ABSTRACT
This reference architecture guide describes the Enterprise Hybrid Cloud 4.1.2 reference architecture that enables IT organizations to deploy an on-premises hybrid cloud delivering infrastructure as a service (IaaS) to their business quickly.

This document is not intended for audiences in China, Hong Kong, Taiwan, and Macao.
The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be the property of their respective owners. Published in the USA August 2017 Reference Architecture H16265.1R.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
Contents

Executive summary........................................................................................................................................4
Hybrid cloud features and functionality .........................................................................................................6
Dell EMC and VMware integration ..................................................................................................................15
Key components ............................................................................................................................................16
Solution architecture .....................................................................................................................................22
Protection services ..........................................................................................................................................25
Converged and hyper-converged systems support ........................................................................................29
Software resources .........................................................................................................................................34
Resource sizing...............................................................................................................................................36
Conclusion .......................................................................................................................................................40
Executive summary

This document describes the reference architecture of Enterprise Hybrid Cloud 4.1.2 that enables IT organizations to deploy an on-premises hybrid cloud that delivers infrastructure as a service (IaaS) to their business quickly.

The document introduces the main features and functionality of Enterprise Hybrid Cloud, the Enterprise Hybrid Cloud topologies and key components, and the validated hardware and software environment. The companion Enterprise Hybrid Cloud 4.1.2 Concepts and Architecture Guide is an enablement reference to begin the planning and design of your hybrid cloud and to prepare for a successful implementation.

The following guides provide further information about various aspects of Enterprise Hybrid Cloud:

- Enterprise Hybrid Cloud 4.1.2 Concepts and Architecture Guide
- Enterprise Hybrid Cloud 4.1.2 Administration Guide
- Enterprise Hybrid Cloud 4.1.2 Security Management Guide
- Enterprise Hybrid Cloud 4.1.1 Infrastructure and Operations Management Guide

This document is intended for executives, managers, architects, cloud administrators, and technical administrators of IT environments who want to implement a hybrid cloud IaaS platform. Readers should be familiar with the VMware vRealize Suite, storage technologies, general IT functions, and requirements, and how a hybrid cloud infrastructure accommodates these technologies and requirements.

Enterprise Hybrid Cloud enables customers to build an enterprise-class, multisite, scalable infrastructure that enables:

- Complete management of the infrastructure service lifecycle
- On-demand access to and control of network bandwidth, servers, storage, and security
- On-demand provisioning, monitoring, protection, and management of the infrastructure services by the line-of-business users
- On-demand provisioning of application blueprints with associated infrastructure resources by line-of-business application owners
- Simplified provisioning of backup, continuous availability, and disaster recovery services as part of the cloud service provisioning process
- Add, modify, or delete services to an application or virtual machine during its complete lifecycle
- Maximum asset utilization
- Increased scalability with centrally managed multisite platforms spanning IT services to all data centers
While many organizations have successfully introduced virtualization as a core technology within their data center, the benefits of virtualization have been restricted primarily to the IT infrastructure owners. End users and business units within customer organizations have not experienced many of the benefits of virtualization, such as increased agility, mobility, and control.

Transforming from the traditional IT model to a cloud-operating model involves overcoming the challenges of legacy infrastructure and processes, such as:

- Inefficiency and inflexibility
- Slow, reactive responses to customer requests
- Inadequate visibility into the cost of the requested infrastructure
- Limited choice of availability and protection services

The difficulty in overcoming these challenges has given rise to public cloud providers who have built technology and business models catering to the requirements of end-user agility and control. Many organizations are under pressure to provide these same service levels within the secure and compliant confines of the on-premises data center without sacrificing visibility and control. As a result, IT departments must create alternatives that are cost-effective and do not compromise enterprise requirements such as data protection, disaster recovery, and guaranteed service levels.

Enterprise Hybrid Cloud integrates the best of Dell EMC™ and VMware products and services, and empowers IT organizations to accelerate the implementation and adoption of a hybrid cloud infrastructure. Enterprise Hybrid Cloud caters to customers who want to preserve their investment and make better use of their existing infrastructure and to those customers who want to build out new infrastructures that are dedicated to a hybrid cloud.

Enterprise Hybrid Cloud takes advantage of the strong integration between Dell EMC technologies and the VMware vRealize and vCloud Suites. Developed by Dell EMC and VMware product and services teams, Enterprise Hybrid Cloud includes Dell EMC scalable storage arrays, converged and hyper-converged infrastructure, integrated Dell EMC and VMware monitoring, and data protection suites to provide the foundation for enabling cloud services within the customer environment.

Enterprise Hybrid Cloud offers several key benefits to customers:

- **Rapid implementation**—Enterprise Hybrid Cloud provides the foundation for IaaS and can be designed and implemented in a validated, tested, and repeatable way based on converged and hyper-converged infrastructure. This increases the time-to-value for the customer while simultaneously reducing risk. Deliver IT as a service (ITaaS) with add-on modules for backup, disaster recovery, continuous availability, virtual machine encryption, applications, application lifecycle automation for continuous delivery, ecosystem extensions, and more.

- **Dell EMC Support**—Implementing Enterprise Hybrid Cloud results in Dell EMC support and further reduces risk that is associated with the ongoing operations of your hybrid cloud.

- **Defined upgrade path**—Customers implementing Enterprise Hybrid Cloud receive upgrade guidance based on the testing and validation that is completed by Dell.
Enterprise Hybrid Cloud 4.1.2
Reference Architecture

Hybrid cloud features and functionality

EMC. This upgrade guidance enables customers, partners, and Dell EMC services teams to perform upgrades faster and with much less risk.

- **Validated and tested integration**—Extensive integration testing across Enterprise Hybrid Cloud makes it simpler to use and manage and more efficient to operate.

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact EMC.Solution.Feedback@emc.com with your comments.

Authors: Ken Gould, Fiona O’Neill

Hybrid cloud features and functionality

Introduction

Enterprise Hybrid Cloud offers a simplified approach to IT functionality for IT organizations, developers, end users, and line-of-business owners.

As a hybrid cloud platform it delivers infrastructure as a service across multiple sites, multiple VMware vCenter endpoints and multiple converged infrastructure systems.

In addition to delivering baseline IaaS, built on a software-defined data center (SDDC) architecture, Enterprise Hybrid Cloud also delivers feature-rich capabilities to expand from IaaS to business-enabling ITaaS.

Backup as a service (BaaS), continuous availability (CA), disaster recovery (DRaaS), and encryption as a service (EaaS) policies can be enabled with just a few clicks across the multisite, multi-vCenter architecture. Resources can be deployed on private cloud or public cloud service providers.

Enterprise Hybrid Cloud includes the following features and functionality, as shown in Figure 1:

- Automation and self-service provisioning
- Workload-optimized storage
- Elasticity and service assurance
- Monitoring and resource management
- Metering and showback
- Dell EMC and VMware integration
Figure 1. Enterprise Hybrid Cloud features and functionality

Enterprise Hybrid Cloud provides self-service provisioning of automated cloud services to end users and infrastructure administrators. Enterprise Hybrid Cloud uses VMware vRealize Automation and VMware vRealize Orchestrator integrated with Dell EMC ViPR™ Controller and VMware NSX to provide the compute, storage, network, and security virtualization services for the software-defined data center. These services enable rapid deployment of business-relevant cloud services across your hybrid cloud and physical infrastructure.

Cloud users can request and manage applications and compute resources within established operational policies; this can reduce IT service delivery times from days or weeks to minutes. Features include:

- **Cross-cloud storefront**—Acts as a service governor that provisions workloads based on business and IT policies
- **Role-based self-service portal**—Delivers a user-specific catalog of IT services
- **Resource reservations**—Enables resources to be allocated to a specific group and ensures that access is limited to that group
- **Service levels**—Defines the amount and type of resources a specific service can receive either during the initial provisioning or as part of any configuration changes
Hybrid cloud features and functionality

- **Build specifications**—Contains the automation policies that specify the process for building or reconfiguring compute resources

vRealize Automation provides lines of business with the ability to deploy cloud applications rapidly and services to meet the demands of the business. Furthermore, it provides the ability to divide a shared infrastructure into logical partitions and assign them to different business units. Using role-based entitlements, business users can manage resources from their own self-service catalog of custom-defined services and blueprints. Each user’s catalog presents the virtual machines, applications, and service blueprints they are entitled to, based on their role within the organization.

Service blueprints, which are powered by vRealize Orchestrator workflows, enable cloud infrastructure administrators to deploy new Dell EMC services that are supported by ViPR Controller for automated storage services, and Dell EMC Avamar™ and Dell EMC Data Domain™ for backup and restore services.

Virtual machine and application blueprints can be added for single machine or multimachine deployments. Multitier-enterprise applications requiring multiple components (application, database, and web) and service levels can be deployed easily from predefined blueprints.

Data protection and encryption policies can be applied to virtual machines at provisioning time or as a day 2 operation, enabling users to request on-demand backups and restores of their virtual machines, and generate backup reports from the vRealize Automation self-service portal.

Figure 2 shows the Enterprise Hybrid Cloud catalog after the initial deployment of storage, backup, and virtual machine provisioning services.

![Figure 2. Enterprise Hybrid Cloud vRealize Automation catalog view](image)

As part of the vRealize Automation provisioning process, you can use VMware NSX virtual networks to provide an on-demand deployment including custom networks that are required as part of a multitier virtual machine provisioning process.

Enterprise Hybrid Cloud is built to work with new and existing infrastructures. It supports the differing requirements of an enterprise’s many business units, and integrates with a wide variety of existing IT systems and best practices.
Multitenancy access requirements in a cloud environment range from shared, open resource access to completely isolated resources. Enterprise Hybrid Cloud provides the ability to enforce physical and virtual separation for multitenancy, offering different levels of security to meet business requirements. This separation can encompass network, compute, and storage resources to ensure appropriate security and performance for each tenant.

Enterprise Hybrid Cloud supports secure multitenancy through vRealize Automation role-based access control (RBAC), enabling vRealize Automation roles to be mapped to Active Directory users and groups. vRealize Automation uses existing authentication and business groupings. The user’s business role governs user access to the self-service portal.

Physical segmentation of resources can be achieved in vRealize Automation to isolate tenant resources or to isolate and contain compute resources for licensing purposes. For example, you can manage Oracle licensing costs by physically isolating all Oracle instances to a set of dedicated VMware ESXi resource pod clusters. Enterprise Hybrid Cloud storage-as-a-service (STaaS) services ensure that any logical unit number (LUN) or VMware vSphere datastore is presented to a single vSphere cluster, further ensuring that Oracle licensing costs might be limited to just those vSphere clusters that are designated to run Oracle instances.

Virtualized compute resources within the SDDC are objects that are inherited from the vSphere endpoint, most commonly representing VMware vSphere ESXi hosts, host clusters, or resource pools. Compute resources can be configured at the vSphere layer to ensure physical and logical separation of resources between functional areas such as Production, and Testing and Development (Test/Dev).

Networking

Valid concerns exist around information leakage and “noisy neighbors” on a shared network infrastructure. Consumers of the provisioned resources must operate in a dedicated environment and benefit from infrastructure standardization. To address these concerns, Enterprise Hybrid Cloud was designed for multitenancy with a defense-in-depth perspective, which is demonstrated through:

- Implementation of virtual local area networks (VLANs) to enable isolation at Layer 2 throughout Enterprise Hybrid Cloud and where it intersects with the enterprise network.
- Implementation of a physical Layer 3 boundary within the environment to provide more isolation by using dedicated networks, isolated routing environments, and opportunities for ACL.
- Support for dynamic routing protocols that allow for automation of networks from software into the physical network environment.
- Network designs that allow for IP mobility through multisite disaster recovery protection services that integrate into the customer’s existing network.

VMware NSX for vSphere

Enterprise Hybrid Cloud can employ VMware NSX for vSphere to offer significant value-added benefits. Enhanced networking and security features in VMware NSX include:
Hybrid cloud features and functionality

- **VMware NSX logical routing and firewalls**—Provides line-rate performance by moving the routing and firewalling operations closer to the virtual machine workload to improve performance and scalability.

- **VXLAN**—Uses overlay networks to segment tenant traffic. It is software that allows for automated provisioning.

- **Distributed logical routers**—Route east-west traffic within the hypervisor when the source and target virtual machines reside on the same host. Routing of east-west traffic is optimized throughout as routing decisions are made at the hypervisor layer, eliminating unnecessary traffic to a north-south router.

- **Logical load balancer**—Enables load sharing across a pool of virtual machines with configurable health check monitoring and application-specific rules for service high availability, URL rewriting, and advanced Secure Sockets Layer (SSL) handling. A distributed firewall enables consistent data-center-wide security policies.

- **Security features**—NSX provides a number of security enhancements over traditional networks. Automated security policies and firewall rules allow isolation of workload regardless of location or IP address details. This includes segmentation of workloads in the same L2 network.

**Security**

Enterprise Hybrid Cloud enables customers to enhance security by establishing a hardened security baseline across the hardware and software stacks supporting their Enterprise Hybrid Cloud infrastructure. Enterprise Hybrid Cloud helps to reduce concerns around the complexities of the underlying infrastructure by showing how to tightly integrate an as-a-service solution stack with a public key infrastructure (PKI) and a common authentication directory to provide centralized administration and tighter control over security.

*Note:* This PKI and authentication directory may pre-exist in the customer environment, as a result providing the integration point between Enterprise Hybrid Cloud and a customer’s existing security management infrastructure.

Enterprise Hybrid Cloud addresses the challenges of securing authentication and configuration management to comply with industry and regulatory standards through:

- Securing the infrastructure with PKI support for authenticity, non-repudiation, and confidentiality
- Converging the various identity sources into a single directory to enable a centralized point of administration and policy enforcement
- Using configuration management tools to generate infrastructure reports for audit and compliance purposes

For details, refer to the *Enterprise Hybrid Cloud 4.1.2 Security Management Guide.*
Enterprise Hybrid Cloud enables customers to take advantage of the proven benefits of Dell EMC storage in an Enterprise Hybrid Cloud environment. Using ViPR Controller storage services and Dell EMC XtremIO™, Dell EMC ScaleIO™, Dell EMC VNX™, EMC Unity™ and Dell EMC VMAX™ capabilities, Enterprise Hybrid Cloud provides policy-based, software-defined storage management of Dell EMC block and file storage.

With scalable storage architecture that uses the latest flash and tiering technologies, XtremIO, ScaleIO, VNX, and VMAX storage arrays enable customers to satisfy any workload requirements with maximum efficiency and performance, in the most cost-effective way. With ViPR Controller, the storage configuration is abstracted and presented as a single storage control point.

Storage administrators maintain control of storage resources and policies while enabling the cloud administrator to provision automatically to the cloud infrastructure.

Enterprise Hybrid Cloud uses a combination of tools to provide environmental visibility and alerts that are required to ensure service levels proactively in virtual and cloud environments. Using vRealize Automation and tools that are provided by Dell EMC, administrators and end users can dynamically add resources as needed, based on their performance requirements.

Infrastructure administrators manage storage, compute, and network resources within resource pools, while end users manage their resources at a virtual machine level to achieve the service levels required by their application workloads.

Cloud users can select from a range of service levels of compute, storage, and data protection for their applications to achieve the most efficient use of the resources within their software-defined data center environment.

Enterprise Hybrid Cloud features automated monitoring capabilities that provide IT administrators with a comprehensive view of the cloud environment to enable intelligent decision making for resource provisioning and allocation. These capabilities are based on a combination of VMware vRealize Operations Manager dashboards, alerts, and analytics, using extensive storage detail provided through Dell EMC analytics adapters.

vRealize Operations Manager provides pre-built and configurable dashboards for real-time performance, capacity, and configuration management. Performance data is interpreted and assigned a health risk value, and efficiency metrics that enable IT administrators to identify evolving performance problems easily.

The ViPR Analytics and Dell EMC Storage Analytics (ESA) management packs are presented through the vRealize Operations Manager custom interface. This enables administrators to identify the health of ViPR Controller virtual arrays quickly as well as Dell EMC RecoverPoint™, Avamar, RecoverPoint for Virtual Machines, ScaleIO, VMAX, VNX, XtremIO, and VPLEX™ storage systems using customized Dell EMC dashboards for vRealize Operations Manager, such as the ViPR Controller dashboard, as shown in Figure 3.
Figure 3. ViPR Analytics with VMware vRealize Operations Manager

Capacity analytics in vRealize Operations Manager identify over-provisioned resources so they can be right-sized for the most efficient use of virtualized resources. What-if scenarios eliminate the need for separate performance and capacity modeling.

ViPR SRM is storage resource management software that offers comprehensive monitoring and reporting for Enterprise Hybrid Cloud. ViPR SRM helps IT departments visualize, analyze, and optimize their software-defined storage infrastructure. Cloud administrators can use ViPR SRM to understand and manage the impact that storage has on their applications and view the topologies of their hybrid cloud from application to storage. Capacity and consumption of ViPR software-defined storage and service-level agreement (SLA) issues can be identified through real-time dashboards and reports to meet the needs of the wide range of hybrid cloud consumers.

In addition, VMware vRealize Log Insight provides the ability to centralize and aggregate system and application logs. Each system in Enterprise Hybrid Cloud can be configured to forward logs to the Log Insight system for event analytics and reporting. When configured with VMware vRealize Log Insight, Dell EMC content packs provide customizable dashboards and user-defined fields specifically for those Dell EMC products that enable administrators to conduct problem analysis and analytics on the storage array and backup infrastructure.

Enterprise Hybrid Cloud uses VMware vRealize Business for Cloud to provide cloud administrators with metering and cost information across all business groups in the enterprise. vRealize Business for Cloud reports the virtual machine and blueprint costs based on business units and application groups across the hybrid cloud environment.

vRealize Business for Cloud uses its own reference database, which has been preloaded with industry-standard and vendor-specific cost data to compute the cost of virtual CPU (vCPU), RAM, and storage. These prices are automatically consumed by vRealize
Automation, where the cloud administrator may change them appropriately. This eliminates the need to configure cost profiles manually and assign them to compute resources in vRealize Automation.

vRealize Business for Cloud is integrated into the vRealize Automation portal for the cloud administrator and presents a dashboard overview of the hybrid cloud infrastructure, as shown in Figure 4.

Data protection backup services
Using Dell EMC customizations for vRealize Orchestrator workflows, administrators can quickly and easily define multilayer data protection policies that users can choose when provisioning their virtual machines. The backup infrastructure takes advantage of Avamar and Data Domain features such as deduplication, compression, and VMware integration.

Avamar provides scalable backup and restore capabilities with integrated data deduplication. This reduces total disk consumption by up to 50 times, enabling cost-effective, long-term retention on Avamar Data Store servers. Avamar can optionally use a Data Domain appliance as the backup target.
Data Protection Advisor™ automates and centralizes the collection and analysis of all data across backup applications, replication technologies, the virtual environment, and supporting infrastructure, providing a single, comprehensive view of your data protection environment and activities.

Using the vRealize Automation application program interface (API) and extensibility toolkits, Enterprise Hybrid Cloud implements custom functionality to provide Avamar-based, image-level backup services for applications and file systems within a single-organization or multiorganization hybrid cloud environment.

**Continuous availability**

A combination of VPLEX, VMware vSphere vMotion, and VMware vSphere High Availability enables hybrid cloud users to distribute applications and their data effectively across multiple sites or within the same site over synchronous distances. With virtual storage and virtual servers working together over distance, your infrastructure can provide load balancing, real-time remote data access, and improved application protection. All mobility and migration of live systems is seamlessly executed between sites, completely transparent to users and applications.

**Disaster recovery**

Enterprise Hybrid Cloud allows cloud administrators to enable disaster recovery protection for their applications and virtual machines when deploying from the vRealize Automation self-service catalog.

Two disaster recovery options are available:

- **RecoverPoint for Virtual Machines-based disaster recovery**—This option provides IT consumers with any point-in-time protection from outages, corruptions, or disasters for individual, or groups of, virtual machines by using the self-service catalog. IT consumers can use the self-service catalog at any time throughout the lifecycle of the virtual machine workload to add, modify, or delete EMC RecoverPoint for Virtual Machines protection. Cloud Administrators can manage automated failover and failback of individual or groups of virtual machines to minimize data loss and application downtime.

- **Site Recovery Manager-based disaster recovery**—Dell EMC customizations automatically place these systems on storage that is protected remotely by EMC RecoverPoint. VMware vCenter Site Recovery Manager, through tight integration with the ViPR Controller Storage Replication Adapters, can automate the recovery of all virtual storage and virtual machines at a recovery or failover site.

**Encryption**

Enterprise Hybrid Cloud allows administrators to use CloudLink SecureVM to apply portable encryption to applications and virtual machines. Dell EMC customizations allow administrators to select the virtual machine volumes to encrypt and then apply encryption to the virtual machines automatically when they provision applications and workloads from the vRealize Automation self-service catalog across multiple sites.
Enterprise Hybrid Cloud enables IT organizations to broker public cloud services. Enterprise Hybrid Cloud has been validated with VMware vCloud Air as a public cloud option that can be accessed directly from a self-service portal by administrators and users. End users can provision virtual machines while IT administrators can perform virtual machine migration (offline) from the on-premises component of their hybrid cloud to vCloud Air using VMware vCloud Connector.

**Dell EMC and VMware integration**

Enterprise Hybrid Cloud significantly simplifies the deployment of a cloud management stack by engineering a platform with many developed and tested integration points between Dell EMC and VMware products.

Figure 5 shows the breadth of integration that is pre-engineered for Enterprise Hybrid Cloud customers.

![Diagram of Enterprise Hybrid Cloud integration points](image-url)
Enterprise Hybrid Cloud storage-as-a-service operations offer catalog-driven storage operations from relevant converged and hyper-converged infrastructure platforms. Managed through ViPR Controller and the ViPR Controller plug-in for VMware vRealize Orchestrator, Enterprise Hybrid Cloud provides an orchestration interface to the ViPR Controller software platform to automate common ViPR operations, such as Virtual Machine File System (VMFS) or Network File System (NFS) datastore provisioning.

The ViPR Management Pack and Storage Analytics for vRealize Operations Manager provide preconfigured dashboards for Dell EMC resources such as VNX, VMAX, VPLEX, ScaleIO, XtremIO, Isilon, RecoverPoint for Virtual Machines, and Avamar, enabling users to view the storage metrics and topologies of the virtualized and physical storage and backup components supporting the Enterprise Hybrid Cloud environment.

Dell EMC also provides storage and data protection content packs for use with VMware vRealize Log Insight. Content packs for VNX and VMAX provide dashboards and user-defined fields specifically for those Dell EMC products that enable administrators to conduct problem analysis.

ViPR Controller Storage Provider plays a key role in Enterprise Hybrid Cloud in identifying the capabilities of the storage that is presented to ESXi servers managed by vCenter. A storage profile is created in vCenter for each class, or tier, of storage presented by ViPR. These storage profiles are used by VMware vRealize Business to classify and charge for each tier of storage that is presented and consumed in vRealize Automation.

Key components

Introduction

This section describes the key components of Enterprise Hybrid Cloud, as shown in Figure 6.

- VMware vRealize Suite including:
  - VMware vRealize Automation
  - VMware vRealize Orchestrator
  - VMware vRealize Operations Manager
  - VMware vRealize Business for Cloud
  - VMware vRealize Log Insight
- VMware vSphere ESXi and VMware vCenter Server
- VMware NSX for vSphere
- VMware vCenter Site Recovery Manager
- VMware vSAN
- Dell EMC ViPR Controller software-defined storage
- Dell EMC VxBlock™, Dell EMC VxRack™, and Dell EMC VxRail™ converged and hyper-converged infrastructure systems
Key components

- Dell EMC Unity, Dell EMC VNX, VMAX, ScaleIO, VPLEX, Dell EMC Isilon™, and XtremIO storage platforms
- Dell EMC RecoverPoint for Virtual Machines (DR customers only)
- Dell EMC RecoverPoint (DR customers only)
- Dell EMC Avamar and Dell EMC Data Domain data protection platforms
- Dell EMC ViPR SRM and Data Protection Advisor
- Dell EMC CloudLink SecureVM

Figure 6. Enterprise Hybrid Cloud components

**VMware vRealize Automation**

VMware vRealize Automation enables customized, self-service provisioning and lifecycle management of cloud services that comply with established business policies across multiple sites. vRealize Automation provides a secure portal where authorized administrators, developers, and business users can request new IT services and manage existing computer resources from predefined user-specific menus.

**VMware vSphere ESXi and VMware vCenter Server**

VMware vSphere ESXi is a virtualization platform for building cloud infrastructures. vSphere enables you to run your business-critical applications confidently to meet your most demanding SLAs at the lowest total cost of ownership (TCO). vSphere combines this virtualization platform with the management capabilities of VMware vCenter Server. Enterprise Hybrid Cloud gives you operational insight into the virtual environment for improved availability, performance, and capacity utilization.

**VMware vRealize Orchestrator**

VMware vRealize Orchestrator is an IT process automation engine that helps automate the cloud and integrates the vCloud Suite with the rest of your management systems. vRealize Orchestrator enables administrators and architects to develop complex automation tasks within the workflow designer. The vRealize Orchestrator library of pre-
built activities, workflows, and plug-ins helps accelerate the customization of vRealize Automation standard capabilities.

**VMware NSX for vSphere**

VMware NSX for vSphere is the next generation of software-defined network virtualization and offers additional functionality and improved performance over vCloud Networking and Security and traditional network and security devices. This additional functionality includes distributed logical routing, distributed firewalling, logical load balancing, and support for routing protocols such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Open Shortest Path First (OSPF).

Where workloads on different subnets share the same host, the distributed logical router optimizes traffic flows by routing locally. This enables substantial performance improvements in throughput, with distributed logical routing and firewalling providing line-rate performance distributed across many hosts, instead of being limited to a single virtual machine, or physical host. VMware NSX also introduces Service Composer which integrates with third-party security services.

**VMware vRealize Operations Manager**

VMware vRealize Operations Manager is the key component of the vRealize Operations Management Suite. It provides a simplified approach to operations management of vSphere, and physical and cloud infrastructures. vRealize Operations Manager provides operations dashboards to gain insights and visibility into the health, risk, and efficiency of your infrastructure, performance management, and capacity optimization capabilities.

**VMware vRealize Log Insight**

VMware vRealize Log Insight delivers automated log management through log aggregation, analytics, and search capabilities. With an integrated cloud operations management approach, it provides the operational intelligence and enterprise-wide visibility that is required to enable service levels proactively and optimize operational efficiency in dynamic hybrid cloud environments.

**VMware vRealize Business for Cloud**

VMware vRealize Business for Cloud delivers the insight IT infrastructure and operations teams need to most efficiently deploy and manage cloud environments. The cost, consumption, comparison, and planning capabilities in vRealize Business for Cloud provide an easy on-ramp for organizations just getting started with cloud computing. Essential for effectively managing hybrid cloud environments, the business management features in vRealize Business for Cloud accelerate time to value.

**VMware vCenter Site Recovery Manager**

VMware vCenter Site Recovery Manager is a disaster recovery management solution that provides automated orchestration and non-disruptive testing of centralized recovery plans to simplify disaster recovery for virtualized applications. Site Recovery Manager integrates with RecoverPoint replication and ViPR automated storage services by means of Storage Replication Adapters (SRAs).

Site Recovery Manager reduces the time and effort that is required to set up and maintain recovery plans. Its simple, centralized recovery plans require significantly less time and coordination to update regularly than complicated, manual runbooks.
**VMware Platform Services Controller**

A VMware Platform Services Controller groups a set of infrastructure services, including vCenter Single Sign-On, License Service, Lookup Service, and VMware Certificate Authority. Enterprise Hybrid Cloud leverages distinct virtual machines (external Platform Services Controllers) to provide these services.

**Dell EMC ViPR Controller**

EMC ViPR Controller is storage automation software that centralizes and transforms multivendor storage into a simple and extensible platform. It abstracts and pools resources to deliver automated, policy-driven storage services on demand through a self-service catalog.

**Dell EMC VNX and Dell EMC VMAX**

EMC VNX and EMC VMAX are powerful, trusted, and smart storage arrays that provide the highest level of performance, availability, and intelligence in the hybrid cloud. VNX and VMAX storage systems offer a broad array of functionality and tools, such as the fully automated storage tiering for virtual pools (FAST VP), enabling multiple storage service levels to support ViPR-driven STaaS offerings in the hybrid cloud environment.

**Dell EMC Unity**

Dell EMC Unity all-flash and hybrid flash storage platforms optimize SSD performance and efficiency, with fully integrated SAN and NAS capabilities. Cloud-based storage analytics and proactive support keep your system available and connected.

**Dell EMC XtremIO**

Dell EMC XtremIO is an all-flash scale-out enterprise storage array that provides substantial improvements to I/O performance. Purpose-built to use flash media, XtremIO delivers new levels of real-world performance, administrative ease, and advanced data services for applications.

**Dell EMC ScaleIO**

Dell EMC ScaleIO is a software-only server-based SAN that brings together storage and compute resources to form a single-layer, enterprise-grade storage product. ScaleIO storage is elastic and delivers linearly scalable performance. Its scale-out server SAN architecture can grow from a few to thousands of servers.

**Dell EMC Isilon**

Dell EMC Isilon is a scale-out network-attached storage (NAS) storage platform that provides a powerful, simple, and efficient way to consolidate and manage enterprise data and applications. Its OneFS Operating System intelligently combines file system, volume manager, and data protection across all nodes within a cluster.

**Dell EMC RecoverPoint**

Dell EMC RecoverPoint is an advanced data protection, replication, and disaster recovery solution designed with the performance, reliability, and flexibility required for enterprise applications in heterogeneous storage and server environments. It provides local replication and bi-directional remote replication for physical, virtual, and cloud environments.
**Key components**

**Dell EMC VPLEX**
The Dell EMC VPLEX family removes physical barriers within, across, and between data centers. VPLEX Local provides simplified management and non-disruptive data mobility for heterogeneous arrays. VPLEX Metro™ provides data access and mobility between two VPLEX clusters within synchronous and asynchronous distances respectively. With unique scale-out architecture, VPLEX advanced data caching and distributed cache coherency provide:

- Workload resiliency
- Automatic sharing, balancing, and failover of storage domains
- Local and remote data access with predictable service levels

**Dell EMC ViPR SRM**
Dell EMC ViPR SRM provides comprehensive monitoring, reporting, and analysis for heterogeneous block, file, and virtualized storage environments. It enables you to visualize applications to storage dependencies, monitor and analyze configurations and capacity growth, as well as optimize your environment to improve return on investment (ROI).

**VMware vSAN**
VMware vSAN (formerly Virtual SAN), is an industry-leading software powering this hyper-converged infrastructure solution. vSAN simplifies enterprise IT, reduces total cost of ownership, and provides flexible scalability while delivering predictable performance.

**Dell EMC storage integration with VMware**
Both VNX and VMAX support VMware vSphere Storage APIs – Array Integration, which offloads virtual machine operation to the array to optimize server performance. Both platforms also support VMware vSphere Storage API for Storage Awareness, which enables VMware administrators to expose the underlying storage performance and protection details to assist them in creating virtual machine storage policies.

**Dell EMC ViPR and Dell EMC Storage Analytics**
Powered by vRealize Operations Management Suite, Dell EMC adapters for ViPR and ESA combine to provide a powerful management tool for VMware and storage administrators to access real-time intelligent analytics for the ViPR software-defined storage layer and the individual VNX, VMAX, VPLEX, and XtremIO platforms. Administrators can get detailed statistics through customizable dashboards, heat maps, and alerts and access topology mappings in a VMware environment.

**Dell EMC data protection workflows for vRealize Orchestrator**
With vRealize Orchestrator, cloud administrators can use data protection workflows to automate Avamar and Data Domain protection of virtual machine workloads. These workflows are added to the vRealize Automation virtual machine provisioning blueprints so that cloud users can easily set up protection at provisioning time and request on-demand restores for specific virtual machines, where they can choose to restore from all available backups.
Cloud infrastructure administrators can also use workflows that carry out the entire protection policy setup on Avamar and vCenter, to facilitate quick and easy deployment of the infrastructure that is required to support end-user protection needs.

**Dell EMC Storage Replication Adapters**

Dell EMC’s SRAs ensure tight integration between VMware vCenter Site Recovery Manager and the RecoverPoint and ViPR products. The SRAs automate the replication and data-sync operations for coordinated disaster recovery failovers and planned migrations.

The RecoverPoint Storage Replication Adapter for VMware vCenter Site Recovery Manager enables Site Recovery Manager to implement disaster recovery using RecoverPoint. The RecoverPoint SRA supports Site Recovery Manager functions, such as failing over, failing back, and failover testing, using RecoverPoint as the replication engine.

The ViPR Controller Storage Replication Adapter for VMware vCenter Site Recovery Manager provides the same functionality for protected storage that is provisioned using EMC ViPR Controller.

**Dell EMC RecoverPoint for Virtual Machines**

Dell EMC RecoverPoint for Virtual Machines is a fully virtualized hypervisor-based replication and automated disaster recovery solution that is highly integrated into the VMware cloud management software. Virtual RecoverPoint appliances are easily installed on any existing ESXi servers with flexible deployment configurations. ESXi splitters reside on all servers with protected workloads, allowing replication and recovery at the virtual disk granularity level. Because the I/O splitter resides within the vSphere hypervisor, RecoverPoint for Virtual Machines can replicate virtual machines to and from any storage array that is supported by VMware.

**Dell EMC Avamar**

Dell EMC Avamar is a fast, efficient backup and recovery system that is provided through a complete software and hardware solution. Equipped with integrated variable-length deduplication technology, Avamar backup and recovery software provides integrated source and global data deduplication, which facilitates fast, full daily backups for hybrid cloud environments.

**Dell EMC Data Domain**

With Avamar, you can choose to direct backups to a Dell EMC Data Domain system instead of the Avamar server. Data Domain deduplication storage systems deduplicate data inline so that written data is already deduplicated on the disk, and requires less disk space than the original dataset. With Data Domain, you can retain backup and archive data on site longer to enable quick and reliable data restores from disk.

**Dell EMC Data Protection Advisor**

With Dell EMC Data Protection Advisor (DPA), you can automate and centralize the collection and analysis of all data across backup applications, replication technologies, the virtual environment, and supporting infrastructure. This provides a single, comprehensive view of your data protection environment and activities. In addition, when integrated with...
Enterprise Hybrid Cloud Data Protection Backup vRealize Orchestrator workflows, DPA provides on-demand reporting of backup statistics and status.

**Dell EMC Secure Remote Support (ESRS)**
ESRS allows Dell EMC personnel to monitor the health of Dell EMC storage arrays in the converged platform remotely, and perform support and maintenance functions. ESRS serves as the conduit for all communications between Dell EMC and the Dell EMC storage arrays. ESRS monitors the health of multiple Dell EMC storage arrays. Dell EMC ESRS is integrated into the Dell EMC base software suite.

**Advanced Management Platform (AMP)**
AMP provides the infrastructure and tools to jump-start the system build and to provide out-of-band management, monitoring, and troubleshooting. It is available in high-availability (HA) and mini-AMP versions.

AMP-2HAP is the second-generation Advanced Management Platform model that provides automatic failover and load balancing of virtual machines (VMs) that are deployed to implement Core and Optional management workloads. The performance option (P) consists of the base configuration plus a third Cisco UCS rack server and 100-GB flash drives to implement FAST VP.

**Dell EMC Vision Intelligent Operations**
The Dell EMC Vision™ software suite provides an integrated set of software products to manage a data center. Vision software is the first software suite to provide an intelligent solution to manage operations in a converged infrastructure environment. These tools enable and simplify converged operations by dynamically providing a high level of intelligence into a customer’s existing management toolset.

**XtremIO Management Server (XMS)**
XMS is a stand-alone dedicated Linux-based server that is used to control the XtremIO system. Each XtremIO cluster requires its own XMS host, which can be either a physical or a virtual server. The array continues to operate if it is disconnected from the XMS, but cannot be configured or monitored.

**Solution architecture**

**Overview**
Enterprise Hybrid Cloud requires distinct functions (known as pods) for management operations. Each pod represents a collection of technologies and components that are designed to provide its function.

How each function and its components are overlaid on the physical infrastructure is flexible, based on:

- The environment and infrastructure type to which they are being deployed
- The overall protection levels that are desired within the environment

*Note: Do not assume that a management pod equates directly to an ESXi cluster.*
During initial deployment of Enterprise Hybrid Cloud, the full management stack must be deployed, including the automation and management components that support the orchestration of the entire environment. Subsequent remote or local endpoints require only a subset of the management stack. The following sections describe both the full and endpoint management stacks.

Full management stack components

When Enterprise Hybrid Cloud is deployed, the first geographic location requires a full management stack to be deployed. Figure 7 shows how the components of the full management stack are distributed among the management pods.

Figure 7. Enterprise Hybrid Cloud full management stack

Note: Figure 7 includes ViPR Controller and ViPR SRM. Neither component is required in VxRail Appliance deployments where vSAN storage is used.

Core Pod

The Core Pod hosts a core set of resources that must exist before the remainder of the cloud can be deployed. These core resources include vCenter Server, Microsoft SQL Server 2012, and VMware NSX Manager. The Core Pod also contains Log Insight forwarders and vRealize Operations Manager collectors to localize and optimize the collection of logs and network usage.
Solution architecture

**Automation Pod**
The Automation Pod hosts the virtual machines that automate and manage the cloud infrastructure supporting the workloads consumed by the cloud’s tenants. The Automation Pod supports the components responsible for functions such as the user portal and automated provisioning, monitoring, metering, and reporting.

**NEI Pod**
The Network Edge Infrastructure (NEI) Pod hosts the VMware NSX Load Balancer, VMware NSX Edge appliances, VMware NSX Distributed Logical Routers (DLRs), and VMware NSX Controllers and is only required if VMware NSX is in use. The NEI Pod becomes the convergence point at which the physical and virtual networks connect.

**Workload Pods**
The Workload Pods are configured and assigned in vRealize Automation as shared resources, to host tenant virtual machines that are deployed by the different business groups in the hybrid cloud environment. These Workload Pods are deployed as VMware vSphere clusters within VMware vCenter endpoints.

**Endpoint management stack**

When an additional vCenter endpoint is configured for use within Enterprise Hybrid Cloud, that endpoint only requires a subset of the management stack to operate. Figure 8 shows the components of the endpoint management stack that are distributed among the management pods.

As with the full management stack, the NEI Pod function is required only if VMware NSX is being used. vRealize Automation Agents are deployed for each endpoint to follow best practice and ensure predictable performance.
Enterprise Hybrid Cloud uses standard VMware- and Dell EMC-supported I/O devices to support Ethernet and Fibre Channel (FC) connectivity.

The VMware Compatibility Guide provides detailed lists of vendor devices that have been either physically tested or are similar to the devices tested by VMware or VMware partners.

Resource sizing information is provided in Resource sizing.

**Protection services**

**Protection service offerings**

Enterprise Hybrid Cloud provides Data Protection services in the form of Backup and Restore, Continuous Availability, and Disaster Recovery, which are offered as five types of protection services:

- **Single-site protection**—Designed to operate when only a single site is available, or when workloads do not require replicated storage or replicated backups. It may be used in its own right, or as the base deployment on top of which you can layer additional multisite service levels. Suitable when you have just a single site and therefore do not require inter-site protection.

- **Continuous Availability (Single Site) protection**—Designed to provide storage and compute resilience for workloads on the same site, using shared backup infrastructure but maintaining nonreplicated backups. Suitable when you want to provide additional resilience for single-site workloads.

- **Continuous Availability (Dual site) protection**—Designed to provide storage and compute resilience for workloads across sites, using local shared backup infrastructure and replicating backup images between sites. It is intended for metro-distance geographic separation. Suitable when you want to provide inter-site resilience for workloads and have two sites within a 10ms latency of each other.

- **Disaster Recovery (RecoverPoint for Virtual Machines) protection**—Designed to provide storage and compute resilience for workloads across sites, using local shared backup infrastructure and replicating backup images between sites. It is intended for distances outside the metro range, allowing virtual machine workloads to be recovered individually. Suitable when you want to provide inter-site resilience for workloads and want individual workload level failover, but have sites greater than 10ms latency apart.

- **Disaster Recovery (Site Recovery Manager) protection**—Designed to provide storage and compute resilience for workloads across sites, using local shared backup infrastructure and replicating backup images between sites. It is intended for distances outside the metro range, allowing virtual machine workloads to be recovered at the ESXi cluster level of granularity. Suitable when you want to provide inter-site resilience for workloads, but have sites greater than 10ms latency apart.
Enterprise Hybrid Cloud provides intra-site and inter-site protection features that can be combined to offer multiple tiers of service to different workloads within the same Enterprise Hybrid Cloud deployment. The attributes of the protection levels include:

- **Converged/Hyper-converged Infrastructure Redundancy**—Virtual machine workloads with this availability attribute benefit from the redundancy of the internal components of a converged infrastructure platform such as VxBlock Systems, VxRack Systems, or VxRail Appliances including redundant compute, network, and storage components.

- **Inter-Converged/Hyper-converged Infrastructure Redundancy**—Virtual machine workloads with this availability attribute are insulated against failure of a converged infrastructure platform by replicating that workload to a second converged infrastructure platform on the same site.

- **Inter-Site Redundancy**—Virtual machine workloads with this availability attribute are insulated against failure of an entire site location by replicating that workload to a second converged infrastructure platform on an alternate site.

- **Local Backup**—Virtual machine workloads with this availability attribute are backed up locally to shared backup infrastructure with a single copy of each backup image retained.

- **Replicated Backup**—Virtual machine workloads with this availability attribute are backed up locally to shared backup infrastructure. Each backup image is replicated to and restorable from a shared backup infrastructure on an alternate site.

Table 1 shows the protection level options and their attributes.

**Table 1. Available Enterprise Hybrid Cloud protection service levels**

<table>
<thead>
<tr>
<th>Protection service level</th>
<th>Converged/ hyper-converged infrastructure redundancy</th>
<th>Inter-converged/ hyper-converged infrastructure redundancy</th>
<th>Inter-site redundancy</th>
<th>Local backup</th>
<th>Replicated backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Site</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Continuous Availability</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>(Single Site)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Availability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Dual Site)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(RecoverPoint for Virtual Machines)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Site Recovery Manager)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Protection services may be combined within a single Enterprise Hybrid Cloud environment to offer multiple tiers of service. The protection services may be combined as shown in Table 2.

Table 2. Supported combination of protection services

<table>
<thead>
<tr>
<th>Protection</th>
<th>Single Site</th>
<th>CA (1 Site)</th>
<th>CA (2 Site)</th>
<th>DR RP4VMs</th>
<th>DR SRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Site</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>CA (1 Site)</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>CA (2 Site)</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>DR RP4VMs</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>DR SRM</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9 shows an example of combining protection services in an Enterprise Hybrid Cloud environment. For more details about each combination, refer to the Enterprise Hybrid Cloud 4.1.2 Concepts and Architecture Guide.
Figure 9. Combining Single Site, Continuous Availability, RecoverPoint for Virtual Machines-based disaster recovery and Site Recovery Manager-based disaster recovery protection services

Note: Figure 9 shows the concept of hardware islands. Hardware islands allow multiple converged infrastructure platforms to be logically aggregated (for scale) or partitioned (for isolation) inside a single vCenter while retaining awareness of physical network, storage, and site boundaries. This awareness is then used to ensure that correct inter-site and intra-site protection services are applied to cloud workloads. For more information about hardware islands, refer to the Enterprise Hybrid Cloud 4.1.2 Concepts and Architecture Guide.
Converged and hyper-converged systems support

Figure 10 shows the converged and hyper-converged systems that Enterprise Hybrid Cloud supports and the relevant services supported on each system.

Note: The VxRack Flex System supports the RecoverPoint for Virtual Machines disaster recovery option only. It does not support continuous availability or vCenter Site Recovery Manager-based disaster recovery, because those protection services use LUN level replication with VPLEX and RecoverPoint respectively.

Note: Existing Vblock customers must convert to VxBlock Systems before deploying Enterprise Hybrid Cloud.

Note: VxRail Appliances do not use Enterprise Hybrid Cloud storage-as-a-service operations because all vSAN storage is fully pre-provisioned at time of VxRail initialization.

VxBlock Systems simplify all aspects of IT and enable organizations to achieve better business outcomes faster. Seamlessly integrating best-in-class compute, network, and storage technologies from industry leaders Dell EMC, Cisco, and VMware, VxBlock Systems provide dynamic pools of resources that can be intelligently provisioned and
Converged and hyper-converged systems support

managed to address changing demands and rapidly shifting business opportunities. Engineered to exacting specifications for the highest levels of performance, capacity, availability, and security, VxBlock Systems address a need for increased choice of network virtualization solutions using VMware NSX.

Dell EMC VxRack Systems

Dell EMC VxRack System 1000 Series is a new hyper-converged offering that complements VCE converged infrastructure systems. These self-contained units of servers and networking are well-suited for the rapid growth in next-generation applications—enabling you to support a growing number of use cases with built-in resiliency and less stringent availability and performance requirements on infrastructure. The VxRack System 1000 Series can incorporate alternate software-defined storage technologies, a choice of hypervisors, and bare metal workloads.

**Note:** Only the VxRack System with FLEX model is supported by Enterprise Hybrid Cloud 4.1.2.

Dell EMC VxRail Appliance

The VxRail Appliance is a hyper-converged infrastructure appliance that delivers virtualization, compute, storage, networking, and data protection in an agile, scalable, and easy-to-manage SDDC Building Block. VxRail Appliances are fully integrated, preconfigured, pretested VMware HCI appliances that scale-out linearly in common modular building blocks that are based on business needs. VxRail Appliances deliver resiliency, quality of service (QoS), and centralized management functionality that enables faster, better, and simpler management of consolidated workloads, virtual desktops, business critical applications, and remote office infrastructure. VxRail Appliances provide the flexibility of a broad set of configuration options at a variety of price and scale points.
Converged and hyper-converged systems support

Figure 11 shows how the full Enterprise Hybrid Cloud management stack components overlay on VxRail Appliance converged infrastructure.

In this case, the Data Protection Module uses EMC Avamar Virtual Edition and EMC Data Domain virtual edition. Data Domain is placed on a separate Dell PowerEdge server to provide a separate fault domain for backup images.

Figure 11. Enterprise Hybrid Cloud Management pod overlay on VxRail Appliance
Converged and hyper-converged systems support

Converged infrastructure management overlay – VxRack System with FLEX

Figure 12 shows how the full Enterprise Hybrid Cloud management stack components overlay on VxRack FLEX converged infrastructure.

Figure 12. Enterprise Hybrid Cloud Management pod overlay on VxRack System architecture
Figure 13 shows how the full Enterprise Hybrid Cloud management stack components overlay on VxBlock System converged infrastructure.
This section provides details, by category, of the software that is certified in Enterprise Hybrid Cloud.

**Note**: For up-to-date supported version information, refer to the [Enterprise Hybrid Cloud Support page](#).

**Table 3. Array software**

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC Enginuity™ for VMAX2</td>
<td>Operating environment for VMAX</td>
</tr>
<tr>
<td>Dell EMC Enginuity for VMAX3</td>
<td>Operating environment for VMAX3</td>
</tr>
<tr>
<td>Dell EMC VNX1 Operating Environment</td>
<td>Operating environment for VNX1 block and file</td>
</tr>
<tr>
<td>Dell EMC VNX2 Operating Environment</td>
<td>Operating environment for VNX2 block and file</td>
</tr>
<tr>
<td>Dell EMC ScaleIO</td>
<td>Operating environment for ScaleIO</td>
</tr>
<tr>
<td>Dell EMC GeoSynchrony™</td>
<td>Operating environment for VPLEX</td>
</tr>
<tr>
<td>Dell EMC XtremIO</td>
<td>Operating environment for XtremIO</td>
</tr>
</tbody>
</table>

**Table 4. Dell EMC software**

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC Connectrix™ Manager Converged Network Edition (CMCNE)</td>
<td>Required by Dell EMC ViPR for Brocade SAN</td>
</tr>
<tr>
<td>Dell EMC PowerPath Virtual Edition</td>
<td>Multi-pathing and load balancing for ESXi hosts</td>
</tr>
<tr>
<td>Dell EMC PowerPath Virtual Appliance</td>
<td>License management for EMC PowerPath Virtual Edition</td>
</tr>
<tr>
<td>Dell EMC RecoverPoint</td>
<td>Dell EMC RecoverPoint software installed on RPAs</td>
</tr>
<tr>
<td>Dell EMC RecoverPoint Storage Replication Adapter (for Windows)</td>
<td>Dell EMC RecoverPoint Storage Replicator Adapter for VMware vCenter Site Recovery Manager</td>
</tr>
<tr>
<td>Dell EMC RecoverPoint for Virtual Machines</td>
<td>Virtual machine level replication for VMware vSphere</td>
</tr>
<tr>
<td>Dell EMC SMI-S Provider for VMAX (for Windows)</td>
<td>SMI-S Provider for Windows x64</td>
</tr>
<tr>
<td>Dell EMC Solutions Enabler for VMAX3 (for Windows)</td>
<td>SMI-S Provider for Windows x64</td>
</tr>
<tr>
<td>Dell EMC SMI-S Provider for VNX (for Windows)</td>
<td>SMI-S Provider for Windows x64</td>
</tr>
<tr>
<td>Dell EMC ViPR Controller</td>
<td>Dell EMC ViPR software-defined storage.</td>
</tr>
</tbody>
</table>
### Table 5. Dell EMC and VMware integration

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC Enterprise Hybrid Cloud Foundation Module</td>
<td>Customization package for STaaS and foundation workflows</td>
</tr>
<tr>
<td>Dell EMC Enterprise Hybrid Cloud Backup Module</td>
<td>Customization package for BaaS workflows</td>
</tr>
<tr>
<td>Dell EMC Enterprise Hybrid Cloud Disaster Recovery Module</td>
<td>Customization package for DRaaS workflows</td>
</tr>
<tr>
<td>Dell EMC ViPR Analytics</td>
<td>Dell EMC ViPR Analytics adapter for VMware vRealize Operations Manager</td>
</tr>
<tr>
<td>Dell EMC Storage Analytics</td>
<td>Dell EMC Storage Analytics adapter for VMware vRealize Operations Manager</td>
</tr>
<tr>
<td>Dell EMC ViPR Controller plug-in for VMware vRealize Orchestrator</td>
<td>Dell EMC ViPR Controller plug-in for vRealize Orchestrator workflows</td>
</tr>
</tbody>
</table>

### Table 6. Dell EMC backup and recovery

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC Avamar</td>
<td>Avamar system software</td>
</tr>
<tr>
<td>Dell EMC Data Domain Operating System (DD OS)</td>
<td>Operating system for Data Domain appliance</td>
</tr>
<tr>
<td>Dell EMC Data Protection Advisor</td>
<td>Data protection management software</td>
</tr>
</tbody>
</table>

### Table 7. VMware virtualization and cloud infrastructure

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>Database server for vCenter Server and vRealize Automation</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>Operating system (OS) for the server environment</td>
</tr>
<tr>
<td>VMware vRealize Automation</td>
<td>VMware cloud management and infrastructure</td>
</tr>
<tr>
<td>VMware vRealize Orchestrator Appliance</td>
<td>vRealize orchestration engine</td>
</tr>
<tr>
<td>VMware vRealize Orchestrator vRA Plug-in</td>
<td>vRealize Automation Center plug-in for vRealize Orchestrator</td>
</tr>
<tr>
<td>VMware vCenter Server (for Windows)</td>
<td>vSphere management server</td>
</tr>
<tr>
<td>VMware vSphere ESXi</td>
<td>Server hypervisor</td>
</tr>
<tr>
<td>VMware NSX for vSphere</td>
<td>Next-generation software-defined networking and security</td>
</tr>
</tbody>
</table>
Resource sizing

### Sample sizing

When sizing a hybrid cloud, it is important to size the management infrastructure so that it has adequate capacity to address the size of the resource clusters that are being planned for deployment.

This section provides sample management infrastructures for four different cloud sizes, namely 500, 1,000, 5,000, and 10,000 workload virtual machines. They are based on a number of assumptions that are likely, and are permitted, to differ in actual installations.

**Note:** The following sizing configurations are sample outputs from the Enterprise Hybrid Cloud Sizing Tool, and do not represent the only permitted configuration. To size for the individual requirements of your own hybrid cloud accurately, and to obtain the exact virtual machine sizing requirements for each component, refer to the EHC Management Sizing Tool, available at: [https://mainstayadvisor.com/go/emc](https://mainstayadvisor.com/go/emc).

### Table 8. Dell EMC security add-on

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC CloudLink SecureVM</td>
<td>Virtual machine encryption software</td>
</tr>
</tbody>
</table>
The following guidelines and assumptions were used when creating the sample management configurations.

- **Mandatory guidelines:**
  - CPU core over-subscription must be no greater than 2:1 for all Enterprise Hybrid Cloud management pods.
  - If a host fails, the ESXi cluster supporting the NEI Pod function (Edges and Controllers) must have at least four nodes when using VMware NSX to avoid a short-term network outage.
  - The ESXi cluster supporting the Automation Pod must have at least three nodes to meet ViPR best practices for ViPR node separation.
  - When an ESXi cluster that supports a management pod uses vSAN-based storage, there must be at least four nodes in the ESXi cluster to ensure that storage can suffer the loss of a cluster node without compromising storage integrity.

- **Recommended guidelines:**
  - Ensure that sufficient infrastructure exists to allow all virtual machines to run in steady state simultaneously.
  - NSX is the recommended networking technology and is used in these samples. **Note:** vSphere Distributed Switches are also supported.
  - Use vSphere HA in each management pod. To enable this, one additional node (ESX server) is suggested over and above the calculated requirements for each pod. **Note:** For ultimate resilience and ease of use during maintenance windows, creating vSphere clusters sizes based on N+2 may be appropriate based on customer preference, where N is the calculated CPU and RAM requirements for the hosted VMS plus host system overhead. The Enterprise Hybrid Cloud sizing tool sizes vSphere clusters based on an N+1 algorithm.
  - Ensure that calculated requirements include a buffer of 20 percent for RAM utilization in the Core, Automation, and NEI Pods (as in these examples). The minimum value that Dell EMC supports is 10 percent.
  - Ensure that calculated requirements include a buffer of 20 percent for CPU core utilization in the Core, Automation, and NEI Pods (as in these examples). The minimum value that Dell EMC supports is 10 percent.

- **Additional inputs were arbitrarily chosen for the purposes of these sample calculations:**
  - Servers for the Core Pod have 20 CPU cores and 256 GB RAM.
  - Servers for the NEI Pod have 10 CPU cores and 64 GB RAM.
  - Servers for the Automation Pod have 20 CPU cores and 256 GB RAM.
Note: Changing the server configuration changes the output. For the NEI Pod, Enterprise Hybrid Cloud mandates a minimum of four servers as NSX best practice recommends that each NSX controller be on a separate physical host and that VMware NSX Edge Services Gateway (ESG) and DLR virtual machines be on separate physical hosts.

- The average tenant resource virtual machine specification is 1 vCPU, 2 GB RAM, and 100 GB disk.
- The number of tenants is one.
- The number of transport zones is one.
- The required north/south bandwidth is 40 Gb/s.
- Datastores are to have 10 percent free capacity after components have reached full size.
- The user has chosen to deploy the Enterprise Hybrid Cloud Data Protection Module.
- The user has chosen to deploy ViPR SRM.
- vRealize Configuration Manager is used.
- vRealize Operations Manager retention is set to six months.
- VxBlock System 540 was the chosen converged infrastructure platform.
- Enterprise Hybrid Cloud single-site protection was the only level of protection chosen.

Cloud sizing sample

This section offers sample sizing of the management components that are required to manage sample clouds of 500, 1,000, 5,000, and 10,000 virtual machine workloads. Table 9 provides the detailed breakdown of the required components and the quantity of each component per cloud size.

<table>
<thead>
<tr>
<th>Management component</th>
<th>EHC</th>
<th>Cluster location</th>
<th>500 VM Cloud</th>
<th>1,000 VM Cloud</th>
<th>5,000 VM Cloud</th>
<th>10,000 VM Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud SQL Server</td>
<td>Core</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cloud vCenter Server (Appliance)</td>
<td>Core</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cloud vCenter PSC (Appliance)</td>
<td>Core</td>
<td>AMP</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Update Manager</td>
<td>Core</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Core</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NSX Controller</td>
<td>NEI</td>
<td>AMP</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Vision</td>
<td></td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vision MSM</td>
<td></td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PowerPath VAPP</td>
<td></td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ESRS VE</td>
<td></td>
<td>AMP</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Table 10 lists the physical hardware that is required for each of the respective Enterprise Hybrid Cloud pod functions. It is based on the Sizing guidelines and assumptions and the

<table>
<thead>
<tr>
<th>Management component</th>
<th>EHC function</th>
<th>Cluster location</th>
<th>500 VM Cloud</th>
<th>1,000 VM Cloud</th>
<th>5,000 VM Cloud</th>
<th>10,000 VM Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element Manager (SMI-S)</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Fabric Manager (Cisco DCNM)</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>XtremIO XMS (540 only)</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vR OPs Collector</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Log Insight Forwarder</td>
<td>AMP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vRA IaaS Agent Server</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NSX Enterprise Edge</td>
<td>NEI</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NSX Tenant Edge</td>
<td>NEI</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NSX DLR</td>
<td>NEI</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vRA Load Balancers</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vRA Appliance</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vRA IaaS DEM Server</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vRA IaaS Web Server</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vRA IaaS Manager Server</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Auto PSC</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Auto SQL</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ViPR Controller</td>
<td>Automation</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>vRealize Operations Manager</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Log Insight Manager</td>
<td>Automation</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>vRealize Business for Cloud</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vRO Appliance</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>DPA App Server</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DPA DB Server</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SRM Frontend</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SRM Primary Backend</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SRM Secondary Backend</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SRM Collector</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CloudLink Secure VM</td>
<td>Automation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VMware Configuration Manager</td>
<td>Automation</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
requirements that are required to satisfy the aggregate virtual machine requirements of the respective cloud sizes that are shown in Table 9.

Table 10. Sample cloud management platform: Physical hardware

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Number of physical hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>500 VM Cloud</td>
</tr>
<tr>
<td>AMP</td>
<td>3</td>
</tr>
<tr>
<td>Edge</td>
<td>4</td>
</tr>
<tr>
<td>Automation</td>
<td>3</td>
</tr>
</tbody>
</table>

Conclusion

Summary

Enterprise Hybrid Cloud enables customers to build an enterprise-class multitenant, scalable, platform for complete infrastructure-as-a-service lifecycle management. It provides on-demand access and control of infrastructure resources and security while enabling customers to maximize asset utilization. Specifically, Enterprise Hybrid Cloud integrates all the key functionality that customers demand of a hybrid cloud and provides a framework and foundation for adding other services.

Enterprise Hybrid Cloud incorporates the following principles:

- Self-service and automated provisioning
- Multitenancy and secure separation
- Security and compliance
- Elasticity and service assurance
- Monitoring
- Metering and showback
- Availability and data protection

Enterprise Hybrid Cloud uses the best of Dell EMC and VMware products and services to empower customers to accelerate the implementation and adoption of a hybrid cloud while enabling customer choice for the compute and networking infrastructure within the data center.