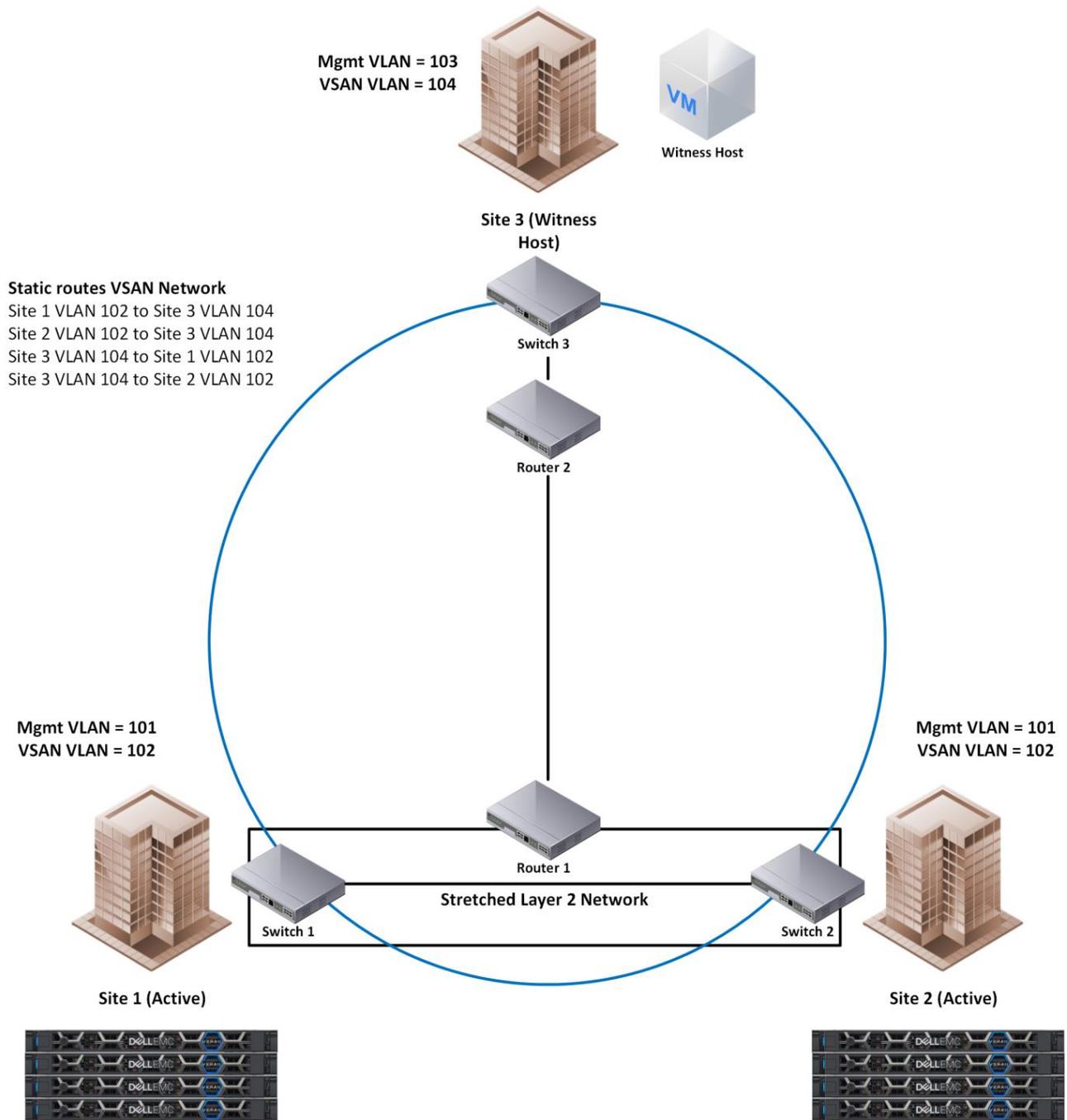
Figure 3 - VxRail Supported Network Topology

Day Two Operations

This section describes some operations of VMware vSAN stretched clusters in a VxRail Cluster.

Planned Maintenance

Figure 4 shows that the virtual machines online move to site B from site A. If the system administrator is planning to upgrade the virtual machines at site A, they should first move the virtual machines running on VxRail at site A to site B. The system administrator can perform this migration of virtual machines with VMware vMotion to ensure that service of virtual machines are not interrupted during the migration.
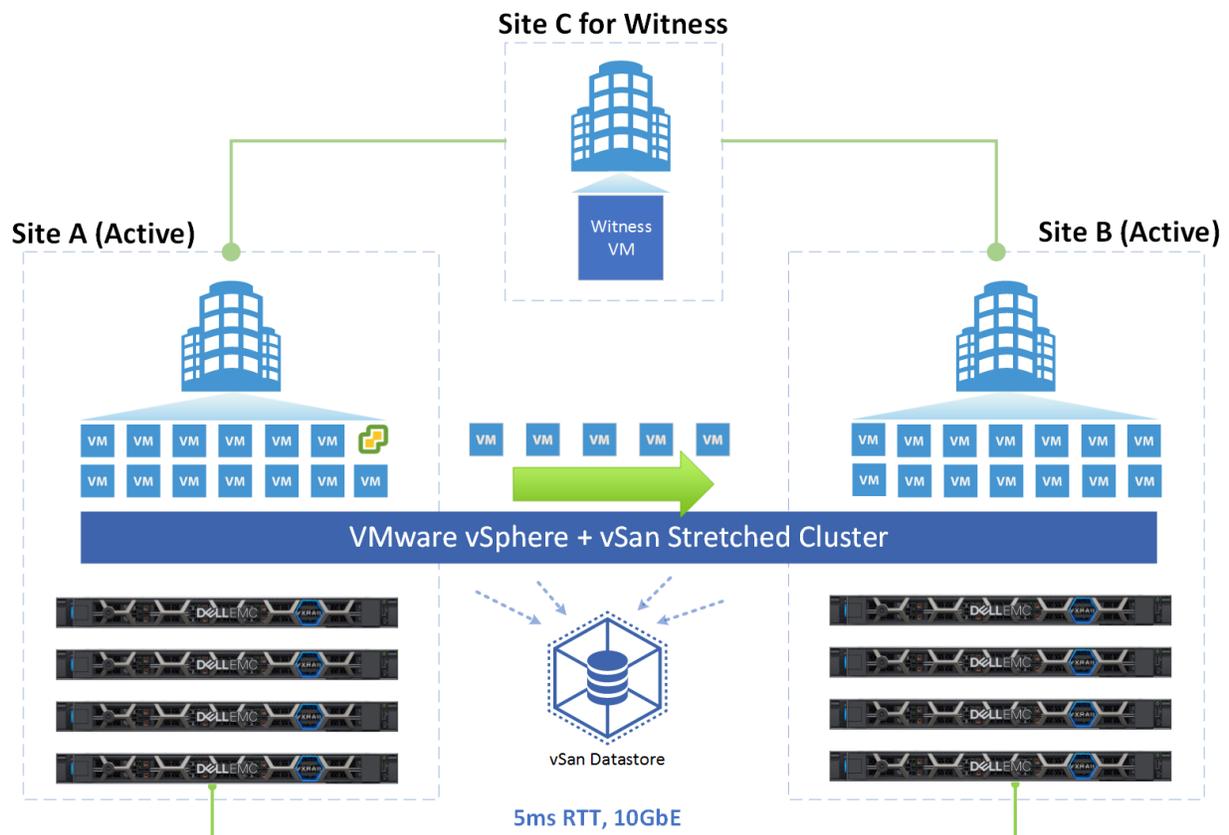
Figure 4 - The virtual machines online move to site B from site A

Unplanned Failure

Figure 5 shows that all of the VxRail appliances faulted at site A. If the site A (preferred site) faulted, all virtual machines on VxRail of the preferred site will trigger VMware High Availability (HA), and restart all virtual machines automatically on VxRail at site B (secondary site). The virtual machines on VxRail of the secondary site will remain running at site B.
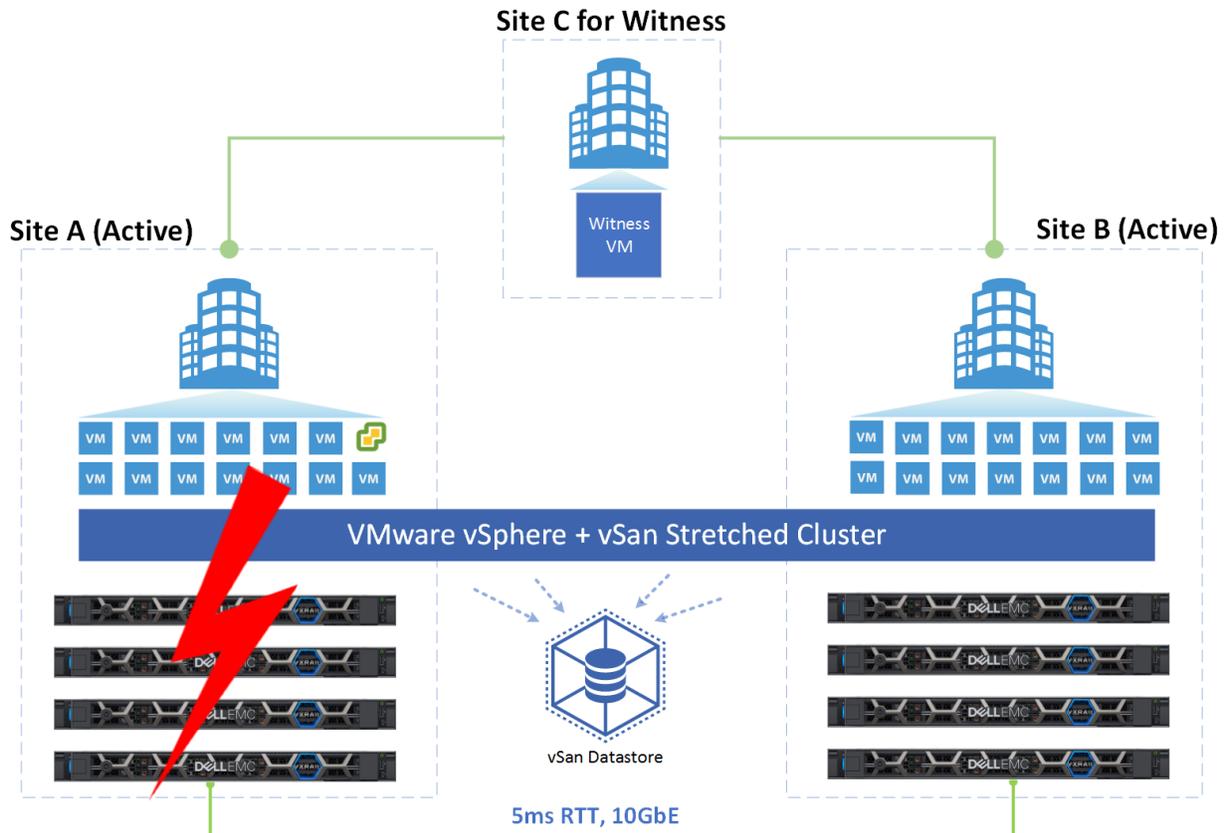

Figure 5 - All of the VxRail appliances faulted at Site A

Figure 6 shows that the vSAN network is disconnected between site A and B. If the vSAN network is disconnected between the preferred site and the secondary site, all virtual machines on VxRail of the secondary site will trigger VMware High Availability (HA) and restart all virtual machines automatically on VxRail at preferred site. The virtual machines on VxRail of the preferred site remain running at site A.
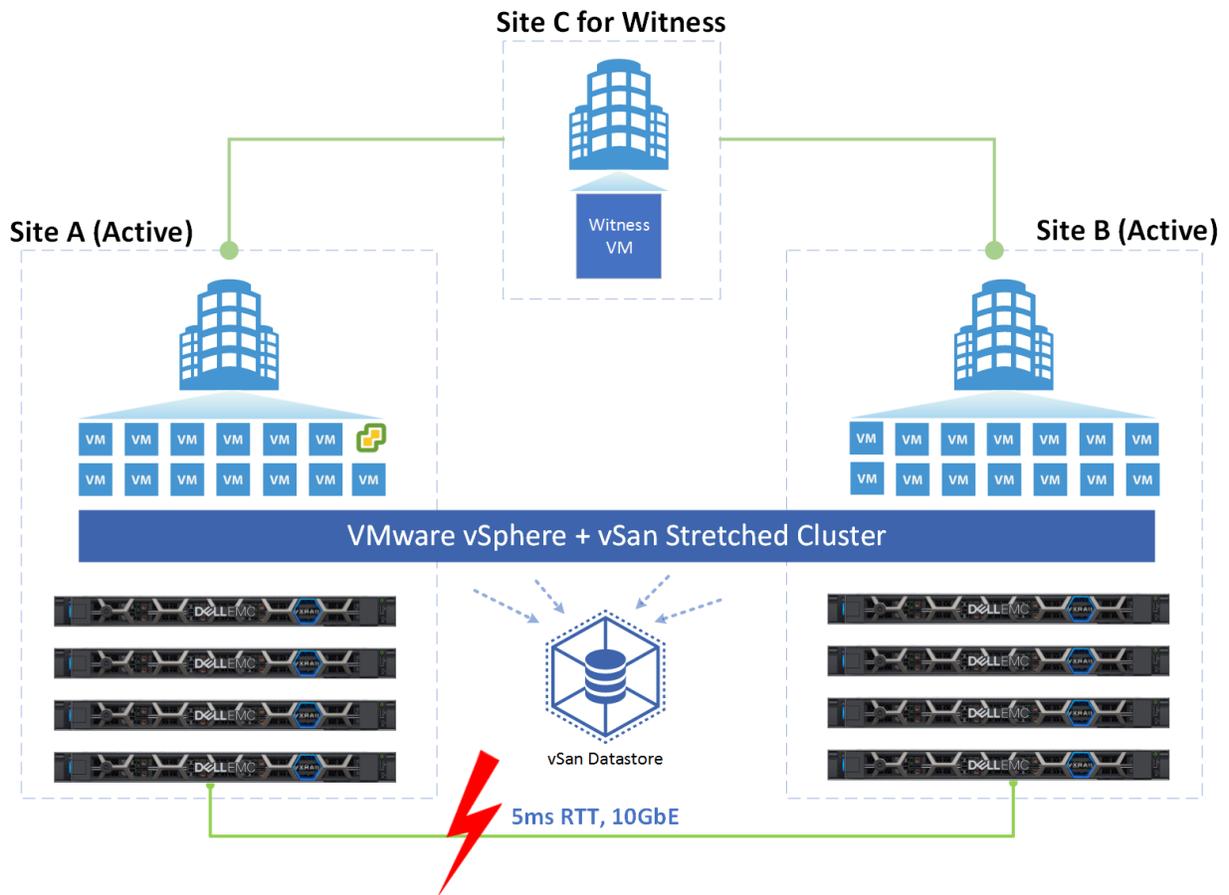

Figure 6 - The vSAN network is disconnected between site A and B

Figure 7 shows that the vSAN network is disconnected between sites A & B and the witness network is disconnected between site A & C. If the vSAN network is disconnected between both data sites and witness network is disconnected between site A & C, all virtual machines on VxRail of secondary site will trigger VMware High Availability (HA). It then restarts all virtual machines automatically on VxRail at the preferred site. The virtual machines on VxRail of the preferred site will remain running at site A.
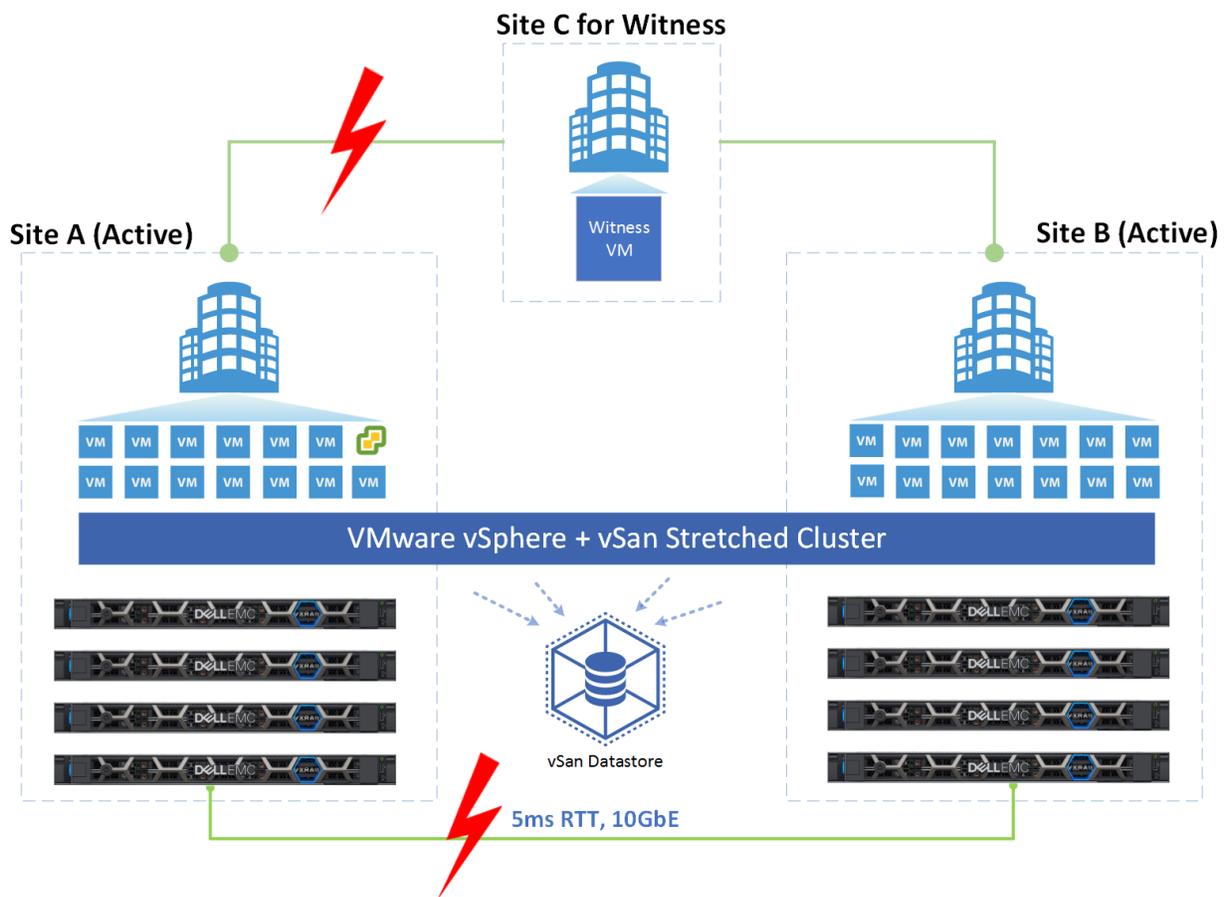
Figure 7 - The vSAN network is disconnected between site A and B, and the witness network is disconnected between site A and C.

Planned Failback

Figure 8 shows that the virtual machines online move to site A from site B. If site A is recovered, the system administrator can perform the VMware vMotion to online move the virtual machines running on VxRail at site B to site A and service of virtual machines are not interrupted.
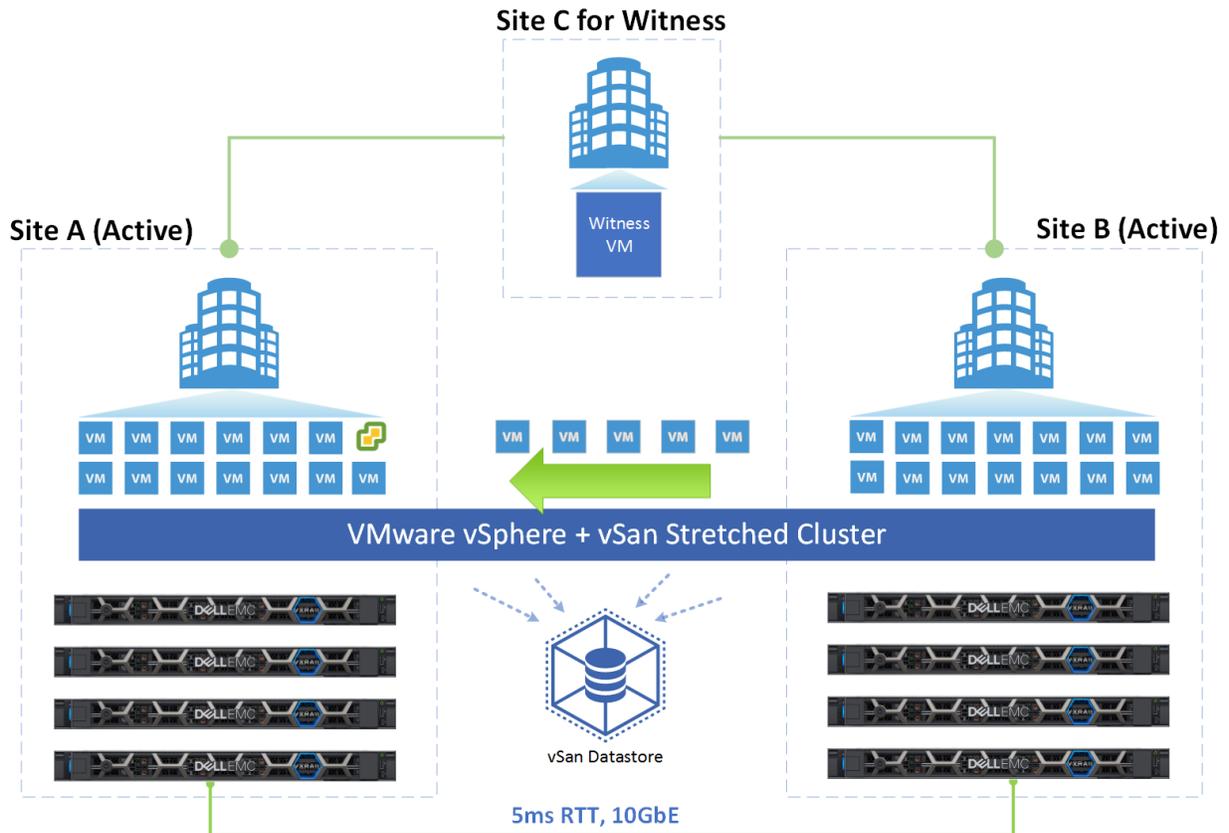

Figure 8 - The virtual machines online move to site A from site B

Benefits

VxRail vSAN stretcher cluster can provide site-level protection with zero data loss and near instantaneous recovery. It can also offer redundancy protection locally and across sites. The virtual machines can be automated to failover in vSAN stretcher cluster in case of site failures. VxRail vSAN stretcher cluster is an Active-Active infrastructure solution. The system administrator doesn't perform a lot of manual operation tasks in case of site failures and maintenance windows, minimizing their daily operational tasks.

Using Storage Based Policy Management (SBPM), the system administrator can create VM policies that assign storage characteristics (e.g. mirroring, RAID-5/6) to individual virtual machine virtual disks (VMDK). VM Storage Policies can easily be changed and/or reassigned if application requirements change. These changes are performed with no downtime and without any storage migration.

For VxRail scaling, new VxRail appliances can be added non-disruptively and **different models** can be mixed within a VxRail cluster. For node upgrade, each node can upgrade or add memory, network adapters, cache drives, and capacity drives.

For VxRail upgrade, **a single software package** can complete the upgrade process. The software upgrade package includes VMware vCenter Server Appliance, vSphere hypervisor and all relevant hardware components. Verification of hardware compatibility lists is not needed, because the software upgrade package is pre-tested and validated by Dell EMC and VMware.

Active-Active-Passive (AAP) Infrastructure

Overview

VxRail can also be integrated with additional software, leveraging your existing investment, e.g. with VMware Site Recovery Manager (SRM) and vSphere Replication (VR) to extend site level protection to many other sites. If vSAN stretched cluster was deployed to protect the data between two separate sites, SRM could help to extend the site level protection to the other sites.

Architecture

Figure 9 shows a high-level overview of the sample Active-Active-Passive infrastructure environment in this scenario.
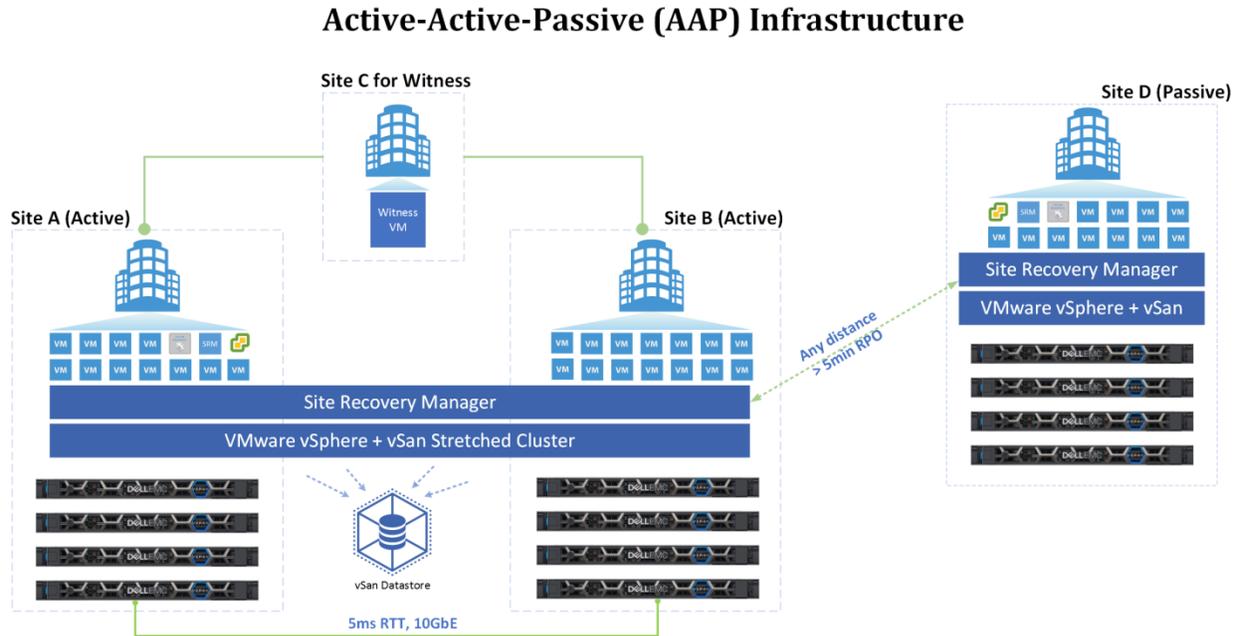

Figure 9 - Architecture Diagram of VMware vSAN Stretched Cluster with SRM

The Active-Active-Passive infrastructure environment consists of the following:

In site A and B

- Four VxRail E560 appliances are running as data node at site A.
- Four VxRail E560 appliances are running as data node at site B.
- A vSAN stretched cluster (4+4+1) is deployed across site A and B.
- A vCenter server appliance that is installed outside of VxRail cluster manages the vSAN stretched cluster.
- VxRail Manager 4.5 manages and monitors all VxRail E560 across site A and B.
- A Site Recovery Manager (SRM) installed at the protected site (Site A and B). It can be installed on a dedicated windows server virtual machine.
- A vSphere Replication (VR) virtual appliance installed at the protected site (Site A and B).

In site C

- A vSAN witness virtual machine is deployed that monitors all vSAN data nodes across site A and B.

In site D

- Four VxRail E560 appliances are running as data node at site D.
- A vCenter server appliance installed outside of VxRail   the vSAN cluster.
- VxRail Manager 4.5 manages and monitors all VxRail E560 at site D.
- A Site Recovery Manager (SRM) installed at the recovery site (Site D) can be installed on a dedicated windows server virtual machine.
- A vSphere Replication (VR) virtual appliance installed at the recovery site (Site D).

Requirements

In the section "Active-Active Infrastructure", we described the requirements to deploy VMware vSAN stretched clusters. You can refer to that section for the requirements of vSAN stretched cluster. In this section, we describe the requirements for deploying the Site Recovery Manager on vSAN stretched cluster.

VxRail Requirements

Refer to the section "Active-Active Infrastructure".

vCenter Server Requirements

Refer to the section "Active-Active Infrastructure".

Site Recovery Manager and vSphere Replication Requirements

VMware vSphere Replication is a 64-bit virtual appliance. It must deploy in a vCenter Server environment by using the OVF deployment wizard on a vSphere host. vSphere Replication requires a dual-core or quad-core CPU, a 13 GB and a 9 GB hard disk, and 8 GB memory. Additional vSphere Replication servers require 716 MB memory.

Site Recovery Manager requires a vCenter Server instance of the appropriate version at both protected site and recovery site. Requirements of SRM installation are:

- Install the same version of Platform Services Controller (PSC), vCenter Server, vSphere Replication and Site Recovery Manager on protected site and recovery site.
- Make use of Fully Qualified Domain Names (FQDN) rather than IP addresses when you install and configure Platform Services Controller, vCenter Server, vSphere Replication and Site Recovery Manager. Make Forward and Reverse DNS records for all the components.
- Make use of centralized Network Time Protocol (NTP) servers to synchronize the clock settings of the systems on all components.

- Site Recovery Manager requires a database. SRM can be installed either with Embedded vPostgres Database or an external database source such as Microsoft SQL or Oracle.
- Obtain a Windows user account with the appropriate privileges to install and run SRM service.
- Obtain the vCenter Single Sign-On administrator username and password for both the protected site and recovery site.

vSphere Replication Network Requirements

It is recommended to determine storage and network bandwidth requirements in order to replicate virtual machines efficiently. Network bandwidth requirements increase if all storage is network-based because data operations between the host and the storage also require the network resource.

Day 2 Operations

This section describes some operations of VMware Site Recovery Manager (SRM) and vSphere Replication (VR) in a VxRail vSAN stretched cluster.

Planned Migration

If the virtual machines of the protected site (Site A and B) require the planned migration into the recovery site (Site D), the system administrator can arrange the maintenance window and offline move all virtual machines into the recovery site (Figure 10). They can execute the SRM recovery plan to complete this migration process. The SRM recovery plan will attempt to gracefully shut down the protected virtual machines in protected site then power on in recovery site. Finally, the system administrator can run "reprotect" to make the recovery site the protected site.
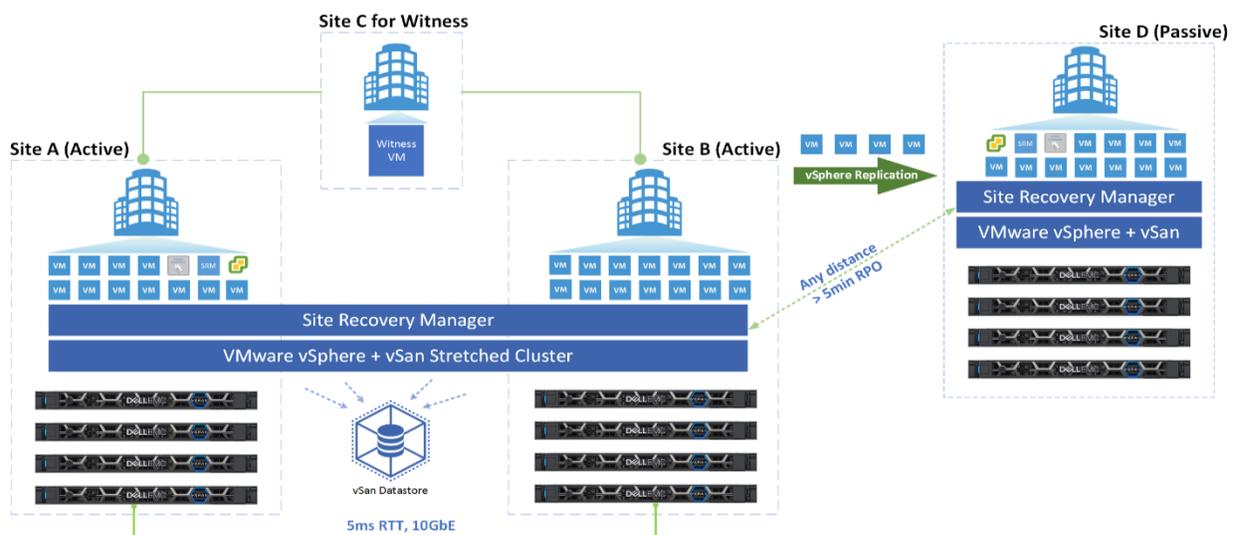

Figure 10 – The virtual machines are replicated to site D from the protected site (A + B)

Disaster Recovery

If the protected site (Site A and B) faulted, all the virtual machines on VxRail vSAN stretched cluster will not respond. The system administrator can then execute the SRM recovery plan (Figure 11). Site Recovery Manager restores virtual machines on the recovery site to their most recent available state according to the recovery point objective (RPO). Finally, the system administrator can run "reprotect" to make the recovery site the protected site.
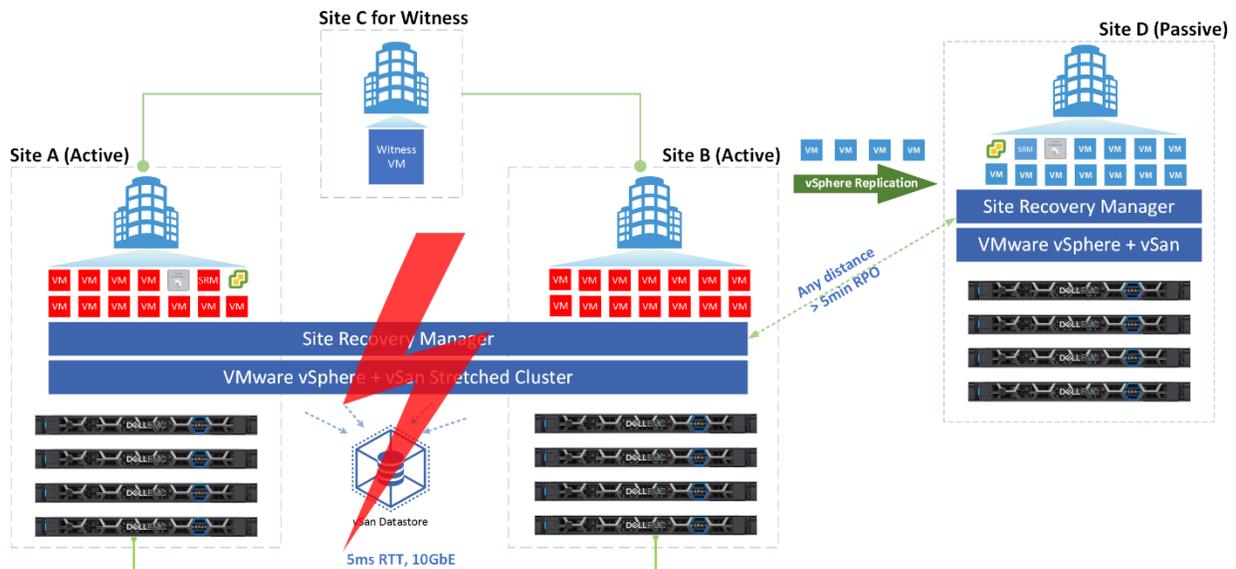

Figure 11 – All of the VxRail appliances faulted at site A and site B

Planned Failback

If the protected site (Site A and B) is recovered, the system administrator can perform a failback recovery plan to restore the original configuration of the protected and recovery sites (Figure 12). The virtual machines of recovery site (Site D) will move to the protected site (Site A and B). Finally, Site A and B will change to the protected site and Site D changes to the recovery site.
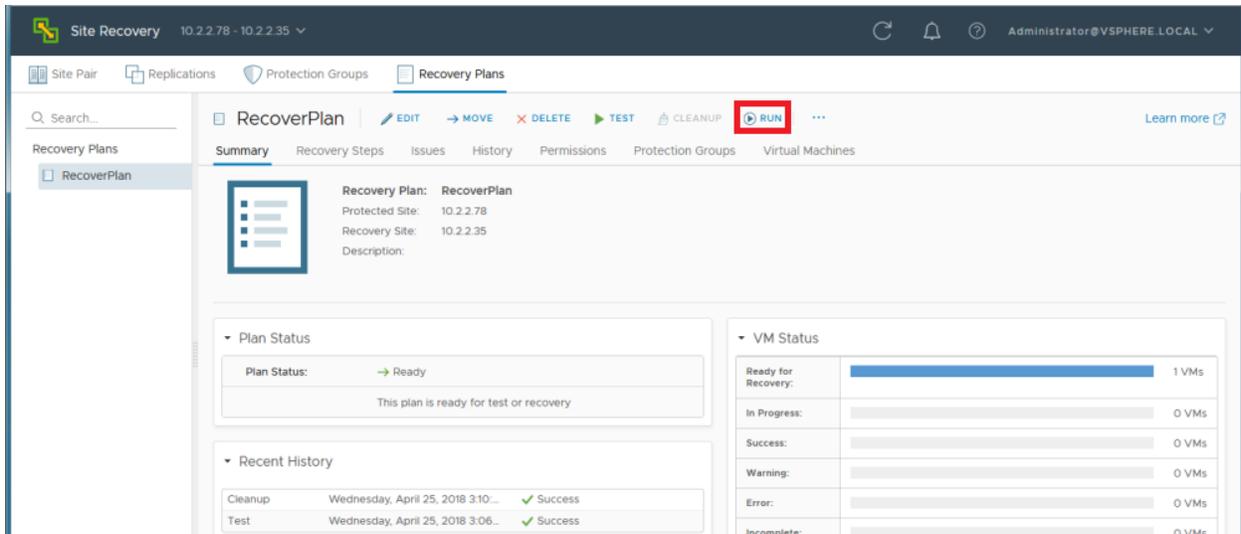
Figure 12 – Run Recovery Plan Icon

Benefits

Site Recovery Manager provides automated orchestration and non-disruptive testing of disaster recovery plans for all virtualized applications. It reduces the recovery time of systems and improves the success of DR recovery. vSAN Stretched clusters offer the ability to balance workloads between two data centers and provides site-level protection with zero data loss and near instantaneous recovery. The features of SRM and vSAN stretched cluster differ. Table 5 shows the coverage map of SRM and vSAN stretched cluster.

Table 5 - Coverage Map of VxRail stretched cluster and Site Recovery Manager

	Site Recovery Manager	vSAN Stretched Cluster
Disaster Recovery	100%	25%
Downtime Avoidance	25%	75%
Disaster Avoidance	75%	50%
Active Site Balancing	50%	100%

Point-in-time Recovery (PITR) Solution

Overview

RecoverPoint for Virtual Machines can protect virtual machines with automated provisioning for disaster and operational recovery with VM-level granularity. System administrators can easily protect and replicate virtual machines with continuous replication for any point in time recovery. It provides local and remote replication over any distance between VxRail Appliances with synchronous or asynchronous replication. It also enables the system administrators to use RecoverPoint features such as point-in-time access, failover, and testing.

Architecture

Figure 10 shows a high-level overview of the RecoverPoint for Virtual Machines (VMs) on VxRail Appliances between site A and site D.
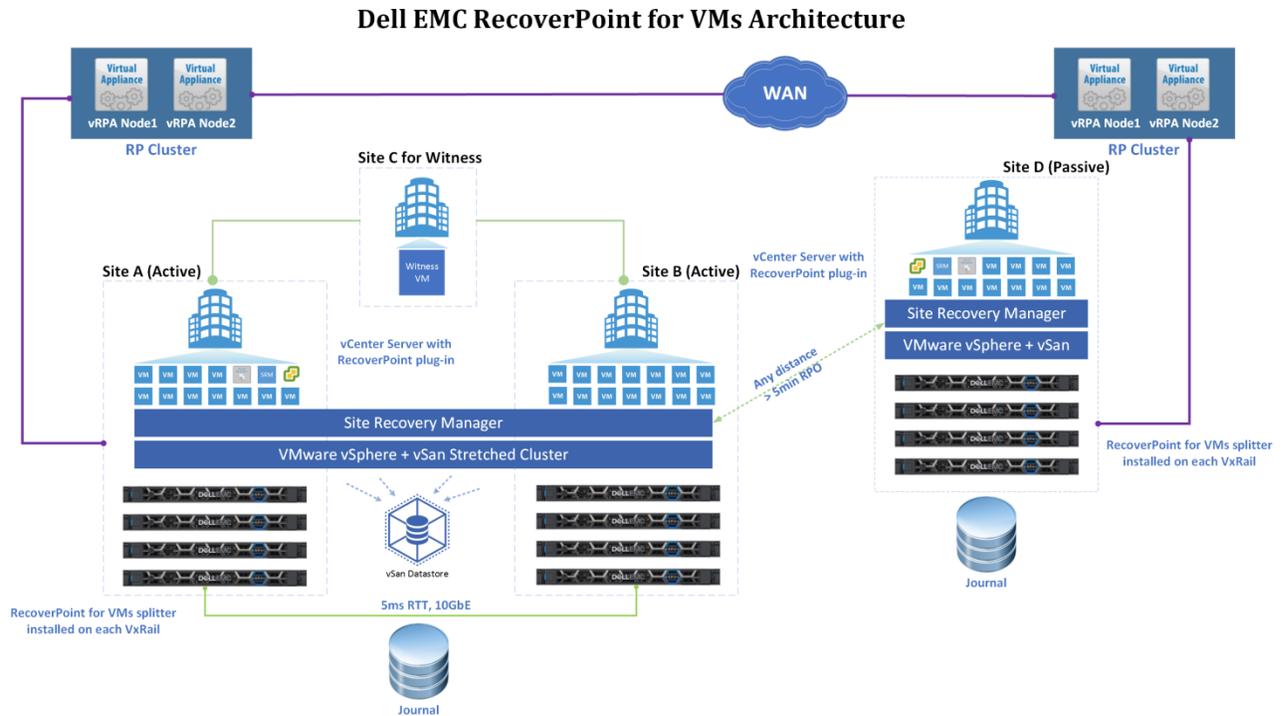
Figure 13 - RecoverPoint for VMs Architecture

The RecoverPoint for Virtual Machines environment consists of the following:

In site A

- One of the Virtual RecoverPoint appliance (vRPA) clusters contain two Virtual RecoverPoint appliances. This cluster manages all of the data replications.
- The RecoverPoint write-splitter is installed on each VxRail Appliance, enabling replication from any source storage to target storage.
- The journal volume stores the protected virtual machines. We can recover the virtual machine from this journal volume.
- RecoverPoint plug-in is enabled with the vCenter server for managing VM replication.

In site D

- One of the vRPA clusters contains two vRPAs. This cluster manages all data replication.
- The RecoverPoint write-splitter is installed on each VxRail Appliance, enabling replication from any source storage to target storage.
- The journal volume stores the protected virtual machines. We can recover the virtual machine from this journal volume.
- RecoverPoint plug-in is enabled with the vCenter server for managing VM replication.

Requirements

This section describes the requirements to deploy vRPA cluster in a VxRail Cluster.

VxRail Requirements

Table 6 shows the compatibility for VxRail and RecoverPoint for VMs.

Table 6 - Compatibility table for VxRail and RecoverPoint for VMs

Hyper-Converged Infrastructure Appliance	VMware vSAN version	RecoverPoint for VMs
VxRail 4.5.215	VMware vSAN 6.6.1 Update 2	5.2.0.2
VxRail 4.5.210	VMware vSAN 6.6.1	5.2.0.2
VxRail 4.5.200	VMware vSAN 6.6.1	5.2.0.2
VxRail 4.5.150	VMware vSAN 6.6.1	5.2.0.2

vRPA Requirements

Different options can be chosen for vRPA profile during vRPA deployment. Table 7 shows the requirements for each option.

Table 7 - Options for choosing the vRPA profile

Configuration	Memory	CPU Resources	Disk Space
Bronze	4GB	2 x CPUs	35GB VMDK capacity
Bronze+	8GB	2 x CPUs	35GB VMDK capacity
Sliver	8GB	4 x CPUs	35GB VMDK capacity
Gold	8GB	8 x CPUs	35GB VMDK capacity

Remark: A vRPA cluster can support up to eight vRPAs.

Network Requirements

RecoverPoint for VMs supports LAN, WAN, and data interfaces distributed across multiple network adapters or combined into one. While deploying vRPA, we need to define three virtual network configurations (LAN, WAN and Data). The option depends on the requirements for high availability and performance. Table 8 shows all options for network configuration.

**Table 8 - The options for three virtual network configuration**

Network Adapter 1	Network Adapter 2	Network Adapter 3	Network Adapter 4	Number of IP addresses	Performance	High Availability
LAN, WAN and Data				1	Not suggested	No
LAN, WAN	Data			2	Better	Yes
WAN	LAN, Data			2	Better	Yes
LAN	WAN	Data		3	Better	Yes
LAN	WAN	Data 1	Data 2	4	Best	Yes

Day Two Operations

This section describes some operations of RecoverPoint for VMs in a VxRail Cluster.

Protect the virtual machines

The system administrator can create virtual machine protection with the vCenter server. Figure 14 shows the virtual machines protection wizard. Either local or remote protection of virtual machines between VxRail Appliances with synchronous or asynchronous replication can be configured.
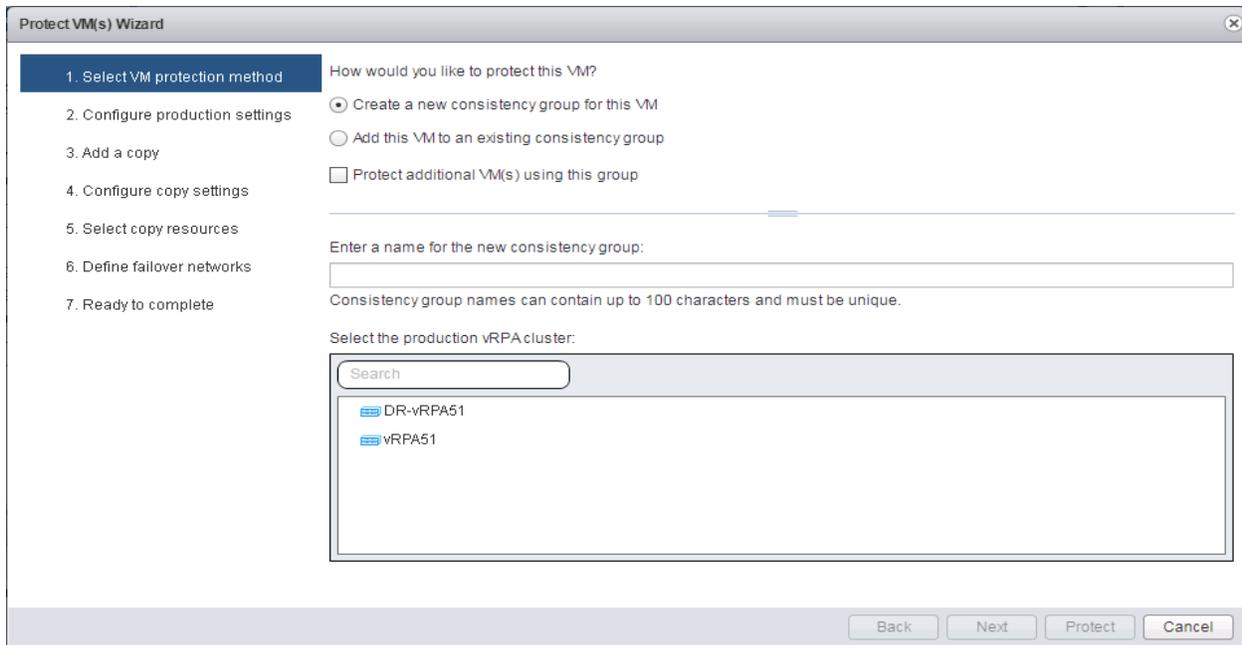
Figure 14 - The protection wizard of virtual machines

A Recovery Point Objective (RPO) setting can be defined for each virtual machine protection. The default RPO setting is 25 seconds (Figure 15).

Figure 15 – The PRO and Replicate Mode settings in protection wizard

Test the Copy VM

If the virtual machine is protected with RecoverPoint for VMs, the system administrator can test the Copy VM in any time. Simply click the following red icon to open the Test a Copy Wizard in the RecoverPoint for VMs Management (Figure 16).
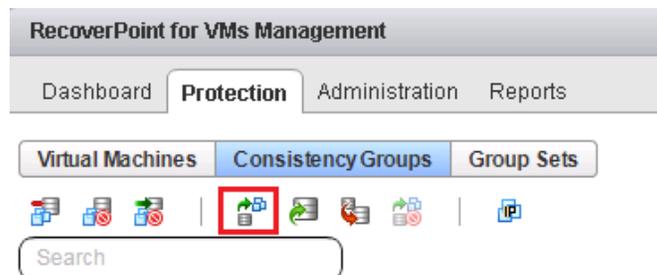
Figure 16 - Test a Copy Icon

The system administrator can select the last snapshot or a specific point in time copy of virtual machine to test the copy. To avoid IP conflicts between the production VMs and copy VMs, there are four options for defining the test network. Figure 17 shows the four options for specifying the test network. They are defined as follow:

- Create an isolated network for each consistency group.
  Automatically creates an isolated network for virtual machines in this group or group set to avoid IP conflicts between the production VM and the tested virtual machine.
- Create an isolated network for each ESX.
  Automatically creates an isolated network for each ESX splitter.
- Use my dedicated network.
  We manually select a pre-configured network. Not relevant for group sets.
- Use a preconfigured failover networks.
  We use the pre-configured failover networks for each copy VM. Not relevant for group sets.
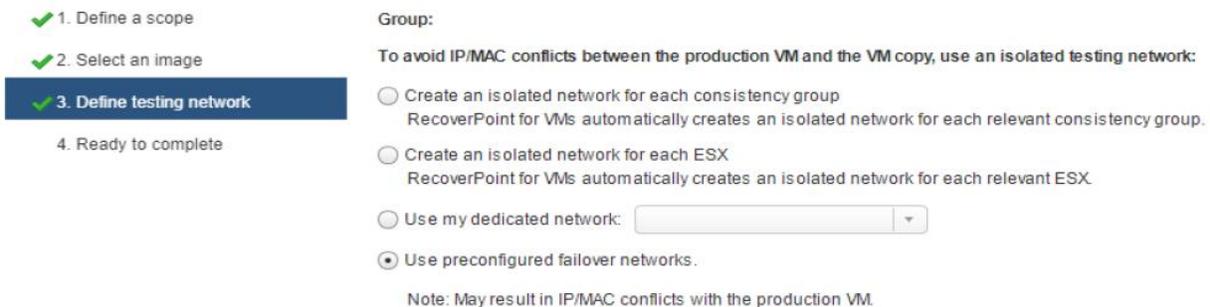
Figure 17 - Define testing network in test a copy wizard.

Recover the virtual machines

If the production virtual machine is corrupted in VxRail cluster, the system administrator can recover the production VMs by the previous point-in-time copy into local VxRail cluster or remote VxRail cluster. Just click the following red icon to open the Recover Production Wizard in the RecoverPoint for VMs Management (Figure 18).
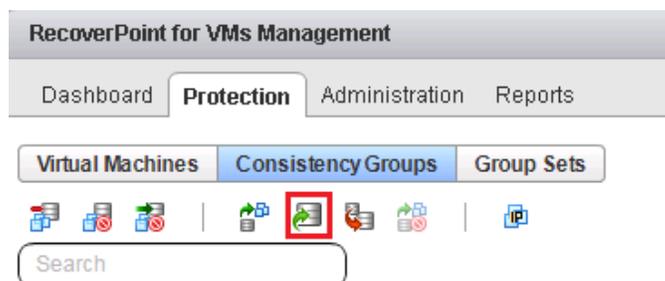

Figure 18 – Recover Production Icon

We suggest testing the Copy VM in an isolated network before recovering the production virtual machines and make sure the Copy VM is running in the health status. The production virtual machine can be recovered from all point-in-time copies on the image menu (Figure 19).

Figure 19 – All point-in-time copies on image menu

Benefits

If planning to deploy the Continuous Data Protection (CDP) solution or Disaster Recovery (DR) solution with any point in time recovery, RecoverPoint for VMs is a good solution. It provides the following core capabilities:

- Fully integrated management with the VMware vSphere Web Client.
- Recovery Operation with any point-in-time (failover, failback and recover to the production virtual machines).
- It is a "No Single Point" of Failure solution.
- Supports VMware vMotion and Storage vMotion.
- Multi-copy replication (one-to-many simultaneous replications).
- Multi-VM Consistency Groups.
- Supports asynchronous and synchronous replication.

- Provides local replication and remote replication across different sites.
- Supports different storage topologies, i.e. SAN, NAS, iSCSI, FCoE, vSAN, etc.
- Supports transparent addition and removal of VMDK and VM from a Consistency Group.
- Supports dynamic switching between asynchronous and synchronous replication.
- Built-in WAN bandwidth supports compression and de-duplication.
- VMware vSphere Hypervisor Based ESXi Splitter.

Summary

This article described how to plan and build the Active-Active Infrastructure, Active-Active-Passive Infrastructure, and Point-in-time Recovery Solution on VxRail Appliance. We have discussed what hyper-converged infrastructure is, the benefits of the VxRail Appliance, and how to build both availability solution and continuous data protection (CDP) solution on VxRail.

Each section of this article examined the main benefits and how to help customers maximize value from VxRail Appliances.

Table 9 shows the summary of each solution feature on VxRail.

Table 9 - Summary of each solution feature on VxRail

Solutions on VxRail	Active-Active Availability	Disaster Recovery	Data protection for multiple sites	Continuous data protection for multiple sites
vSAN Stretched Cluster	Supported	Supported		
vSAN Stretched Cluster + SRM	Supported	Supported	Supported	
vSAN Stretched Cluster + RecoverPoint for VMs	Supported	Supported	Supported	Supported

Bibliography

Dell EMC VxRail Appliance TechBook

https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/h15104-vxrail-appliance-techbook.pdf

Dell EMC VxRail vSAN Stretched Clusters Planning Guide

https://www.dellemc.com/resources/en-us/asset/white-papers/products/converged-infrastructure/h15275-vxrail-planning-guide-virtual-san-stretched-cluster.pdf

Introduction to Stretched Clusters

https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-1BDC7194-67A7-4E7C-BF3A-3A0A32AEECA9.html

Understanding Storage Policy-Based Management

https://blogs.vmware.com/virtualblocks/2017/01/16/understanding-storage-policy-based-management/

Administrator's Guide - Dell EMC RecoverPoint for Virtual Machines

https://www.emc.com/collateral/TechnicalDocument/docu85469.pdf

Installation and Deployment Guide - Dell EMC RecoverPoint for Virtual Machines

https://www.emc.com/collateral/TechnicalDocument/docu85417.pdf

Stretched Clusters & VMware Site Recovery Manager

https://storagehub.vmware.com/t/site-recovery-manager-3/stretched-clusters-vmware-site-recovery-manager/

VMware Site Recovery Manager Installation and Configuration

https://docs.vmware.com/en/Site-Recovery-Manager/8.1/srm-install-config-8-1.pdf

SRM 8.1 Technical Overview

https://storagehub.vmware.com/t/site-recovery-manager-3/srm-8-1-technical-overview/

vSphere Replication Administration

https://docs.vmware.com/en/vSphere-Replication/8.1/vsphere-replication-81-admin.pdf

vSphere Replication™ 6.5 Technical Overview

https://storagehub.vmware.com/t/site-recovery-manager-3/vsphere-r-replication-tm-6-5-technical-overview-1/

White Paper - Deploy RecoverPoint for Virtual Machines Version 5.2 with VxRail