Dell EMC™ VxRail™ - Accelerating the Journey to VMware Software-Defined Data Center (SDDC)

VMware Validated Designs for SDDC (VVD) on Dell EMC VxRail

Abstract

Dell EMC can help to accelerate organizations on their journey to build their VMware SDDC environment with HCI for any choice of path: custom (DIY), guided, or automated. VxRail Appliance is the platform of choice for customers that are looking for the fastest possible IT outcomes. VVD on VxRail, discussed in this paper, provides a great balance between simplicity and flexibility for their SDDC deployments.

January 2019

Revisions

Date	Description
Jan 18, 2019	Minor updates based on the additional feedback received.
Dec 17, 2018	Initial release.

Acknowledgements

This paper was produced by the VxRail and VxRack SDDC Technical Marketing team.

Content Owner: Karol Boguniewicz

Table of contents

Executive summary

Information Technology (IT) departments are under significant pressure to deliver new applications to market, to innovate with technology to beat competitors and to do it faster with more choice. At the same time, there are requirements for stricter compliance, improved security, controlled costs and increased efficiency. To solve these problems, the modern data center is trending towards converged and hyper-converged infrastructures, virtualization and software-defined infrastructures and public and hybrid cloud solutions.

The VMware vision of the modern data center is a software-defined, standardized architecture. It is a fully integrated hardware and software stack, simple to manage, monitor and operate. The VMware architecture for the software-defined data center (SDDC) empowers companies to run hybrid clouds and to leverage unique capabilities to deliver key outcomes that enable efficiency, agility and security. The VMware SDDC is based on VMware vSphere®, VMware vSAN® and VMware NSX® to provide compute, storage and networking virtualization to the SDDC and on the VMware vRealize® Suite for additional management, self-service, automation, intelligent operations and financial transparency.

VMware sees three paths for building an SDDC:

- **Custom**, “Do It Yourself” (DIY)
- **Guided** with VMware Validated Designs (VVD)
- **Automated** with VMware Cloud Foundation™

Dell EMC shares VMware’s vision of the modern data center and extends that to the infrastructure. With VVD on VxRail, Dell EMC provides services and additional automation beyond the self-guided VVD path. It is the solution that provides the best combination of design flexibility, integration, automation and speed of deployment for most customers.

Dell EMC provides a full range of cloud platforms to accelerate digital business transformation with less risk and greater savings, offering varying levels of pre-engineered solutions for VMware, Pivotal and Microsoft-based clouds. Dell EMC’s best-of-breed hardware is combined with the right level of integration, tooling and documentation to accelerate business results, simplify daily operations and achieve greater levels of efficiency and transparency.

This whitepaper explains why Dell EMC’s VxRail is the platform of choice for customers who would like to accelerate the journey to the VMware hybrid-cloud.

VxRail is a fully integrated hyper-converged appliance that enables a software-defined data center. The VxRail Appliance is architected with a software stack for appliance management, virtualization, and VM management. VxRail Manager provides: automation and orchestration for day 0 to day 2 appliance-based operational tasks, single-click upgrades of hardware firmware components and software, and monitoring with dashboards for health, events and detailed physical node views.

Dell EMC is #1 in hyper-converged systems, all based on the Dell EMC PowerEdge™ server platform. VxRail Appliances are jointly engineered by Dell EMC and VMware and are the only fully integrated, preconfigured and tested HCI appliance powered by VMware vSAN technology for software-defined storage. Dell EMC has completed the certification process for the VMware Validated Design Certified Partner Architecture on the VxRail making it the only HCI appliance currently certified for the VVD.

VxRail nodes are available with different hardware configurations varying the compute power, memory, cache, storage and GPU configurations to closely match the requirements of new and expanding use cases. As requirements grow, the system easily scales out and scales up in granular increments. VxRail software

includes VxRail Manager for appliance management, operations and automation and can offer additional data protection options integrated with VMware. VxRail greatly simplifies the infrastructure management via automation, lifecycle management (LCM), and configuration flexibility so you can deploy the infra for a VMware SDDC to most closely match your workload needs,

Dell EMC support is recognized with over a 95% customer satisfaction rating[1] and has received multiple awards. Dell EMC Professional Services offers ProDeploy installation and implementation services to ensure smooth and rapid integration of VxRail Appliances into customer networks and consulting for the VMware stack. Dell EMC simplifies the process of VxRail fabric creation, administration and operation with automated design, fabric creation and operation. Dell EMC also protects customer investment with the future-proof loyalty program.

In short, by deploying VVD on VxRail, customers can accelerate time to market, de-risk deployment and operations, increase efficiency, drive IT agility, operate in confidence and future-proof their infrastructure to get ready for VMware hybrid cloud.

This paper also includes references of where to look for more information and there are appendices to provide additional detail on VMware products used in the SDDC, VMware Validated Designs, VMware Cloud Foundation and some of the complimentary VMware integrated data protection options from Dell EMC.

[1] http://i.dell.com/sites/doccontent/business/solutions/brochures/en/Documents/prosupport-enterprise-suite-brochure.pdf

1 Business IT challenges and trends

1.1 Business IT challenges

Technology is transforming the way we live and work at an ever-increasing pace. This is a new digital era. It is the dawn of the Internet of Everything (IOT), what many have called the next industrial revolution. While previous industrial eras were driven by steam, coal and electricity, this one is driven by data. It is ruthlessly changing the business landscape and reinventing our future.

Business Information Technology (IT) departments are under significant pressure. IT is no longer just responsible for keeping the lights-on and treated as a cost center. IT is becoming a business partner, responsible for playing a significant role in digital transformation. There is an imperative to deliver new applications to market, to innovate with technology to beat competitors and to do it faster with more choice. At the same time there are requirements for stricter compliance, improved security, controlled costs and increased efficiency. Lowering risk with disaster recovery (DR) and business continuity (BC) solutions becomes even more critical.

Traditional IT infrastructure is custom designed to fit a business' particular needs using any solution from any vendor. This flexibility comes with drawbacks, including the extensive time needed to research and get the initial or expanded infrastructure ordered, installed and ready to deploy applications. Infrastructure from multiple hardware and software vendors leads to separately managed operational silos, relying on multiple IT staff with different areas of expertise. Without centralized management, achieving security and compliance is much more difficult. When there is a problem, support issues may get stuck in circular finger pointing where vendors blame one another. Even with careful planning, upgrades run into complications and increased risk from interactions between products from different vendors.

Each product in this type of legacy stack is likely to be grossly overprovisioned, using its own resources (CPU, memory and storage) to address the intermittent peak workloads of resident applications. The value of a single shared resource pool, offered by server virtualization, is still generally limited to the server layer. All other components, such as networks and storage, are islands of overprovisioned resources that are often not shared. Therefore, low utilization of the overall stack results in the ripple effects of high acquisition, space and power costs. Too many resources are wasted in traditional legacy environments.

The physical infrastructure consists of complex hardware silos that are difficult to manage or automate. Regular maintenance tasks and hardware outages require expensive downtime. Mitigating the problem using dedicated standby hardware is expensive. The hardware-centric architecture results in operational inefficiencies because of factors such as the limited capacity of the CPUs in running applications, a single operating system image per machine and inflexible infrastructure that is difficult to troubleshoot.

These problems can be mitigated by trading off a highly flexible choice of vendors and applications for building the infrastructure with a more restricted infrastructure that is easier to support and maintain. Traditional IT can use product compatibility lists to help alleviate multi-vendor support issues by limiting the scope of solutions that can be considered for use to products included in the compatibility list. However, without easy automation solutions and with limited IT staff, achieving compliance is still very challenging.

1.2 Trend to converged and hyper-converged infrastructures

Both converged and hyper-converged infrastructures limit the choice of multi-vendor products, reducing the time, cost and risk of deploying, configuring and managing hardware and software components separately.

Converged infrastructure (CI) is largely systems integration, where an entire solution is built and sold as a single unit.

CI systems take the responsibility of system integration and validation of infrastructure components off the hands of customers and assure lifecycle management. Customers can spin up virtual machines, containers and even bare metal servers without having to worry about selecting, integrating or upgrading the infrastructure. A custom management interface and a combination of professional services for setup and upgrades shortens the time to get the solution running.

Hyper-converged infrastructure (HCI) software defines the storage that is installed inside individual servers into a single, shared pool of storage and then runs workloads on those same servers. HCI uses software-defined technologies to provide compute, storage, and networking infrastructure services rather than using traditional purpose built hardware components. HCI is usually deployed on standard server components; providing a simplified scale-out architecture with intelligence and rich data services moved to the software layer. With a much narrower set of potential hardware and software combinations, HCI vendors more thoroughly test their hardware and software stack, providing easier software and hardware upgrades.

Organizations are transforming from traditional do-it-yourself infrastructure and adopting CI and HCI solutions to help them meet their business IT challenges. With CI and HCI infrastructures, multiple pre-engineered and pre-integrated components operate under a single controlled architecture with a single point-of-management and a single source for end-to-end support. HCI provides a localized single resource pool that enables a higher overall resource utilization than can be achieved with legacy infrastructure. Overall total cost of ownership (TCO) is lower with operational savings from simplified management. In the data center, HCI typically has a smaller footprint with less cabling and can be deployed much faster and at lower total cost than traditional infrastructure.

Industry infrastructure deployment is transforming as customers begin to shift from a “build” to a “consume” approach. This deployment shift is being driven by the need for IT to focus limited economic and human capital resources on driving business innovation, which results in fewer resources available to focus on infrastructure. While a “build-your-own” deployment strategy can achieve a productive IT infrastructure, this strategy can be difficult and lengthy to implement, vulnerable to higher operating costs and susceptible to greater risk related to component integration, configuration, qualification, compliance and management. A “consume” deployment strategy for HCI provides the benefits of previously integrated, configured, qualified and compliant components. Purchasing an HCI system provides a single optimized IT solution that is quick and easy to deploy. A “consume” deployment strategy for HCI provides a simple and effective alternative to “build-your-own” and it has been widely adopted.

1.3 Trend to virtualization and software-defined infrastructures

Virtualization transforms physical systems into a virtual environment by creating a logical version of a device or resource - anything from a server to an operating system. Virtualization helps solve problems with utilization and rapid scalability. Without virtualization, traditional server utilization is typically in only the 6% to 12% range.

Traditional hardware comes in fixed sizes and is hard to scale and fully utilize. Virtualization allows organizations to purchase more powerful equipment with better performance and put many optimally-sized virtualized resources on it. Technologies such as overprovisioning, automatic load balancing, clustering and parallel processing optimize resources and improve uptime. Virtualization technology emulates hardware

using software that hides details of the underlying physical hardware. Multiple hardware components and the functionality of that hardware can be efficiently emulated on less expensive, non-specialized hardware.

Server virtualization is mature and proven technology with high adoption rates in data centers of all sizes. Both storage and network virtualization are growing trends. Storage virtualization groups physical storage from multiple storage devices so that it looks like a single storage device. Software-defined storage (SDS) includes storage virtualization and goes further to abstract all storage services from hardware devices using software to create, deploy and manage storage resources and infrastructure. SDS enables expensive proprietary storage solutions to be replaced with software-defined storage that utilizes x86 technology. By utilizing industry-standard x86 technology, SDS helps eliminate the need for storage area networks (SANs) and proprietary storage expertise. Organizations can also reduce their storage footprint, which lowers hosting and cooling costs

Software-defined networking (SDN) is a computer networking architecture that separates the data plane from the control plane in routers and switches. The control plane is implemented in servers using software and is separate from networking hardware. The data plane is implemented in networking hardware. In traditional networking, when a data packet arrives at a switch or router, the firmware tells the hardware where to forward the packet and sends all packets to that destination via the same path. All packets are treated the same. More advanced smart switches equipped with application-specific integrated circuits (ASICs) recognize different types of packets and treat them differently based on the ASIC programming. These switches, however, are expensive.

SDN decouples networking control from the hardware's firmware. The network administrator can centrally configure network traffic without changing the settings of individual switches. The administrator can change network rules, prioritization and selectively block packets with greater control. SDN provides better control of network traffic and offer better security options while using less expensive commodity switches as the underlying hardware layer.

1.3.1 Software-defined data center (SDDC) solution

Combining server, storage and network virtualization together leads to a completely software-defined infrastructure. *The Why, the What and the How of the Software-Defined Data Center* (Osterman Research, May 2017) identifies the business benefits of the SDDC solution:

Improved speed and productivity of IT staff

- Because of its software-defined nature, with proper tools, an SDDC is easier to configure, reconfigure and keep secure, resulting in IT operations that are more responsive to change and more efficient. SDDC also permits frequent service updates and rapid standup/teardown of test environments.

Improved security

- SDDC's software-defined nature enables consistently-enforced policies that act on logical, abstracted characteristics of the workload and its data. Traditional data center operations must distribute rules across a range of different hardware devices that will need to be manually updated with inevitable hardware and configuration changes. In an SDDC, relevant policies remain in place and automatically adjust to changes in the underlying physical environment of SDDC workloads.

Improved utilization of hardware

- Virtualization increases the hardware utilization, allowing organizations to make more efficient use of their capital expenditures. For example, it allows several workloads to share software-defined

computing, storage and network resources. SDDC unifies networking functions using non-specialized hardware avoiding lock-in to specific networking equipment.

Enabled interoperable cloud

- SDDC helps organizations realize the benefits of hybrid clouds without vendor or technology lock-in. The combination of automation, abstraction, visibility and control fosters consistency that will ease the placing of workloads into public or private clouds to an even greater extent than virtualization alone would permit.

1.4 Trend to public and hybrid cloud

The ability of cloud computing to offer solutions to the business IT challenges stated above is driving more organizations to use cloud computing as a key part of their IT infrastructure. Cloud computing provides an option to entirely replace a hardware data center with a service offering where it is not necessary to be concerned about the underlying hardware supporting it. Cloud computing can also extend a hardware data center by providing on-demand resources faster, in smaller increments and reduces the capital and operational expense of adding hardware to the data center.

The National Institute of Standards and Technology (NIST) provides a definition of cloud computing.

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[2]

The five essential characteristics of cloud computing are:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

A public cloud is formed when a cloud provider makes computing resources publicly available over the internet. In a public cloud, setup for a consumer is usually quick and easy. Users pay for resources used rather than for direct hardware. Some providers also charge a subscription fee. If more resources are needed, the cloud can instantly provide them. There is no need to install additional hardware or software. One of the concerns and barriers for organizations using the public cloud is data security and governance.

Private cloud describes a computing infrastructure privately held by an organization that has capabilities similar to a public cloud but is completely internal and therefore more secure. Virtualization provides many cloud-like resource allocation features. The addition of cloud management tools can be used to build a private cloud.

Hybrid cloud supports an organization's applications on a mix of private and public clouds. Applications that provide strategic value to the organization and may contain sensitive information are often kept on a private

[2] https://csrc.nist.gov/publications/detail/sp/800-145/final

cloud, while a public cloud is used for everything else. There are many reasons, including the cost of rewriting legacy applications to run in a new environment and avoiding the risk of breaking something that is currently working, that keep applications in the corporate data center. As the public cloud becomes increasingly secure and new applications are written for the cloud, more applications will migrate to the public cloud. With a hybrid cloud, companies can transition to the cloud at their own pace, with less risk and at a lower cost.

2 VMware software-defined data center (SDDC)

VMware is a leader in providing both the virtualization and management products that support a software-defined data center and in integrating them into a cohesive solution.

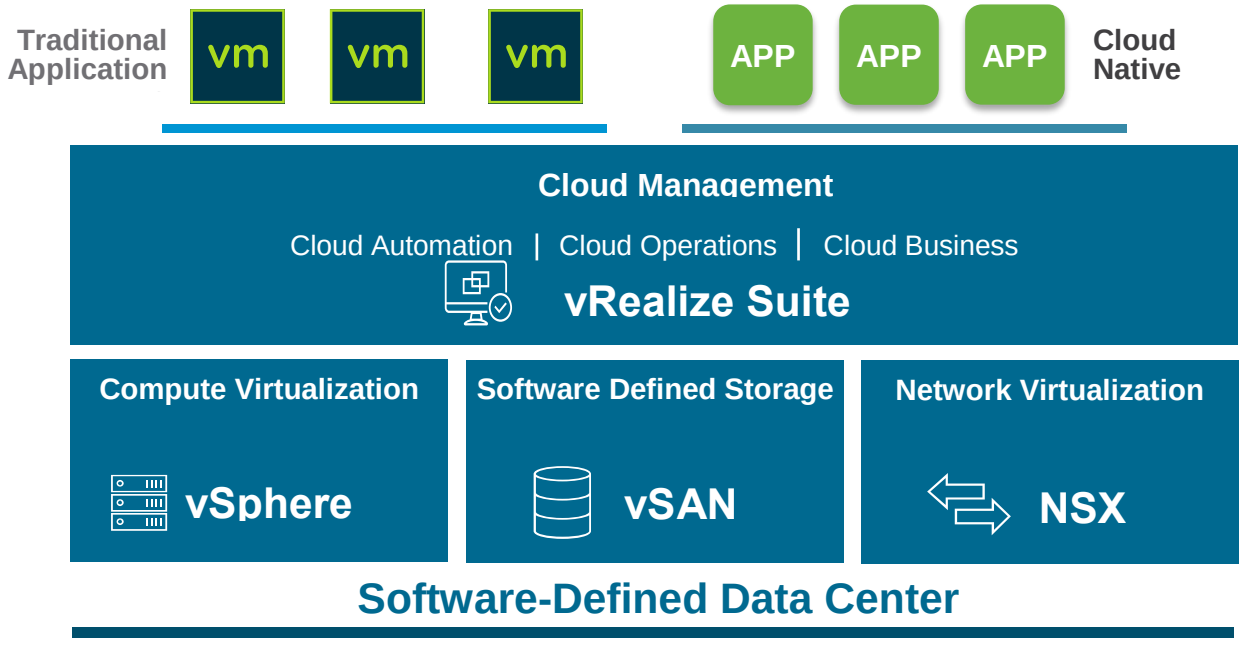
2.1 VMware SDDC vision

The VMware vision of the modern data center starts with a foundation of software-defined infrastructure and is based on the value customers realize from a standardized architecture. It is a fully integrated hardware and software stack, simple to manage, monitor and operate. The VMware approach to the SDDC delivers a unified platform that supports any application and provides flexible control. The VMware architecture for the SDDC empowers companies to run private and hybrid clouds and to leverage unique capabilities to deliver key outcomes that enable efficiency, agility and security.

The fully virtualized data center is automated and managed by intelligent, policy-based data center management software, vastly simplifying governance and operations. A unified management platform enables centralized monitoring and administration of all applications across physical geographies, heterogeneous infrastructure and hybrid clouds. Workloads can be deployed and managed in physical, virtual and cloud environments with a unified management experience. IT becomes agile, elastic and responsive to a degree never before possible.

The VMware SDDC is based on well-established products from VMware. vSphere, vSAN and NSX provide compute, storage and networking virtualization to the SDDC and the vRealize Suite brings additional management, self-service, automation, intelligent operations and financial transparency. This forms a solid foundation to host both traditional and cloud-native application workloads.

Figure 1 VMware software-defined data center architecture



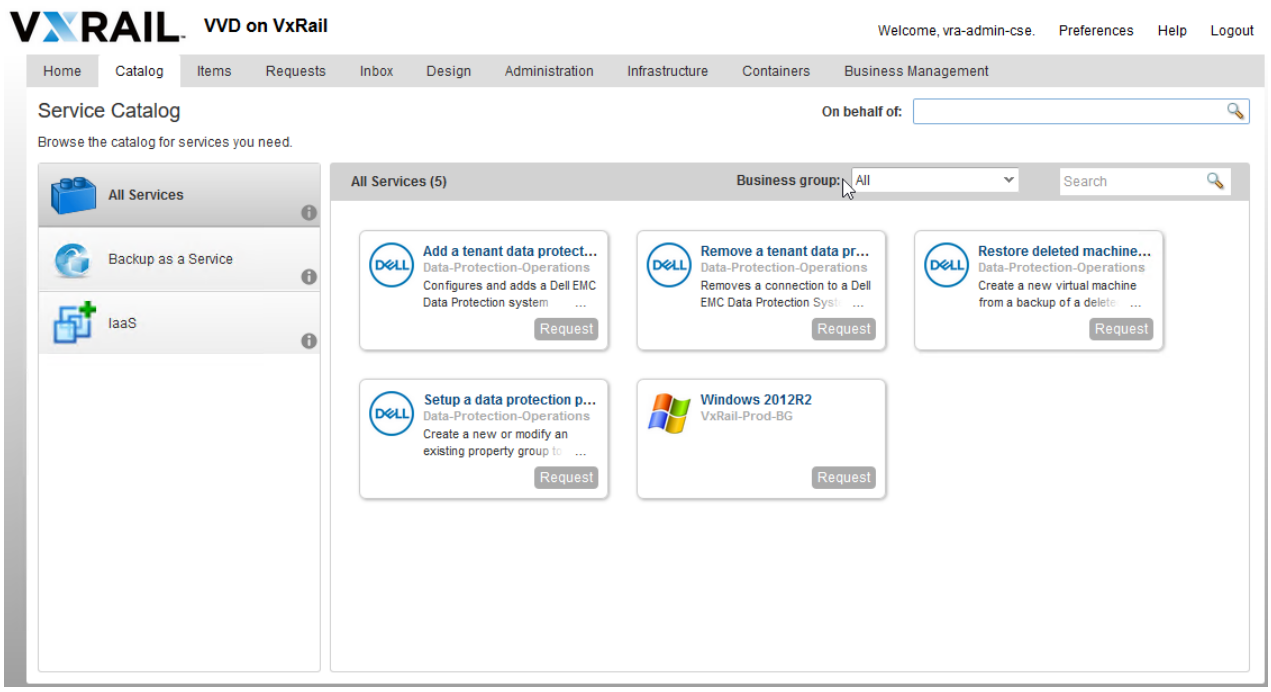
2.1.1 IT service delivery automation

Organizations that are running traditional hardware data center architectures are forced to rely on manual processes, scripting, and complicated communication between teams to get new applications to market. They experience lengthy and costly challenges provisioning networks, and troubleshooting manual process configuration errors. By transforming to an SDDC, organizations can automate and manage IT processes in software. A fully automated environment can dramatically reduce the production-ready infrastructure and application component provisioning time from days or weeks down to a matter of minutes.

As part of the VMware SDDC cloud management platform, VMware vRealize Automation™ (vRA), can solve the challenges observed in traditional data center architectures with comprehensive and extensible automation capabilities, providing a self-service cloud experience. The ability to integrate into existing processes maximizes the SDDC platform return on investment (ROI) and ensures, that it is not just an island in the environment.

Service architects use a convenient visual interface to design service blueprints that can span one or multiple VM templates, logical networks, load balancers, security policies, software components and scripts. Using this approach they can model comprehensive IaaS and application services, which then can be exposed to end-users via the customizable self-service catalog as shown by the example in Figure 2. Provisioning and lifecycle management of these standardized services (e.g. scaling out of the application components, change requests, de-provisioning) can be fully automated, accelerating IT service delivery and eliminating error-prone operations, that translates into reduced operational costs and improved end-user experience.

Figure 2 Sample self-service catalog configured within vRealize Automation



With built-in orchestration and a rich choice of pre-defined plugins, automated workflows can be built to integrate the platform with the external environment, including backup, configuration management, CMDB, service desk systems, and other ITSM tools. By leveraging orchestrator workflows, it is possible to define and expose XaaS (anything-as-a-service) in the self-service catalog. All of these services can be consumed by end-users via a web-based portal, or by developers through the API or CLI.

vRealize Automation policies provide governance for the IT services being offered via the platform. The service catalog can be customized, making sure that the services are only exposed to appropriate users and groups. Reservation policies can be used to prioritize the assignment of infrastructure resources and stay below quotas and to alert administrators when approaching defined thresholds. Multiple levels of approval policies can be defined for request approval from both business (cost) and technical (configuration) perspectives, eliminating potential VM-sprawl enabled by the self-service automated consumption.

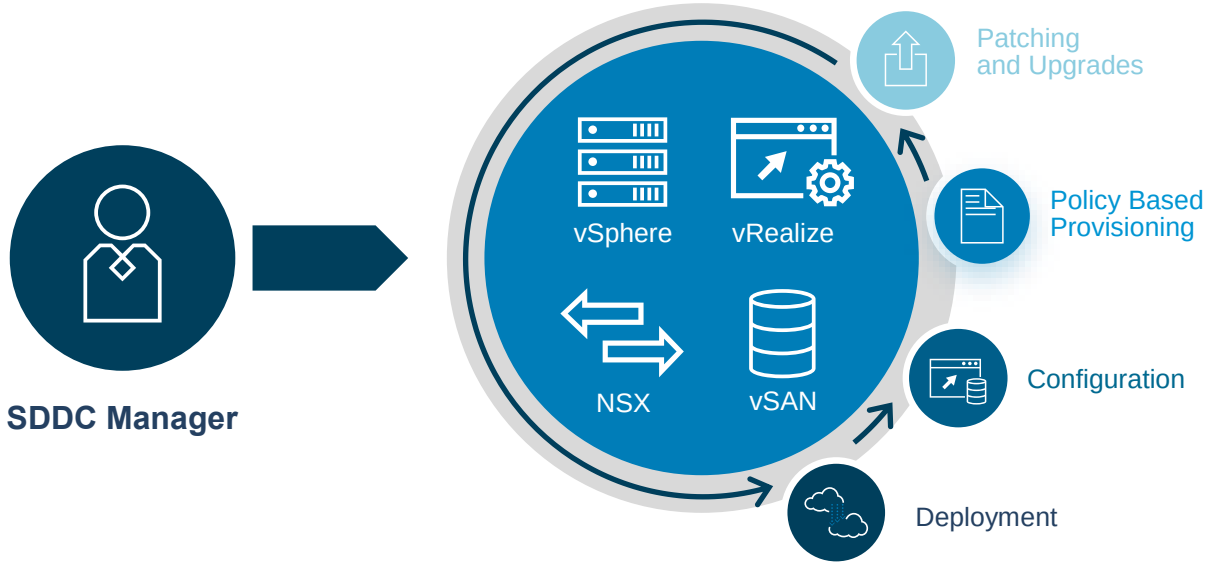
It's worth noting, that the orchestration capabilities provided by vRealize Automation are focused more on workloads and integration with the external environment, enabling end users to consume these as services and at scale.

2.1.2 SDDC platform automation

Managing and updating of a software-defined data center, especially at a large scale, may become a challenge. Customers, who value fully automated approach to lifecycle management of the entire SDDC stack, can benefit from SDDC Manager™, which is an optional component.

SDDC Manager and vRealize Automation orchestrate different aspects of building and running SDDC or private and public clouds. SDDC Manager automates the installation and lifecycle management of the vSphere, vSAN, and NSX from bring-up and configuration to patching and upgrading, making it simple for the administrators to build and maintain the SDDC. It also automates the installation and configuration of vRealize Suite components.

Figure 3 SDDC Manager - automation of day 0 to day 2 operations



2.1.3 Security

Security is historically one of the top concerns of organizations adopting a cloud operating model. VMware SDDC provides a holistic approach to security, which exceeds the capabilities typically found in a traditional data center architecture, very often dependent on perimeter security. In a diverse traditional infrastructure environment, it is challenging to maintain consistent operations and compliance. vRealize Automation, used in

conjunction with NSX, automates an application's network connectivity, security, performance, and availability.

Network virtualization provided by NSX decouples the workloads from the underlying physical infrastructure by leveraging a network overlay technology and moves the intelligence of the network from hardware to software. A key innovation of NSX is the ability to provide network and security functions, such as switching, routing and firewalling in a distributed fashion across all hosts and within the kernel-level module of the hypervisor.

One of the great benefits provided by this approach is an enhanced distributed security model, where security policies are applied closer to the workload, using virtualization-aware, higher-level security constructs, and where security policies move with the workload. NSX helps to segment the environment, decreasing risk and the attack surface while increasing the security.

NSX **micro-segmentation** is a specific security capability that decreases the level of risk and increases the security posture of a data center. It is achieved with a distributed stateful firewalling, implemented at the kernel-level of the hypervisor and distributed across all hosts in the environment. Security policies are applied at the vNIC level, independently from the underlying physical network topology, with per-workload granularity. A grouping construct called Security Group can be leveraged to dynamically identify workloads based on matching criteria, such as VM name, Security Tag, OS type, Active Directory group, etc. Especially helpful is that when workloads are moved between hosts, the security policies automatically move with the workloads.

The IT administrator can define vRealize Automation application blueprints that specify NSX security policies that contain firewall rules, intrusion detection integration, and agentless anti-virus scanning at each application tier to allow application and per-tier security. Deploying network security at the application level or between application tiers to ensure that firewall rules are placed as close to the virtual machine as possible provides a true defense-in-depth solution that was too expensive and difficult to implement for a transitional hardware-based infrastructure.

vRealize Automation provisions, updates and decommissions network and security services in lockstep with virtualized applications. Network and security services are deployed as part of the automated delivery of the application, consistent with its connectivity, security, and performance requirements.

2.1.4 Hybrid cloud ready

VMware SDDC can be deployed as a private cloud on premises or off-site using secure infrastructure-as-a-service (IaaS) operated by VMware or VMware certified partners.

Customers can build a true hybrid cloud, by integrating their private cloud with VMware Cloud® on AWS. With Hybrid Linked Mode a VMware Cloud on AWS vCenter Server instance can be linked with an on-premises VMware vCenter® Single Sign-On domain. Once linked the inventories of both vCenters can be viewed and managed from a single vSphere Client interface, and workloads can be easily migrated between them.

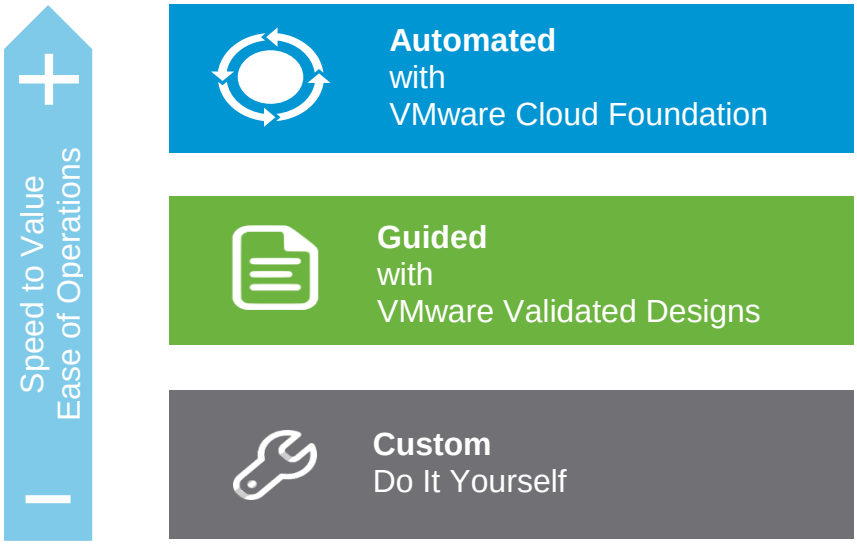
Multiple public cloud providers can be connected to vRealize Automation as endpoints. In this case, the automated service provisioning and basic lifecycle management operations can be extended to popular public cloud IaaS services using the same self-service portal, while maintaining the same governance principles as in the private cloud. This provides greater transparency, increases internal control and eliminates “shadow IT.” The organization IT department can become a service broker for their internal customers, enabling a multi-cloud experience. The VMware vRealize® Business™ for Cloud component, integrated into the same self-service portal, can be used to provide cost transparency and showback.

Additionally, optional NSX Hybrid Connect component improves workload mobility between enterprise sites and VMware Cloud® on AWS. It provides large scale application mobility between sites with secure live migration enabling customers to transform their applications and datacenters more rapidly and securely.

2.2 VMware SDDC architecture approaches

There are three paths to deploy a VMware SDDC as shown in Figure 2.

Figure 4 Three paths to deploy a VMware SDDC



Custom “Do It Yourself”

Custom, one-off design manually documented and maintained by the customer. Customers self-validate product interoperability and manually deploy and maintain individual software components. This approach is recommended for the customer that prefers a completely custom and self-validated design and has strong technical skillsets.

Guided with VMware Validated Designs

VMware Validated Designs (VVDs) are extensively tested, standardized SDDC architectures prescribed by VMware. Customers use guidance from VVD documentation, or contract professional services or certified partners, to deploy the SDDC. VVD codifies VMware best practices into standardized architectural designs. Recommended for the customer that values design customization over out-of-the-box integration and automation, wants flexibility to use vSAN or external storage as the primary storage architecture, and that prefers an incremental, component-based approach to adopting the SDDC.

Automated with VMware Cloud Foundation

VMware Cloud Foundation is an integrated SDDC platform with built-in lifecycle automation for the software stack. Cloud Foundation automatically deploys a standardized SDDC architecture in accordance with a VVD. It builds on VVD with lifecycle automation in a fully integrated SDDC platform. Recommended for the customer that desires an out-of-the-box private/hybrid cloud user experience, wants hyper-converged infrastructure as the primary storage architecture and puts greater value on automation and ease of use over design customization.

2.3 VMware Validated Designs (VVD)

This whitepaper focuses on VVD on VxRail as the solution that provides the best combination of design flexibility, integration, automation and speed of deployment for most customers. It is helpful to better understand VMware Validated Designs, before exploring the VxRail hardware and added software automation value. More detailed information on the VMware products can be found in Appendix B, VMware SDDC product details.

VMware Validated Designs (VVD) simplify the process of deploying and operating an SDDC. They are comprehensive, solution-oriented designs that provide a consistent and repeatable production-ready approach to the SDDC. By definition, they are prescriptive blueprints that include comprehensive deployment and operational practices for the SDDC.

A VMware Validated Design is composed of a standardized, scalable architecture backed by VMware's technical expertise and a software bill of materials (BOM) comprehensively tested for integration and interoperability that spans compute, storage, networking and management. Detailed guidance that synthetizes best practices on how to deploy, integrate and operate the SDDC is provided to aid end users to achieve performance, availability, security and operational efficiency.

2.3.1 Standardized data center level design

Instead of addressing elements in the SDDC stack individually, VMware Validated Designs look at how all components – compute, storage, networking, operations, management, data protection, recovery and extensibility – are used together to design the most optimal solution for the SDDC based on the specific capabilities and objectives in each design.

For each version of VMware Validated Designs, the BOM lists the exact version of the individual component software. In addition to the foundational components listed earlier (vSAN, NSX and vRealize Suite) VMware Site Recovery Manager™ and VMware vSphere® Replication™ provide disaster recovery functionality if required. As an example, Table 1 displays an example BOM for a VVD for an SDDC release (version numbers have been left out for simplification purposes).

Table 1 Example VVD Software BOM

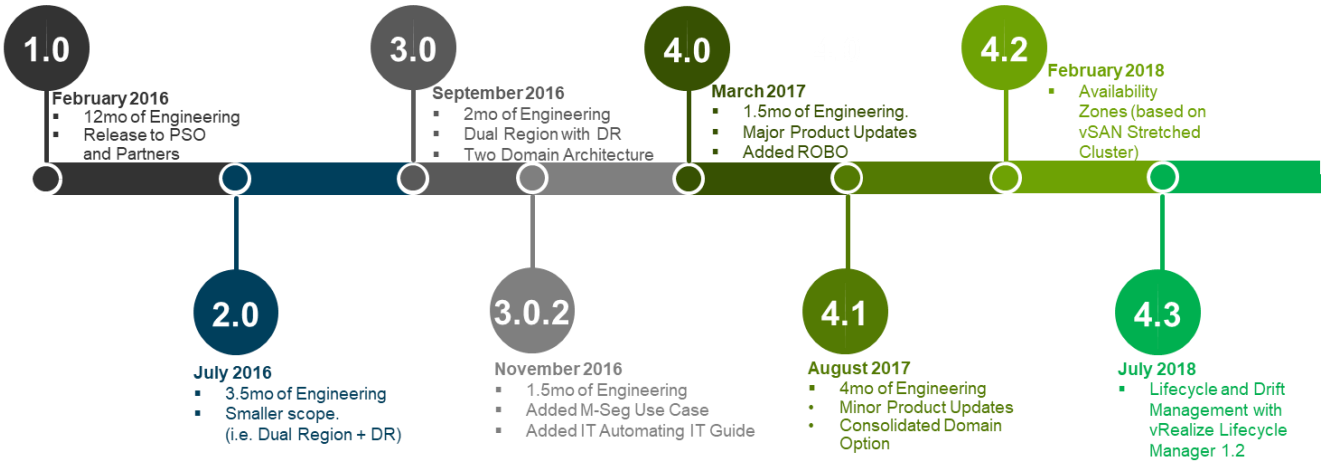
Product Group and edition	Product name
VMware vSphere® Enterprise Plus Edition™	VMware ESXi®
	VMware vCenter Server® Appliance™
	VMware vSphere® Update Manager™
	VMware vSphere Replication
VMware vSAN Standard or higher	VMware vSAN
VMware NSX® Data Center Advanced or higher	NSX Data Center for vSphere
VMware vRealize Suite Lifecycle Manager	VMware vRealize Suite Lifecycle Manager
VMware vRealize® Operations Manager™ Advanced or higher	VMware vRealize Operations Manager
	Management Pack™ for NSX for vSphere
	Management Pack for Storage Devices
	Management Pack for Site Recovery Manager
VMware vRealize® Log Insight™ VMware vRealize® Log Insight™ Content Pack™	vRealize Log Insight
	Content Pack for NSX for vSphere
	Content Pack for vRealize Automation
	Content Pack for vRealize Orchestrator
	Content Pack for vRealize Business
	Content Pack for Microsoft SQL Server
	Content Pack for Linux
	Content Pack for Site Recovery Manager
VMware vRealize Automation Advanced or higher	vRealize Automation
VMware vRealize® Business™ for Cloud Advanced	vRealize Business for Cloud
VMware Site Recovery Manager Enterprise	Site Recovery Manager

2.3.2 Proven and robust designs

Each design is developed by experts and rigorously tested and validated to ensure successful deployment and efficient operations. These experts include VMware engineering teams and resources from professional services, engineering and global support. These experts have produced designs that ensure an SDDC that follows the designs will be architected in the best, most supportable way.

Unlike most reference architecture and designs that are frozen in a single point-in-time, VMware Validated Designs are continuously updated and re-validated. As VMware releases new versions, updates, patches and even new capabilities in components of the SDDC, these updated and new products must be tested to ensure that the design remains completely validated. If the design must change, the needed changes must come with a transitional process to help customers rapidly assimilate the updated design. VMware's interoperability testing ensures that a validated design stays valid as subsequent versions of component products are released.

Figure 5 VMware Validated Designs progression over time



The first version of VMware Validated Designs was released in February 2016 after 12 months of intense engineering work. VMware Validated Designs have matured to support a much broader set of use cases and offer enterprise-class features, such as disaster recovery and stretched clusters. The 4.3 version released in July 2018 provides significant simplification of the vRealize Suite deployment with vRealize Suite Lifecycle Manager.

2.3.3 Applicable to a broad set of scenarios

VMware Validated Designs provide an agile platform to achieve a wide variety of outcomes delivered by the SDDC. The SDDC shifts an organization's focus towards use-cases and away from the products needed to support the data center solution. VMware Validated Designs are a critical part of that shift. These designs are available in a variety of scenarios including SDDC, IT Automating IT, Intelligent Operations and Remote Office Branch Office (ROBO). They provide the guidance to achieve a wide variety of desired IT outcomes delivered by the SDDC, including application security, IT automation, monitoring and alerting, high availability and disaster recovery.

2.3.4 Comprehensive documentation

VMware Validated Designs provide the most comprehensive set of prescriptive documentation for customers and partners to build an SDDC.

The VMware Validated Designs are captured in a set of documents that describes the design objectives, architecture design decisions, software bill of materials, as well as the best practices on how to deploy, integrate and operate the SDDC in a single or dual-region environment.

Unlike the vast majority of publicly available reference architectures, VVD includes extensive guidance for day two operations, which is critical to customers. Within VVD customers can find the operational guidance for basic operational tasks like start up and shut down of the complex SDDC, how to monitor and how to perform maintenance. More complex operational tasks are also included, like business continuity operations, how to perform upgrades from the previous to the current version and troubleshooting.

The full set of VMware Validated Designs is available at vmware.com/go/vvd

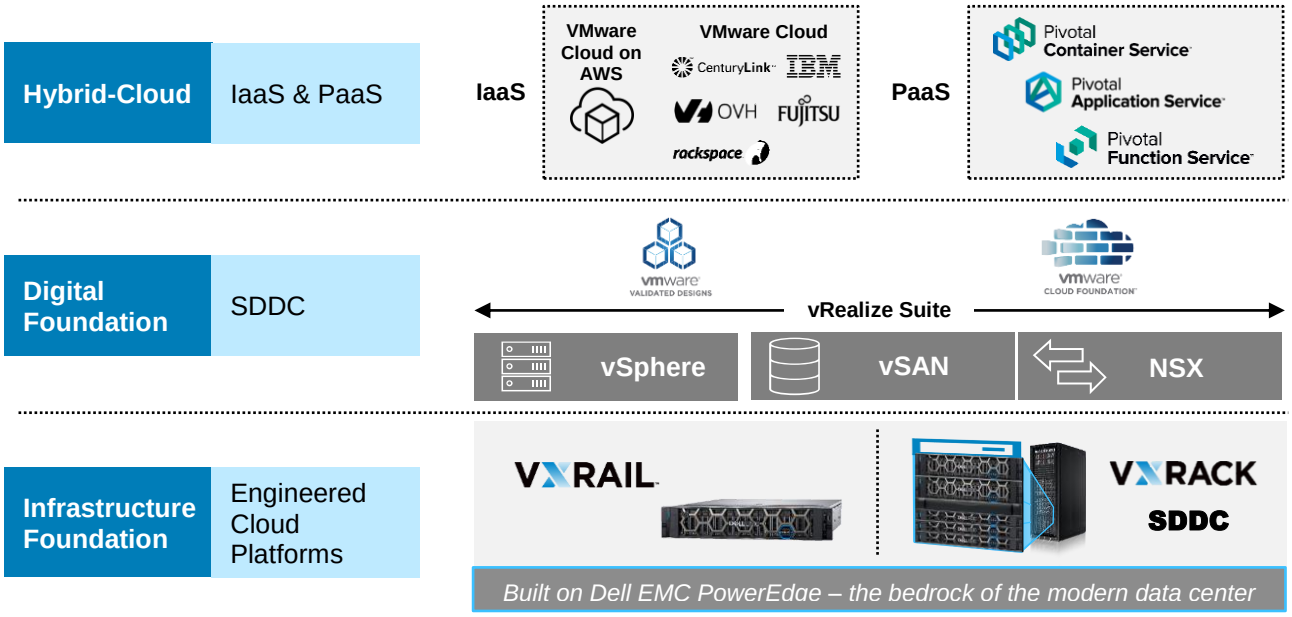
3 VVD on VxRail

3.1 Accelerate journey to the VMware hybrid cloud with Dell EMC

Dell EMC offers a full range of cloud platforms to accelerate digital business transformation with less risk and greater savings. Dell EMC offers varying levels of a pre-engineered solution for VMware, Pivotal and Microsoft-based cloud solutions. Dell EMC's best-of-breed hardware is combined with the right level of integration, tooling and documentation to accelerate time to results, simplify daily operations and achieve greater levels of efficiency and transparency. The customer can choose the platform that is most suitable for their IT environment, depending on the actual requirements and preferred technology of the cloud stack.

For customers that choose VMware as the primary technology for modernizing their data center or building a multi-cloud IT environment, Dell EMC offers a broad choice of solutions, shown in Figure 6 below.

Figure 6 Dell EMC VMware cloud products positioned by increasing cloud maturity and speed-to-cloud



All on-premises solutions are based on Dell EMC PowerEdge servers.

For customers wanting the consume approach using integrated HCI infrastructure, there is VxRail. VxRail is Dell EMC's leading hyper-converged solution and the only vSAN-powered appliance jointly engineered with VMware. Innovation with leading edge technologies is ongoing to make VxRail even more flexible and powerful. Customers can build their own SDDC using the VMware Validated Designs documentation and VxRail as the compute and storage platform. Building an SDDC can be simplified and accelerated by using Dell EMC VVD on VxRail configurations certified to the latest VVD versions with additional Dell EMC features and services.

VxRack™ SDDC is a complete, turnkey, rack-scale HCI system running the complete VMware Cloud Foundation stack (vSphere, vSAN, NSX, vRealize Suite and SDDC Manager) for the fastest and easiest path to implementing an SDDC. VxRack SDDC does not offer the full flexibility of configurations available with VVD on VxRail such as choice of networking as an example. These options have been pre-selected in order to achieve a more turnkey outcome.

If the customer wants any of the following features, VVD on VxRail is the best solution:

- Distributed multi-site architecture with multi-cluster workload domains
- Multi-site use cases: DR or stretched clusters
- VxRail cluster-level hardware/software lifecycle management (LCM)
- Network flexibility for a distributed multi-site VVD architecture

See appendix B.2.1 VVD multi-region architecture and B.2.2 Availability zones (vSAN stretched cluster) for more information.

3.2 Why Dell EMC VxRail Appliance is the platform of choice for VVD

VxRail Appliances are jointly engineered by Dell EMC and VMware and are the only fully integrated, preconfigured and tested HCI appliance powered by VMware vSAN technology for software-defined storage. Managed through the industry-standard VMware vCenter Server interface, VxRail provides a familiar vSphere experience that enables streamlined deployment and the ability to extend the use of existing IT tools and processes. Starting with ESXi 6.7U1, synchronous releases between VxRail and VMware will speed time to value with adoption of latest VMware releases very quickly (VVD on VxRail follows the VVD BOM update timeline).

VxRail Appliances are fully loaded with integrated, mission-critical data services from Dell EMC and VMware including compression, deduplication, replication and backup. VxRail delivers resiliency and centralized-management functionality enabling faster, better and simpler management of consolidated workloads, virtual desktops, business-critical applications and remote-office infrastructure. As the only HCI infrastructure appliance from Dell EMC and VMware, VxRail is the easiest and fastest way to stand up a fully virtualized VMware environment.

VxRail is the only HCI appliance on the market that fully integrates Intel-based Dell EMC PowerEdge Servers with VMware vSphere and vSAN. VxRail is jointly engineered with VMware and supported as a single product, delivered by Dell EMC. VxRail seamlessly integrates with existing (and optional) VMware eco-system and cloud management solutions, including vRealize, NSX, VMware Horizon® and any solution that is a part of the vast and robust vSphere ecosystem.

Dell EMC Data Protection Suite™ for VMware is an optional data protection solution, available with VxRail, enabling the SDDC with additional, more granular data protection capabilities. Tight integration into VMware delivers simplified deployment and administration. It is available as a software-only solution. The suite provides backup and recovery, continuous data protection for any point-in-time recovery, backup to the cloud, proactive monitoring and analysis, as well as search capabilities. See Appendix C Optional VMware integrated data protection options, to learn more about this and other Dell EMC data protection options.

3.2.1 VVD on VxRail certification

Dell EMC has completed the first certification process for the VMware Validated Design (v4.2) Certified Partner Architecture on the Dell EMC VxRail 4.5 based on PowerEdge 14g. This formally certifies that the VxRail architecture designs and best practices align with the VMware Validated Designs and best practices. Dell EMC committed to certify future releases on VxRail, including currently available VVD v4.3.

There is significant additional value that Dell EMC brings with the certification of VVD on VxRail:

- **BOM alignment** – Dell EMC ensures consistent alignment between VVD BOM and VxRail software releases, to make sure VVD can run on VxRail as the infrastructure platform without any issues.

- **End-to-end validation of VVD deployment on VxRail** for each of the following topologies: Single Region, Dual Region, Multiple Availability Zones. For all of these topologies, Dell EMC creates a VxRail-specific deployment documentation. Dell EMC also prepares the upgrade guidance to the latest VVD release.
- **New VVD features assessment** – Dell EMC Engineering makes the assessment of the new features in each subsequent release for their impact and possible validation and inclusion in VVD on VxRail, examples include Multi-AZ in VVD 4.2 and vRSLCM support in VVD 4.3.
- **VxRail software feature enhancements** – Dell EMC implements software feature enhancements in VxRail software to streamline VVD deployment and operations on VxRail. Examples include vCenter externalization utilities and UI enhancements.

The Dell EMC VxRail team published the following documents to support the VMware certification of the VxRail into the VMware Validated Design program:

- SolVe document highlighting the process to deploy the VxRail in a configuration compatible with the VMware Validated Design. This document is SolVe Internal and Partner accessible. SolVe is the procedure generator used by Dell EMC services and partners deploying the VxRail.
- Dell EMC versions of the *VMware Validated Design Deployment Guides* that highlight how to properly deploy the components of the VMware Validated Design on a VxRail. These documents are posted publicly at Dell EMC Community Network (https://community.emc.com/docs/DOC-66332).

3.2.2 VxRail software

While the VxRail hardware helps differentiate the VxRail from other HCI solutions, VxRail is a complete appliance that includes software that enables a software-defined data center. The VxRail Appliance is architected with a software stack for appliance management, virtualization and VM management. The stack comes preinstalled and simply requires running a configuration wizard on site to integrate the appliance into an existing network environment. VxRail Manager is included for appliance management, operations and automation. The VMware virtualization and virtual-infrastructure management software includes vCenter Server, vSphere ESXi, vSAN and vRealize Log Insight.

The base VxRail includes two data protection options: RecoverPoint for Virtual Machines and vSphere Replication. These are included in the price of the appliance and can be activated in the VxRail Manager user interface. See appendix C.1.1 Dell EMC RecoverPoint for Virtual Machines for more information.

VxRail Manager, the VxRail management platform, is the appliance hardware lifecycle management and serviceability interface for VxRail clusters. It is a strategic advantage for VxRail and further reduces operational complexity. No build-it-yourself HCI solution provides this level of lifecycle management, automation and operational simplicity.

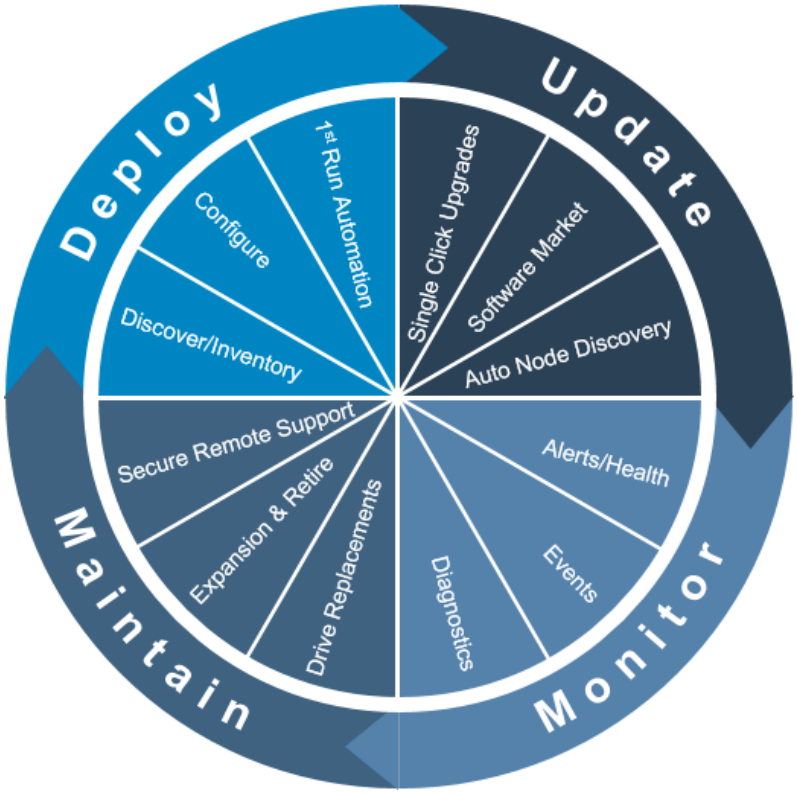
3.2.3 VxRail Manager

VxRail Manager provides out-of-the-box automation and orchestration for day 0 to day 2 appliance-based operational tasks, which reduces the overall IT operating expense required to manage the stack. With VxRail Manager, upgrades are simple and automated with a single-click, bringing the system from one good known state to the next, including all managed software and hardware component firmware. There is no need to verify hardware compatibility lists, run test and development scenarios, or sequence and trial upgrades. VxRail Manager also provides monitoring with dashboards for health, events and detailed physical node views.

Customers, who deploy VVD on VxRail can greatly benefit from the automated lifecycle management, simplified deployment and support experience offered by VxRail Manager.

All virtualization management is performed using the familiar vSphere vCenter interface. VxRail Manager is used for all stages of lifecycle management: deploy, update, monitor and maintain as shown in Figure 7.

Figure 7 VxRail Manager



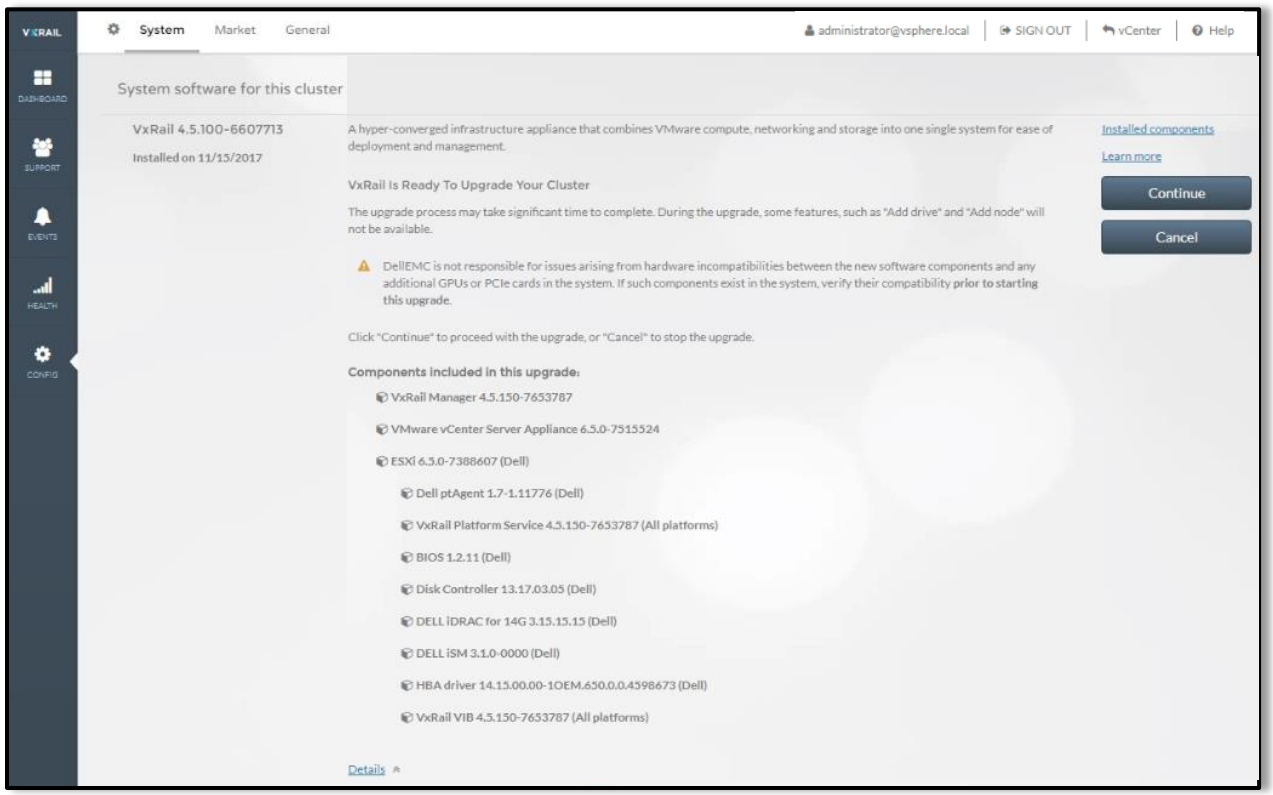
VxRail Manager features a user-friendly dashboard for automating VxRail deployment and configuration and for monitoring the health of individual appliances and individual nodes in the cluster. VxRail Manager is preinstalled on the VxRail Appliance as a single VM and it can be accessed by pointing a browser at the VxRail Manager IP address or the DNS host name. File-based back-ups of VxRail Manager help ensure business continuity in the rare event the VxRail Manager VM need to be rebuilt.

The VxRail Manager dashboard displays storage, CPU and memory utilization at the cluster, appliance and individual-node level. It also incorporates functionality for hardware serviceability and appliance platform lifecycle management. For instance, it guides system administrators through adding new appliances to an existing cluster and it automatically detects new appliances when they come online. VxRail Manager is also used to replace failed disk drives without disrupting availability, to generate and download diagnostic log bundles and to apply VMware updates or software patches non-disruptively across VxRail nodes.

VxRail Manager lifecycle management includes VxRail hardware firmware, VMware vSphere and vSAN. Other VMware software, such as NSX and vRealize Suite components, are not included. Starting with VVD version 4.3, vRealize Suite components lifecycle management is performed by the vRealize Suite Lifecycle Manager (vRSLCM). In this initial release of vRSLCM as a part of VVD, it offers the automated deployment of vRealize Suite, but not yet the upgrade.

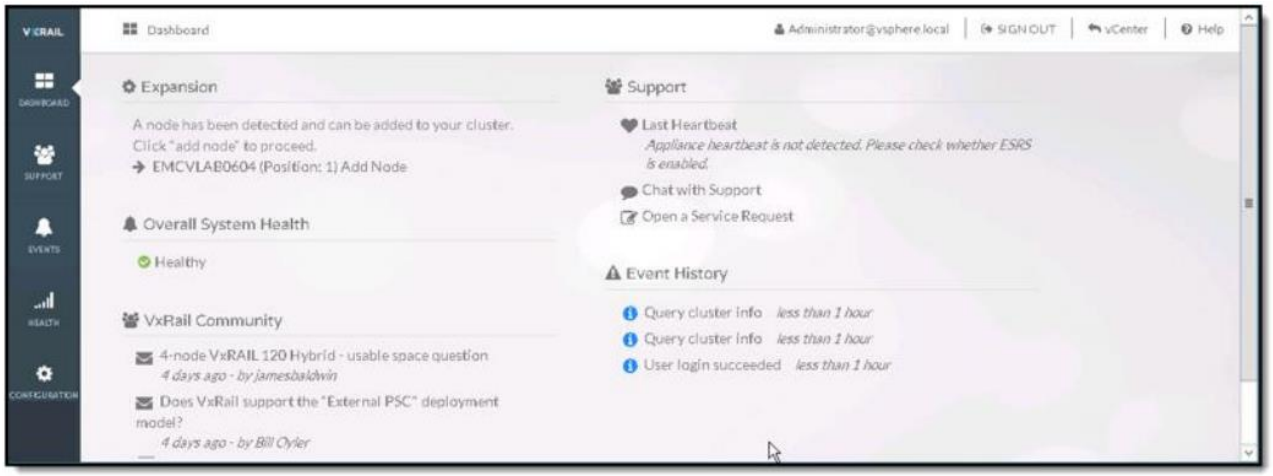
A screen from the upgrade lifecycle management process performed by VxRail Manager is shown in Figure 8.

Figure 8 VxRail Manager upgrade process screenshot



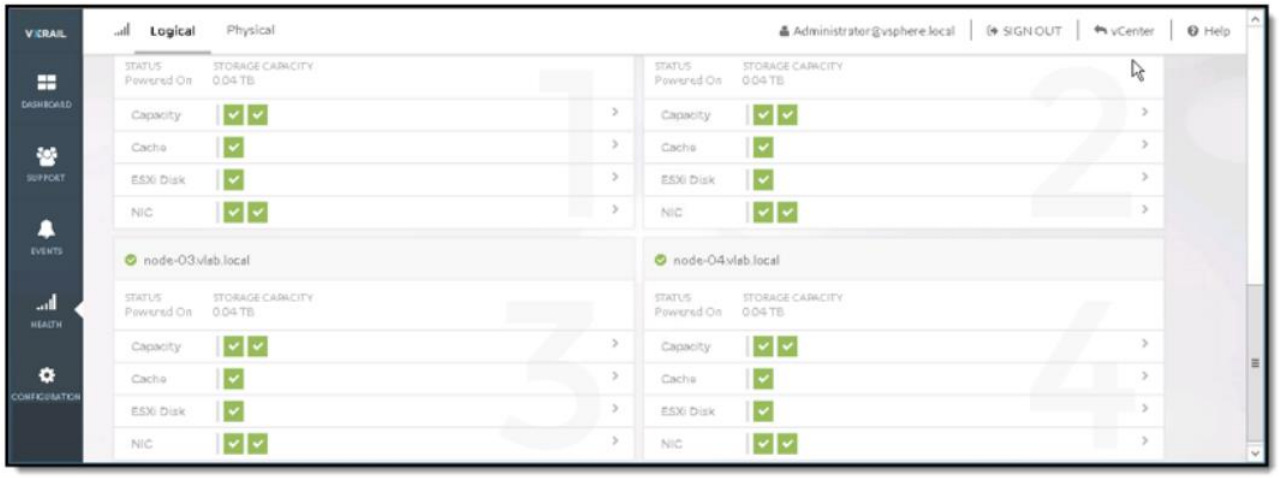
The VxRail Manager main dashboard, shown in Figure 9, displays the current status of overall system health.

Figure 9 VxRail Manager main dashboard



From the Health tab, administrators can access real-time system health details for both logical and physical resources and can view and analyze resource operability, performance and utilization data as shown in Figure 10.

Figure 10 VxRail Manager Health tab for logical resources



VxRail also leverages VMware vRealize Log Insight to monitor system events and provide ongoing holistic notifications about the state of the virtual environment and appliance hardware. It delivers real-time automated log management for the VxRail Appliance with log monitoring, intelligent grouping and analytics to provide better troubleshooting at scale across VxRail physical, virtual and cloud environments. Furthermore, VxRail Manager simplifies appliance platform lifecycle management by delivering patch software and update notifications that can be automatically installed without interruption or downtime.

The VxRail Manager Support tab provides access to Dell EMC Software Remote Services (SRS), including online chat support and opening a service request. The Support tab also provides links to VxRail Community pages for Dell EMC Knowledgebase articles and user forums for FAQ information and VxRail best practices. Figure 11 shows an example of the support view.

Figure 11 VxRail Manager Support tab

VxRail Manager provides access to a digital market for finding and downloading qualified software packages such as Data Domain® Virtual Edition, RecoverPoint for VM, VMware vSphere® Data Protection™ and other software options for VxRail Appliances.

3.2.4 VxRail flexible hardware configurations

While the VVD provides guidance for compatible hardware, it does not lock customers into fixed configurations. VxRail nodes are available with different compute power, memory and cache configurations to closely match the requirements of new and expanding use cases. As requirements grow, the system easily scales out and scales up in granular increments.

Dell EMC delivers the #1 hyper-converged infrastructure portfolio purpose-built for HCI with the newest 14th-generation Dell EMC PowerEdge server platform. This portfolio delivers tailor-made performance and reliability powerful enough for any workload, combined with an advanced approach to intelligent deployment and operations that simplify and accelerates IT. Dell EMC HCI on next gen PowerEdge servers are powerful and purposeful and hyper-converged platforms that provide the ideal foundation for software-defined data center initiatives.

With up to 150 customer HCI requirements built-in, PowerEdge servers are designed specifically for and tailored to HCI workloads that depend on both servers and storage. This results in a more consistent, predictable and reliable high-performing HCI that can meet any use case. With a comprehensive portfolio, Dell EMC can deliver the best fit for organization specific HCI needs – from workload requirements, to customer environment/standardization, to deployment preferences.

Dell EMC leads in hyper-converged sales with over 30% market share according to IDC[3]. More customers are choosing Dell EMC HCI over all others. Dell EMC PowerEdge is the world's bestselling server. Industry-leading Dell EMC HCI built on industry-leading PowerEdge, coupled with a single point of support and full lifecycle management for the entire system, makes for a winning solution.

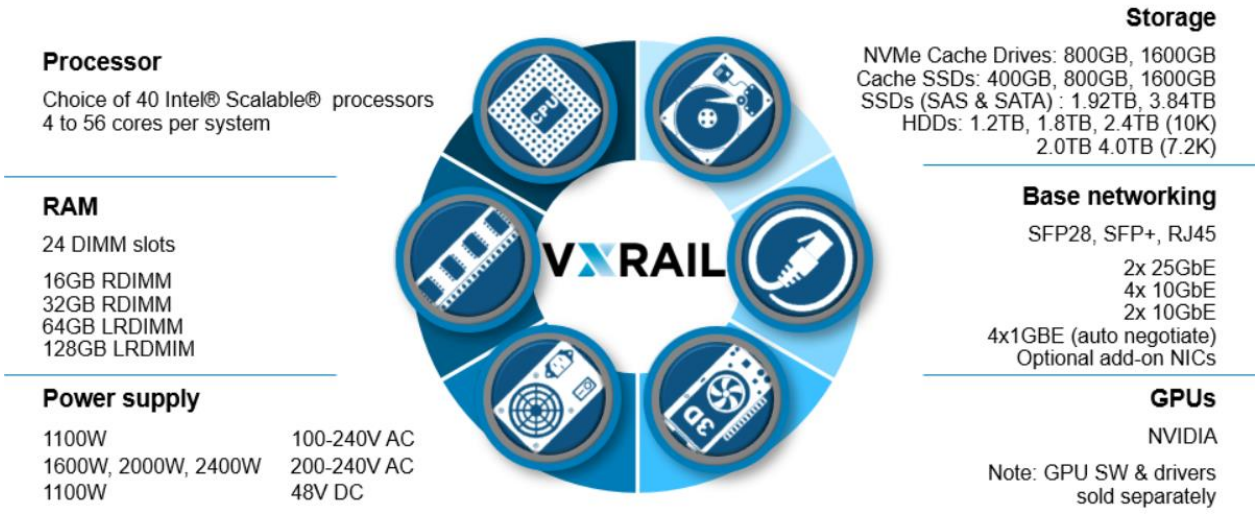
VxRail environments are configured as a cluster, with each node containing internal storage drives. VxRail systems are delivered with the software loaded, ready to attach to a customer-provided network. While most environments use 10Gb Ethernet for internal and external communications, 25Gb or 1Gb Ethernet connectivity is also available. Using a simple wizard at the time of install, the system can be configured to match unique site and networking requirements.

Dell EMC VxRail Appliances offer a choice of Dell EMC PowerEdge servers, powered by new Intel® Scalable® processors, variable RAM and storage capacity, allowing customers to purchase what they need now. Single-node scaling and storage capacity expansion provide a predictable, "pay-as-you-grow" approach for future scale up and out as business and user requirements evolve.

Figure 12 shows the comprehensive set of options available across the family. Customers can be assured their VxRail is configured to best match their workload requirements in a very prescriptive manner, with millions of possible configuration combinations in the VxRail Appliance Series. More information on VxRail hardware configurations is available in the Dell EMC VxRail Appliance TechBook[4].

[3] Based on IDC converged Tracker Q1 2018, June 2018
[4] https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/h15104-vxrail-appliance-techbook.pdf

Figure 12 Component options available across the VxRail Appliance.



VxRail's automated lifecycle management enables scale out where new appliances can be added non-disruptively and different models can be mixed within a VxRail cluster. By adding the latest technology appliances into existing clusters and decommissioning aging appliances, an evergreen HCI environment can be obtained; no need to worry about costly SAN data migrations ever again. Flexible storage options also allow a node to start with a few drives and add drives as capacity requirements grow. Appliances may also be scaled-up where the VxRail nodes can be non-disruptively upgraded with additional memory, GPU, NIC cards, cache SSD and capacity drives to meet changing requirements. Single-node scaling and expansion provide a predictable, "pay-as-you-grow" approach for future scale up and out as business and user requirements evolve.

3.2.5 Dell EMC Fabric Design Center support for VxRail

With very flexible, customer selectable network options, VxRail network design has been a manual process. Network infrastructure is critical for the high-performance access, delivery and response times needed in VxRail environments. Despite documentation, the network continues to be prone to configuration and management issues.

With the introduction of VxRail 4.7 and Dell EMC Networking OS10 Enterprise Edition SmartFabric Services, Dell EMC simplifies the process of VxRail fabric creation, administration and operation:

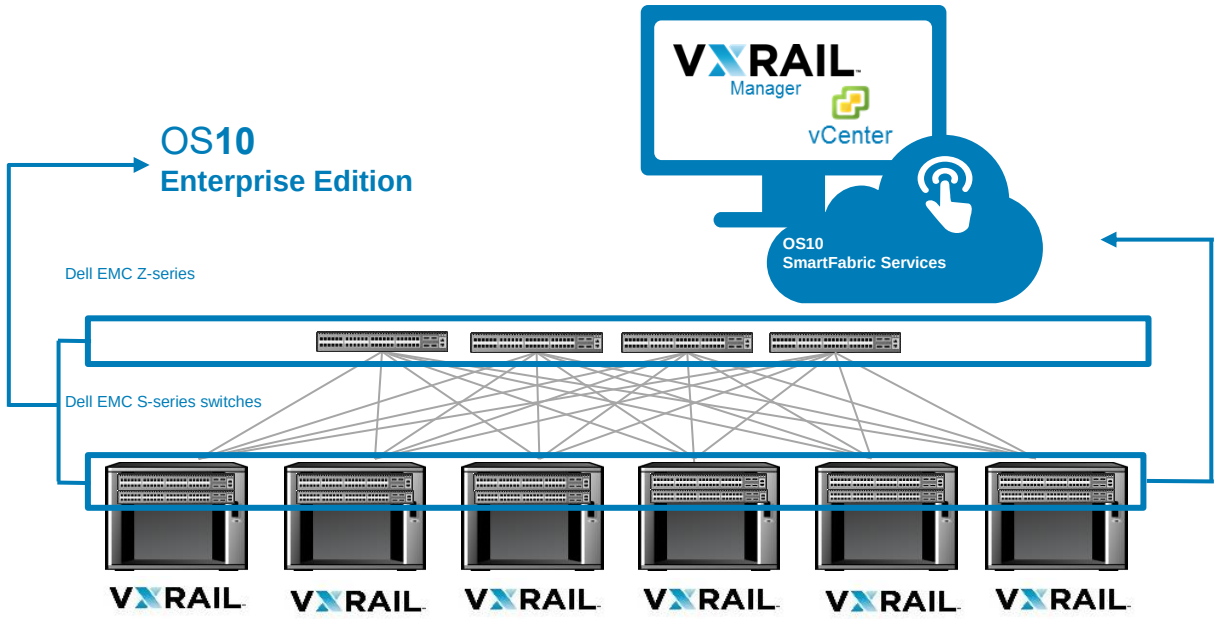
- **Dell EMC Validated Deployment Guides**: Customize fabrics for DIY IT based on prescriptive guidance provided by Dell EMC.
- **Dell EMC Fabric Design Center (FDC)**: Design and deploy fabrics faster by customizing fabrics based on the Dell EMC-provided fabric design wizard. This network design customization and configuration tool accelerates time to value, automates network deployment, offers faster time to production and provides an interoperable network fabric sized specifically for the environment.
- **Dell EMC SmartFabric Services**: Automate fabric creation and operation by leveraging Dell EMC Open Manage Network Integration and VxRail Manager.

VxRail is the first HCI appliance with network configuration automation with SmartFabric services for VxRail:

- Form VxRail clusters automatically: There is awareness between VxRail and the switch. For example, the switch will detect VxRail during installation and allows the user to create one or more clusters with the detected nodes on the same fabric.

- Operate networks as HCI user, through VxRail Manager: Once the cluster has formed, the user performs normal operation through VxRail Manager, available directly in vCenter.
- Elastic network provisioning: SmartFabric Services is automatically aware of required network changes through a vCenter plugin, so the network dynamically responds to VM changes.
- Integrated with VMware applications: Visibility and control through vCenter and vRealize Suite.
- Enhanced support experience: World class Dell EMC HCI and fabric services; Fabric integrated into VxRail services and support experience.

Figure 13 SmartFabric services for VxRail



Note: The currently available VVD 4.3 on VxRail release has been certified on VxRail software 4.5.225. With this release, customers can benefit from Dell EMC Fabric Design Center for simplified design and deployment of the network fabric. In order to fully benefit from the SmartFabric services, customers would have to deploy a VVD release certified on 4.7.x VxRail software.

3.2.6 Dell EMC support

With VVD on VxRail, the support model provides Dell EMC support for all components on the VxRail that are deployed, managed and lifecycled by VxRail Manager. All software VMware components that are not under management by VxRail Manager (including vCenter) are supported by VMware.

The optional data protection components, such as Dell EMC Avamar, Dell EMC RecoverPoint for VMs are covered by Dell EMC product support.

Enterprises need unwavering support for hardware and software and a smart way to manage the mix of vendors in the data center. Dell EMC ProSupport for Enterprise offers a single source with the expertise, know-how and capabilities to deliver world-class support.

ProSupport offers highly trained experts around the clock and around the globe to address IT needs, minimize disruptions and maintain a high level of productivity. With over 55,000 Dell EMC and partner professionals across 165 countries speaking more than 55 languages, Dell enables organizations to:

1. Maximize productivity by leveraging Dell EMC scale and skill
2. Minimize disruptions with around the clock access to highly trained experts
3. Gain efficiency through a single source for all support needs

Single source, 24x7 global support is provided for VxRail Appliance hardware and software via phone, chat, or instant message. Support also includes access to online support tools and documentation, rapid on-site parts delivery and replacement, access to new software versions, assistance with operating environment updates and remote monitoring, diagnostics and repair with Dell EMC Secure Remote Services (SRS).

Dell EMC's 12 Centers of Excellence and Joint Solution Centers deliver in-house collaboration and industry-leading levels of support, leveraging Dell EMC's alliances with leading application providers such as Oracle and Microsoft. Dell EMC's 87 technical support sites are comprised of 71 Dell Tech Support Sites and 16 Dell EMC Customer Service Centers.

3.2.6.1 Secure Remote Services (SRS)

Secure Remote Services is a highly secure, two-way remote connection between the customer's Dell EMC products and Dell EMC Customer Support that helps customers avoid and resolve issues much faster. Secure Remote Services is completely virtual and offers flexibility for enterprise environments of any size. Secure Remote Services is available at no additional cost with an active ProSupport Enterprise or warranty contract.

Secure Remote Services delivers a wide range of benefits and services:

- Proactive wellness monitoring and issue prevention.
- Automated issue detection, notification and case creation for quicker uptime.
- Predictive, analytics-based recommendations through MyService360 and product consoles.

The Secure Remote Services lifeline is a heartbeat that pulses outbound from the Secure Remote Services gateway to Dell EMC Customer Service in 30-second intervals, providing Dell EMC with connectivity status as well as the status of each product. The heartbeat ensures continuous monitoring, notification and if necessary, proactive remote troubleshooting to ensure high availability of Dell EMC products. As a result, customers experience faster resolution and greater uptime.

In addition to proactive remote support, Secure Remote Services enables a richer Dell EMC online experience through MyService360 and product consoles such as Unity CloudIQ. Using proactive wellness monitoring, Secure Remote Services provides a continuous data feed into the secure Dell Data Lake – sending product-generated alerts and configuration files – ensuring that the data available throughout Online Support, MyService360™, CloudIQ and other product consoles, is up-to-date and high value. Based on this current information, Dell EMC is then able to provide enhanced product and service health recommendations to maximize the Dell EMC investment.

The security of customer data is Dell EMC's top priority. From collection to transport to storage, Secure Remote Services employs multiple security layers throughout each step in the remote connectivity process to ensure that customers and Dell EMC can use the solution with confidence.

3.2.7 Dell EMC Professional Services

Dell EMC Services accelerate VVD on VxRail deployment and helps customers realize the full value of their VxRail platform investment through a full range of services for every stage of solution deployment.

Dell EMC offers ProDeploy installation and implementation services to ensure smooth and rapid integration of VxRail Appliances into customer networks. The standard service, optimal for a single appliance, provides an expert on site to perform a pre-installation checklist with the data center team, confirm the network and top of rack (TOR) switch settings, conduct site validation, rack, cable, configure and initialize the appliance. To complete the deployment, the service technician configures Secure Remote Services (SRS) and conducts a brief functional overview on essential VxRail administrative tasks.

A custom version of this installation and implementation service is available for larger-scale VxRail deployments, including those with multiple appliances or stretched cluster environments. Also offered is VxRail Appliance extended service, which is delivered remotely and provides an expert service technician to rapidly implement VxRail Appliance pre-loaded data services, RecoverPoint for VMs.

Dell EMC Consulting helps clients realize additional platform value with integration of the VMware vRealize Suite, NSX deployments, availability strategies and development of additional service blueprints. Beyond these infrastructure integrations, Dell EMC helps clients to migrate applications, including profiling of applications to determine the best fit for VxRail and the VMware stack. Dell EMC can help customers overcome the common skills and process gaps needed to effectively adopt a flexible cloud operating model. Dell EMC Education Services can help customers improve their skills with Dell EMC platforms, VMware software and IT as a service.

3.2.8 Future-Proof Loyalty Program

The Future-Proof Loyalty Program[5] is a customer-facing program designed to provide investment protection with a set of world class technology capabilities and programs that enable Dell EMC's Storage, Data Protection and VxRail HCI products to provide value for the entire lifetime of our customer's applications. It is available to customers at no additional cost either in terms of higher maintenance price or higher product price.

VxRail participates in the following pillars of the Future-Proof Loyalty program:

- 3 -year satisfaction guarantee
- All-inclusive software
- Hardware investment protection
- Never worry data migrations
- Clear price
- Cloud consumption
- Cloud enablement

[5] https://www.dellemc.com/en-us/storage/future-proof-loyalty-program.htm

3.3 VVD on VxRail hardware architecture

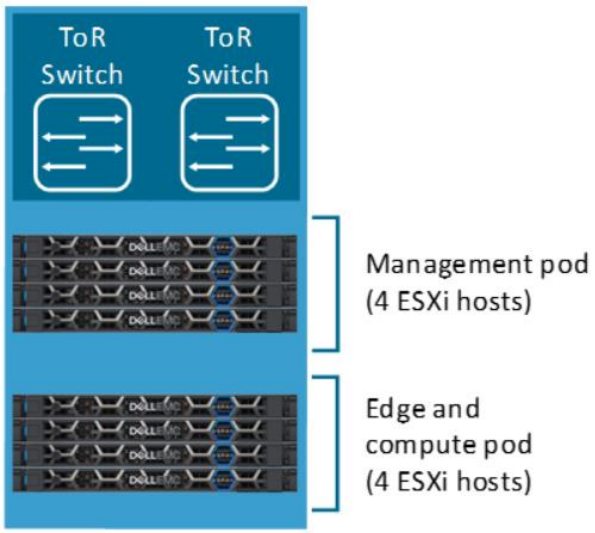
Currently VVD on VxRail supports the standard VVD two-domain architecture design, where the management workloads and compute/edge workloads are segregated (see Appendix B.2 VMware Validated Designs (VVD) technical implementation for more information about VVD workload domains).

Management workloads have their own dedicated VxRail-based vSphere cluster, while the compute/edge reside on a separate VxRail-based vSphere cluster. This two-domain design requires at least eight ESXi hosts, four for management and four for shared compute and edge workloads. The VVD standard architecture supports both single and dual-region deployments. By definition, dual-region deployments have two data centers located in geographically dispersed locations, leveraging vSphere replication and Site Recovery Manager (SRM) to protect the workloads. The architecture also supports multiple availability zones (multi-az), leveraging vSAN stretched clustering to protect against a complete data center (availability zone) failure within a single region. For more details on multi-region and multi-az, please consult appendix B.2.1 and B.2.2 respectively. With custom services, Dell EMC can implement VVD on VxRail in complex, multi-site architectures.

The Management Cluster resides in the management workload domain and runs the VMs of the components that manage the data center, such as vCenter Server, VMware NSX® Manager™, VMware NSX® Controller™, vRealize Operations Manager, vRealize Log Insight, vRealize Automation and other management components. Minimum capacity requirements for the VxRail nodes are shown in Figure 14.

Figure 14 Hardware architecture of VVD on VxRail

Management Cluster (Min 4 Required)	
CPU	2 Socket / 8 Cores
RAM	192 GB
HDD	16 GB SSD for booting 200 GB SSD for the caching tier 2x 1 TB HDD for the capacity tier
NICS	4x10GbE & 1x1GbE BMC
NODE	E or P recommended
Compute/Edge Cluster (Min 4 Required)	
CPU / RAM / STORAGE	
NICS	4x10GbE & 1x1GbE BMC
NODE	Sized based on customer workload



The shared edge and compute cluster resides in the first cluster in the virtual infrastructure workload domain and runs the required NSX services to enable north-south routing between the data center and the external network and east-west routing inside the data center. This shared cluster also hosts the tenant VMs (sometimes referred to as workloads or payloads).

As the environment grows, additional compute-only clusters can be added to support a mix of different types of workloads for different types of service level agreements (SLAs). Requirements for this cluster should be based on the actual capacity requirements for the customer workloads. In general, a single cluster can be scaled out up to 64 nodes and more clusters can be added as needed.

4 Conclusion

With VMware software-defined data center (SDDC), customers can solve the challenge of quickly delivering new innovative applications, while controlling costs, and improving compliance, security and efficiency. They can accelerate the journey to the VMware SDDC with Dell EMC VxRail. Dell EMC provides services and additional automation beyond the self-guided VVD path with a solution that provides the best combination of design flexibility, integration, automation and speed of deployment.

With VxRail Manager, customers can significantly simplify not only the deployment of VMware SDDC on VxRail, but also on-going operations. VxRail greatly simplifies the infrastructure management via automation, lifecycle management (LCM), and configuration flexibility.

Dell EMC is #1 in hyper-converged systems with the newest 14th-generation Dell EMC PowerEdge server platform. VxRail Appliances are jointly engineered by Dell EMC and VMware and is the only HCI appliance currently certified for the VVD.

VxRail nodes are available with different hardware configurations varying the compute power, memory, cache and storage configurations to closely match the requirements of new and expanding use cases. As requirements grow, the system easily scales out and scales up in granular increments.

By deploying VVD on VxRail, customers can accelerate time to market, de-risk deployment and operations, increase efficiency, drive IT agility, operate in confidence and future-proof their infrastructure to get ready for the VMware hybrid cloud. VVD on VxRail enables them to build a multi-cloud environment by integrating multiple public cloud services and providing common operations framework with SDDC built-in cloud management capabilities.

A References

- VMware Software-Defined Data Center (SDDC)
  https://www.vmware.com/solutions/software-defined-datacenter.html

- VMware Validated Designs
  http://vmware.com/go/vvd
  https://www.vmware.com/support/pubs/vmware-validated-design-pubs.html

- VMware vRealize Suite
  https://www.vmware.com/products/vrealize-suite.html
  https://docs.vmware.com/en/vRealize-Suite/index.html

- VMware Cloud Foundation
  https://www.vmware.com/products/cloud-foundation.html
  https://docs.vmware.com/en/VMware-Cloud-Foundation/

- VMware Validated Designs on Dell EMC VxRail VMware KB article:
  https://kb.vmware.com/s/article/54816

- Dell EMC VxRail
  https://www.dellemc.com/en-us/converged-infrastructure/vxrail/index.htm
  https://community.emc.com/community/products/vxrail

- 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 Community Network, VMware Validated Design 4.x on VxRail Deployment Guides:
  https://community.emc.com/docs/DOC-66332

- Dell EMC Data Protection
  https://www.dellemc.com/en-us/data-protection/index.htm

- Dell EMC Online Support site (registration required)
  https://support.emc.com.

B VMware SDDC product details

B.1 VMware common SDDC components

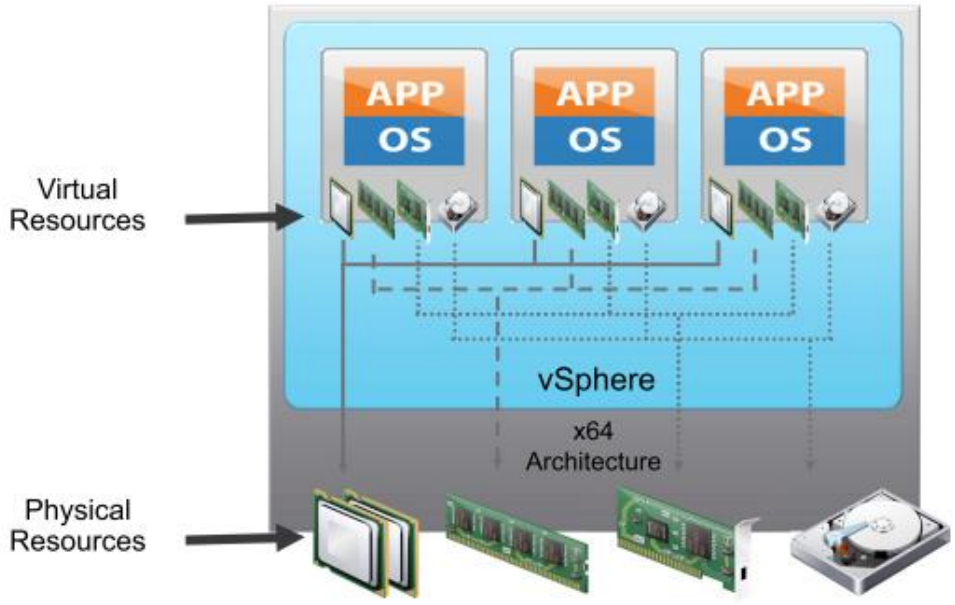
B.1.1 VMware vSphere

The VMware vSphere software suite delivers an industry-leading virtualization platform to provide application virtualization within a highly available, resilient, efficient on-demand infrastructure. ESXi and vCenter are components of the vSphere software suite. ESXi is a hypervisor installed directly onto a physical server node, enabling it to be partitioned into multiple virtual machines (VMs). VMware vCenter server is a centralized management application that is used to manage the ESXi hosts and VMs.

vCenter Server is the centralized console for managing a VMware environment. It is the primary point of management for both server virtualization and vSAN. vCenter Server is the enabling technology for advanced capabilities such as VMware vSphere® vMotion®, VMware vSphere® Distributed Resource Scheduler™ (DRS) and VMware vSphere® High Availability (HA). vCenter supports a logical hierarchy of datacenters, clusters and hosts, which allows resources to be segregated by use cases or lines of business and allows resources to move dynamically as needed. This is all done from a single interface.

VMware ESXi is an enterprise-class hypervisor that deploys and services VMs. Figure 15 illustrates the basic ESXi architecture.

Figure 15 vSphere ESXi architecture



ESXi partitions a physical server into multiple secure, portable VMs that can run side-by-side on the same physical server. Each VM represents a complete system with processors, memory, networking, storage and BIOS. Guest operating systems and software applications can be installed and run in the VM without any modification.

The hypervisor provides physical-hardware resources dynamically to VMs as needed to support the operation of the VMs. The hypervisor enables VMs to operate with a degree of independence from the underlying

physical hardware. For example, a VM can be moved from one physical host to another. Also, the VM's virtual disks can be moved from one type of storage to another without affecting the functioning of the VM.

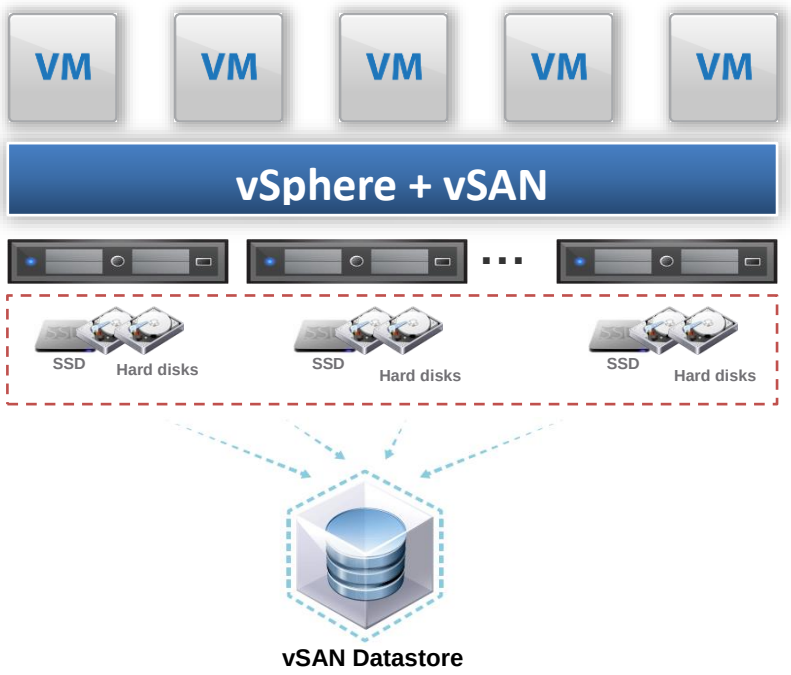
ESXi also isolates VMs from one another. When a guest operating system on a host fails, other VMs on the same physical host are unaffected and continue to run. VMs share access to CPUs and the hypervisor is responsible for CPU scheduling. In addition, ESXi assigns VMs a region of usable memory and provides shared access to the physical network cards and disk controllers associated with the physical host. Different VMs can run different operating systems and applications on the same physical computer.

B.1.2 VMware vSAN

vSAN is VMware's software-defined storage solution built from the ground up for vSphere VMs. It abstracts and aggregates locally attached disks in a vSphere cluster to create a storage solution that can be provisioned and managed from vCenter and the vSphere Web Client. vSAN integrates with the entire VMware stack, including features like vMotion, HA and DRS. VM storage provisioning and day-to-day management of storage service level agreements (SLAs) can be all be controlled through VM-level policies that can be set and modified on-the-fly. vSAN delivers enterprise-class features, scale and performance, making it the ideal storage platform for VMs.

The figure below shows an example of a hybrid configuration where each node contributes storage capacity to the shared-storage vSAN datastore. The SSD drive provides caching to optimize performance and hard disk drives (HDD) for capacity. All-flash configurations (not shown) use flash SSDs for both the caching tier and capacity tier.

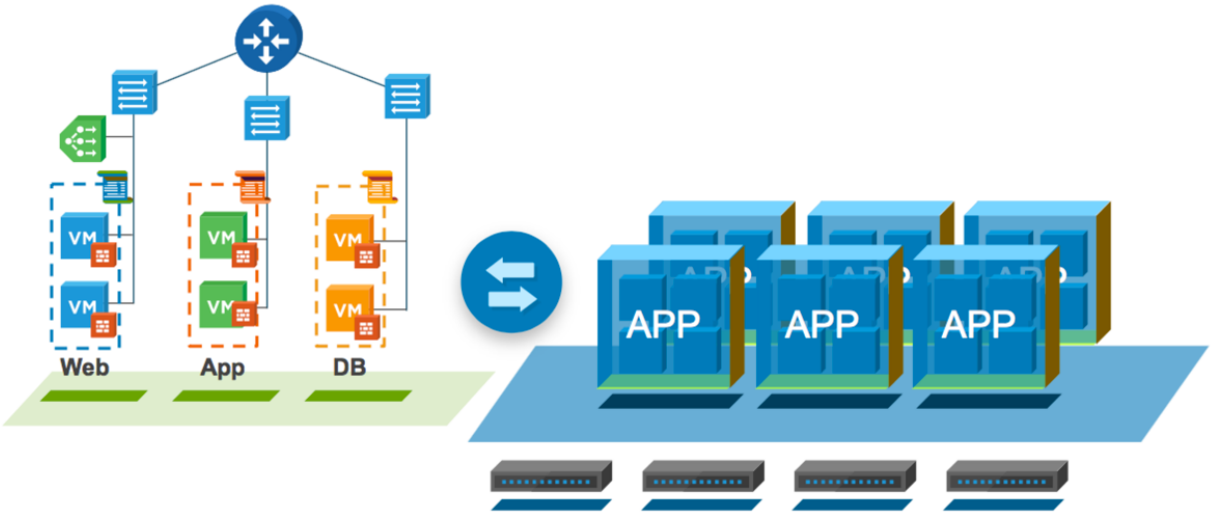
Figure 16 vSAN datastore



B.1.3 VMware NSX

NSX network virtualization delivers the operational model of a VM to the network infrastructure. NSX software-defined networking injects improved security into the entire data center infrastructure. With NSX, network functions including switching, routing and firewalling are embedded in the hypervisor and distributed across the environment. This effectively creates a “network hypervisor” that acts as a platform for virtual networks and services as shown in Figure 17 below.

Figure 17 NSX software-defined networking



NSX virtual networks leverage automated, policy-based provisioning and multi-tenant isolation to simplify network management, even for complex multi-tier network topologies. NSX reproduces the entire network model in software, enabling any network topology to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX, to build more agile and secure environments.

B.1.4 vRealize Suite

Most software-defined data centers are hybrid, with workloads a mix of traditional and modern application architectures. They are provisioned in an increasingly virtualized mix of physical and virtual environments, managed both on-premises in private clouds and off-premises in public clouds. The concept of a cloud management platform has evolved as a response to this complex set of management requirements. VMware's vRealize cloud management platform delivers the management capabilities to effectively manage the complete lifecycle of services delivered in a hybrid IT environment.

VMware's vRealize cloud management platform includes:

- **vRealize Automation** automates the delivery of IaaS or application services via blueprints (templates) that bind compute, storage, networking and security resources through policies.
- **vRealize Business for Cloud** automates costing, usage metering and service pricing of virtualized infrastructure and cloud services.
- **vRealize Operations** provides intelligent health, performance, capacity and configuration management. vRealize Operations offers performance and health monitoring and capacity planning as well as custom dashboards, capacity modeling and customized alerting. These insights help administrators maintain compliance and efficiently detect and resolve any issues that may arise.
- **vRealize Log Insight** provides real-time log management and log analysis. vRealize Log Insight lets administrators monitor physical and virtual infrastructure to avoid failures and performance issues. vRealize Log Insight provides centralized log aggregation and analysis with search and filter capabilities. This provides the ability to monitor all workloads from a single place.
- **vRealize Suite Lifecycle Manager** provides automated installation, configuration, upgrade, patch, drift remediation, health and content management of vRealize products.

B.2 VMware Validated Designs (VVD) technical implementation

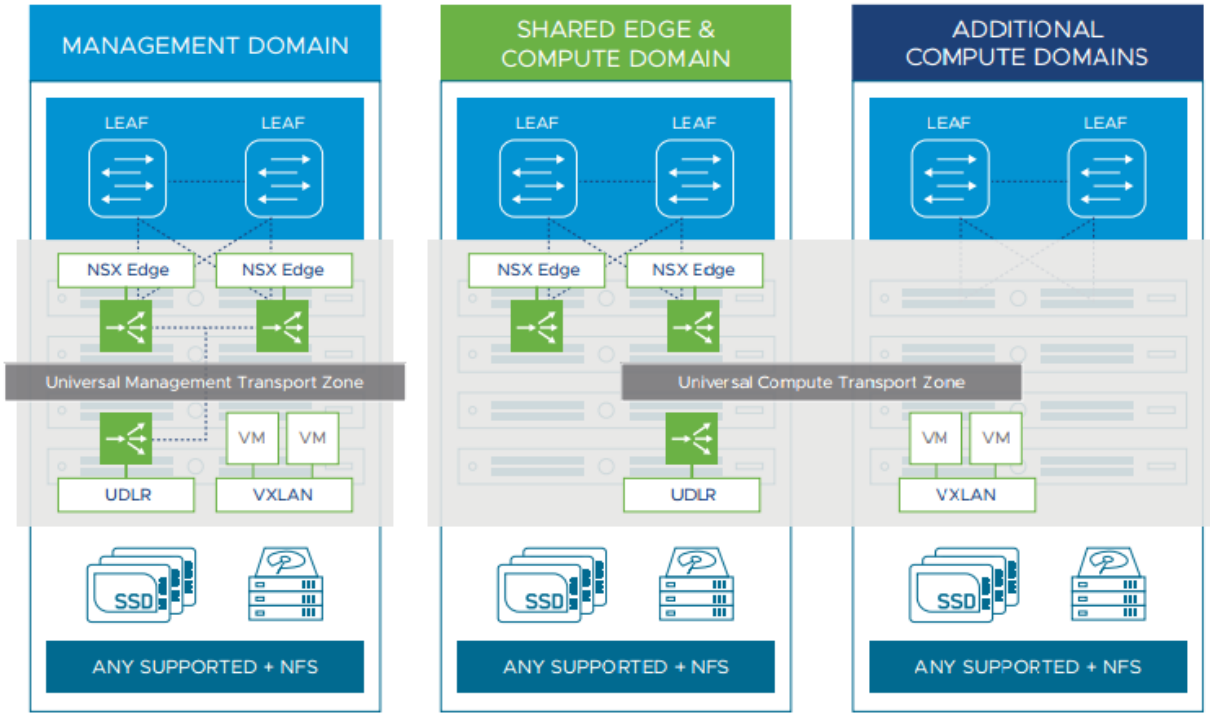
VVDs are implemented on a collection of common building blocks, referred to as workload domains. Each workload domain represents the logical grouping of hardware and software needed to support specific functions within the SDDC.

The **Management Workload Domain** hosts the infrastructure components used to instantiate, manage and monitor the SDDC. These components include Platform Services Controllers, vCenter Server Instances, NSX Managers and vRealize Log Insight. Cloud management and operations capabilities can be extended with additional solutions like vRealize Automation. VMware vSAN is recommended for hosting virtual machines running in this cluster, while NFS is used for storing backup images, log, archives and virtual machine templates.

The **Shared Edge and Compute Workload Domain** provides north-south networking access for initial organization and end-user workloads. It is typically located inside the same rack as the management domain, although in larger environments it may be installed in a dedicated rack. Any supported vSphere storage may be used.

As an organization grows, additional **Compute Workload Domains** can be added to expand the SDDC capacity. Any supported vSphere storage may be used.

Figure 18 VVD workload domain architecture



B.2.1 VVD multi-region architecture

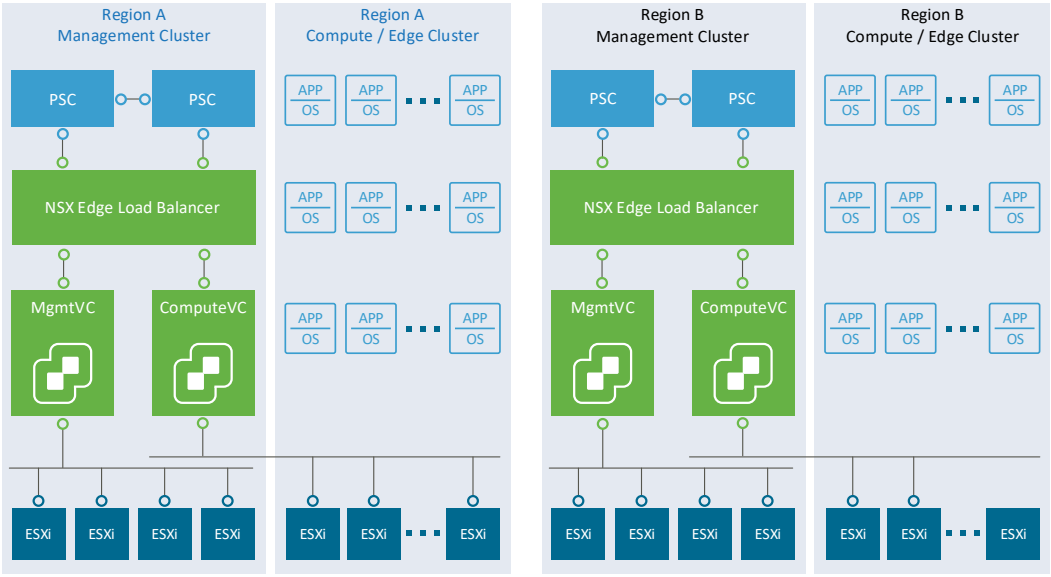
VVD supports a multi-region architecture. The term **region** describes a large geographical separation between data centers. The reference architecture supports network latency between regions up to 150ms. The term **availability zones** is used for local separation.

Note: Each region is treated as a separate SDDC and multiple regions are not treated as a single SDDC.

The main use cases for regions within the VVD reference architecture are:

1. To provide disaster recovery capabilities, based on vSphere replication between regions.
2. To distribute workloads and data closer to customers, including supporting data privacy laws that may require keeping tenant data within a region in the same country.

Figure 19 VVD multi-region architecture



B.2.2 Availability zones (vSAN stretched cluster)

With VVD 4.2, VMware added steps on how to design and implement a dual-region SDDC that supports multiple availability zones. Availability zones enhance resiliency of the SDDC and improve SLAs by:

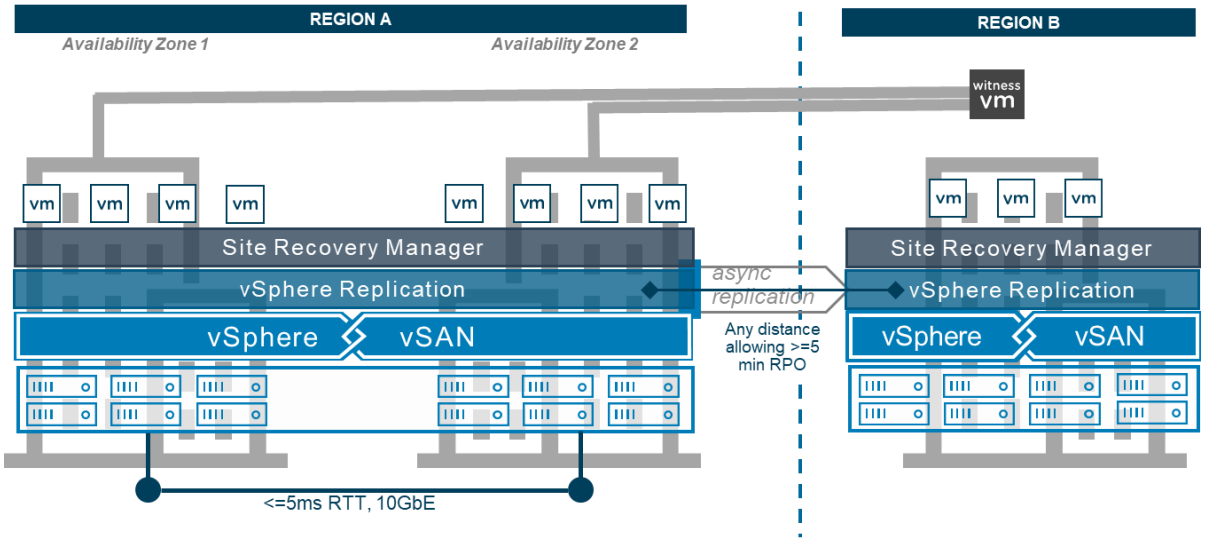
- Allowing identification of separate fault domains within the primary region.
- Leveraging the stretch-clustering capabilities of vSAN to distribute workloads across the availability zones.

Separate availability zones should always be physically isolated and have independent power, cooling, network and security. The whole idea of availability zones is to ensure that should an outage occur in one zone, the surviving zone would have everything it needs to sustain the organization until such time as the outage is resolved, or a disaster declared and operations moved to the recovery region.

Starting with VVD 4.2, up to two availability zones can be defined in the primary region. The physical distance between these zones can be up to approximately 30 miles (50 kilometers) and must be interconnected using a low, single-digit latency and high bandwidth fiber connection. Workloads can operate across availability zones in an active/active manner using a single vCenter Server instance.

The vSAN cluster is split across availability zones in the primary region. Each availability zone is a separate vSAN fault domain (FD). The secondary region hosts the witness VM. A more sophisticated data protection architecture can be built by combining two availability zones in the primary region with Site Recovery Manager-based DR between regions, as show in Figure 20 below.

Figure 20 VVD vSAN stretched cluster with disaster recovery support



B.2.3 VVD implementation options

Organizations can implement VMware Validated Designs in three ways:

1. **VMware Professional Services**: Purchase a VMware Validated Design for SDDC Deploy Service available from VMware Professional Services.
2. **Certified Partner Architecture**: Work with a VMware Partner that offers advanced solutions based on the VVDs, such as VVD on VxRail.
3. **Build Your Own**: Implement VVDs with in-house skillsets by following the public documentation available for free on vmware.com/go/vvd-docs

B.3 VMware Cloud Foundation

VMware Cloud Foundation is an integrated software platform that automates the deployment and lifecycle management of a complete software-defined data center on standardized hyper-converged architecture. It can be deployed on premises on a broad range of supported hardware or consumed as a service in the public cloud. With integrated cloud management capabilities, the end result is a hybrid cloud platform that spans private and public environments, offering a consistent operational model based on well-known vSphere tools and processes and freedom to run applications anywhere without the complexity of re-writing applications.

B.3.1 Key features and capabilities

Integrated stack: An engineered solution that integrates the entire VMware software-defined stack with guaranteed interoperability, freeing organizations from dealing with complex interoperability matrixes.

- **Enterprise-grade services**, based on market-leading VMware technologies: vSphere, vSAN, NSX, vRealize Suite, delivering enterprise-ready services for both traditional and containerized applications.
- **Built-in intrinsic security** delivers network-level micro-segmentation, distributed firewalls and Virtual Private Network (VPN), compute-level encryption for VM, hypervisor and vMotion and storage-level encryption for data at rest and clusters.
- **Self-driving operations** enable self-driving health, performance, capacity and configuration management to scale and manage the environment efficiently.
- **Self-service automation** automates the delivery of application services via blueprints (templates) that bind compute, storage, networking and security resources through policies.

Standardized architecture automatically deploys a hyper-converged architecture based on a VMware Validated Design, ensuring quick, repeatable deployments while eliminating risk of misconfiguration.

- **Storage elasticity and high performance** implements a hyper-converged architecture with all-flash performance and enterprise-class storage services including deduplication, compression and erasure coding.

Automated lifecycle management includes unique lifecycle management services that automates day 0 to day 2 operations, from deployment to configuration of the cloud environment, to on-demand provisioning of infrastructure clusters (workload domains) to patching/upgrades of the complete software stack.

- **Automated deployment** automates the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of storage, cluster creation and provisioning.

- **Infrastructure cluster provisioning** enables on-demand provisioning of isolated infrastructure clusters to enable workload separation.
- **Simplified patching and upgrades** enable a simplified patching/upgrading process of the software platform (including VMware vCenter Server). Cloud admins have the flexibility to choose the timing and scope of the updates.

Simple path to hybrid cloud dramatically simplifies the path to hybrid cloud by delivering a common platform for private and public clouds, enabling a consistent operational experience and the ability to quickly and easily move workloads at scale across clouds without re-architecting applications, leveraging VMware NSX® Hybrid Connect™.

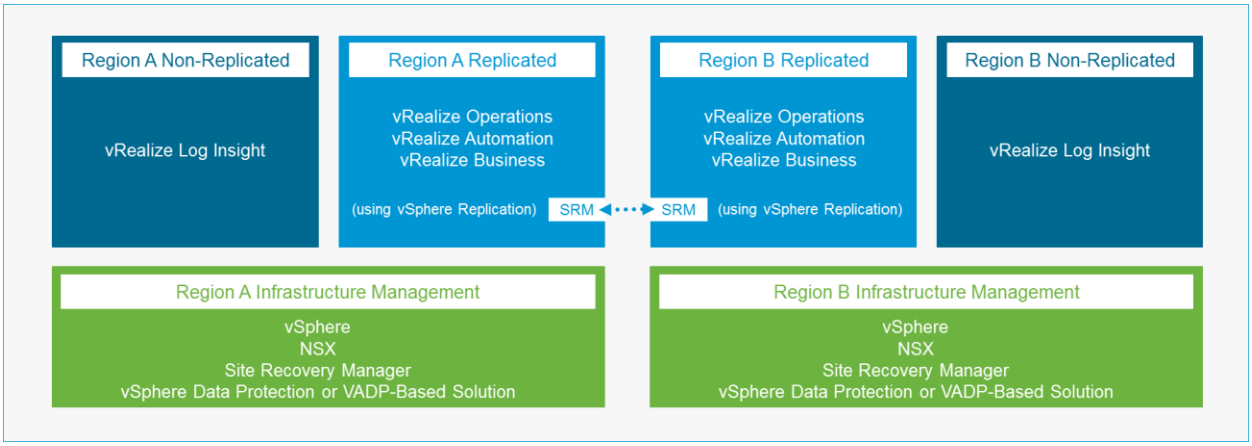
B.3.2 SDDC Manager

VMware Cloud Foundation is more than just a bundling of VMware products, it fully integrates those pieces together through the SDDC Manager, enabling an organization to build a complete SDDC in record time. The SDDC Manager automates the bring up, deployment, configuration, provisioning and lifecycle management of the entire SDDC stack. Deployment is automated for all primary components in the stack. Current Cloud Foundation versions support lifecycle automation patching and upgrading for SDDC Manager, vSphere, vSAN and NSX, with future support for vRealize and other products in the stack.

C Optional VMware integrated data protection options

VVD provides prescriptive guidance for protecting components in the management domain, as shown in Figure 21. In general, VVD recommends vSphere Replication for data replication and Site Recovery Manager for orchestrating disaster recovery (DR) tasks, such as failover, failback and DR testing. Within this reference architecture, the vRealize components such as vRealize Operations, vRealize Automation and vRealize Business are protected. This model can be expanded to cover the tenant workloads in the compute domain, which are typically much more important for customers.

Figure 21 VVD guidance for protecting the management domain



In general, VVD recommends vSphere Replication for data replication and Site Recovery Manager for orchestrating disaster recovery (DR) tasks, such as failover, failback and DR testing. Within this reference architecture, the vRealize components such as vRealize Operations, vRealize Automation and vRealize Business are protected. This model can be expanded to cover the tenant workloads in the compute domain, which are typically much more important for customers.

VVD does not prescribe compute domain data protection, instead leaving it open for custom design depending on actual customer requirements. In general, VVD supports VMware vSphere® Storage APIs - Data Protection (VADP) compliant backup solutions, such as Dell EMC Avamar®.

VMware environments generate new data protection challenges. The convenience of deploying virtual machines enables VMs to be provisioned at a rapid pace, causing VM sprawl. In addition, new VMs are being provisioned without governance or data protection. This increases the risk for data loss and inconsistent recoveries. Administrative roles for data protection have changed during the transformation to virtualization. Backup admins are responsible for configuring polices that adhere to business requirements. Application admins are responsible for assigning data protection to their applications. This change increases the number of data protection solutions installed within a data center. Multiple data protection solutions increase the risk of inconsistent application recovery.

While a majority of corporations have the goal to move their applications into a fully virtualized or cloud environment, there is still a need to protect data residing on physical servers. Traditional agent-based backup and recovery solutions do not provide the scalability or flexibility needed for the protection of virtual environments.

C.1 Dell EMC Data Protection Suite for VMware

Data Protection Suite for VMware provides industry-leading data protection to meet the Recovery Point Objectives (RPO) of VMware servers and applications. The suite provides backup and recovery, continuous data protection for any point-in-time recovery, backup to the cloud, proactive monitoring and analysis, as well as search capabilities. The suite supports virtual and physical servers along with protection of network-attached storage (NAS). The suite provides the freedom to deploy various levels of data protection based on business needs and application consistency for a broad array of enterprise applications. It is available as a software-only solution.

Dell EMC Data Protection Suite for VMware is an optional data protection solution enabling the SDDC with self-service data protection. Tight integration into VMware delivers simplified deployment and administration. It is available as a software-only solution.

Data Protection Suite for VMware is designed to provide flexibility when it comes to protecting VMware environments. It provides the freedom to deploy various levels of data protection based on business needs.

Administration is simplified by allowing admins to manage data protection within native VMware interfaces (vSphere). Additional benefits are available to vRealize customers. Data Protection Suite for VMware embeds backup and recovery into the vRealize Automation blueprints, ensuring that data protection will be automatically included during the provisioning process.

Part of the Data Protection Suite Family, Dell EMC Avamar provides flexible deployment options for fast, daily full backups including virtualized and physical environments. Avamar's tight integration with Dell EMC Data Domain uses a multi-streaming, deduplication approach, resulting in faster, more efficient backups.

Avamar divides backup data into variable-length sub-file segments, compresses and applies a unique hash identifier to each segment during the backup process. Avamar then determines if a segment has been previously backed up and only backs up the unique segments, greatly reducing backup times. Deduplication dramatically reduces the amount of data sent and stored, eliminating backup bottlenecks and reducing storage costs.

Data Protection Suite for VMware is deployed with Dell EMC Data Domain or Data Domain Virtual Edition as the storage target, further optimizing backup infrastructure. It can be easily scaled to meet the demands of the largest of enterprises.

Data Domain is an inline deduplication storage system, which has revolutionized disk-based backup, archiving and disaster recovery that utilizes high-speed processing. The Data Domain Operating System (DD OS) is the intelligence that powers Dell EMC Data Domain high-speed scalable deduplication. It provides the agility, security and reliability that enables the Data Domain platform to deliver scalable, high-speed and cloud-enabled protection storage for backup, archive and disaster recovery.

There are significant benefits to Data Domain integration:

- Network bandwidth reduced by up to 99%
- Backup times reduced by up to 50%
- Backup storage reduced by up to 30x

C.1.1 Dell EMC RecoverPoint for Virtual Machines

RecoverPoint for VMs (RP4VMs) redefines data protection for VMware virtual machines, enabling local, remote and concurrent local and remote replication with continuous data protection for recovery to any point-in-time (PiT). It protects VMware VMs with VM level granularity. It is a VMware hypervisor based, storage agnostic, software-only data protection tool with built-in orchestration and automation capabilities accessible via the VMware vSphere web client plug-in.

RecoverPoint for VMs uses a journal-based implementation to hold the PiT information of all changes made to the protected data. Providing the shortest recovery time to the latest PiT via journal technology that delivers “DVR like” roll back in time capability, providing short RPO to any selected PiT enabling recovery to just seconds before data corruption occurred, reversing the error.

With RecoverPoint technology, data is protected by Consistency Groups (CGs), preserving relational dependencies during recovery such as those of a database and a database log. The CG depends on the use of journal volumes that hold all the historical changes in order to preserve write order fidelity. Furthermore, the CG Sets feature enables recovery activities to be performed to the same consistent PiT across all data in the CG set simultaneously.

RecoverPoint for VMs delivers remote data replication over WAN, sync or async, at lower costs. Its built-in WAN optimization consists of compression and advanced bandwidth reduction algorithms that reduce WAN bandwidth consumption up to 90%. WAN optimization also ensures replication robustness with an improved resiliency that sustains 50% longer round-trip time (RTT) and higher packet loss to fully utilize the available bandwidth.

RP4VMs can be used as another replication-based data protection option available for VVD (which by default leverages the combination of vSphere Replication and Site Recovery Manager), offering more granular recovery and consistency groups. These capabilities might be required to improve recoverability of critical workloads and meet more demanding RTO/RPO requirements. This can be used to protect only customer workloads running in the Compute Workload Domains.

VxRail includes licenses for RecoverPoint for VMs.