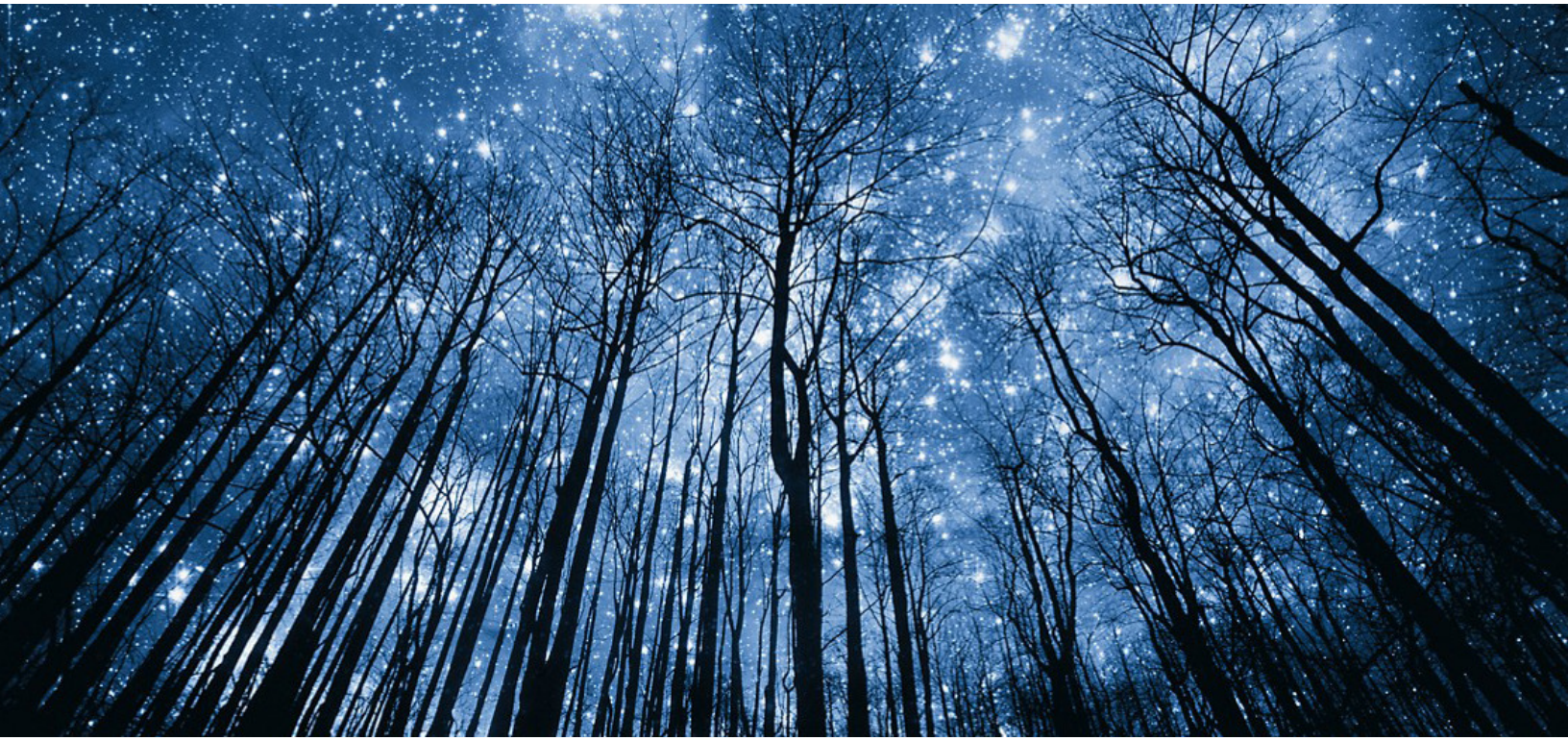
DELL Technologies

CYBER RESILIENT FOR THE MODERN DATA CENTER



Victor Wu

Senior Solution Expert, Business Consultation
BoardWare Information System Limited

DELL Technologies
Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across Dell's multiple technologies and products with both skill and outcome-based certifications.

Proven Professional exams cover concepts and principles which enable professionals working in or looking to begin a career in IT. With training and certifications aligned to the rapidly changing IT landscape, learners can take full advantage of the essential skills and knowledge required to drive better business performance and foster more productive teams.

Proven Professional certifications include skills and solutions such as:

- Data Protection
- Converged and Hyperconverged Infrastructure
- Cloud and Elastic Cloud
- Networking
- Security
- Servers
- Storage
- …and so much more.

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Table of Contents

Preface

In the digital economy, the service of mission-critical applications cannot be disrupted because it may impact organization's service. How can it operate as an "always-on" enterprise? How can it ensure that data is safe, and compliance goals are met? By delivering 24/7 data, high availability, and accelerating backup and recovery.

A data backup and recovery solution are critical for all mission-critical applications. A System Architect needs to know how to design Business Continuity and Disaster Recovery (BCDR) solutions for all mission-critical applications. Then, how can the business prevent Ransomware attacks? Many factors are considered for the BCDR solution and its architectural design.

Most of the elements are:

- Recovery Point Objective (PPO) - The point in time to which system's data must be recovered after an outage.
- Recovery Time Objective (RTO) - The amount of time within which a system must be recovered after an outage.
- Business requirements and constraints
- System platform being used (e.g., Microsoft Windows, Red Hat Enterprise Linux, VMware vSphere, etc.)
- Business Continuity and Disaster Recovery approach
- Process to ensure data is safe and compliance goals are met
- Process to prevent ransomware attacks
- A solution which supports immutable backup (i.e., Write Once Read Many (WORM) feature).
- A data recovery solution which supports multi-platforms (e.g., physical platform, virtual platform, or Kubernetes)

Introduction

This technical article provides information on multi-tier Business Continuity and Disaster Recovery (BCDR). It will consider how to plan and design a cyber-resilient architecture for data recovery across three separate locations and it will discuss the high-level and low-level design of this data recovery solution. This cyber-resilient architecture includes software-defined storage (SDS), unified backup and recovery software, and backup hardware appliances. In the design phase of this cyber-resilient architecture, it will consider:

- The Datacenter allocation requirement - Design how to allocate the servers and network equipment into each data center for cyber-resilient architecture.
- The Business Continuity and Disaster Recovery design - Plan and design cyber-resilient architecture.
- Active-Active-Passive data center design - Plan and design the hyper-converged infrastructure architecture for Active-Active-Passive (AAP) solution across three separate data centers.
- The system integration of bo th BCDR and hyper-converged infrastructure.

- The automation flow of Business Continuity and Disaster Recovery when the data recovery service is faulty in a primary data center.
- The failure scenarios for different data centers - List the business/application service status based on different failure scenarios across each data center.
- Scale-up and scale-out cyber-resilient architecture - Plan and design the data recovery service components (e.g., data repository) allocated between the different data centers.

Architecture

In this section, we will go over the architecture of cyber resilient for the modern data center. Figure 1 is the high-level hardware diagram for this solution, including the core hardware components and data center location. This solution includes three core architectures, **VxRail vSAN Stretched Cluster**, **Business Continuity and Disaster Recovery**, and **Data Recovery Methodology** for allowing an entire site failure to be tolerated or the primary backup data to be corrupted.

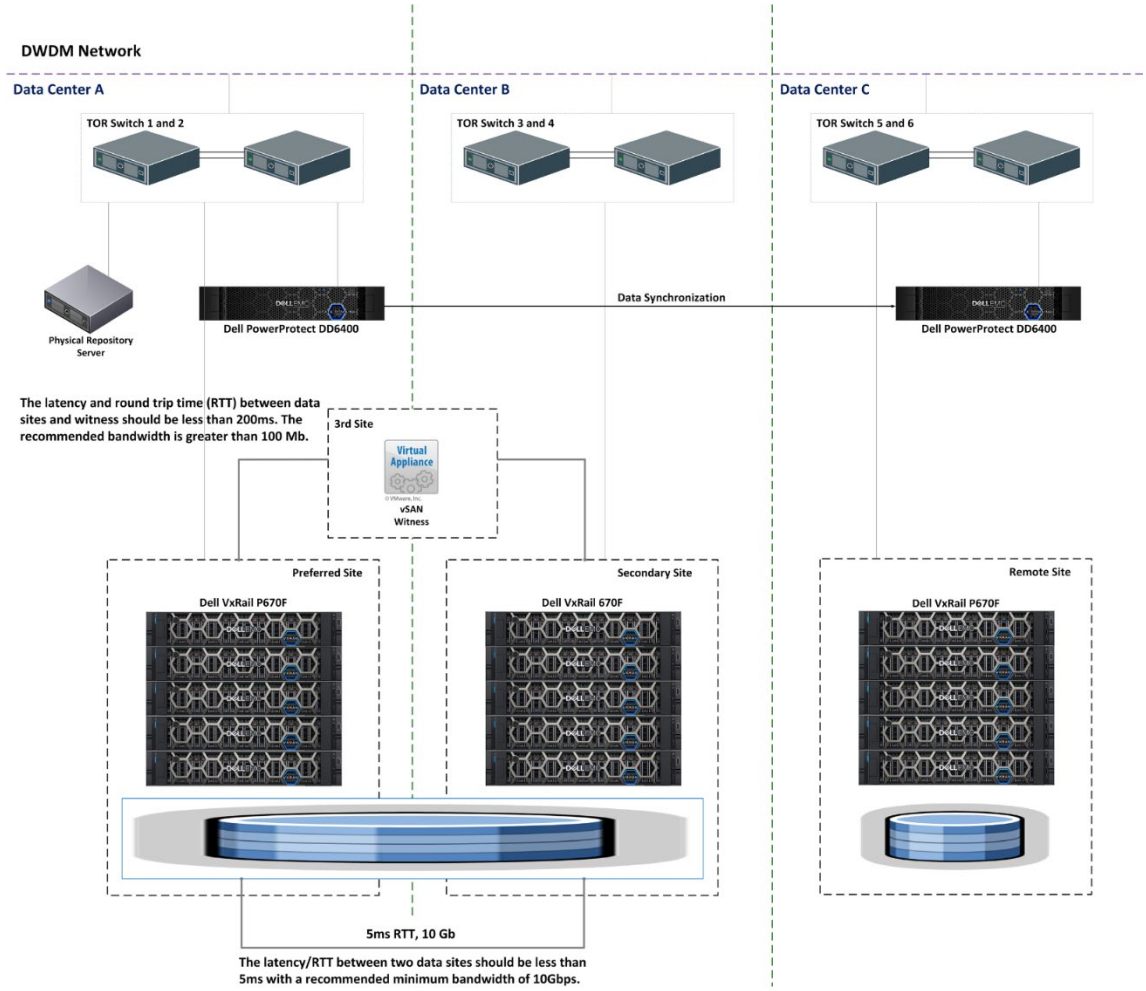


Figure 1 - The architecture of cyber resilient for modern data center

Figure 1 shows three separate data centers (Data Center A/B/C). The Dense Wavelength Division Multiplexing (DWDM) technology is enabled across these three data centers. DWNM technology is used to increase the bandwidth of existing fiber networks, combining the data signals from various

sources over a pair of optical fibers. Two 10Gb network switches are used to connect the Hyper-Converged Infrastructure (HCI) platform and data protection appliance in each data center. Two Dell PowerProtect DD6400 systems are used for primary and secondary backup for this environment.

Table 1 shows the hardware inventory in Figure 1.

Locations	Equipment	Description
Data Center A	2 x 10Gb Network Switch	The TOR Switches are used for the Hyper-Converged Infrastructure platform and data protection appliance in Data Center A.
	5 x Dell VxRail P670F	The VxRail P670F are primary nodes on the VxRail Stretched cluster.
	1 x Dell PowerProtect DD6400	Data Backup Appliance includes a data deduplication feature.
	1 x Dell PowerEdge R750 Server	Veeam Physical Repository Server is used to restore virtual machine's backup data.
Data Center B	2 x 10Gb Network Switch	The TOR Switches are used for the Hyper-Converged Infrastructure platform and data protection appliance in Data Center B.
	5 x Dell VxRail P670F	The VxRail P670F are secondary nodes on the VxRail Stretched cluster.
Data Center C	2 x 10Gb Network Switch	The TOR Switches are used for the Hyper-Converged Infrastructure platform and data protection appliance in Data Center C.
	5 x Dell VxRail P670	The VxRail P670F are standby nodes in Data Center C.
	1 x Dell PowerProtect DD6400	Data Backup Appliance includes a data deduplication feature.

Table 1 - The hardware inventory of cyber resilient for modern data center

Now, let us look at the core software components in each data center.

Figure 2 is the high-level logical diagram of this solution, including the core software management and application tools, including VMware vCenter Server, VxRail Manager, Veeam Backup & Replication Server, VMware Site Recovery Manager, and vSphere Replication.

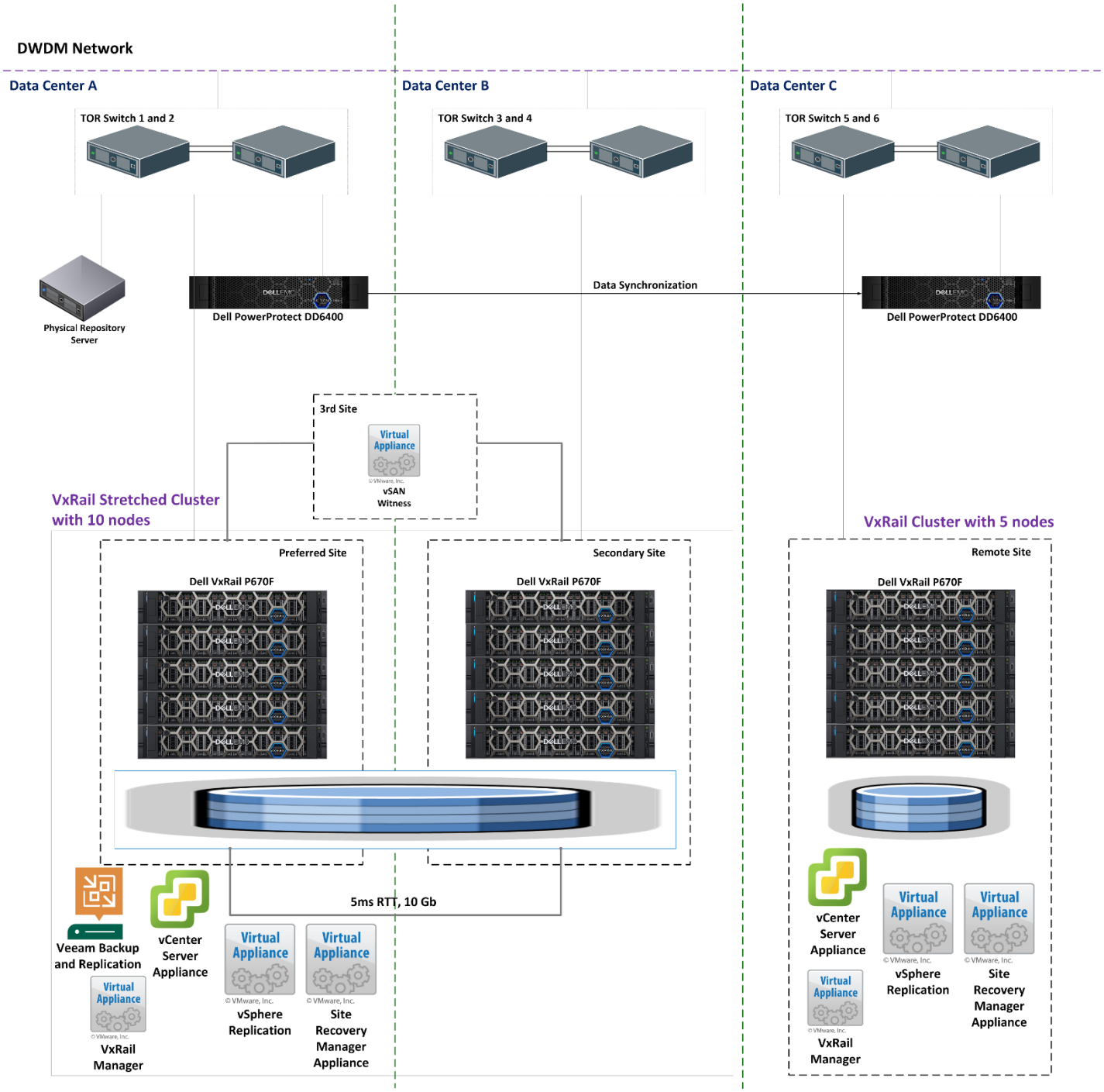


Figure 2 - The high-level logical diagram of cyber resilient for modern data center

Table 2 shows each data center's core application and data recovery components. The VxRail vSAN Stretched Cluster with ten VxRail P670F nodes is enabled across Data Center A and B. The VxRail Standard cluster with five VxRail P670F nodes at Data Center C. An Veeam Backup and Replication server is running at Data Center A and backup all the virtual machines allocated on the vSAN Stretched Cluster across Data Center A, and B. VMware Site Recovery Manager and vSphere Replication are the core components of Business Continuity and Disaster Recovery.

Locations	Core Components	Description
Data Center A	Veeam Backup and Replication Server	The management plane of Veeam Backup and Replication Server v11. It is used to manage the backup tasks of virtual machines at Data Center A.
	vCenter Server Appliance	The management plane of VxRail Manager and virtual machines at Data Center A.
	VxRail Manager	The virtual appliance manages and controls all of the operational tasks for the VxRail vSAN Stretched Cluster. And VxRail plugin for vCenter is enabled with VMware vCenter Server, and we can handle all operational tasks of VxRail via the vCenter Server.
	vSphere Replication	The virtual appliance manages the virtual machine's replication session in either a single site or across two sites with 5 minutes RPO (minimum RPO).
	Site Recovery Manager Appliance	The virtual appliance manages the recovery plan of virtual machines with either virtual machine replication or storage-based replication across two sites.
Data Center C	vCenter Server Appliance	The management plane of VxRail Manager and virtual machines at Data Center C.
	VxRail Manager	The virtual appliance manages and controls all of the operational tasks for the VxRail Standard cluster. And VxRail plugin for vCenter is enabled with VMware vCenter Server, and we can handle all operational tasks of VxRail via the vCenter Server.
	vSphere Replication	The virtual appliance manages the virtual machine replication session in either a single site or across two sites with 5 minutes RPO (minimum RPO).
	Site Recovery Manager Appliance	The virtual appliance manages the recovery plan of virtual machines with either virtual machine replication or storage-based replication across two sites.
3rd Site	vSAN Witness Appliance	The virtual appliance creates the majority vote to prevent a split-brain scenario.

Table 2 - The host inventory list in Figure 2

We will discuss the overview of three core architectures in the next section.

VxRail vSAN Stretched Cluster

Stretched Cluster is an advanced solution on the VxRail platform. This solution can provide the active-active Data Center across two separate locations. The stretched cluster uses fault domain technologies to provide redundancy and failure protection across sites. It requires three fault domains, including the preferred site, secondary site, and witness site.

Figure 3 is the high-level logical diagram of Stretched Cluster on VxRail, and there are five VxRail P670F All-Flash nodes on the Preferred (Data Center A) and Secondary (Data Center B) Sites. The virtual machines can be moved into the standby VxRail nodes in the Stretched Cluster if one of the sites is faulted. The witness virtual appliance must be allocated to the 3rd site. This architecture can provide a high-performance and active-active Data Center solution across two separate locations.

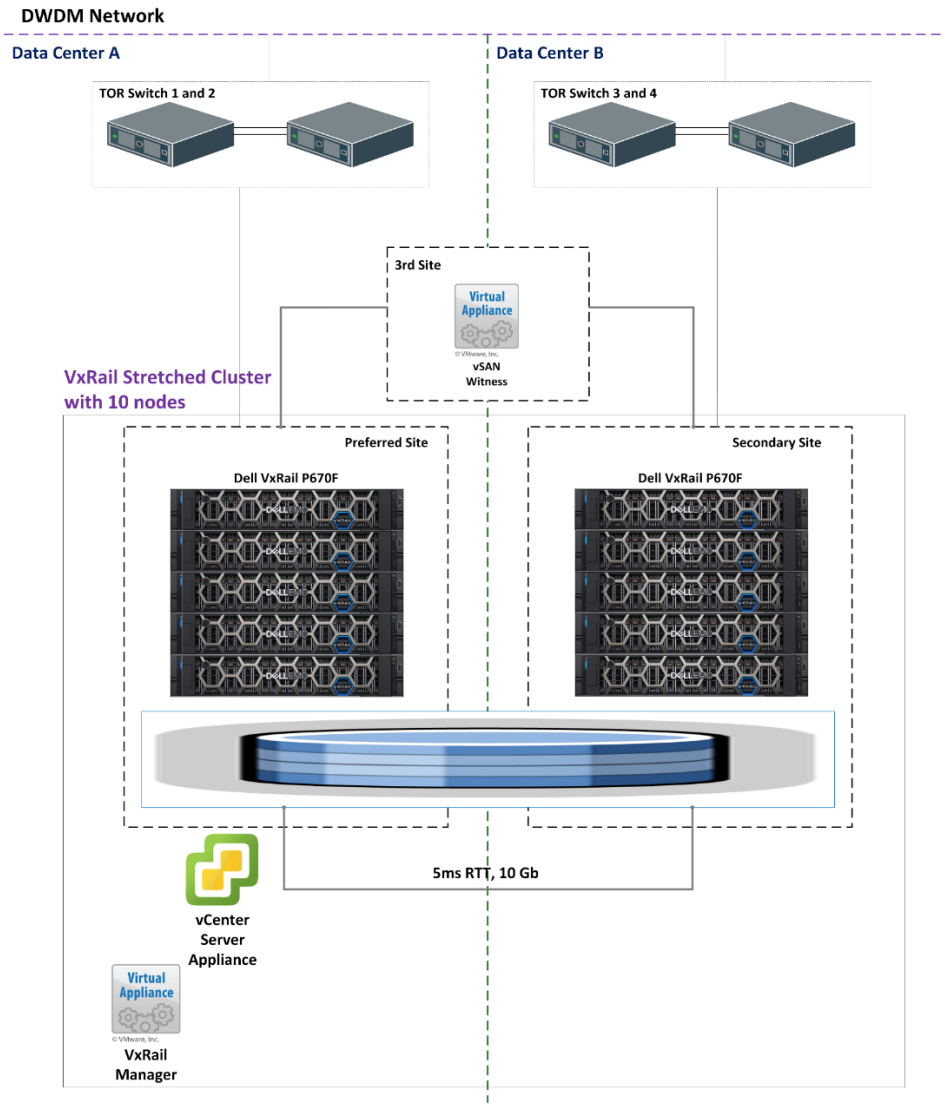


Figure 3 - logical architecture diagram of the VxRail vSAN Stretched Cluster

Business Continuity and Disaster Recovery

Now, let's take a look at the architecture of BCDR. Figure 4 shows the logical architecture diagram of VMware Site Recovery Manager. There is one Site Recovery Manager Appliance and one vSphere Replication Appliance installed at each primary site (Data Center A/B) and secondary site (Data Center C). All protected virtual machines can be recovered automatically into the remote hosts (VxRail Standard Cluster) at Data Center C if both Data Center A and B are down. In this solution, the Veeam Backup and Replication virtual machine must be protected with Site Recovery Manager and then it can be recovered into Data Center C if either the Veeam Backup and Replication is corrupted, or the site fails.

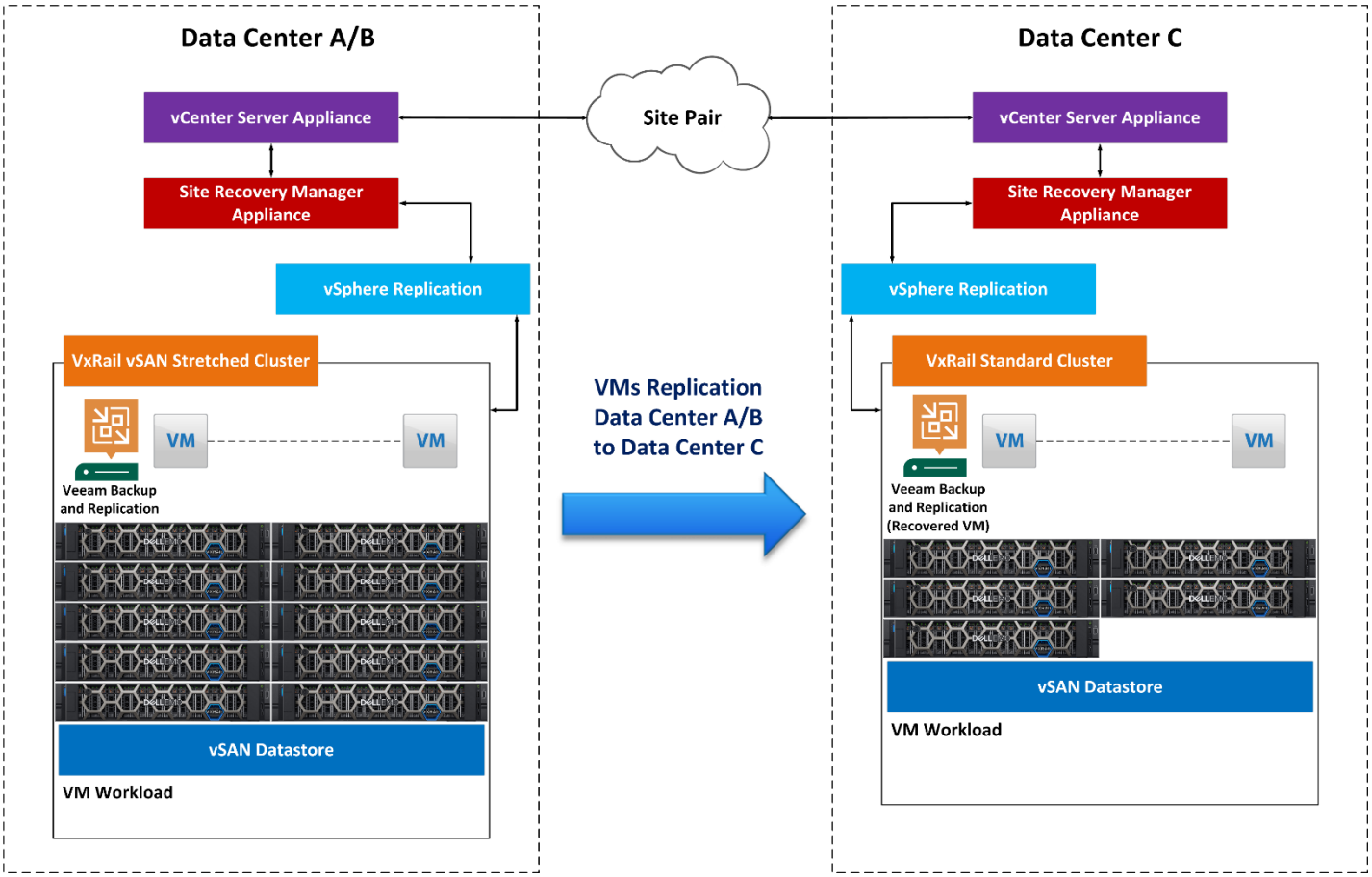


Figure 4 - The logical architecture diagram of the VMware Site Recovery Manager

Data Recovery Methodology

Now we will discuss the Data Recovery methodologies and architecture. Figure 5 shows the logical diagram of Veeam Backup and Replication. The management plane of Veeam Backup and Replication is a virtual machine. The primary backup of virtual machines is stored on Local disks

and SAN disks, and the secondary backup is stored on Dell PowerProtect DD6400 A. The secondary backup will replicate into the Dell PowerProtect DD6400 B at Data Center C. In this architecture, there are three full data copies for data recovery.

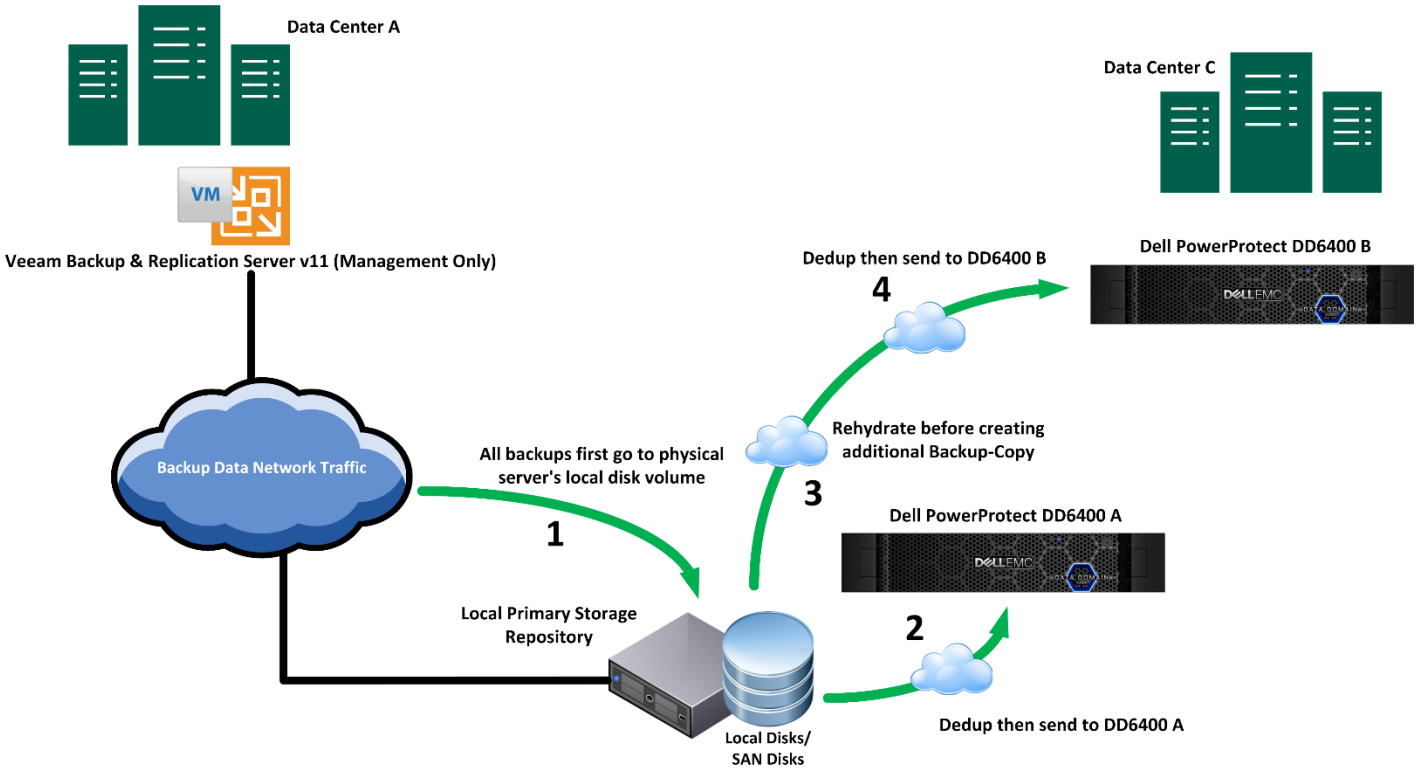


Figure 5 - The logical diagram of Veeam Backup and Replication

Requirements

This section details this solution's hardware and software requirements (cyber resilient for the modern data center).

Hardware Requirements

Each VxRail P670F includes two 800GB SSDs and ten 7.68TB SSDs. For the vSAN configuration, we will create two vSAN disk groups (1+4) on each node. The VxRail vSAN Stretched contains ten All-Flash nodes. Table 3 shows the hardware configuration of VxRail P670F.

VxRail Series	VxRail P670F
CPU Model	2 x Intel Gold 6348 CPU (28-Cores, 2.6GHz)
Memory	512GB (8 x 64GB)
Network Adapter	2 x Broadcom 57504 Quad Port 10/25GbE SFP28

Cache Drive	2 x 800GB SSD SAS drive
Capacity Drive	10 x 7.68TB SSD SAS drive
Power Supply	Dual Hot-Plug 1400W Power Supply
VxRail Software	VxRail Manager 7.0
VMware vSphere	VMware vSphere Enterprise Plus Edition
VMware vSAN	VMWare vSAN Enterprise Edition

Table 3 - The hardware configuration of VxRail P670F

Each Dell Backup Appliance includes a 32TB usable capacity license and enabled DD Boost and replication features. Table 4 shows the hardware configuration of PowerProtect DD6400.

PowerProtect DD Series	PowerProtect DD6400
Hardware	ES40 SHELF 12G 15X8TB SAS
Network	4 x 10GB SFP+ ports
Software	DD6400 Capacity License Bundle 1TBu

Table 4 - The hardware configuration of PowerProtect DD6400

Veeam Physical Repository Server

Table 5 shows the hardware configuration of the Veeam Physical Repository Server.

Model	Dell PowerEdge R750 Server
CPU Model	2 x Xeon Silver 4309Y CPU (8-Cores, 2.8GHz)
Memory	1TB (16 x 64GB)
Network Adapter 1	1 x Broadcom 57412 Dual Port 10GbE SFP+, OCP NIC 3.0
Network Adapter 2	1 x Broadcom 5719 Quad Port 1GbE BASE-T Adapter, PCIe Full Height
Fibre Channel Host Bus Adapter	1 x QLogic 2692 Dual Port 16Gb Fibre Channel HBA, PCIe Full Height, V2
Local SAS HDDs (Operating system)	2 x 600GB Hard Drive SAS ISE 12Gbps 10k 512n 2.5in with 3.5in HYB CARR Hot-Plug

Local NLSAS HDDs (Backup data)	7 x 12TB 7.2K RPM NLSAS 12Gbps 512e 3.5in Hard Drive
Power Supply	Dual Hot-Plug 1400W Power Supply
Microsoft Windows License	Windows Server 2022 Standard - 16 Core License Pack

Table 5 - The hardware configuration of the Veeam Physical Repository Server

Veeam Backup and Replication Server

Table 6 shows the hardware configuration of the Veeam Physical Repository Server.

VM or Physical	VM
vCPU	8 x Cores
Memory	16GB RAM
Operating System	Windows Server 2022 Standard
VMDK1	1 x 100GB VMDK virtual disk (For the operating system)
VMDK2	1 x 100GB VMKD virtual disk (For the Veeam binaries and DB)
NIC	1 x VMXNET3 network adapter

Table 6 - The hardware configuration of the Veeam Backup and Replication Server

VMware vSphere Replication Virtual Appliance

Table 7 shows the requirements of vSphere Replication Virtual Appliance.

VM	Virtual Appliance
vCPU	Dual-core or quad-core
Memory	8GB RAM
Operating System	Linux Platform 64-bit
VMDK1	1 x 16GB VMDK virtual disk
VMDK2	1 x 17GB VMKD virtual disk
NIC	1 x VMXNET3 network adapter

Table 7 - The system requirement of vSphere Replication Virtual Appliance

VMware Site Recovery Manager Virtual Appliance

Table 8 shows the requirements of the Site Recovery Manager Virtual Appliance.

VM	Virtual Appliance
vCPU	4 x vCPU
Memory	8GB RAM
Operating System	Linux Platform 64-bit
VMDK1	1 x 16GB VMDK virtual disk
VMDK2	1 x 4GB VMKD virtual disk
NIC	1 x VMXNET3 network adapter

Table 8 - The system requirement of the Site Recovery Manager Virtual Appliance

Software requirements

Table 9 shows the required software for each core component at each data center.

Location	Data Center A	Data Center B	Data Center C
VxRail Software	VxRail 7.0.xxx	VxRail 7.0.xxx	VxRail 7.0.xxx
vSAN Cluster Type	vSAN Stretched Cluster (preferred nodes)	vSAN Stretched Cluster (secondary nodes)	vSAN Standard Cluster
VMware vSphere Edition	10 x VMware vSphere Enterprise Plus per CPU	10 x VMware vSphere Enterprise Plus per CPU	10 x VMware vSphere Enterprise Plus per CPU
VMware vSAN Edition	10 x vSAN Enterprise per CPU	10 x vSAN Enterprise per CPU	10 x vSAN Enterprise per CPU
VMware vCenter Edition	1 x vCenter Server Standard Instance	N/A	1 x vCenter Server Standard Instance
VMware Site Recovery Manager	VMware Site Recovery Manager Standard Edition (Protected 50 VMs per site)	N/A	VMware Site Recovery Manager Standard Edition (Protected 50 VMs per site)

Veeam Software License	Veeam Backup & Replication Universal Subscription License (10 instance pack) Remark: The instance license depends on the number of protected VMs.	N/A	N/A

Table 9 - The summary of all required software licenses

Network Requirements

Each P670F contains two four 10GB ports Ethernet Adapters. P1 to P4 ports are used for VxRail's deployment and P5 to P6 ports are used for the backup server.

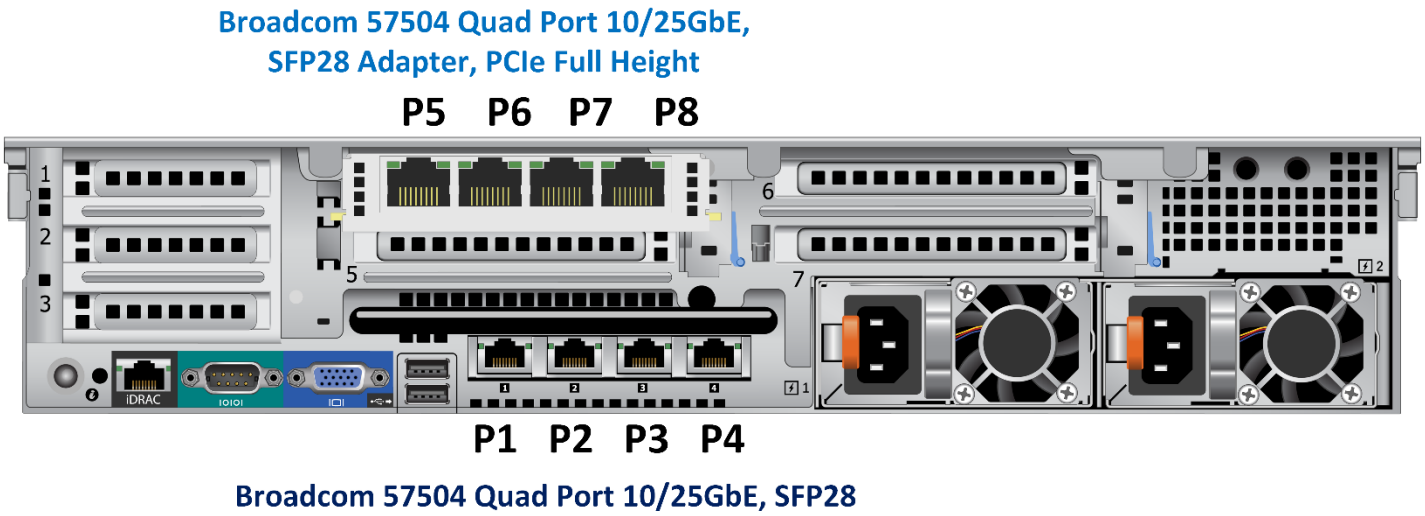


Figure 6 - The rear view of VxRail P670F

For the network design of the VxRail Cluster, reference the following table. Table 10 shows a network layout used for VxRail Cluster.

Network Traffic	NIOC Shares	VMKernel	P1	P2	P3	P4
Management Network	40%	vmk2	Standby	Active	Unused	Unused
vCenter Server Management Network	N/A	N/A	Standby	Active	Unused	Unused
VxRail Management Network	N/A	vmk2	Standby	Active	Unused	Unused

vSAN Network	100%	vmk2	Unused	Unused	Active	Standby
vMotion Network	50%	vmk2	Unused	Unused	Standby	Active
Virtual Machines Network	60%	N/A	Active	Standby	Unused	Unused

Table 10 - The Network Layout of VxRail

For the network design of the Veeam Backup and Replication server, reference the following table. Table 11 shows a network layout used for Veeam Backup and Replication server.

Network Traffic	NIOC Shares	VMKernel	P5	P6	P7	P8
Backup Network for VMs	100%	N/A	Active	Standby	Unused	Unused

Table 11 - The Network Layout of Veeam Backup and Replication server

Figure 7 shows the physical network diagram for Veeam Backup and Replication server and PowerProtect DD6400 in Data Center A. There are two 10BbE ports and one 1GbE port on each component. The 10GbE ports are used for the Production Network and 1GbE ports are used for OOB Management Network.

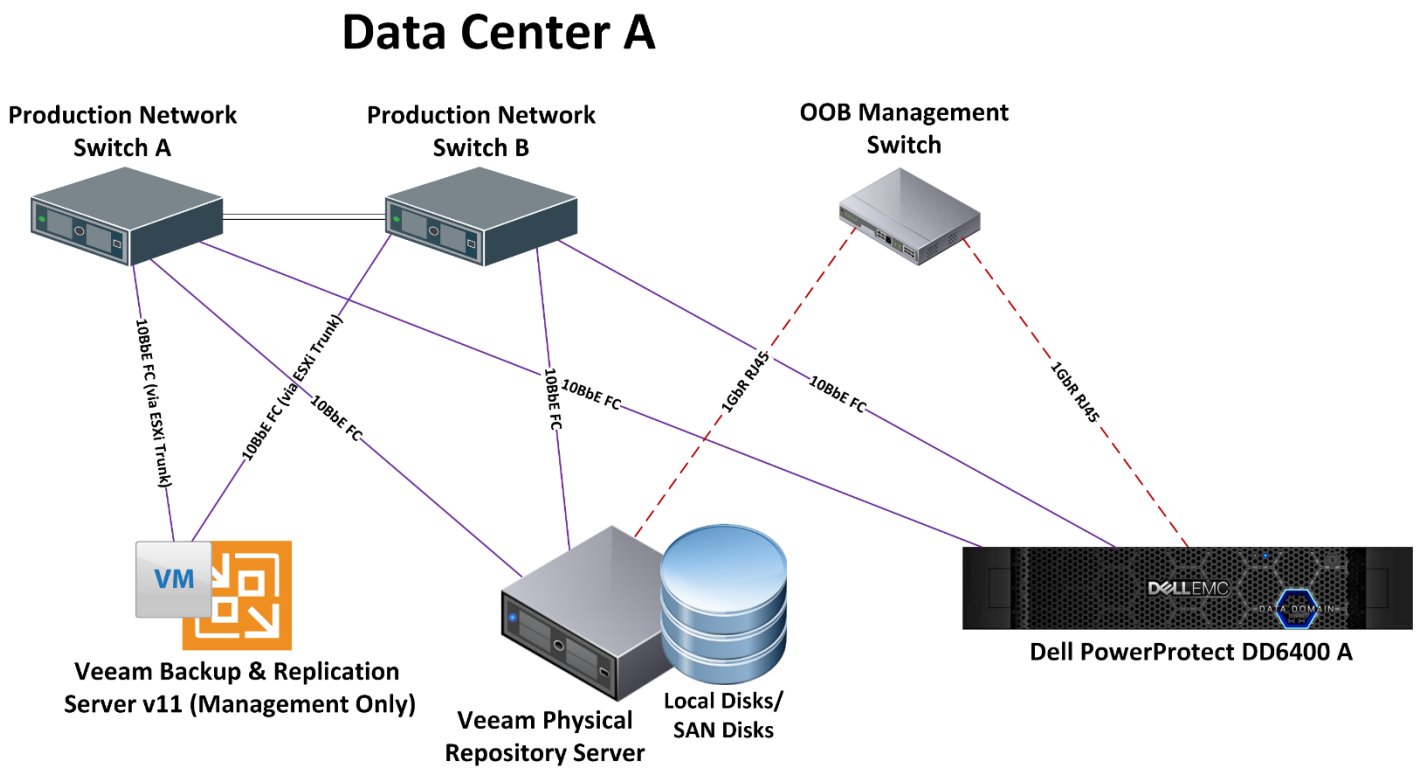


Figure 7 - Physical network diagram for Veeam Backup and Replication server and DD6400 in Data Center A

Figure 8 shows the physical network diagram for the DD6400 in Data Center C. There are two 10BbE ports and one 1GbE port on PowerProtect DD6400. =The 10GbE ports are used for the Production Network and 1GbE ports are used for OOB Management Network.

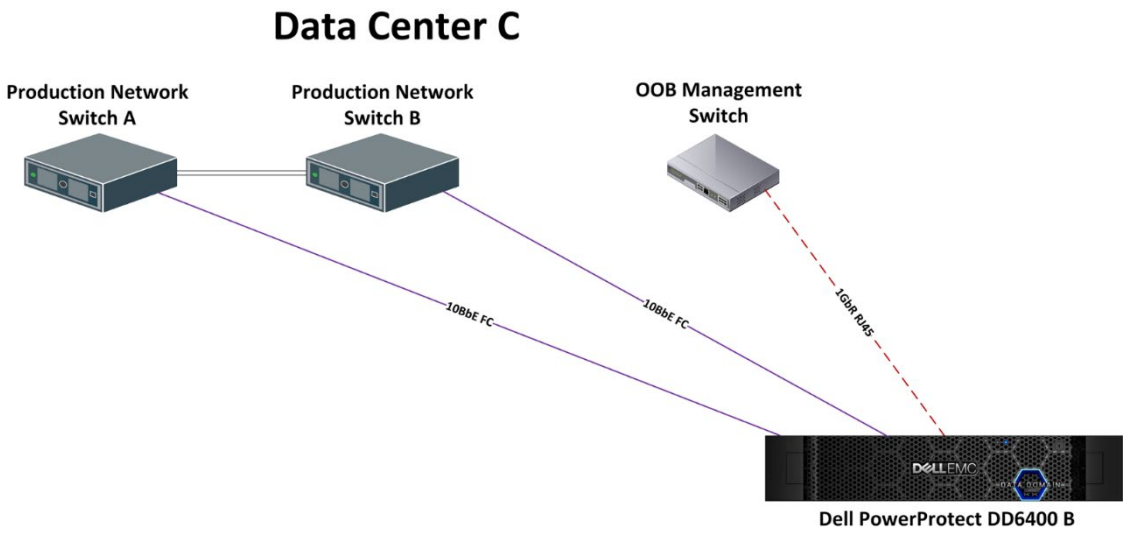


Figure 8 - Physical network diagram for the DD6400 in Data Center C

Figure 9 shows the network ports for VMware Site Recovery Manager Appliance and vSphere Replication Appliance and the required network ports for each core component.

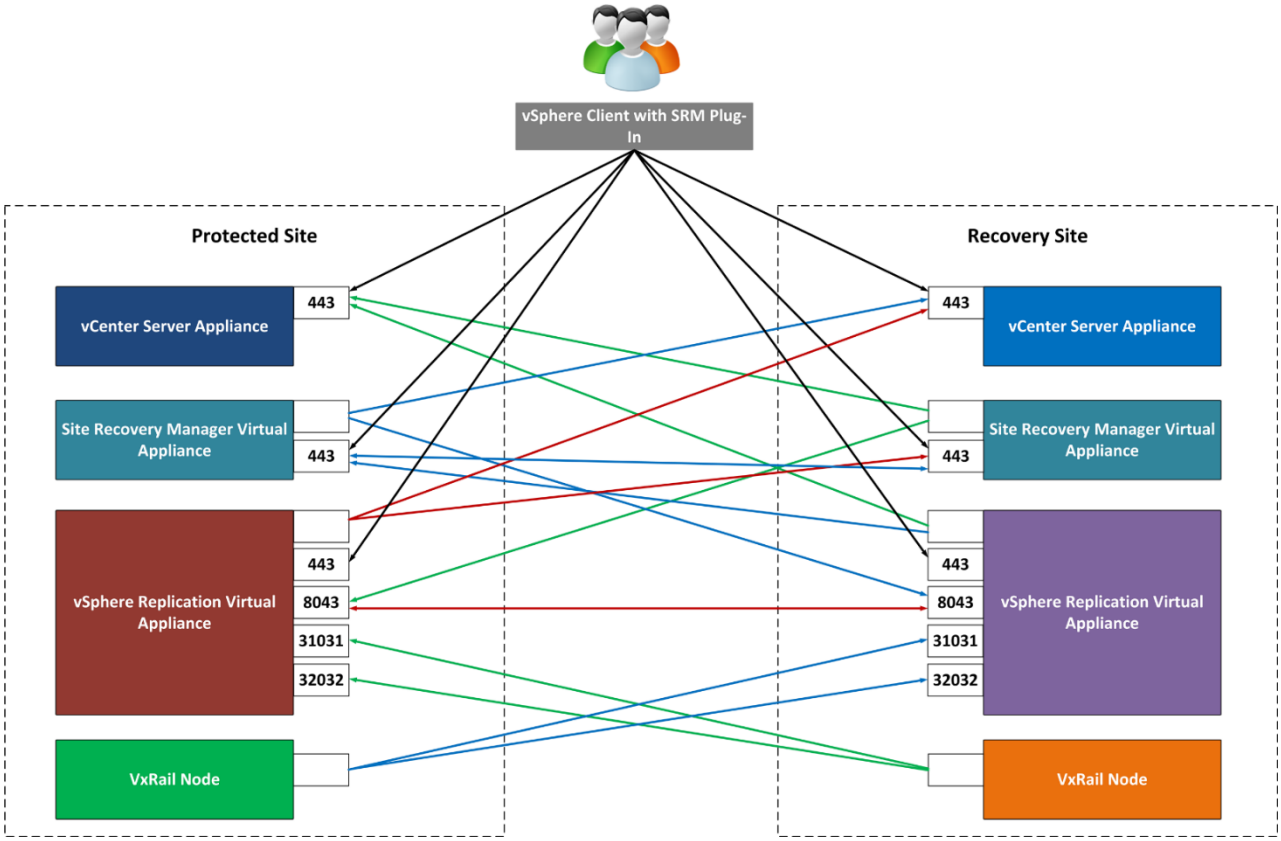


Figure 9 - Network Ports for VMware Site Recovery Manager Appliance and vSphere Replication Appliance

Recovery Scenarios

This solution is not only used for disaster recovery and active-active features. It can also provide a cyber-resilient feature. In this section, we will discuss the different data recovery scenarios.

Scenario One

If the virtual machines are attacked by ransomware in Data Center A, we can recover the virtual machines from Physical Repository Server with Veeam Backup and Replication Server.

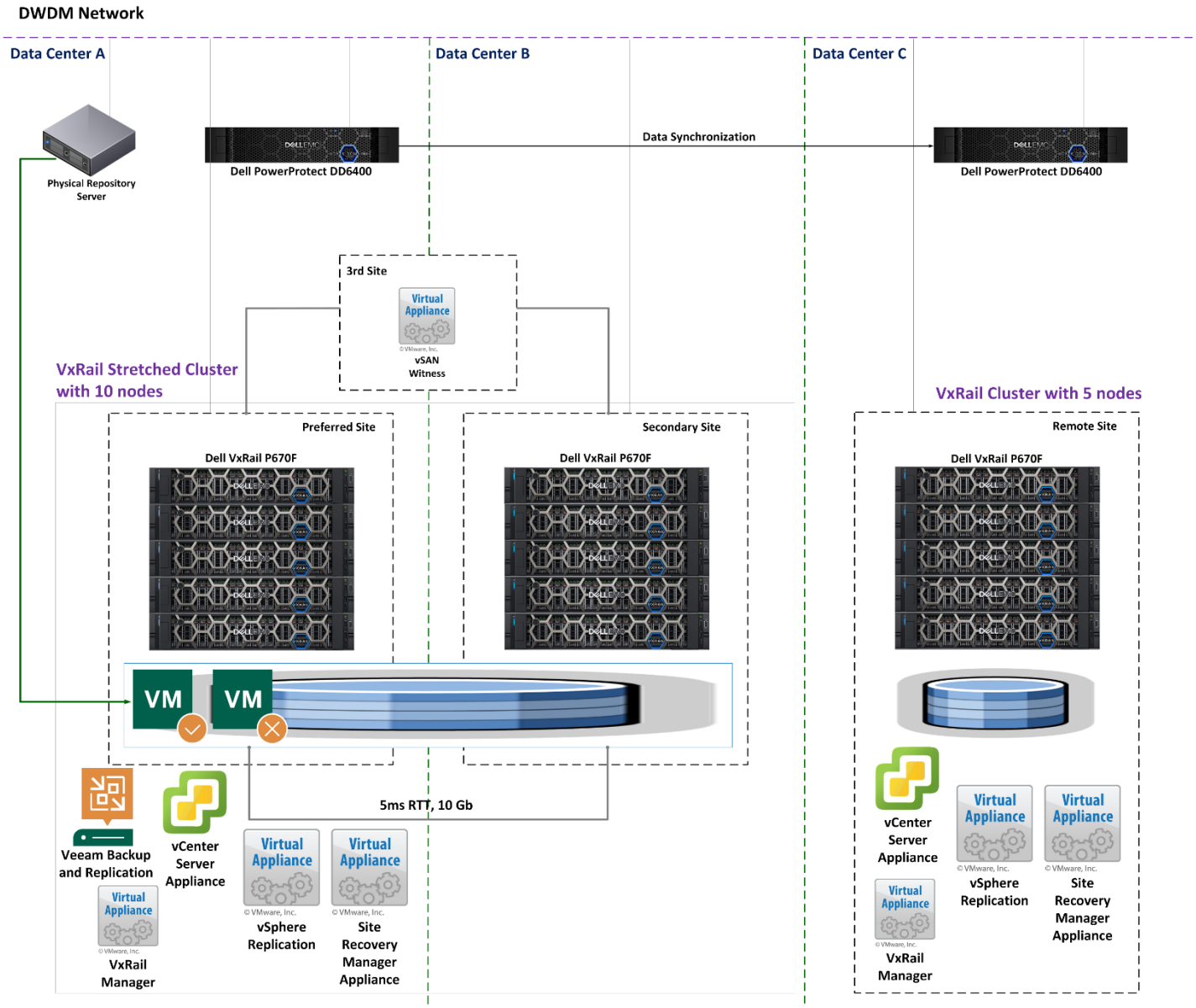


Figure 10 - Scenario one for data recovery

Scenario Two

Suppose the virtual machines and Physical Repository Server are attacked by ransomware in Data Center A. In that case, we can still recover the virtual machines from PowerProtect DD6400 with Veeam Backup and Replication Server because this DD6400 appliance stored the secondary backup of virtual machines.

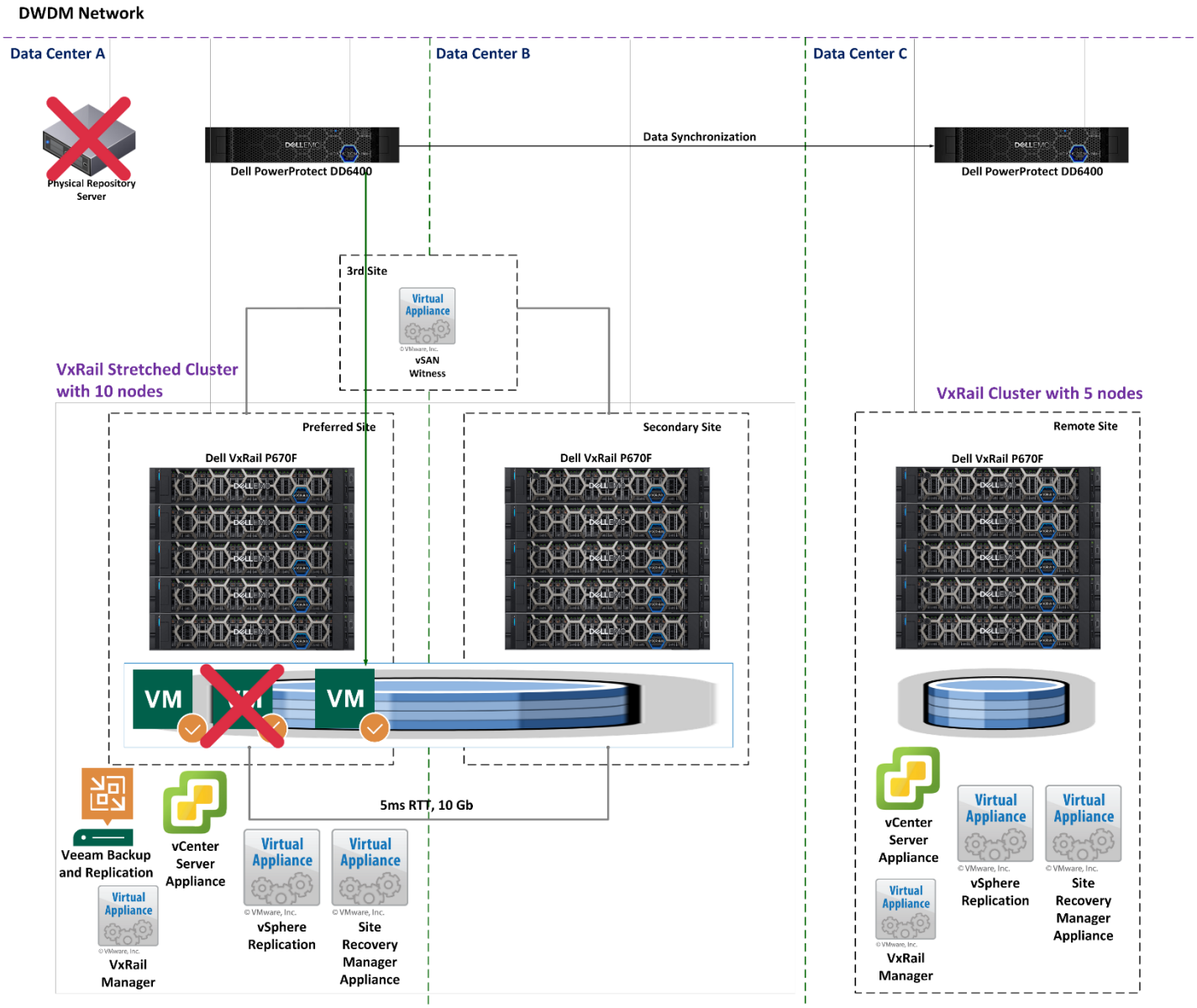


Figure 11 - Scenario two for data recovery

Scenario Three

If the virtual machines and Veeam Backup and Replication Server are attacked by ransomware in Data Center A, we cannot recover the virtual machines. We need to trigger the **SRM Recovery Plan** to recover Veeam Backup and Replication Server in Data Center C, then we can recover the virtual machines from either PowerProtect DD6400 or Physical Repository Server with Veeam Backup and Replication Server.

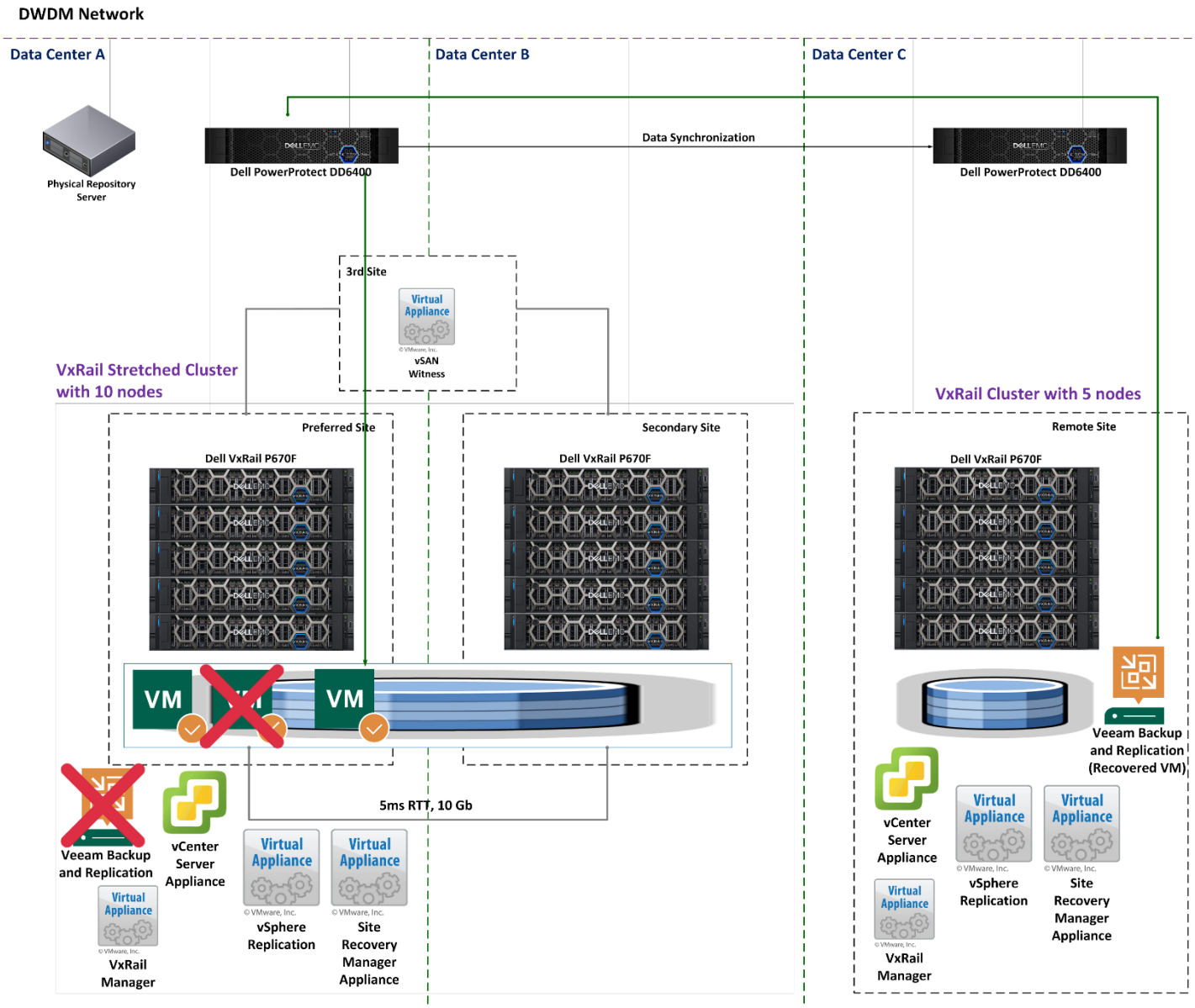


Figure 12 - Scenario three for data recovery

Scenario Four

If the virtual machines, Physical Repository Server. and PowerProtect DD6400 are all attacked by ransomware in Data Center A, we still can recover the virtual machines from PowerProtect DD6400 (installed in Data Center C) with Veeam Backup and Replication Server because this DD6400 appliance stored the replication backup of virtual machines.

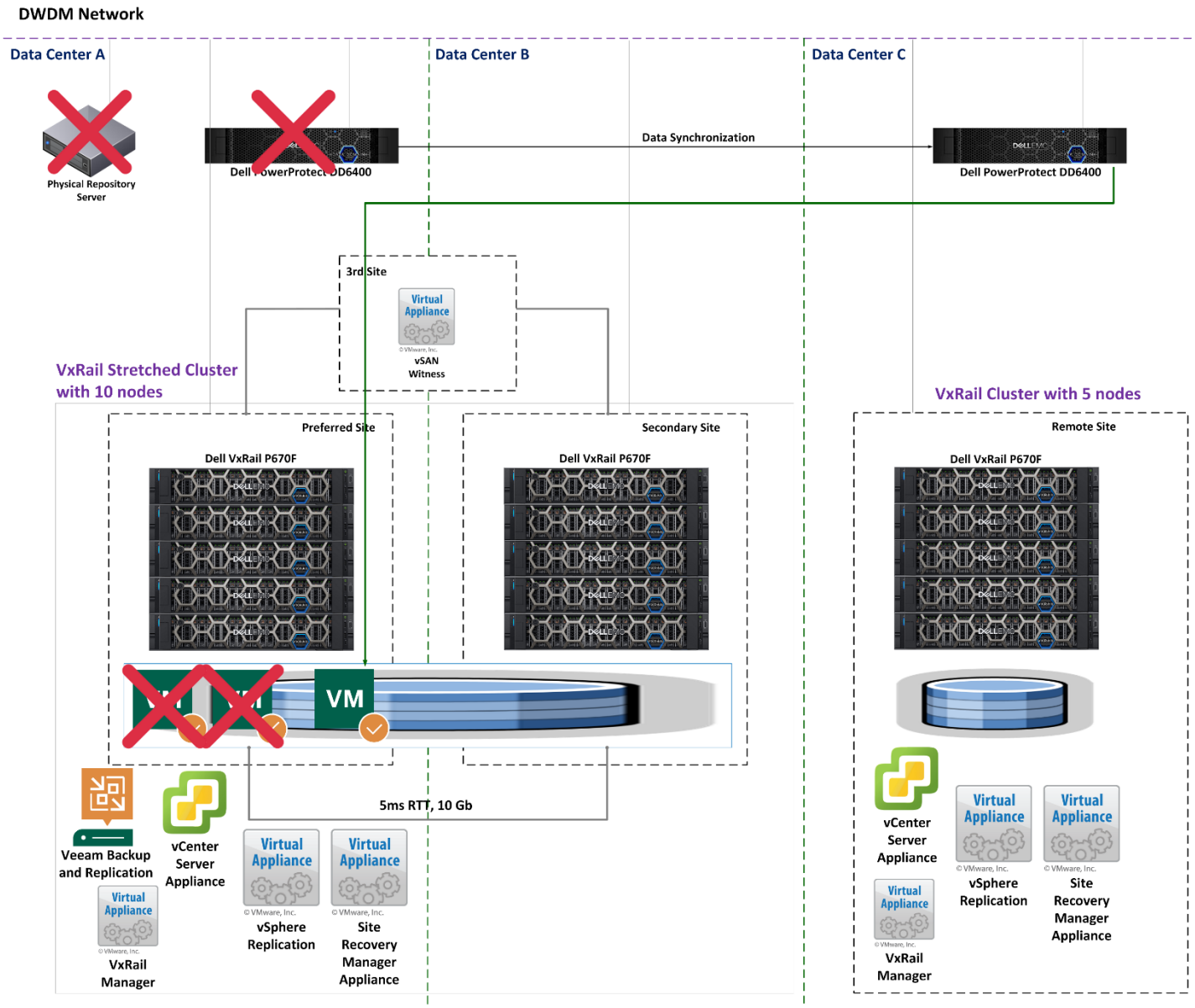


Figure 13 - Scenario four for data recovery

Scenario Five

If the virtual machines and all backup components are attacked by ransomware in Data Center A, we will not recover the virtual machines. We would then need to trigger the **SRM Recovery Plan** to recover Veeam Backup and Replication Server in Data Center C. Then we can recover the virtual machines from PowerProtect DD6400 (installed in Data Center C) with Veeam Backup and Replication Server.

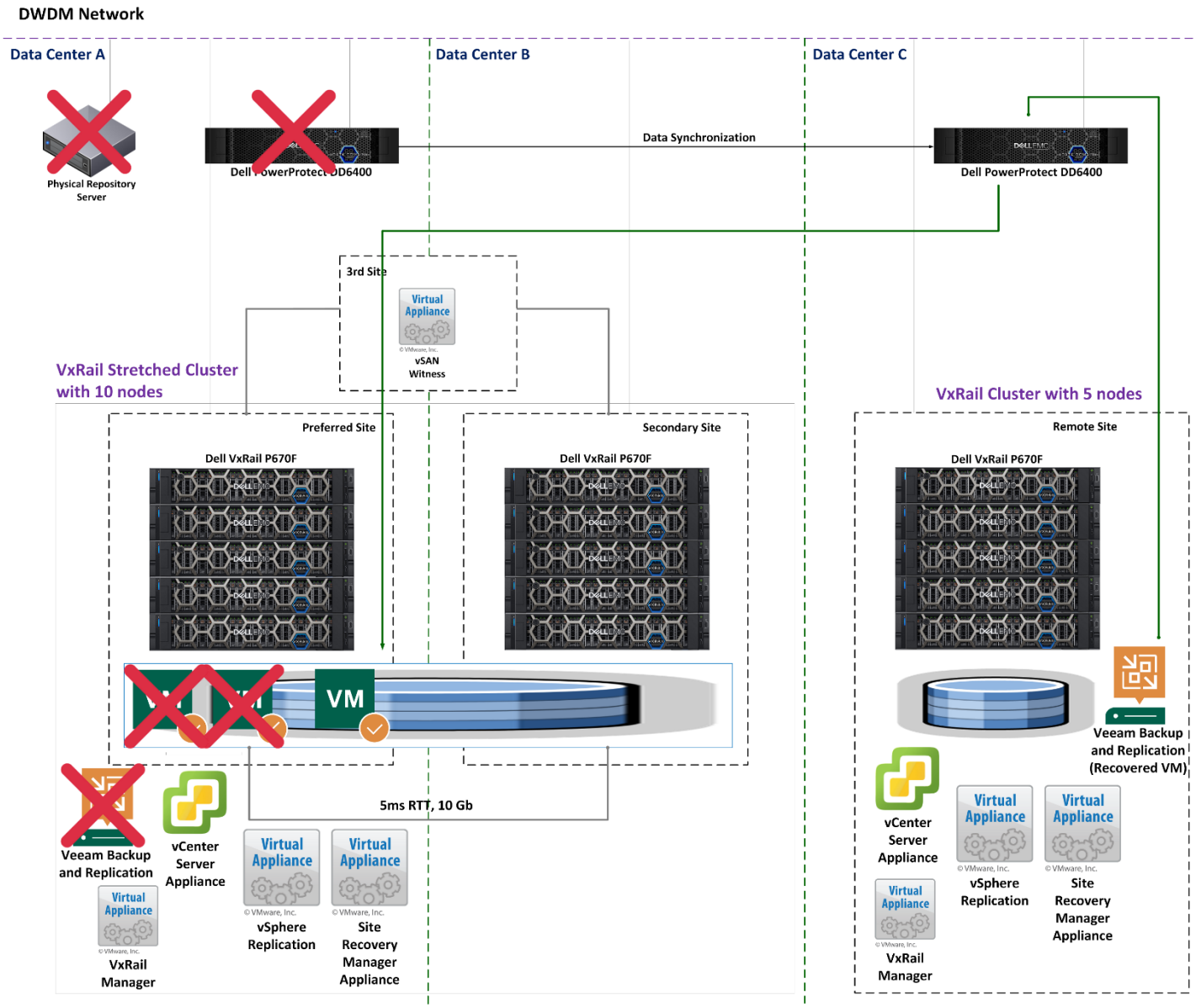


Figure 14 - Scenario five for data recovery

Based on the above scenarios, this solution can provide different data recovery methodologies

when the backup data and backup server are corrupted or attacked by ransomware.

Benefits

The design of this architecture can provide the following benefits:

- VxRail vSAN Stretched Cluster can provide the active-active Data Center across two separate locations, and can be integrated with VMware SRM, which could help to extend the site level protection to the other sites.
- The SRM Recovery Plan can provide automatic disaster recovery & data replication features.
- Dell PowerProtect DD6400 is used as Secondary Storage due to rehydration performance.
- For future options, it supports Tape-Out from Veeam Physical Repository Server.
- Rehydration for restore will be faster when restoring from a Veeam Physical Repository Server.
- It avoids the rehydration process that happens during PowerProtect DD6400 to DD6400 replication.
- It requires a lower virtual machine resource requirement for the Veeam Backup and Replication Server.
- It requires a lower virtual machine storage requirement for the Veeam Backup and Replication Server.
- VMware SRM can protect the Veeam Backup and Replication Server due to the Veeam Backup and Replication VM not being used as a Primary Storage Repository.
- This solution includes three backup copies of all virtual machines, i.e., primary storage, secondary storage, and replication copy.
- For future expansion, Dell VxRail supports scale-out to 64 nodes in a cluster.
- The Dell Data Domain appliance also supports scale-up and scale-out in a data pool for backup data expansion.
- We can still recover the production data into the remote site if all core backup servers and backup storage are corrupted in primary and secondary Data Centers.
- It can offer low RTO/RPO and ensure business continuity.

Conclusion

This infrastructure design of cyber resilient solution is simple to use, flexible, and reliable. It includes two core features - resilient infrastructure and resilient data recovery. It provides data life-cycle management for data centers, remote offices, and cloud-based workloads. It ensures data availability while enabling a business to be more agile by using data to accelerate business success and reduce overall costs. Table 12 shows the summary of this infrastructure design.

Features	Description	Supported / Not Supported
Site Availability	The infrastructure can deliver the active-active data center.	VxRail Stretched Cluster can deliver active-active data center.
WORM	The solution should support immutable Backup. (i.e., Write Once Read Many (WORM) feature).	This backup appliance can support the WORM feature.
Single Management Dashboard	Single console to handle system backup tasks and management.	All workloads can be handled in a single console.
Scale-up and Scale-out	HCI/Backup capacity and performance easy to scalable and upgrade without service interruption.	HCI platform and Backup Appliance can support scale-up and scale-out.
Multiple backup copies	It supports one to many backup copies	This solution can provide primary and secondary backup copies and replicate the backup copies to the other sites.
Instant Recovery	A fast recovery function to resume services in a short period (10-15 minutes), and service uninterrupted for live migration after recovery, is preferable to ease the subsequent recovery process.	This solution supports this feature.
Ransomware detection	It has the ability to predict, detect and protect against Ransomware using Artificial Intelligence.	This solution supports this feature.
Agentless backup and restore	Support agentless backup and restore operations towards the different hypervisors, e.g., VMware, Microsoft Hyper-V, Nutanix AHV, etc.	This solution supports Agent and Agentless data backup and recovery.

Table 12 - The features summary of this infrastructure design

Bibliography

Dell EMC VxRail 7.0 vSAN Stretched Cluster Planning Guide
https://www.delltechnologies.com/asset/en-us/products/converged-infrastructure/industry-market/h19413-vxrail-stretched-cluster-planning-guide-for-7-0.pdf

Dell VxRail vCenter Server Planning Guide
https://www.delltechnologies.com/asset/en-us/products/converged-infrastructure/technical-support/vxrail-vcenter-server-planning-guide.pdf

TechBook - Dell EMC VxRail System
https://infohub.delltechnologies.com/l/techbook-dell-emc-vxrail-system-2/data-protection-115

Overview of Dell EMC PowerProtect DD6400
https://infohub.delltechnologies.com/l/dell-emc-powerprotect-dd-6400/overview-2407

Overview of VMware vCenter Site Recovery Manager
https://docs.vmware.com/en/Site-Recovery-Manager/5.5/com.vmware.srm.install_config.doc/GUID-C1E9E7D0-B88F-4D2E-AA15-31897C01AB82.html

Veeam Backup & Replication 11 - User Guide for VMware vSphere
https://helpcenter.veeam.com/docs/backup/vsphere/emc_dd.html?ver=110

Veeam Alliance Technical Programs
https://www.veeam.com/alliance-partner-technical-programs.html