Reference Architecture Guide

EMC DESKTOP AS A SERVICE: VMWARE HORIZON DAAS WITH EMC XTREMIO ALL-FLASH ARRAY

EMC Solutions

March 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

Part Number H13869

Table of contents

Executive summary

Document purpose

This document describes the solution reference architecture for EMC desktop as a service (DaaS) with the VMware Horizon DaaS infrastructure. The solution uses an EMC® XtremIO™ all-flash array to provide storage for the virtual desktops and either an EMC Isilon® or EMC VNX® array to provide tenant user data storage. This document includes information about the main features and functionality of the solution and provides an overview of key components.

The *EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Solution Guide* provides more detailed information concerning deployment and implementation of this solution.

Solution purpose

This solution provides cloud service providers (CSPs) with a scalable, cost-effective DaaS platform. It offers easy deployment and outstanding performance, reliability, security, and manageability, while providing a rich mobile user experience.

This solution enables CSPs to offer enterprise customers a fully managed infrastructure. For CSPs, it provides a guided DaaS deployment, with build instructions, sizing guidelines, and best practices, and includes an optional post-deployment EMC Professional Services offering. In addition, CSPs can integrate the solution with their existing customer-facing portal, if they choose to do so.

Business case

Enterprise IT organizations seeking to decrease capital expenditures and shed administrative costs and responsibilities are increasingly turning to CSPs for managed DaaS offerings. These enterprises not only must understand the immediate impact on their operating expenses, but they also want the ability to confidently predict future subscription costs.

CSPs need a comprehensive offering that can provide a full range of services for their existing and potential enterprise customers, and they need a competitive DaaS solution that can be deployed quickly and effectively. Furthermore, for CSPs to increase their customer win rates, they must be able to calculate and communicate the per-desktop cost of the service according to the selected service-level structure.

EMC end-user computing (EUC) solutions enable CSPs to deliver virtual workspaces, including full desktops, shared desktops, and applications, as a monthly subscription service. The solutions enable CSPs to provide customers with risk-free evolution to a complete next-generation workspace, with desktops and applications that are delivered through an easily managed, integrated cloud service. Enterprises can rapidly provision desktops and applications to their users on any device, anywhere, through their CSP. By doing so, they transform desktop virtualization from the CAPEX outlay inherent to enterprise onsite desktops to a predictable, easily budgeted OPEX item.

Technology solution

This solution, which has been tested and validated by EMC Solutions, integrates the VMware virtual desktop environment with EMC storage technologies to provide CSPs with a comprehensive and scalable multitenant DaaS offering. The solution enables CSPs to provide customers a virtual desktop service with outstanding performance, a full range of services, and predictable costs.

The key solution components include:

- VMware Horizon DaaS platform
- VMware vSphere virtualization platform
- EMC XtremIO all-flash storage array for tenant virtual desktops
- EMC VNX or EMC Isilon storage for tenant user data

Key components

Introduction

The following are the key components that were used to build and validate this solution:

- DaaS platform—The VMware Horizon DaaS platform provides the features that are required to deploy, manage, and provide services in a multitenant virtual desktop environment.
- Virtualization and cloud management—The VMware vSphere virtualization platform hosts the tenant virtual desktops and the Horizon DaaS infrastructure.
- EMC storage services:
  - The XtremIO all-flash array provides the high levels of performance that tenant virtual desktops require. At the same time, it offers advanced deduplication and compression capabilities that enable CSPs to host large numbers of desktops in a small amount of rack space.
  - The VNX and Isilon platforms enable CSPs to provide tenants with additional options for storing critical user data. This solution supports either or both platforms for providing this service.
- Network—The networking infrastructure for the solution can be from any vendor if the infrastructure meets the requirements that are outlined in this Reference Architecture Guide.

VMware Horizon DaaS platform

Tenant IT staff can use Horizon DaaS to implement EUC solutions, saving time and money without sacrificing enterprise requirements for security and control.

The Horizon DaaS platform enables tenant IT organizations to do the following:

- Provide user access to Windows desktops from the cloud on any device, including tablets, smartphones, laptops, PCs, thin clients, and zero clients
- Tailor desktops to meet the simplest or most demanding workloads, from call center software to CAD and 3D graphics packages
- Deliver cloud-hosted virtual desktops to end users from a single platform that enables them to get up and running quickly without the complexity of deploying and managing their own desktop virtualization infrastructure
- Manage desktop images, virtual machines, user assignments, and multiple desktop models, including 1:1 persistent virtual desktops, shared desktops, and nonpersistent desktops, from a single console
- Rapidly provision desktops for remote or contract workers and for employees whose physical desktops are unavailable due to a disaster or other interruption

VMware vSphere virtualization and cloud management

This solution uses the VMware vSphere virtualization platform to administer and manage the virtual infrastructure. vSphere provides flexibility and cost savings by enabling the consolidation of large, inefficient server farms into nimble, reliable infrastructures. The core vSphere components are the VMware ESXi hypervisor and VMware vCenter Server.

VMware vSphere ESXi hypervisor

The vSphere ESXi hypervisor is the underlying virtualization layer. Installed on top of a physical server, it partitions the server into multiple virtual machines. The bare-metal architecture of the hypervisor requires no operating system. Virtualization functionality is enabled through vCenter Server.

VMware vCenter Server

vCenter Server is a centralized platform for managing vSphere environments. It provides a single interface for all aspects of monitoring, managing, and maintaining the virtual infrastructure and can be accessed from multiple devices.

vCenter Server is also responsible for managing advanced features such as vSphere High Availability (HA), vSphere Distributed Switch, vSphere Storage DRS, vSphere vMotion and Storage vMotion, and vSphere Update Manager.

VMware vSphere Distributed Switch

vSphere Distributed Switch provides a centralized, streamlined interface from which CSPs can configure, monitor, and administer tenant network resources.

vSphere Distributed Switch offers the following benefits:

- A simplified tenant virtual machine network configuration, which reduces the effort that is required to configure new vSphere hosts to access the required tenant networks
- Enhanced network monitoring and troubleshooting capabilities using IPFIX Netflow version 10, SNMPv3, and RSPAN and ERSPAN protocols for remote network analysis
- Support for advanced vSphere networking features such as templates that can be used to back up and restore the virtual networking configuration, and network health-check capabilities to verify the configuration between vSphere and the physical network

VMware vSphere PowerCLI

vSphere PowerCLI is a command-line and scripting tool that is built on Windows PowerShell. It provides hundreds of commands, which are known as cmdlets, that can be used for managing and automating vSphere functions.

In this solution, vSphere PowerCLI provides the ability to automate several optimization and maintenance operations involving vSphere and the XtremIO array.

VMware vSphere Storage DRS

vSphere Storage DRS continuously balances vSphere datastore utilization and storage I/O load while avoiding resource bottlenecks.

In this solution, vSphere Storage DRS enables the automation of the following tasks:

- Balancing newly provisioned tenant desktops among all available vSphere datastores
- Redistributing tenant desktops among newly provisioned vSphere datastores
- Migrating tenant desktops from existing vSphere datastores to new datastores hosted on an XtremIO array

EMC storage services

This solution uses multiple EMC products to provide storage services, optimize the performance of the storage infrastructure, provide integrated vSphere based storage maintenance, and enable advanced storage performance analytics and monitoring.

EMC XtremIO

The XtremIO all-flash array, which is designed to maximize the use of flash storage media, provides these key benefits:

- Incredibly high levels of I/O performance, particularly for random I/O workloads that are typical in virtualized environments
- Consistently low (submillisecond) latency
- True inline data reduction that removes redundant information in the data path and writes only unique data on the storage array, thus lowering the amount of capacity required
- A full suite of enterprise array capabilities, N-way active controllers, high availability, strong data protection, and thin provisioning

The X-Brick is the fundamental building block of a scaled-out XtremIO clustered system. Using a Starter X-Brick, you can begin with a small virtual desktop deployment (up to 1,250 full-clone desktops), and expand further, when needed, to nearly any scale required. The XtremIO system expands capacity and performance linearly as building blocks are added, greatly simplifying EUC sizing and management of future growth.

For virtual desktop environments, the benefits of XtremIO lead to an unparalleled user experience for all desktop types, at enterprise scale and at all times; a radically simple administrator experience with an easy, efficient, and cost-effective deployment model; and low dollar-per-desktop and total cost of ownership.

XtremIO Operating System

The XtremIO Operating System (XIOS) manages the XtremIO storage cluster without administrator intervention. XIOS provides the following benefits:

- Eliminates the need for the complex configuration that traditional arrays require. With XIOS, you do not have to set RAID levels, determine drive group sizes, set stripe widths, set caching policies, build aggregates, or do any other such configuration.
- Ensures that all solid-state drives (SSDs) in the system are evenly loaded, providing the highest possible performance as well as endurance that stands up to demanding workloads for the entire life of the array.
- Automatically and optimally configures every volume at all times. I/O performance on existing volumes and data sets automatically increases when the cluster is expanded with additional X-Bricks. Every volume can receive the full performance potential of the entire XtremIO system.

Ease of use

The XtremIO array requires only a few basic setup steps that can be completed in minutes, and it does not require tuning or ongoing administration to achieve and maintain high performance levels. The XtremIO system can be taken from shipping box to deployment readiness in less than an hour.

Datacenter economics

Up to 2,500 full-clone desktops are easily supported on an X-Brick (1,250 on a Starter X-Brick) that requires as few as five rack units of space and approximately 750 W of power.

EMC Isilon series

Multitenancy plays a key role in the formation of a shared infrastructure in which tenant business units pool their data for storage. Multitenancy means, among other things, that the storage platform enables CSPs to segregate tenants both from one another and others within the same tenant organization, such as by their tenant business units and data sets.

Based on an architectural model unlike that of traditional storage platforms, Isilon storage solutions enable efficient storage at large scales. An Isilon cluster can scale to over 15 petabytes in size, all in one file-system space. CSPs that are providing file storage for DaaS tenants can optimize their investment by simplifying the underlying storage infrastructure and, in keeping with the dynamic nature of DaaS, make it vastly more scalable.

By combining file and folder hierarchy, volume management, and data protection within a single file system, Isilon systems provide for simplified management while delivering significantly greater storage scalability.

Isilon architecture

An Isilon array comprises storage nodes—which themselves include processor, memory, network, and disk resources—and the overlying software components and modules that enable the full functionality of the Isilon platform.

Storage nodes

Based on the needs of the CSP tenants, an Isilon cluster may comprise multiple different node types to achieve the required performance and capacity levels. Isilon nodes are segmented into one of the following classes, based on their functionality and performance characteristics:

- S-Series—IOPS-intensive applications and workloads
- X-Series—High-concurrency and throughput-driven workloads
- NL-Series—Near-primary accessibility, with near-tape value
- HD-Series—High density, for CSPs who need maximum storage capacity

An Isilon array starts with as few as three nodes and can scale up to 144 nodes. The Isilon system can aggregate all node types into a single cluster in which different node types provide discrete capacity-to-performance ratios. An internal InfiniBand network between all nodes in the cluster supports intranode communication, cache synchronization, data movement, and workload management.

Access zones

Although the default view of an Isilon cluster is that of one physical machine, clusters can be partitioned into multiple virtual containers called access zones. Access zones enable CSPs to isolate data and control which tenant can access data in each zone.

Access zones support all configuration settings for authentication and identity management services on a cluster, so CSPs can configure authentication providers, and provision Server Message Block (SMB) file shares and Network File System (NFS) exports, on a zone-by-zone basis. Creating an access zone automatically creates a local provider, thus enabling the configuration of each access zone with a list of local users and groups. Tenants can also authenticate through a different authentication provider in each access zone.

SmartPools

Isilon SmartPools enable CSPs to use a policy-based approach to manage tenant data and move it automatically across multiple tiers of Isilon scale-out storage based on the specific data storage requirements of their tenants. This functionality enables CSPs to use the appropriate storage resources for the tenants' specific workflow and data management requirements—automatically and transparently.

SmartPools enable CSPs to seamlessly adapt and respond to tenant workflow changes and demands for new capacity without affecting applications or workflows. With Isilon scale-out storage, you can add capacity or performance, or both, on demand in 60 seconds, enabling seamless expansion of any tier.

EMC VNX series

The VNX flash-optimized unified storage platform is ideal for storing tenant user data and Windows profiles in a VMware Horizon DaaS infrastructure. It delivers innovation and enterprise capabilities for file, block, and object storage in a single, scalable, and easy-to-use solution. Ideal for mixed workloads in physical or virtual environments, the VNX platform combines powerful and flexible hardware with advanced efficiency, management, and protection software to meet the demanding needs of virtualized application environments.

The VNX platform helps CSPs achieve their multitenancy goals using several architectural features that include the following:

- Data Movers and Storage Processors with dedicated CPU, memory, and network resources.
- EMC Unisphere® Quality of Service Manager (UQM), which enables you to manage VNX resources based on service levels by using policies to set performance goals. These policies direct the management of array performance aspects, including response time, bandwidth, and throughput, and ensure that the activities of one tenant do not impact the activities of another.
- Unique and secure address spaces that ensure the privacy of tenant data.

Today's VNX platform includes many features and enhancements, including the following, that are built on the success of the first-generation VNX:

- More capacity and better optimization with EMC MCx™ technology components—Multicore Cache, Multicore RAID, and Multicore FAST™ Cache
- Greater efficiency with a flash-optimized hybrid array
- Better protection by increasing availability with active/active storage processors
- Easier administration and deployment with the new Unisphere Management Suite

Flash-optimized hybrid array

VNX provides automated tiering to deliver the best performance to tenants' critical data while intelligently moving less-frequently accessed data to lower-cost disks. This hybrid array can play a key role if a tenant needs occasional levels of flash-like performance for user data.

In this hybrid approach, a small percentage of flash drives in the overall system can provide a high percentage of the overall IOPS. Flash-optimized VNX takes full advantage of the low latency of flash to deliver cost-saving optimization and high-performance scalability. EMC Fully Automated Storage Tiering Suite (FAST Cache and FAST VP) tiers both block and file data across heterogeneous drives and boosts the most active data to the flash drives. This functionality ensures that customers never have to make concessions for cost or performance.

VNX file shares

Many tenant environments require a common location for storing files that are accessed by many users. Common Internet File System (CIFS) or NFS file shares, which are available from a file server, provide this functionality. VNX storage arrays can provide this service along with centralized management, client integration, advanced security options, and efficiency improvement features. For more information about VNX file shares, refer to *EMC VNX Series: Configuring and Managing CIFS on VNX*.

EMC SnapSure

EMC SnapSure™ technology is a VNX File software feature that enables CSPs to create and manage point-in-time logical images of a tenant production file system (PFS). SnapSure uses a copy-on-first-modify principle. A PFS consists of blocks of data. When a block is modified, SnapSure saves a copy containing the original contents of the block—a *checkpoint*—to a separate volume called the SavVol.

Using SnapSure, tenants can be quickly granted access to earlier versions of their user data file systems without the need to restore data using a backup platform.

Subsequent changes that are made to the same block in the PFS are not copied into the SavVol. SnapSure reads the original blocks from the PFS in the SavVol and the unchanged PFS blocks remaining in the PFS, according to a bitmap and blockmap data-tracking structure. These blocks combine to provide the checkpoint, a complete point-in-time image.

A checkpoint reflects the state of a PFS at the time the checkpoint is created. SnapSure supports the following checkpoint types:

- Read-only checkpoints—Read-only file systems that are created from a PFS
- Writeable checkpoints—Read/write file systems that are created from a read-only checkpoint

SnapSure can maintain a maximum of 96 read-only checkpoints and 16 writeable checkpoints per PFS, while allowing PFS applications continued access to realtime data. *Using VNX SnapSure* provides more details.

EMC Storage Analytics

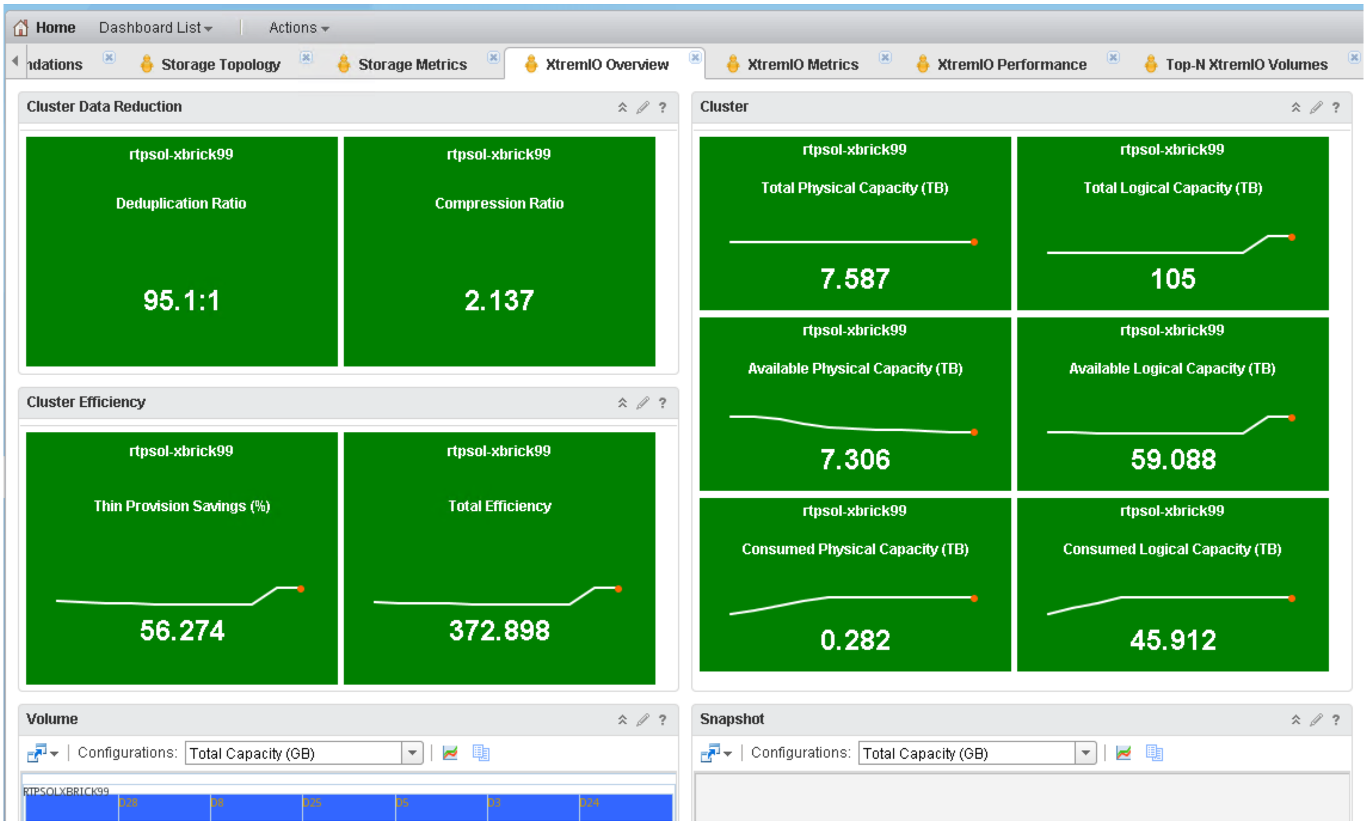
EMC Storage Analytics (ESA) is a management solution designed for VMware and storage administrators to access realtime intelligent analytics for EMC storage platforms. ESA enables administrators to get detailed statistics via customizable dashboards, heat maps, and alerts while accessing topology mapping in a VMware or physical environment.

The challenges that CSPs face are unique—without the in-depth knowledge into workloads that their customers have, proactive monitoring is critical to a properly performing environment. With the built-in analytics in ESA, which are based on machine learning, CSPs can identify anomalous behavior in individual applications, virtual machines, storage components, and so on, without needing to understand the application that the customer is using. ESA generates warnings and alerts before anomalous behaviors become a problem for the many customers housed in a single environment. This helps CSPs to better meet critical and revenue-impacting SLAs.

Furthermore, by using these learning analytics, and the dashboards built by EMC engineers, CSP administrators are immediately guided to the most important places to look for anomalous events and for the possible root causes that ESA identifies, without having to spend hours collecting logs and wait for support calls.

The combination of machine learning, deep and granular storage visibility across the EMC product line, and dashboards built by engineers with decades of experience in performance troubleshooting means that CSPs can use ESA to stay in SLA, predict issues, and meet customer expectations.

Figure 1 shows an example of an overview dashboard, which is one of several default dashboards included with the ESA platform. CSPs can use the default dashboards, as well as others that can be customized to individual specifications, to obtain detailed information about current and historical data concerning the status and performance of multiple EMC storage services.



Cluster Data Reduction

rtpsol-xbrick99 Deduplication Ratio 95.1:1

rtpsol-xbrick99 Compression Ratio 2.137

Cluster Efficiency

rtpsol-xbrick99 Thin Provision Savings (%) 56.274

rtpsol-xbrick99 Total Efficiency 372.898

Cluster

rtpsol-xbrick99 Total Physical Capacity (TB) 7.587

rtpsol-xbrick99 Total Logical Capacity (TB) 105

rtpsol-xbrick99 Available Physical Capacity (TB) 7.306

rtpsol-xbrick99 Available Logical Capacity (TB) 59.088

rtpsol-xbrick99 Consumed Physical Capacity (TB) 0.282

rtpsol-xbrick99 Consumed Logical Capacity (TB) 45.912

Volume

Configurations: Total Capacity (GB)

Snapshot

Configurations: Total Capacity (GB)

Figure 1. EMC Storage Analytics—Overview dashboard

EMC Virtual Storage Integrator for VMware vSphere

EMC Virtual Storage Integrator (VSI) for VMware vSphere is a plug-in for VMware vCenter that simplifies management of EMC storage within the vSphere environment.

With VSI, storage tasks can be efficiently managed and delegated through the familiar vCenter interface, and daily management tasks can be performed with up to 90 percent fewer clicks and up to 10 times higher productivity. Furthermore, individual VSI features can be added and removed to provide a customized user environment.

CSPs can use VSI to seamlessly provision new XtremIO or VNX Virtual Machine File System (VMFS) datastores within the vSphere Client. We used the VSI for vSphere plug-in when validating this solution. We also used it to reclaim physical capacity on the XtremIO array that was no longer being used.

The *EMC VSI for VMware vSphere Web Client Product Guide*, which is available on EMC Online Support, provides more information about VSI.

EMC PowerPath/VE

EMC PowerPath®/VE host-based software enables automated data path management, failover and recovery, and optimized load balancing. PowerPath/VE automates, standardizes, and optimizes data paths in virtual desktop infrastructure (VDI) environments and cloud deployments to deliver high availability and performance.

Solution architecture

Horizon DaaS technology overview

A VMware Horizon DaaS deployment includes multiple redundant virtual appliances. CSPs and tenants use their own dedicated appliances. Each appliance serves specific functions as outlined in this section.

Horizon DaaS appliances

Horizon DaaS management appliances are virtual machines that are used to control and run the Horizon DaaS platform. Table 1 lists the Horizon DaaS appliances and their functions.

Note: The Horizon DaaS infrastructure is deployed using two different Open Virtualization Appliance (OVA) files. The Service Provider, Resource Manager, Tenant, and Desktop Manager appliances are all deployed using the same OVA file, while the Desktop Remote Access Manager (dtRAM) appliance is deployed using an OVA file that is designed for that appliance.

Table 1. Horizon DaaS appliances and functions

Appliance	Function
Service Provider	Hosts the Service Center web-based UI, which provides access to the Horizon DaaS infrastructure. It also acts as a transit point for enabling Secure Shell (SSH) access to all the management appliances in the datacenter. The Service Provider appliance is the first appliance that is installed in the CSP datacenter. It provides the foundation to install the remainder of the Horizon DaaS platform.
Resource Manager	Integrates with the physical and virtual infrastructure in a CSP datacenter. A single Resource Manager appliance can be shared across multiple tenants. The Resource Manager abstracts all specifics of the infrastructure from the Tenant appliances, allowing tenants to focus on deploying on the desktops rather than managing the infrastructure itself.
Tenant	Provides the tenant with both end user and administrative access to their Horizon DaaS virtual desktops. End users can access and manage their individual virtual desktops via the Horizon DaaS tenant desktop portal. Administrators can create and manage their virtual desktops via the Tenant Enterprise Center.
Desktop Manager	Functions as a tenant appliance that does not include the components that are used to provide end-user brokering and administrative user access. Desktop Manager appliances serve two key purposes: • Desktop capacity scale-out—The Horizon DaaS Tenant appliance provides capacity for up to 5,000 virtual desktops per datacenter. When an individual tenant must scale beyond 5,000 desktops, Horizon DaaS Desktop Manager appliances can be added to provide the required capacity. Each additional Desktop Manager appliance pair can support up to 5,000 desktops. • Compute resource optimization—A Desktop Manager is designed to treat the individually assigned compute resources equally. If a specialized desktop workload is required, the workload can be optimized by creating a Desktop Manager pair to which only the compute resources for that workload are assigned. Some examples of specialized workloads include delivering standard VDI, VDI with GPU, and Microsoft RDS. The compute resources for the workloads in such cases would be separate and distinct from each other.

Appliance	Function
Desktop Remote Access Manager	Enables tenant end users outside their internal network to access their Horizon DaaS virtual desktops without VPN software. The dtRAM runs on two virtual servers to provide high availability, including automatic failover in the event of an appliance failure or other outage. Once a tenant virtual desktop session is established, all traffic between the client and the virtual desktop passes through the dtRAM server.

Horizon DaaS architecture

All Horizon DaaS management appliances are connected to the Horizon DaaS backbone link-local network as well as the CSP or tenant network, as shown in Figure 2. Horizon DaaS requires that all management appliances be installed as HA pairs. To ensure high availability of physical hardware, all Horizon DaaS management appliance pairs are automatically distributed across separate physical Horizon DaaS management vSphere hosts.

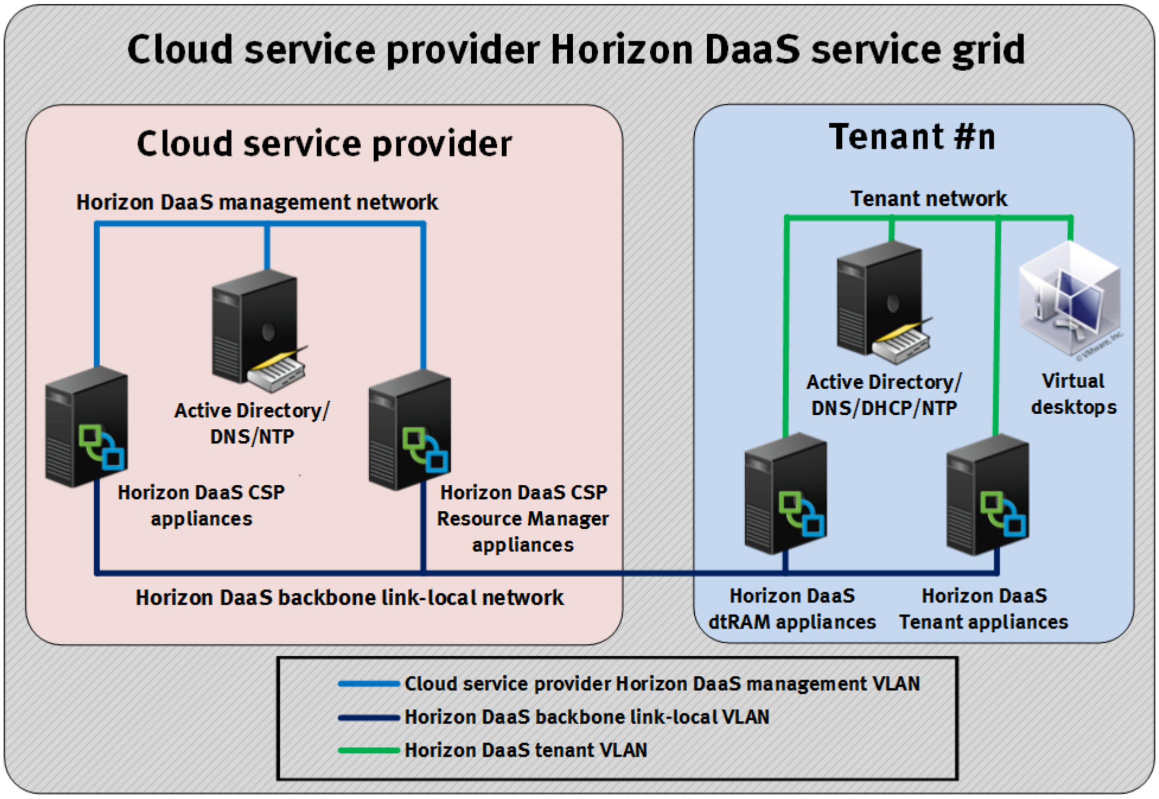

Cloud service provider Horizon DaaS service grid
Cloud service provider
Horizon DaaS management network
Active Directory/ DNS/NTP
Horizon DaaS CSP appliances
Horizon DaaS CSP Resource Manager appliances
Horizon DaaS backbone link-local network
Tenant #n
Tenant network
Active Directory/ DNS/DHCP/NTP
Virtual desktops
Horizon DaaS dtRAM appliances
Horizon DaaS Tenant appliances
Cloud service provider Horizon DaaS management VLAN
Horizon DaaS backbone link-local VLAN
Horizon DaaS tenant VLAN

Figure 2. VMware Horizon DaaS: CSP and tenant architecture

The Horizon DaaS management appliances allow monitoring via the standard Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) interface. For information about the types of CIM classes, recommended thresholds, and monitoring in general, see the Horizon DaaS documentation on the VMware website. Also see the Horizon DaaS documentation for more information about the underpinnings of the Horizon DaaS platform, including advanced details concerning the function and interoperability of platform components.

Solution architecture overview

This EMC DaaS solution supports block storage for tenant virtual desktops and associated Horizon DaaS and other infrastructure services. In addition to the Horizon DaaS components described in the preceding section, the solution includes the following components:

- Link between the tenant corporate site and the CSP site—This link provides direct connectivity between the tenant private network and the tenant network in the CSP datacenter. This connection enables Microsoft Active Directory communication between sites and provides clients direct access to their Horizon DaaS desktops without needing to use a Horizon DaaS Remote Access Manager server.
- Tenant Microsoft Active Directory Services—Each Horizon DaaS tenant requires access to its own Active Directory, DNS, DHCP, and NTP services. Tenant desktops in the Horizon DaaS infrastructure can use remote, tenant-hosted Active Directory domain services as well as DHCP, DNS, and NTP servers. However, EMC recommends that tenants deploy replicas of these services within the dedicated tenant Horizon DaaS infrastructure. This deployment ensures that the tenant retains desktop access if the remote services are unavailable or the link between the CSP site and the tenant corporate network is interrupted.
- VMware vSphere clusters—Individual vSphere clusters for each tenant facilitate the assignment of dedicated vSphere resources. Each tenant requires at least one vSphere cluster, and, if the tenant or CSP requires it, each tenant can be configured with multiple clusters. The Horizon DaaS CSP components are on a separate vSphere cluster, ensuring that the resources required for those components do not impact and are not impacted by tenant resource utilization.
- EMC XtremIO—The XtremIO array provides storage for Horizon DaaS tenant virtual desktops and, optionally, the Horizon DaaS CSP components.
- EMC Isilon and VNX—An Isilon or VNX array provides storage for tenant user data. In some cases, a CSP might already have an existing platform for this purpose. In those cases, CSPs should analyze the performance and capacity of the platform to ensure that it meets the needs of the tenants before granting tenants access to it. If tenants require more capacity or higher performance, CSPs can supplement or replace the existing platform with either an Isilon or VNX array.

Figure 3 shows the logical architecture of a solution implementation, including a sample tenant. Figure 3 also shows the XtremIO array being used to host the CSP Horizon DaaS components, although it is not a requirement. Any available vSphere datastore that is supported by a highly available storage platform with sufficient free space, as outlined in this section, is acceptable.

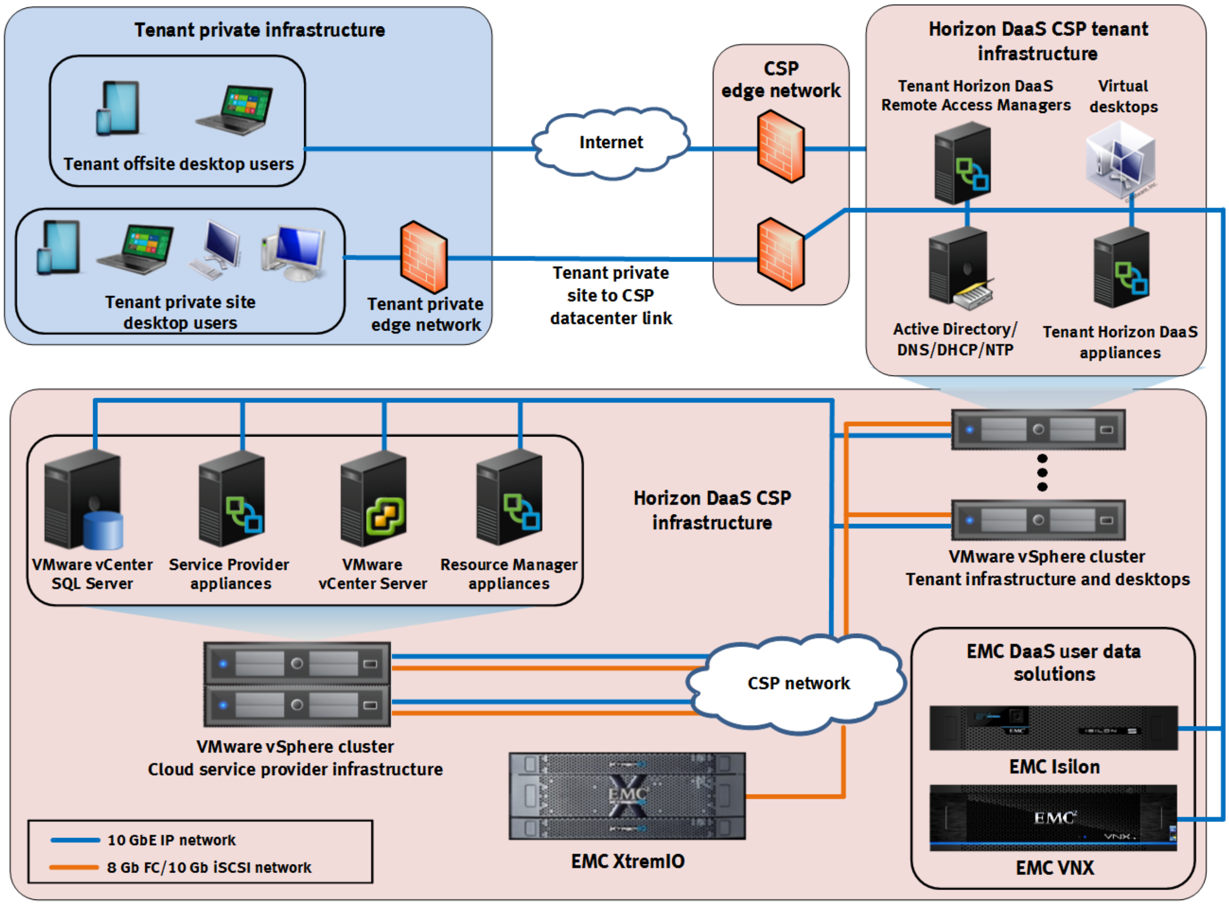

Tenant private infrastructure
Tenant offsite desktop users
Tenant private site desktop users
Tenant private edge network
Internet
Tenant private site to CSP datacenter link
CSP edge network
Horizon DaaS CSP tenant infrastructure
Tenant Horizon DaaS Remote Access Managers
Virtual desktops
Active Directory/ DNS/DHCP/NTP
Tenant Horizon DaaS appliances
VMware vCenter SQL Server
Service Provider appliances
VMware vCenter Server
Resource Manager appliances
Horizon DaaS CSP infrastructure
VMware vSphere cluster Tenant infrastructure and desktops
CSP network
VMware vSphere cluster Cloud service provider infrastructure
EMC DaaS user data solutions
EMC Isilon
EMC VNX
EMC XtremIO
10 GbE IP network
8 Gb FC/10 Gb iSCSI network

Figure 3. Logical architecture for solution with Horizon DaaS implementation

The portion of the infrastructure labeled “Horizon DaaS CSP tenant infrastructure” is unique to each tenant and must be duplicated as more tenants are added. The Horizon DaaS Remote Access Managers are required only if the tenant desktops will be accessed over a public Internet connection.

The portion of the infrastructure shaded light blue represents the existing private infrastructure of the tenant. The portions shaded light red represent individual portions of the CSP infrastructure, including those portions that host the tenant Horizon DaaS desktops and associated infrastructure services.

Assuming that the tenant allows it, the tenant Horizon DaaS desktops that are hosted by the CSP are free to access applications or other resources on the private infrastructure of the tenant. Allowing this access is not explicitly required from a solution standpoint, but might be so from a tenant perspective.

Horizon DaaS infrastructure requirements

Table 2 lists the virtual machine resources that are required for each of the Horizon DaaS appliances.

Table 2. Horizon DaaS appliance virtual machine resource requirements

Appliance	Number of appliances	Number of vCPUs	RAM	Disk space (GB)
Service Provider appliance	2	1	3 GB	20
Resource Manager appliance	2	1	3 GB	20
Tenant appliance	2	1	3 GB	20
Desktop Remote Access Manager appliance	2	1	512 MB	3

A Horizon DaaS environment begins with two Horizon DaaS management hosts, each with one Service Provider appliance, one Resource Manager appliance, and one Tenant appliance. From there, CSPs can add tenants to the datacenter by adding another Tenant appliance to each management host. The size of the management host is generally referred to by the number of tenants it can support.

As tenants are added in the Horizon DaaS CSP Service Center, additional Horizon DaaS Tenant appliances are created automatically. The figures in Table 2 are for each tenant, so multiply those values by the number of tenants to determine the total resources required.

vCenter Server infrastructure requirements

The vCenter Server that is used with Horizon DaaS has varying requirements that are based on the number of vSphere hosts and virtual machines to be managed. Table 3 provides the minimum requirements of both the vCenter Server host server and a server running Microsoft SQL Server 2012 to provide the necessary database services. These specifications apply to Horizon DaaS infrastructures that support up to 3,500 desktops.

Table 3. vCenter Server virtual machine resource requirements

Server	CPU	RAM	IOPS	Storage capacity
SQL Server	2 vCPUs	6 GB	100	200 GB
vCenter Server	4 vCPUs	8 GB	100	80 GB

For environments that will support more than 3,500 desktops or use a database platform other than Microsoft SQL Server, refer to *vSphere Installation and Setup* from VMware for sizing guidance.

XtremIO requirements

We designed the solution to support either of the following specialized XtremIO configurations, testing the configurations individually to validate their respective desktop scale points:

- Starter X-Brick—A Starter X-Brick contains 13 SSDs and supports up to 1,250 full-clone virtual desktops. If support for additional desktops is later required, a Starter X-Brick can be upgraded to an X-Brick via the addition of the SSDs required.
- X-Brick—A single X-Brick contains 25 SSDs—the maximum number that is supported—and supports up to 2,500 full-clone virtual desktops. Providing more virtual desktop capacity requires additional X-Bricks.

These values are considered the maximum number of desktops that are supported on a Starter X-Brick or X-Brick that contains 400 GB SSDs. The sizing information in this section is strictly for Horizon DaaS virtual desktop storage. Tenant user data storage requirements should be calculated separately using the EMC sizing tools for Isilon and VNX, as described in Isilon and VNX requirements on page 23.

XtremIO: Sizing for virtual desktop capacity

The number of desktops either X-Brick configuration supports varies depending on the tenant desktop configuration and the number of unique tenants the X-Brick is providing storage for. The number of supported desktops varies because the introduction of new tenant desktop configurations has an impact on the effectiveness of the deduplication and compression capabilities of the XtremIO array. Examples of scenarios that can have an impact on the effectiveness of those features include the following:

- One or more tenants that use multiple, unique gold images for their desktops. Gold images are also known master images, which are configured by the tenants and used to deploy their Horizon DaaS virtual desktops.
- Tenants whose desktop usage profile generates large amounts of data that is generally more difficult to deduplicate or compress, such as large image files. This type of scenario emphasizes the importance of storing tenant user data on Isilon or VNX arrays.

Because of these and similar scenarios, when sizing an XtremIO array, CSPs should select a deduplication ratio that best matches the expected tenant virtual desktop configuration. Doing so ensures that as tenant desktops are added, and later on when they have been in production for an extended period, the XtremIO array will have sufficient physical capacity.

Table 4 provides XtremIO data reduction ratios for a range of multitenant environments. CSPs can use these ratios to calculate the number of desktops a single XtremIO X-Brick will support.

Table 4. XtremIO data reduction ratios in multitenant virtual desktop environments

Number of tenants	Data reduction ratio: One unique image per tenant	Data reduction ratio: Two unique images per tenant
1	12	11
2	10	9
3	9	8
4	8	7
5	7	6
6	6	5

CSPs can use the data reduction ratios in Table 4 with the XtremIO sizing tool at mainstayadvisor.com/go/emc to determine the required X-Brick configuration for the proposed Horizon DaaS environment. CSPs without access to this tool should consult their EMC representative for appropriate sizing guidance.

The following example demonstrates how the sizing tool uses a data reduction ratio to determine the XtremIO physical capacity required:

- A 400 GB single X-Brick cluster contains 7.58 TB of physical capacity, which is usable capacity after all deduplication and compression operations have taken place.
- Tenant A has a 32 GB gold image and will deploy 1,000 desktops.
- Tenant B has a 24 GB gold image that is wholly unique from the image being used by Tenant A. Tenant B will deploy 1,250 desktops.
- Based on the information in Table 4, we assume that the data reduction ratio will be 10:1 over the life of the tenant desktops.
- The XtremIO physical capacity requirements can be determined using the following calculation:

  ```
  [(Tenant A image size/expected data reduction ratio) * number
  of desktops] + [(Tenant B image size/expected data reduction
  ratio) * number of desktops] = Total amount of XtremIO
  physical capacity required
  ```

  Using the numbers in this example results in the following calculation:

  ```
  [(32 / 10) * 1000] + [(24 / 10) * 1250] = 6200 GB, or 6.05 TB
  ```

  Based on this calculation, the proposed tenant desktop configuration requires 6.05 TB of the 7.58 TB capacity of a single X-Brick cluster over time, leaving approximately 20 percent of the array physical capacity free.

XtremIO: Sizing for virtual desktop performance

A single XtremIO X-Brick is rated to deliver 150,000 IOPS at a 50 percent read/50 percent write ratio. Based on the maximum number of full-clone virtual desktops supported (2,500), the X-Brick provides for up to 60 sustained IOPS per desktop. A Starter X-Brick provides similar per-desktop IOPS capabilities for up to 1,250 full-clone virtual desktops.

The XtremIO sizing tool accepts the number of per-desktop IOPS required as one of its inputs and can assist in determining the number of X-Bricks required based on the expected IOPS load.

Isilon and VNX requirements

We designed the solution to support both Isilon and VNX arrays to provide tenant user data storage. Because tenant user data performance and capacity requirements vary, CSPs should refer to the EMC sizing tool at mainstayadvisor.com/go/emc to determine the configuration that is required for the proposed Horizon DaaS environment. CSPs who do not have access to this tool should consult their EMC representative for appropriate sizing guidance.

Software resources

Table 5 lists the software that was used to validate the solution.

Table 5. Solution software

Software	Configuration
XtremIO (FC-connected shared storage for vSphere datastores)	
XtremIO XIOS Operating System	Release 3.0.1 build 11
Network infrastructure	
Cisco Nexus 5020	Version 4.2(1)N1(1)
Virtualization infrastructure	
VMware vSphere	5.5 Update 2
VMware vCenter Server and Microsoft SQL Server	
Host OS	Windows 2012 R2
Database server	
Microsoft SQL Server	2012
Desktop broker	
VMware Horizon DaaS	6.1
Desktop agents	
VMware Horizon DaaS agent	6.1.0-22158
VMware Horizon View agent	6.0.1-2089044
VMware Horizon View Direct Connection agent	6.0.1-2088845

Software	Configuration
Virtual desktops	
OS	• Microsoft Windows 7 Enterprise SP1 (32-bit) • Microsoft Windows Server 2012 R2 (64-bit; VDI configuration)
VMware Tools	9.4.10 build-2092844

Network requirements

Table 6 describes the network requirements for this solution.

Table 6. Network requirements

Network	Service	Minimum link speed
Private network for Horizon DaaS backbone communications	Automated deployment, management, and monitoring of all tenant Horizon DaaS appliances **Note**: This network should be used only by Horizon DaaS appliances and only for these purposes. It should not be used for any other services or be accessible by any other network hosts.	10 GbE
Dedicated network for each tenant	Tenant infrastructure services including virtual desktops and Horizon DaaS appliances	10 GbE
CSP infrastructure network	Management of Horizon DaaS environment and EMC storage services	10 GbE
Storage network	Storage management	8 Gb FC, 10 Gb CEE with FCoE, or 10 GbE with iSCSI

Hardware resources

Table 7 lists the storage, server, and network hardware that was used to validate the performance of this solution.

Table 7. Hardware used to validate solution performance

Hardware	Quantity	Configuration	Notes
EMC XtremIO Starter X-Brick	1	• A single managed system of 1 Starter X-Brick • 13 x 400 GB eMLC SSD drives per Starter X-Brick	Shared storage for tenant virtual desktops and Horizon DaaS infrastructure servers
EMC XtremIO X-Brick	1	• A single managed system of 1 X-Brick • 25 x 400 GB eMLC SSD drives per X-Brick	Shared storage for tenant virtual desktops and Horizon DaaS infrastructure servers

Hardware	Quantity	Configuration	Notes
Intel based servers	27	• Memory: 256 GB of RAM • CPU: 2 x Intel Xeon E7-2870 with 2.40 GHz deca-core processor • Internal storage: 1 x 146 GB internal SAS disk • External storage: XtremIO (FC) • NIC: Dual-port 10 GbE adapter • FC HBA: Dual-port 8 Gbps adapter	• 25 servers—Horizon DaaS tenant desktop clusters • 2 servers—vSphere cluster for hosting infrastructure virtual machines
Cisco Nexus 5020	4	• 40 x 10 Gb ports • 2 Ethernet ports per server • 2 FC ports per server	Redundant FC and LAN A/B configuration

During our testing, we used different ratios for the number of desktops per vSphere host CPU core, according to which virtual desktop OS was used:

- Windows 7 32-bit—Eight desktops per server core
- Windows Server 2012 R2 VDI configuration—Five desktops per server core

In practice, the ratio of tenant desktops per vSphere host server core varies based on the number of vCPUs each desktop requires and by the vCPU load of those desktops. For example, if a tenant requires two vCPUs in its virtual desktops, then the number of desktops per server core is likely to be reduced by half.

Regardless of the ratio used, CSPs should monitor the CPU utilization of the vSphere hosts in those clusters to ensure that allocated resources are sufficient.

Conclusion

This solution provides a blueprint of a validated VMware Horizon DaaS solution that is enabled by an EMC XtremIO all-flash array, EMC Isilon, EMC VNX, and the VMware vSphere virtualization platform. This solution provides CSPs with a comprehensive DaaS offering that delivers outstanding performance, reliability, and ease of administration, and one that can scale to and support thousands of virtual desktops.

The Horizon DaaS platform provides the features that are required to deploy, manage, and provide services in a multitenant virtual desktop environment. With the Horizon DaaS infrastructure, tenants have a single platform for delivering and managing virtual Windows desktops, which users can access from any device.

The vSphere virtualization platform hosts the Horizon DaaS infrastructure and the tenant virtual desktops. It partitions a server into multiple virtual machines and provides a single interface for managing the virtual infrastructure.

The XtremIO all-flash array enables Horizon DaaS environments to achieve high levels of performance, scale as needed, be easier to administer, and require fewer overall infrastructure resources.

The performance capabilities of the XtremIO array enable virtual desktop application response times that mirror the SSD experience of the most modern physical desktops. XtremIO enables this response time even if the virtual desktop is not optimized to minimize the I/O footprint, as is required with some storage solutions.

The deduplication and compression capabilities of the XtremIO array dramatically reduce the storage that is required for full-clone Horizon DaaS virtual desktops. As few as five rack units of space can provide storage for up to 2,500 full-clone desktops, which allows for an attractive storage cost per desktop even with the benefit of 100 percent flash storage.

The Isilon and VNX arrays provide CSPs with a platform that is optimized for tenant user data storage, preserving XtremIO capacity for use with the virtual desktops where it is needed the most.

References

EMC documentation

The following documents, which are located on EMC Online Support or EMC.com, provide additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your EMC representative.

- *Deploying Microsoft Windows 7 Virtual Desktops with VMware View—Applied Best Practices*
- *Deploying Microsoft Windows 8 Virtual Desktops—Applied Best Practices*
- *EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Solution Guide*
- *EMC PowerPath/VE Installation and Administration Guide*
- *EMC PowerPath Viewer Installation and Administration Guide*
- *EMC Storage Analytics Installation and User Guide*
- *EMC Storage Analytics Release Notes*
- *EMC VNX Series Version 8.1: Configuring and Managing CIFS on VNX*
- *EMC VNX Series Release 8.1: Using Quotas on VNX*
- *EMC VNX Series Release 8.1: Using VNX SnapSure*
- *EMC VNX Unified Best Practices for Performance—Applied Best Practices Guide*
- *EMC VSI for VMware vSphere Web Client Product Guide*
- *EMC XtremIO Storage Array Operations Guide*
- *EMC XtremIO Storage Array Security Configuration Guide*
- *EMC XtremIO Storage Array User Guide*
- *Flash Implications in Enterprise Storage Array Designs*
- *Isilon OneFS Web Administration Guide*

VMware documentation

Refer to the following VMware documentation:

- *Installing and Administering VMware vSphere Update Manager*
- *Installing or Migrating vRealize Operations Manager*
- *Understanding Memory Resource Management in VMware vSphere 5.0 Technical White Paper*
- *vCenter Server and Host Management*
- *VMware Horizon DaaS Platform 6.1 Blueprint*
- *VMware Horizon DaaS 6.1 Downloading SSL Certificate for Gold Pattern*
- *VMware Horizon DaaS Platform 6.1 Enterprise Center Handbook*
- *VMware Horizon DaaS Platform 6.1 Release Notes*

- *VMware Horizon DaaS Platform 6.1 Service Provider Installation – vCenter*
- *VMware Horizon DaaS Platform 6.1 Tenant Installation – vCenter*
- *VMware vSphere Resource Management*
- *vRealize Operations Manager vApp Deployment and Configuration Guide*
- *vSphere Installation and Setup*
- *vSphere Networking*
- *vSphere Storage*
- *vSphere Virtual Machine Administration*

Other documentation

The following documents, available on the Microsoft TechNet, provide additional and relevant information:

- *Install and Deploy Windows Server 2012 R2 and Windows Server 2012*
- *Installation for SQL Server 2012*