Solution Guide

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

EMC Solutions

Abstract

This Solution Guide describes the architecture, features, and implementation of the EMC® Desktop-as-a-Service solution based on VMware Horizon DaaS and EMC XtremIO™, EMC Isilon®, and EMC VNX® storage.

March 2015

Published 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.

EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Solution Guide

Part Number H13804

Contents

Figures

Tables

Chapter 1 Executive Summary

This chapter presents the following topics:

Document purpose

This Solution Guide describes the EMC® desktop-as-a-service (DaaS) solution for the VMware Horizon DaaS platform. The solution uses an EMC XtremIO™ all-flash array to provide storage for virtual desktops, and either an EMC Isilon® or an EMC VNX® array to provide storage for tenant user data. This guide introduces the solution architecture and key components, and provides guidelines, instructions, and best practices for deploying, configuring, and managing the solution.

The EMC DaaS solution enables cloud service providers (CSPs) to deliver managed, cloud desktop offerings to their customer base. Organizations both large and small can also use the solution to provide DaaS offerings to their internal customers.

This guide is a companion to the *EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Reference Architecture Guide*, which provides a general overview of the solution, inventories of the hardware and software used to validate the solution, and general sizing guidelines.

Audience

This guide is intended for architects, cloud administrators, and technical administrators of IT environments who wish to implement this EMC DaaS solution to deliver cloud-hosted desktops to external and internal customers. Readers should be familiar with VMware vSphere virtualization, the VMware Horizon DaaS platform, and general IT functions and requirements in a DaaS architecture.

Business case

Enterprise IT organizations seeking to decrease capital expenditures and shed administrative costs and responsibilities are increasingly turning to cloud service providers (CSPs) for managed DaaS offerings. These enterprises not only need to 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 they can deploy quickly and effectively, and at reduced cost. 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 agreed 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 a 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 with lower cost per user and lower total cost of ownership.

Solution overview

This solution provides CSPs with a scalable, cost-effective platform for delivering DaaS based on a combination of the VMware Horizon DaaS platform and EMC XtremIO all-flash storage. 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 guided DaaS deployment, with deployment and configuration instructions, sizing guidelines, and best practices. In addition, CSPs can integrate the solution with their existing customer-facing portal, if they choose to do so.

This solution, which was tested and validated by EMC Solutions, integrates the VMware virtual desktop environment with EMC storage technologies to provide CSPs with a scalable, multitenant DaaS platform. It 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 Isilon or EMC VNX storage or both (for tenant user data)

Key benefits

The key benefits of this EMC DaaS solution include:

- A fully managed DaaS offering for CSPs and enterprise customers, with sizing tools for costing and pricing different DaaS configurations
- A validated reference architecture, with best practices and guidance for setting up and managing multitenant services
- Scale-out storage for virtual desktops that eliminates complex planning and deployment—start small and grow incrementally to nearly any scale without service disruption
- Multitenant storage for user data
- Uncompromising, fully customizable desktop experience—every user can have their own dedicated virtual desktop, customized to their specific applications, and with the same look and feel as their physical desktops or laptops
- High-performance virtual desktops that can be tailored for the simplest to the most demanding workloads, including call center software, and CAD and 3D graphics packages

- Outstanding user experience with unparalleled I/O performance and consistently low response times, at scale, all the time, and for all user types—applications respond instantly and consistently, faster than on physical desktops, and without being affected by boot storms, antivirus scans, suspend and resume operations, or application peak demands
- Powerful but simple to use from the ground up, delivering a radically simple administrative experience—an intuitive, easy-to-use interface and zero tuning requirements enable smooth roll-outs and live upgrades, patches, and desktop rollback
- Advanced data reduction techniques—unique inline data deduplication, compression, and copy services reduce desktop storage capacity needs and the data center footprint to deliver lower CAPEX and OPEX for CSPs or organizations

The EMC DaaS solution with EMC XtremIO offers exceptional performance, capacity savings, and ease of use, leading to low $/desktop and breakthrough total cost of ownership in DaaS environments.

The EMC DaaS solution with VMware Horizon DaaS provides all the features required to deploy and manage desktops in a multitenant, virtual desktop environment.

Chapter 2 Solution Overview

This chapter presents the following topics:

Solution architecture

This EMC DaaS solution integrates the best of products and services from EMC and VMware to provide CSPs with a highly scalable multitenant DaaS offering.

Overview

VMware Horizon DaaS provides the features required to deploy, manage, and provide services in a multitenant virtual desktop environment. The VMware vSphere virtualization platform hosts the tenant virtual desktops and the Horizon DaaS infrastructure. Horizon DaaS uses individual vSphere clusters for each tenant to 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. A separate vSphere cluster is used for the Horizon DaaS CSP components, ensuring that the resources required for those components do not impact and are not impacted by tenant resource utilization.

The EMC XtremIO all-flash array provides block storage for the tenant virtual desktops, associated Horizon DaaS infrastructure, and other infrastructure services. This 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 EMC Isilon and EMC VNX 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. In some cases, a CSP might already have an existing platform for storing user data. 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 performance, CSPs can supplement or replace the existing platform with either an Isilon or VNX array.

Figure 1 on page 15 shows the logical architecture of a solution implementation, including a sample tenant. In this implementation, the XtremIO array is used to host the Horizon DaaS CSP components, although this is optional. Any available vSphere datastore is acceptable for this purpose, if it is supported by a highly available storage platform with sufficient free space to meet the Horizon DaaS infrastructure requirements.

Note: For all EMC DaaS solution sizing operations for XtremIO, Isilon, and VNX arrays, refer to the EMC sizing tool at mainstayadvisor.com/go/emc. If you do not have access to this tool, consult your EMC representative for appropriate sizing guidance. Refer to the *EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Reference Architecture Guide* for an overview of sizing recommendations.

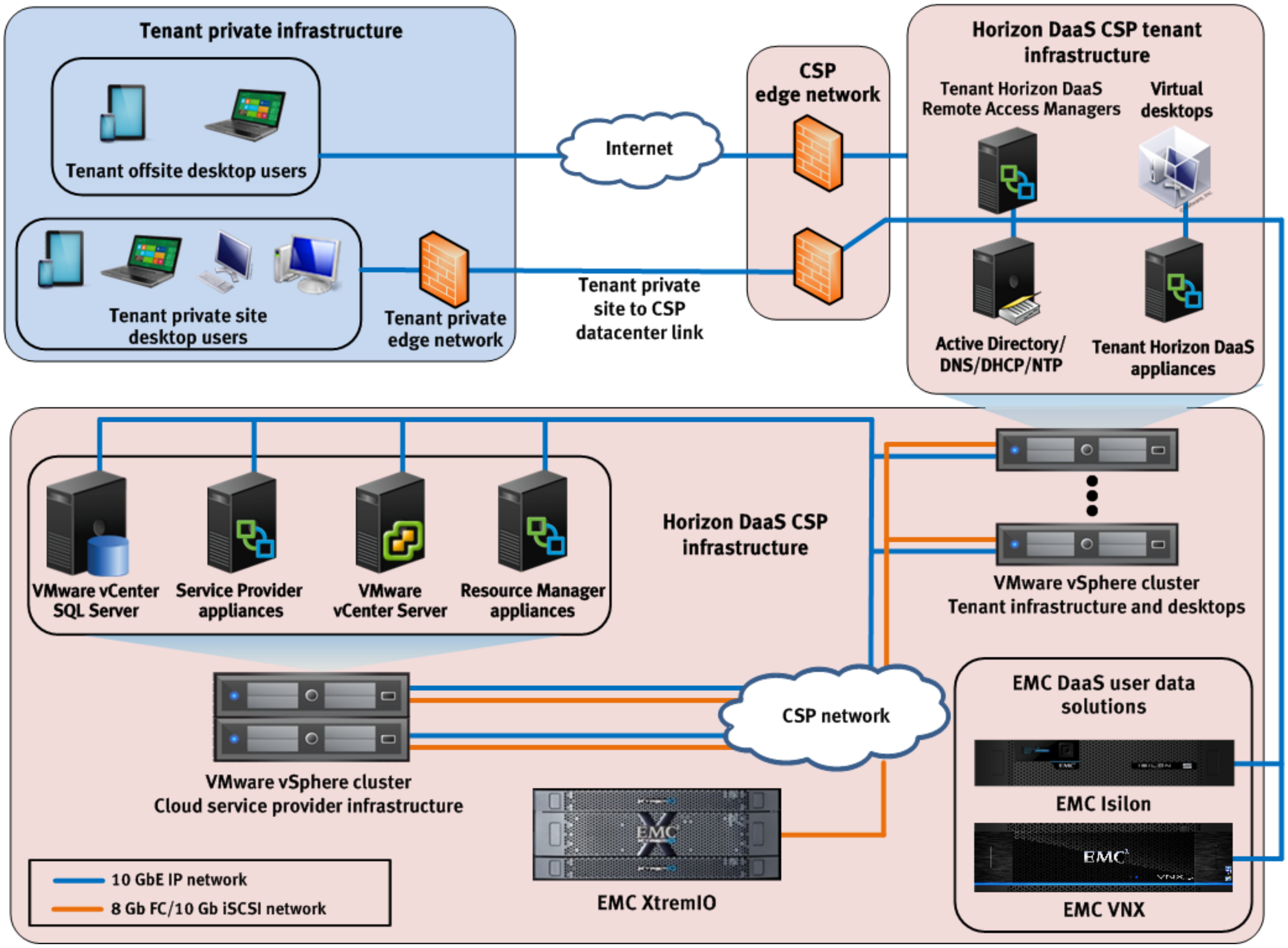

Tenant private infrastructure
Tenant offsite desktop users
Tenant private site desktop users
Tenant private edge network
Internet
Tenant private site to CSP datacenter link
CSP edge network
Horizon DaaS CSP tenant infrastructure
Tenant Horizon DaaS Remote Access Managers
Virtual desktops
Active Directory/ 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
VMware vSphere cluster Cloud service provider infrastructure
CSP network
EMC DaaS user data solutions
EMC Isilon
EMC VNX
EMC XtremIO
10 GbE IP network
8 Gb FC/10 Gb iSCSI network

Figure 1. EMC DaaS solution: Logical architecture

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

Horizon DaaS tenant infrastructure

The Horizon DaaS CSP tenant infrastructure is unique to each tenant and must be duplicated for each new tenant added. The Horizon DaaS Remote Access Managers are required if the tenant desktops will be accessed over a public Internet connection.

The link between the tenant corporate site and the CSP site provides direct connectivity between the tenant private network and the tenant network in the CSP data center. This connection enables Microsoft Active Directory communication between sites and provides clients with direct access to their Horizon DaaS desktops without needing to use a Horizon DaaS Remote Access Manager server. Assuming that the tenant allows it, the tenant's CSP-hosted Horizon DaaS desktops are free to access applications or other resources on the tenant's corporate infrastructure. Allowing this access is not explicitly required from a solution standpoint, but might be so from a tenant's perspective.

Each Horizon DaaS tenant requires access to its own Active Directory domain services, and DNS, DHCP, and NTP servers. Tenant desktops in the Horizon DaaS infrastructure can use remote, tenant-hosted Active Directory domain services and 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 in the event that the remote services are unavailable or the link between the CSP site and the tenant corporate network is interrupted.

Networking

This solution uses the following networks:

Note: Unless otherwise specified, all networks require a dedicated or shared 10 GbE IP network.

- A private network for Horizon DaaS backbone communications; this enables automated deployment, management, and monitoring of all tenant Horizon DaaS appliances. This network should be dedicated for use by Horizon DaaS appliances and should not be accessible by other network hosts.
- A dedicated network for each tenant’s virtual desktops, Horizon DaaS appliances, and other required infrastructure services.
- A service provider infrastructure network for managing the Horizon DaaS environment and EMC storage services.
- A storage network that uses 8 Gb FC, 10 Gb CEE with FCoE, or 10 GbE with iSCSI.

A tenant might also require backhaul connectivity to their private corporate network. The network components for this option will vary based on tenant requirements and on the configuration of the service provider and tenant infrastructures.

VMware Horizon DaaS architecture and components

A VMware Horizon DaaS deployment includes multiple redundant virtual appliances. The CSP 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 dtRAM appliance is deployed using an OVA file that is specifically 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. This is the first appliance that is installed in the CSP datacenter and 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. The Resource Manager abstracts the specifics of the infrastructure from the Tenant appliances, allowing tenants to focus on deploying the desktops rather than managing the infrastructure. A single Resource Manager appliance can be shared across multiple tenants.
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	A tenant appliance that does not include the components that provide brokering or end-user and administrative access. Desktop Manager appliances serve two key purposes: · Desktop capacity scale-out—The initial Tenant appliance supports up to 5,000 virtual desktops per datacenter. When a tenant needs to scale beyond this, Horizon DaaS Desktop Manager appliances can be added to provide the capacity required. Each additional Desktop Manager appliance pair can support up to 5,000 desktops. · Compute resource optimization—A Desktop Manager treats the individually assigned compute resources equally. If a specialized desktop workload is required, it can be optimized by creating a Desktop Manager pair with only the compute resources for that workload assigned to it. Some examples of specialized workloads include delivering standard Virtual Data Infrastructure (VDI), VDI with graphics processing unit (GPU), and Microsoft Remote Desktop Services (RDS). In such cases, the compute resources for the workloads would be separate and distinct from each other.
Desktop Remote Access Manager (dtRAM)	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. After a tenant virtual desktop session is established, all traffic between the client and the virtual desktop passes through the dtRAM server.

Horizon DaaS architecture

Figure 2 shows the CSP and tenant architecture in Horizon DaaS.

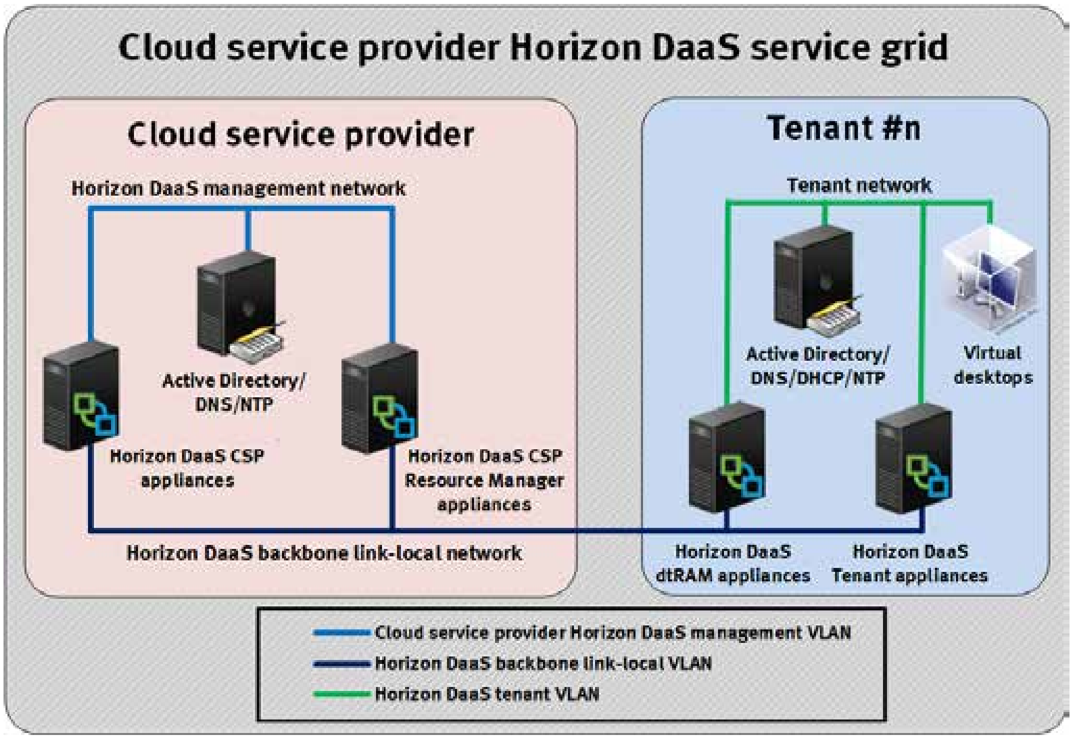

Cloud service provider Horizon DaaS service grid
Cloud service provider
Horizon DaaS management network
Active Directory/ DNS/NTP
Horizon DaaS CSP appliances
Horizon DaaS CSP Resource Manager appliances
Horizon DaaS backbone link-local network
Tenant #n
Tenant network
Active Directory/ DNS/DHCP/NTP
Virtual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

All Horizon DaaS management appliances are connected to the Horizon DaaS backbone link-local network and to the CSP's or tenant's own network. Horizon DaaS requires that all management appliances be installed as high availability (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.

The Horizon DaaS management appliances enable 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, refer to this documentation for more information about the underpinnings of the Horizon DaaS platform, including advanced details concerning the function and interoperability of platform components. Chapter 12: References lists the most relevant documents.

Key solution components

This section provides an overview of the key components of this EMC DaaS solution, as listed Table 2. For information about qualified components and versions required for the initial release of the solution, refer to the *EMC Desktop as a Service: VMware Horizon DaaS with EMC XtremIO All-Flash Array Reference Architecture Guide*.

Table 2. Key solution components

Category	Product
Desktop-as-a-service platform	· VMware Horizon DaaS platform
Virtualization and cloud management	· VMware vSphere · VMware vCenter Server · VMware vSphere Distributed Switch (VDS) · VMware vSphere PowerCLI · VMware vSphere Storage DRS
EMC storage services	· EMC XtremIO all-flash array (for virtual desktops) · EMC Isilon series (for user data) · EMC VNX series (for user data) · EMC Storage Analytics (ESA) · EMC Virtual Storage Integrator (VSI) · EMC PowerPath®/VE

DaaS platform: VMware Horizon DaaS

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 virtual desktops for remote or contract workers and for employees whose physical desktops are unavailable due to a disaster or other interruption

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 hypervisor’s bare-metal architecture requires no operating system. Virtualization functionality is enabled through vCenter Server.

VMware vCenter Server

VMware 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 VMware vSphere High Availability (HA), VMware vSphere Distributed Switch (VDS), VMware vSphere Storage DRS, VMware vSphere vMotion and VMware vSphere Storage vMotion, and VMware vSphere Update Manager.

VMware vSphere Distributed Switch

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

VDS provides 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, Remote Switched Port Analyzer (RSPAN), and Encapsulated Remote Switched Port Analyzer (ERSPAN) protocols for remote network analysis
- Support for advanced vSphere networking features such as templates, to enable backup and restore for the virtual networking configuration, and network health-check capabilities to verify the network configuration between vSphere and the physical network

VMware vSphere PowerCLI

vSphere PowerCLI is a command-line and scripting tool that is built on Microsoft Windows PowerShell. It provides hundreds of commands, 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 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 (sub-millisecond) 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
- A scale-out design that adds performance and capacity in a building block approach, with all building blocks forming a single clustered system

The X-Brick, which supports up to 2,500 full-clone desktops, is the fundamental building block of an XtremIO clustered system. With a Starter X-Brick, you can begin with a small virtual desktop deployment (up to 1,250 full-clone desktops). You can then expand to nearly any scale by upgrading the Starter X-Brick to an X-Brick, and then adding further X-Bricks. 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
- 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 complex configuration required by traditional arrays. 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 similar drive 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.

Data center economics

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

EMC Isilon series

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 making it vastly more scalable, which is in keeping with the dynamic nature of DaaS. 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.

The concept of multitenancy is key to 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 can segregate tenants from one another, and can segregate users within the same tenant organization by their business units or data sets, for example. With an Isilon storage cluster, multitenancy is implemented through secure access zones.

Isilon architecture

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

The Isilon product family includes several node types, differentiated by their functionality and performance characteristics as follows:

- 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 cluster can combine multiple nodes of different types to achieve the performance and capacity levels required by tenants.

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 intra-node communication, cache synchronization, data movement, and workload management.

Access zones

Although the default view of an EMC 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 SMB shares and 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.

EMC Isilon SmartPools

EMC Isilon SmartPools® technology enables a policy-based approach for automatically moving tenant data across multiple tiers of Isilon scale-out storage. This enables CSPs to use the right storage resources for a tenant’s specific workflow, data storage, and data management requirements—automatically and transparently.

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

EMC VNX series

The EMC 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.

Today's VNX platform includes many features and enhancements that are built on the success of the first-generation VNX. These features and enhancements include:

- 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 EMC Unisphere® Management Suite

The VNX platform provides several features that help CSPs achieve their multitenancy goals, including:

- Data Movers and storage processors with dedicated CPU, memory, and network resources.
- Unisphere Quality of Service Manager, 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 attributes such as 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 ensure the privacy of tenant data.

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. 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 Version 8.1: Configuring and Managing CIFS on VNX* on EMC Online Support.

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's production file system

(PFS). With 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.

SnapSure uses a copy-on-first-modify principle. A PFS consists of blocks of data. When a block within the PFS is modified, SnapSure saves a copy containing the block's original contents to a separate volume called the SavVol. Subsequent changes 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 blocks remaining in the PFS, according to a bitmap and blockmap data-tracking structure. These blocks combine to provide a complete point-in-time image called a checkpoint.

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

- Read-only checkpoints—Read-only file systems created from a PFS
- Writeable checkpoints—Read/write file systems 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*, available on EMC Online Support, 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 waiting 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.

ESA includes several default storage dashboards, including XtremIO dashboards. CSPs can use the default dashboards, as well as dashboards customized to individual specifications, to get current and historical information about the status and performance of multiple EMC storage services.

EMC Virtual Storage Integrator for VMware vSphere

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

With VSI, you can efficiently manage and delegate storage tasks through the familiar vCenter Server interface, and perform daily management tasks with up to 90 percent fewer clicks and up to 10 times higher productivity. Furthermore, you can customize the user environment by adding and removing individual VSI features.

CSPs can use VSI to seamlessly provision new XtremIO or VNX Virtual Machine File System (VMFS) datastores within the VMware vSphere Web Client. We[1] used the VSI for vSphere plug-in when validating this solution, including for reclaiming physical capacity on the XtremIO array that was no longer being used.

The *EMC VSI for VMware vSphere Web Client Product Guide*, 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 VDI environments and cloud deployments to deliver high availability and performance.

[1] In this paper, "we" refers to the EMC Solutions engineering team that validated the solution.

Chapter 3 Deploying the Physical DaaS Infrastructure

This chapter presents the following topics:

Overview

This chapter discusses installation and configuration of the key components of this EMC DaaS with VMware Horizon DaaS infrastructure solution, including:

- Configuring the Horizon DaaS network infrastructure
- Configuring the EMC XtremIO array
- Implementing the VMware virtualization infrastructure
- Implementing the VMware Horizon DaaS platform

The chapter also outlines the basic validation tests you need to perform before placing the solution in production.

Where appropriate, the chapter provides external references to vendor documentation for detailed information about particular topics. Chapter 12: References provides a full list of this documentation.

Pre-deployment checklist

A VMware Horizon DaaS deployment requires the following components:

- VMware vSphere
- VMware vCenter Server
- VMware Horizon DaaS platform
- EMC Virtual Storage Integrator (VSI) for VMware vSphere Web Client
- Microsoft Windows Server 2012 R2 (used to host vCenter Server and Microsoft SQL Server resources)
- Microsoft SQL Server 2012 (used as the vCenter Server database server)
- Microsoft Active Directory domain services, and DNS, DHCP, and NTP servers
- Infrastructure, tenant, service provider, and storage network infrastructure

This chapter discusses deployment requirements specific to this EMC DaaS solution. Full documentation for installing and configuring the required components is available on the individual vendor websites. EMC recommends that you review this documentation prior to implementing the VMware Horizon DaaS platform.

Configuring the Horizon DaaS network infrastructure

This section describes the requirements for preparing the network infrastructure that supports the solution.

Configuring the service provider infrastructure network

The service provider infrastructure network requires redundant network links for each vSphere host, the storage array, switch interconnect ports, and switch uplink ports. This configuration provides both redundancy and additional network bandwidth.

This configuration is required regardless of whether the network infrastructure for the solution already exists or is being deployed with other components of the solution.

Configuring the VLANs

The solution requires the following VLANs:

- **Tenant network**—Each tenant requires a single VLAN for hosting the tenant virtual desktops, the tenant infrastructure services, and the tenant Horizon DaaS appliance virtual machines.
- **Service provider infrastructure network**—This VLAN carries network traffic, including VMware Horizon DaaS infrastructure traffic, vSphere management traffic, EMC storage services management traffic, and VMware vMotion and Storage vMotion traffic. You can place vMotion and Storage vMotion traffic on a separate VLAN if required.
- **Service provider Horizon DaaS backbone network**—This VLAN is used for communication between Horizon DaaS infrastructure appliances. The VLAN should be private and not accessible from other networks.

Configuring the storage network

This solution requires a dedicated storage network to connect vSphere hosts to the XtremIO array. The storage network can use 8 Gb FC, 10 Gb CEE with FCoE, or 10 GbE with iSCSI. An iSCSI storage network requires a dedicated VLAN. FC and FCoE networks do not require an additional VLAN.

For testing the solution, we used an FC storage network. This network requires redundant FC switches and links for each vSphere host and for the storage array. This configuration provides both redundancy and additional storage network bandwidth. We connected each vSphere host to both FC switches, and each switch to each Storage Controller on the storage array. We then placed each FC connection between the vSphere host and the storage array in a separate FC zone.

Figure 3 shows the storage network architecture we used for testing the solution.

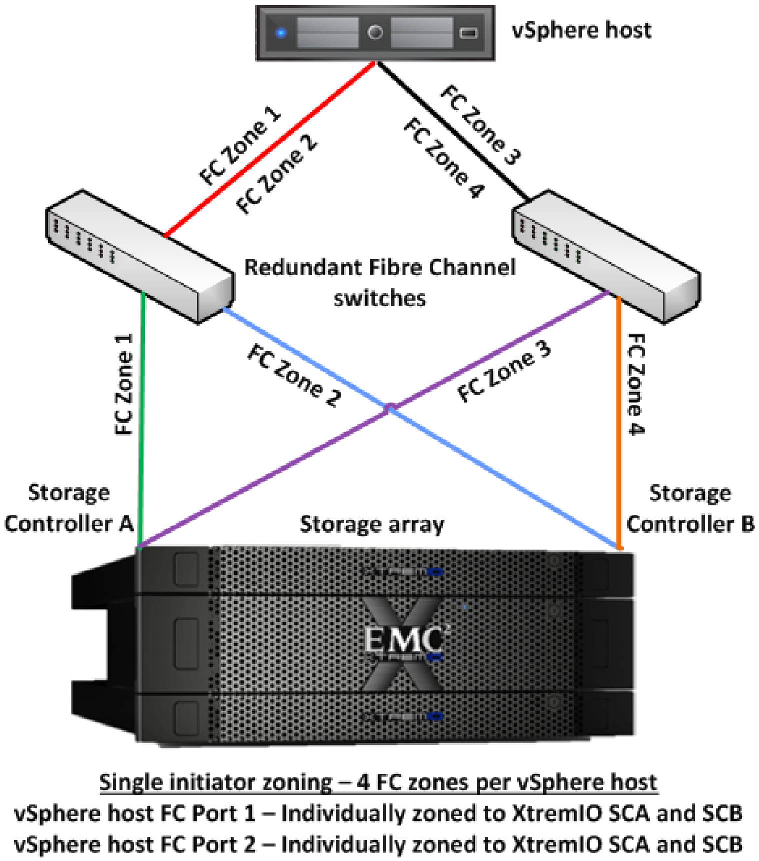

vSphere host
FC Zone 1
FC Zone 2
FC Zone 3
FC Zone 4
Redundant Fibre Channel switches
FC Zone 1
FC Zone 2
FC Zone 3
FC Zone 4
Storage Controller A
Storage array
Storage Controller B
EMC
Single initiator zoning – 4 FC zones per vSphere host
vSphere host FC Port 1 – Individually zoned to XtremIO SCA and SCB
vSphere host FC Port 2 – Individually zoned to XtremIO SCA and SCB

Figure 3. Example FC storage network architecture

Completing the network cabling

Ensure that all solution servers, storage arrays, switch interconnects, and switch uplinks have redundant connections and are plugged into separate switching infrastructures.

Configuring the EMC XtremIO array

EMC or EMC partner engineers are responsible for installing and configuring EMC XtremIO storage arrays. When installation is complete, the CSP administrator carries out these final configuration steps:

- Configure custom XtremIO event handlers to ensure that alerts are sent to the appropriate monitoring facilities or individuals.
- Configure XtremIO volumes for use with the Horizon DaaS tenant vSphere desktop hosts—in this solution, the XtremIO array provides VMware Virtual Machine File System (VMFS) data storage for the vSphere hosts.

Configuring custom XtremIO event handlers

Service providers can configure XtremIO event handlers to forward alerts to specified email recipients, and to event logging mechanisms such as SNMP and syslog, when particular event types occur. Alerts are automatically written to the local XtremIO log files.

Table 3 summarizes the main XtremIO event classifications that administrators should monitor closely. For a full list of XtremIO errors and alerts, and the thresholds or events associated with them, refer to the *EMC XtremIO Storage Array User Guide.*

Table 3. XtremIO events to monitor

Category	Severity	Entity	Description
All	Critical	All	All critical events within the XtremIO cluster
All	Major	All	All major events within the XtremIO cluster
Software	Minor	Cluster	Cluster capacity, XtremIO Management Server (XMS) to cluster communication, and other events
Software	Minor	Storage Controller	XMS to Storage Controller communication, Storage Controller journal, and other events
Activity	All	All	XMS authentication failures, configuration failures, and other events

The following procedure describes how to create an event handler for Software–Minor–Cluster events, which include events related to free physical capacity on the XtremIO cluster and to the connection between the XMS and the XtremIO cluster.

To create the event handler:

1. In the XtremIO Storage Management Application, select **Alerts & Events** > **Events**.
2. In the **Events** window, click the **Display Event Handlers** button, as shown in Figure 4.

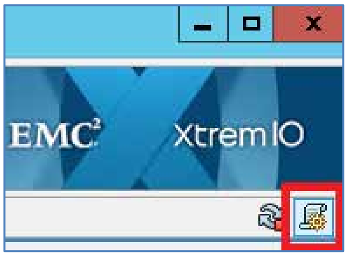


Figure 4. XtremIO Storage Management: Display Event Handlers

3. In the **Event Handlers** dialog box, click **Add**.

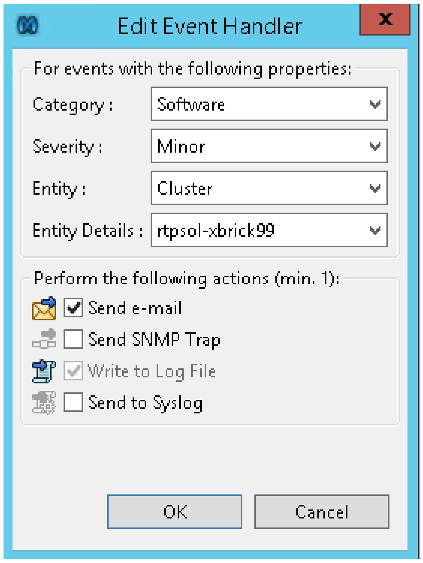
4. In the **Add Event Handler** dialog box, set the following event properties, as shown in Figure 5:

   § **Category**: Software

   § **Severity**: Minor

   § **Entity**: Cluster

   § **Entity Details**: Select the relevant XtremIO cluster; the cluster is identified by the name specified during installation of the XtremIO array.



Edit Event Handler

For events with the following properties:

Category : Software

Severity : Minor

Entity : Cluster

Entity Details : rtpsol-xbrick99

Perform the following actions (min. 1):

☑ Send e-mail

□ Send SNMP Trap

☑ Write to Log File

□ Send to Syslog

Figure 5. XtremIO Storage Management: Edit Event Handler

5. Select the actions to be performed following the event, and then click **OK**:

   a. Select **Send email** to send alerts to particular email recipients.

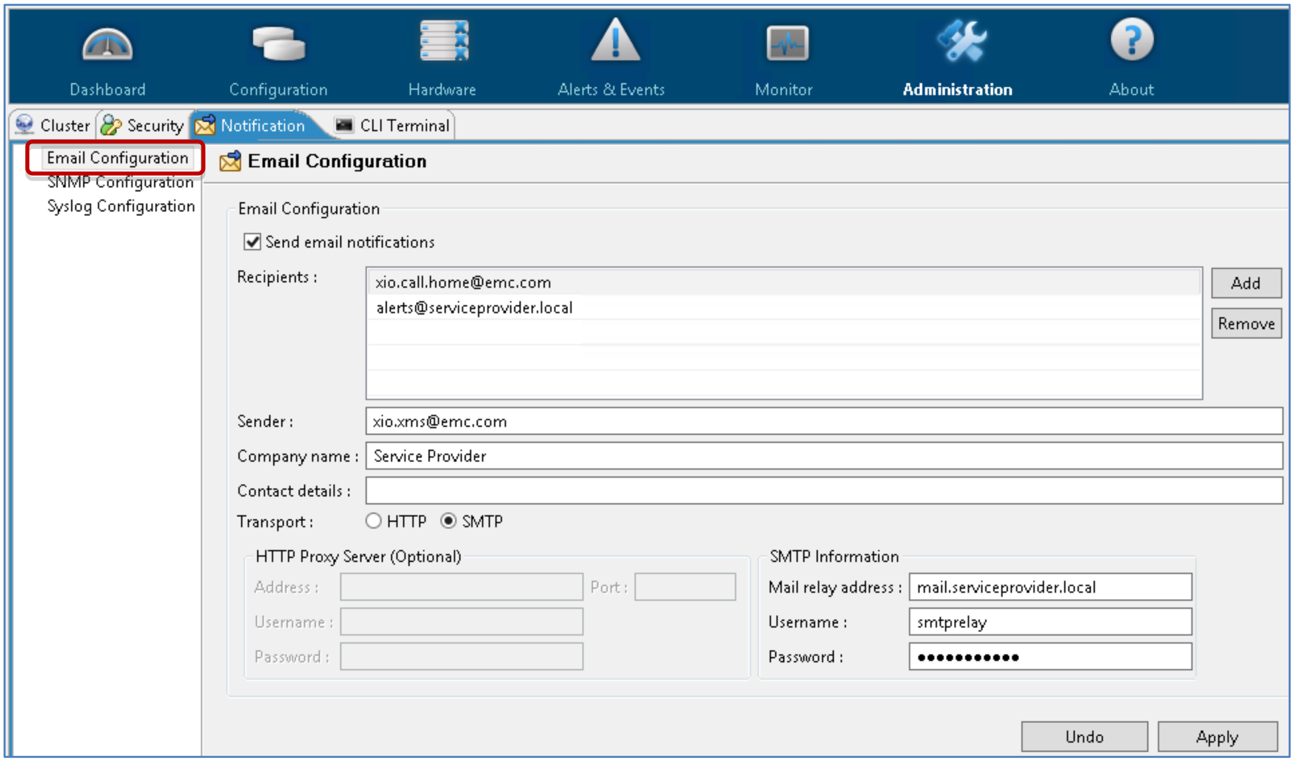
   b. Select **Send SNMP Trap** or **Send to Syslog** or both to use those options for sending alerts.

6. Click **Administration** in the menu bar.

7. Select **Notification** > **Email Configuration**, as shown in Figure 6.

8. For **Email Configuration**, use the **Add** button to select the email addresses that you want to receive copies of the XtremIO alerts, as shown in Figure 6.

   If not already configured, provide SMTP (email) relay information in the **SMTP Information** fields. When finished, click **Apply**.



Email Configuration

Email Configuration

☑ Send email notifications

Recipients : xio.call.home@emc.com
alerts@serviceprovider.local

Sender : xio.xms@emc.com

Company name : Service Provider

Contact details :

Transport : ○ HTTP ● SMTP

HTTP Proxy Server (Optional)

Address :
Port :
Username :
Password :

SMTP Information

Mail relay address : mail.serviceprovider.local

Username : smtprelay

Password : ●●●●●●●●●●●

Figure 6. XtremIO Storage Management: Notification

9. For the SNMP and syslog options in step 5, configure as follows (if not already configured):
    a. To add an SNMP server, click **SNMP Configuration**, set the required options, and click **Apply**.
    b. To add a syslog server, click **Syslog Configuration**, set the required options, and click **Apply**.

Provisioning XtremIO storage for vSphere datastores

Provisioning XtremIO storage for Horizon DaaS tenant desktops involves configuring volumes on the XtremIO array, and then connecting the volumes to the appropriate vSphere hosts as described in Connecting the vSphere datastores.

EMC recommends that each XtremIO volume hosts no more than 125 desktops. This ensures that vSphere maintenance operations, such as SCSI UNMAP, can be completed in a reasonable amount of time. Reclaiming XtremIO physical capacity provides additional information about vSphere SCSI UNMAP operations.

Sizing examples

Table 4 provides two sizing examples for determining the number of volumes to configure and the volume size. In the examples, the Starter X-Brick and X-Brick are configured to support the recommended maximum number of full clone desktops—that is, 1,250 and 2,500 desktops respectively.

Table 4. XtremIO sizing examples

XtremIO configuration	Number of desktops	Desktop type	Number of volumes	Volume size
Starter X-Brick	1,250	Full clone: Microsoft Windows 7 or Microsoft Windows Server 2012 R2 VDI image	10	5 TB
X-Brick	2,500		20	

Both examples provide 32,768 GB of space for each tenant desktop in an XtremIO volume. This leaves 20 percent of free space for SCSI UNMAP operations. The volume size can be adjusted up or down based on tenant requirements.

You calculate the required volume size by multiplying the total space needed for the desktops by 1.25—this ensures that the volume has 20 percent of free space:

```
((Desktop gold image thick virtual hard disk size in GB + Amount
of RAM configured for the desktop image in GB) * 125 desktops) *
1.25
```

For the examples in Table 4, the calculation is:

```
((30.768 GB + 2 GB) * 125) * 1.25 = 5120 GB or 5 TB per XtremIO
volume
```

After the required volume size is determined, calculate the number of volumes required by dividing the required number of desktops by 125:

```
Number of desktops / 125 desktops per volume = Number of volumes
required
```

For example, to deploy 5,000 desktops, you need 40 volumes:

```
5000 desktops / 125 desktops per volume = 40 volumes
```

Configuring XtremIO volumes

To configure volumes on the XtremIO array for storing tenant virtual desktops:

1. In the XtremIO Storage Management Application, click **Configuration** in the menu bar.
2. In the **Volume** pane of the **Configuration** workspace, click **Add**.
3. In the **Add New Volumes** dialog box, click **Add Multiple**.
4. In the **Add Multiple Volumes** dialog box, set the following properties and click OK:
   - **Number of Volumes**—Type the required number of volumes, based on the XtremIO configuration (Starter X-Brick or X-Brick) and the number of virtual desktops.
   - **Name**—Type a common LUN name. A numeric suffix is assigned automatically to the name of each volume.
   - **Size**—Type the required volume size—for example, 5,000 GB is the volume size we used for testing the solution.

Implementing the VMware virtualization infrastructure

This section provides information about installing and configuring the VMware virtualization infrastructure required to support the solution architecture, including:

- Installing and configuring the vSphere hosts
- Configuring vSphere host networking
- Installing vCenter Server
- Connecting the vSphere datastores
- Deploying EMC Virtual Storage Integrator (VSI)
- Optimizing the vSphere hosts for XtremIO
- Enabling and configuring vSphere Storage DRS

Installing and configuring the vSphere hosts

On initial power up of the servers being used for vSphere, confirm or enable the hardware-assisted CPU virtualization setting and the hardware-assisted MMU virtualization setting in the server's BIOS. If the servers are equipped with a RAID controller, EMC recommends that you configure mirroring on the local disks.

Start up the vSphere installation media and install the hypervisor on each of the servers. vSphere host names, IP addresses, and a root password are required for installation.

Configuring vSphere host networking

The *VMware vSphere Networking* guide describes vSphere networking configuration, including load balancing, link aggregation, and failover options. Choose the appropriate load-balancing option based on what your network infrastructure supports. Refer to the list of documents in Chapter 12: References for more information.

Network interface cards

The vSphere installation process creates a standard virtual switch (vSwitch). By default, vSphere chooses only one physical network interface card (NIC) as a vSwitch uplink. To maintain redundancy and bandwidth requirements, configure an additional NIC, either by using the vSphere console or by connecting to the vSphere host from the vSphere Client.

If your environment uses a vSphere Distributed Switch (VDS), use the vSphere Web Client to configure the VDS after the target vSphere host has been added to vCenter Server. When creating a VDS, the vSphere Web Client prompts you to import existing vSphere NICs and VMkernel interfaces, including those currently assigned to the standard vSwitch.

Each vSphere host should have multiple interface cards for each virtual network to ensure redundancy and to support network load balancing, link aggregation, and network adapter failover.

Virtual machine port groups and VMkernel ports

Create VMkernel ports and virtual machine port groups or Distributed Virtual Port Groups (DVPG) as required, based on your infrastructure configuration:

- VMkernel port for vMotion
- Service provider virtual machine port groups or DVPGs (used by the service provider for the Horizon DaaS infrastructure virtual machines)
- Service provider Horizon DaaS backbone port group (used for communication between Horizon DaaS appliances)
- Tenant virtual machine port groups or DVPGs (used by the tenant virtual desktops to communicate on the network)

Note: DVPGs must be configured to use ephemeral port binding.

The VMware document *vSphere Networking* describes the procedure for configuring these settings.

Installing vCenter Server

The solution requires a minimum of one vCenter Server instance for managing the virtual infrastructure. To enable redundancy within the data center, or for scaling purposes, multiple vCenter Server instances can be deployed. Consult VMware vSphere Documentation for information about vCenter Server hardware and software requirements, and for detailed installation and configuration instructions.

The following steps must be completed after vCenter Server is installed and the vSphere hosts have been added to the management console:

- Create at least one vSphere cluster to use with a tenant deployment and populate it with the required number of vSphere hosts; ensure that sufficient resources exist to host the number of desktops that the tenant initially intends to deploy.
- Create a vSphere cluster to host the Horizon DaaS infrastructure virtual machines.
- If required, create a VDS, and add or import any existing vSphere host VMkernel interfaces and NICs. Additionally, create any required service provider and tenant virtual machine port groups.
- If your environment uses EMC PowerPath/VE, deploy the software by using the VMware vSphere Update Manager. Refer to *EMC PowerPath/VE for VMware vSphere Installation and Administration Guide* for details.
- If your solution uses PowerCLI scripts instead of the EMC VSI plug-in to optimize vSphere for use with the XtremIO array, refer to Using scripts to optimize vSphere and XtremIO performance for information about the setting changes required before XtremIO volumes are presented to the vSphere hosts.

Connecting the vSphere datastores

Connect and format the XtremIO volumes, configured in Configuring the EMC XtremIO array, to the appropriate vSphere cluster or individual hosts, including the volumes configured for:

- Tenants' virtual desktop storage
- Service provider's Horizon DaaS infrastructure virtual machine storage (if required)

To enable vSphere hosts to access the XtremIO volumes, configure an XtremIO initiator group for each vSphere cluster and add the appropriate vSphere hosts to the initiator group, as follows:

1. In the XtremIO Storage Management Application, click **Configuration** in the menu bar.
2. In the **Initiator Groups** pane in the **Configuration** workspace, click **Add**.
3. In the **Add New Initiator Group** dialog box, type a name for the initiator group, and click **Add**.
4. In the **Add Initiator** dialog box, specify the following settings and click **OK**:
   - **Initiator Name**: Type a name for the new initiator.
   - **Initiator Port Address**: Select the initiator port of a vSphere host to add to the initiator group.
5. Repeat step 4 to add all target initiator ports to the initiator group. Then click **Finish**.
6. In the **Configuration** workspace, map the target volumes to the initiator group:
   a. Select the target volumes in the **Volumes** pane.
   b. Select the target initiator group in the **Initiator Groups** pane.
   c. Click **Map All**.
   d. Click **Apply** to complete the process and grant the vSphere hosts access to the selected volumes.
7. In the vSphere Web Client, perform a **Rescan for Datastores** operation on the vSphere hosts so that they can immediately see the XtremIO volumes to which they have been granted access.
8. Repeat steps 1–7 as needed to create an initiator group for each vSphere cluster.

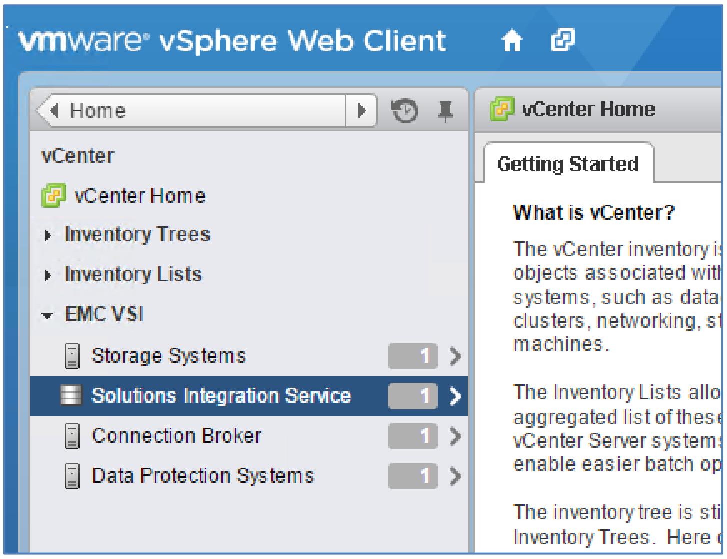
The VMware document *vSphere Storage* provides instructions on how to format the vSphere datastores after the XtremIO initiator groups are configured. Refer to the list of documents in Chapter 12: References for more information.

Deploying EMC Virtual Storage Integrator (VSI)

The EMC VSI plug-in enables administrators to perform most common XtremIO administrative tasks from the vSphere Web Client, instead of having to use the XtremIO management console. Furthermore, administrators can use the plug-in to perform key vSphere host optimizations for XtremIO, instead of having to use vSphere PowerCLI. If a VNX array is deployed as part of this solution, administrators can use the VSI plug-in to manage this storage also.

If your solution uses the VSI plug-in, refer to the *EMC VSI for VMware vSphere Web Client Product Guide* for installation, configuration, and operation instructions.

Figure 7 shows an EMC VSI installation that has been successfully integrated with the vSphere Web Client, as displayed on the **vCenter Home** page.



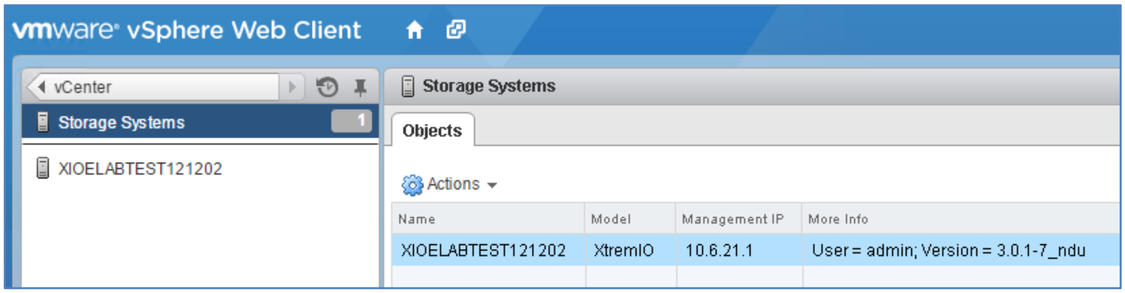
The vCenter inventory i
objects associated wit
systems, such as data
clusters, networking, s
machines.

The Inventory Lists allo
aggregated list of these
vCenter Server system
enable easier batch op

The inventory tree is sti
Inventory Trees. Here

Figure 7. vSphere Web Client: EMC VSI integration

The **vCenter Home** > **Storage Systems** option lists all EMC storage systems after you have added them to the VSI plug-in. In the example in Figure 8, the XtremIO array has been successfully added and is available for management in the vSphere Web Client.



Name	Model	Management IP	More Info
XIOELABTEST121202	XtremIO	10.6.21.1	User = admin; Version = 3.0.1-7_ndu

Figure 8. vSphere Web Client: EMC VSI Storage Systems

After you have added an array to the VSI plug-in, the vSphere Web Client lists all of the array’s datastores. Right-click a datastore and select **All EMC VSI Plugin Actions** to access all actions you can apply to that datastore, as shown in Figure 9.

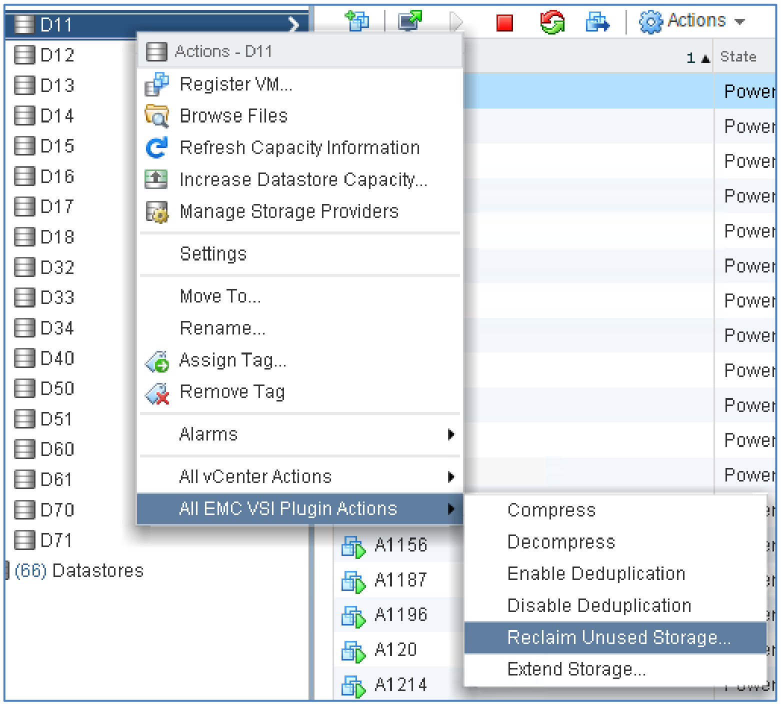


Figure 9. vSphere Web Client: EMC VSI XtremIO datastore actions

Optimizing the vSphere hosts for XtremIO

You must update multiple vSphere host settings to ensure optimal performance of the XtremIO array with vSphere. The *EMC XtremIO Storage Array User Guide* outlines these settings.

You can use either of the following to implement the required settings:

- EMC VSI plug-in
- vSphere PowerCLI scripts

Both options produce the same results. However, the EMC VSI plug-in provides the quickest and easiest way to implement the required settings. The PowerCLI scripts automate the process, and are useful in environments where automated implementation of the settings is specifically preferred.

If the XtremIO volumes have already been presented to the vSphere hosts, you must use the EMC VSI plug-in instead of the PowerCLI scripts to implement the settings.

Note: The settings apply only to vSphere hosts connected to XtremIO arrays. Do not apply them to block datastores hosted on other array types, including other EMC arrays. However, you can apply the settings to vSphere hosts that are connected to NFS datastores, because the settings have no effect on communication with those NFS datastores.

Using the EMC VSI plug-in to optimize vSphere and XtremIO performance

To configure the optimization settings with the EMC VSI plug-in:

1. Log in to the vSphere Web Client with an account that has administrative permissions for both vSphere and the EMC VSI plug-in.
2. Navigate to the **Hosts and Clusters** window.

3. In the list of vSphere hosts, identify a host that requires the updated settings, right-click it, and select **All EMC VSI Plugin Actions** > **ESX Host Settings**, as shown in Figure 10.

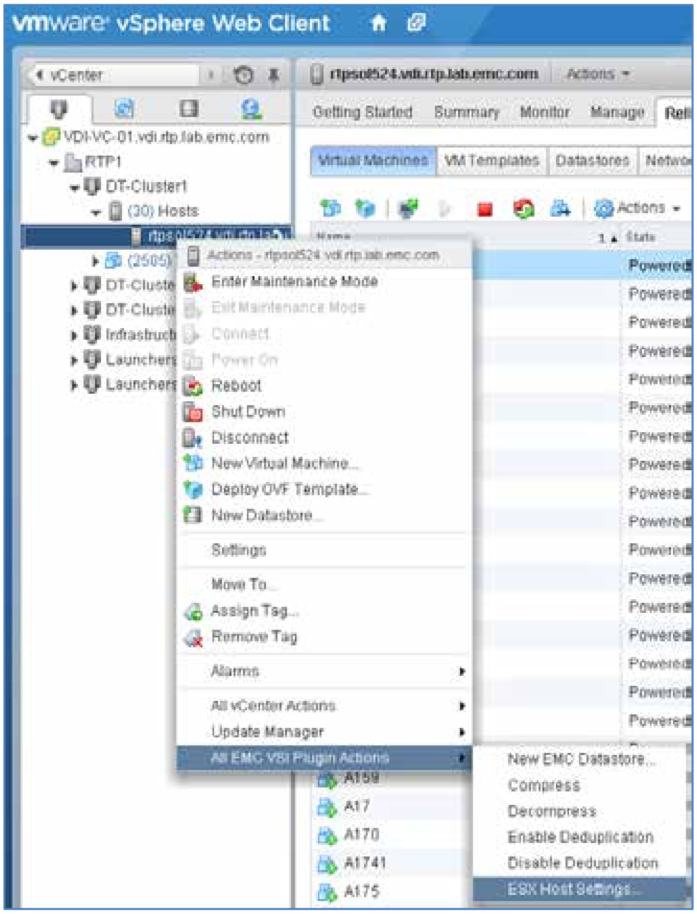
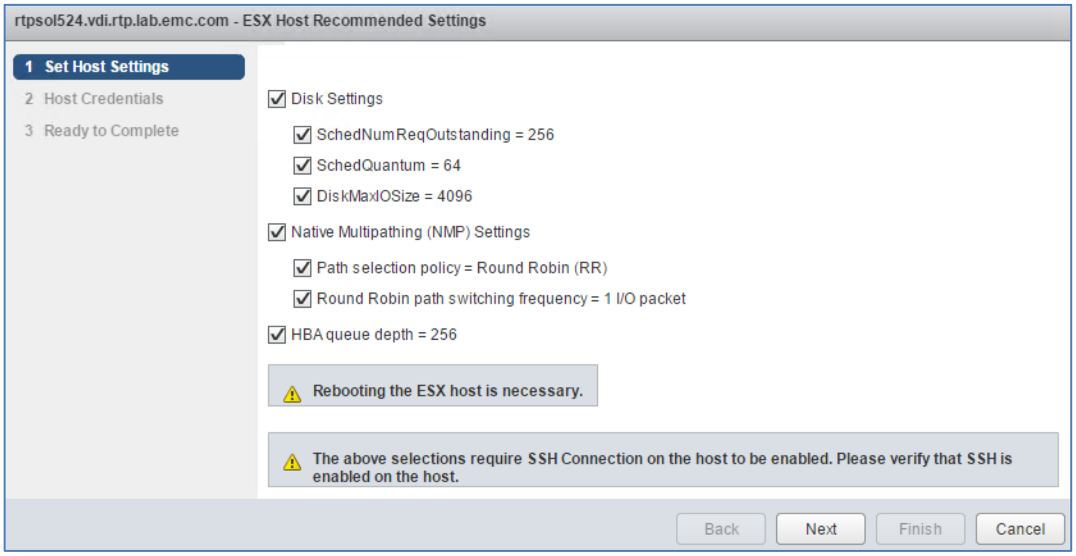


Figure 10. vSphere Web Client: EMC VSI Host Settings

4. In **Set Host Settings**, select all available options, as shown in Figure 11, and then click **Next**.

Note: SSH access to the vSphere host is required, and a reboot is required to implement all of the settings.


rtpsol524.vdi.rtp.lab.emc.com - ESX Host Recommended Settings

☑ Disk Settings

☑ SchedNumReqOutstanding = 256

☑ SchedQuantum = 64

☑ DiskMaxIOSize = 4096

☑ Native Multipathing (NMP) Settings

☑ Path selection policy = Round Robin (RR)

☑ Round Robin path switching frequency = 1 I/O packet

☑ HBA queue depth = 256

⚠ Rebooting the ESX host is necessary.

⚠ The above selections require SSH Connection on the host to be enabled. Please verify that SSH is enabled on the host.

Figure 11. vSphere Web Client: EMC VSI Set Host Settings

5. In **Host Credentials**, type the credentials for a local account on the vSphere host and click **Next**.

Note: The local account must have root access.

---

6. In **Ready to Complete**, review the proposed changes, and then click **Finish**.
7. Repeat steps 3–6 for the other vSphere hosts in the cluster.

At this point, the vSphere hosts are configured with the optimal settings for use with XtremIO.

Using scripts to optimize vSphere and XtremIO performance

To configure the required optimization settings with vSphere PowerCLI scripts, execute the two scripts provided in this section:

- **Script 1**—Changes multiple default settings that affect the XtremIO volumes that are presented to the vSphere hosts
- **Script 2**—Changes the maximum number of outstanding disk requests for each vSphere datastore to 256

Script 2 requires that the XtremIO volumes have already been presented to and formatted by the target vSphere hosts, so ensure that Script 1 has successfully completed before you run Script 2.

Script 1

Save the script as a text file with the .ps1 extension, and then execute the script within a vSphere PowerCLI session. When prompted, type the name of the vSphere cluster that contains the hosts whose settings you want to update.

```
$clusterName= Read-Host 'Please enter the target vSphere cluster
name to create the XtremIO NMP rules'
$vmhosts = get-vmhost –location $clusterName
foreach ($vmhost in $vmhosts) {
Set-VMhostAdvancedConfiguration -vmhost $vmhost Disk.SchedQuantum
-Value 64
Set-VMhostAdvancedConfiguration -vmhost $vmhost Disk.DiskMaxIOSize
-Value 4096
$esxcli = get-esxcli -vmhost $vmhost
$esxcli.storage.nmp.satp.rule.add($null, "tpgs_off", "XtremIO-
ActiveActive", $null, $null, $null, "XtremApp", $null,
"VMW_PSP_RR", "iops=1", "VMW_SATP_DEFAULT_AA", $null, "vendor",
"XtremIO")
}
```

Script 2

Save the script as a text file with the .ps1 extension, and then execute the script within a vSphere PowerCLI session. When prompted, type the name of the vSphere cluster that contains the hosts whose datastore settings you want to update.

```
$clusterName= Read-Host 'Please enter the target vSphere cluster
name to update the Disk.SchedNumReqOutstanding value for all
XtremIO datastores'
$vmhosts = get-vmhost –location $clusterName
foreach ($vmhost in $vmhosts) {
$esxcli = get-esxcli -vmhost $vmhost
$AllLUNs = get-scsilun -vmhost $vmhost | where {$_.vendor -eq
"XtremIO"}
foreach ($lun in $AllLUNs) {
$CN = $lun.canonicalname
$EsxCli.storage.core.device.set($null, $cn, $null, $null, $null,
$null, $null, 256, $on)
}
}
```

Enabling and configuring vSphere Storage DRS

This solution uses vSphere Storage DRS to distribute desktops across all the datastores in a tenant's vSphere cluster. The solution requires this feature because Horizon DaaS will only deploy desktops to the datastore where a tenant's gold image[2] is located, even if multiple datastores are present. You can also use vSphere Storage DRS to automate the migration of desktops from one set of vSphere datastores to another, even if the datastores are located on different storage arrays.

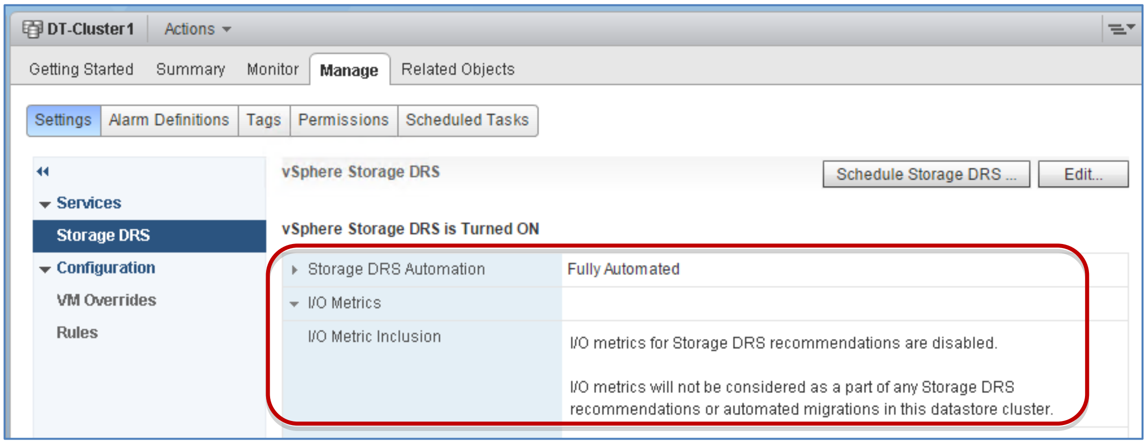
Refer to the VMware document *vSphere Resource Management* for instructions on how to enable and configure vSphere Storage DRS for a vSphere cluster. It is important to review the Storage DRS documentation prior to implementing Storage DRS in a production environment, because a large number of concurrent Storage DRS

[2] A gold image is a master image or template for a tenant's virtual desktops.

Storage vMotion operations might become noticeable to a tenant that is using a desktop when the operations occur. By default, Storage DRS runs only when the difference in space utilization by the datastores in a given datastore cluster is five percent or greater; this value is optimal in most cases.

For this solution, EMC recommends the following vSphere Storage DRS settings:

- Enable vSphere Storage DRS for each tenant datastore cluster.
- Disable I/O metrics for vSphere Storage DRS recommendations, as shown in Figure 12. This feature is not required when using an XtremIO array.

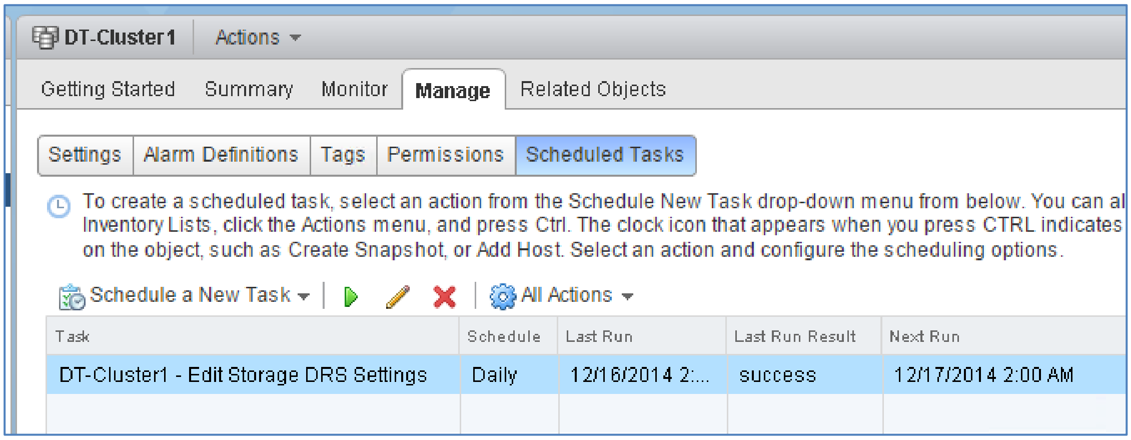


vSphere Storage DRS is Turned ON

Storage DRS Automation	Fully Automated
I/O Metrics	
I/O Metric Inclusion	I/O metrics for Storage DRS recommendations are disabled. I/O metrics will not be considered as a part of any Storage DRS recommendations or automated migrations in this datastore cluster.

Figure 12. vSphere Web Client: Storage DRS Settings

- In **Schedule Storage DRS**, set Storage DRS to run only during off-peak hours for the tenant, as shown in Figure 13.



To create a scheduled task, select an action from the Schedule New Task drop-down menu from below. You can al Inventory Lists, click the Actions menu, and press Ctrl. The clock icon that appears when you press CTRL indicates on the object, such as Create Snapshot, or Add Host. Select an action and configure the scheduling options.

Task	Schedule	Last Run	Last Run Result	Next Run
DT-Cluster1 - Edit Storage DRS Settings	Daily	12/16/2014 2:...	success	12/17/2014 2:00 AM

Figure 13. vSphere Web Client: Schedule Storage DRS

Whenever a tenant deploys more desktops than can fit on a single vSphere datastore, such as when their Horizon DaaS environment is first provisioned, the Storage DRS scheduled task must be executed manually to immediately balance storage utilization. To do this, click **Run** (the green triangle shown in Figure 13).

Implementing the VMware Horizon DaaS service provider infrastructure

This section summarizes the prerequisites and the high-level tasks for installing and configuring the VMware Horizon DaaS service provider infrastructure. Chapter 8: Provisioning Horizon DaaS Tenants provides similar information for the Horizon DaaS tenant infrastructure.

For detailed information about deploying and configuring the Horizon DaaS service provider and tenant infrastructure, refer to the following VMware documents:

- *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter*
- *Horizon DaaS Platform 6.1 Tenant Installation – vCenter*

Service provider infrastructure prerequisites

Before installing the Horizon DaaS service provider infrastructure, the following resources must be available:

Note: Some of these resources are discussed in earlier sections of this guide, but are included here for completeness.

- A VLAN for the service provider's Horizon DaaS and vSphere infrastructure.
- A private VLAN for the Horizon DaaS backbone network.
- A vSphere cluster, or at least two vSphere hosts, for the Horizon DaaS and vSphere infrastructure virtual servers.
- An Active Directory infrastructure and DNS, DHCP, and NTP services for the server provider infrastructure.

  Refer to *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter* for additional information about this requirement.
- Two accounts in the service provider Active Directory domain:
  - An account with the required vSphere permissions in the service provider's vCenter Server instance. Refer to VMware Horizon DaaS documentation for information about the required permissions.
  - An account that will be granted full administrative permissions within the service provider Horizon DaaS infrastructure.
- A subnet with sufficient IP space for the service provider network, and five IP addresses for the Horizon DaaS appliances:
  - Two IP addresses for the Service Provider appliances.
  - One IP address for use as a shared floating IP address.

    To manage Horizon DaaS using a DNS name, create a DNS record that points to the shared IP address.
  - Two IP addresses for the service provider's Resource Manager appliances.

- At least a /22 network if the Horizon DaaS backbone network uses the link-local IP space. If Horizon DaaS will be deployed to multiple datacenters, each link-local IP space should use a unique range of IP addresses.

  Refer to *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter* for additional information about this requirement.

- A datastore for the service provider's Horizon DaaS virtual appliances. The appliances can use the datastore that hosts the vCenter Server instance, if that datastore is already configured and has sufficient free space.

  Each Horizon DaaS appliance uses up to 23 GB of storage, including swap space, so the target datastore must initially have at least 100 GB of free space to accommodate the four Horizon DaaS appliances required for the service provider infrastructure. If the Horizon DaaS deployment uses multiple vCenter Server instances, each instance requires an additional pair of Horizon DaaS appliances; each pair of appliances requires another 50 GB of storage.

- The Horizon DaaS installation media, which includes the following:
  - The installation package for the Horizon DaaS appliance Open Virtualization Appliance (OVA) file.
  - The Debian installation package.
  - DaaS Agent.
  - Desktop Remote Access Manager (dtRAM).

- The VMware Horizon View Agent and Agent Direct Connect Plug-in installers, and the PCoIP.adm group policy template from the VMware Horizon View GPO bundle, which are required for the tenant desktops.

- An SSL Certificate in Apache2 format to use with the Horizon DaaS appliances, if required.

  Refer to *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter* for additional information about this requirement.

Installing and configuring the service provider infrastructure

To install and configure the service provider portion of the Horizon DaaS infrastructure, use the procedures outlined in *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter*. These procedures deploy the following components:

- Horizon DaaS appliances:
  - A Horizon DaaS appliance virtual machine—this provides a template for expanding the Horizon DaaS service provider infrastructure and for deploying the Horizon DaaS tenant appliances.

    Note: As indicated in the Horizon DaaS documentation, do not power on this virtual machine after it has been configured.

  - A pair of redundant Service Provider appliances—these provide the primary management interface for the Horizon DaaS infrastructure.
  - A pair of redundant Resource Manager appliances—these manage the interface with the vCenter Server instance and provide tenant access to vSphere resources.

- Global tenant desktop models:

  These control the desktop types that tenants can deploy, and the amount of CPU and RAM resources that can be assigned to the desktops.

  These desktop models offer a variety of static and dynamic (non-persistent) desktop configurations to support different tenant desktop requirements in relation to desktop operating system, application load, and user type.

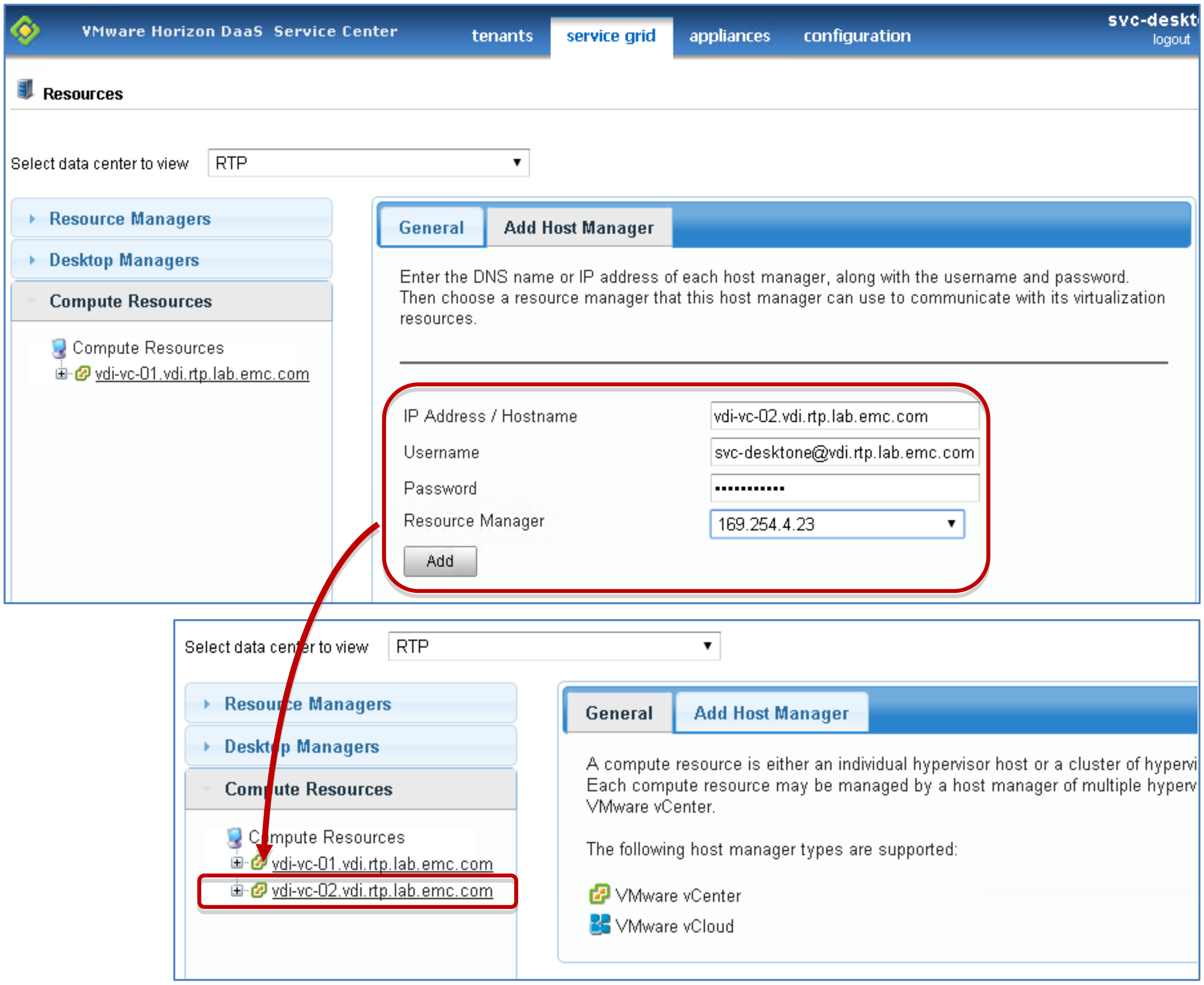
At this point, the Horizon DaaS infrastructure is ready to deploy a tenant, as outlined in Chapter 8: Provisioning Horizon DaaS Tenants.

Deploying multiple vCenter Server instances

For a Horizon DaaS infrastructure that requires multiple vCenter Server instances, use the CSP Horizon DaaS Service Center to add them, after completing the Installing and configuring the service provider infrastructure process. Follow these steps:

1. Navigate to the **service grid** option in the CSP Horizon DaaS Service Center, and select **Compute Resources** > **Add Host Manager**, as shown in Figure 14.
2. In the **Add Host Manager** dialog box, specify the following options:
   - **IP Address/Hostname**—The vCenter Server DNS name
   - **Username**—An account with the necessary permissions for the vCenter Server instance
   - **Password**—The password for the specified account
   - **Resource Manager**—An available Horizon DaaS Resource Manger
3. Click **Add**.

The **Compute Resources** option now includes the newly added vCenter Server instance, as shown in Figure 14. vSphere host resources managed by the vCenter Server instance can now be assigned to tenants as needed.



Select data center to view RTP

Enter the DNS name or IP address of each host manager, along with the username and password. Then choose a resource manager that this host manager can use to communicate with its virtualization resources.

IP Address / Hostname: vdi-vc-02.vdi.rtp.lab.emc.com
Username: svc-desktone@vdi.rtp.lab.emc.com
Password: ••••••••••••
Resource Manager: 169.254.4.23

A compute resource is either an individual hypervisor host or a cluster of hypervi
Each compute resource may be managed by a host manager of multiple hyperv
VMware vCenter.

The following host manager types are supported:

Figure 14. Horizon DaaS Service Center: Add Host Manager

Validating the VMware Horizon DaaS infrastructure

You must validate the functionality of the individual components of the VMware Horizon DaaS infrastructure prior to placing the solution into production. This section describes basic validation tests of the core components needed for the solution to function, both in general terms and in the event of a failure.

The basic validation tests include the following:

- Verifying the configuration of the Horizon DaaS platform
- Verifying vSphere configuration and functionality
- Verifying the redundancy of the EMC storage services

Verifying the configuration of the Horizon DaaS appliances

The CSP Horizon DaaS Service Center provides several status views that you can use to verify that the Horizon DaaS appliances are functioning properly and can successfully interact with other infrastructure components.

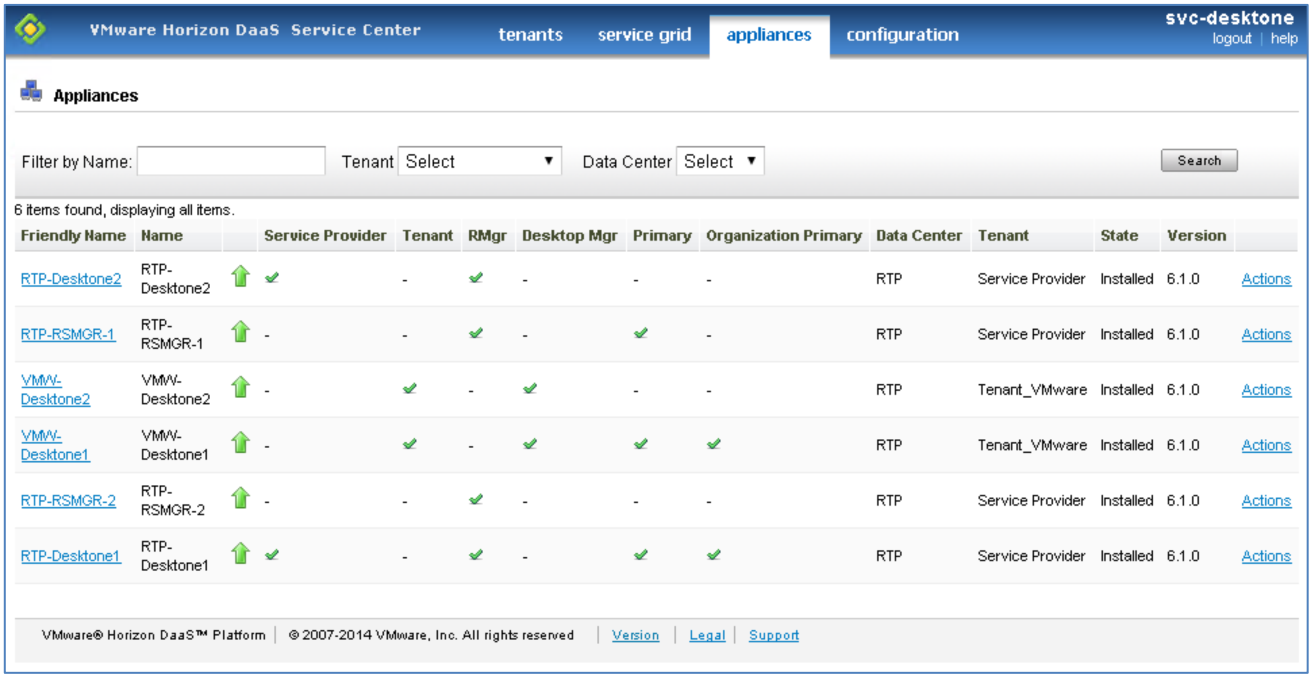
Complete the following steps in the CSP Horizon DaaS Service Center to verify the configuration and basic operation of the Horizon DaaS platform.

Note: if troubleshooting is required, refer to the VMware Horizon DaaS and VMware vSphere documentation for troubleshooting steps.

---

1. The **Appliances** status window displays the status of each Horizon DaaS appliance deployed in the environment, both for the service provider and for the tenants, as shown in Figure 15. The arrows to the right of the appliance **Name** column indicate the status of the appliances.

   Verify that each appliance is running; a green arrow denotes this. A red arrow denotes an error; in this case, perform the appropriate troubleshooting to resolve the error.



Filter by Name: Tenant Select Data Center Select

6 items found, displaying all items.

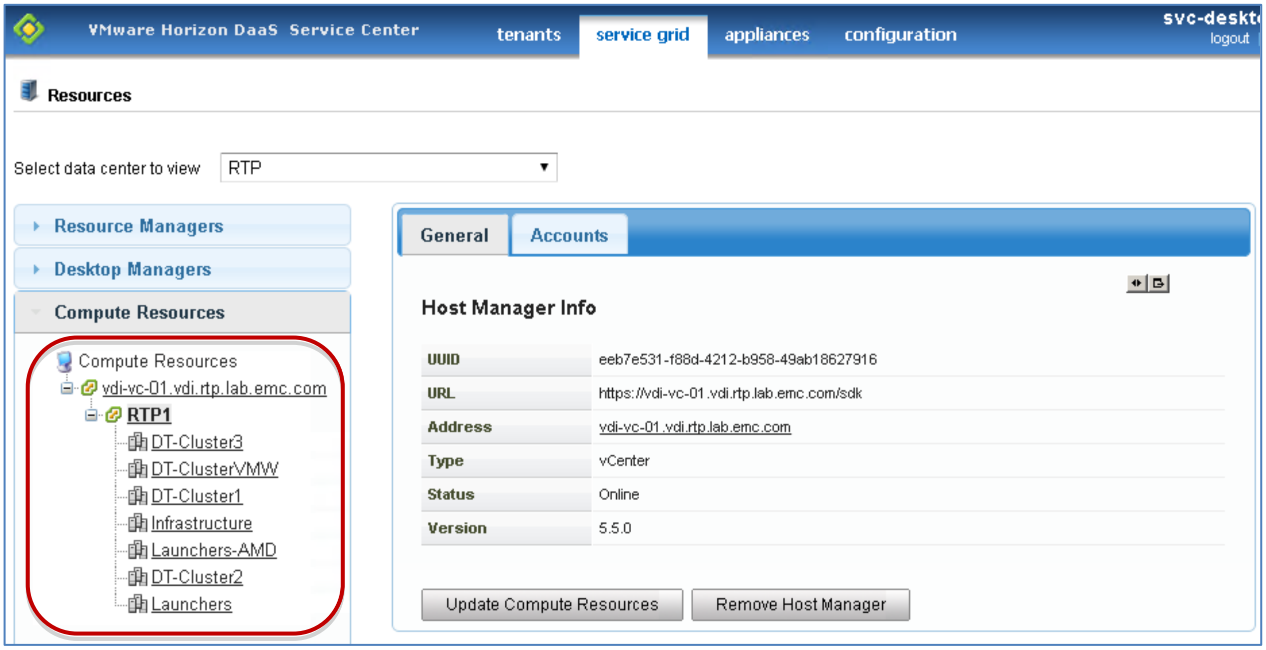
Friendly Name	Name		Service Provider	Tenant	RMgr	Desktop Mgr	Primary	Organization Primary	Data Center	Tenant	State	Version	
RTP-Desktone2	RTP-Desktone2	⇧	✓	-	✓	-	-	-	RTP	Service Provider	Installed	6.1.0	Actions
RTP-RSMGR-1	RTP-RSMGR-1	⇧	-	-	✓	-	✓	-	RTP	Service Provider	Installed	6.1.0	Actions
VMW-Desktone2	VMW-Desktone2	⇧	-	✓	-	✓	-	-	RTP	Tenant_VMware	Installed	6.1.0	Actions
VMW-Desktone1	VMW-Desktone1	⇧	-	✓	-	✓	✓	✓	RTP	Tenant_VMware	Installed	6.1.0	Actions
RTP-RSMGR-2	RTP-RSMGR-2	⇧	-	-	✓	-	-	-	RTP	Service Provider	Installed	6.1.0	Actions
RTP-Desktone1	RTP-Desktone1	⇧	✓	-	✓	-	✓	✓	RTP	Service Provider	Installed	6.1.0	Actions

VMware® Horizon DaaS™ Platform | © 2007-2014 VMware, Inc. All rights reserved | Version | Legal | Support

Figure 15. Horizon DaaS Service Center: Appliances

2. The **service grid** > **Compute Resources** option lists each vCenter Server instance that is linked to the Horizon DaaS infrastructure, and the vSphere clusters that each instance contains, as shown in Figure 16.

   Verify that the list includes each vCenter Server instance required by your Horizon DaaS deployment and any vSphere clusters that have been created within each instance for tenant deployments. If a vCenter Server instance or one of the vSphere clusters is not listed, perform the appropriate troubleshooting to resolve the error.



Select data center to view: RTP

Host Manager Info

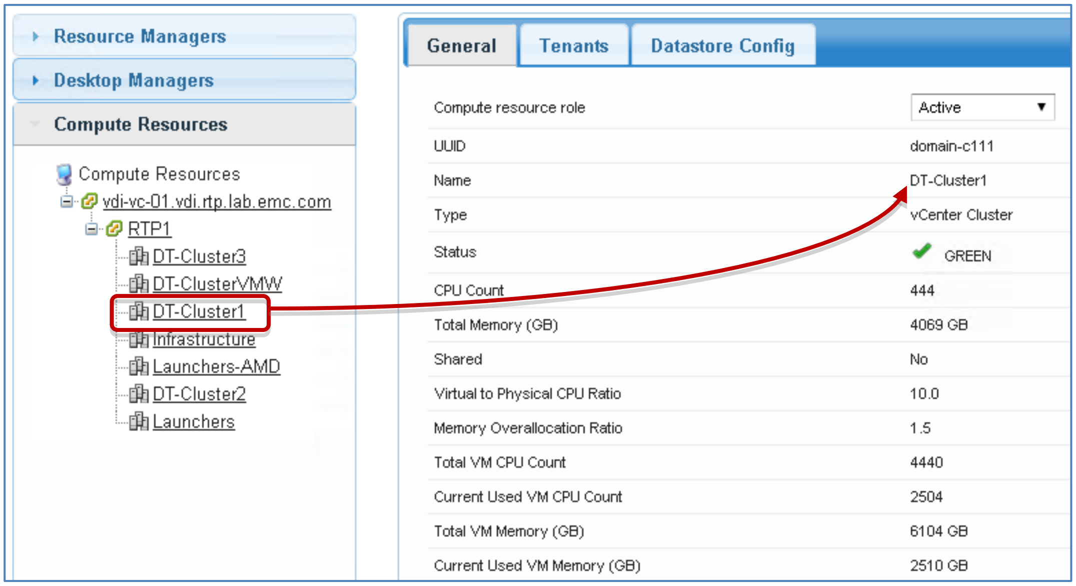
UUID	eeb7e531-f88d-4212-b958-49ab18627916
URL	https://vdi-vc-01.vdi.rtp.lab.emc.com/sdk
Address	vdi-vc-01.vdi.rtp.lab.emc.com
Type	vCenter
Status	Online
Version	5.5.0

Figure 16. Horizon DaaS Service Center: vCenter Server instances and vSphere clusters in Compute Resources

3. In the **Compute Resources** list that you opened in step 2, select one of the tenant vSphere clusters to view its attributes, as shown in Figure 17.

   Review the resources on the **General** tab and verify that they match those in the vCenter Server console for the selected cluster. Review the datastores on the **Datastore Config** tab and verify that they also match those shown in the vCenter Server console.

   If the cluster or datastore details in the Service Center do not match those in the vCenter Server console, perform the appropriate troubleshooting to resolve the error.



Compute resource role	Active
UUID	domain-c111
Name	DT-Cluster1
Type	vCenter Cluster
Status	✓ GREEN
CPU Count	444
Total Memory (GB)	4069 GB
Shared	No
Virtual to Physical CPU Ratio	10.0
Memory Overallocation Ratio	1.5
Total VM CPU Count	4440
Current Used VM CPU Count	2504
Total VM Memory (GB)	6104 GB
Current Used VM Memory (GB)	2510 GB

Figure 17. Horizon DaaS Service Center: Cluster details

Verifying vSphere configuration and functionality

Verifying that the following configuration tasks have been completed properly is critical to the functionality of the vSphere portion of this EMC DaaS solution and must be completed before deploying the solution into production.

On each vSphere host used as part of this solution, verify the following:

- For standard vSphere virtual switches, verify that they are configured with sufficient ports to support the maximum number of tenant virtual machines that each vSphere host can accommodate.
- Verify that all the required tenant virtual machine port groups (standard or DVPG) are configured based on the service provider and tenant requirements.
- Verify that each vSphere host has access to the required XtremIO volumes.
- Verify that the vSphere host VMkernel interfaces are configured correctly for vMotion and Storage vMotion. Refer to the VMware document *vSphere Networking* for details.

Refer to VMware vSphere Documentation for detailed information about how to verify these settings, and make any configuration changes that are needed.

Verifying the redundancy of the EMC storage services

To ensure that the various components of the solution maintain availability during maintenance or a hardware failure, perform the following verification tasks.

XtremIO array

Restart each XtremIO Storage Controller in turn and verify that connections to the vSphere datastores are maintained. Complete the following steps:

1. Log in to Storage Controller A using the **xinstall** account.
2. Restart the controller by selecting option **6** in the **Install** menu.
3. During the restart cycle, check for the presence of the vSphere datastores on the vSphere hosts.
4. With the XtremIO Storage Management Application, verify that Storage Controller A comes back online by monitoring the **Alerts** window or the **Hardware** workspace.
5. Repeat the procedure for Storage Controller B.

Isilon array

If an Isilon array is deployed as part of the solution, connect to any available node in the Isilon cluster with a serial cable or network drop. Then shut down each node in the cluster in turn and verify that access to the CIFS file systems is reestablished or maintained:

1. Determine the IP address of the node you are shutting down by using the **isi status –q** command.
2. From the node that you connected to, open a SSH connection to the node that is to be shut down by typing the **ssh** command.
3. Shut down the node by typing the **shutdown -p now** command.

4. Verify that the node is shut down by typing the **isi status -q** command.

   Confirm that the node has a status of **D--R** (Down, Read Only), as shown for node 3 in the following example:

```
ID |IP Address |DASR| In Out Total| Used / Size | Used / Size
---+---------------+----+-----+-----+-----+------------------+-
1|10.53.217.201 | OK | 48M| 0| 48M| 19G/ 6.2T(< 1%)|(No SSDs)
2|10.53.217.202 | OK | 46M| 0| 46M| 23G/ 6.2T(< 1%)|(No SSDs)
3|10.53.217.203 |D--R| n/a| n/a| n/a| n/a/ n/a( n/a)| n/a/n/a(
n/a)
```

5. While the node is down, verify that access to the CIFS file systems is reestablished or maintained.
6. Power on the node and repeat step 4 to verify that the node has returned to **OK** status.

VNX array

If a VNX array is deployed as part of the solution, perform the following verification tasks:

1. Restart each VNX storage processor (SP) in turn and verify that the connections to the CIFS file systems are maintained. Complete the following steps:
   a. Log in to the VNX Control Station with administrator privileges.
   b. Navigate to **/nas/sbin**.
   c. Restart SPA with the **./navicli -h spa rebootsp** command.
   d. During the restart cycle, verify that connections to the CIFS file systems are reestablished or maintained.
   e. When the cycle completes, restart SPB with the **./navicli -h spb rebootsp** command.
2. Perform a failover of each VNX Data Mover in turn and verify that the connections to the CIFS file systems are reestablished. For each Data Mover, type `server_cpu` *`movername`* `-reboot` at the Control Station $ prompt, where *movername* is the name of the Data Mover.

Network switching

To verify that network redundancy features function as expected, disable each of the redundant switching infrastructures in turn. While each of the switching infrastructures is disabled, verify that all the components of the solution maintain connectivity to each other and to any existing client infrastructure.

Virtual machine migration

On a vSphere host that contains at least one virtual machine, enable maintenance mode and verify that the virtual machine can migrate to an alternate host.

Chapter 4 Adding XtremIO Capacity to the Horizon DaaS Infrastructure

This chapter presents the following topics:

Overview

This chapter discusses the options for adding XtremIO storage capacity to an existing Horizon DaaS infrastructure, and describes how to make the expanded capacity available to existing Horizon DaaS tenants.

The chapter describes the following options to expand XtremIO capacity:

- Deploying an additional stand-alone XtremIO X-Brick
- Expanding an existing XtremIO cluster by adding an X-Brick
- Expanding an XtremIO Starter X-Brick by adding SSDs

Deploying additional XtremIO X-Bricks

Options

Consider the following options when deploying an additional X-Brick to an existing Horizon DaaS infrastructure:

- Add a stand-alone X-Brick to the infrastructure
- Add an X-Brick to an existing XtremIO cluster in the infrastructure

The solution performs identically with whichever option you choose for adding XtremIO storage capacity to the infrastructure.

Stand-alone X-Bricks

Adding a stand-alone X-Brick is the more flexible option and the optimal choice for this EMC DaaS solution. The benefits of this option include:

- Stand-alone X-Bricks offer the maximum choice for deploying additional XtremIO storage, because you cannot add a Starter X-Brick to an existing XtremIO cluster. With the stand-alone option, you have a choice of two flash drive configurations:
  - A Starter X-Brick with 13 drives
  - A standard X-Brick with up to of 25 drives
- With XIOS version 3.0, you must reinitialize the XtremIO array if you later remove an X-Brick that was added to an existing XtremIO cluster; this process is destructive. By deploying stand-alone X-Bricks, you retain the maximum flexibility for how you use the storage that each X-Brick provides, including the flexibility to relocate X-Bricks to alternate data centers.
- Multiple stand-alone X-Bricks deliver the same total performance capabilities as a single XtremIO cluster with multiple X-Bricks.

XtremIO cluster with multiple X-Bricks

In some cases, an XtremIO cluster with multiple X-Bricks might be the optimal choice—for example, if a single tenant has storage I/O or capacity requirements that necessitate an XtremIO cluster with multiple X-Bricks. In addition, an XtremIO cluster with multiple X-Bricks requires only one instance of the XtremIO Storage Management Application; this single instance sends consolidated alerts for all X-Bricks in the cluster. Multiple XtremIO clusters, however, require a separate management console for each cluster.

Adding a stand-alone X-Brick

Introducing a new stand-alone X-Brick into the Horizon DaaS infrastructure creates a new XtremIO cluster. After EMC or EMC partner engineers have completed setting up and configuring the stand-alone X-Brick, follow the procedure in Configuring the EMC XtremIO array in Chapter 3 to complete the cluster configuration. That is, perform the following tasks for the new cluster:

- Configure custom XtremIO event handers for the cluster to ensure that alerts are sent to the appropriate monitoring facilities or individuals.
- Provision additional XtremIO volumes for the vSphere tenant desktop hosts.

If the EMC VSI plugin, the EMC Storage Analytics solution, or both are used in the environment, you must also add the new XtremIO cluster to those applications, as described in the following documents:

- *EMC VSI for VMware vSphere Web Client Product Guide*
- *EMC Storage Analytics 3.0 Installation and User Guide*

Adding an X-Brick to an existing XtremIO cluster

EMC or EMC partner engineers are responsible for adding a new X-Brick to an existing XtremIO cluster during installation of the X-Brick. After the XtremIO cluster expansion is complete, follow the procedure in Provisioning XtremIO storage for vSphere datastores in Chapter 3 to provision additional XtremIO volumes for use by tenant desktop hosts.

Expanding an XtremIO Starter X-Brick

A service provider that has purchased a Starter X-Brick has the option of expanding it when needed. The expansion process is nondisruptive—that is, it does not affect the performance of any tenant desktops that are currently hosted on the array.

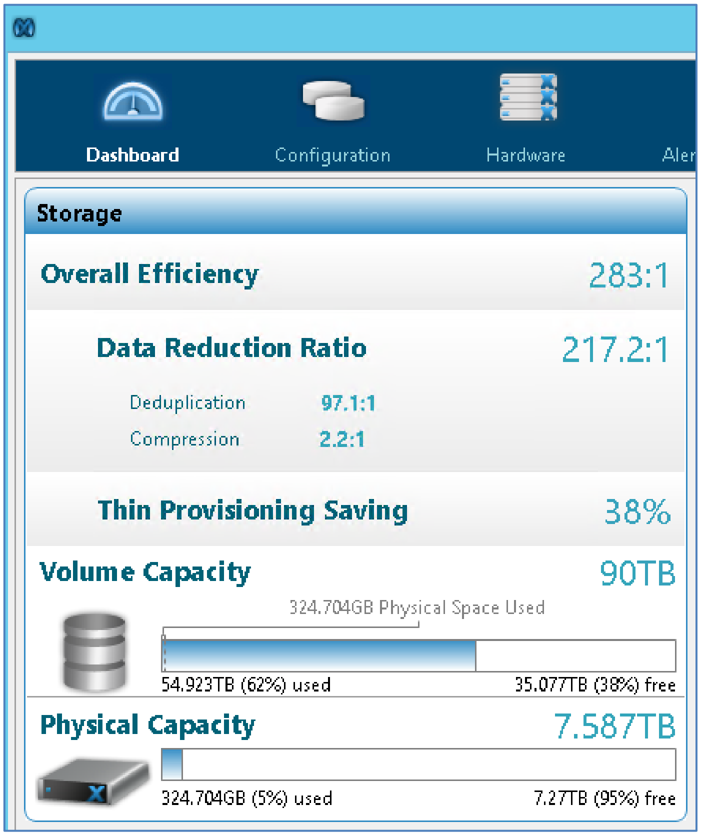
The expansion process includes installing the additional SSDs into the existing Starter X-Brick and must be carried out by EMC or EMC partner engineers.

Verifying the expansion

After the EMC or EMC partner engineer confirms that the expansion process is complete, you can verify the expansion in the XtremIO Storage Management Application, as follows:

- The **Storage** pane in the **Dashboard** workspace displays the new capacity values, as shown in Figure 18.
- The **X-Brick** pane in the **Hardware** workspace shows that all 25 SSDs are populated and are members of the XtremIO cluster, as shown by the highlighted portion of Figure 19.

At this stage, the XtremIO array is ready for you to provision additional volumes for use by tenant vSphere desktop hosts.



Storage

Overall Efficiency 283:1

Data Reduction Ratio 217.2:1

Deduplication 97.1:1

Compression 2.2:1

Thin Provisioning Saving 38%

Volume Capacity 90TB

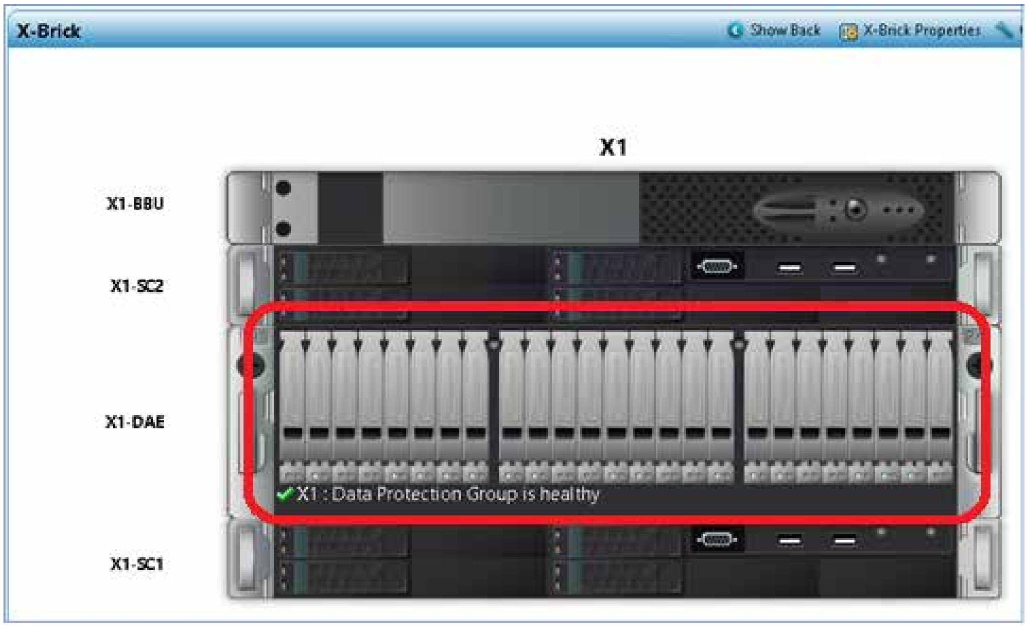
324.704GB Physical Space Used

54.923TB (62%) used 35.077TB (38%) free

Physical Capacity 7.587TB

324.704GB (5%) used 7.27TB (95%) free

Figure 18. XtremIO Storage Management: Storage pane in Dashboard workspace



✓X1 : Data Protection Group is healthy

Figure 19. XtremIO Storage Management: X-Brick pane in Hardware workspace

Adding new XtremIO storage capacity to existing Horizon DaaS tenants

After an expanded or newly provisioned XtremIO X-Brick is added to the environment, and volumes have been configured on the new XtremIO storage, you can proceed to add the new storage to existing tenants in the environment, as described in this section.

Adding the new storage to an existing cluster

Refer to the relevant sections in Chapter 3 for details of the procedures for adding the newly provisioned XtremIO volumes to the existing vSphere hosts. The high-level steps are as follows:

1. Connect the vSphere datastores to the appropriate vSphere hosts, as described in Connecting the vSphere datastores.
2. Optimize the vSphere hosts for XtremIO, as described in Optimizing the vSphere hosts for XtremIO.

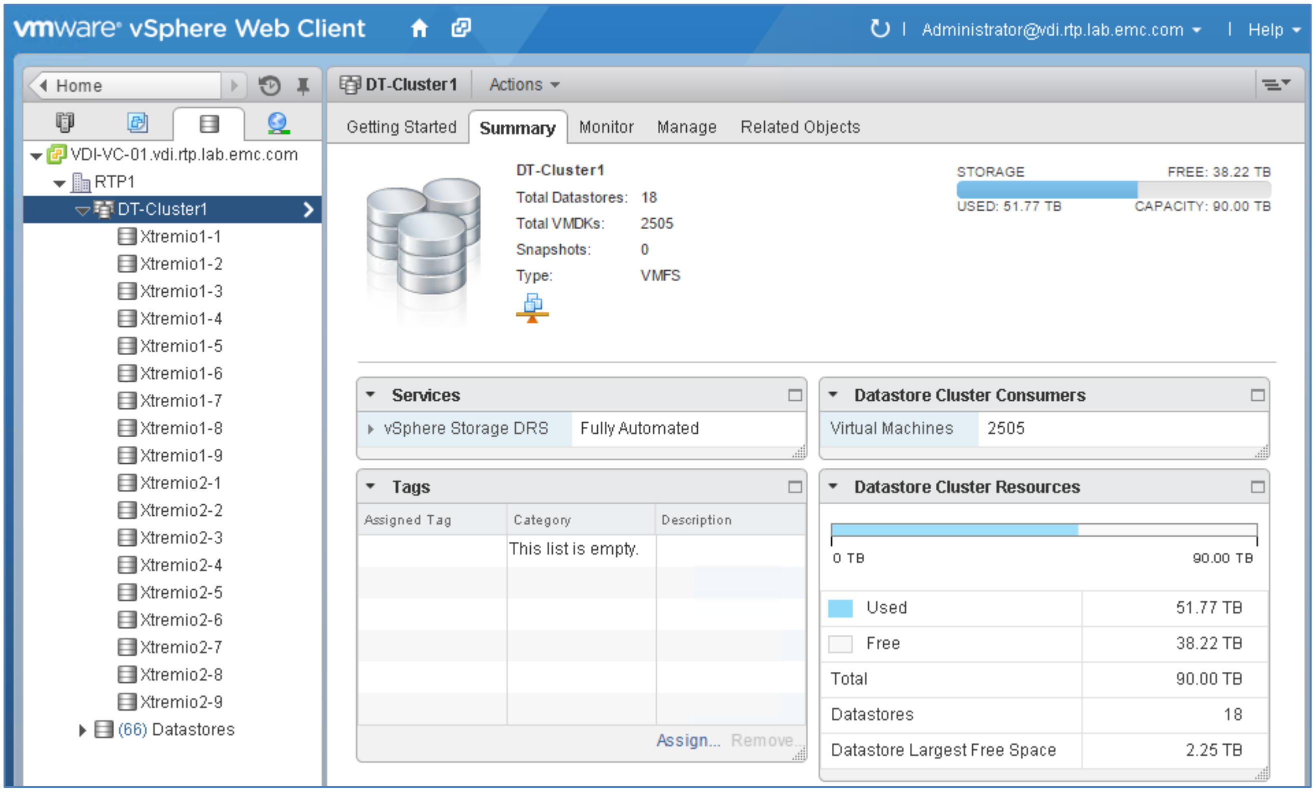
   If scripts were used to perform the initial vSphere host optimization, then the **Disk.SchedNumReqOutstanding** script (the second script) is the only script you need to run to perform the necessary optimizations.

   If the EMC VSI plug-in is used to perform the optimization tasks, you must reboot the vSphere hosts to complete the process.
3. Add the new vSphere datastores to the existing datastore cluster by dragging them into the cluster on the vSphere Web Client **Storage** page. Do not create a second datastore cluster.

   Refer to the VMware document *vSphere Resource Management* for instructions on how to add datastores to existing vSphere datastore clusters.

After the new datastores have been formatted and added to the vSphere datastore cluster, vSphere Storage DRS automatically rebalances the desktops the next time a scheduled rebalance operation occurs. You can also start the task manually to perform an immediate rebalance, as described in Enabling and configuring vSphere Storage DRS.

Figure 20 shows a vSphere datastore cluster that was expanded using the procedures outlined in this chapter. In this example, Storage DRS has already completed the rebalance operation and has redistributed the desktops across the nine new vSphere datastores.



DT-Cluster1

Total Datastores:	18
Total VMDKs:	2505
Snapshots:	0
Type:	VMFS

STORAGE FREE: 38.22 TB
USED: 51.77 TB CAPACITY: 90.00 TB

Services

vSphere Storage DRS	Fully Automated

Datastore Cluster Consumers

Virtual Machines	2505

Tags

Assigned Tag	Category	Description
	This list is empty.	

Datastore Cluster Resources

0 TB 90.00 TB

🟦 Used	51.77 TB
□ Free	38.22 TB
Total	90.00 TB
Datastores	18
Datastore Largest Free Space	2.25 TB

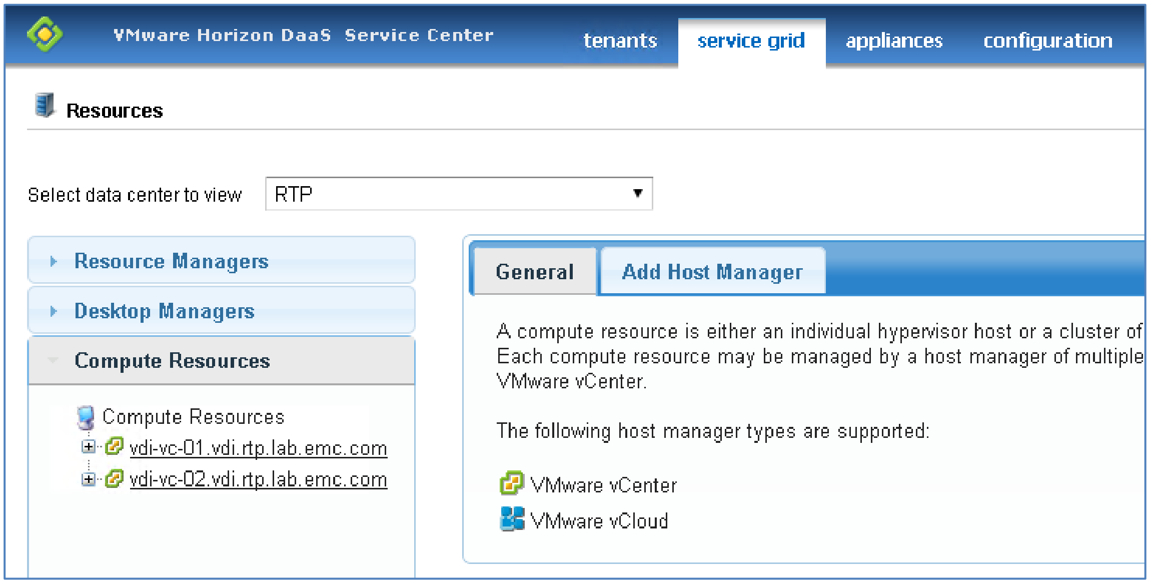
Figure 20. vSphere Web Client: Datastore Cluster Summary

Manually refreshing the Horizon DaaS compute resources

vSphere Storage DRS operates independently of Horizon DaaS. Thus, Storage DRS can perform the rebalance operation even if Horizon DaaS has not yet detected that more storage is available.

To ensure that Horizon DaaS is immediately aware of new storage presented to the tenant vSphere clusters, manually refresh the compute resources as follows:

1. Log in to the CSP Horizon DaaS Service Center and select **service grid** > **Compute Resources**, as shown in Figure 21.



Select data center to view: RTP

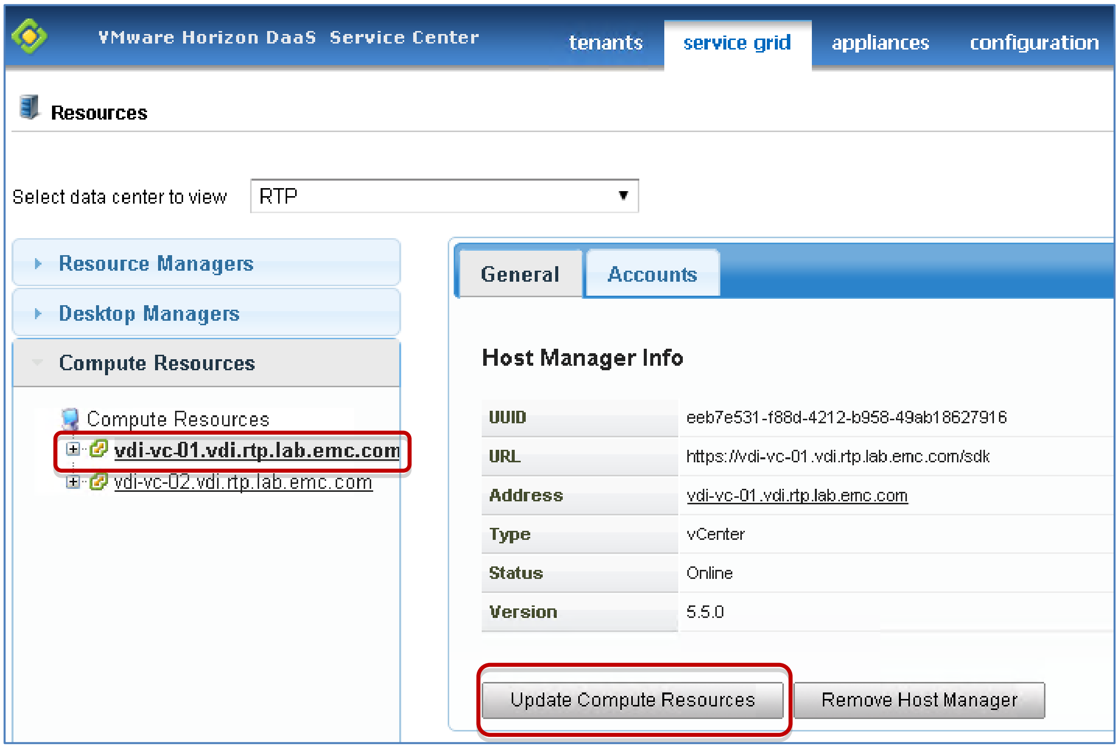
A compute resource is either an individual hypervisor host or a cluster of
Each compute resource may be managed by a host manager of multiple
VMware vCenter.

The following host manager types are supported:

- VMware vCenter
- VMware vCloud

Figure 21. Horizon DaaS Service Center: vCenter Server instances in Compute Resources

2. Select the vCenter Server instance that manages the vSphere cluster to which you added the new datastores, and then click **Update Compute Resources** to refresh the resource information, as shown in Figure 22.



Select data center to view: RTP

Host Manager Info

UUID	eeb7e531-f88d-4212-b958-49ab18627916
URL	https://vdi-vc-01.vdi.rtp.lab.emc.com/sdk
Address	vdi-vc-01.vdi.rtp.lab.emc.com
Type	vCenter
Status	Online
Version	5.5.0

Figure 22. Horizon DaaS Service Center: Host Manager Info

3. Repeat step 2 for any datastores added to vSphere clusters managed by other vCenter Server instances.

Chapter 5 Migrating Existing Horizon DaaS storage to EMC XtremIO

This chapter presents the following topics:

Overview

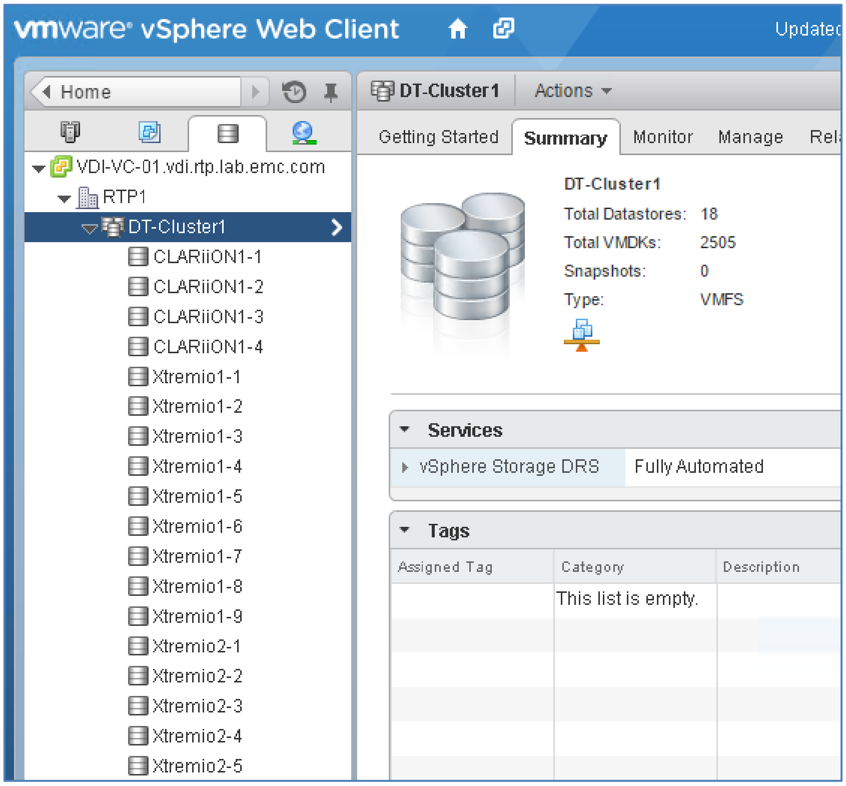
VMware vSphere Storage DRS enables service providers to automate the migration of tenant virtual desktops to new datastores, including virtual desktops that are located on different storage arrays. This chapter describes how to use Storage DRS to migrate tenant desktops from existing storage to newly provisioned XtremIO datastores.

Prerequisites

The datastore migration procedure outlined in this chapter presumes that the new XtremIO datastores have already been added to the vSphere datastore cluster, as described in Adding the new storage to an existing cluster in Chapter 4.

It is not necessary to manually run the vSphere Storage DRS rebalancing process after adding the new datastores. The migration procedure evacuates and removes the datastores that you no longer plan to use, and redistributes the virtual desktops across the new datastores.

Figure 23 shows the example datastore cluster before datastore migration. The cluster contains both the legacy datastores that you are taking out of use (identified by the CLARiiON® prefix) and the new XtremIO datastores (identified by the XtremIO prefix).



- VDI-VC-01.vdi.rtp.lab.emc.com
  - RTP1
    - DT-Cluster1
      - CLARiiON1-1
      - CLARiiON1-2
      - CLARiiON1-3
      - CLARiiON1-4
      - Xtremio1-1
      - Xtremio1-2
      - Xtremio1-3
      - Xtremio1-4
      - Xtremio1-5
      - Xtremio1-6
      - Xtremio1-7
      - Xtremio1-8
      - Xtremio1-9
      - Xtremio2-1
      - Xtremio2-2
      - Xtremio2-3
      - Xtremio2-4
      - Xtremio2-5

DT-Cluster1

Total Datastores:	18
Total VMDKs:	2505
Snapshots:	0
Type:	VMFS

vSphere Storage DRS	Fully Automated

Assigned Tag	Category	Description
	This list is empty.	

Figure 23. vSphere Web Client: Datastore cluster before datastore migration

Using vSphere Storage DRS to migrate desktops to new XtremIO datastores

To migrate tenant virtual desktops to new vSphere datastores hosted by an XtremIO array, perform the following steps in the vSphere Web Client:

1. Navigate to the datastore cluster view, as shown in Figure 24.

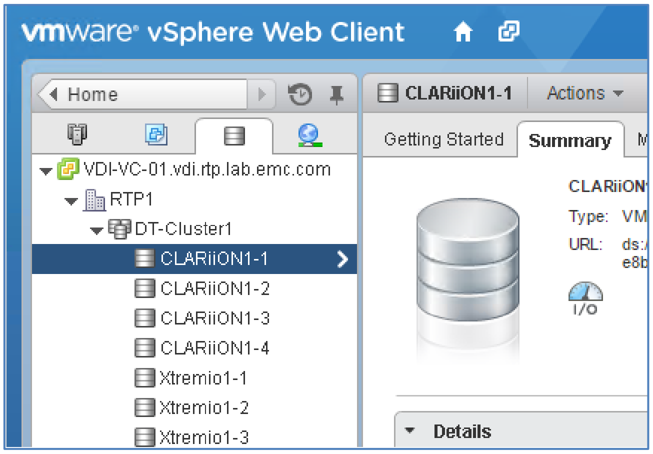


Figure 24. vSphere Web Client: Datastore cluster view

2. Place in maintenance mode the first datastore from which you want to migrate the tenant desktops, as shown in Figure 25:

   a. Right-click the datastore.

   b. Select **All vCenter Actions** > **Enter Maintenance Mode**.

   c. Confirm that the datastore is in maintenance mode. The datastore icon updates to indicate this, as shown in Figure 25.

      After the datastore has successfully been placed in maintenance mode, vCenter Server uses Storage vMotion to migrate all desktops on the datastore to other datastores in the datastore cluster.

3. Repeat step 2 for each of the remaining datastores whose tenant desktops you want to migrate to the new XtremIO datastores.

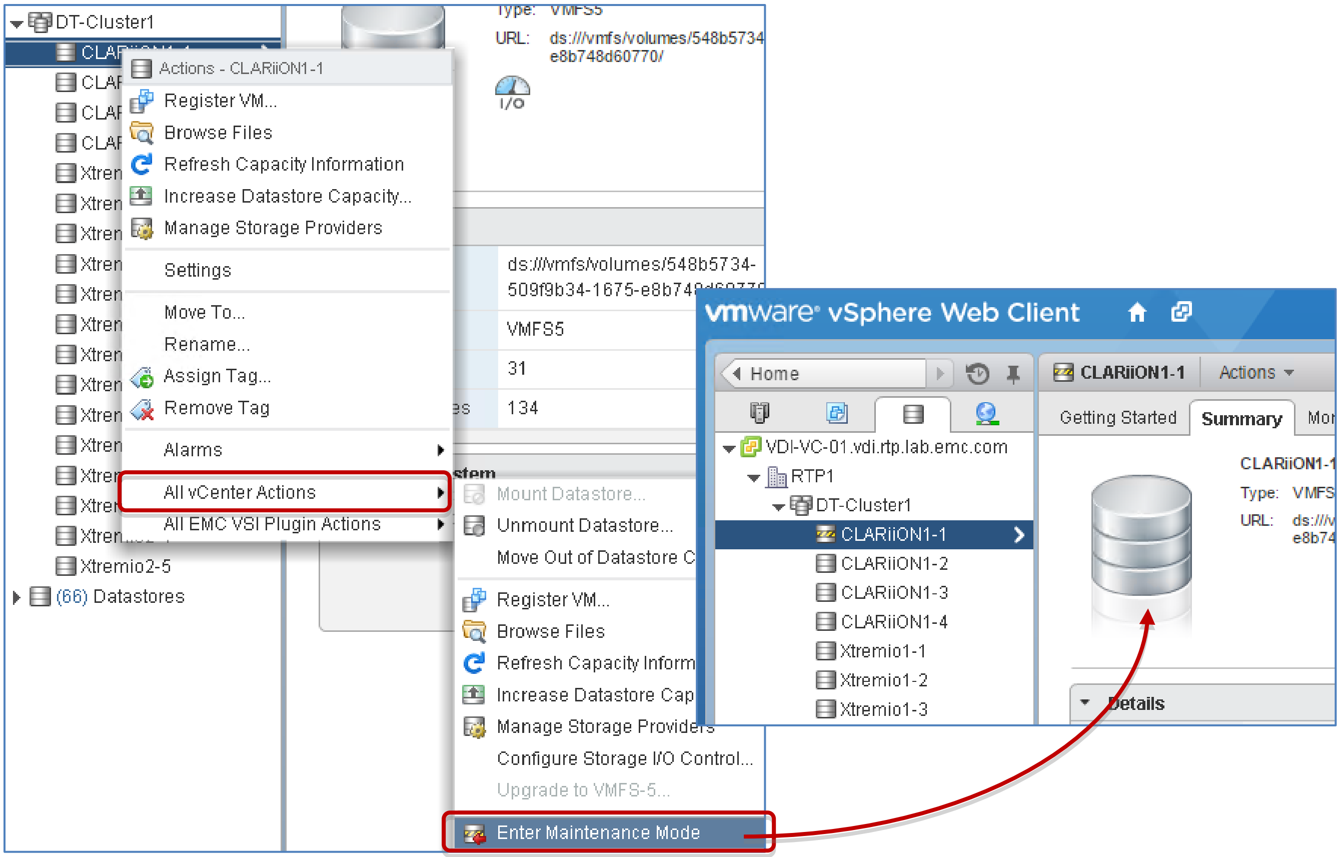


Figure 25. vSphere Web Client: Enter Maintenance Mode

4. Prepare each of the legacy datastores for deletion by right-clicking it and selecting **All vCenter Actions** > **Move Out of Datastore Cluster**.

5. If the datastores you removed in step 4 were NFS-based, unmount each one by right-clicking it and selecting **All vCenter Actions** > **Unmount Datastore**.

6. In the administrative console for the storage array that hosts the removed datastores, delete the underlying LUNs or file systems for those datastores.

7. In the vSphere Web Client, rescan the storage for the datastore cluster:

   a. Right-click the cluster.

   b. Select **All vCenter Actions** > **Rescan Storage**.

   c. In the **Rescan Storage** dialog box, click **OK**.

At this point, the Horizon DaaS tenant desktops have been successfully migrated to new datastores hosted on the XtremIO array.

Chapter 6 Setting Up Monitoring for EMC Storage Services

This chapter presents the following topics:

Overview

The XtremIO Storage Management Application provides a dashboard view of current storage efficiency, utilization, performance, and alerts. The alert system has a pre-defined set of cluster-related alerts, and provides options for viewing, editing, and acknowledging alerts. In addition, service providers can configure XtremIO event handlers to forward alerts to specified email recipients, and to event logging mechanisms such as SNMP and syslog, when particular event types occur, as outlined in Configuring custom XtremIO event handlers in Chapter 3.

EMC Storage Analytics (ESA) offers advanced monitoring and analysis of XtremIO array performance and utilization. The product provides deep visibility, metrics, and a rich collection of storage analytics for EMC storage systems. With ESA, storage provider administrators can get detailed metrics through customizable dashboards, widgets, heat maps, and alerts, while also accessing topology mappings of the entire storage infrastructure, from virtual machine to LUN and every point in between.

This chapter provides a high-level overview of how to deploy and use ESA, including:

- The infrastructure resources required to deploy ESA
- A high-level overview of the ESA deployment process
- An introduction to the default XtremIO dashboards included with ESA

While this chapter focuses on using ESA to monitor XtremIO, ESA supports other EMC platforms, including VNX.

EMC Storage Analytics requirements

EMC Storage Analytics is powered by the VMware vRealize Operations analytics engine and presents its customized dashboards, alerts, reports, and other content through the VMware vRealize Operations Manager interface. ESA links vRealize Operations Manager to EMC storage arrays by using the EMC Adapter, with individual adapter instances providing access to different array types.

VMware Realize Operations is deployed as a virtual application (vApp). The VMware document *vRealize Operations Manager vApp Deployment and Configuration Guide* provides detailed information about the system requirements and the available configuration options. Because ESA monitors EMC storage systems and virtual machines only, and not the entire vSphere infrastructure, the default configuration (Small) is sufficient in most cases.

The Small configuration requires the following resources:

- 4 vCPUs
- 16 GB of RAM
- 282 GB of storage

  ESA typically requires less than 20 GB of storage when deployed using thin provisioned virtual disks. However, deploy the full amount of storage capacity to accommodate increased utilization over time.

Refer to the VMware Knowledge Base article *vRealize Operations Manager Sizing Guidelines* (2093783), or the product documentation, for additional information about the available configuration options.

EMC Storage Analytics deployment overview

The *EMC Storage Analytics Installation and User Guide* outlines the process for deploying ESA. The guide cross-references the *vRealize Operations Manager vApp Deployment and Configuration Guide* for instructions on installing the vRealize Operations Manager vApp. These guides describe the following high-level deployment tasks:

1. Deploy and configure the vRealize Operations Manager vApp.
2. Import the EMC Adapter for ESA and vRealize Operations Manager by using the vRealize Operations Manager console.
3. Add an EMC Adapter instance for vCenter Server. This adapter instance enables services to view and traverse vRealize Operations Manager health trees from the vSphere components through to the EMC storage environment.
4. Add an EMC Adapter instance for the XtremIO array.

   If the Horizon DaaS infrastructure includes multiple EMC arrays, repeat this step for each array. An ESA license is required for each EMC array that ESA monitors.

When these steps are finished, ESA starts to collect data from the storage arrays.

Introducing the default EMC Storage Analytics XtremIO dashboards

ESA contains a number of default dashboards that are designed to provide rapid access to key EMC storage service metrics through the vRealize Operations Manager interface. This section provides an overview of these dashboards and their purpose. Refer to the *EMC Storage Analytics Installation and User Guide* for additional information.

Note: You can view details of every object in every widget in a dashboard by selecting the object and clicking the **Object Detail** icon at the top of the widget.

Storage Topology dashboard

The Storage Topology dashboard provides an entry point for viewing resources and the relationships between storage and virtual infrastructure objects.

The Storage Topology dashboard contains the following widgets:

- **Storage System Selector**—This Resource widget lists all configured EMC Adapter instances. To populate the Storage Topology and Health widget, select an instance name.

- **Storage Topology and Health**—This Health Tree widget provides a navigable visualization of storage and virtual infrastructure resources. To populate the Parent Resources and Child Resources widgets, select a resource in this widget.
- **Parent resources**—This widget lists the parent resources of the resource selected in the Storage Topology and Health widget.
- **Child resources**—This widget lists the child resources of the resource selected in the Storage Topology and Health widget.

Storage Metrics dashboard

The Storage Metrics dashboard displays resources and metrics for storage systems, including graphs of the resource metrics.

The Storage Metrics dashboard contains the following widgets:

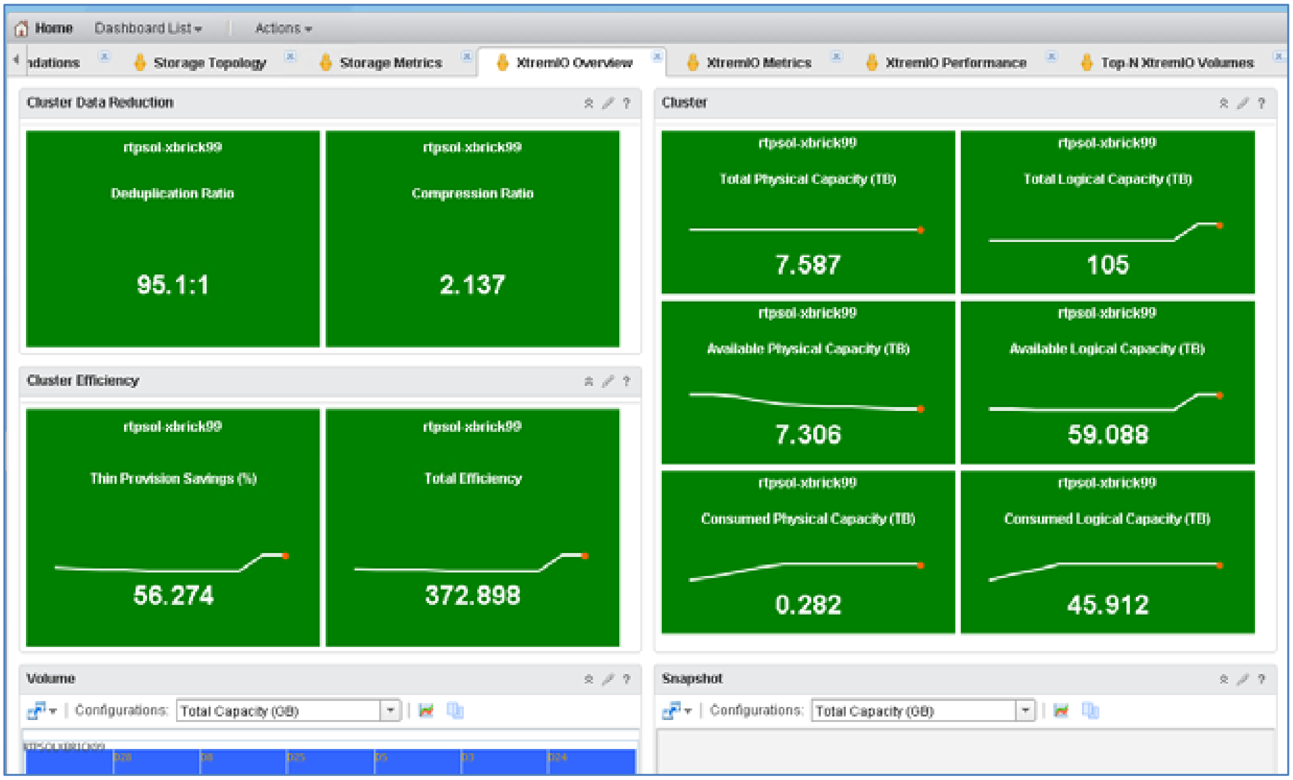
- **Storage System Selector**—This Resource widget lists all configured EMC Adapter instances. To populate the Resource Selector widget, select an instance name.
- **Resource Selector**—This Health Tree widget lists each resource associated with the adapter instance selected in the Storage System Selector widget. To populate the Metric Picker widget, select a resource.
- **Metric Picker**—This widget lists all the metrics that are collected for the resource selected in the Resource Selector widget. The search feature of this widget enables users to locate specific objects. Double-click a metric to create a graph of the metric in the Metric Graph widget.
- **Metric Graph**—This widget graphs the metrics selected in the Metric Picker widget. You can display multiple metrics simultaneously in a single graph or in multiple graphs.

XtremIO Overview dashboard

The XtremIO Overview dashboard displays a collection of scorecard widgets that provide an overview of the health of the XtremIO system, as shown in Figure 26.

The XtremIO Overview dashboard displays two types of heat maps:

- Metrics with definitive measurements are assigned color ranges from lowest (green) to highest (red).
- Metrics with varied values that cannot be assigned a range show relative values from lowest (light blue) to highest (dark blue).



Configurations: Total Capacity (GB)

Configurations: Total Capacity (GB)

Figure 26. EMC Storage Analytics: XtremIO Overview dashboard

The XtremIO Overview dashboard contains the following widgets:

- **Cluster Data Reduction**—Displays the Data Deduplication Ratio and Compression Ratio of each cluster.
- **Cluster Efficiency**—Displays the Thin Provisioning Savings (%) and the Total Efficiency of each cluster.
- **Volume**—Displays volumes as either Total Capacity or Consumed Capacity. Select a volume to display its sparkline charts.
- **Cluster**—For each cluster, displays the Total Physical and Logical Capacity, the Available Physical and Logical Capacity, and the Consumed Physical and Logical Capacity.
- **Snapshot**—Displays snapshots as either Total Capacity or Consumed Capacity. Select a snapshot to display its sparkline charts.

XtremIO Metrics dashboard

The XtremIO metrics dashboard displays resources and metrics for the XtremIO array, including graphs of the resource metrics.

The XtremIO Metrics dashboard contains the following widgets:

- **Resource Tree/Environment Overview**—Displays the end-to-end topology and health of resources across the vSphere and storage domains. You can configure the hierarchy that is displayed by changing the widget settings. Changing these settings does not alter the underlying object relationships in the database. Select any resource in this widget to view related resources in the stack.

- **Metric Selector/Metric Picker**—Lists all the metrics that are collected for the resource selected in the Resource Tree/Environment Overview widget. Double-click a metric to create a graph of the metric in the Metric Graph/Metric Chart widget.
- **Metric Graph/Metric Chart**—Graphs the metrics selected in the Metric Selector/Metric Picker widget. You can display multiple metrics simultaneously in a single graph or in multiple graphs.

XtremIO Performance dashboard

The XtremIO Performance dashboard displays the percent utilization of the Storage Controller CPUs, and key volume and SSD metrics and sparkline charts.

The XtremIO Performance dashboard displays two types of heat maps:

- Metrics with definitive measurements such as CPU usage (0% to 100%) are assigned color ranges from lowest (green) to highest (red).
- Metrics with varied values that cannot be assigned a range show relative values from lowest (light blue) to highest (dark blue).

The XtremIO Performance dashboard contains the following widgets:

- **Storage Controllers CPU 1 Utilization (%)**—Shows the percent utilization of CPU 1.
- **Storage Controllers CPU 2 Utilization (%)**—Shows the percent utilization of CPU 2.
- **Volume**—Provides several modes, including Total Operations, Total Bandwidth, Total Latency, Unaligned (%), and Average Block Size. Select a volume in this widget to display its sparkline charts.
- **SSD**—Provides Endurance Remaining and Disk Utilization modes. Select an SSD in this widget to display its sparkline charts.

Top-N XtremIO Volumes dashboard

The Top-N XtremIO Volumes dashboard displays an at-a-glance view of the top performing volumes. ESA selects the top performers based on the current value of the metric that is configured for each widget. You can change the time period. You can also configure each widget to show more than the default number of top performers.

By default, the Top-N XtremIO Volumes dashboard shows the top 10 devices in the following categories:

- Top-10 by Read (IO/s)
- Top-10 by Write (IO/s)
- Top-10 by Read Latency (usec)
- Top-10 by Write (usec)
- Top-10 by Read Block Size (KB)
- Top-10 by Write Block Size (KB)
- Top-10 by Total Capacity (GB)

Chapter 7 Managing XtremIO Capacity Utilization

This chapter presents the following topics:

Overview

Monitoring and managing storage capacity utilization are fundamental tasks for service providers. While the deduplication and compression capabilities of the XtremIO array enable significant reductions in the SSD capacity required in a virtual desktop environment, service providers must closely monitor physical capacity utilization for many reasons, including:

- Over time, Horizon DaaS tenants typically have increased data storage requirements, and some data generated might not be suitable for deduplication and compression.
- As the service provider's DaaS environment grows, additional XtremIO capacity might be required, and a long-term monitoring and managing strategy is crucial to understanding this.
- vSphere does not automatically mark blocks as available after their contents are deleted. Thus, the XtremIO array may prematurely reach physical capacity thresholds unless the unused blocks are regularly released for reuse.

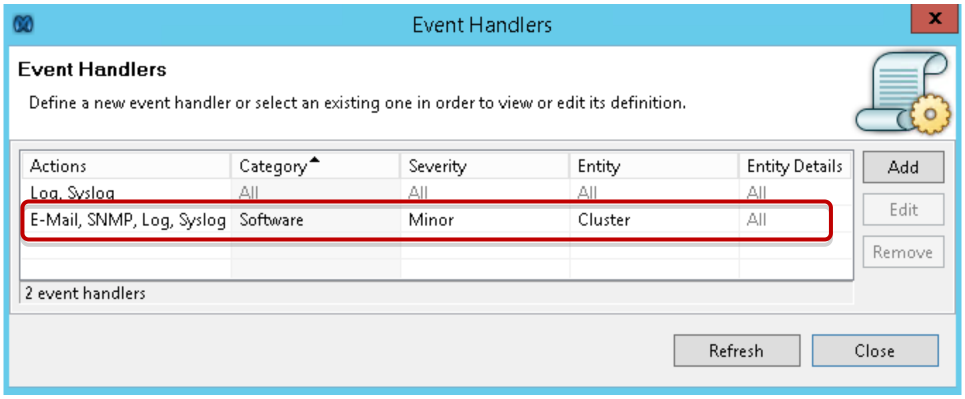
This chapter reviews the options available for monitoring XtremIO physical capacity utilization, describes how to recover unused space on the array, and presents a high-level strategy for managing capacity utilization and determining when additional XtremIO capacity might be required.

Monitoring XtremIO physical capacity utilization

Chapter 3: Deploying the Physical DaaS Infrastructure and Chapter 6: Setting Up Monitoring for EMC Storage Services outline how to use native XtremIO event handlers and the alerting functionality of the EMC Storage Analytics platform to monitor XtremIO array alerts, performance, and capacity. This section reviews these monitoring options in relation to physical capacity utilization.

Using XtremIO event handlers

XtremIO Software–Minor–Cluster events include events related to XtremIO cluster capacity, and should be actively monitored. Figure 27 shows details of an event handler that we created for these events. The event handler is configured to notify all possible event logging mechanisms, including email, SNMP, local XtremIO log files, and syslog.



Event Handlers

Event Handlers

Define a new event handler or select an existing one in order to view or edit its definition.

Actions	Category	Severity	Entity	Entity Details
Log, Syslog	All	All	All	All
E-Mail, SNMP, Log, Syslog	Software	Minor	Cluster	All

2 event handlers

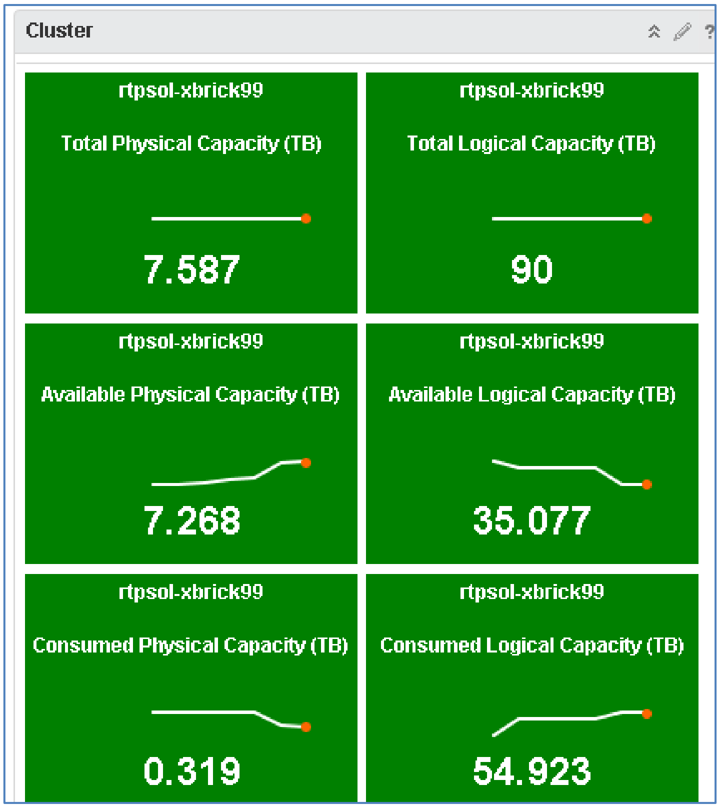
Figure 27. XtremIO Storage Management: Event Handlers

Using EMC Storage Analytics

The ESA platform enables long term monitoring of XtremIO physical capacity utilization and other statistics. If a service provider needs to automatically monitor and review XtremIO physical capacity utilization over time—to determine when additional storage might be required, for example—ESA could be the optimal choice.

ESA XtremIO Overview dashboard

The ESA XtremIO Overview dashboard includes a wide range of XtremIO cluster and volume capacity statistics. Figure 28 shows some of the Cluster widgets available in the dashboard. These widgets provide details about average XtremIO physical capacity utilization, consumed physical capacity, and total physical capacity. They also provide information about the logical capacity, which identifies how much space can be allocated to XtremIO volumes and presented to vSphere or other hosts.



Cluster

rtpsol-xbrick99
Total Physical Capacity (TB)
7.587

rtpsol-xbrick99
Total Logical Capacity (TB)
90

rtpsol-xbrick99
Available Physical Capacity (TB)
7.268

rtpsol-xbrick99
Available Logical Capacity (TB)
35.077

rtpsol-xbrick99
Consumed Physical Capacity (TB)
0.319

rtpsol-xbrick99
Consumed Logical Capacity (TB)
54.923

Figure 28. EMC Storage Analytics: XtremIO cluster widgets

ESA alerts

The ESA platform leverages vRealize Operations Management options for providing alerts. Figure 29 shows the various alert options, which include log files, emails, SNMP, and other options. Refer to the VMware document *vRealize Operations Manager vApp Deployment and Configuration Guide* for instructions about configuring and using these options.

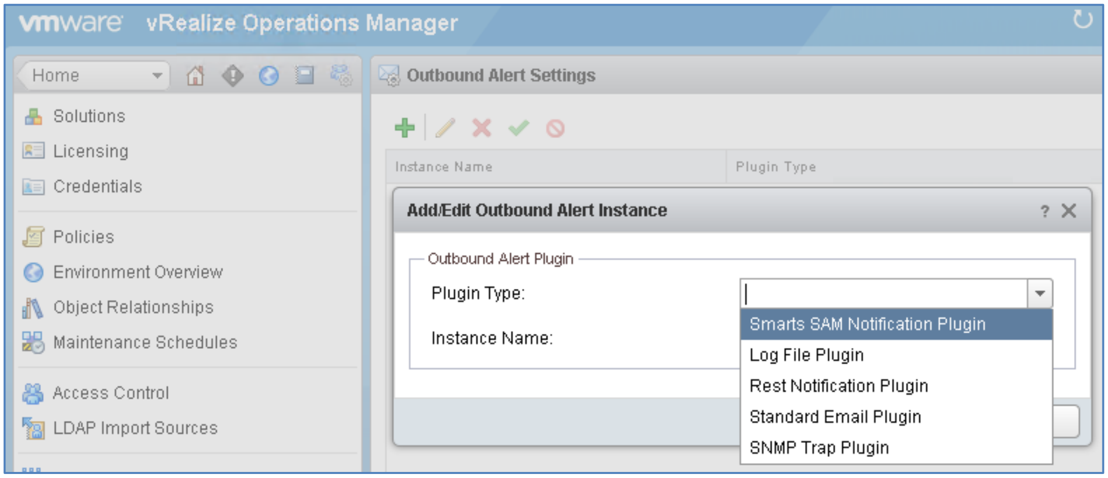


Figure 29. EMC Storage Analytics: Add/Edit Outbound Alert Instance

Reclaiming XtremIO physical capacity

vSphere does not automatically mark blocks as available after their contents are deleted. To return unused space to the XtremIO array for further use, you must perform a SCSI UNMAP operation for each vSphere datastore. The procedure works with any block-based storage array that is being used to provide storage for vSphere hosts.

You can perform a SCSI UNMAP operation with either of the following methods:

- Use a script to run the **esxcli storage vmfs unmap** command on any one of the vSphere hosts that is attached to the target datastore. The command is available in vSphere 5.5 and later, and is ideal for environments where it is preferable to automate the SCSI UNMAP process.
- Use the EMC VSI plug-in to quickly perform the operation in the vSphere Web Client. This method requires that the EMC VSI plug-in is installed and configured in the vSphere environment and is associated with the target XtremIO array.

Both methods produce the same result, so select whichever method fits best with your regular vSphere maintenance regime. Refer to the VMware Knowledge Base article *Using esxcli in vSphere 5.5 to reclaim VMFS deleted blocks on thin-provisioned LUNs (2057513)* for further information about the SCSI UNMAP operation.

SCSI UNMAP operation considerations

A SCSI UNMAP operation requires approximately 20 percent free space on the vSphere datastore. If the datastore does not have sufficient free space, it will fill to capacity during the SCSI UNMAP operation, and the vSphere hosts will typically stun one or more of the virtual machines on the datastore until space frees up.

SCSI UNMAP operations are I/O intensive. So perform these operations during periods when the XtremIO array is least used. This reduces the likelihood that tenants with desktops hosted on the array will notice degradation in performance. However, if the physical capacity of the array is low, perform the SCSI UNMAP operation immediately, without regard to the current I/O load.

Using a script to perform SCSI UNMAP operations

To reclaim unused storage blocks with the **esxcli** command, run the command from a vSphere host that is connected to the target datastore. You can run the command either within a SSH session to the vSphere host or through a VMware vSphere Management Assistant session that connects to the host.

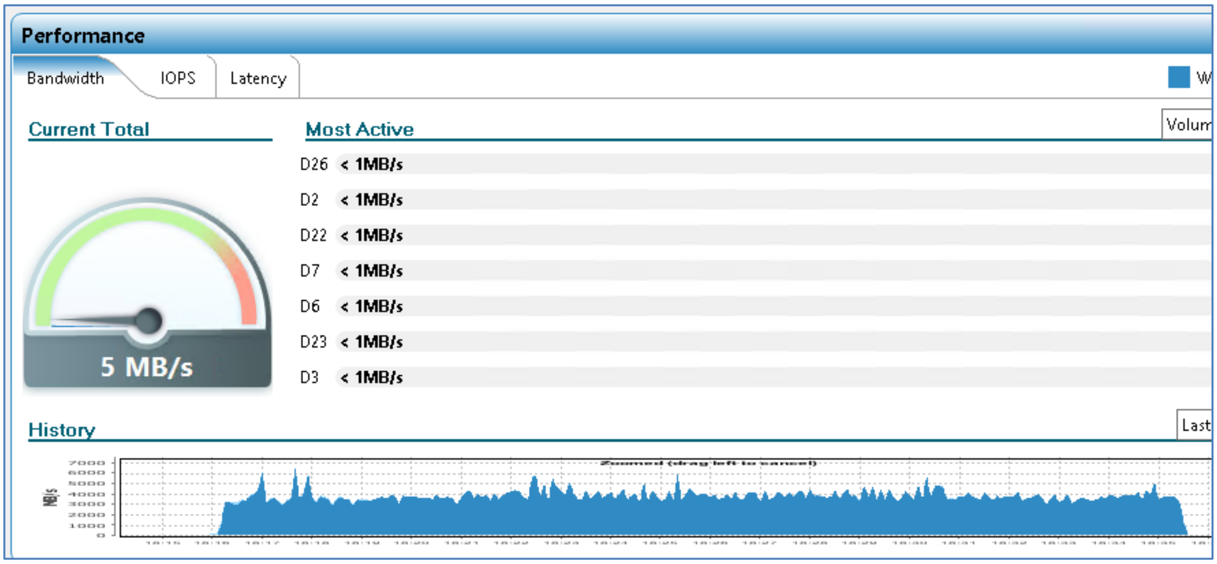
Use the following command syntax, where *vSphereDatastoreName* is the name of the datastore for which you want to perform the SCSI UNMAP operation:

```
esxcli storage vmfs unmap -l vSphereDatastoreName -n 20000
```

The command produces no output, and the **Recent Tasks** pane in the vSphere Web Client displays no status information for the command. However, you can view the bandwidth history in either the XtremIO Storage Management Application or the EMC Storage Analytics interface to verify that the operation is finished:

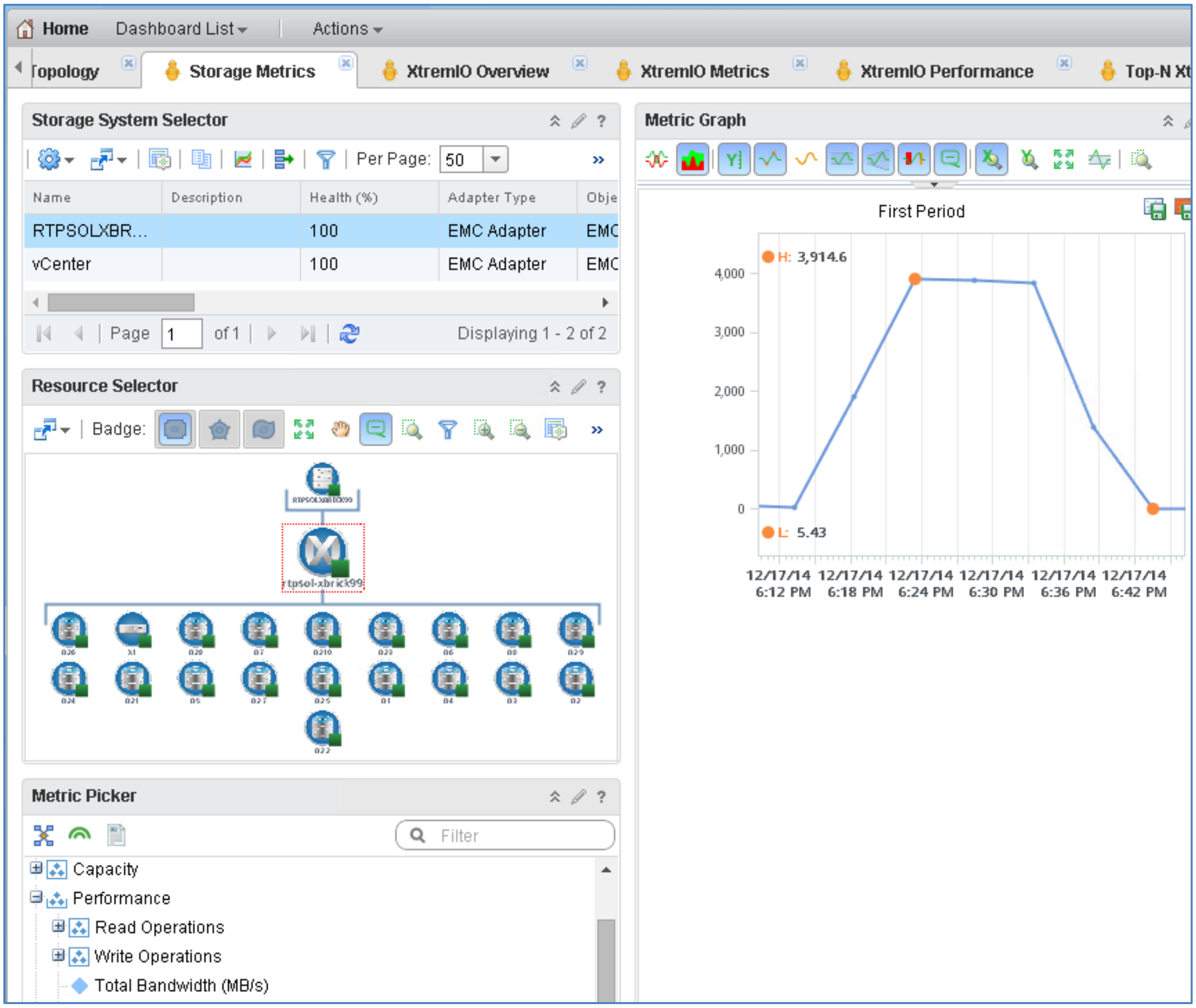
- In the XtremIO Storage Management Application, select **Dashboard** > **Performance** > **Bandwidth**.
- In the ESA interface, select **Storage Metrics** > **Metric Picker** > **Total Bandwidth**.

As shown in Figure 30 and Figure 31, you can easily identify the impact of the SCSI UNMAP operation by the significant increase in bandwidth while the command is running.



D26	< 1MB/s
D2	< 1MB/s
D22	< 1MB/s
D7	< 1MB/s
D6	< 1MB/s
D23	< 1MB/s
D3	< 1MB/s

Figure 30. XtremIO Storage Management: Performance Bandwidth graph



Per Page: 50

Name	Description	Health (%)	Adapter Type	Obje
RTPSOLXBR...		100	EMC Adapter	EMC
vCenter		100	EMC Adapter	EMC

Page 1 of 1

Displaying 1 - 2 of 2

Figure 31. EMC Storage Analytics: Storage Metrics Bandwidth graph

Using EMC VSI to perform SCSI UNMAP operations

If your solution uses the EMC VSI plug-in, you can quickly perform a SCSI UNMAP operation from the vSphere Web Client by completing the following steps:

1. On the vSphere Web Client **Home** page, click the **Storage** icon.
2. Right-click the target XtremIO datastore for the SCSI UNMAP operation, and select **All EMC VSI Plugin Actions** > **Reclaim Unused Storage**, as shown in Figure 32.

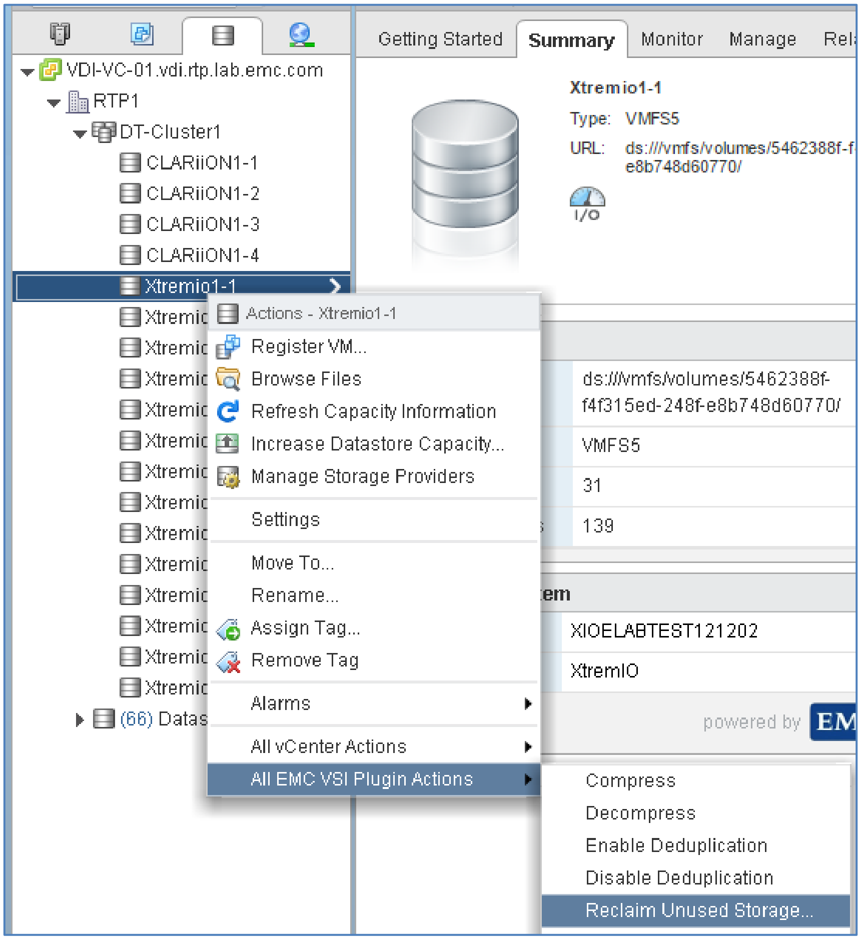
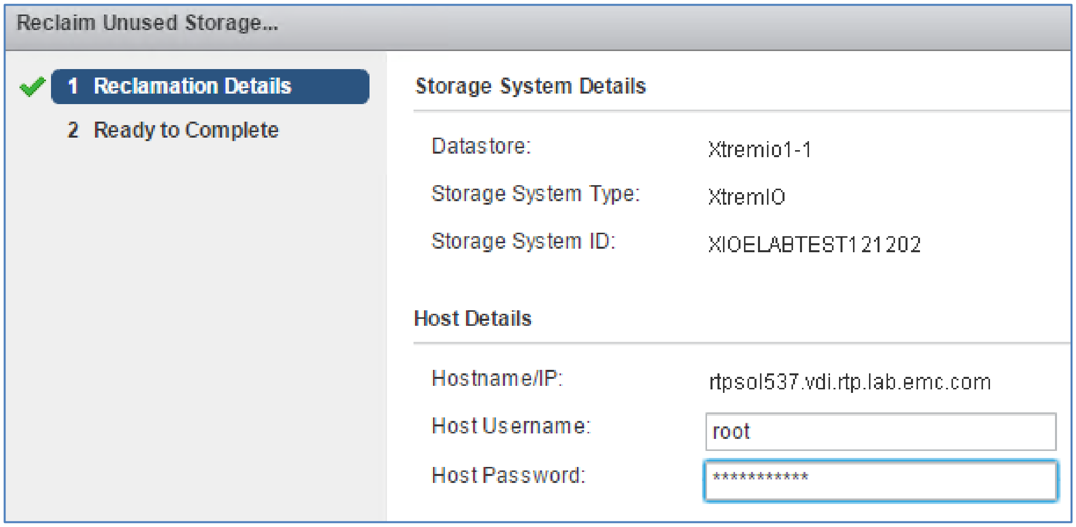


Figure 32. vSphere Web Client: EMC VSI Reclaim Unused Storage

3. For **Reclamation Details** in the **Reclaim Unused Storage** dialog box, type the username and password for a local account on the selected vSphere host, and then click **Next**.

Note: The local account must have root access.

EMC VSI automatically selects a host to use to perform the SCSI UNMAP operation, as shown in Figure 33.


Reclaim Unused Storage...

1 Reclamation Details

2 Ready to Complete

Storage System Details

Datastore: Xtremio1-1

Storage System Type: XtremIO

Storage System ID: XIOELABTEST121202

Host Details

Hostname/IP: rtpsol537.vdi.rtp.lab.emc.com

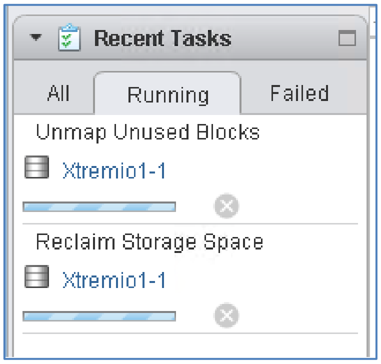
Host Username: root

Host Password: ***********

Figure 33. vSphere Web Client: Reclamation Details

4. For **Ready to Complete** in the **Reclaim Unused Storage** dialog box, review the details for the SCSI UNMAP operation, and then click **Finish**.

5. Navigate to the **Recent Tasks > Running** option to view the status of the SCSI UNMAP operation, as shown in Figure 34. You can also review the status of the operation by viewing the XtremIO array bandwidth statistics, as described in Using a script to perform SCSI UNMAP operations.


Recent Tasks

All | Running | Failed

Unmap Unused Blocks

Xtremio1-1

Reclaim Storage Space

Xtremio1-1

Figure 34. vSphere Web Client: Running view in Recent Tasks

Determining when additional XtremIO storage capacity is required

The native XtremIO event handlers generate alerts when array physical capacity reaches any of three different levels of severity, as outlined in the *EMC XtremIO Storage Array User Guide*. ESA can generate even more granular alerts based on your particular business requirements, and can alert on much more than just array physical capacity utilization.

In general, when an XtremIO array reaches 80 percent physical capacity utilization, do the following to gain more capacity:

- Perform a SCSI UNMAP operation on each vSphere datastore that is hosted on the target XtremIO array. Then review how much, if any, physical capacity the operations reclaim.

- If significant physical capacity cannot be reclaimed, and the amount of physical capacity being used continues to increase, purchase and deploy additional XtremIO storage in the near future.

Understanding the physical capacity needs of the environment over time is crucial for determining when additional XtremIO capacity will be required. Performing SCSI UNMAP operations as part of regular vSphere maintenance is essential to this understanding.

EMC recommends the following strategy to ensure that decisions made about long-term XtremIO capacity requirements are based on the maximum possible information:

- Perform monthly SCSI UNMAP operations of all XtremIO volumes.

  The frequency with which you need to perform these operations depends on the level of tenant activity, which is difficult to predict over the long term. If physical capacity utilization of the XtremIO array fluctuates significantly from week to week, you might need to perform the operations more frequently.

- Use the EMC Storage Analytics platform to automate the retention of XtremIO physical capacity utilization data over time.

  The historical data that ESA retains can help you identify any patterns or trends in capacity utilization.

- Consult with tenants about using NAS services for storing user data.

  User data is one of the most significant sources of long-term storage capacity growth. However, in most cases, user data does not require the level of performance provided by the XtremIO all-flash array. Storing some or all user data on EMC NAS platforms such as a VNX or Isilon array will free up capacity on the XtremIO array for more tenant desktops and provide more predictable growth in physical capacity utilization of the XtremIO array.

Chapter 8 Provisioning Horizon DaaS Tenants

This chapter presents the following topics:

Overview

This chapter summarizes the prerequisites and high-level tasks for provisioning a new tenant in VMware Horizon DaaS. For detailed information about provisioning tenants, refer to the VMware document *Horizon DaaS Platform 6.1 Tenant Installation – vCenter.*

Tenant infrastructure requirements

The tenant infrastructure must have the following resources available before you deploy the tenant in Horizon DaaS:

Note: Some of these resources are discussed in earlier sections of this guide, but are included here for completeness.

- (Optional) A network infrastructure for tenant backhaul connectivity to the corporate network.
- Active Directory domain services and DNS, DHCP, and NTP servers.

  Tenants can use their corporate-hosted resources for this purpose. In that case, EMC recommends deploying replicas of these services within the Horizon DaaS environment to ensure availability.
- One account in the tenant Active Directory domain. This account will be granted full administrative permissions within the service provider Horizon DaaS infrastructure.
- Two security groups in the tenant Active Directory domain:
  - A security group to be used to grant the member accounts with administrative access to the tenant's Horizon DaaS infrastructure.
  - A security group to be used to grant the member accounts the ability to log in to the tenant's Horizon DaaS user portal.
- A vSphere virtual machine port group or Distributed Virtual Port Group (DVPG) for the tenant network; this port group is specified when deploying the tenant in Horizon DaaS.
- A subnet with sufficient IP space for the tenant's current and future desktop needs.
- Up to seven IP addresses for Horizon DaaS components:
  - Two IP addresses for the tenant's Horizon DaaS management appliances.
  - One IP address for use as a shared floating IP address.

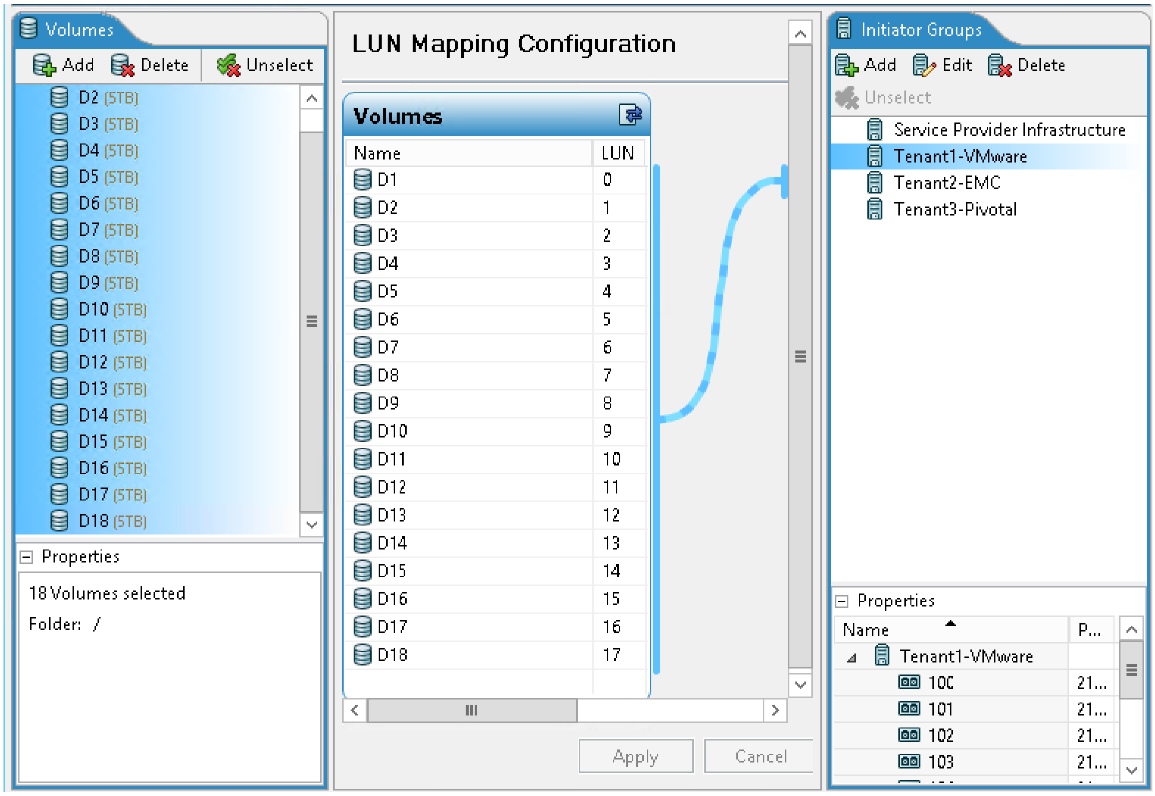
    If the tenant wants to manage Horizon DaaS using a DNS name, create a DNS record that points to the shared IP address.
  - (Optional) Three IP addresses for the Horizon DaaS dtRAM appliance if the tenant requires remote access over the public Internet.

§ (Optional) One IP address for the DHCP relay service if the tenant wants to use the backhaul connection into their corporate network to access remote DHCP servers.

Configuring XtremIO storage in a multitenant environment

The EMC XtremIO array requires no specific configuration to support a multitenant Horizon DaaS environment. In this solution, except for dedicated VLANs, the only feature that differentiates one tenant from another is the vSphere cluster or clusters that contain a tenant's virtual desktops.

In this solution, from the perspective of XtremIO, tenants are differentiated by using unique XtremIO initiator groups. For each vSphere cluster assigned to a tenant, we created a unique initiator group and populated the group with the vSphere hosts contained in the cluster. Figure 35 shows the Configuration workspace in the XtremIO Storage Management Application, with an example of an array that is configured in this way. For the example, we created three initiator groups for three different tenants, and one initiator group for the service provider infrastructure. For each initiator group, there is a corresponding vSphere cluster.



D2 (5TB)
D3 (5TB)
D4 (5TB)
D5 (5TB)
D6 (5TB)
D7 (5TB)
D8 (5TB)
D9 (5TB)
D10 (5TB)
D11 (5TB)
D12 (5TB)
D13 (5TB)
D14 (5TB)
D15 (5TB)
D16 (5TB)
D17 (5TB)
D18 (5TB)

Properties

18 Volumes selected

Folder: /

Volumes

Name	LUN
D1	0
D2	1
D3	2
D4	3
D5	4
D6	5
D7	6
D8	7
D9	8
D10	9
D11	10
D12	11
D13	12
D14	13
D15	14
D16	15
D17	16
D18	17

Service Provider Infrastructure
Tenant1-VMware
Tenant2-EMC
Tenant3-Pivotal

Properties

Name	P...
Tenant1-VMware	
100	21...
101	21...
102	21...
103	21...

Figure 35. XtremIO Storage Management: Configuration workspace

After the initiator groups are created, and the required number of XtremIO volumes are added to each, all you need do to prepare the datastores for use with vSphere is perform a vSphere **Rescan for Datastores** operation and format the datastores. Refer to Provisioning XtremIO storage for vSphere datastores for further information.

Adding and configuring Horizon DaaS tenants

The VMware document *Horizon DaaS Platform 6.1 Tenant Installation – vCenter* details the requirements and steps for deploying a new Horizon DaaS tenant, including creating, configuring, and entitling the tenant.

Prior to deploying the new tenant, verify that all prerequisites are met, as outlined in Tenant infrastructure requirements and in the Horizon DaaS documentation. If the tenant requires remote access to Horizon DaaS desktops over the public Internet, create dtRAM appliances for the tenant, as described in the Horizon DaaS documentation.

The tenant installation process deploys the following Horizon DaaS appliances:

- A pair of redundant Horizon DaaS Tenant appliances, used by the tenant to manage their Horizon DaaS infrastructure.
- (Optional) A pair of redundant Horizon DaaS dtRAM appliances, used by the tenant to provide access to Horizon DaaS desktops over the public Internet.

Refer to Chapter 10 for information about creating virtual desktop images for use with Horizon DaaS.

Chapter 9 Using EMC Isilon and EMC VNX Storage for User Data

This chapter presents the following topics:

Overview

This solution uses EMC VNX or EMC Isilon storage arrays to provide user data storage in the Horizon DaaS multitenant environment. This chapter provides a high-level overview of how to provide tenants with access to services hosted on either platform.

Using an EMC Isilon array to provide user home directories

The EMC document *Isilon OneFS Web Administration Guide* provides the procedures for implementing Isilon-hosted home directories within a tenant's environment.

The following resources are required to deploy an Isilon virtual file server in the tenant's environment:

- One unused IP address on the tenant's network, and associated network information such as DNS servers, DNS domain name, and the network subnet mask.
- A DNS network name for the Isilon SmartConnect™ interface on the tenant's network, and a DNS record for that interface on the tenant's DNS server.
- The amount of storage space on the Isilon array that the tenant requires, including any per-user quota and file system snapshot requirements.

  Refer to the *Isilon OneFS Web Administration Guide* for information about how to configure quotas and snapshots on Isilon OneFS®.
- (Optional) The credentials for an account with permission to join computers to the tenant's Active Directory domain. Alternatively, the tenant can enter this information during configuration of the Isilon Active Directory services. The tenant is responsible for creating this account if required.

After these prerequisites are met, the service provider can deploy the tenant's Isilon virtual file server and configure the Isilon volumes and folder structures as needed.

Using an EMC VNX array to provide user home directories

EMC VNX Series Version 8.1: Configuring and Managing CIFS on VNX provides the procedures for implementing VNX-hosted home directories within a tenant's environment.

The following resources are required to deploy a VNX CIFS server in the tenant's environment:

- One unused IP address on the tenant's network, and associated network information such as DNS servers, DNS domain name, and the network subnet mask.
- A DNS network name for the VNX CIFS server on the tenant's network, and a DNS record for that CIFS server on the tenant's DNS server.

- The amount of storage space on the VNX array that the tenant requires, including any per-user quota and file system snapshot requirements.
  - Refer to *EMC VNX Series Release 8.1: Using Quotas on VNX* for information about how to configure quotas on VNX file systems.
  - Refer to *EMC VNX Series Release 8.1: Using VNX SnapSure* for information about how to use EMC SnapSure to create and manage VNX snapshots.
- (Optional) The credentials for an account with permission to join computers to the tenant's Active Directory domain. Alternatively, the tenant can enter this information during configuration of the VNX CIFS servers. The tenant is responsible for creating this account if required.

After these prerequisites are met, the service provider can deploy the tenant's CIFS server and configure the VNX file systems and folder structures as needed.

Chapter 10 Configuring Desktop Images

This chapter presents the following topics:

Overview

This chapter provides a high-level overview of how to create, prepare, and maintain virtual desktop images for use with VMware Horizon DaaS. For full details about these processes, refer to the VMware document *Horizon DaaS Platform 6.1 Tenant Installation – vCenter.*

Creating virtual desktop images

We validated this solution with two different virtual desktop images, one that uses Microsoft Windows 7 as the base OS, and a second that uses Microsoft Windows Server 2012 R2 with the Desktop Experience feature. The solution supports both options, provided that Microsoft guidelines for minimum system requirements are met.

Regardless of which base OS the virtual desktop image uses, the tenant should verify that the OS is configured correctly for their environment prior to supplying the image to the service provider. For Windows Server 2012 R2 desktop images, the tenant should also install the Desktop Experience feature if they have not already done so.

Note: The Microsoft TechNet topic *Desktop Experience Overview* provides information about the Desktop Experience feature of Windows Server 2012 R2, including installation and configuration options.

The tenant should provide the CSP with, at minimum, a gold image in OVA file or VMDK file format that will be used to deploy desktops in Horizon DaaS. If the image is in VMDK format, verify the OS version and hardware configuration of the image with the tenant prior to creating the virtual machine to which you will attach the VMDK file.

The service provider typically imports the file manually into the tenant’s Horizon DaaS vSphere cluster. The tenant can then proceed to prepare the gold image and deploy tenant desktops from it.

Preparing a gold image and deploying tenant desktops

The VMware document *Horizon DaaS Platform 6.1 Tenant Installation – vCenter* details the steps that tenants use to prepare a gold image for use with VMware Horizon DaaS. These steps include installation and configuration of the Horizon DaaS agent and other software components that enable support for all possible client connection protocols. EMC also recommends optimizing the desktop image as described in Optimizing desktop images for virtual environments.

When the gold image is ready, the tenant can use it to deploy as many virtual desktops as is permitted based on the resources entitled to the tenant by the service provider.

Optimizing desktop images for virtual environments

The following documents provide information on how to optimize desktop images for use in a virtual desktop environment. This type of optimization is not mandatory but can help tenants reduce the Horizon DaaS infrastructure resources that their virtual desktops require.

EMC documents

- *Deploying Microsoft Windows 7 Virtual Desktops with VMware View —Applied Best Practices*
- *Deploying Microsoft Windows 8 Virtual Desktops—Applied Best Practices*

VMware document

- *VMware Horizon with View Optimization Guide for Windows 7 and Windows 8*

Note: These documents do not include recommendations for desktops based on Windows Server 2012 R2.

Optimizing tenant desktop maintenance

EMC recommends that, where possible, tenants apply a level of randomization to the schedule they use to install software patches or antivirus pattern updates to their virtual desktops. The reasons for this include the following:

- Some desktop maintenance tasks generate a much higher load than is typical on the Horizon DaaS vSphere clusters. Services such as vSphere host CPU and RAM, as well as network and storage array performance, could all be negatively affected, and other Horizon DaaS desktop users and tenants using those shared resources might experience degradation in performance as a result.

- In the case of major maintenance tasks such as desktop service pack installations or application upgrades, when these are performed at scale they can lead to a rapid change in storage capacity utilization, which could potentially leave the service provider with insufficient time to address any problems that might occur.

This solution does not explicitly require that these and other desktop maintenance operations be spread out over a longer period, but doing so reduces the possibly of performance degradation across the infrastructure.

Chapter 11 Conclusion

This chapter presents the following topics:

Summary

This solution provides a blueprint of a validated VMware Horizon DaaS solution enabled by an EMC XtremIO all-flash array, EMC VNX, EMC Isilon, and the VMware vSphere virtualization platform. This solution provides CSPs with a 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 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 EMC XtremIO array enable virtual desktop application response times that mirror the SSD experience of the most modern physical desktops, even if it 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 EMC XtremIO array dramatically reduce the storage required for full-clone Horizon DaaS virtual desktops. As few as five rack units of space can provide the storage required for up to 2,500 full-clone desktops. This allows for an attractive storage cost per desktop, even with the benefit of 100 percent flash storage.

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

Findings

By using the XtremIO storage system as the foundation for Horizon DaaS deployments, service providers gain the following unique advantages that cannot be achieved with any other Horizon DaaS deployment architecture:

- **Superior Horizon DaaS tenant experience**—Test results showed that every desktop in an XtremIO deployment gets reliable and massive I/O potential, both in sustained IOPS and in the ability to burst to much higher levels as dictated for demanding applications such as Microsoft Outlook, desktop search, and antivirus scanning.

- **Lower cost per virtual desktop**—Horizon DaaS deployments that leverage a combination of XtremIO and Isilon or VNX storage are surprisingly affordable. Due to the inline data reduction and massive performance density of XtremIO, and the user data services capabilities of the Isilon and VNX arrays, the cost per desktop is lower than with other Horizon DaaS solutions, enabling virtual desktops to be deployed for less than their physical desktop counterparts.

- **Rapid provisioning and rollout**—Because XtremIO is simple to set up and requires no tuning, complex planning is eliminated. Horizon DaaS deployments can be designed and rolled out quickly and tenants deployed with assured success.

- **No need for third-party tools**—XtremIO solves all I/O-related Horizon DaaS deployment challenges. Deployment does not require additional caching, host-based deduplication schemes, or any other point solutions that increase expense and complexity.

- **No change to desktop administration**—Whatever methods tenants are using to manage their existing physical desktops can be directly applied to their Horizon DaaS virtual desktops when XtremIO is used. No software updates, operating system patching, antivirus scanning, or other procedures are required to lighten the I/O load on shared storage. Instead, service providers and tenants can confidently rely on the high performance provided by XtremIO.

- **No change to desktop setup**—Many virtual desktop best practices currently demand multiple changes to the desktop image to reduce the I/O load on shared storage. None of these changes are explicitly required with XtremIO, enabling the desktop to remain fully functional while maintaining a strong user experience.

Chapter 12 References

This chapter presents the following topics:

EMC documentation

The following documentation on EMC Online Support or EMC.com provides 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 Reference Architecture Guide*
- *EMC PowerPath/VE for VMware vSphere Installation and Administration Guide*
- *EMC PowerPath Viewer Installation and Administration Guide*
- *EMC Storage Analytics 3.0 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 User Guide*
- *EMC XtremIO Storage Array Security Configuration Guide*
- *Flash Implications in Enterprise Storage Array Designs*
- *Isilon OneFS Web Administration Guide*

VMware documentation

The following documentation on the VMware website provides additional and relevant information:

- *Horizon DaaS Platform 6.1 Blueprint*
- *Horizon DaaS 6.1 Downloading SSL Certificate for Gold Pattern*
- *Horizon DaaS Platform 6.1 Enterprise Center Handbook*
- *Horizon DaaS Platform 6.1 Release Notes*
- *Horizon DaaS Platform 6.1 Service Provider Installation – vCenter*
- *Horizon DaaS Platform 6.1 Tenant Installation – vCenter*
- *Installing and Administering VMware vSphere Update Manager*

- *Installing or Migrating vRealize Operations Manager*
- *Preparing the Update Manager Database*
- *Preparing vCenter Server Databases*
- *Understanding Memory Resource Management in VMware vSphere 5.0 Performance Study*
- *Using esxcli in vSphere 5.5 to reclaim VMFS deleted blocks on thin-provisioned LUNs (2057513)*
- *VMware vCenter Server and Host Management*
- *VMware Horizon with View Optimization Guide for Windows 7 and Windows 8*
- *vRealize Operations Manager Sizing Guidelines* (2093783)
- *vRealize Operations Manager vApp Deployment and Configuration Guide*
- *vSphere Installation and Setup*
- *vSphere Networking*
- *vSphere Resource Management*
- *vSphere Storage*
- *vSphere Virtual Machine Administration*
- *vSphere Virtual Machine Management*

Other documentation

The following documents, available on the Microsoft TechNet website or the Microsoft Developer Network website, provide additional and relevant information:

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