VMware Cloud on Dell EMC

Technical overview

vmware® | **D∕ELL**EMC

Table of Contents

Introduction

Today's customers are comfortable running business critical workloads and cloud native applications in the Public Cloud. Many are also extending a cloud operating model and application runtime to places not traditionally considered to be in "The Cloud." In other words, customers want the Public Cloud's operating model – both its technical and financial attributes – regardless of where their workloads run, whether that is in a core data center, the edge, or in a public cloud offering. They are increasingly comfortable decoupling the operating model and application runtime from a specific location. This movement away from a monolithic definition of cloud computing is part of a movement toward multi-cloud solutions. However, before diving into how VMware addresses this movement we should define the cloud operating model.

A cloud operating model is based on ease of consumption, elastic scalability, automated lifecycle management, vendor managed service levels, open-source developer tools, and intrinsic security. These attributes are common to most cloud providers where customers can easily order and scale the service from a web portal. Also, they can easily build and run modern applications on the service. In these offerings the provider automates lifecycle management, proactively monitors the service, offers open-source tools, and ensures security and compliance. All of this can be summarized into three defining principles of a cloud operating model:

1. Simplicity
2. Scale
3. Trust

The real challenge for customers and providers is how to consistently deliver this operating model beyond the public cloud context.

Delivering a consistent experience for infrastructure, operations, and applications across cloud contexts is how VMware distinguishes itself in a multi-cloud world. One of the defining characteristics of VMware's cloud strategy and services is that we provide consistent infrastructure and operations wherever a customer uses our technology. For example, if a customer installs VMware Cloud Foundation™ in their data center, they will have an operating experience that is consistent with the service they would consume in VMware Cloud™ on AWS. If they run containerized applications, VMware Tanzu will provide the same developer friendly orchestration experience for Kubernetes in the public cloud as in their private data center. VMware can deliver this operating model across clouds, in private data centers, at colocation data centers, and edge locations.

Public Cloud consumption has accelerated dramatically over the past several years. Given this fact, many people wonder whether all workloads should simply migrate to public cloud providers. While that notion is rather compelling, there are strong forces that inhibit customers from moving all of their workloads to these providers. Those forces include network latency, application performance, cloud licensing, and governance. These challenges require an expanded definition of the cloud operating model to include local cloud as a service (LCaaS). Let's explore what is meant by local cloud as a service.

Local Cloud as a Service

IDC defines Local Cloud as a Service (LCaaS)
a recently developed private/dedicated provider–operated cloud service option and offers a flexible consumption options that organizations can use to consume infrastructure as a resource rather than individual products.

LCaaS operates where a public cloud service provider takes responsibility for, and retains control of, patching and upgrading of all prebundled cloud platform software. While the public cloud provider also owns the infrastructure hardware assets, the LCaaS solution can be located at a service provider's datacenter or any type of client datacenter. LCaaS can be a standalone service operated by a public cloud provider, or as is increasingly the case, include value-added services provisioned by managed service providers (SPs). This would include life-cycle services (e.g., architecting, developing, testing, deploying, and ongoing monitoring and management) for any type of hardware and software (e.g., middleware, application, and development tools) used in conjunction with LCaaS.

LCaaS will serve as a next-generation replacement for the hardware/software deployed in existing "self-built" enterprise private clouds in core datacenters (internal and colocation) and a growing range of edge locations. It will also serve as a new platform for delivery of dedicated hosted private cloud by cloud service providers. The adoption of LCaaS solutions will play a critical role in boosting business velocity, enabling dynamic business scaling, and ensuring greater business operational flexibility.

Vendors offering LCaaS solutions include AWS Outposts (AWS and VMware Cloud versions), Microsoft's Azure Stack and Google's Anthos (delivered as LCaaS by HPE, Dell EMC, Lenovo, etc.), Oracle's Dedicated Region Cloud@Customer, and VMware Cloud™ on Dell EMC.[1]

VMware Cloud on Dell EMC aligns to the LCaaS category by combining the simplicity and agility of the public cloud with the security and control of on-premises infrastructure delivered as a service to data center and edge locations. VMware's offering extends the cloud operating model into traditional customer data centers. This is different from customer deployed and managed private cloud infrastructure because prescriptive, preinstalled, and configured hardware and software are delivered as a single unit of consumption. This unit of cloud infrastructure is then activated and directly managed by VMware throughout the term of the service contract. This service is procured from our cloud portal leveraging a predictable and flexible payment model that allows customers to shift their IT spending from CapEx to OpEx. Once activated, the customer simply consumes this service just as they would from the public cloud. The difference is that they consume the service within their own data center or in a hosted colocation data center.

VMware Cloud on Dell EMC combines VMware's software products with Dell EMC VxRail hyperconverged infrastructure. The service provides fully automated lifecycle management for both the hardware and the software. VMware manages this combined offering from the cloud, monitors the health of the entire stack, and instantiates security and compliance in a shared responsibility model with the customer. Ongoing maintenance and repair for both the software and hardware is included in the service at no additional charge to the customer.

The VMware Cloud on Dell EMC offering is built on three main pillars:

VMware Cloud Console
The VMware Cloud Console is the primary customer interface that enables provisioning, consumption, and high-level resource monitoring. Since it is delivered as a service, there is no software to install. This also minimizes the need for additional management infrastructure at the customer's site which further differentiates the solution from private cloud deployments. Finally, the Console serves as the interface for VMware to monitor and maintain the infrastructure and engage directly with customers.

Rack infrastructure
The VMware Cloud on Dell EMC infrastructure rack is built and fully configured in a Dell EMC facility so that it arrives fully cabled, with the software installed, configured, and ready to use. The rack is equipped with VxRail HCI instances, high-performance networking, power distribution, and secure management.

Automated lifecycle management
Automated lifecycle management ensures that the latest updates to software and firmware are applied to the service. This is important because customers can take advantage of the latest product capabilities and the most current security patches.
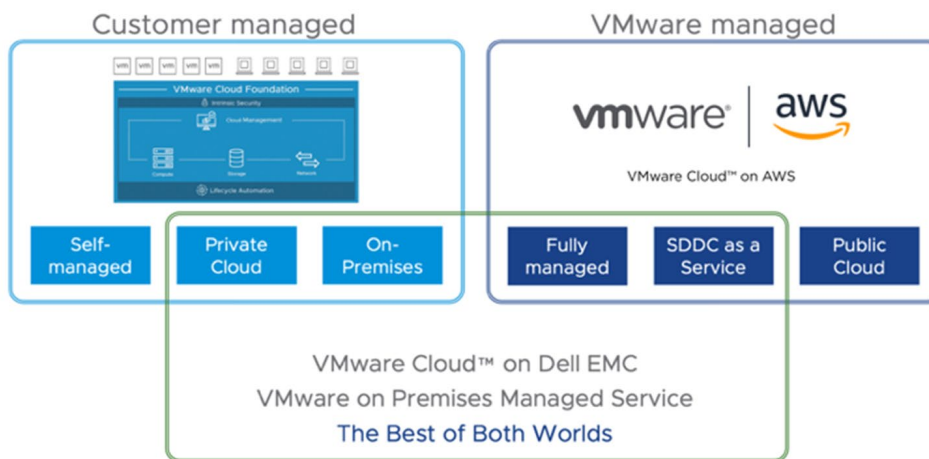

FIGURE 1. VMware Cloud on Dell EMC captures the best attributes of VMware Cloud on AWS and on-premises deployments

Use cases

VMware Cloud on Dell EMC helps customers address the most critical technology and industry specific challenges. The following section covers some of the most common use cases.

Virtual Desktop Infrastructure (VDI)

Desktop administrators will acknowledge that a great end user experience depends on a reliable foundation of software, hardware, and operational excellence. VMware Cloud on Dell EMC's prescriptive service offering provides significant benefits to VDI deployments. VMware has certified VMware Horizon VDI to run on VMware Cloud on Dell EMC. With this certification, customers can build out their virtual desktop deployments with VMware Cloud on Dell EMC as the underlying digital foundation for their virtual desktop infrastructure. The combined solution provides enterprise-class security and certified support for VMware Horizon environments. VMware Horizon on VMware Cloud on Dell EMC also provides superior workspace density and high performance for a great end-user experience when running the most demanding desktop applications.

A key benefit of combining VDI with this managed service is that it provides a known, prescriptive infrastructure that maintains consistency wherever it is deployed. This guaranties a level of reliability and performance that is difficult to maintain with customer managed infrastructure. This translates into a reliable desktop service and an improved end-user experience.

See the resources section of this paper for more information about deploying Horizon on VMware Cloud on Dell EMC.

Multi-cloud native applications

Much as desktop administrators want consistent infrastructure and operations to underpin VDI deployments, developers want to see the applications they write deployed with open-source tools that can be decoupled from underlying infrastructure. They want their applications to run in a multi-cloud context for maximum reach and availability. Kubernetes has become the undisputed open-source tool for orchestrating modern multi-cloud native applications, and VMware's Tanzu solutions embrace and expand Kubernetes's capabilities. Customers can leverage Tanzu Kubernetes Grid* to deploy Kubernetes on top of VMware Cloud on Dell EMC to orchestrate containerized micro-services based applications. This allows customers to streamline the deployment of a conformant Kubernetes distribution that is built upon the open-source Kubernetes community. Tanzu dramatically streamlines container orchestration and includes key features that make deployments and ongoing management of containers consumer simple and enterprise ready.

Tanzu clusters are portable and run on vSphere or multi-cloud environments. In addition, customer DevOps teams can leverage a declarative method (using tools they are familiar with such as vRealize Automation, Terraform, etc.) to control Kubernetes clusters. Tanzu provides services such as networking, authentication, ingress control, and logging that production Kubernetes environments require.

Just as VMware Cloud on Dell EMC dramatically simplifies infrastructure for traditional business applications, Tanzu simplifies runtime for modern containerized applications. Combined, these two offerings provide an easy to consume cloud operating model that supports the needs of both IT operations teams and DevOps teams. This unified solution allows customers to quickly develop and deploy the applications that differentiate their business.

Financial services

Financial Services customers rely heavily on secure, high performance infrastructure to drive value to their business. But maintaining security and meeting performance expectations requires significant operational overhead. Also, with more employees working from home, virtual desktop workloads that can be secured and accessed remotely are now even more critical to business success. Many financial services IT teams are experiencing rapid growth for these workloads and require new infrastructure purchases to support them. The teams responsible for managing these projects are challenged to reduce the time to value for their new purchases while maintaining a patched, secure, and performant environment. They need to do all of this while reducing the operational overhead associated with infrastructure management. Consuming infrastructure from a managed, on premises, cloud service allows these customers to meet business demands while maintaining control over data, ensuring application performance, and controlling costs.

---

*Embedded Harbor Registry and vSphere Pod VMs are not supported on VMC

Manufacturing

Manufacturing customers have factory sites that are often located far from administrative offices to take advantage of less expensive real estate or for supply chain reasons. Factory workers need access to both local and corporate applications using a wide range of endpoint devices. Operations managers need real-time information to make business decisions on the production line. Executives at the central office need assurances that their infrastructure is efficient, robust, and secure across the enterprise. They need a solution that keeps business-critical infrastructure performing at headquarters while extending a consistent operating model to remote infrastructure locations that lack permanent IT staff thereby lowering operational costs. A managed, on premises, cloud service is a great fit to address these challenges.

Healthcare

Healthcare presents many unique IT challenges. Patient care is often an urgent matter and health services need to reach people in urban centers and rural locations. At the same time, medicine is highly dependent on IT systems and endpoint infrastructure that are secure, up-to-date, and constantly monitored to maintain availability and performance. To support this essential mission, IT staff require dependable solutions that provide critical tools to doctors and nurses so they can reliably treat patients wherever they are. A managed, on premises, cloud service affords healthcare providers the ability to care for patients without having to care for the infrastructure that supports health services.

Public sector

The Public Sector provides important safety, utility, transportation, and welfare services to citizens. The success of these services depends on trust that taxpayer dollars are being well spent and that constituents have a positive experience when engaging with their government. This mission requires robust and distributed infrastructure that ensures citizens' needs are met in their communities. All of this must be done under tight budgets and operational cost controls. Public sector IT teams need vendor managed infrastructure solutions that are dependable and offer a predictable all-inclusive consumption model to inspire public confidence and serve the common good. A managed, on premises, cloud service can address these needs by allowing government IT teams to focus on the services they provide to citizens instead of managing armies of professional services engineers to keep IT services running.

Solution benefits and value propositions

To understand how VMware Cloud on Dell EMC addresses customer use cases and challenges it is important to understand some fundamental concepts of the solution.

A managed cloud service

VMware Cloud on Dell EMC is a complete solution for managed data center infrastructure based on industry-leading virtualization technology from VMware and proven hyperconverged hardware from Dell EMC. The software components include VMware vSphere compute, VMware vSAN™ all-flash storage, and VMware NSX-T® networking and security. Physical hardware is based on VxRail hyperconverged infrastructure appliances and high-performance top of rack network switches.
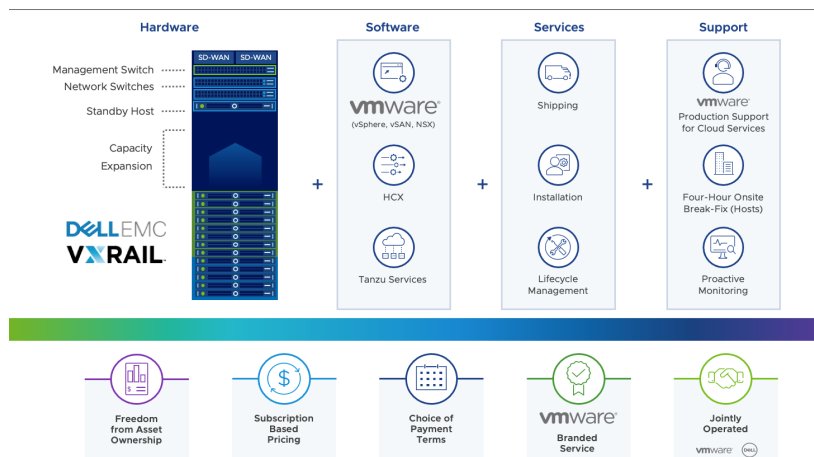

FIGURE 2. What's included in the VMware Cloud on Dell EMC service

Shared responsibility model

Those responsible for providing enterprise data center infrastructure are familiar with the day-2 operations of maintaining a robust and secure service. This is not a trivial task. Maintaining network quality of service, ensuring applications are supplied with enough compute cycles or IOPs for optimal performance, and navigating complex upgrade and patching windows, is hard to do. Add changing business requirements, new security threats, and enforcing policy controls to the mix, and one can see why consuming infrastructure as a service has become so compelling. If you have ever had to upgrade your hypervisor, add storage capacity, patch a vulnerable operating system, and respond to compliance audit surveys all at the same time, you are keenly aware of these challenges.

The reason a cloud operating model is so compelling for IT executives is because maintaining the fundamentals of data center uptime can overwhelm an IT team. This constrains their ability to meet business demands and take on new projects. In a managed cloud service such as VMware Cloud on Dell EMC; however, the IT team benefits from VMware taking on a significant amount of the operational burden for maintaining the infrastructure. Consider the diagram below. It shows that roughly 70% of managing the software infrastructure is handled by VMware. In addition, VMware constantly monitors the health of the underlying VxRail instances and will proactively dispatch a technician if there are signs of trouble.
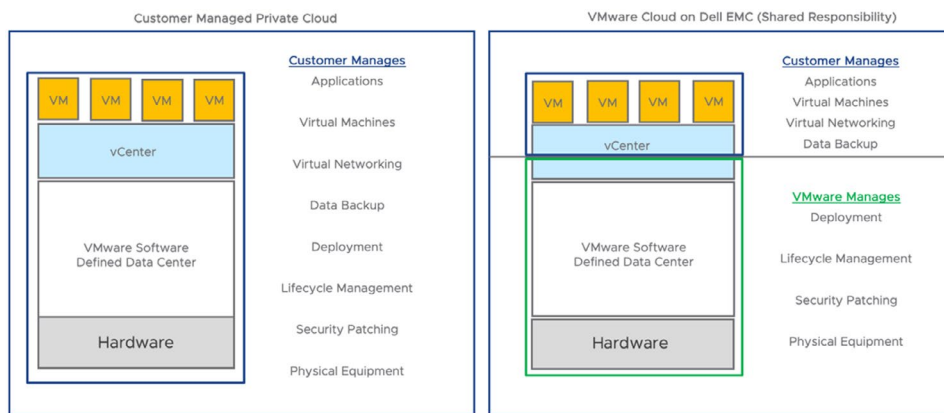

FIGURE 3. VMware Cloud on Dell EMC shared responsibility model

To further illustrate the importance of a shared responsibility model, let's consider security and governance in a managed cloud service. For example, VMware Cloud on Dell EMC provides unique benefits to customers who want to meet compliance standards as cost effectively and as quickly as possible. However, to meet this goal a customer must look at compliance from an auditor's perspective. The auditor sees compliance as a sacred trust to ensure that the customer has properly implemented the controls or processes of specific guidelines that intended to protect consumer privacy or deny bad actors an opportunity to do harm. A customer and an auditor must work together to measure the customer's systems and operations and assess whether specific compliance requirements are met. The end result of this collaboration is that together the customer and the auditor can attest that the environment being measured is compliant. The General Data Protection Regulation (GDPR) and ISO/IEC 27001:2013 are examples of these compliance requirements.

Reaching this state of compliance in an IT environment depends on two important factors. The first is establishing a "known architecture." The second represents the controls or processes contained in a specific set of guidelines like GDPR. For IT environments there are many paths to a production ready state. Typically, customers or professional services engineers will leverage a combination of learned experience, best practices, and product documentation to implement an architecture. When the customer takes control of the architecture, they apply their existing operational model to managing it. While the environment may perform well and meet the reliability needs of the business it may be challenging for the customer to provide a clearly documented account of their systems and operations. This puts a burden on the customer to respond to an auditor's survey. If they fail an audit, it requires even more effort to remediate their architecture and operations so that they can pass the audit.

VMware Cloud on Dell EMC provides a major benefit in this situation because of the shared responsibility model. Let's say a customer would like to attain ISO/IEC 27001:2013 compliance. The compliance measurement is based in part on guidelines published by the ISO/IEC governing bodies. The VMware Cloud architecture is a known state that has consistent infrastructure and operations wherever it is instantiated. Also, VMware ensures that there is no configuration drift outside of that known state. VMware partners with respected auditing firms such as Schellman and PricewaterhouseCoopers to review both the compliance guidelines and the known architecture to produce an attestation of ISO/IEC 27001:2013 compliance for the service that VMware is responsible for. A VMware Cloud on Dell EMC

customer can provide these attestation certificates directly to an auditor. This allows the customer to focus their compliance remediation and attestation efforts only on the part of the infrastructure that they are responsible for. They do not have to worry what VMware manages and this removes a significant burden from the customer's plate.

VMware's Cloud Trust Center program publishes compliance certifications to produce for auditors. VMware Cloud on Dell EMC has achieved compliance certifications for ISO 27001/17/18, SOC 2 Type 1, SOC 2 Type 2, CCPA, and GDPR. For more information on our compliance certifications please see the resources section of this paper.

Automated lifecycle management

Another key benefit that addresses customer challenges is that VMware Cloud on Dell EMC is delivered as a service to customers. Being a service, the offering includes full lifecycle management of all physical components in the rack, from the VxRail and network device firmware and to the virtual elements of the VMware software stack. This relieves customers of time-consuming tasks such as planning, testing, and patching. Lifecycle management is fully automated and is an extension of established VMware Cloud operational processes.

In addition to regular patching and updating, the entire rack is constantly monitored for potential issues, service degradation, or hardware failures. VMware site reliability engineers (SREs) – a global, 24x7 engineering team – have the expertise to diagnose and resolve issues that may arise. If a hardware component requires replacement, an SRE dispatches Dell EMC technicians to the customer's site in a timely fashion to ensure the rack is fully restored to a healthy state. See the Service Description document for break-fix SLA details.

Ease of consumption

Choosing the right hardware for any new IT service is an important decision that defines the success or failure of any deployment or service. Many customers are familiar with the traditional approach to planning, procuring and deploying private cloud infrastructure. Once application requirements are documented for a budgeted project there is a tendency to customize the design and procure more infrastructure than is immediately necessary. It is human nature to plan for every contingency and reserve resources so they can quickly scale to meet hypothetical future demand. This lengthy and sometimes tedious process often leads to delayed projects and overprovisioning. This is because customers must sometimes forecast 5 years into the future to maximize precious CAPEX funds. This often results in underutilized infrastructure or not enough infrastructure when demand increases.

VMware Cloud on Dell EMC dramatically simplifies the design and procurement process, shortens the time to value from months to weeks, and helps customers right-size their infrastructure to business needs. This is because ordering a cloud service is easier and more forgiving than the old way of doing things. While customers still need to understand the performance requirements of the applications they will support, they do not have to customize, over provision, or overspend. They can simply subscribe to the service with OPEX dollars and easily increase capacity when needed. They can deploy their infrastructure with confidence and adjust capacity over time. The diagram shows the VMware Cloud Console where a customer orders the service from their web browser.

Now that we've established how easy it is to consume the service let's consider the specific components that a customer selects when ordering VMware Cloud on Dell EMC.
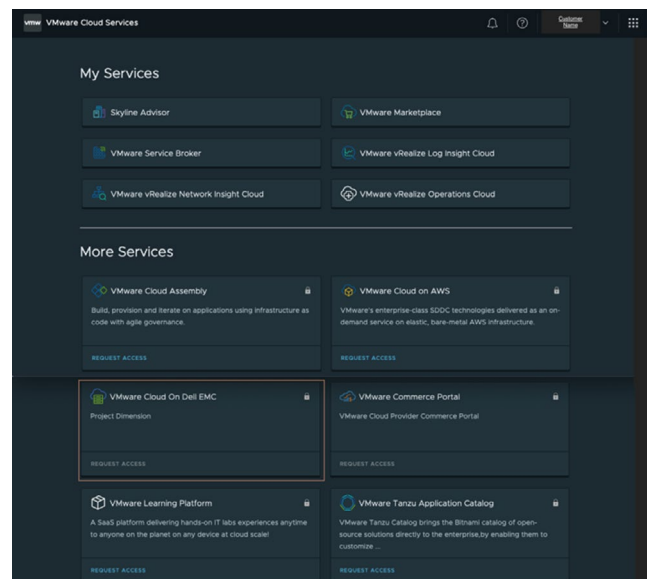

FIGURE 4. VMware Cloud onsole

Compute Hosts

The fundamental building blocks for this service are the Dell EMC VxRail hyperconverged infrastructure (HCI) appliances. These HCI hosts come in prescriptive configurations that are jointly engineered by VMware and Dell EMC. They are designed and optimized for performance, reliability, and simplicity. VxRail provides a powerful digital foundation for a cloud operating model because it is easy to consume as an integrated block of compute and storage, it is simple to scale on demand, it is engineered for automated lifecycle management, and includes intrinsic security features such as vSAN encryption. See the tables for the VxRail compute instances available in the service.

HOSTS						
Instance Type	M1d.xSmall	G1s.small	M1s.medium	M1d.medium	M1d.xLarge	X1d.xLarge
Chassis	1U1N (VxRail E560F)	1U1N (VxRail E560F)	1U1N (VxRail E560F)	1U1N (VxRail E560N)	1U1N (VxRail E560F)	1U1N (VxRail E560F)
CPU cores	56 (2x28)	28	28	56 (2x28)	56 (2x28)	56 (2x28)
vCPUs[1]	112	56	56	112	112	112
CPU frequency	2.2 GHz All Core Turbo	2.2GHz All Core Turbo	2.2 GHz All Core Turbo	2.2 GHz All Core Turbo	2.2 GHz All Core Turbo	2.2 GHz All Core Turbo
RAM	768 GB	256 GB	384 GB	768 GB	768 GB	1536 GB
Cache storage	1.6 TB SSD SAS	1.6 TB SSD SAS	1.6 TB SSD SAS	3.2 TB NVMe	3.2 TB NVMe	3.2 TB NVMe
Primary storage	3.8 TB SSD	11.5 TB SSD	23 TB SSD	23 TB NVMe	61 TB SSD	61 TB SSD
Disk Groups	2	2	2	2	2	2
Power Supplies	Redundant x 1100W 100-240V	Redundant x 1100W 100-240v	Redundant x 1100W 100-240v	Redundant x 1100W 100-240v	Redundant x 1100W 100-240V	Redundant x 1100W 100-240V

See *Data Sheet* for power details

There are several instance options to choose from so that customers can hit the cost vs performance sweet spot. Before ordering VxRail instances a customer must consider whether their workloads are general purpose, compute intensive, memory intensive, storage capacity intensive, or read/write throughput intensive. For example, general purpose workloads align to the G1s.small instances. M1s.medium instances could be leveraged for licensing constrained databases. For virtual desktop infrastructure (VDI) a customer may chose the M1d.medium for its higher CPU core count and fast NVMe interconnect on both the cache and storage tiers. The X1d.xLarge might be a good fit for certain database workloads due to its compute and storage capacity. Finally, VMware recently added the M1d.xLarge instance to its lineup that emphasizes CPU cores over storage capacity. Please note that we recommended customers go through a sizing exercise with a presales consultant to ensure they order instances that align to their budget and technical requirements.

Once a customer has gathered their workload requirements and selected their host instances, they need to consider the appropriate rack configuration to order. VMware Cloud on Dell EMC includes a 42U rack that includes redundant SD-WAN devices for remote management, two top of rack switches, an out of band management switch, and redundant intelligent power distribution units (PDUs).

The "R2" or full-rack is a 42U data center rack that supports three network fabric options. Customers can choose between 2 x 1 GbE , 2 x 10 GbE or 2 x 25 GbE network fabric uplinks. Customers can also select from either single phase or three phase PDUs to support a maximum of 26 production hosts. The R2 can be energized from either floor or ceiling power whips. Every rack is shipped with one extra standby VxRail instance for maintenance or continuity of business purposes. The standby instance only becomes usable when activated by a VMware SRE in coordination with the customer to manage upgrades or mitigate hardware failures.

RACK SPECIFICATIONS	
	RACK R2 (42U)
Number of VxRail E560 nodes	• Single-phase power: Min. 3 – Max 12 • Three-phase power: Min. 3 – Max. 26
Spare / standby hosts per rack	1
Power requirements*	• 4 x 30 amp** | 32 amp*** | single-phase PDUs • 4 x 415v | 20 amp** | three-phase PDUs • 4 x 30 amp** | 4 x 16 amp*** | three-phase PDU IEC 60309 20 A 3P + N + PE**
Power source location	Floor or ceiling
Top of rack switches	2 x 1 GbE , 2 x 10GbE or 2 x 25GbE
Secure management	SD-WAN™ by VeloCloud® devices - (HA pair)

See *Data Sheet* for power details

All of the equipment referenced above is ordered through the VMware Cloud Console. The order form also requests contact information, basic networking details, and the subscription terms. For payment, a customer may select 1-year, 3-year, or monthly billing options. Once the order is submitted an automated delivery process is initiated. VMware ensures that the latest versions of the cloud software stack, including vSphere, vSAN, and NSX-T, are installed on the hardware specified in the ordering process. Then the entire rack is shipped to the customer site where a certified technician unloads the equipment, secures it in the datacenter, connects to power and networking, and activates the service. The delivery process takes approximately 5-6 weeks compared to 5 to 6 months for a typical procurement cycle, and the activation only takes a few hours once the equipment is on site. Billing does not commence until the service is activated in a customer's datacenter. Once activated, the service is ready to consume.

** For US and EU
*** For UK

Mulit-Rack Scale

VMware Cloud on Dell EMC supports a scalable architecture that supports multi-rack deployments as a fully managed service. The result is that customers can order data center scale configurations of the service that allows IT to mitigate the need for significant infrastructure refresh capital expenditures. Instead converting their infrastructure to an operational expense subscription service that deploys in a matter of hours to days, not weeks and months. When customers order a multi-rack configuration the second rack has two additional spine switches added to the rack creating a spine leaf network architecture across the racks. This provides a highly resilient network architecture that can scale to meet the needs of a modern business.

Storage

The VMware Cloud on Dell EMC offering is based on hyperconverged infrastructure (HCI) powered by vSAN. VMware vSAN all-flash datastores provide extremely high performance for a wide range of demanding workloads. Also, because the management plane for vSAN is embedded in vSphere, customers benefit from storage policy-based management (SPBM) which dramatically reduces operational overhead and complexity.

HCI storage scales proportionally with compute. This means storage capacity is only increased when compute nodes are added.

Finally, customer data is protected by vSAN datastore encryption with encryption keys maintained in the tamper resistant trusted platform module (TPM2) present on each instance in the cluster. Also note that customers are responsible for data protection and backup. VMware does not make copies of data, nor does VMware intrude into customer VMs or virtual disks.

Networking

The network relationship between VMware Cloud and a customer's existing infrastructure is one of the most important aspects of the cloud service. This is because in a customer managed private cloud context the customer is solely responsible for the network. In a managed cloud service networking is a shared responsibility. While there are similarities in this networking model between VMware Cloud on AWS and VMware Cloud on Dell EMC there are important differences because the later deploys into a customer's existing data center or colocation. Those differences lie across two primary dimensions: the SD-WAN connectivity to the VMware Cloud control plane, and the layer 3 uplinks to the customer's on premises infrastructure. The SD-WAN links traverse the customers network and firewall infrastructure to gain egress to the Internet. Outbound TCP port 443 and UDP port 2426 are required so that VMware's site reliability engineers can remotely manage the service.

For workloads, data, and applications to straddle both existing infrastructure and the on premises cloud service the VMware Cloud on Dell EMC rack is outfitted with a pair of top-of-rack switches (ToRs). Each ToR has two physical uplinks to the customer's upstream network switches. As previously mentioned, the R2 rack supports either 2 x 1 GbE, 2 x 10 GbE or 25 GbE fiber connectivity. Every host in the rack has a connection to each of the two ToRs for a total of four links and these are configured for redundancy with vSphere teaming policies.

There is also a dedicated management switch in the rack that is connected to the iDRAC ports on each server and to the applicable management ports for other devices, such as the smart PDUs. These connections provide out-of-band access so that VMware engineers can monitor and troubleshoot the physical infrastructure without traversing the primary management network.

During the ordering process, customers are asked to allocate two IP subnets that do not overlap or conflict with other networks in their enterprise. A /23 routable CIDR network is used for the management network to provide VMware ESXi™, vSAN, and NSX-T connectivity. For troubleshooting via direct console connections to the equipment, a /24 non-routable CIDR network is also allocated for the out-of-band management network used only by VMware engineers. The architecture between the VMware Cloud on Dell EMC infrastructure and upstream customer environments is a routed, layer 3 (L3) topology and the load is balanced through equal-cost multi-path routing (ECMP). Therefore, the network devices on the customer's data center side must be routers or switches with routing capabilities. For maximum availability, we recommend connecting to two separate network devices. To enable IP connectivity across these connections, a point-to-point network is configured for each physical link by allocating /30 or /31 networks. Figure 5 provides an overview of the networking components and relationships in the service.

There are several aspects of networking that customers must consider when connecting to VMware Cloud on Dell EMC . Each rack includes VMware NSX-T which makes it simple to create new workload network segments, to enable firewalling and configure micro segmentation for enhanced application security. VMware Cloud on Dell EMC supports eBGP (external border gateway protocol). Dynamic routing with eBGP enables fast routing fail-over in the event of a TOR switch failure or upstream aggregation switch failure. Fail-over from one TOR switch to the other requires the underlay network to update its routing tables so that packets can route to the right destination bi-directionally. eBGP automates this in a quick and efficient way without manual customer intervention.

In order to securely connect from the cloud-based management infrastructure to each on-premises rack, VMware Cloud on Dell EMC includes an HA pair of physical VMware SD-WAN network devices. This solution makes it easy for each rack to initiate a secure outbound tunnel over any Internet connection without the need for complicated IPSEC firewall configurations. As previously mentioned, so long as outbound connections to TCP port 443 and UDP port 2426 are allowed, the connection will be established automatically. Note that the included SD-WAN network devices are restricted to VMware administrative use only.

FIGURE 5. VMware Cloud on Dell EMC networking overview

Finally, customers have the option to implement static routing between the service TORs and their upstream aggregation switches if they prefer.

Integrations and workload migration

Each VMware Cloud on Dell EMC rack includes a vCenter Server® Appliance (VCSA) for management of the underlying infrastructure and workloads. Customers have the option of using Hybrid Linked Mode (HLM) to integrate with their existing vSphere environment and present a single pane of glass for workload management.

Once the VMware Cloud on Dell EMC rack is deployed and the networking is configured to integrate with existing data center networks, administrators can take that integration a step further and extend existing VLANs into the new rack through a layer 2 VPN (L2VPN). This allows the new rack to run workloads that use IP addresses from an existing on-premises network.

If a L2VPN is configured, it is possible to perform zero-downtime live migrations with vMotion from existing infrastructure onto the new rack. This is critical for applications that cannot be easily re-addressed or cannot be disrupted until a later time.

Cold VM migrations or manual uploads of ISO images and VM templates are all also possible and do not require a L2VPN.

For large environments that require bulk migration, customers can leverage HCX. HCX is VMware's automated workload migration platform. With this add-on service customers can now enable HCX Advanced with no additional cost or license. VMware provides end to end support for HCX to help customers resolve technical problems and answer questions about migrating workloads to and from VMware Cloud on Dell EMC.

vRealize integration

VMware vRealize Suite combines the automation and operations capabilities of vRealize Cloud Management to provide consistent operations and governance for customers' hybrid cloud environments. VMware has now certified key products of the vRealize Suite to integrate with VMware Cloud on Dell EMC. This enables customers to combine VMware Cloud on Dell EMC with their existing on-premises or public cloud instances and gives customers a unified cloud management portal for managing all of their compute, network, and storage.
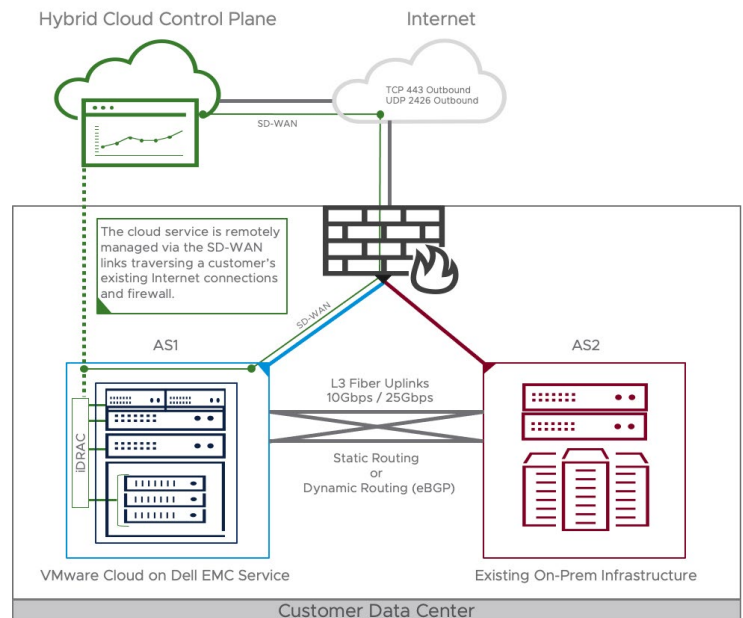
Modern Kubernetes workloads

VMware Cloud on Dell EMC now includes VMware Tanzu services. VMware Tanzu Services includes a fully Managed Tanzu Kubernetes Grid (TKG) as well as Tanzu Mission Control (TMC) essentials cluster management. Together, this powerful combination ensures customers can run modern enterprise applications through having the resources to run, containerize, and easily manage their modern Kubernetes applications. Deployment of VMware Tanzu Services is simplified through the VMware Cloud Console. Once deployed, VMware administrators can create vSphere Namespaces which grants pools of compute, memory and storage resources to Kubernetes developers. Developers can then quickly authenticate to their assigned vSphere Namespaces and begin deploying Kubernetes applications on VMware Cloud on Dell EMC infrastructure.

Disaster Recovery as a Service

VMware Site Recovery ™ brings VMware enterprise-class Software-Defined Data Center (SDDC) Disaster Recovery as a Service to the VMC on Dell EMC Cloud. It enables customers to protect and recover applications to a VMC on Dell EMC dedicated secondary site. It is delivered, sold, supported, maintained, and managed by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools—without the difficulties of learning new abilities or utilizing new tools.

VMware Site Recovery is an add-on feature to VMware Cloud on Dell EMC. VMware Cloud on Dell EMC integrates VMware's flagship compute, storage, and network virtualization products—VMware vSphere, VMware vSAN ™, and VMware NSX®—along with VMware vCenter Server® management. It optimizes them to run on bare-metal Dell EMC VxRail infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now get instant business value via the VMC Cloud on-premises.

VMware Site Recovery extends VMware Cloud on Dell EMC to provide managed disaster recovery, disaster avoidance, and non-disruptive testing capabilities to an existing on-premises data-center or a secondary co-lo facility.

VMware Site Recovery works in conjunction with VMware Site Recovery Manager ™ and VMware vSphere Replication ™ to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads.

VMware Site Recovery utilizes VMware Site Recovery Manager appliances to coordinate the operations of the VMware SDDC. This is so that as virtual machines at the protected site are shut down, copies of these virtual machines at the recovery site startup. By using the data replicated from the protected site these virtual machines assume responsibility for providing the same services.

VMware Site Recovery can be used between a customer's existing datacenter and an secondary remote site where VMware Cloud on Dell EMC instance is deployed. Or it can be used between two VMC on Dell EMC SDDCs deployed to different availability zones or regions. The second option allows VMware Site Recovery to provide a fully VMware-managed and maintained Disaster Recovery solution.

Migration of protected inventory and services from one site to the other is controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools to which they are allocated, and the networks they can access. VMware Site Recovery enables the testing of recovery plans, using a temporary copy of the replicated data, and isolated networks in a way that does not disrupt ongoing operations at either site. Multiple recovery plans can be configured to migrate individual applications or entire sites providing finer control over what virtual machines are failed over and failed back. This also enables flexible testing schedules.

VMware Site Recovery extends the feature set of the virtual infrastructure platform to provide for rapid business continuity through partial or complete site failures.
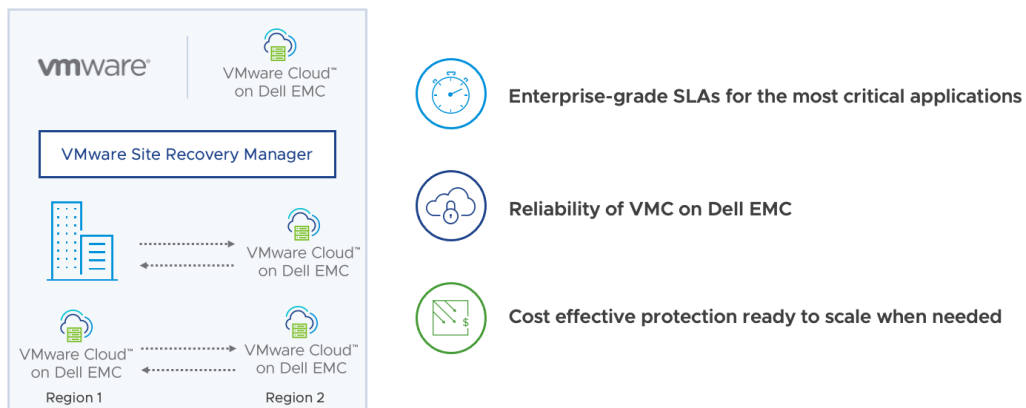
Security

As mentioned earlier in this paper, security is both a requirement and an attribute of cloud environments. Infrastructure security contributes to application uptime by preventing unwanted intrusions and unauthorized configuration changes. VMware Cloud on Dell EMC architecture includes several security benefits.

Customers no longer have to keep track of security bulletins for potential vulnerabilities related to their deployments because VMware Cloud on Dell EMC includes full lifecycle management. When security patches are needed, they are thoroughly tested by VMware engineers before being rolled out. This is a major time and cost saver for customers, as they do not need to maintain a test or staging environment for assessing the impact of new patches. Also, they don't need to plan and schedule patching and updating operations across their infrastructure, which can be a time-consuming task or force downtime. Customers are consulted before patches or upgrades are applied so that they can be performed at a time of the customer's choosing.

Role-based security ensures that permissions to manage the infrastructure layer are tightly controlled, preventing accidental or malicious propagation of critical credentials. Customers have access to a reduced administrator role that can fully manage workloads but not the underlying hosts. Networks are segregated with workload network segments for customer VMs and management networks for the infrastructure appliances and interfaces. By not commingling this traffic, risk is reduced.

Regional availability

VMware Cloud on Dell EMC has two major dependencies for availability in a particular region. First, the VMware Cloud Service must be available in a specific region. Second, Dell EMC must have the local infrastructure to support VxRail and rack assembly and the distribution network to provide delivery and support.

VMware Cloud on Dell EMC is currently available in the following locations

•The Continental United States
•The United Kingdom, France, The Federal Republic of Germany

Conclusion: The cloud operating model is based on simplicity, scale, and trust.

VMware Cloud on Dell EMC is a local cloud as a service offering that best embraces this operating model. It is easy for customers to order and start consuming; it has a shared responsibility model that eases administrative burden; and it includes Lifecycle management that automates keeping the service healthy and up to date. Customers are also able to scale the service by easily adding compute and storage and extend services through networking innovations that make integration with existing data center infrastructure simple to implement. It supports a variety of use cases and helps customers right size the service to support business critical workloads from databases to VDI to Kubernetes. Finally, VMware Cloud on Dell EMC instills trust by meeting compliance needs and providing a stable platform that VMware ensures is always running and secure.

Business and technical drivers continue to fuel demand for cloud services, delivered in a cloud operating model anywhere a business operates, or employees work. Whether workloads run in a hyperscaler, on-premises, in a colocation, or at the edge, is no longer the most important consideration for IT teams. What matters most is that applications and data can be easily accessed and securely consumed by users wherever they reside. Meeting this need requires a cloud operating model that transcends any one cloud or location. VMware's mission is to build solutions for customers so they may thrive in a new multi-cloud world, and VMware Cloud on Dell EMC is a critical dimension of that mission by providing simplicity, scale and trust.

Resources

VMware Cloud on Dell EMC

VMware Cloud on Dell EMC for Virtual Desktops and Applications Solution Overview

Horizon on VMware Cloud on Dell EMC – Reference Architecture

Horizon on VMware Cloud on Dell EMC – Deployment Guide

Compliance and Certification Resources

1. [IDC, IDC TechScape: Worldwide Future of Digital Infrastructure, 2020, January 2021, #US47085020]