



# EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition

---

*Foundation Infrastructure Solution Guide*

## Abstract

This Solution Guide provides an introduction to VMware vCloud Suite, and the EMC hardware, software, and services portfolio. This document is an enablement reference to begin the planning and design of a hybrid cloud.

December 2014



Copyright © 2014 EMC Corporation. All rights reserved. Published in the USA.

Published December 2014

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.

EMC<sup>2</sup>, EMC, ViPR, VNX, Symmetrix, VMAX, Avamar, Data Domain, Data Protection Advisor, VSI, Virtual Storage Infrastructure, Syncplicity, Unisphere, PowerPath, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com (<http://www.emc.com/legal/emc-corporation-trademarks.htm>).

**EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition  
Foundation Infrastructure Solution Guide**

Part Number H13530



EMC<sup>2</sup>

Pivotal

RSA

vmware®

# Contents

<b>Chapter 1</b>	<b>Executive Summary</b>	<b>11</b>
	Document purpose.....	12
	Audience.....	12
	Solution purpose.....	13
	Business challenge .....	13
	Technology solution .....	14
	Key components.....	14
	Terminology .....	16
<b>Chapter 2</b>	<b>Software-Defined Data Center Overview</b>	<b>19</b>
	Overview .....	20
	Automation and self-service provisioning.....	21
	Multitenancy and secure separation.....	23
	Workload-optimized storage .....	25
	Elasticity and service assurance .....	25
	Monitoring and resource management .....	25
	Metering and chargeback.....	27
	Modular add-on components .....	28
	Application services .....	28
	Data protection services .....	28
	Continuous availability .....	28
	Disaster recovery .....	28
	Public cloud services.....	29
	EMC and VMware integration.....	29
	Storage services .....	29
	Orchestration.....	30
	Operational management and monitoring .....	30
	Metering.....	30
	Summary.....	30
<b>Chapter 3</b>	<b>Solution Architecture and Design</b>	<b>31</b>
	Solution architecture.....	32
	Hybrid cloud architecture.....	32



Solution design .....	37
Tenant design .....	37
Storage design and consumption .....	39
Network design.....	41
EMC Enterprise Hybrid Cloud software resources.....	44
EMC Enterprise Hybrid Cloud sizing .....	44
<b>Chapter 4   Cloud Services</b> .....	<b>45</b>
Self-service catalog .....	46
Virtual machine lifecycle services.....	47
Virtual machine blueprints.....	47
Use case 1: Provision virtual machine.....	48
Use case 2: Reconfigure an existing virtual machine.....	55
Use case 3: Decommission a virtual machine .....	56
Storage services.....	57
Overview .....	57
Storage services pre-conditions.....	57
Use case 1: Storage provisioning.....	57
Use case 2: Select virtual machine storage .....	61
Use case 3: Metering storage services .....	62
Storage services summary .....	63
Networking services .....	64
Overview .....	64
Provisioning three-tiered virtual applications.....	64
Use case 1: Configure pre-provisioned multimachine blueprint .....	65
Use case 2: Create on-demand multimachine blueprints .....	68
Networking services summary .....	72
<b>Chapter 5   Operational Management</b> .....	<b>73</b>
Overview .....	74
Integrated and intelligent operational monitoring.....	74
EMC ViPR Analytics and Storage Analytics .....	75
Centralized log management .....	81
Resource management.....	87
Storage resource management .....	87
Storage compliance management.....	89
Virtual machine resource management.....	92
Metering.....	95



Metering analysis .....	97
Summary.....	104
<b>Chapter 6 Security</b>	<b>105</b>
Overview of cloud security challenges .....	106
Public key infrastructure X.509 integration .....	107
Enterprise PKI architecture.....	107
Enterprise PKI solution integration.....	108
Converged authentication .....	109
Secure authentication .....	110
Microsoft Active Directory .....	112
VMware vCenter SSO .....	113
TACACS+ authentication integration .....	113
Role-based access control.....	113
Infrastructure administrator.....	114
Tenant administrator .....	114
Fabric group administrator.....	114
Business group.....	115
Centralized log management .....	115
VMware vCenter Log Insight.....	116
Security configuration and management .....	119
vCenter host profiles.....	119
vSphere Update Manager .....	120
vCenter Configuration Manager.....	121
Multitenancy .....	123
Network security.....	123
Security virtualization .....	125
Summary.....	128
<b>Chapter 7 Conclusion</b>	<b>129</b>
Conclusion .....	130
<b>Chapter 8 References</b>	<b>131</b>
EMC documentation .....	132
Other documentation .....	132



**Figures**

Figure 1. EMC Enterprise Hybrid Cloud solution components ..... 14

Figure 2. EMC Enterprise Hybrid Cloud features and functionality ..... 21

Figure 3. Self-service provisioning through the vCAC portal..... 22

Figure 4. EMC ViPR Analytics with VMware vCenter Operations Manager..... 26

Figure 5. ITBM Suite overview dashboard for hybrid cloud ..... 27

Figure 6. EMC ViPR integration points with VMware ..... 29

Figure 7. EMC Enterprise Hybrid Cloud solution architecture ..... 32

Figure 8. Cloud management terminology and hierarchy..... 33

Figure 9. Software-defined data center tenant design and endpoints..... 37

Figure 10. Business group resource reservations ..... 38

Figure 11. Storage service offerings for the hybrid cloud ..... 39

Figure 12. Blueprint storage configuration in vCAC..... 40

Figure 13. Physical topology of the network ..... 42

Figure 14. Logical network overview..... 43

Figure 15. Self-service portal and service catalog overview ..... 46

Figure 16. Deploy new virtual machines from available blueprints ..... 47

Figure 17. Create a new VMware vSphere virtual machine blueprint..... 48

Figure 18. Create a new blueprint ..... 49

Figure 19. Select vSphere template for cloning ..... 49

Figure 20. Complete build information for new blueprint ..... 50

Figure 21. Select custom build profiles for virtual machine ..... 51

Figure 22. Enable virtual machine operations for cloud user ..... 51

Figure 23. Deploy new virtual machine blueprint from the self-service portal ..... 52

Figure 24. Complete request information for virtual machine ..... 52

Figure 25. Select storage reservation policy for virtual machine ..... 53

Figure 26. Virtual machine details and available actions ..... 53

Figure 27. Application services: Provision databases and applications..... 54

Figure 28. Reconfigure virtual machine resources ..... 55

Figure 29. Schedule reconfiguration of virtual machine..... 56

Figure 30. Decommission virtual machine..... 56

Figure 31. Storage Services: Provision cloud storage ..... 57

Figure 32. Provision cloud storage: Select vCenter cluster..... 58

Figure 33. Storage provisioning: Select datastore type..... 59

Figure 34. vCAC storage provisioning: Choose ViPR storage pool ..... 59

Figure 35. Storage provisioning: Enter storage size ..... 60

Figure 36. Provision storage: Storage reservation for vCAC business group..... 61



Figure 37.	Set storage reservation policy for VMDKs.....	61
Figure 38.	Create new virtual machine storage profile for Tier-2 storage.....	62
Figure 39.	Automatic discovery of storage capabilities.....	62
Figure 40.	VMware ITBM chargeback based on storage profile of datastore .....	63
Figure 41.	Three-tiered application .....	64
Figure 42.	Pre-provisioned blueprint with build information configuration .....	65
Figure 43.	Blueprint network and security group configuration.....	65
Figure 44.	Virtual machine properties: EHC-75 database-tier .....	66
Figure 45.	Virtual machine web client properties: EHC-75 database-tier.....	67
Figure 46.	NSX service composer security groups membership view .....	67
Figure 47.	Copying an existing network profile to a blueprint .....	68
Figure 48.	Multimachine network properties.....	68
Figure 49.	Multimachine build configuration for load balanced blueprints.....	69
Figure 50.	Web-tier blueprint configuration.....	69
Figure 51.	Multimachine web-tier load balancer configuration.....	70
Figure 52.	Machine properties for an on-demand provisioned virtual machine.....	70
Figure 53.	Logical switches view .....	71
Figure 54.	Interface configuration for on-demand provisioned NSX Edge 5.5.....	71
Figure 55.	Load balancing configuration of the provisioned NSX Edge 5.5 .....	72
Figure 56.	NAT configured on the engineering on-demand NSX Edge 5.5.....	72
Figure 57.	vCenter Operations Manager dashboard high-level overview.....	74
Figure 58.	Architecture overview of vC Ops vApp including ESA.....	75
Figure 59.	EMC ViPR Capacity dashboard in vCenter Operations Manager.....	76
Figure 60.	EMC ViPR Performance dashboard in vCenter Operations Manager.....	77
Figure 61.	EMC ViPR at-a-glance dashboard in vCenter Operations Manager.....	78
Figure 62.	EMC storage metrics dashboard with VMAX LUN metrics .....	80
Figure 63.	EMC VMAX overview dashboard displaying object heat maps.....	80
Figure 64.	Centralized logging of components with vCenter Log Insight .....	82
Figure 65.	Customized hybrid cloud security dashboard .....	83
Figure 66.	Search logs for cloud management platform.....	84
Figure 67.	Log Insight filtering logs for the management cluster components.....	84
Figure 68.	Sample of the dashboard view: VNX content pack.....	85
Figure 69.	Example of EMC VMAX content pack dashboard views .....	86
Figure 70.	EMC ViPR SRM: Overview of ViPR virtual array.....	88
Figure 71.	EMC ViPR virtual pool details.....	88
Figure 72.	EMC ViPR SRM: Storage pools supporting ViPR virtual pools.....	89
Figure 73.	EMC ViPR SRM: Physical storage systems .....	89



Figure 74. Create a storage compliance policy: Description.....90

Figure 75. Create storage compliance policy: Scope .....90

Figure 76. Create storage compliance policy: Rules.....91

Figure 77. Breach Report: Active breaches by severity and policy.....91

Figure 78. All Active Breaches report.....92

Figure 79. Virtual machine capacity for the cloud management platform .....93

Figure 80. Specify a reference virtual machine configuration.....93

Figure 81. What-if scenario: Adding 20 new virtual machines .....94

Figure 82. Edit policy to specify thresholds for virtual machines .....94

Figure 83. List of oversized virtual machines.....95

Figure 84. ITBM overview .....96

Figure 85. ITBM operational analysis of a hybrid cloud environment .....97

Figure 86. ITBM: Set expected utilization of CPU and RAM .....98

Figure 87. ITBM Demand Analysis of hybrid cloud.....98

Figure 88. ITBM Demand Analysis: Application costs .....99

Figure 89. ITBM Demand Analysis: Virtual machine costs.....99

Figure 90. ITBM Server report: Part I.....100

Figure 91. ITBM Server report: Part II Server Hardware.....100

Figure 92. ITBM Server report: Part III OS Licensing .....100

Figure 93. ITBM VMs report .....101

Figure 94. ITBM VMs report with Total VM Monthly Cost.....101

Figure 95. ITBM cloud cost overview .....102

Figure 96. ITBM cloud cost: Server Hardware details .....102

Figure 97. ITBM cloud cost: Edit monthly costs of server hardware.....103

Figure 98. ITBM Automatic cost profile for storage resources in vCAC.....103

Figure 99. VMware ITBM chargeback based on storage profile of datastore .....104

Figure 100. PKI hierarchy for EMC Enterprise Hybrid Cloud solution stack .....108

Figure 101. Authentication relationships between the solution components .....111

Figure 102. Overview of vCenter Log Insight log collection types .....116

Figure 103. Example of a vCenter Log Insight dashboard showing logins .....118

Figure 104. vC Ops dashboard displaying Risk badge score.....122

Figure 105. vC Ops dashboard displaying compliance status summary .....122

Figure 106. EMC Enterprise Hybrid Cloud network architecture .....124

**Tables**

Table 1. Terminology .....16

Table 2. Edge network connectivity.....41





Table 3. Comparison of the NSX Edge features supported by vCAC .....128



EMC<sup>2</sup>

Pivotal™

RSA

vmware®



EMC<sup>2</sup>

Pivotal™

RSA

vmware®

# Chapter 1 Executive Summary

This chapter presents the following topics:

- Document purpose** ..... 12
- Audience** ..... 12
- Solution purpose** ..... 13
- Business challenge** ..... 13
- Technology solution**..... 14
- Terminology**..... 16



## Document purpose

This Solution Guide is a comprehensive overview of the EMC Enterprise Hybrid Cloud solution, and describes how it can be used to enable IT organizations to quickly deploy an on-premises hybrid cloud that delivers infrastructure as a service (IaaS) and other cloud services to your business. This guide introduces the key components, architecture, use cases and functionality of the EMC Enterprise Hybrid Cloud solution.

The *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Foundation Infrastructure Reference Architecture* and this Solution Guide describe the reference architecture and the foundation that EMC Enterprise Hybrid Cloud add-on solutions are built on.

The following documents provide further information about how to implement specific capabilities or enable specific use cases within the EMC Hybrid Cloud solution:

- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Continuous Availability Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Disaster Recovery Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Backup Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Hadoop Applications Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Pivotal CF Platform as a Service Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Security Management Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Public Cloud Integration Guide*

## Audience

This document is intended for executives, managers, architects, cloud administrators, and technical administrators of IT environments who want to implement or use the EMC Enterprise Hybrid Cloud solution. Readers should be familiar with VMware® vCloud Suite®, storage technologies, and general IT functions and requirements, and how they fit into a hybrid cloud architecture.



## Solution purpose

The EMC Enterprise Hybrid Cloud solution enables EMC customers to build an enterprise-class, scalable, multitenant cloud that enables:

- Complete management of the infrastructure service lifecycle
- On-demand access to and control of network bandwidth, servers, storage, and security
- Provisioning, monitoring, and management of the infrastructure services by the line-of-business end user, without IT administrator involvement
- Provisioning of application blueprints with associated infrastructure resources by line-of-business application owners without IT administrator involvement
- Provisioning of backup, continuous availability, and disaster recovery services as part of the cloud service provisioning process
- Maximum asset utilization

The EMC Enterprise Hybrid Cloud solution provides a reference architecture and best practice guidance that is necessary to integrate all the key components and functionality of a hybrid cloud.

## Business challenge

While many organizations have successfully introduced virtualization as a core technology within their data center, the benefits of virtualization have largely been restricted to the IT infrastructure owners. End users and business units within customer organizations have not experienced many of the benefits of virtualization, such as increased agility, mobility, and control.

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

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

The difficulty in overcoming these challenges has given rise to public cloud providers who have built technology and business models specifically catering to the requirements of end-user agility and control. Many organizations are under pressure to provide these same service levels within the secure and compliant confines of the on-premises data center. As a result, IT departments need to create cost-effective alternatives to public cloud services, alternatives that do not compromise enterprise features such as data protection, disaster recovery, and guaranteed service levels.



## Technology solution

This EMC Enterprise Hybrid Cloud solution integrates the best of EMC and VMware products and services, and empowers IT organizations to accelerate implementation and adoption of hybrid cloud infrastructure, while still enabling customer choice for the compute and networking infrastructure within the data center. The solution caters to customers who want to preserve their investment and make better use of their existing infrastructure and to those who want to build out new infrastructures dedicated to a hybrid cloud.

This solution takes advantage of the strong integration between EMC technologies and the VMware vCloud Suite. The solution, developed by EMC and VMware product and services teams includes EMC scalable storage arrays, integrated EMC and VMware monitoring, and data protection suites to provide the foundation for enabling cloud services within the customer environment.

### Key components

This section describes the key components of the solution, as shown in Figure 1.

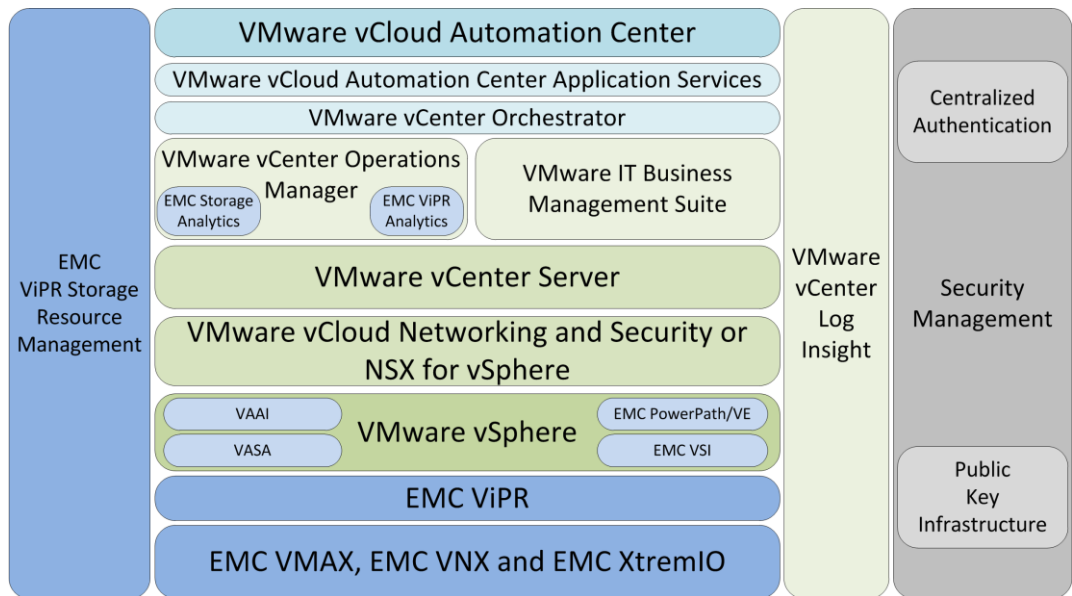


Figure 1. EMC Enterprise Hybrid Cloud solution components

### Data center virtualization and cloud management

#### VMware vCloud Automation Center

VMware vCloud<sup>®</sup> Automation Center<sup>™</sup> (vCAC) enables customized, self-service provisioning and lifecycle management of cloud services that comply with established business policies. vCAC provides a secure portal where authorized administrators, developers, and business users can request new IT services and manage existing computer resources from predefined user-specific menus.



***VMware vSphere ESXi and VMware vCenter Server***

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

***VMware vCenter Orchestrator***

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

***VMware vCloud Networking and Security***

VMware vCloud Networking and Security™ (vCNS) is a software-defined networking and security solution that enhances operational efficiency, unlocks agility, and enables extensibility to rapidly respond to business needs. It provides a broad range of services in a single solution, including virtual firewall, virtual private network (VPN), load balancing, and VXLAN-extended networks.

***Premium deployment option: VMware NSX for vSphere***

An alternative deployment option to vCNS is VMware NSX™ for vSphere. NSX is the next generation of software-defined network virtualization and offers additional functionality and improved performance over vCNS and traditional network and security devices. This additional functionality includes distributed logical routing, distributed firewalling, logical load balancing, and support for routing protocols. Where workloads on different subnets share the same host, the distributed logical router optimizes traffic flows by routing locally. This enables substantial performance improvements in throughput, with distributed logical routing and firewalling providing line-rate performance distributed across many hosts. NSX also introduces Service Composer, which integrates with third-party security services.

***VMware vCenter Operations Manager***

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



***VMware vCenter Log Insight***

VMware vCenter Log Insight™ delivers automated log management and aggregation. With an integrated cloud operations management approach, Log Insight provides the operational intelligence through log analytics and search for enterprise-wide visibility. It provides service-level awareness to ensure operational efficiency in dynamic hybrid cloud environments.

***VMware IT Business Management Suite***

VMware IT Business Management™ (ITBM) Suite provides transparency and control over the cost and quality of IT services. By providing a business context to the services that IT offers, ITBM helps IT organizations move from a technology orientation to a service-broker orientation, delivering a portfolio of IT services that aligns with the needs of business stakeholders.

**EMC storage services**

***EMC ViPR***

EMC ViPR® is a lightweight, software-only solution that transforms existing storage into a simple, extensible, and open platform. ViPR extends current storage investments to meet new cloud-scale workloads, and enables simple data and application migration out of public clouds and back under the control of IT (or vice versa). ViPR gives IT departments the ability to deliver on-premises, fully automated storage services at price points that are at or below public cloud providers.

***EMC ViPR SRM***

EMC ViPR SRM, storage resource management software, provides comprehensive monitoring, reporting, and analysis for heterogeneous block, file, and virtualized storage environments. It enables you to visualize applications to storage dependencies, monitor and analyze configurations and capacity growth, and optimize your environment to improve return on investment.

## Terminology

Table 1 lists the terminology used in the guide.

**Table 1. Terminology**

Term	Definition
ACL	Access control list
AD	Active Directory
AIA	Authority Information Access
API	Application programming interface
Blueprint	A blueprint is a specification for a virtual, cloud, or physical machine and is published as a catalog item in the common service catalog





<b>Term</b>	<b>Definition</b>
Business group	A managed object that associates users with a specific set of catalog services and infrastructure resources
CA	Certification authority
CBT	Changed Block Tracking
CDP	CRL Distribution Point
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
Fabric group	A collection of virtualization compute resources and cloud endpoints managed by one or more fabric administrators
FQDN	Fully qualified domain name
HSM	Hardware security module
IaaS	Infrastructure as a service
IIS	Internet Information Services
LAG	Link aggregation that bundles multiple physical Ethernet links between two or more devices into a single logical link can also be used to aggregate available bandwidth, depending on the protocol used.
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL
MCCLI	Management Console Command Line Interface
PEM	Privacy Enhanced Electronic Mail
PKI	Public key infrastructure
PVLAN	Private virtual LAN
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
VDC	Virtual device context
vDS	Virtual distributed switch
VLAN	Virtual local area network
VRF	Virtual routing and forwarding
VSI	Virtual Storage Integrator
VXLAN	Virtual Extensible LAN





EMC<sup>2</sup>

Pivotal™

RSA

vmware®

## Chapter 2 Software-Defined Data Center Overview

This chapter presents the following topics:

<b>Overview .....</b>	<b>20</b>
<b>Automation and self-service provisioning .....</b>	<b>21</b>
<b>Multitenancy and secure separation .....</b>	<b>23</b>
<b>Workload-optimized storage.....</b>	<b>25</b>
<b>Elasticity and service assurance .....</b>	<b>25</b>
<b>Monitoring and resource management .....</b>	<b>25</b>
<b>Metering and chargeback .....</b>	<b>27</b>
<b>Modular add-on components .....</b>	<b>28</b>
<b>Public cloud services.....</b>	<b>29</b>
<b>EMC and VMware integration .....</b>	<b>29</b>
<b>Summary.....</b>	<b>30</b>



## Overview

The EMC Enterprise Hybrid Cloud is an engineered solution that offers a simplified approach to IT functionality for IT organizations, developers, end users, and line-of-business owners. In addition to delivering baseline infrastructure as a service (IaaS), built on the software-defined data center (Software-Defined Data Center) architecture, the EMC Enterprise Hybrid Cloud also delivers feature-rich capabilities to expand from IaaS to business-enabling IT as a service (ITaaS).

Backup as a service (BaaS) and disaster recovery as a service (DRaaS) policies can be enabled with just a few clicks. End users and developers can quickly gain access to a marketplace of application resources, from Microsoft, Oracle, SAP, EMC Syncplicity, Pivotal, and third-party vendors as needed. Resources can be deployed on private cloud or EMC-powered public cloud service providers, including VMware vCloud Air™.

This solution includes the following features and functionality, as shown in Figure 2:

- **Automation and self-service provisioning**
- **Multitenancy and secure separation**
- **Workload-optimized storage**
- **Elasticity and service assurance**
- **Monitoring and resource management**
- **Metering and chargeback**
- **EMC and VMware integration**





Figure 2. EMC Enterprise Hybrid Cloud features and functionality

## Automation and self-service provisioning

This EMC Enterprise Hybrid Cloud solution provides self-service provisioning of automated cloud services to end users and infrastructure administrators. The EMC Enterprise Hybrid Cloud uses VMware vCloud Automation Center (vCAC), integrated with EMC ViPR and VMware NSX, to provide the compute, storage, network, and security virtualization services for the software-defined data center. These services enable rapid deployment of business-relevant cloud services across your hybrid cloud and physical infrastructure.

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

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



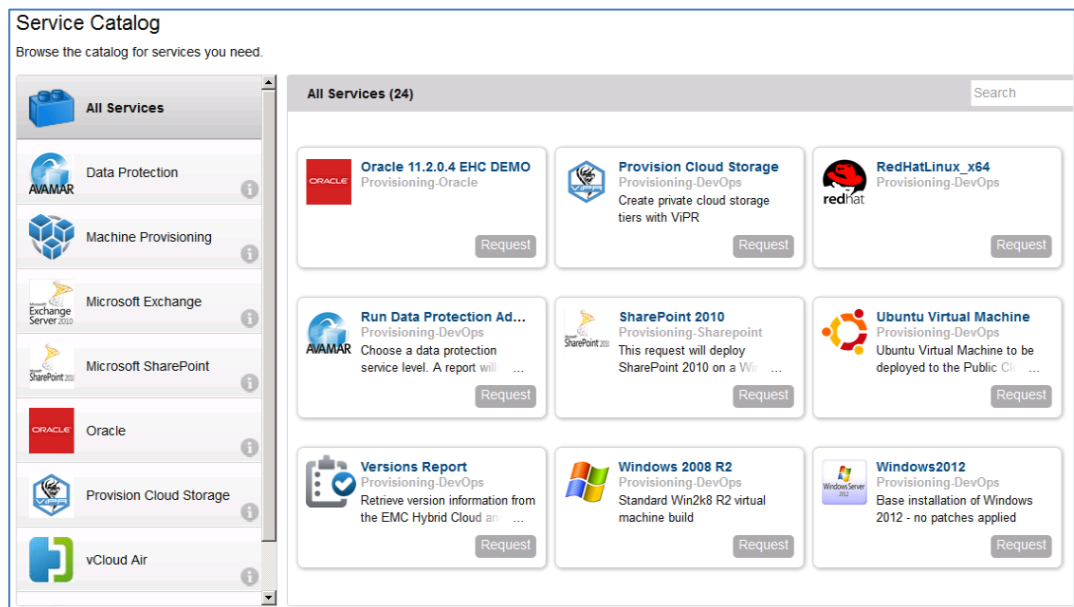
- **Build specifications:** Contain the automation policies that specify the process for building or reconfiguring compute resources

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

Service blueprints enable cloud infrastructure administrators to deploy new EMC services supported ViPR for automated storage services, and Avamar® and Data Domain® for backup and restore services.

Virtual machine and application blueprints can be single machine or multimachine, covering both bare metal server and virtual machine deployments. Multitier enterprise applications requiring multiple components (application, database, and web) and service levels can be deployed easily from predefined blueprints.

Figure 3 shows the EMC Enterprise Hybrid Cloud self-service portal in VMware vCAC.



**Figure 3. Self-service provisioning through the vCAC portal**

Data protection policies can be applied to virtual machine resources at provisioning time, which later enables users to request on-demand backups and restores of their virtual machines, and generate backup reports from the vCAC self-service portal.

As part of the vCAC provisioning process, NSX virtual networks can be used to provide an on-demand deployment model including custom networks. This enables a custom



network configuration to be established as part of a multi-tier virtual machine provisioning process.

This solution is built to work with new and existing infrastructures. It supports the differing requirements of an enterprise's many business units, and integrates with a wide variety of existing IT systems and best practices.

## Multitenancy and secure separation

Multitenancy access requirements in a cloud environment range from shared, open resource access to completely isolated resources. This solution provides the ability to enforce physical and virtual separation for multitenancy, offering different levels of security to meet business requirements. This separation can encompass network, compute, and storage resources, to ensure appropriate security and performance for each tenant.

The solution supports secure multitenancy through vCAC role-based access control (RBAC), enabling vCAC roles to be mapped to Active Directory groups. vCAC uses existing authentication and business groupings. User access to self-service portal is governed by the user's business role.

Physical segmentation of resources can be achieved in vCAC to isolate tenant resources or to isolate and contain compute resources for licensing purposes. For example, Oracle licensing costs can be managed by limiting the amount of CPU resources assigned to a particular resource group.

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

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

- Implementing virtual local area networks (VLANs) to enable isolation at Layer 2 throughout the solution and where it intersects with the enterprise network
- Implementing network security controls such as PVLANS, VRFs, and VDCs to provide isolation at Layer 3
- Using VXLAN overlay networks to segment tenant and business group traffic flows
- Integrating with firewalls functioning at the hypervisor level to protect virtualized applications and enable security policy enforcement in a consistent fashion throughout the solution



- Deploying provider and business group edge firewalls to protect the business group and tenant perimeters

For more details refer to **Network security** and the *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Security Management Solution Guide*.

### Security

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

The solution addresses the challenges of securing authentication and configuration management to comply with industry and regulatory standards through:

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

### VMware NSX for vSphere

The EMC Enterprise Hybrid Cloud can employ NSX for vSphere to offer significant advancements over the vCNS networking and security feature set. Enhanced networking and security features in NSX include:

- **NSX logical routing and firewalls:** Provide line-rate performance distributed across many hosts instead of being limited to a single virtual machine or physical host.
- **Distributed logical routers:** Contain East-West traffic within the hypervisor when the source and target virtual machines reside on the same host.
- **Logical load balancer:** Enables load sharing across a pool of virtual machines with configurable health check monitoring and application-specific rules for service high availability, URL rewriting, and advanced Secure Sockets Layer (SSL) handling. A distributed firewall enables consistent data-center-wide security policies.
- **Security policies:** Can be applied directly to security groups enabling greater flexibility in enforcing security policies.





## Workload-optimized storage

This solution enables customers to take advantage of the proven benefits of EMC storage in an EMC Enterprise Hybrid Cloud environment. Using EMC ViPR storage services and ExtremIO, VNX, and VMAX capabilities, this solution provides policy-based, software-defined storage management of EMC block and file storage.

With a scalable storage architecture that uses the latest flash and tiering technologies, ExtremIO, VNX, and VMAX storage arrays enable customers to satisfy any workload requirements with maximum efficiency and performance, in the most cost-effective way. With ViPR the storage configuration is abstracted and presented as a single storage control point, enabling cloud administrators to access all heterogeneous storage resources within a data center as if they were a single large array.

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

## Elasticity and service assurance

This solution uses a combination of tools to provide environmental visibility and alerts required to proactively ensure service levels in virtual and cloud environments. Using vCAC and tools provided by EMC, administrators and end users can dynamically add resources as needed, based on their performance requirements.

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

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

## Monitoring and resource management

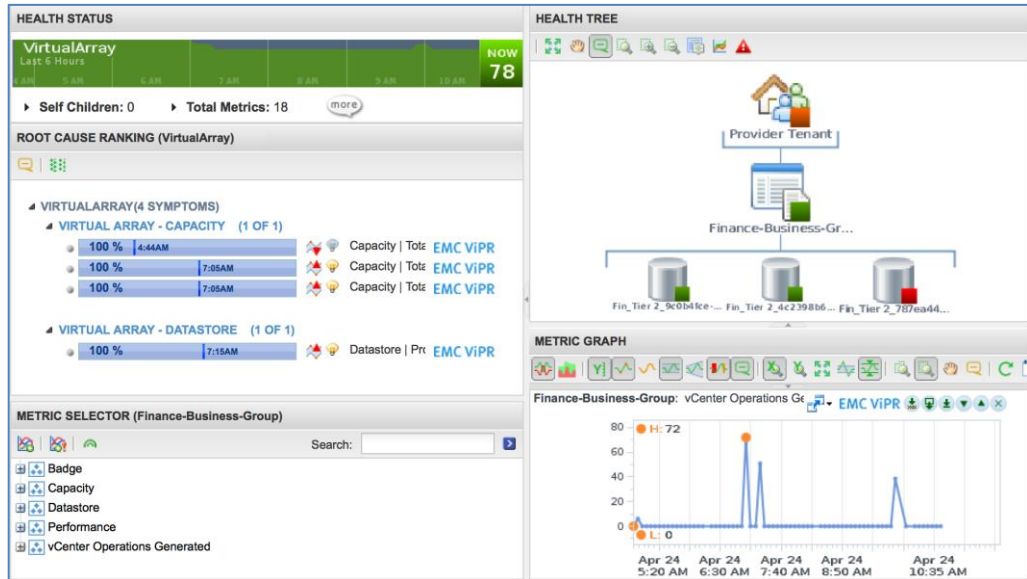
This solution features automated monitoring capabilities that provide IT administrators with a comprehensive view of the cloud environment to enable intelligent decision making for resource provisioning and allocation. These capabilities are based on a combination of VMware vCenter Operations Manager (vC Ops) dashboards, alerts, and analytics, using extensive storage detail provided through EMC analytics adapters for ViPR, VNX, and VMAX.

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



Analytics enables full end-to-end visibility of the entire infrastructure, from virtual machine to LUN and every point in between.

The ViPR Analytics and EMC Storage Analytics (ESA) packs are presented through the vC Ops custom interface. This enables administrators to quickly identify the health of EMC ViPR virtual arrays, physical EMC VMAX, VNX, and VPLEX arrays using customized EMC dashboards for vC Ops, such as the EMC ViPR dashboard shown in Figure 4.



**Figure 4. EMC ViPR Analytics with VMware vCenter Operations Manager**

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

EMC ViPR SRM offers comprehensive monitoring and reporting for this hybrid cloud solution that helps IT visualize, analyze, and optimize their software-defined storage infrastructure. Cloud administrators can use ViPR SRM to understand and manage the impact that storage has on their applications and view the topologies of their hybrid cloud from application to storage. Capacity and consumption of EMC ViPR software-defined storage and SLA issues can be identified through real-time dashboards or reports in order to meet the needs of the wide range of hybrid cloud consumers.

In addition, VMware vCenter Log Insight provides the ability to centralize and aggregate system and application logs. Each system in the hybrid cloud solution can be configured to forward logs to the Log Insight system for event analytics and reporting. When configured with vCenter Log Insight, EMC content packs for Avamar, VNX, and VMAX provide customizable dashboards and user-defined fields specifically for those EMC products, which enable administrators to conduct problem analysis and analytics on the storage array and backup infrastructure.

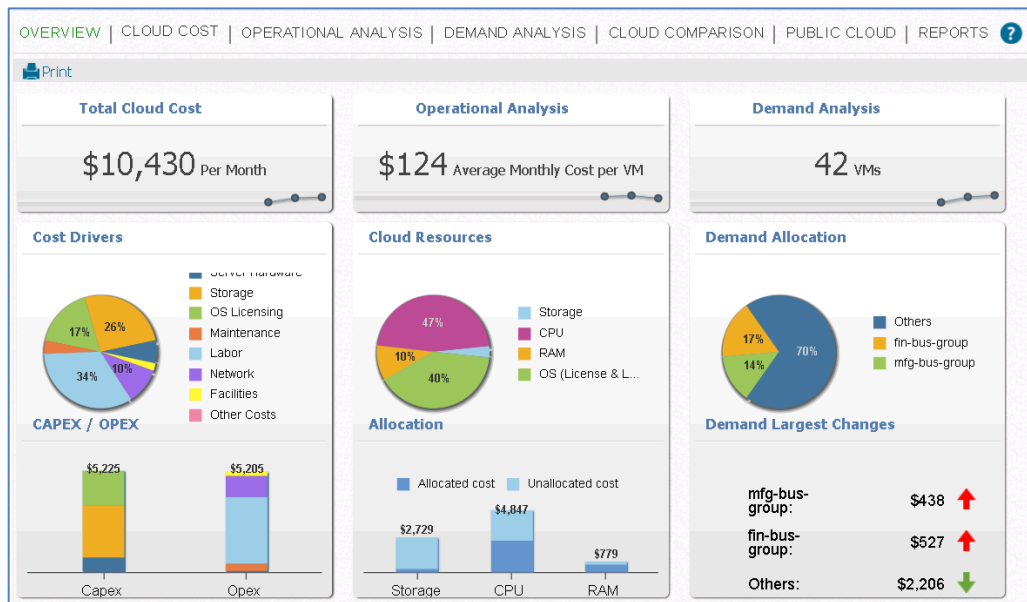


## Metering and chargeback

The solution uses VMware IT Business Management (ITBM) Suite to provide cloud administrators with metering and cost information across all business groups in the enterprise. ITBM reports the virtual machine and blueprints costs based on business units and application groups across the hybrid cloud environment.

VMware ITBM Standard Edition uses its own reference database, which has been preloaded with industry-standard and vendor-specific cost data to compute the cost of virtual CPU (vCPU), RAM, and storage. These prices, which default to cost of CPU, RAM, and storage, are automatically consumed by vCAC, where the cloud administrator can change them as appropriate. This eliminates the need to manually configure cost profiles in vCAC and assign them to compute resources.

ITBM is integrated into the vCAC portal for the cloud administrator and presents a dashboard overview of the hybrid cloud infrastructure, as shown in Figure 5.



**Figure 5. ITBM Suite overview dashboard for hybrid cloud**

ITBM is also integrated with VMware vCenter and can import existing resource hierarchies, folder structures, and vCenter tags to associate hybrid cloud resource usage with business units, departments, and projects.



## Modular add-on components

### Application services

The EMC Enterprise Hybrid Cloud uses VMware vCloud Application Director™ to optimize application deployment and release management through logical application blueprints in vCAC. A drag-and-drop user interface lets you quickly and easily deploy blueprints for applications and databases such as Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint, Oracle, SAP, and Cloud Foundry.

### Data protection services

Using EMC customized vCenter Orchestrator workflows, administrators can quickly and easily set up multitier data protection policies that users can assign when provisioning their virtual machines. The backup infrastructure takes advantage of Avamar and Data Domain features such as deduplication, compression, and VMware integration.

Avamar provides scalable backup and restore capabilities with integrated data deduplication, which reduces total disk storage by up to 50 times and enables cost-effective, long-term retention on Avamar Data Store servers. Avamar can alternatively use a Data Domain appliance as the backup target.

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

With this solution, enterprise administrators can offer IaaS with EMC backup to end users who want a flexible, on-demand, automated backup infrastructure without having to purchase, configure, or maintain it.

### Continuous availability

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

### Disaster recovery

The EMC Enterprise Hybrid Cloud enables cloud administrators to select DR protection for their applications and virtual machines when deploying from the vCAC self-service catalog. EMC ViPR automatically places these systems on storage that is protected remotely by EMC RecoverPoint. VMware vCenter Site Recovery Manager™, through tight integration with the EMC RecoverPoint Storage Replication Adapter (SRA), can automate the recovery of all virtual storage and virtual machines at a recovery or failover site.



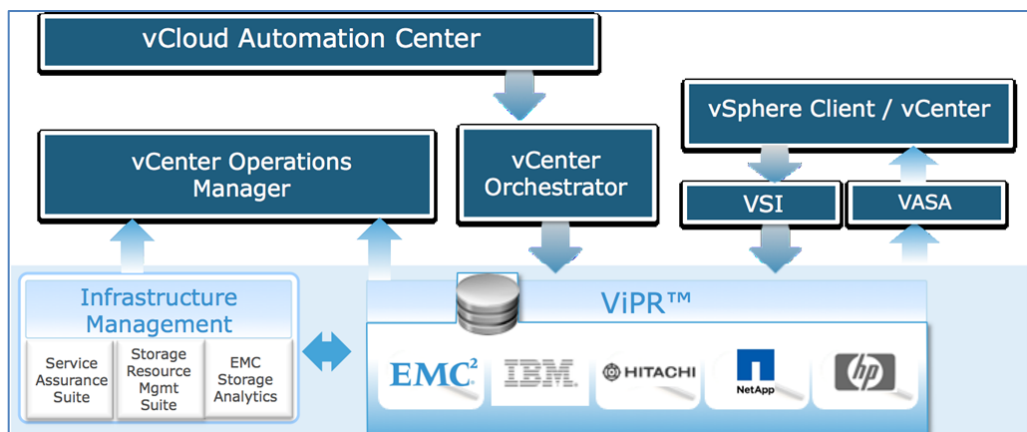
## Public cloud services

This EMC Enterprise Hybrid Cloud solution enables IT organizations to broker public cloud services. This solution has been validated with VMware vCloud Air as a public cloud option that can be accessed directly from the solution's self-service portal by administrators and users. End users can provision virtual machines while IT administrators can perform virtual machine migration (offline) from the on-premises component of their hybrid cloud to vCloud Air using VMware vCloud Connector®.

## EMC and VMware integration

This EMC Enterprise Hybrid Cloud solution contains many integration points between EMC and VMware products. This section highlights some of the key integration points and what they mean to the overall solution.

Some of the EMC ViPR-based integration points are shown in Figure 6.



**Figure 6. EMC ViPR integration points with VMware**

## Storage services

While managed by ViPR, VNX and VMAX storage arrays both support VMware vSphere Storage APIs—Array Integration (VAAI), which offloads ESXi host operations to the arrays to optimize server performance.

The ViPR Storage Provider integrates ViPR with VMware vSphere Storage API for Storage Awareness™ (VASA). This enables vCenter to collect and report the storage capabilities of ViPR-provisioned datastores. Administrators use the VASA information to make intelligent placement decisions and optionally configured virtual machine and datastore service-level storage policies.

All VMware vSphere ESXi servers run EMC PowerPath/VE for automatic path management and I/O load balancing in the SAN. EMC PowerPath/VE automates failover and recovery and optimizes load balancing of data paths in virtual environments to ensure availability, performance, and the ability to scale-out mission-critical applications.



**Orchestration** The ViPR plug-in for VMware vCenter Orchestrator (vCO) provides an orchestration interface to the EMC ViPR software platform. The EMC ViPR plug-in has pre-packaged workflows that automate common ViPR operations such as Virtual Machine File System (VMFS) or Network File System (NFS) datastore provisioning. The EMC ViPR plug-in is installed in the vCO configuration interface.

**Operational management and monitoring** The EMC ViPR Analytics pack for vC Ops provides advanced metrics for virtual resources at the EMC ViPR virtual array and virtual pool level. The ESA adapter for EMC VNX, VMAX, and VPLEX provides preconfigured dashboards for VMware vC Ops users to view storage metrics and topologies of the individual storage components beneath EMC ViPR.

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

**Metering** EMC ViPR Storage Provider plays a key role in this solution in identifying the capabilities of the storage presented to ESXi servers managed by vCenter. A storage profile is created in vCenter for each class, or tier, of storage presented by ViPR. These storage profiles are used by VMware ITBM to classify and charge for each tier of storage presented and consumed in vCAC.

## Summary

This solution enables customers to build an enterprise-class, scalable, multitenant platform for complete management of their compute service lifecycle. This solution provides on-demand access and control of compute resources and security while enabling customers to maximize asset use. Specifically, this solution integrates all of the key functionality that customers demand, and provides a framework and foundation for adding other services.

This solution supports a VMware vCloud Suite stack with EMC storage and data protection services, providing the flexibility to deliver cloud-based services with the functionality EMC customers expect.



## Chapter 3 Solution Architecture and Design

This chapter presents the following topics:

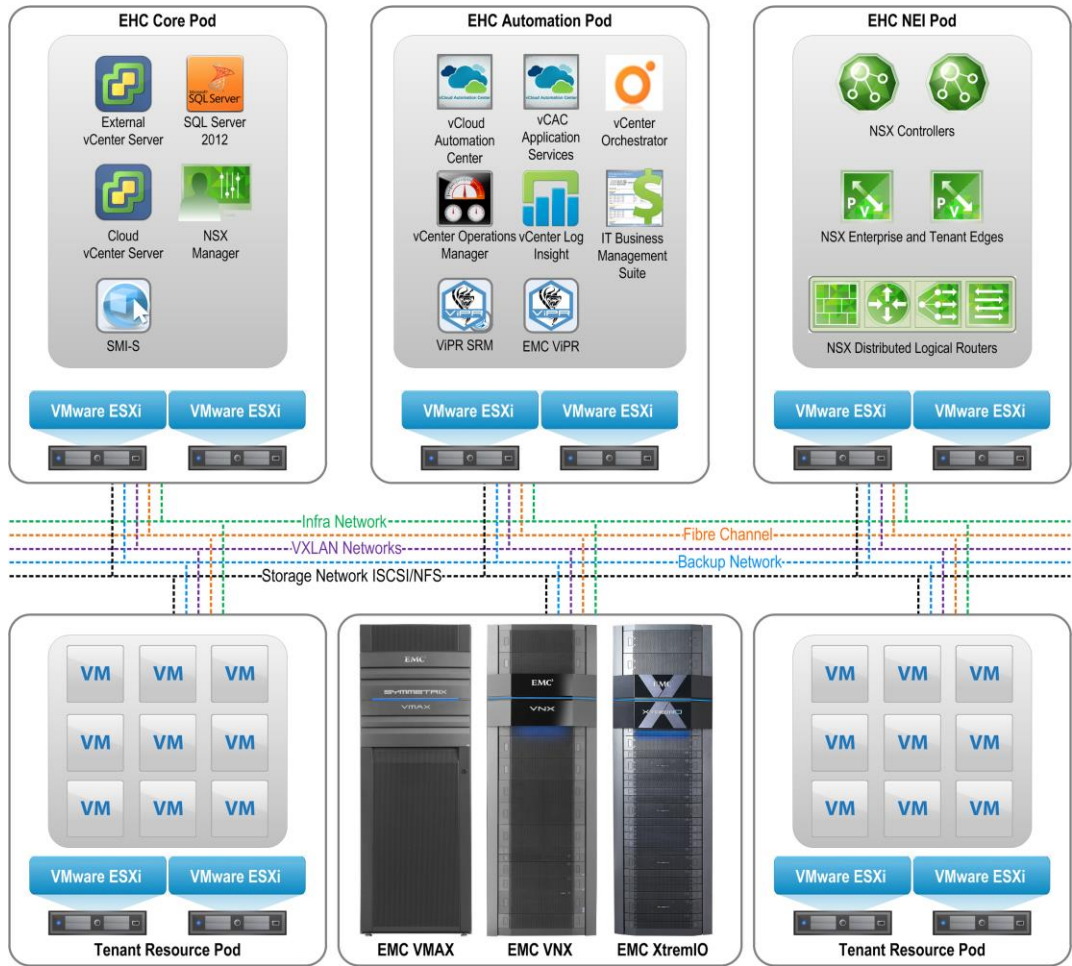
<b>Solution architecture</b> .....	<b>32</b>
<b>Solution design</b> .....	<b>37</b>
<b>EMC Enterprise Hybrid Cloud software resources</b> .....	<b>44</b>
<b>EMC Enterprise Hybrid Cloud sizing</b> .....	<b>44</b>



## Solution architecture

### Hybrid cloud architecture

This section describes the EMC Enterprise Hybrid Cloud architecture. Figure 7 shows the solution architecture.



**Figure 7. EMC Enterprise Hybrid Cloud solution architecture**

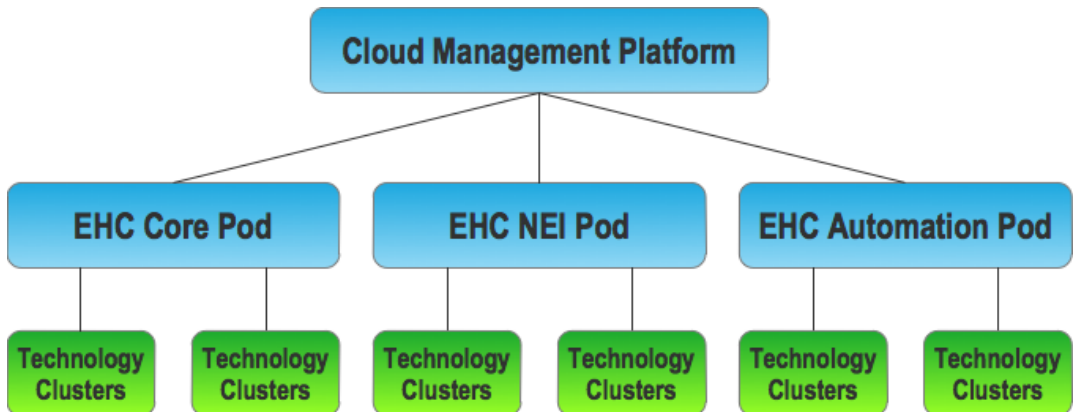
The cloud management platform supports the entire management infrastructure for this solution. The infrastructure is divided into pods, which consist of one or more ESXi clusters. The EHC solution includes several pods, which perform solution-specific functions and are used to provide high availability and load balancing.

vSphere ESXi clusters configured in High Availability mode provide virtual machine protection. Increased levels of fault tolerance are provided through application and operating system cluster services, such as Windows Failover Clustering, PostgreSQL clustering, load balancer clustering, or farms of machines that work together natively to provide a resilient architecture.





Figure 8 is a relationship model of the management platform and the pods, and clusters in the solution. It is helpful to understand these relationships before proceeding through the rest of the document.



**Figure 8. Cloud management terminology and hierarchy**

The architecture for the solution, displayed in Figure 8, requires four sets of resources:

- EHC Core Pod
- EHC Network Edge Infrastructure (NEI) Pod
- EHC Automation Pod
- Tenant Resource Pods: resources to be consumed by the business groups

These pods have a hierarchical dependency and they should be installed in the order listed above.

### EHC Core Pod

The Core Pod provides the base set of resources to establish the EMC Enterprise Hybrid Cloud solution services. It is primarily an infrastructure pod that consists of:

- **Cloud VMware vCenter Server:** This vCenter instance is used to manage the EHC, NEI, and Automation pods/clusters. VMware vCAC uses this vCenter Server as its endpoint from which the appropriate ESXi clusters are reserved for use by vCAC business groups.
- **Microsoft SQL Server:** Hosts the respective SQL Server databases used by the Cloud vCenter Server, VMware Update Manager™, and VMware vCAC IaaS databases.
- **NSX/vCNS Manager:** Used to deploy and manage the Tenant Resource Pod and the management infrastructure virtual networks.
- **EMC SMI-S:** Management infrastructure required for EMC ViPR deployment.

The Core Pod is also an ESXi cluster that needs to be configured into an existing vCenter Server instance. This external vCenter Server instance is also shown in the



EHC Core Pod (Figure 7), but may exist elsewhere, depending on the chosen deployment.

The following scenarios fulfill this deployment:

- In a brownfield customer environment, an existing vCenter Server can be used to host the Core Pod resources and no additional hardware resources are required. In this brownfield scenario, the EHC Core Pod, shown in Figure 7, already exists or is deployed to an existing vCenter Server.
- In a greenfield environment, a distinct set of hardware resources are deployed and configured to support the Core Pod. In this scenario, an ESXi server cluster is deployed, and virtual machines are created for both the SQL Server and external vCenter Server instance at a minimum.

When the external vCenter Server instance is functional, the ESXi host it resides on, and any other hosts that are to be used in the EHC Core Pod, can be brought under vCenter management. The remaining virtual machines are then deployed and configured. These resources are shown in Figure 7 as a dedicated EHC Core Pod.

The hardware hosting the EHC Core Pod is not under cloud management, but the virtual machines it hosts provide the critical services for the cloud.

All of the virtual machines on the EHC Core Pod are deployed on non-ViPR storage. The virtual machines can use existing SAN connected storage or any highly available storage in the customer environment. If provisioning from an EMC storage system, the EMC Virtual Storage Integrator (VSI) tool for the vSphere Web Client can be used to create and manage the devices supporting the EHC Core Pod.

The EMC Hybrid Cloud supports Fibre Channel, iSCSI, and NFS storage from EMC VNX Storage Systems. Though not mandatory, Fibre Channel connectivity between the EHC Core Pod and the EMC Enterprise Hybrid Cloud array is strongly recommended. All storage should be RAID protected and all ESXi servers should be configured with EMC PowerPath/VE for automatic path management and load balancing.

### **EHC Network Edge Infrastructure (NEI) Pod**

The EHC NEI Pod is used to host all of the North-South VMware vCloud networking and security Edge components of the virtualized network. If NSX is used, it also hosts the NSX Controller appliances. This pod provides the convergence point for the physical and virtual networks.

The NEI Pod uses dedicated vSphere clusters to simplify the configuration required to connect the physical and virtual networks. It also eliminates the critical networking components competing for resources as the solution scales, and the demands of other areas of the cloud management platform increase.

Storage for this pod can be provisioned with the EMC VSI tool. Like the EHC Core Pod, the plug-in on the vSphere Web Client connects to the cloud vCenter Server. Storage for this pod should be RAID protected and Fibre Channel connections are recommended. ESXi hosts should run EMC PowerPath/VE for automatic path management and load balancing.



Refer to **EMC Enterprise Hybrid Cloud sizing** for NEI pod sizing guidelines.

### **EHC Automation Pod**

The EHC Automation Pod hosts all of the virtual machines used for automating and managing the cloud infrastructure, except for services installed in the Core Pod. The Automation Pod supports the services responsible for functions such as the user portal, automated provisioning, monitoring, and metering. The Automation Pod hardware is registered with the Cloud vCenter Server instance; however it is dedicated to automation and management services. Therefore the hardware resources from this pod are not exposed to vCAC business groups.

The Automation Pod requires a number of VMware vSphere ESXi hosts configured in a vSphere cluster using VMware vSphere Distributed Resource Scheduler™ (DRS) and VMware vSphere HA. This vSphere cluster does not share host, network, or storage resources with the production resource clusters. Storage provisioning for the Automation Pod follows the same guidelines as the EHC NEI Pod. Refer to **EMC Enterprise Hybrid Cloud sizing** for cloud management platform sizing guidelines.

The minimum set of components for the Automation Pod is listed as follows. The Automation Pod may contain additional items such as load balancers if required.

- VMware vCloud Automation Center Virtual Appliance
- VMware IT Business Management Suite
- VMware vCloud Automation Center IaaS roles
- EMC PowerPath/VE Manager
- VMware vCenter Orchestrator
- EMC ViPR Controllers
- VMware vCenter Operations Manager
- EMC ViPR Storage Resource Manager (SRM)
- VMware vCenter Log Insight

### **Tenant Resource Pods**

Tenant Resource Pods are configured and assigned to fabric groups in vCAC. Available resources are used to host virtual machines deployed by business groups in the EMC Enterprise Hybrid Cloud environment. All business groups share the available vSphere ESXi cluster resources.

Server, network, and storage resources for existing Tenant Resource Pods are easily modified. Once new resources have been made available to vSphere, a new vCAC data collection and appropriate resource reservation changes make the new resources available for consumption.

EMC ViPR service requests are initiated from the VMware vCAC catalog to provision Tenant Resource Pod storage.

All storage provisioned by EMC ViPR is connected using Fibre Channel, where the SAN zoning can be manually configured in advance or automatically configured by ViPR at



deployment time. When manual zoning is chosen, best practices for high availability should be implemented to provide HA on the server and the storage arrays. All ESXi servers run EMC PowerPath/VE for automatic path management and load balancing.

Refer to **EMC Enterprise Hybrid Cloud sizing** for tenant resource cluster sizing guidelines.

### **Solution connectivity**

The solution uses the following networks:

- **Fibre Channel:** Provides block storage connectivity between the hosts and the EMC storage systems
- **Infrastructure network:** All the hardware components of the solution are connected to it
- **Management network:** Where all of the cloud management virtual machines are connected
- **Business group networks:** Dedicated networks per business group

### **Architectural assumptions**

The following assumptions and justifications apply to the EMC Enterprise Hybrid Cloud architecture:

- The vCenter Server full installation is used for the following reasons:
  - Enables the use of vCenter Server Heartbeat and vCenter Server HA
  - Provides support for an external Microsoft SQL Server database
  - Resides on a Windows System that also supports the VMware Update Manager (VUM) service
- vCenter Single Sign-On (SSO) is used instead of vCAC identity appliance because it enables SSO to be made highly available in tandem with vCenter Server. SSO is configured independently on each vCenter Server instance, with vCAC and vCO integrating with the Cloud vCenter SSO server.



## Solution design

### Tenant design

User groups, roles, responsibilities and entitlements are used throughout VMware vCAC. The administration of users and compute resources in vCAC is managed through the vCAC console, which is the administrative portal.

The primary vCAC groups, users, and roles that this solution focuses on are summarized as follows:

- IaaS administrators
- Fabric group administrators
- Business group administrators/users

A primary task of an IaaS administrator is to configure the infrastructure endpoints which vCAC uses for provisioning compute resources and operations. These endpoints include on-premises resources such as VMware vCenter and vCO, and off-premises endpoints such as VMware vCloud Air or Amazon Web Services (AWS). The endpoints provide the compute resources, which can be assigned to a single or multiple fabric groups. vCAC enables compute resources to be divided into logical units and shared across multiple business groups, as shown in Figure 9.

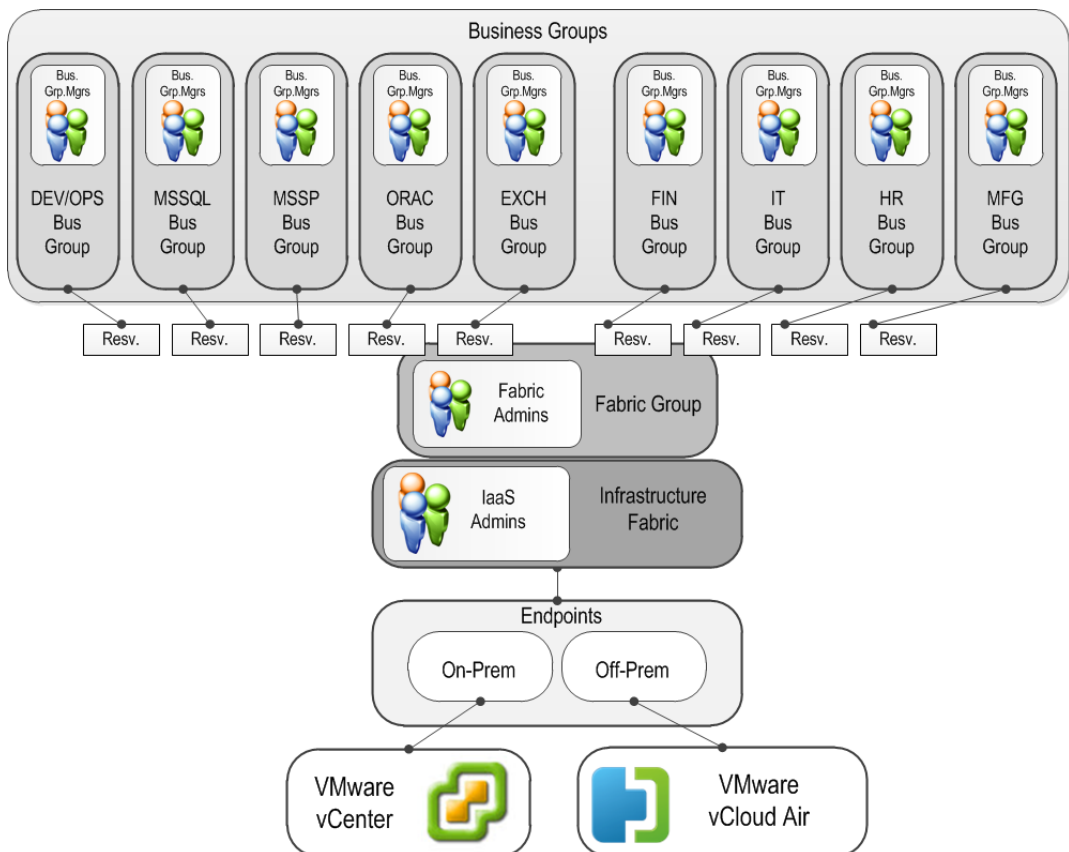
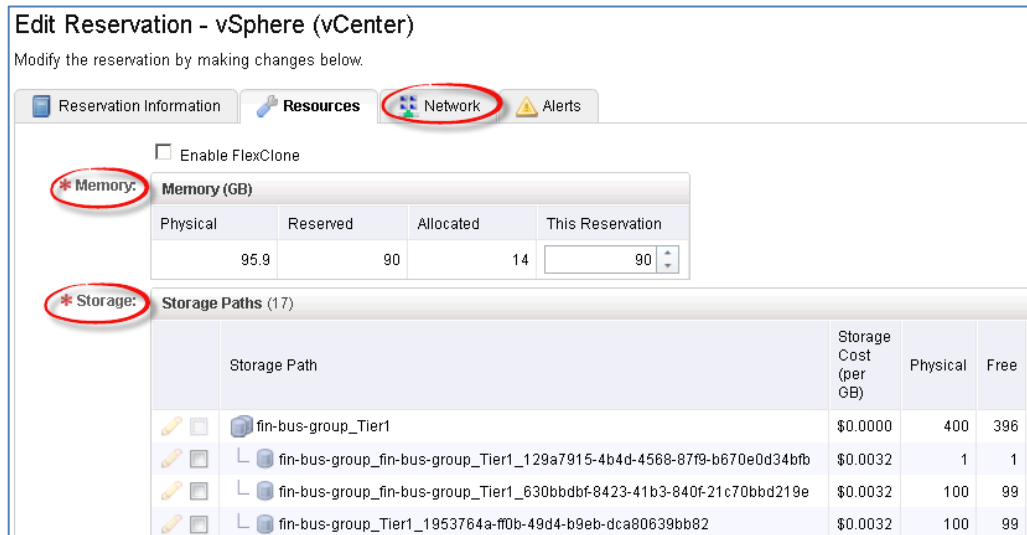


Figure 9. Software-defined data center tenant design and endpoints



Fabric group administrators manage cloud resources for their respective business groups, as defined by the infrastructure administrator. As shown in Figure 10, fabric group administrators can reserve memory, storage, and network resources for their business groups using reservation policies.



**Figure 10. Business group resource reservations**

The compute resources supporting the various business groups as presented from the vCenter Server endpoint for vCAC can be shared between the various business groups using capacity reservations and policies.

Business group members are the users and consumers of the infrastructure provided to them by their fabric group administrator. The business group manager and users are the primary consumers in this group:

- **Business group manager:** Can access all virtual machines, create and publish blueprints for end users, manage approval requests, and work on behalf of other users in their group.
- **User role:** These users are the vCAC end users. They can deploy from blueprints the business group manager has made them entitled to.

Users with a business group user role are the primary consumers of the vCAC self-service portal. They can use the portal to provision and manage their virtual machines. Users and groups can be created in an Active Directory server and assigned to support the various roles in vCAC, as described in the *vCloud Automation Center Installation Guide*.

---

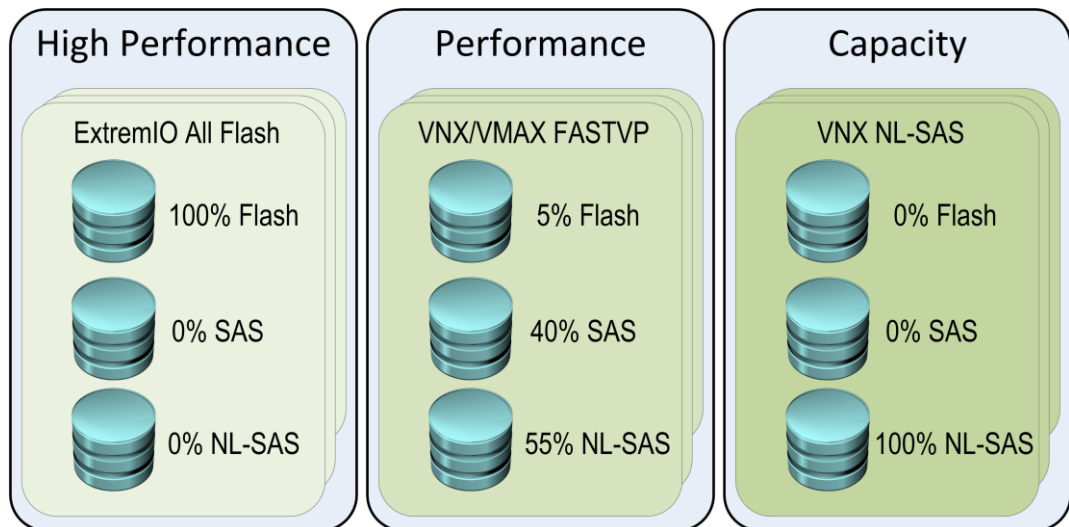
**Note:** This EMC Enterprise Hybrid Cloud solution uses a single EMC ViPR tenant with a ViPR project created to correspond to each VMware vCAC tenant.

---



## Storage design and consumption

This EMC Enterprise Hybrid Cloud solution presents storage in the form of storage service offerings that greatly simplify virtual storage provisioning. The storage service offerings are based on ViPR virtual pools, which are tailored to meet the performance requirements of general IT systems and applications. Multiple array storage pools, consisting of different disk types, are configured and brought under ViPR management. ViPR presents the storage as virtual storage pools by abstracting the underlying storage details and allowing provisioning tasks to be aligned with the application's class of service. This storage service offering concept is summarized in Figure 11.



**Figure 11. Storage service offerings for the hybrid cloud**

**Note:** The storage service offerings in Figure 11 are suggestions only. Storage service offerings can be configured and named as appropriate to reflect their functional use.

Each ViPR virtual pool representing a storage service offering can be supported or backed by multiple storage pools of identical performance and capacity on the storage back end.

The storage service offerings suggested in Figure 11 can be configured as follows:

- **High Performance** provides ExtremIO, all-flash storage, supported by multiple ExtremIO storage pools.
- **Performance** provides EMC VNX block or file-based VMFS or NFS storage devices and is supported by multiple storage pools using FAST VP and FAST Cache.
- **Capacity** provides EMC VNX block- or file-based VMFS or NFS storage and is supported by multiple storage pools using a single storage type of NL-SAS.

These storage service offerings are suggested only to highlight what is possible in this EMC Enterprise Hybrid Cloud environment. Many other storage service offerings can be configured to suit business and application needs as appropriate. Refer to

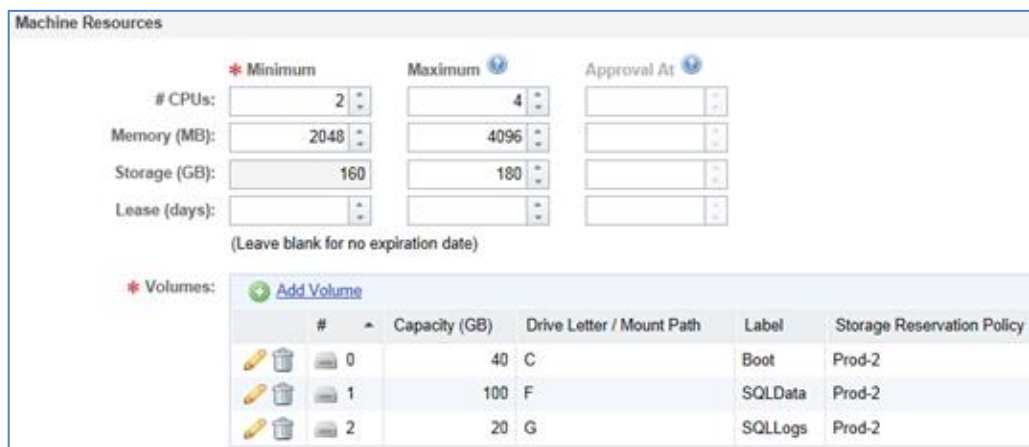


**EMC Enterprise Hybrid Cloud sizing** for information on calculating and sizing storage pools to support storage service offerings.

VMware vCAC provides the framework to associate one or more classes of storage with each line of business so that they can be consumed through the service catalog. Initially, the physical storage pools are configured on the physical storage array and made available to the EMC ViPR virtual array where they are configured into their respective virtual pools. At provisioning time, LUNs or file systems are configured from these virtual pools and presented to vSphere as VMFS or NFS datastores. The storage is then discovered by vCAC and made available for assignment to business groups within the enterprise.

This storage service offering approach greatly simplifies the process of storage administration. Instead of users having to configure the placement of individual virtual machine disks (VMDKs) on different disk types such as SAS and FC, they simply select the appropriate storage service level required for their business need. Virtual disks provisioned on FAST VP storage benefit from the intelligent data placement. While frequently accessed data is placed on disks with the highest level of service, less frequently used data is migrated to disks reflecting that service level.

When configuring virtual machine storage, a business group administrator can configure blueprints to deploy virtual machines onto any of the available storage service levels. In the example in Figure 12, a virtual machine can be deployed with a single machine blueprint hosting a SQL Server database, which supports an application with performance requirements suitable for a storage service offering named Prod-2.



**Figure 12. Blueprint storage configuration in vCAC**

The various devices for this SQL Server database machine have different performance requirements, but rather than assigning different disk types to each individual drive, each virtual disk can be configured on the Prod-2 storage service offering. The vCAC storage reservation policy ensures that the VMDKs are deployed to the appropriate storage.





This solution supports the ability to pin all storage devices in a virtual machine blueprint to a single storage service offering, and the ability to manually place virtual disks on multiple storage service offerings if required.

The storage service offerings made available to vCAC can be shared and consumed across the various business groups using the capacity and reservation policy framework in vCAC.

## Network design

This solution provides a network architecture design that is resistant to failure, provides for optimal throughput for workloads, and ensures multitenancy and secure separation. The network and security architecture is designed for either of two deployment options, VMware vCNS, or NSX for vSphere. The network services showcased in this solution with VMware vCAC are supported with both vCNS and NSX.

Table 2 lists the edge networks configured to support this solution.

**Table 2. Edge network connectivity**

Name	Configured	Purpose
ESXi Management	ESXi host	Management of ESXi hosts
EHC Automation	Management Virtual distributed switch (vDS)	Network hosting EHC Automation and Core Pod virtual machines
vMotion	ESXi host	Migration of workloads
NFS	ESXi host	Network

### Supporting infrastructure services

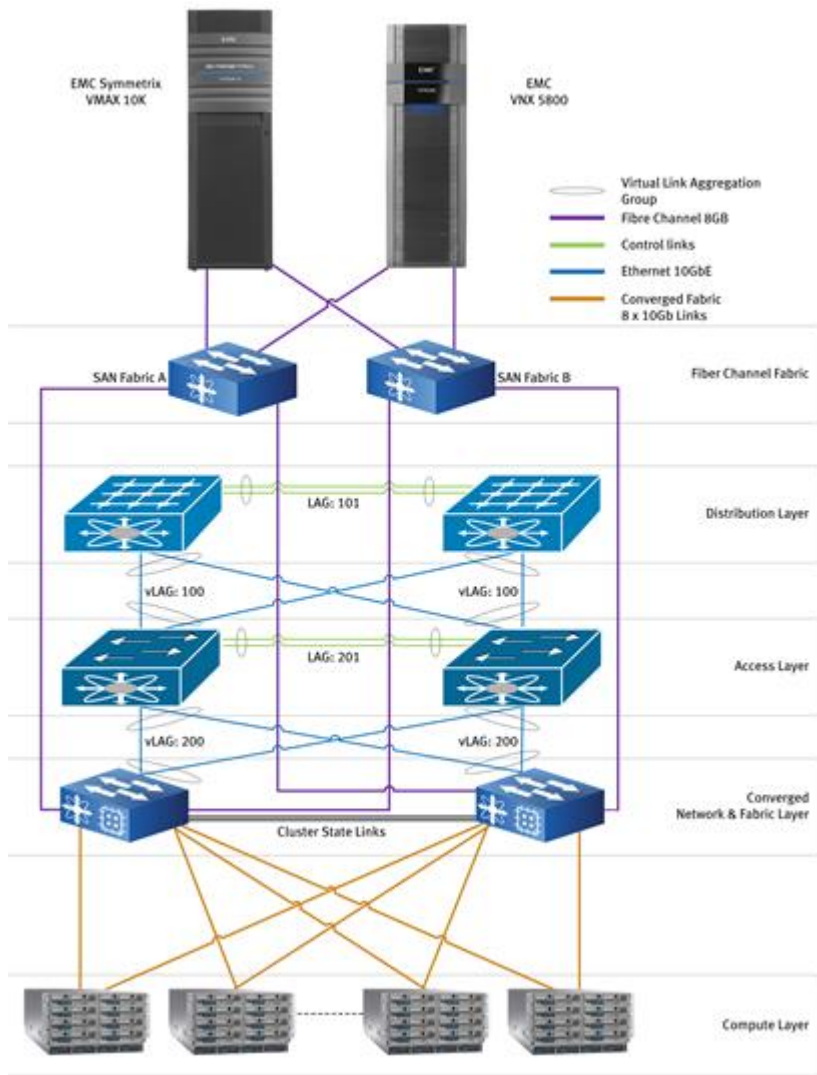
To support infrastructure operations, each ESXi host in the environment is configured with VMkernel interfaces for NFS and vMotion.

### Physical connectivity

In designing the physical architecture, the main considerations were high availability, performance, and scalability. Each layer in the architecture is fault tolerant with physically redundant connectivity throughout. The loss of any one infrastructure component or link does not result in loss of service to the tenant; if scaled appropriately, there is no impact on service performance.

Figure 13 shows the connectivity between the physical storage, network, and converged fabric components deployed in this EMC Enterprise Hybrid Cloud solution.





**Figure 13. Physical topology of the network**

In this environment, physical network and Fibre Channel connectivity to the compute layer is provided over a converged network and fabric to converged network adapters on each compute blade. Each link is capable of 10 Gb/s. This enables up to eight 10 GbE network interfaces to be presented to each ESXi host.

**Logical network topology**

The logical topology is designed to address the requirements of multitenancy and secure separation of the tenant resources. It is also designed to align with security best practices, from vendors such as VMware, for segmenting networks according to the purpose or traffic type.



Figure 14 shows a logical representation of the EMC Enterprise Hybrid Cloud environment and highlights the management platform, tenant resource pods, and clusters.

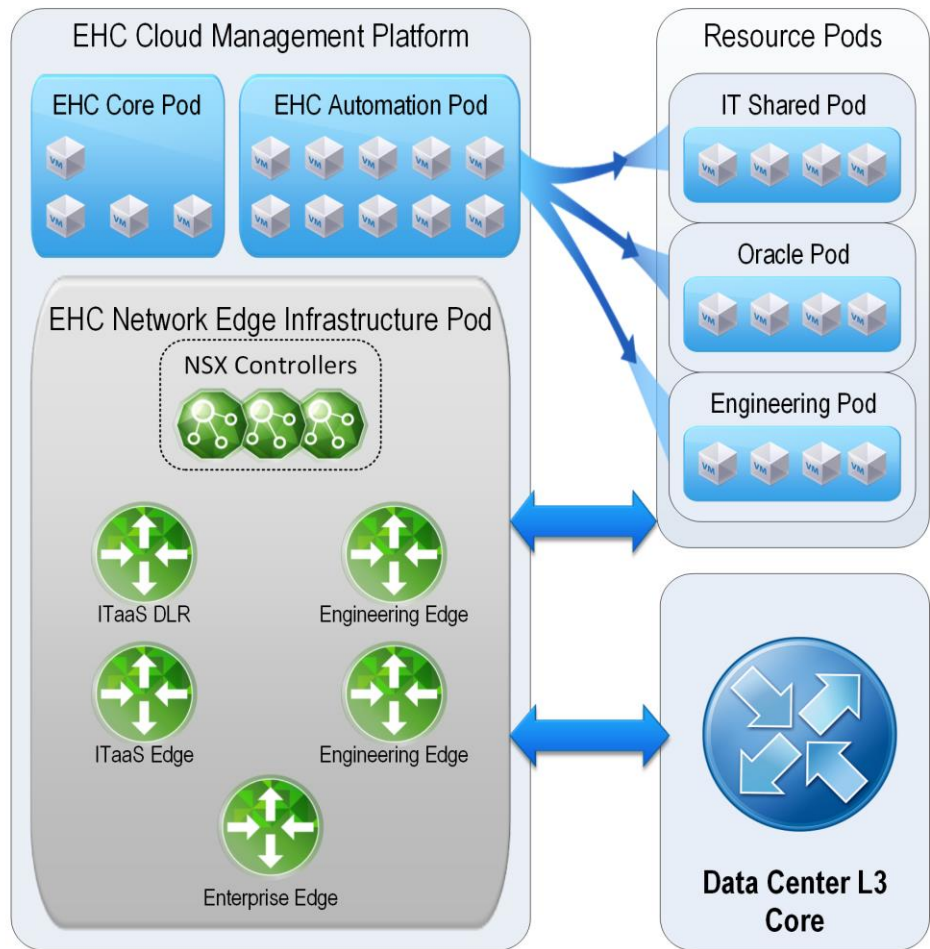


Figure 14. Logical network overview



## EMC Enterprise Hybrid Cloud software resources

Refer to the EMC ELab EMC Simple Support Matrix (ESSM) for up-to-date supported code versions:

[https://elabnavigator.emc.com/vault/pdf/EMC\\_Hybrid\\_Cloud\\_2.5\\_ESSM.pdf](https://elabnavigator.emc.com/vault/pdf/EMC_Hybrid_Cloud_2.5_ESSM.pdf). The EMC Support Matrix home is <https://elabnavigator.emc.com/eln/elhome>.

---

**Note:** Refer to VMware KB Article 1014508 for correlating VMware product build numbers to update levels.

---

### Important notice - ShellShock/Bash security vulnerability

Refer to the EMC and VMware websites for advisories on patching updates for components affected by the GNU Bash Shellshock security vulnerability.

- [\*Bash Code Injection Vulnerability \(ShellShock/BashBug\) in EMC products\*](#)
- [\*VMware remediation of Bash Code Injection Vulnerability via Specially Crafted Environment Variables KB: 2090740\*](#)

## EMC Enterprise Hybrid Cloud sizing

Refer to the EMC Mainstay sizing tool for all EMC Enterprise Hybrid Cloud sizing operations, available at <https://mainstayadvisor.com/go/emc>.



# Chapter 4 Cloud Services

This chapter presents the following topics:

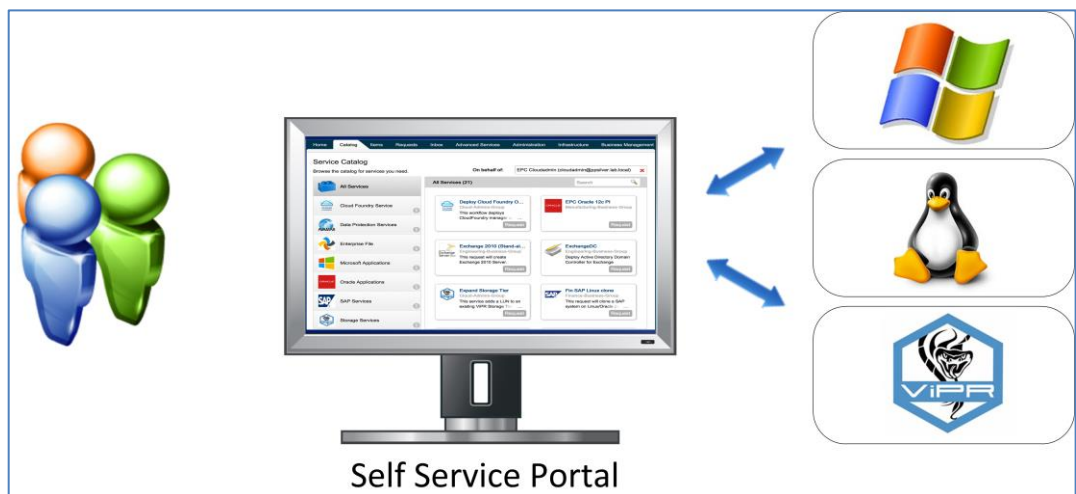
<b>Self-service catalog .....</b>	<b>46</b>
<b>Virtual machine lifecycle services .....</b>	<b>47</b>
<b>Storage services .....</b>	<b>57</b>
<b>Networking services.....</b>	<b>64</b>



## Self-service catalog

VMware vCloud Automation Centre (vCAC) provides a unified self-service portal, as shown in Figure 15, for delivering infrastructure, application, data, or anything as a service (XaaS).

A service catalog of customized and approved services and applications is presented to users of this EMC Enterprise Hybrid Cloud solution. These catalog items are the result of pre-engineered storage and infrastructure services that have been customized to meet the many needs of the business. All of the service specifications and policies can be preconfigured and approved by cloud administrators, enabling end users to provision, manage, and dispose of their own systems.



**Figure 15. Self-service portal and service catalog overview**

The self-service portal, using existing and specialized customization processes, offers cloud users a range of cloud operations, including:

- A catalog of storage and data protection services
- A catalog of systems and applications
- Streamlined deployment of systems and applications
- Automatic protection of business and mission-critical machines
- On-demand backup, restore, and billing operations<sup>1</sup>

Users can execute simple and efficient processes that satisfy their requirements, without the need to administer the underlying technologies and services within the hybrid cloud.

<sup>1</sup> Backup and recovery data protection functionality is a modular add-on to this EHC foundational infrastructure and its details are not within the scope of this document. For details refer to the *EMC Enterprise Hybrid Cloud 2.5, Federation SDDC: Data Protection Backup Solution Guide*.



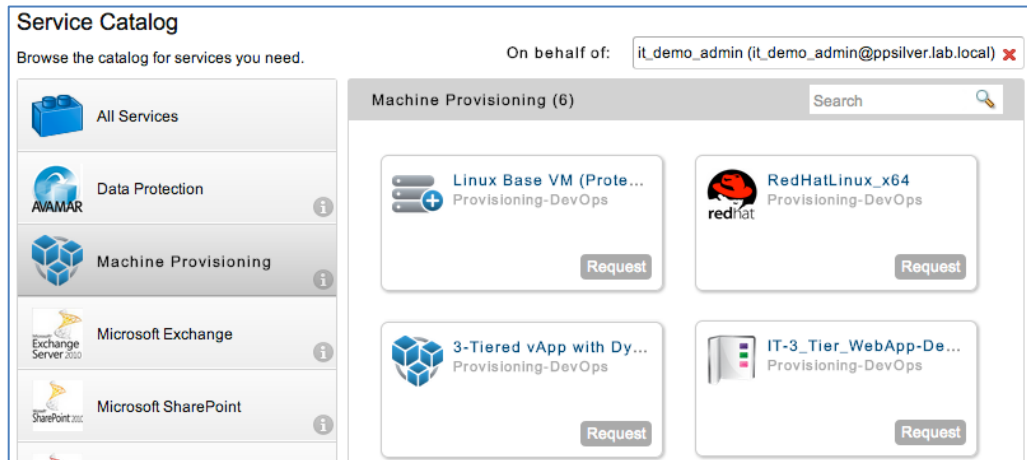
VMware vCAC enables the presentation of personalized, user-appropriate catalogs of IT services through the application of entitlements that define which users have access to each service. For example, storage services are only available to vCAC IaaS administrators so that they can configure and manage storage service offerings. Similarly, vCAC business group users only see virtual machine provisioning services within their catalog, where they can request and provision their own virtual machines.

## Virtual machine lifecycle services

The following use cases provide an overview of some of the more common tasks in the lifecycle of virtual machines in this EMC Enterprise Hybrid Cloud solution.

### Virtual machine blueprints

A blueprint must be created for a virtual machine before it can be provisioned from the vCAC service catalog. A blueprint is the complete specification for a virtual machine, determining the machine's attributes, the manner in which it is provisioned, and its policy and management settings. When users request a machine using the self-service portal, they must select the blueprint from which it will be created, as shown in Figure 16.



**Figure 16. Deploy new virtual machines from available blueprints**

The blueprint sets the policies that apply to a machine, such as any approvals required, expiration date, and owner operations.

Blueprints can be single machine or multimachine, including multitier enterprise applications that require multiple components (application, database, and web). A multimachine blueprint contains multiple individual machine blueprints.



**Use case 1:  
Provision virtual  
machine**

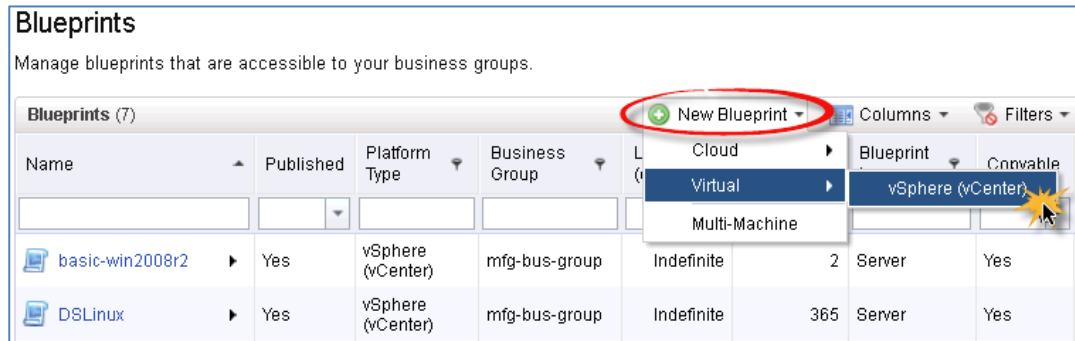
When a virtual machine is provisioned, it is deployed from a vSphere template virtual machine and customized within a vCAC virtual machine blueprint.

Fabric group administrators and business group managers (or a user who is both) can create a global blueprint, which is available to all business groups, or a local blueprint, which is available only to a single business group.

**Create local blueprint**

To create a local blueprint in the vCAC console:

1. Log in as a fabric or business group manager.
2. Select **Infrastructure > Blueprints**.
3. Select **New Blueprint > Virtual**.
4. Select **vSphere (vCenter)**, as shown in Figure 17, to open the **New Blueprint** window.



**Figure 17. Create a new VMware vSphere virtual machine blueprint**

Complete information in the **New Blueprint** window in the following areas:

- Blueprint Information
- Build Information
- Properties
- Actions

Each of the areas contains input fields that combine to define the final blueprint.

**Blueprint Information**

The new blueprint is set as a master blueprint so that it can be copied for subsequent blueprint creations. Other properties, such as reservation policy, business group, and virtual machine name prefix are configured here, as shown in Figure 18.





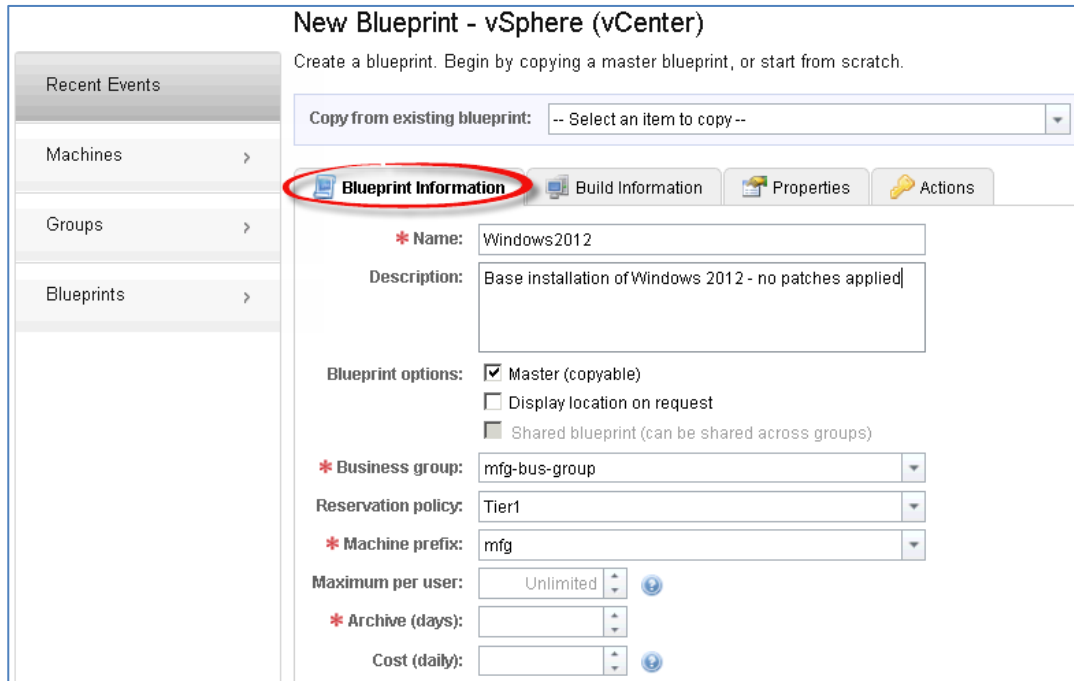


Figure 18. Create a new blueprint

**Build Information**

Under **Build Information**, the blueprint type is **Server** and the action is **Clone**, which means that a cloning workflow is based on an existing template in vSphere. In this example, a number of pre-built Windows and Linux virtual machine templates exist within vSphere. The required template can be selected from the **Clone from** list, as highlighted in Figure 19. In this example, the **Win20GB** template is selected.

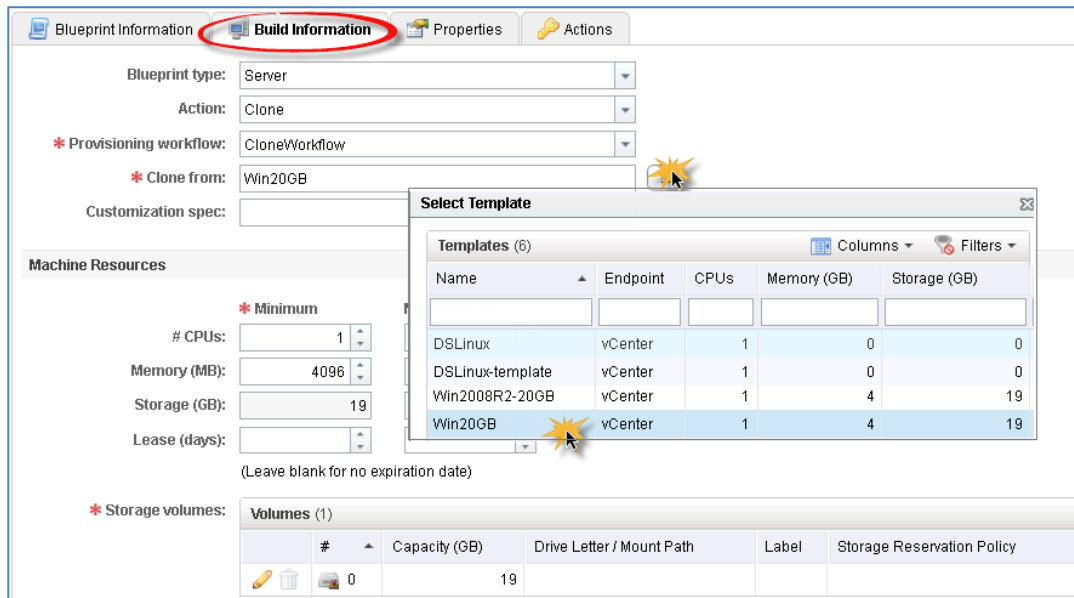


Figure 19. Select vSphere template for cloning



The virtual machine inherits the minimum required resources defined within the virtual machine template. You can set the blueprint to allow these values to be increased to the maximum value at a later time. Figure 20 shows where you can set the machine resources maximum values, and specify the storage service level to be used (Storage Reservation Policy).

The screenshot displays the 'Build Information' configuration page. Under 'Machine Resources', there are two columns: '\* Minimum' and 'Maximum'. The values are: # CPUs (1, 4), Memory (MB) (4096, 8192), Storage (GB) (69, 100), and Lease (days) (blank, blank). Below this is a table for 'Storage volumes' with two entries. The 'Storage Reservation Policy' column is circled in red, showing 'Tier1' for both volumes. A checkbox at the bottom is labeled 'Allow user to see and change storage reservation policies'.

#	Capacity (GB)	Drive Letter / Mount Path	Label	Storage Reservation Policy
0	19		Tier1	Tier1
1	50		Tier1	Tier1

**Figure 20. Complete build information for new blueprint**

In this example, the minimum machine resources are inherited from the vSphere template and the maximum values have been manually set to be higher than the minimum values. This means that at deployment time this virtual machine can be deployed with resources up to the maximum values. Later in this configuration, we<sup>2</sup> describe how to reconfigure the virtual machine resources after deployment.

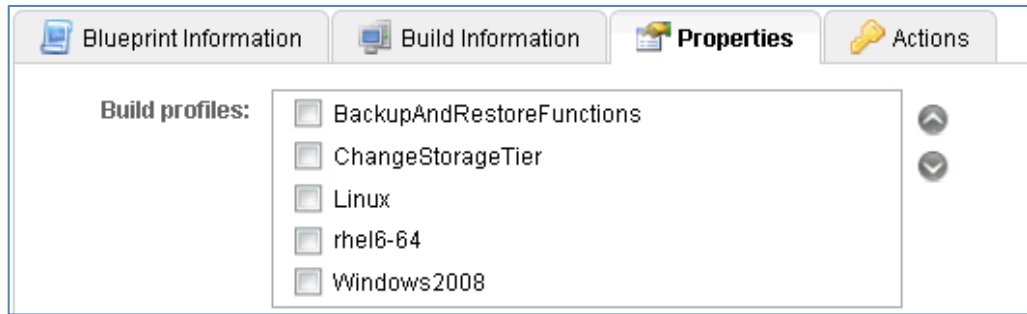
**Properties**

The **Properties** screen for a blueprint contains a number of build profiles, some of which are specific to each operating system and others that are applicable to all virtual machines.

A build profile contains a set of properties applied to a machine when it is provisioned. For this blueprint, we selected a build profile specific to Windows 2008 virtual machines, as shown in Figure 21.

<sup>2</sup> In this document, "we" refers to the Federation engineering team that validated the solution.



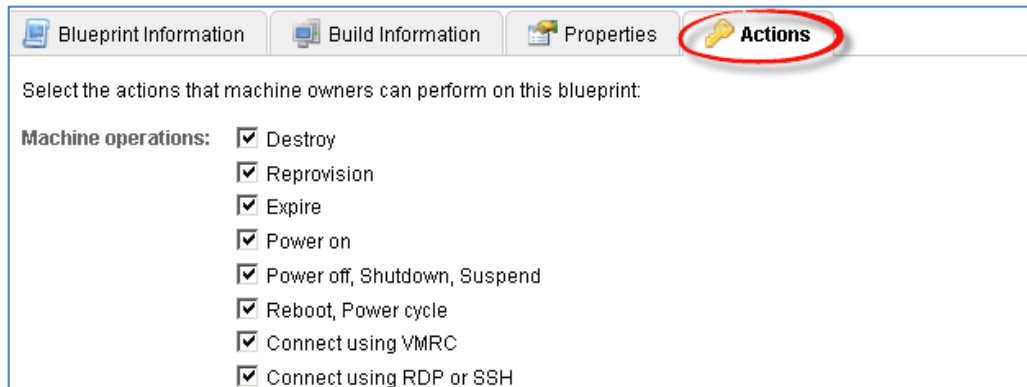


**Figure 21. Select custom build profiles for virtual machine**

Figure 21 also shows the **BackupAndRestoreFunctions** build profile. This build profile adds data protection actions to the virtual machine. Backup and recovery data protection functionality is a modular add-on to this EMC Enterprise Hybrid Cloud foundation infrastructure. Its details are not within the scope of this document. For details, refer to the *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Backup Solution Guide*.

### Actions

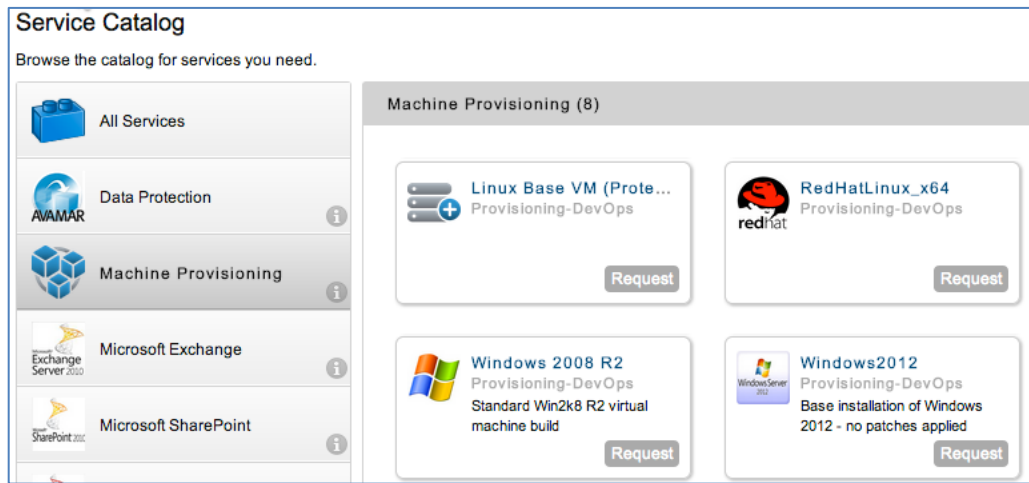
Under **Actions**, administrators can specify the actions, operations, and reconfiguration options that users can assign to this blueprint, as shown in Figure 22.



**Figure 22. Enable virtual machine operations for cloud user**

The blueprint must be published before being added as a catalog item and made available to end users in self-service portal, as shown in Figure 23.

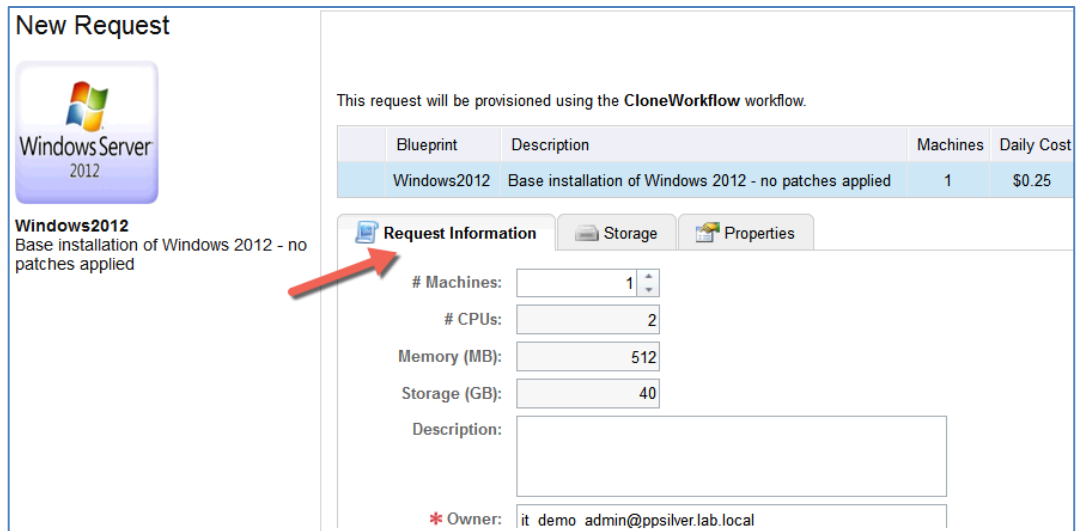




**Figure 23. Deploy new virtual machine blueprint from the self-service portal**

To provision the virtual machine, in this case the Windows 2012 virtual machine, the vCAC user can request the virtual machine from their service catalog, as shown in Figure 24.

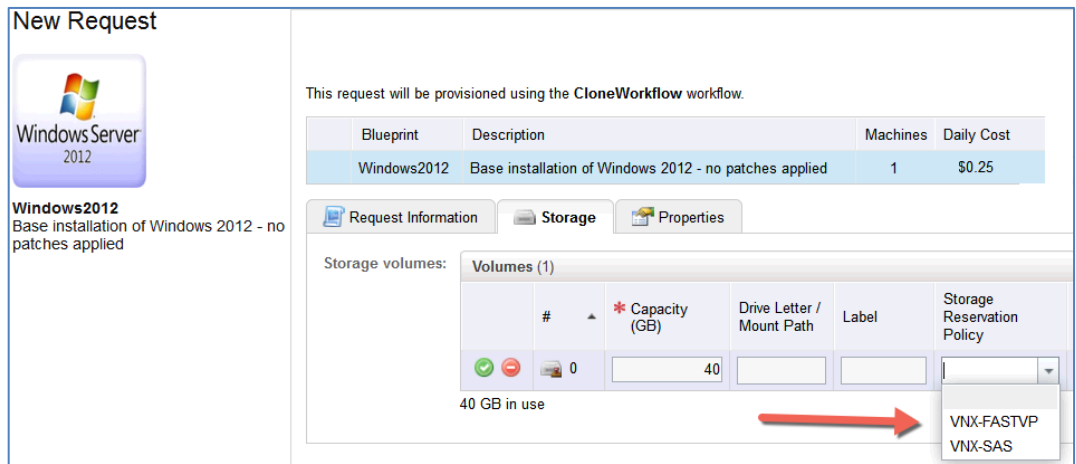
The request process may require user input to confirm the number of virtual machines to be provisioned, and any increases in CPU, memory, or storage. The ability to change any of these settings is controlled by the blueprint itself and can be set accordingly.



**Figure 24. Complete request information for virtual machine**

The example shown in Figure 25 shows where the requestor selects the storage service level for the virtual machine. To do this, select the corresponding vCAC storage reservation policy for the virtual machine.

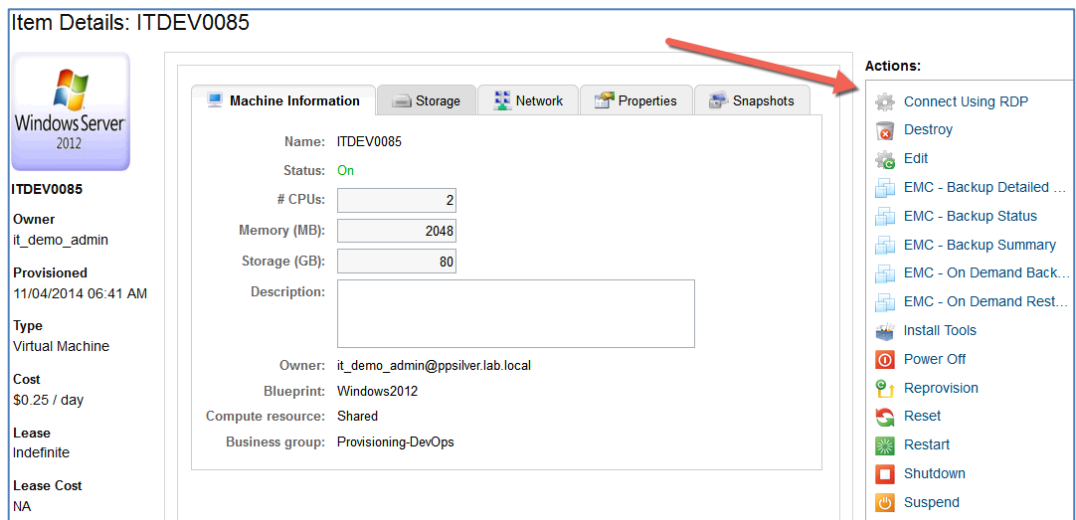




**Figure 25. Select storage reservation policy for virtual machine**

Users can click **Submit** after the virtual machine is configured to initiate the provisioning process. The provisioning process can be used to configure approval operations, either with vCAC or with integrated third-party approval or ticketing systems.

When the provisioning process is complete, the user can access the virtual machine through the **Actions** menu in the vCAC console, as shown in Figure 26.



**Figure 26. Virtual machine details and available actions**

For more information on creating virtual machine blueprints, refer to *vCloud Automation Center Operating Guide v6.0*.



### Application provisioning and services

This EMC Enterprise Hybrid Cloud solution framework supports application provisioning using VMware Application Director (AppD) with vCAC.

vCloud AppD uses the cloud resources available in vCAC to provide application services to the hybrid cloud environment.

Individual vCAC blueprints are registered to AppD cloud templates, which then makes the vCAC blueprint available in the AppD catalog. Application administrators can then configure application-specific services from the AppD catalog and make them available through the vCAC service catalog for consumption by IT administrators, as shown in Figure 27.

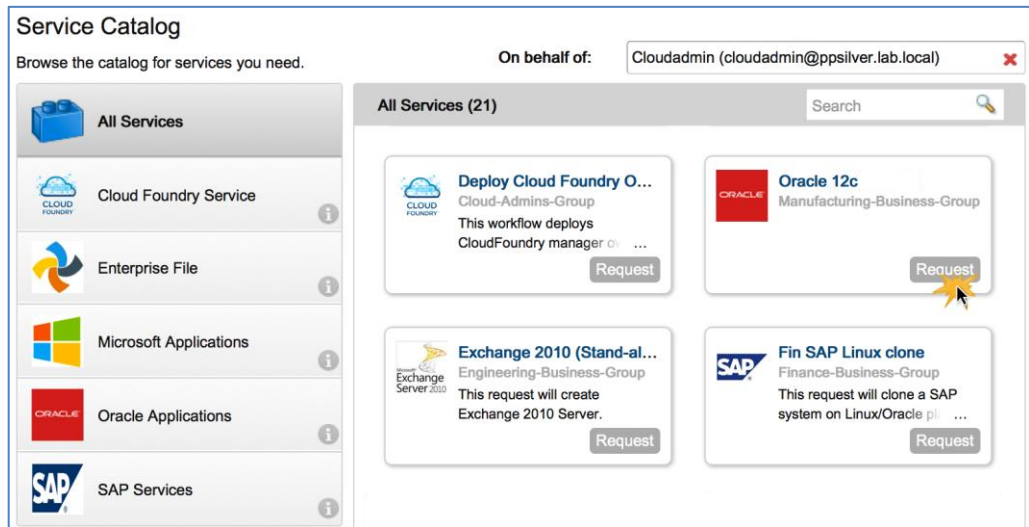


Figure 27. Application services: Provision databases and applications

vCAC provides the infrastructure resources for the virtual machine while AppD configures the application specific services and components. The AppD customizations are implemented and applied as part of an execution plan.

---

**Note:** VMware vCloud Application Director is not a required component for this hybrid cloud solution.

---

For more application services information, refer to the application-specific documents for the EMC Enterprise Hybrid Cloud solution that highlight applications such as Oracle, SAP, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, Cloud Foundry, and Hadoop.



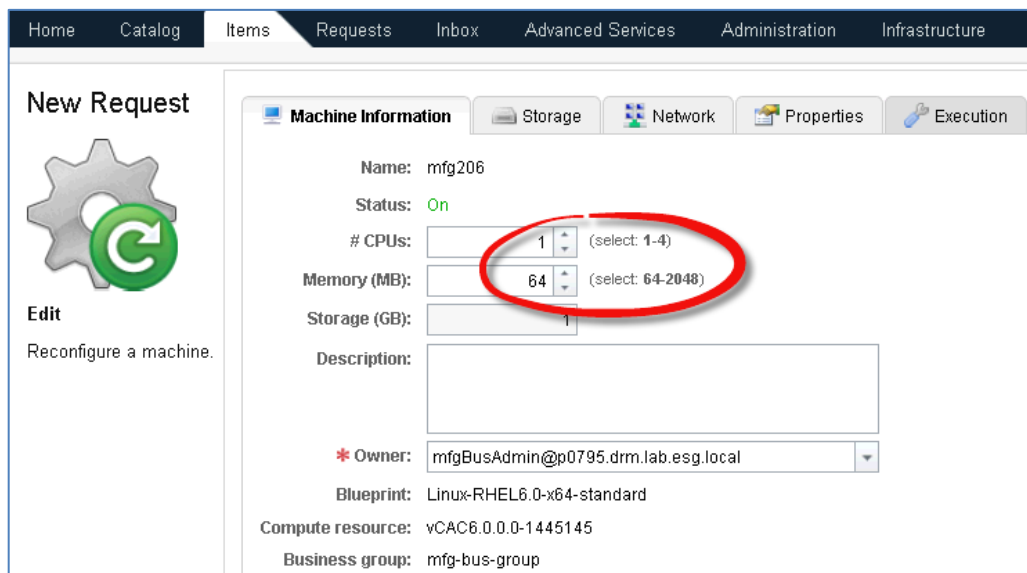
**Use case 2:  
Reconfigure an  
existing virtual  
machine**

Cloud users can reconfigure the resources assigned and available to their virtual machines. The scope of possible reconfiguration by a business group user can be restricted, as appropriate, by their business group manager.

Business group users can reconfigure one of their virtual machines if their business group manager has enabled this in the blueprint. A machine owner can make any of the following changes to a provisioned machine:

- Increase or decrease memory
- Increase or decrease the number of CPUs
- Modify storage by adding, removing, or increasing the size of volumes (SCSI disks only)
- Modify networks by adding, removing, or updating network adapters

Changes to each of these parameters are subject to the upper limits defined in the blueprint originally used to provision the machine, as shown in Figure 28.



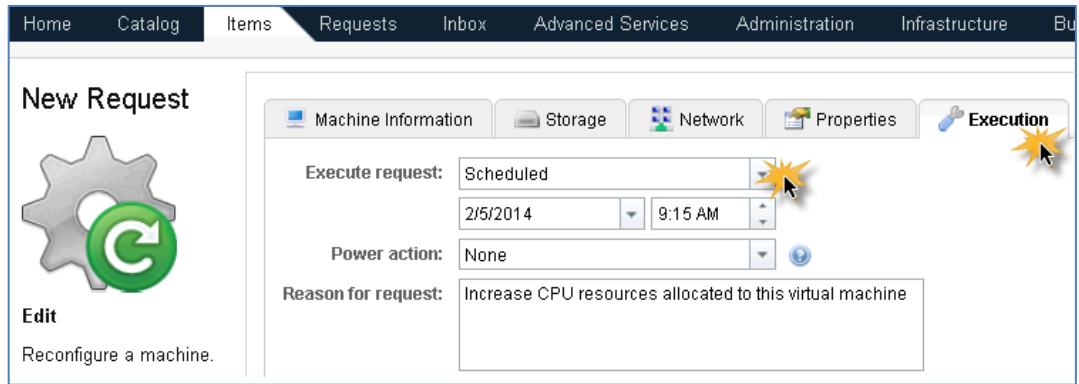
The screenshot shows a web interface for reconfiguring a virtual machine. The top navigation bar includes Home, Catalog, Items, Requests, Inbox, Advanced Services, Administration, and Infrastructure. The main content area is titled 'New Request' and features a gear icon with a refresh symbol and an 'Edit' button labeled 'Reconfigure a machine.' The form itself is titled 'Machine Information' and includes tabs for Storage, Network, Properties, and Execution. The form fields are as follows:

- Name: mfg206
- Status: On
- # CPUs: 1 (select: 1-4)
- Memory (MB): 64 (select: 64-2048)
- Storage (GB): 1
- Description: (empty text area)
- \* Owner: mfgBusAdmin@p0795.drm.lab.esg.local
- Blueprint: Linux-RHEL6.0-x64-standard
- Compute resource: vCAC6.0.0.0-1445145
- Business group: mfg-bus-group

**Figure 28. Reconfigure virtual machine resources**

Storage and network resources can also be modified. Reconfiguring a virtual machine's resources can be restricted in the virtual machine blueprint by its creator, where minimum and maximum values can also be applied to limit the scope of reconfiguration. The execution of the reconfiguration can be immediate, scheduled, or queued for the virtual machine owner, as shown in Figure 29.



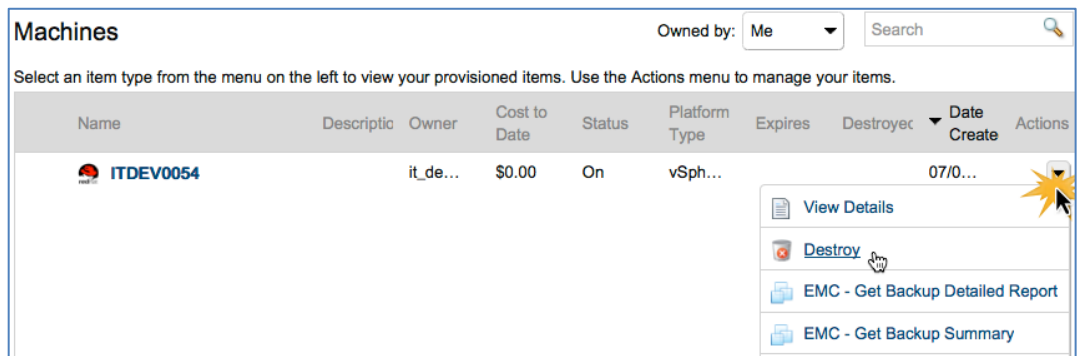


**Figure 29. Schedule reconfiguration of virtual machine**

**Use case 3:  
Decommission a  
virtual machine**

When the virtual machine’s lease expires, or the machine is manually expired, the virtual machine is either archived or destroyed, depending on whether its blueprint specifies an archive period.

When the end of the archive period is reached, or if there is no archive period, the virtual machine is destroyed. The business group user can also manually destroy the virtual machine, as shown in Figure 30.



**Figure 30. Decommission virtual machine**

When a virtual machine is destroyed, all charges relating to it are removed and its resources are recycled and made available to provision new machines.





## Storage services

### Overview

Storage is provisioned, allocated, and consumed by different cloud users in this solution.

For EMC Enterprise Hybrid Cloud storage administrator users, the storage services provided in the vCAC service catalog are used to provision storage resources that will be allocated to and consumed by other cloud users.

When the storage resources are available, fabric group administrators can assign the resources to business groups. From here, the business group managers can configure their blueprints to use those particular storage resources for the VMDKs.

When provisioning virtual machines, cloud users consume the storage and, depending on their entitlements, may choose the storage service for their virtual machines.

### Storage services pre-conditions

The storage services in the VMware vCAC self-service catalog are dependent on the initial configuration and preparation of EMC ViPR. This involves the discovery of the relevant storage arrays, SAN switches, and VMware vCenter Server before configuring the ViPR virtual array, virtual pools, and user roles. For more details, refer to **Chapter 3**.

### Use case 1: Storage provisioning

This use case demonstrates how ViPR software-defined storage is provisioned for the hybrid cloud from the VMware vCAC self-service catalog.

EMC Enterprise Hybrid Cloud storage administrator users can provision storage from the vCAC self-service portal, by selecting the storage provisioning item from the vCAC service catalog, as shown in Figure 31.

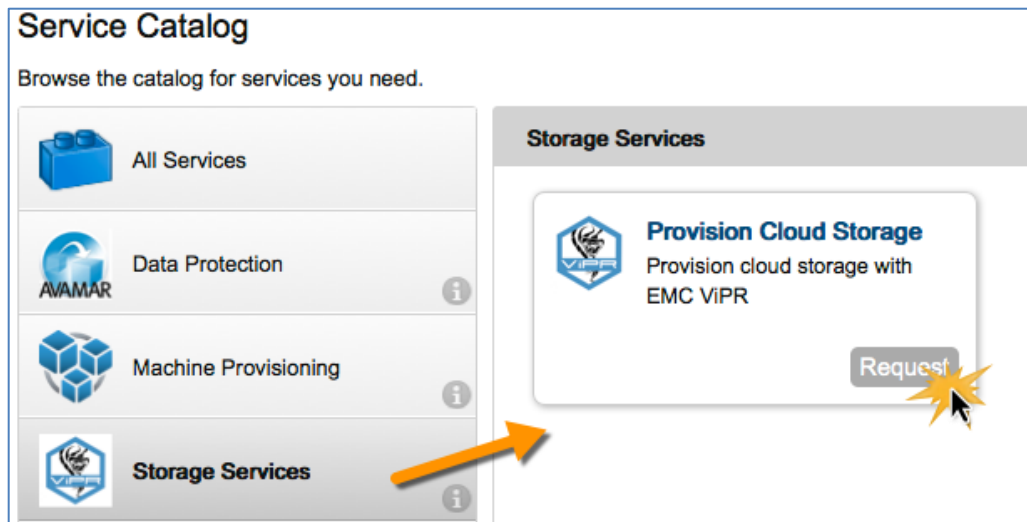


Figure 31. Storage Services: Provision cloud storage



The storage service blueprint can be created using vCAC anything-as-a-service (XaaS) functionality in the vCAC Advanced Service Designer. EMC ViPR provisioning workflows, presented to the vCAC service catalog by vCO, define the storage services.

The storage provisioned by the storage administrator user enables the fabric group administrator to make storage resources available to their business group. The storage provisioning request requires very little input from the vCAC IaaS user. The main inputs required are:

- vCenter cluster
- Storage type: VMFS or NFS
- Storage tier
- Datastore size

Most of these inputs, except datastore size, are selected from lists whose items are determined by the cluster resources available through vCenter and the virtual pools available in ViPR.

### vCenter Cluster

After the user has entered a description and reason for the storage-provisioning request, they are prompted to enter their password, and presented with the **Choose vCenter Cluster** option, as shown in Figure 32.

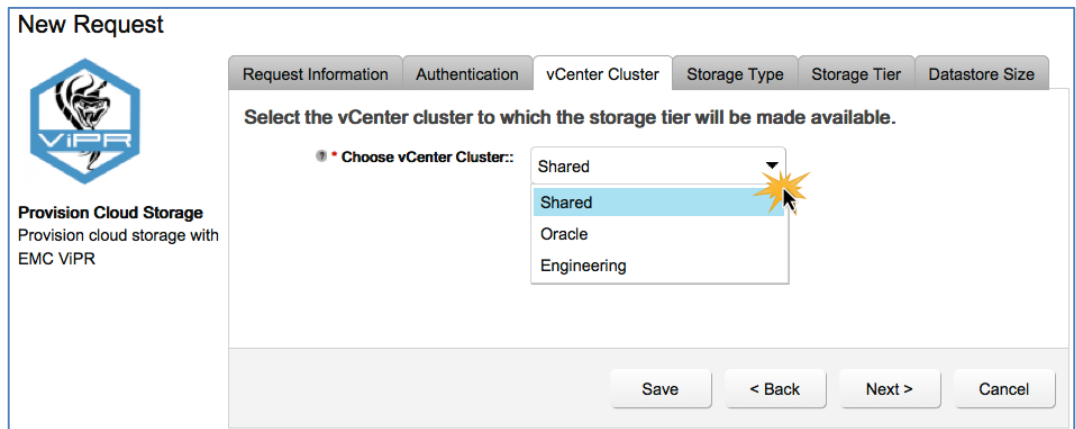


Figure 32. Provision cloud storage: Select vCenter cluster

vCenter Server manages multiple ESXi clusters; therefore, the correct vCenter cluster must be selected to instruct the provisioning operation where to assign the storage device.



## Storage Type

The user can select which type of datastore is required from a list, based on the storage types in the underlying infrastructure, as shown in Figure 33.

The screenshot shows a 'New Request' window for 'Provision Cloud Storage' with EMC ViPR. The 'Storage Type' tab is active, and the instruction is 'Select the type of datastore provision.' A dropdown menu is open, showing 'NFS' selected. Other options visible are 'VMFS' and 'NFS'. Navigation buttons at the bottom include 'Save', '< Back', 'Next >', and 'Cancel'.

**Figure 33. Storage provisioning: Select datastore type**

A datastore type of VMFS requires block storage, while NFS requires file storage. Other data services such as disaster recovery and continuous availability are displayed only if they are detected in the underlying infrastructure.

## Storage Tier

On **Storage Tier**, the user must select the storage tier from which the new storage device should be provisioned. The list of available tiers is based on the storage type selected, such as VMFS or NFS, and the matching virtual pools available from the ViPR virtual array. Pools can be selected from ExtremIO, VNX, VMAX and VPLEX storage types.

In this example, a single NFS-based ViPR virtual pool is available from which to provision storage. The available capacity of the virtual pool is also displayed to the user, as shown in Figure 34.

The screenshot shows the 'Storage Tier' step of the 'New Request' wizard. The instruction is 'Select the ViPR pool from which capacity for the storage will be provisioned.' A dropdown menu is open, showing two options: 'VNX File; available:1795GB'. The first option is selected. Navigation buttons at the bottom include 'Save', '< Back', 'Next >', and 'Cancel'.

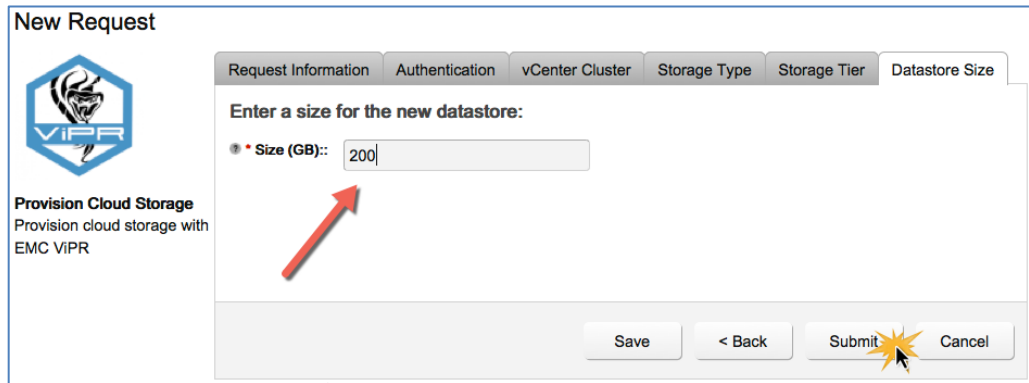
**Figure 34. vCAC storage provisioning: Choose ViPR storage pool**

These storage tiers have been configured in the ViPR virtual array and their storage capabilities are associated with storage profiles created in vCenter.



### Datastore Size

On **Datastore Size**, the user must enter the size required for the new storage, which is measured in GB, as shown in Figure 35.



**Figure 35. Storage provisioning: Enter storage size**

### Additional steps

In this example, a number of required input variables, such as LUN or datastore name, have been masked from the user during the storage provisioning request process. Some of these values are locked-in and managed by the orchestration logic to ensure consistency.

Beyond the initial provisioning of storage to the ESXi cluster at the vSphere layer, this solution provides further automation and integration of the new storage into the vCAC layer. The ViPR storage provider automatically tags the storage device with the appropriate storage profile based on its storage capabilities.

The remaining automated steps in this solution are:

- vCAC rediscovery of resources under vCenter endpoint
- vCAC storage reservation policy is assigned to the new datastore
- vCAC fabric group administrator is notified of the availability of a new datastore



In the last manual step, the fabric group administrator reserves the new storage for use by a business group, as shown in Figure 36.

Physical	Reserved	Allocated	This Reservation
95.9	144	0	20

Storage Path	Storage Cost (per GB)	Physical	Free	Reserved	* This reservation reserved	This reservation allocated	* Priority	Disabled
Shared_VNX File_1403545317898	\$0.0000	1	1	0				
Shared_VNX File_1403629168540	\$0.0000	1	1	0				
Shared_VNX File_1403800442880	\$0.0000	1	1	0				
Shared_VNX File_1403803087167	\$0.0000	1	1	0				
Shared_VNX File_1404227012815	\$0.0000	1	1	0				
Shared_VNX File_1404477755453	\$0.0000	197	197	0	197		1	

**Figure 36. Provision storage: Storage reservation for vCAC business group**

The automated process sends an email notification to the fabric group administrator that the storage is ready and available in vCAC. The administrator can then assign capacity reservations on the device for use by the business group.

**Use case 2: Select virtual machine storage**

This use case demonstrates how cloud users can consume the available storage service offerings. This use case is part of the broader virtual machine deployment use case but it is highlighted here because it relates directly to how the business group manager and users can manage the storage service offerings available to them.

VMware vCAC business group managers and users can select the appropriate storage for their virtual machine through the VMware vCAC user portal.

For business group managers, the storage type for the VMDKs can be set during the creation of a virtual machine blueprint. As shown in Figure 37, the appropriate storage reservation policy can be applied to each of the virtual disks.

Machine Resources

\* Minimum      Maximum

# CPUs: [ 1 ] [ ]

Memory (MB): [ 1024 ] [ ]

Storage (GB): [ 48 ] [ ]

Lease (days): [ ] [ ]

(Leave blank for no expiration date)

\* Storage volumes: Volumes (2) [ + New Vx ]

#	Capacity (GB)	Drive Letter / Mount Path	Label	Storage Reservation Policy	Custom Prop
0	40			VNX File	Edit
1	8			VNX File	

Allow user to see and change storage reservation policies

Maximum volumes: [ 15 ]

Maximum network adapters: [ Unlimited ]

**Figure 37. Set storage reservation policy for VMDKs**



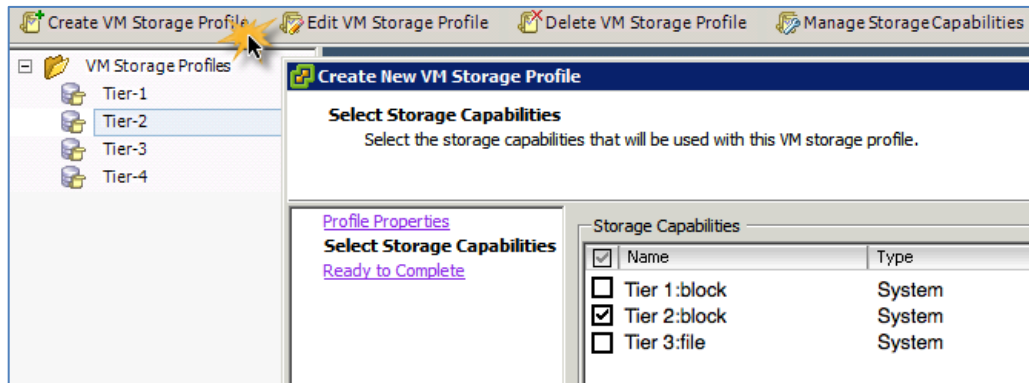
When the storage reservation policy is set, the blueprint will always deploy this virtual machine and its virtual disks to that storage type. If more user control is required at deployment time, the business group manager can permit business group users to reconfigure the storage reservation policies at deployment time by selecting the **Allow users to see and change storage reservation policies** checkbox.

**Use case 3:  
Metering storage  
services**

This solution uses VMware ITBM to provide chargeback information on the storage service offerings for the hybrid cloud. Through its integration with VMware vCenter and vCloud Automation Center, ITBM enables the cloud administrator to automatically track utilization of storage resources provided by EMC ViPR.

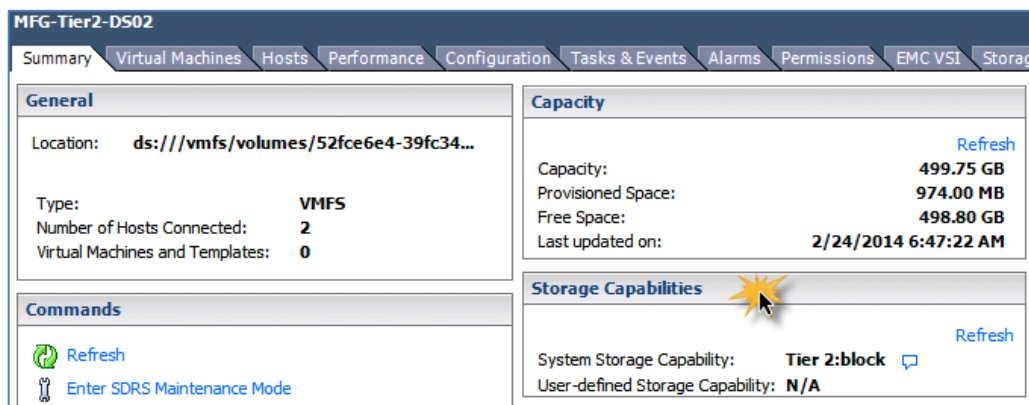
EMC ViPR VASA provider in vCenter automatically captures the underlying storage capabilities of LUNs provisioned from virtual pools on the EMC ViPR virtual array. Storage profiles are created based on these storage capabilities, which are aligned with the storage service offerings. This integration enables ITBM to automatically discover and group datastores based on predefined service levels of storage.

In this solution, a separate virtual machine storage profile was created for each of the storage service offerings, as shown in Figure 38.



**Figure 38. Create new virtual machine storage profile for Tier-2 storage**

The storage capabilities are displayed automatically in vSphere, as shown in Figure 39, where Tier 2 EMC ViPR storage is supporting a datastore.



**Figure 39. Automatic discovery of storage capabilities**



**Note:** Storage capabilities are only visible in the traditional vSphere client and not in the web client. Also, the web client uses virtual machine storage policies in place of virtual machine storage profiles.

After the EMC ViPR storage provider has automatically configured the datastores with the appropriate storage profiles, the datastores can be grouped and managed in ITBM, according to their storage profile. Figure 40 shows that the cost profiles created in vCenter are discovered by ITBM. This enables the business management administrator to group tiered datastores provisioned with ViPR and set the monthly cost per GB as needed.

Edit the total monthly cost per GB for storage based on:

Storage Profile  Storage Type

Storage monthly costs by storage profile					
Profile	Datastores	Total GB	Reference Cost	Monthly Cost Per GB	Monthly Cost
Tier-2	2	999.5	\$0.10	\$0.07	\$70
Tier-3	2	999.5	\$0.10	\$0.05	\$50
Uncategorized	28	47344.05	\$0.10	\$0.10	\$4,734
<b>Total:</b>					<b>\$4,854</b>

**Figure 40. VMware ITBM chargeback based on storage profile of datastore**

### Storage services summary

VMware vCAC provides a storefront of catalog items for storage services used by cloud users. These service catalog items use EMC ViPR software-defined storage services based on multiple service levels across EMC ExtremIO, VNX, and VMAX storage arrays, each offering varying levels of availability, capacity, and performance to satisfy the operational requirements of different lines of business.

This solution combines EMC ViPR with EMC array-based, FAST-enabled storage service level offerings and VMware vSphere to simplify storage operations for hybrid cloud customers.



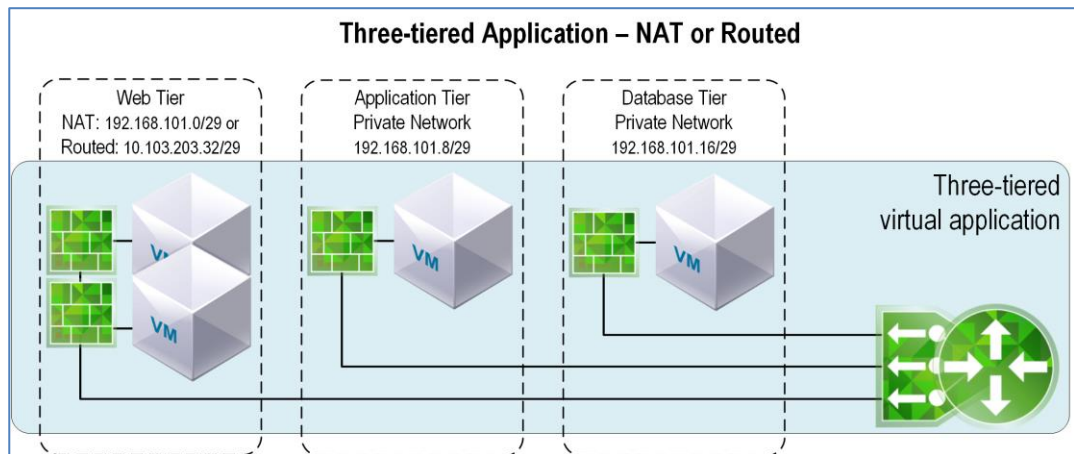
## Networking services

### Overview

Deploying a virtual application can be done in minutes. However, planning, designing, and configuring the network and security elements to support it can often take days or weeks. Using the automation capabilities of vCAC, NSX can significantly reduce the amount of time the provision, update, and removal process takes. Networks, router, firewall, and load balancers can be deployed dynamically with the virtual machine components of a blueprint. This enables an application stack and supporting services to be delivered to production users in minutes.

### Provisioning three-tiered virtual applications

Three-tier applications are the most commonly deployed model in enterprises. Each tier requires a specific configuration and changes that can use the NSX capability with vCAC. A three-tier application can be used to demonstrate the network and security provisioning capabilities of vCNS or NSX when integrated with vCAC. The web-tier is external facing and is load balanced, serving web pages to users. Each web server needs to communicate with the application server; the application server in turn writes to and retrieves data from the database server, as shown in Figure 41.



**Figure 41. Three-tiered application**

Within the context of networking and security, two deployment models are enabled by vCAC: pre-provisioned, and on-demand. The key difference between them is that, with a pre-provisioned deployment, the networks and router must exist before vCAC can provision the virtual machines. With the on-demand deployment model, the web, application, and database virtual machines are all deployed in conjunction with the network infrastructure they require. Virtual networks and routers are created dynamically when a multimachine blueprint is executed using the on-demand deployment model.

In both deployment scenarios, the network adapters of the deployed virtual machines are connected to their respective virtual network and an IP address assigned either using DHCP or, as in our implementation, a static IP address.

The virtual machines are also assigned to their respective security groups by the vCAC blueprint. These security groups are associated with security policies (firewall





rules) enforced by the vCNS or NSX firewalls. The deployed virtual machines in each tier inherit their specific security policy because of their security group membership, which ensures that applications are protected from the moment of deployment.

**Use case 1:  
Configure pre-  
provisioned  
multimachine  
blueprint**

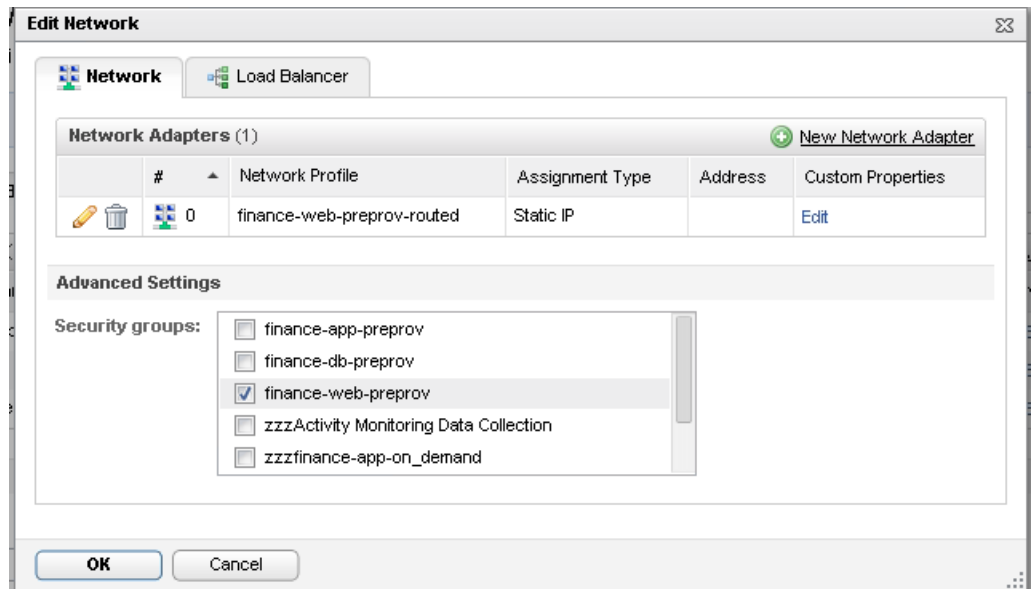
A multimachine blueprint was created with the name **Finance-Pre-Provisioned**, and was configured as follows:

1. Under **Build Information**, the three single-machine blueprints created earlier are added, as shown in Figure 42.

Blueprints (3)				
	Name	Blueprint	Min	Max
	linux-app	linux-app	1	
	linux-db	linux-db	1	
	linux-web	linux-web	1	3

**Figure 42. Pre-provisioned blueprint with build information configuration**

2. In **Build Information**, each component blueprint is edited, and a new network adapter is created, which is then mapped to the corresponding network profiles and the security groups, as shown in Figure 43.



**Figure 43. Blueprint network and security group configuration**

This blueprint connects virtual machines to pre-created networks; therefore, no new network profiles were added (on the **Network** screen of the main blueprint properties window), this would create dynamic networks.



In this use case, the blueprint connects only the virtual machines to the VXLAN networks created when preparing the environment.

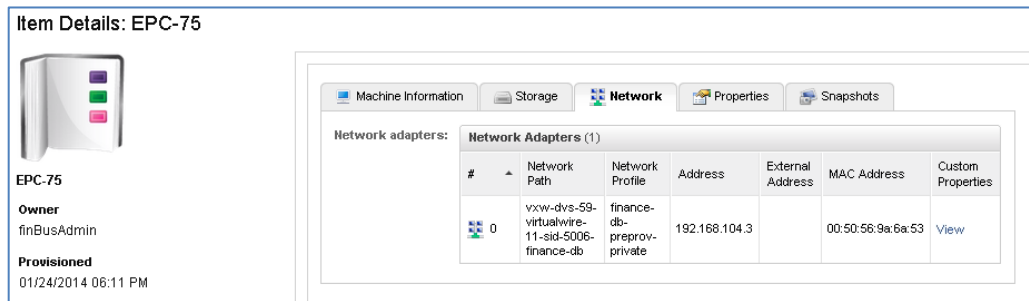
**Note:** Both the multimachine blueprint and the component blueprints have a Network screen, which may cause some confusion. The multimachine blueprint has a Network screen on its main properties window where the transport zone and network profiles (to trigger dynamic networks) are specified. The component blueprint’s Network screen is displayed when you edit the component blueprint in **Build Information**. The configurable options on this screen are **Network Adaptors** and **Security** groups.

The blueprint is published and added to the catalog where it is made available to the finance business group users.

Based on the blueprint, vCAC clones the virtual machines and attaches them to their respective logical switch networks. It also configures the provisioned virtual machines with static IP addresses from the IP address ranges already configured in the corresponding network profiles, and adds them to the appropriate security groups.

**Verify pre-provisioned deployment**

Figure 44 shows an example of the vCAC machine properties for a provisioned database virtual machine. The virtual machine is connected to the **vxw-dvs-59-virtual-wire-11-sid-5006-finance-db** logical switch, or VXLAN network, and configured with a static IP address of 192.168.104.3.



**Figure 44. Virtual machine properties: EHC-75 database-tier**

The same virtual machine properties in the web client are shown in Figure 45.



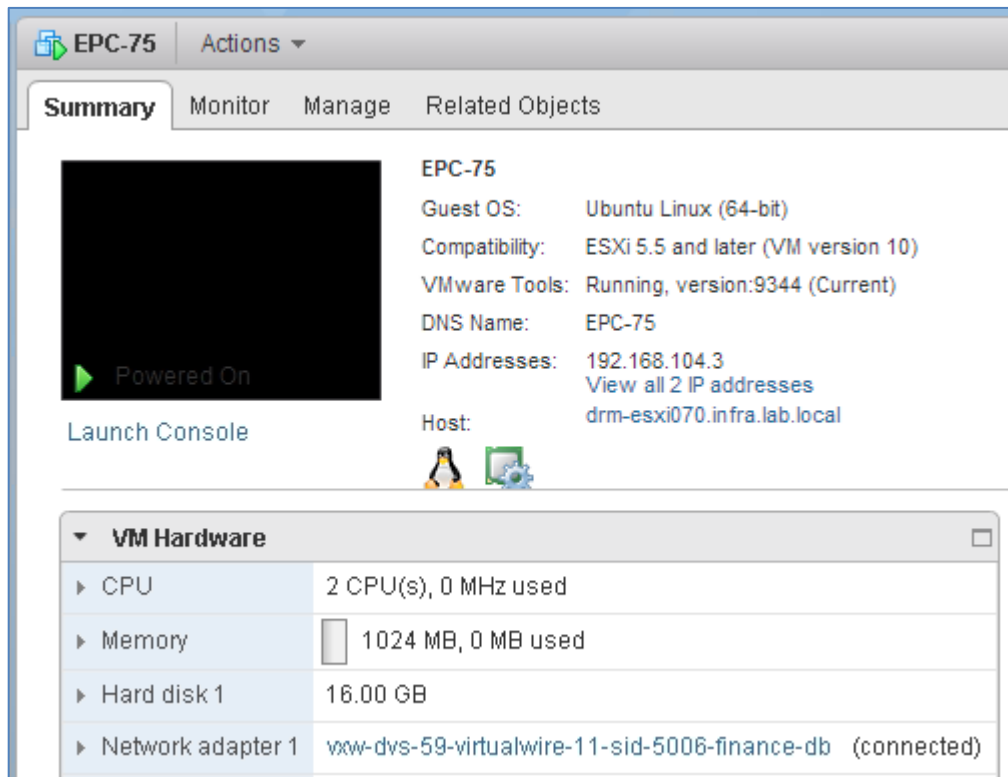


Figure 45. Virtual machine web client properties: EHC-75 database-tier

To verify that the database-tier virtual machine was placed in the correct security group, check the security group membership under the **Service Composer** in the **Networking & Security** web client, as shown in Figure 46.

The database virtual machine was added to the **finance-db-preprov** security group and therefore inherited the firewall rules configured for the database-tier security policy.

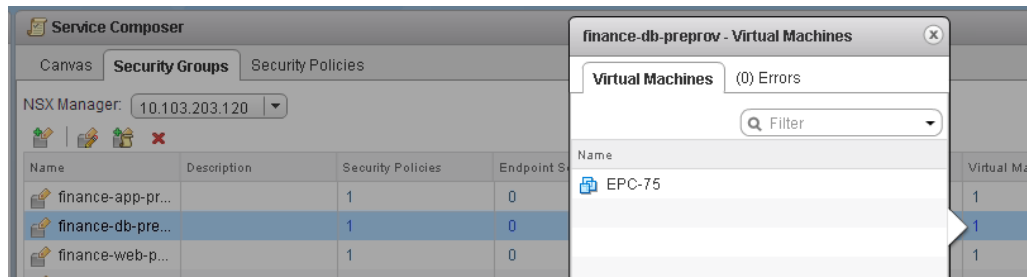


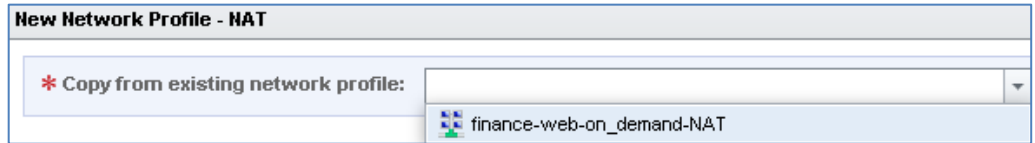
Figure 46. NSX service composer security groups membership view



**Use case 2: Create on-demand multimachine blueprints**

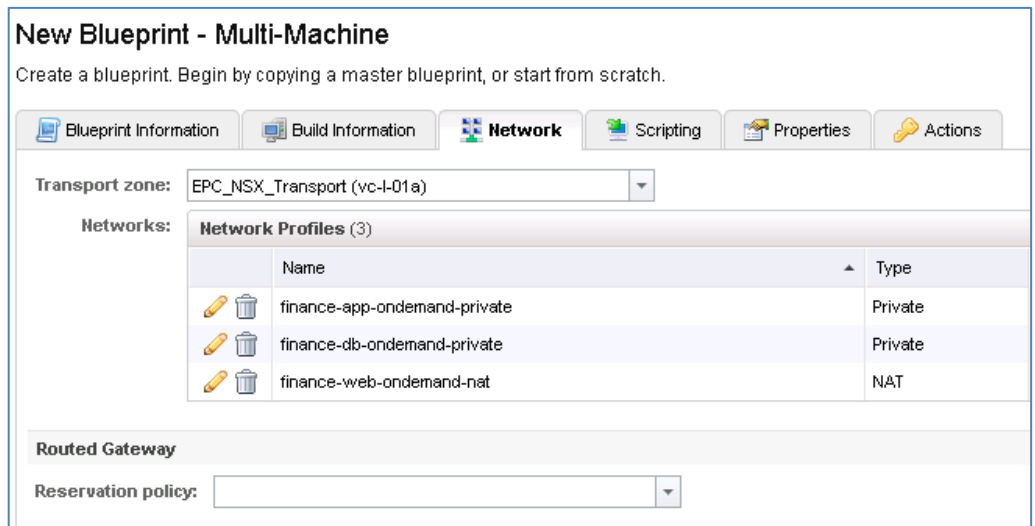
To create a multimachine blueprint (for example, **Finance-On-Demand**) that uses these network profiles and security groups:

1. Under **Network**, add the NAT network profile by clicking **New Network Profile** > **NAT**.
2. Select the network profile created earlier from the **Copy from existing network profile** list, as shown in Figure 47.



**Figure 47. Copying an existing network profile to a blueprint**







3. Repeat the process for the private networks, as shown in Figure 48, and then configure the build information.



**Figure 48. Multimachine network properties**

4. Add single-machine blueprints.  
 Since load balancing will be configured, there can be multiple instances of a particular workload, as the maximum value for the web blueprint shows in Figure 49.



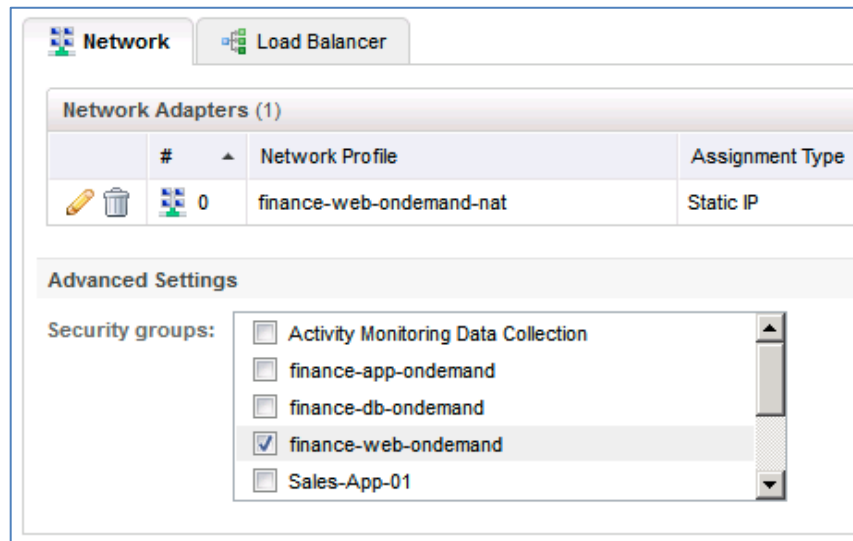
Blueprints (3)				
	Name	Blueprint	Min	Max
 	linux-app	linux-app	1	
 	linux-db	linux-db	1	
 	linux-web	linux-web	1	3

**Figure 49. Multimachine build configuration for load balanced blueprints**

5. Edit each single-machine blueprint to add a new network adapter.

The web-tier blueprint is shown in Figure 50, and is configured to use the **finance-web-ondemand-nat** network profile and the **finance-web-ondemand** security group. When provisioned from this blueprint, all virtual machines are added to the **finance-web-ondemand** security group.

**Note:** In this solution, we did not configure IP addresses on these adapters, because vCAC automatically configures the network adapters from the ranges specified in the network profiles.



**Figure 50. Web-tier blueprint configuration**

6. Configure the blueprint to deploy three web-tier virtual machines, and configure load balancing. When configuring the load balancer, it is important that you specify the web server ports to be load balanced, as shown in Figure 51.

Also, specify the network profile from which the virtual IP addresses are allocated to provide NAT to the web-tier virtual machines' private IP addresses.



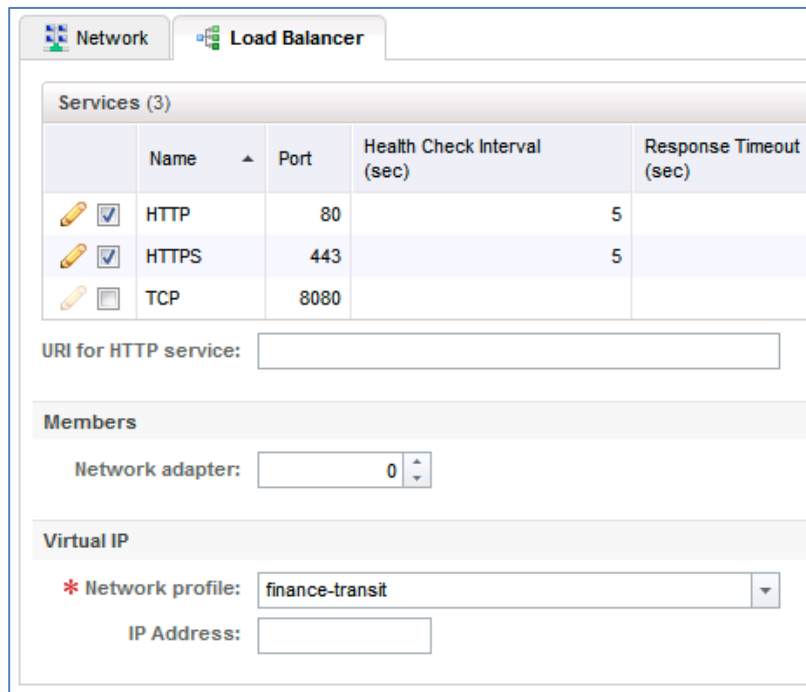


Figure 51. Multimachine web-tier load balancer configuration

7. Assign the network profiles and security groups to their corresponding application and database-tier network adapters.

After these steps, publish the blueprint and add it to the catalog so that it is available to the finance business group users. When a user requests this catalog item, the multimachine blueprint is executed and the logical switches are created. vCAC then deploys the NSX Edge 5.5 router with an interface on each logical switch and the finance transit network. Then the virtual machines are deployed and configured with IP addresses from the network profile ranges.

**Verify on-demand deployment**

Figure 52 shows an example of the machine properties for a provisioned web-tier virtual machine. The virtual machine’s network path shows that it is **Managed Externally**, which means the path is determined by the NSX Edge 5.5 router provisioned by vCAC as the gateway, and configured with a private static IP address of 192.168.101.2.

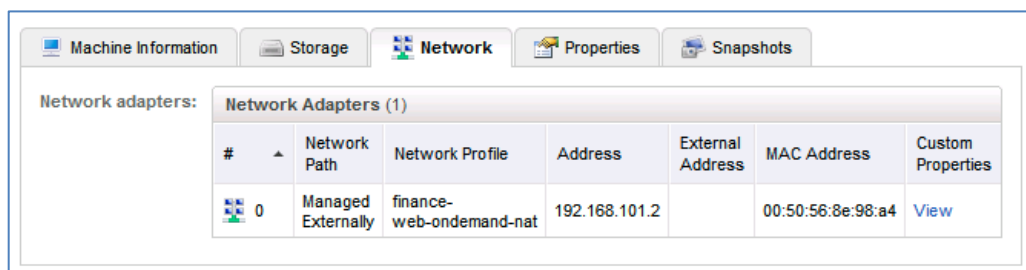
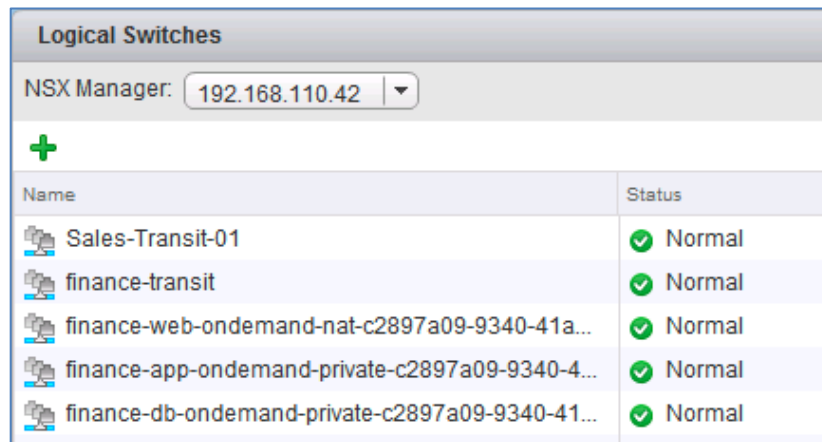


Figure 52. Machine properties for an on-demand provisioned virtual machine



To verify the on-demand deployment:

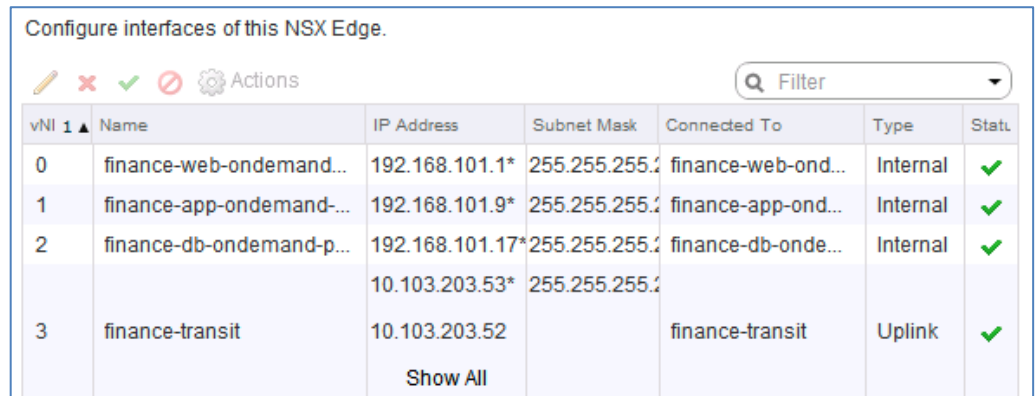
1. Verify that the logical switches are created by viewing the list of logical switches in the Networking & Security web client. Figure 53 shows an example of the provisioned on-demand networks.



Logical Switches	
NSX Manager: 192.168.110.42	
+	
Name	Status
Sales-Transit-01	✓ Normal
finance-transit	✓ Normal
finance-web-ondemand-nat-c2897a09-9340-41a...	✓ Normal
finance-app-ondemand-private-c2897a09-9340-4...	✓ Normal
finance-db-ondemand-private-c2897a09-9340-41...	✓ Normal

**Figure 53. Logical switches view**

2. Verify that vCAC has configured the NSX Edge 5.5 by viewing its interface properties in the Networking & Security web client. Figure 54 shows the configured IP addresses, the connected networks, and the routable IP addresses used for the gateway NAT and load balancer.



Configure interfaces of this NSX Edge.						
vNI	Name	IP Address	Subnet Mask	Connected To	Type	Status
0	finance-web-ondemand...	192.168.101.1*	255.255.255.255	finance-web-ond...	Internal	✓
1	finance-app-ondemand...	192.168.101.9*	255.255.255.255	finance-app-ond...	Internal	✓
2	finance-db-ondemand-p...	192.168.101.17*	255.255.255.255	finance-db-onde...	Internal	✓
3	finance-transit	10.103.203.52	255.255.255.255	finance-transit	Uplink	✓

**Figure 54. Interface configuration for on-demand provisioned NSX Edge 5.5**

3. Verify that the load balancer configuration in the Networking & Security web client is enabled and configured as intended, as shown in Figure 55.



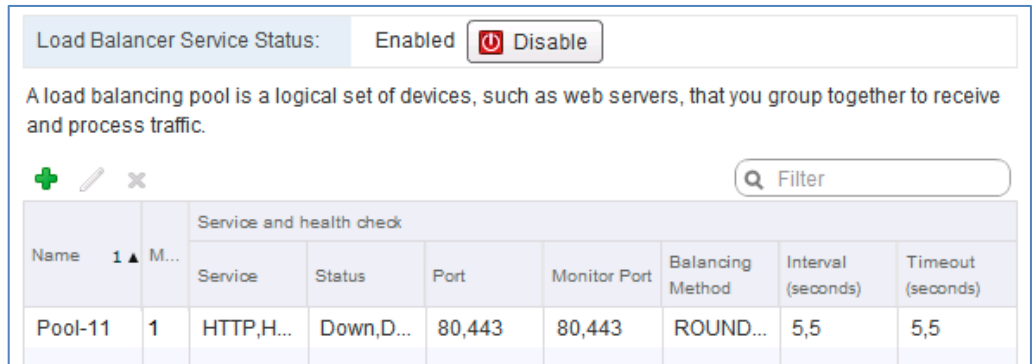


Figure 55. Load balancing configuration of the provisioned NSX Edge 5.5

4. Open the NAT view of the NSX Edge 5.5 gateway in the Networking & Security web client to view the NAT configuration. As shown in Figure 56, a static NAT rule is configured for the internal private 192.168.101.0/29 network with a routable IP address on the **finance-transit** network.

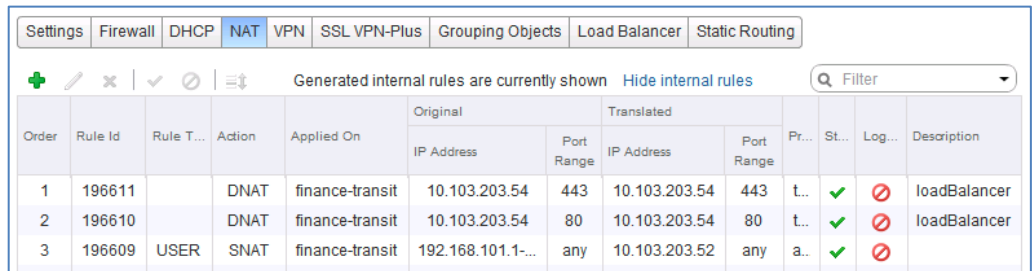


Figure 56. NAT configured on the engineering on-demand NSX Edge 5.5

**Networking services summary**

The three-tier application use cases showcased both pre-provisioned and on-demand deployment models, while explaining the differences and benefits of each. VMware NSX and vCAC offer flexible creation and deployment of workload resources, while providing richer functionality and improved performance over the vCNS solution.





# Chapter 5 Operational Management

This chapter presents the following topics:

- Overview .....74**
- Integrated and intelligent operational monitoring .....74**
- Resource management.....87**
- Metering .....95**
- Summary.....104**



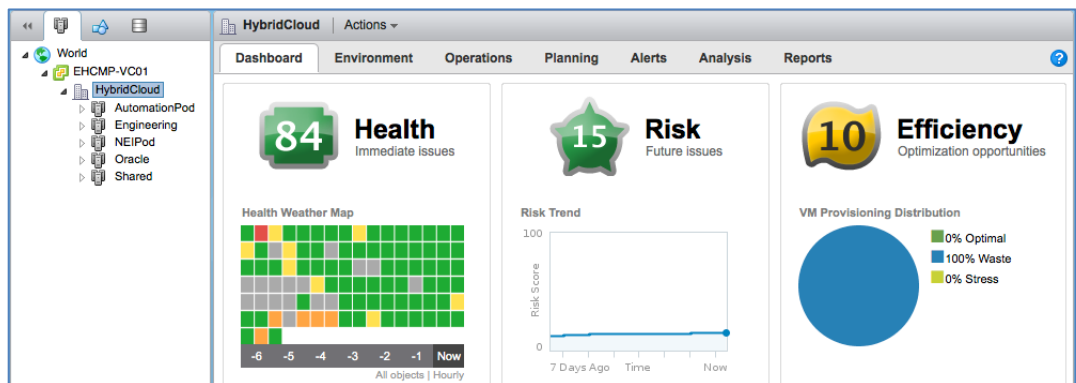
## Overview

Infrastructure maintenance and operations teams need the end-to-end visibility and intelligence to make fast, informed operational decisions to proactively ensure service levels in cloud environments. They need to get promptly to the root cause of performance problems, optimize capacity in real time, and maintain compliance in a dynamic environment of constant change.

This solution provides the ability to intelligently monitor and manage resources and systems in the hybrid cloud environment using EMC and VMware product integration and interoperability.

## Integrated and intelligent operational monitoring

The VMware vC Ops dashboard provides a comprehensive view into the environment, as shown in Figure 57. The main dashboard is divided into three logical entities that provide high-level information about current overall health and issues of all managed resources, risks of future issues, and resource efficiency trends in the environment.



**Figure 57. vCenter Operations Manager dashboard high-level overview**

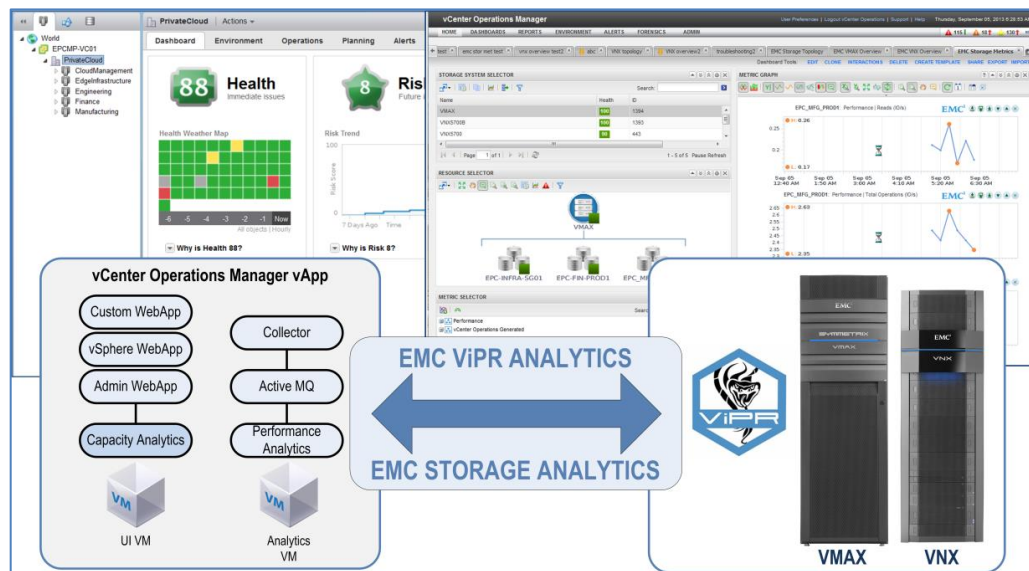
The three primary logical entities in vC Ops are:

- **Health:** Calculates health scores based on patented algorithms that dynamically observe behavioral trends of the cloud environment and display color coded red, yellow, and green status of the virtual machines, datastores, and clusters. Systems operations can identify where problems are, what the issues are, and if any trend of abnormal behavior exists in the environment.
- **Risk:** Provides insight into the resource consumption to provide advanced notification of a resource running out of capacity, as well as which resources will run out.
- **Efficiency:** Proactively optimizes the environment and reclaims waste.



## EMC ViPR Analytics and Storage Analytics

EMC provides integrated services that allow vC Ops to collect and report EMC ViPR and EMC storage array resource metrics. Using EMC ViPR Analytics and EMC Storage Analytics (ESA), VMware and storage administrators gain visibility into the software-defined storage environment, continuously available VPLEX devices, and the individual VMAX and VNX storage platforms. Health and risk analytics can be used to assist with problem resolution. Storage metrics are presented directly to vC Ops through customizable dashboards providing complete visibility into ViPR and storage array performance and capacity metrics.



**Figure 58. Architecture overview of vC Ops vApp including ESA**

The EMC ViPR and ESA adapters can be installed on an existing instance of an enterprise-licensed vC Ops.

### EMC ViPR Analytics

The EMC ViPR Analytics Pack provides enhanced capabilities for VMware vCenter Operations Management Suite by linking EMC ViPR Analytics with vC Ops. This integration delivers custom analytics and visual representation of the resources within the EMC software-defined infrastructure.

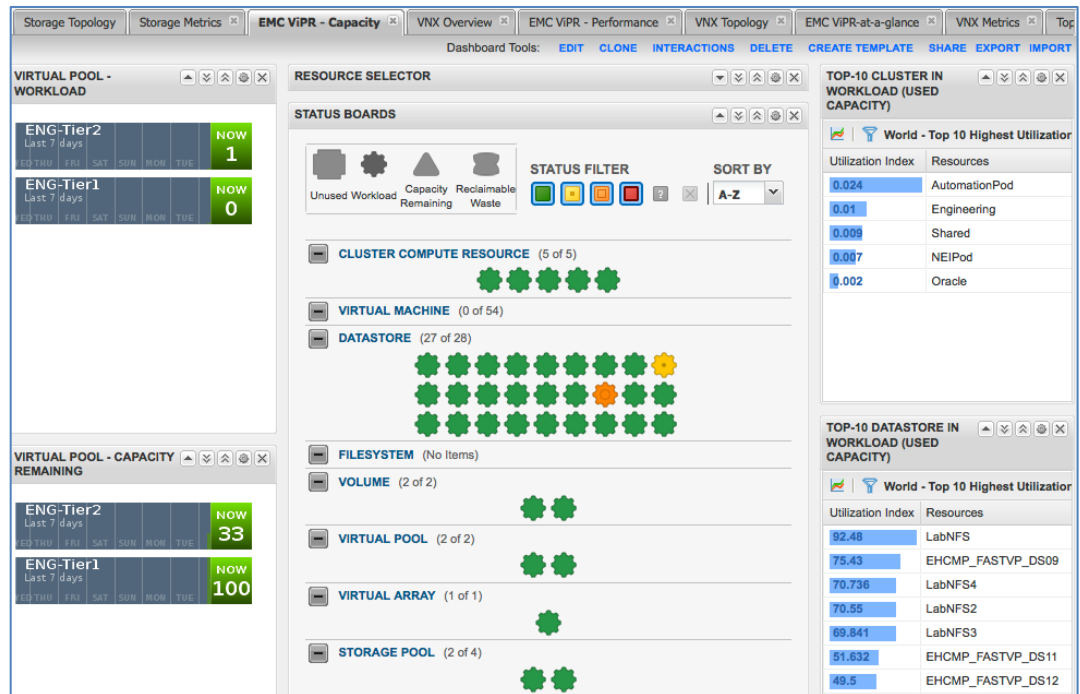
EMC ViPR inventory, metering, and event data is imported into vC Ops and displayed through pre-configured dashboards that show collections of volume, storage port, storage system, and virtual pool data. vC Ops uses the data to compute key resource status scores. Resource details, individual metrics, and EMC ViPR event alerts are also presented in dashboard views. The health scores of EMC ViPR resources can be improved by using performance data from VNX/VMAX adapters.

The preconfigured dashboards provided by the EMC ViPR Analytics Pack include capacity, performance, and higher-level at-a glance information.



***ViPR Capacity dashboard***

The ViPR Capacity dashboard enables users to monitor virtual storage pool capacity and datastore disk usage, as shown in Figure 59.



**Figure 59. EMC ViPR Capacity dashboard in vCenter Operations Manager**

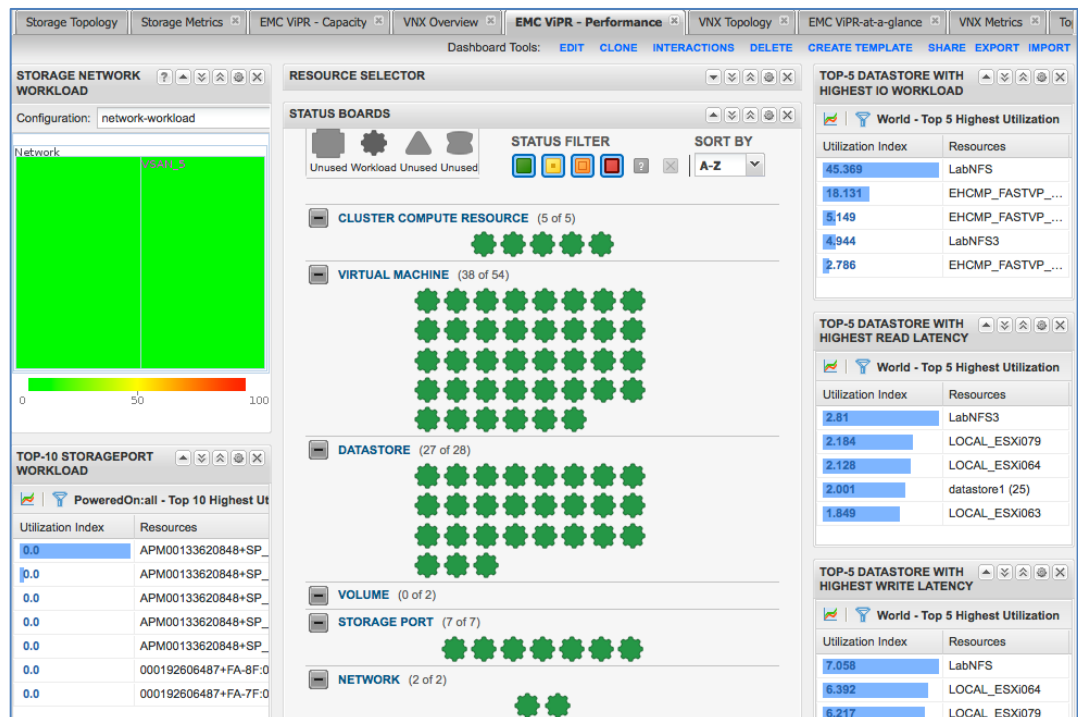
The ViPR Capacity dashboard consists of the following components:

- **Virtual storage pool workload:** Displays the provisioned capacity consumed by the datastores
- **Virtual storage pool capacity remaining:** Displays the available storage pool capacity
- **Resource selector:** Enables you to search for a specific resource
- **Status boards:** Displays various status and relationship information for ViPR resources
- **Clusters in workload:** Displays the top clusters in disk capacity workload
- **Datastores in workload:** Displays the top datastores in disk capacity workload



### ViPR Performance dashboard

The ViPR Performance dashboard, shown in Figure 60, enables users to monitor storage network and datastore latency performance data.



**Figure 60. EMC ViPR Performance dashboard in vCenter Operations Manager**

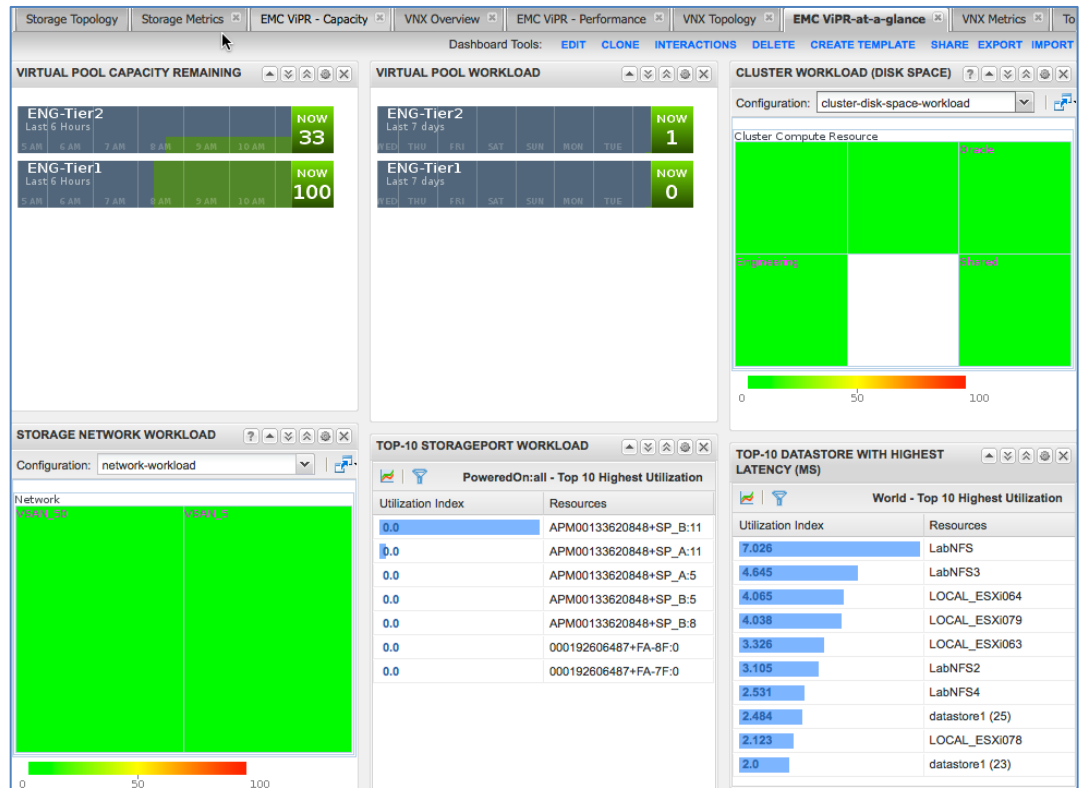
The ViPR Performance dashboard consists of the following components:

- **Storage network workload:** Displays the collected I/O utilization for all storage ports in a network
- **Storage port workload:** Displays the I/O workload for storage ports
- **Resource selector:** Used to search for a specific resource
- **Status boards:** Displays various status and relationship information for ViPR resources
- **Datastores with highest IO workload:** Displays the top datastores with the highest I/O workload
- **Datastores with highest read latency:** Displays the top datastores with the highest read latency
- **Datastores with highest write latency:** Displays the top datastores with the highest write latency



**ViPR at-a-glance dashboard**

The ViPR at-a-glance dashboard, shown in Figure 61, enables users to monitor performance and capacity data from a single dashboard.



**Figure 61. EMC ViPR at-a-glance dashboard in vCenter Operations Manager**

The ViPR at-a-glance dashboard consists of the following components:

- **Capacity Status Monitoring:** Combines the Virtual Storage Pool Workload, Virtual Storage Pool Capacity Remaining, and Clusters in Workload components to create a single dashboard for monitoring capacity status
- **Performance Status Monitoring:** Combines the Storage Network Workload, Storage Port Workload, and Datastores with highest latency components to create a single dashboard for monitoring performance status

**EMC Storage Analytics**

vC Ops integration with ESA software combines the features and functionality of vC Ops with VNX, VMAX, and VPLEX storage. It delivers custom analytics and visualizations that provide detailed visibility into your EMC infrastructure, enabling you to troubleshoot, identify, and take quick action on storage performance and capacity management problems.

Within the vC Ops custom portal, ESA presents separate dashboards, some that are universal and others that are specific to VNX and VMAX arrays. Each dashboard is fully customizable and can be adjusted to display the required details and metrics or additional widgets.



By default, ESA enables the following dashboards in the vC Ops custom portal. These dashboards provide information about EMC storage systems:

- **EMC Storage Topology dashboard:** Provides a view of resources and relationships between storage and virtual infrastructure objects
- **EMC Storage Metrics dashboard:** Displays resources and metrics for storage systems
- **EMC Overview dashboard:** Represents a single view of performance and capacity of VNX/VMAX resources

#### *EMC Storage Topology dashboard*

Topology mapping is viewed and traversed graphically using vCenter Operations Manager health trees. The dashboards developed for ESA use topology mapping to display resources and metrics.

ESA establishes mappings between:

- Storage system components
- Storage system objects and vCenter objects

Topology mapping enables health scores and alerts for storage system components, such as storage processors and disks, to be shown in the context of vCenter objects, such as LUNs, datastores, and virtual machines. Topology mapping between storage system objects and vCenter objects uses a vCenter adapter instance.

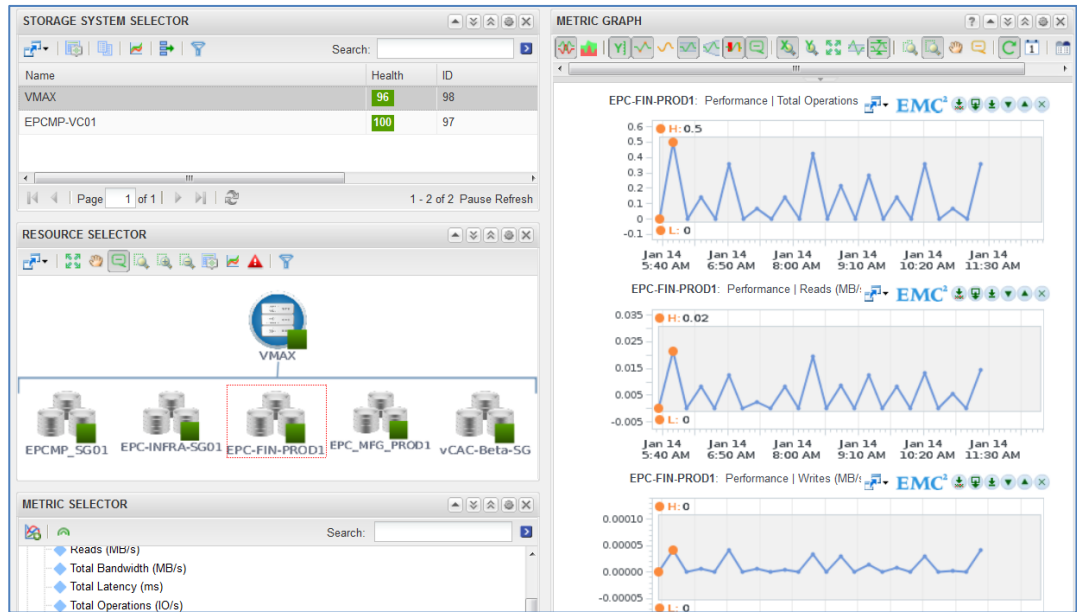
The Storage Topology dashboard enables you to view resources and relationships between storage and virtual infrastructure objects for VNX, VMAX, and VPLEX adapter instances. Details for every object in every widget are available by selecting the object and clicking the **Resource Detail** icon at the top of each widget. ESA displays all related VMware objects, which enables you to navigate end-to-end into the underlying storage array components, from vSphere datastore clusters and virtual machines to VMAX storage groups and Fast Ethernet (FE) ports.

#### **EMC Storage Metrics dashboard**

The EMC Storage Metrics dashboard, shown in Figure 62, displays a graph with each EMC resource and the metrics associated with it. Navigation is from the top down, so after choosing the storage system and a specific resource, you can select multiple metrics for display on the **Metric Graph** pane.

Figure 62 shows the total operations, reads, and writes in MB/s metrics for a VMAX storage group. You can download any one or all of the metric charts by clicking the applicable icons.

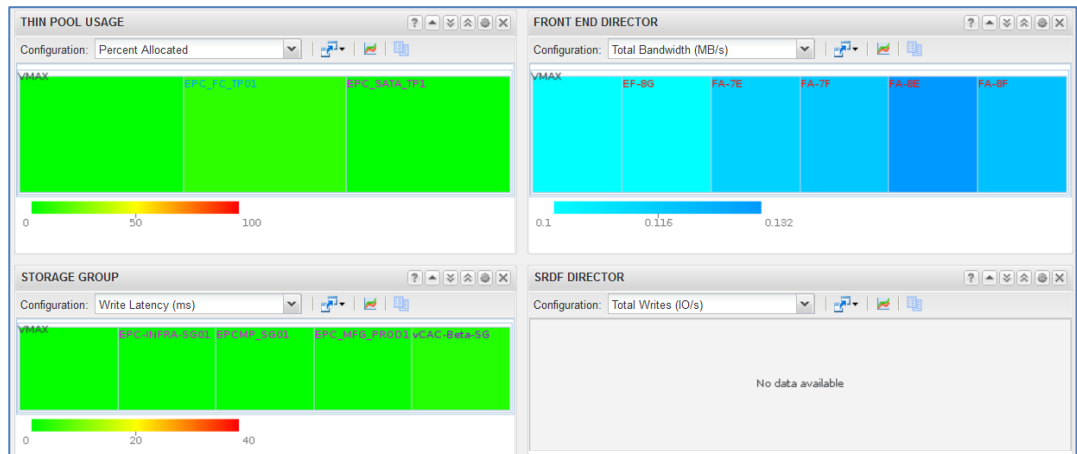




**Figure 62. EMC storage metrics dashboard with VMAX LUN metrics**

*Overview dashboard*

EMC VNX, VMAX, and VPLEX systems have separate dashboards with details presented as heat maps, as shown in Figure 63. This dashboard displays the main storage system resource types, thin pools, storage groups, LUNs, front-end ports, storage processors, FAST Cache performance, and the metrics for each one.



**Figure 63. EMC VMAX overview dashboard displaying object heat maps**

The heat map colors work on two different levels, the green to red legend represents either usage (for example, thin pool allocation) or performance (for example, latency). The blue legend represents relative usage across that metric within an array (for example, total writes). For any one of the objects displayed, a full historical perspective is available on the EMC Storage Metrics dashboard.





### Customized dashboards

Custom- or cloud-specific dashboards can be created for any environment using the objects and details provided by the various EMC and VMware solution packs.

The EMC ViPR and Storage Analytics packs present high-level information in a storage-centric manner, to support easy status identification at the object level. vC Ops supports grouping inventory objects into additional dashboards to create service and resource views focused on a particular set of resources.

The vC Ops Custom UI enables dashboards to be created and exported, provided the dashboard does not have any dependencies on the resource ID, which is the unique identity number assigned by vC Ops to each inventory object.

### Centralized log management

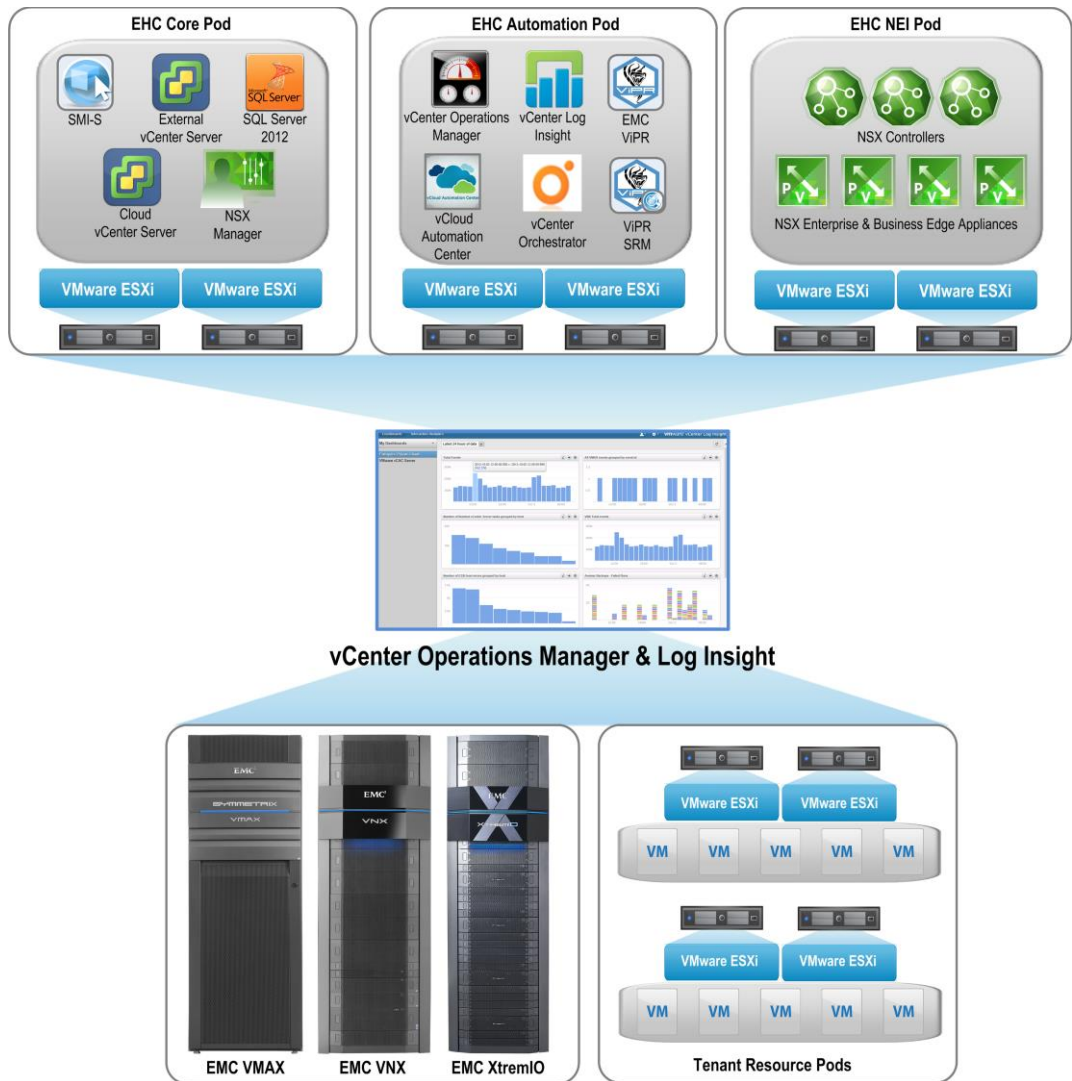
VMware vCenter Log Insight, shown in Figure 64, delivers automated log management with system analytics, aggregation, and search. With an integrated cloud operations management approach, it provides the operational intelligence and enterprise-wide visibility needed to proactively ensure service levels and operational efficiency in dynamic cloud environments.

Log Insight can analyze log events from any vCloud Suite component that supports syslog forwarding including all components of the management cluster and infrastructure. Some of this log forwarding configuration is enhanced using pre-packaged VMware and EMC content packs.

When integrated with Log Insight, EMC content packs for VNX and VMAX provide dashboards and user-defined fields specifically for those EMC products enabling administrators to conduct problem analysis on their EMC arrays or backup infrastructure.

Content packs are immutable, or read-only, plug-ins to vCenter Log Insight that provide predefined knowledge about specific types of events, such as log messages. The goal of a content pack is to provide specific event knowledge in a format easily understandable by administrators, engineers, monitoring teams, and executives. Each content pack is delivered as a file, and can be imported into any instance of Log Insight.





**Figure 64. Centralized logging of components with vCenter Log Insight**

In large environments with numerous log messages, Log Insight provides runtime field extraction to enable users to instantly locate the most important data fields. Any field from the data can be extracted using regular expressions.

Dashboards and widgets can be manually created for those components for which content packs do not exist.

Each widget provided by a content pack can be cloned and added to a personalized dashboard with views required by the user. Figure 65 provides an example of this, where the hybrid cloud dashboard contains widgets from each of the content packs installed for this solution.



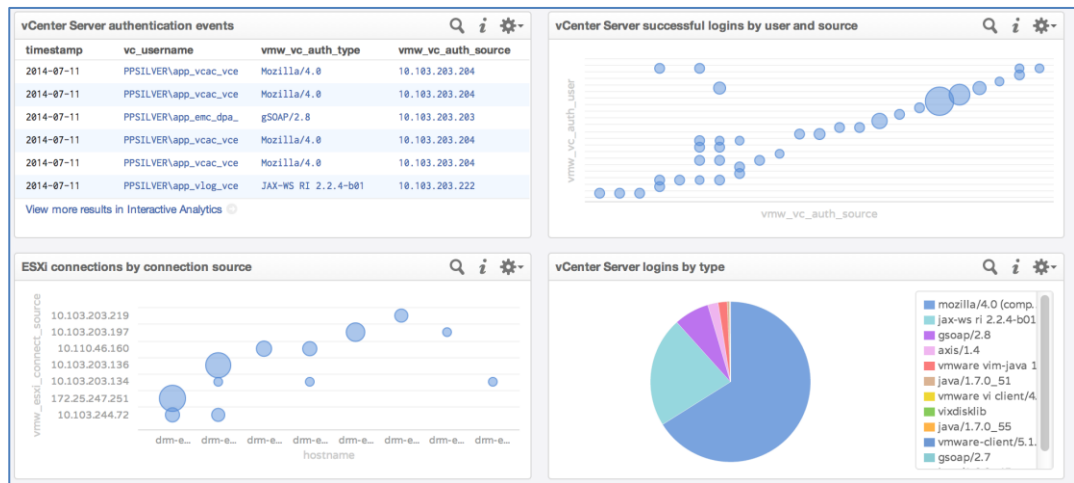


Figure 65. Customized hybrid cloud security dashboard

### vCloud component integration

vCenter Log Insight ships with the VMware vSphere content pack, which provides detailed insight into VMware vSphere logs and events. Content packs are also available for vCenter Operations Manager and VMware vCAC.

The vSphere content pack provides important information about the vSphere environment, providing several dashboards containing a comprehensive list of events and event types such as:

- vCenter Servers and ESX/ESXi Hosts
- SCSI/iSCSI and NFS
- Events, tasks, and alarms

The content pack for vCenter Operations Manager presents its log data in a more meaningful way and analyzes all of the logs that are redirected from a vCenter Operations Manager instance.

The vCenter Operation Manager content pack provides the following:

- Collection of logs from vCenter Operations Manager servers
- Default queries to expose key fields and events
- Pre-configured dashboards to make troubleshooting quick and easy

The queries and dashboards can be used to monitor and troubleshoot issues in the vCenter Operations Manager environment.

In addition to the content pack, VMware vC Ops Manager can be integrated in the following independent ways:

- Log Insight can send notification events to vC Ops Manager
- The **Launch in context** menu of vC Ops Manager can display actions related to Log Insight



The **Enable launch in context** functionality enables users in vC Ops to view events related to a specific object by launching vCenter Log Insight directly in the context of that object.

The example in Figure 66 uses the integration between Log Insight and vC Ops. Using the **Actions** menu in vC Ops triggers a search of all relevant Log Insight information on the selected item.

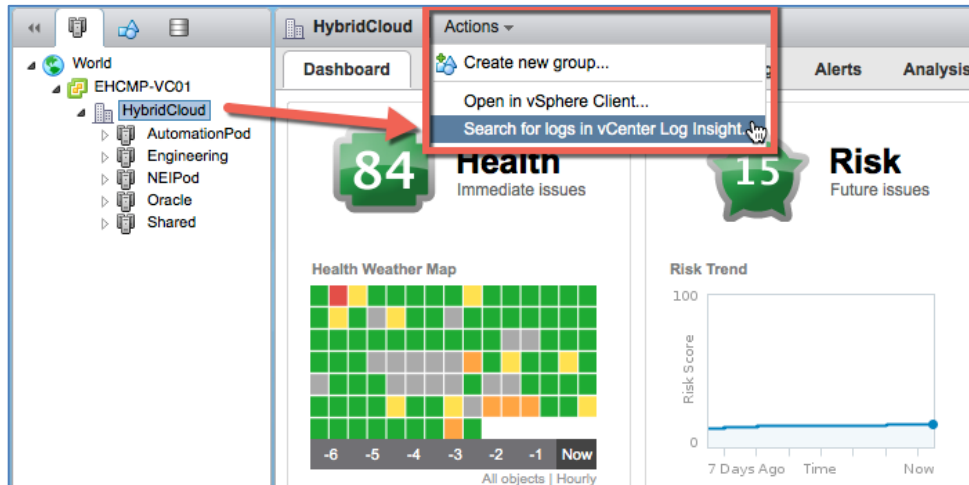


Figure 66. Search logs for cloud management platform

The launch-in-context action filtered the logs using the constraint **hostname equals <each hostname>**, which results in only events that match that criteria being displayed, as highlighted in Figure 67.

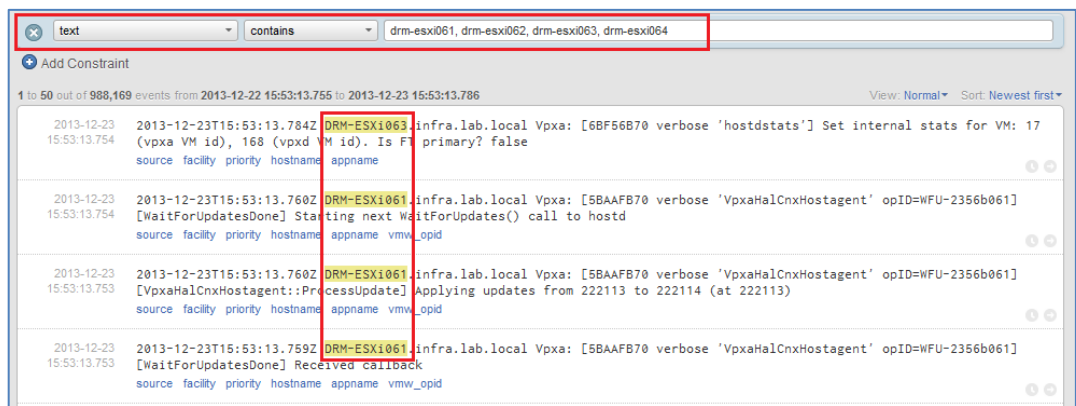


Figure 67. Log Insight filtering logs for the management cluster components

The vCloud Automation Center 6.0 content pack for Log Insight provides important information across all components of the vCAC environment and key dependencies such as vCenter Orchestrator and SSO. vCAC is composed of multiple components, each of which must be configured to forward their respective logs to Log Insight.



The vCloud Automation Center 6.0 content pack for Log Insight includes analytics for the following components:

- vCAC CAFE services
- IaaS services
- Application Director
- SSO
- Apache

For Windows-based hybrid cloud components, such as those hosting the SMI-S server or SQL Server databases, vCenter Log Insight 2.0 can collect data from Windows systems with an easy-to-deploy vCenter Log Insight Windows monitoring agent.

### EMC component integration

EMC has developed and provides Log Insight content packs for EMC VNX and VMAX in order to present the logging details in a more meaningful way. Customized dashboards and user-defined fields for VNX and VMAX enable root cause analysis on the arrays or backup infrastructure.

The EMC VNX content pack provides the following dashboards:

- Overview
- Alerts, Faults, and System Notifications
- Commands and Background Processes

Each dashboard contains multiple widgets specific to their parent dashboard. Figure 68 displays the widgets available in the **Overview** dashboard for VNX.

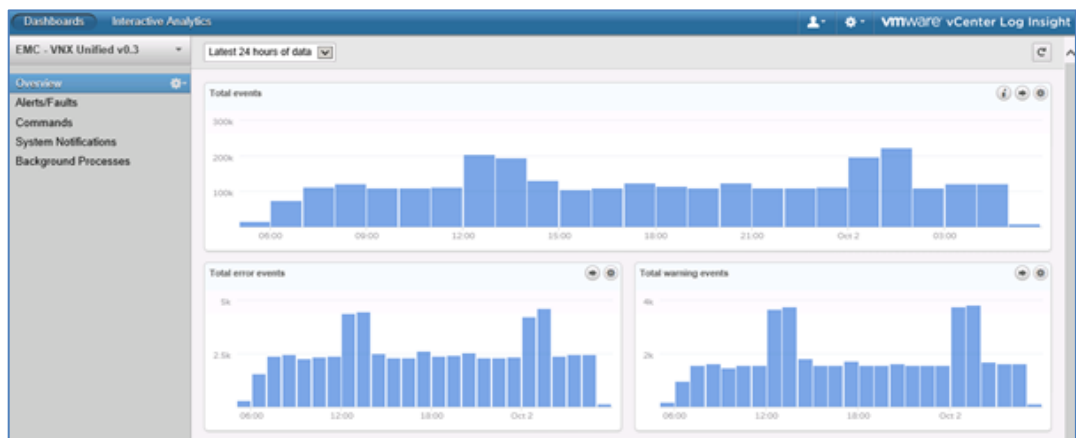


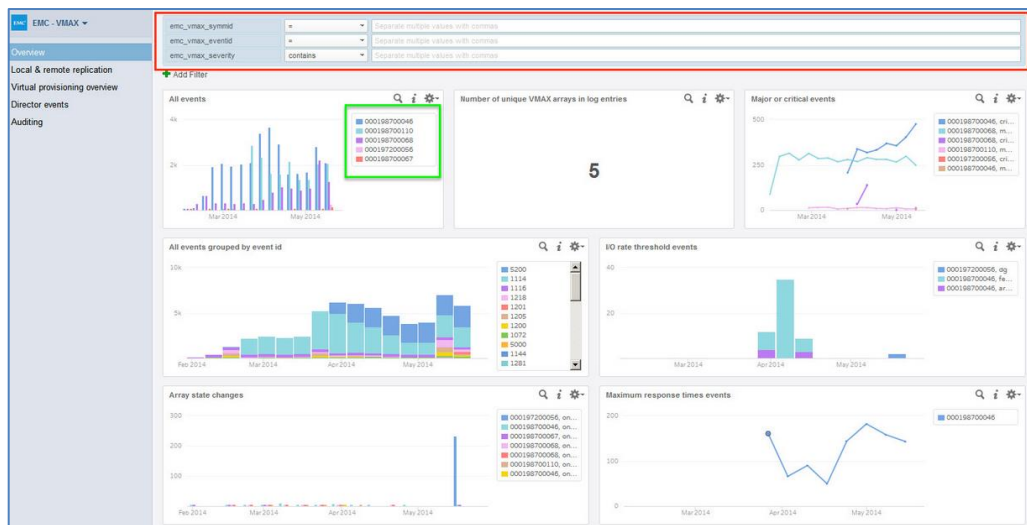
Figure 68. Sample of the dashboard view: VNX content pack



EMC has developed a custom content pack for VMAX log information and provides several dashboards that contain widgets:

- **Overview:** Widgets with information about all VMAX data in the Log Insight instance
- **Local and Remote Replication:** Widgets specific to log messages generated by SRDF or TimeFinder
- **Virtual Provisioning Overview:** Widgets with information about thin pool and device events
- **Director Events:** Widgets with information about any front-end or back-end director events on the VMAX
- **Auditing:** Widgets that display all audit log information

An example dashboard included with the VMAX content pack is provided in Figure 69.



**Figure 69. Example of EMC VMAX content pack dashboard views**

For detailed information about the VMAX content pack, refer to *Using the EMC VMAX Content Pack for VMware vCenter Log Insight White Paper*.

**References**

By navigating to the **Content Packs** area in the Log Insight UI, individual content packs can be downloaded from the VMware Solution Exchange and then imported. More information on available content packs and downloads for Log Insight is available on the [VMware Solution Exchange](#).



## Resource management

This solution uses the comprehensive resource management and reporting functionality available with EMC ViPR SRM and VMware vC Ops.

Cloud administrators can use EMC ViPR SRM through real-time dashboards or reports to understand and manage capacity and consumption of EMC ViPR software-defined storage, and monitor SLA compliance.

VMware vC Ops provides powerful virtual resource consumption and capacity planning functionality to help predict behavior, and understand the potential impact of future growth on the resources supporting the hybrid cloud environment.

### Storage resource management

The EMC Storage Resource Management Suite provides comprehensive monitoring, reporting, and analysis for heterogeneous block, file, and virtualized storage environments. It enables you to visualize application storage dependencies, analyze configurations, monitor capacity growth, and optimize the environment to improve return on investment.

ViPR SRM identifies how much raw storage is in the hybrid cloud environment, how much of the total raw storage is configured for use, how much remains unconfigured, and how much of that unconfigured storage is available on specific arrays.

Multiple storage dashboards and views are available to instantly analyze overall storage capacity and consumption in the environment.

#### **Use case: Identify and view EMC ViPR storage capacity**

The EMC ViPR virtual array consists of multiple virtual pools supported by one or more storage arrays. ViPR SRM provides the ability to analyze the virtual array and virtual pool down to the physical storage pools residing on different storage arrays.

Starting with the ViPR virtual array, a high-level report, as shown in Figure 70, provides details of available and provisioned storage capacity and the virtual pools configured in the virtual array.

---

**Note:** More details about file systems, block volumes, and storage ports are available in this report, but are not shown in Figure 70.

---



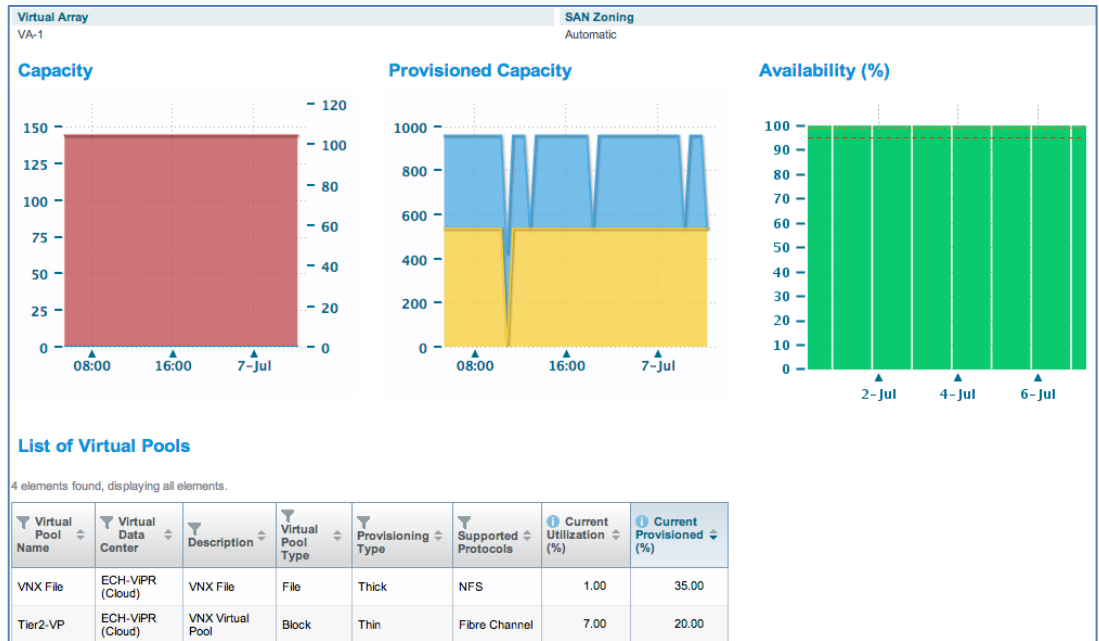


Figure 70. EMC ViPR SRM: Overview of ViPR virtual array

As shown in Figure 71, in addition to the high-level ViPR virtual pool details, the user can view lower-level details on a particular ViPR pool, including type and protocol, the provisioning and assignment types, and the capacity and utilization figures.

The virtual pool details include the physical storage array to which the virtual pool belongs. In the example in Figure 71, the virtual pool named VNX File contains a storage pool named **File Pool**, and belongs to the VNX file storage system.

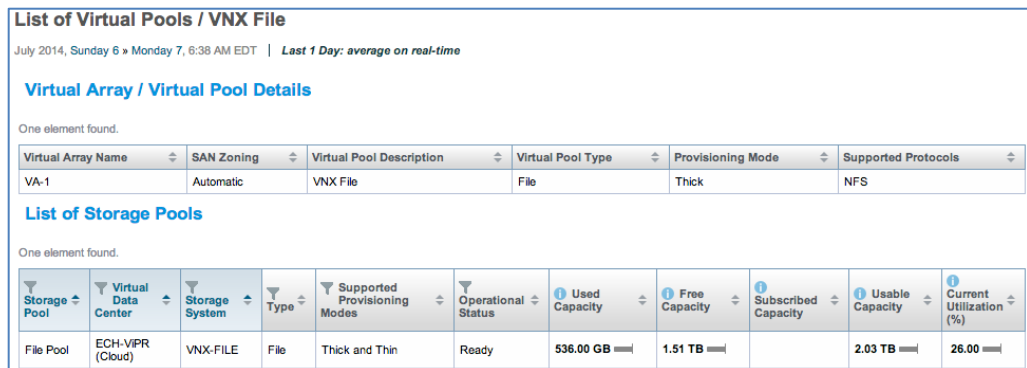
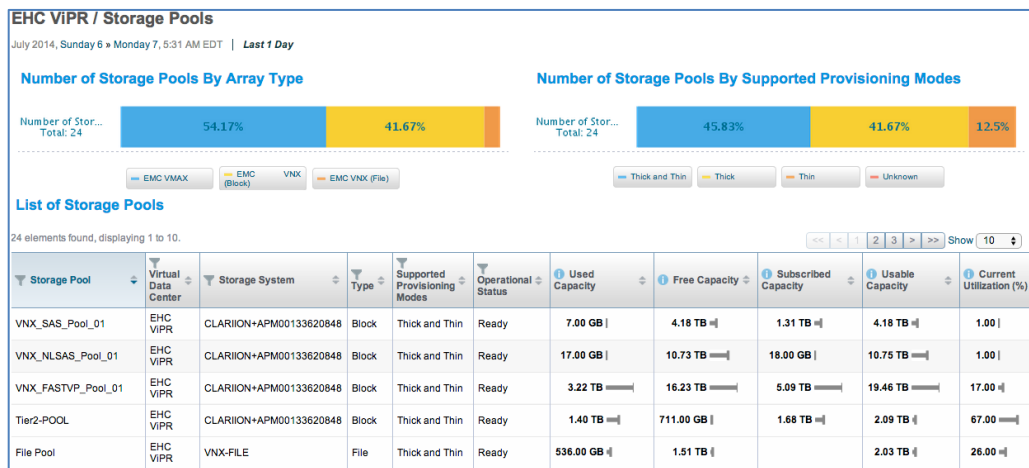


Figure 71. EMC ViPR virtual pool details

Reports can be run and views generated to display details on the physical storage pools supporting the EMC ViPR virtual pools, as shown in Figure 72. The storage pool details presented in Figure 72 map directly to the physical storage arrays that EMC ViPR manages.

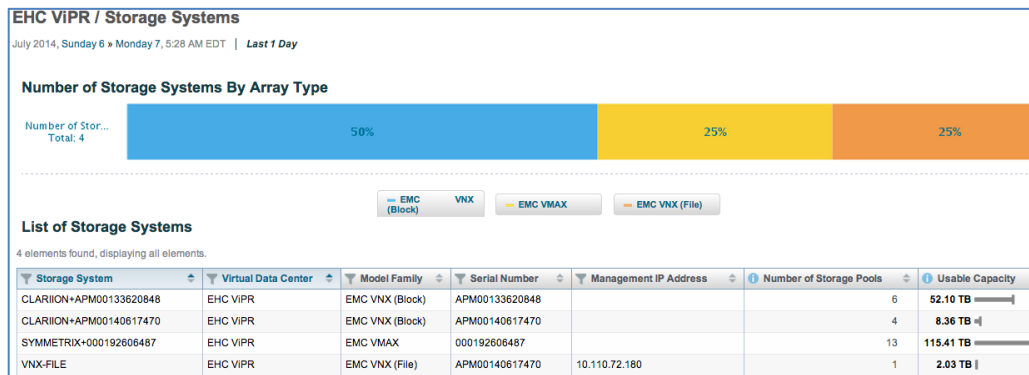






**Figure 72. EMC ViPR SRM: Storage pools supporting ViPR virtual pools**

Details on the various storage systems configured with EMC ViPR are available in the storage system report, as shown in Figure 73.



**Figure 73. EMC ViPR SRM: Physical storage systems**

All of these reports and views are available in the EMC ViPR SRM Report Library under EMC ViPR.

**Storage compliance management**

The EMC Storage Resource Management Suite provides visibility into the physical and virtual relationships in this hybrid cloud infrastructure to ensure consistent service levels.

The SRM Suite Storage Compliance SolutionPack automates the process of validating the customer’s storage infrastructure configuration against EMC’s proven best practices, providing the following functionalities:

- Monitors compliance with best practice and the EMC Support matrix
- Identifies configuration issues proactively
- Ensures that hosts, SAN, and networking are configured to meet service levels

The workflow of Storage Resource Compliance Management starts with SRM policy management. Through the SRM Administration Portal, an administrator can employ a



default user-defined SRM policy to detect configuration changes to the hybrid cloud environment that result in a breach of compliance.

**Use case: Create storage compliance policy**

This use case describes how an administrator can create a storage compliance policy.

1. Log into the SRM Administration Portal and create a new policy under **Operations > Compliance > Storage Compliance > Manage Rules & Policies > Create Policy**.
2. Select a template from the drop-down list, as shown in Figure 74.

**Figure 74. Create a storage compliance policy: Description**

3. Type the relevant policy name and description and set the state of the policy to **Enabled**.
4. Under **Scope**, create a new user-defined scope with the scope name and criteria, as shown in Figure 75.

<input type="checkbox"/>	Name	Filter
<input type="checkbox"/>	All Arrays	devtype='Array'
<input type="checkbox"/>	All ESX Servers	devtype='Hypervisor'
<input type="checkbox"/>	All Fabrics	devtype='FabricSwitch' & (partype='Fabric'   partype='VSAN')

**Figure 75. Create storage compliance policy: Scope**

The scope can be as broad or as specific as required for the storage compliance use case. Once the rules are created and the severity set, as shown in Figure 76, a schedule must be applied before the policy can be saved.



**Create Policy**  
 Select Policy from template: **EMC Best Practice Configuration**

Description Scope **Rules** Schedule

[Edit Rule](#)

Name	Description	Type
Host Must Be Provisioned with Storage	Identifies hosts that are connected to a fabric but do not have a fully established path to a storage volume; either because the host was never provisioned, or because the host has been de-provisioned but is still physically connected to a fabric.	Pathing
Masking Entry on Unmapped Volume	Violation is fired when there is a masking entry without corresponding mapping entry. This rule is applicable only to Physical Hosts and ESX Servers.	Masking

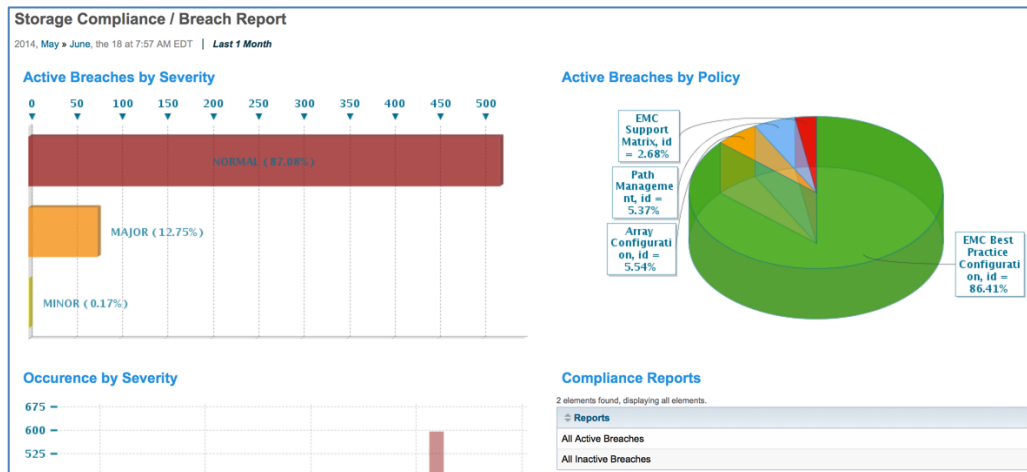
**Figure 76. Create storage compliance policy: Rules**

The new storage compliance policy can now be enabled and is ready to run.

The Storage Compliance SolutionPack downloads the EMC Support Matrix and validates your SAN's compliance with its recommendations to ensure that the configuration has been thoroughly evaluated by EMC E-Lab standards.

If there are any breaches in compliance, EMC ViPR SRM creates a breach report to enable administrators to analyze the issue. A policy breach occurs when an object in the data center violates a user-defined policy.

Figure 77 shows an example of all active breaches by severity and policy in the data center.



**Figure 77. Breach Report: Active breaches by severity and policy**

An active breach report for SAN zoning is shown in Figure 78 and is divided into three sections:

- **Breaches:** Provides information on each breach severity, device name, device type, policy, rules and breach timeline
- **Breach details:** Shows the cause of the breach and recommendation that complies with the customer and EMC best practices



- **Drill-down into device:** Provides the device summary that helps to investigate further the compliance issues

Breaches						
Severity	BreachName	Device	Device Type	Affected Objects	Policy	Rule
MAJOR	Unused Volume Masking Entries	000192606487	Array	LUN:0049	EMC Best Practice Configuration	Unused Volume Masking Entries
MAJOR	Unused Volume Masking Entries	000192606487	Array	LUN:0206	EMC Best Practice Configuration	Unused Volume Masking Entries
MAJOR	Unused Volume Masking Entries	000192606487	Array	LUN:002D	EMC Best Practice Configuration	Unused Volume Masking Entries
MAJOR	Unused Volume Masking Entries	000192606487	Array	LUN:0046	EMC Best Practice Configuration	Unused Volume Masking Entries
MAJOR	Base Connectivity Interoperability for Hosts	drm-esxi083.infra.lab.local	Hypervisor		EMC Support Matrix	Base Connectivity Interoperability for Hosts

Breach details		Drill-down into device
Message	Recommendation	Reports
1. The storage port is not actively zoned with the host port. 2. A physical connection in the path is unplugged/down.	1. Verify that the host port is up and exists in the same active zone as the storage port. 2. Verify that storage objects in the physical path are up and running. When this alert is generated, you can immediately manually rediscover the storage array to update the Repository; you do not have to wait for the next poll as specified in the relevant data collection policy.	Device Summary

**Figure 78. All Active Breaches report**

As with all reports in EMC ViPR SRM, the breach reports can be sent automatically to the relevant management team and administrators.

**Virtual machine resource management**

The use of virtual machine resources, both overutilization and underutilization, can be identified easily and managed with VMware vC Ops. Once identified, the relevant virtual machines can be remediated or resized appropriately. Capacity planning for virtual machines based on past and current consumption is also possible in vC Ops, enabling cloud administrators to calculate and plan more efficiently for current and future virtual machine deployments.

**Virtual machine capacity planning**

The capacity planning component of vC Ops provides statistics on the current utilization. It can also provide predictive what-if scenarios where infrastructure in the environment might be influenced by an increase or decrease in the number of ESX hosts, storage, or virtual machines on existing or new consumption profiles. By implementing the what-if scenario, vC Ops models can predict the impact for planning capacity requirements in advance.

As shown in Figure 79, the capacity figures are based on demand and consumption trends currently operating virtual machines.



Virtual Machine Capacity						
	Capacity Remaining	Time Remaining	VM Capacity	Deployed	Powered On	Capacity
Host CPU	19 VMs	106 days	33 VMs	13 VMs	13 VMs	73 GHz
Host Memory	1.1 VMs	11 days	14 VMs	13 VMs	13 VMs	143 GB
Disk Space	150 VMs	> 1 year	164 VMs	13 VMs	13 VMs	33 TB
Disk I/O Read	1,010 VMs	> 1 year	1,024 VMs	13 VMs	13 VMs	31 MBps
Disk I/O Write	1,010 VMs	> 1 year	1,024 VMs	13 VMs	13 VMs	61 MBps
Disk I/O Reads per Second	1,010 VMs	> 1 year	1,024 VMs	13 VMs	13 VMs	1,587 Tps
Disk I/O Writes per Second	1,002 VMs	> 1 year	1,015 VMs	13 VMs	13 VMs	1,567 Tps
Network I/O Received Rate	337 VMs	> 1 year	350 VMs	13 VMs	13 VMs	25 MBps
Network I/O Transmitted Rate	338 VMs	> 1 year	351 VMs	13 VMs	13 VMs	25 MBps
Summary	1.1 VMs	11 days	14 VMs	13 VMs	13 VMs	-

**Figure 79. Virtual machine capacity for the cloud management platform**

To plan the capacity requirements for future growth, the user can create a what-if scenario that contains a virtual machine profile that is based on an existing virtual machine or a new one, as shown in Figure 80.

The screenshot shows a 'What-if scenario' configuration window. The main section is titled 'New virtual machine configuration' and includes a 'Virtual machine count' of 20. Below this, there are sections for 'Specify new virtual machines' and 'Specify Virtual Disk configuration'. The 'Specify new virtual machines' section includes fields for vCPU (2), Reservation (0), Limit (0), Memory (2048 MB), and Utilization (35%). The 'Specify Virtual Disk configuration' section includes fields for Virtual Disk Type (Thin), Configuration (50 GB), and Utilization (50%). On the right side, there is a 'VM Population' summary panel showing 'Population Summary' and 'Population Details' for 'Small VM Profile', 'Medium VM Profile', and 'Host Population'.

**Figure 80. Specify a reference virtual machine configuration**

As shown in Figure 80, the virtual machine profile can be tailored to specify not just the allocation of resources but also their actual usage and consumption. After adding 20 new virtual machines, details for virtual machine capacity are updated to display the new values for capacity remaining, as shown in Figure 81.



Capacity Remaining		
	Actual	Add 20 New VMs
Host CPU	19 VMs	4.1 VMs
Host Memory	<b>1.1 VMs</b>	<b>Over by 5 VMs</b>
Disk Space	150 VMs	259 VMs
Disk I/O Read	1,010 VMs	990 VMs
Disk I/O Write	1,010 VMs	990 VMs
Disk I/O Reads per Second	1,010 VMs	990 VMs
Disk I/O Writes per Second	1,002 VMs	976 VMs
Network I/O Received Rate	337 VMs	335 VMs
Network I/O Transmitted Rate	338 VMs	336 VMs
<b>Summary</b>	<b>1.1 VMs</b>	<b>Over by 5 VMs</b>

Figure 81. What-if scenario: Adding 20 new virtual machines

### Virtual machine resource optimization

In situations where resources are limited, vC Ops can identify reclaimable, underutilized resources in idle or oversized virtual machines. For resource optimization, the **Waste** dashboard compares configured and recommended CPU and memory metrics and determines oversized virtual machines, according to actual resource consumption over a defined time period.

The definition of underutilized or overutilized virtual machines is based on policy and is customizable to suit specific business requirements, as shown in Figure 82. Multiple policies can be created and applied, as appropriate.

Figure 82. Edit policy to specify thresholds for virtual machines

The dashboard detail provides a list of oversized virtual machines, with recommended optimal resource configurations of appropriate values for CPU and RAM resources according to real consumption history, as shown in Figure 83.



Details			
Oversized Virtual Machines			
Virtual Machine ▾	Policy	Configured vCPU	Recommended vCPU
Win2k8R2_SP2010	Default Policy	2 vCPUs	1 vCPUs
WIN2K8R2_Exchange	Default Policy	2 vCPUs	1 vCPUs
vipr3	Default Policy	4 vCPUs	1 vCPUs
vipr2	Default Policy	4 vCPUs	1 vCPUs
vipr1	Default Policy	4 vCPUs	2 vCPUs
vCloud Automation Center - IaaS	Default Policy	4 vCPUs	4 vCPUs
vCloud Automation Center	Default Policy	2 vCPUs	1 vCPUs
vCloud Application Director	Default Policy	2 vCPUs	1 vCPUs
vCenter Orchestrator	Default Policy	2 vCPUs	2 vCPUs
vCenter Log Insight	Default Policy	4 vCPUs	2 vCPUs

**Figure 83. List of oversized virtual machines**

### Running vC Ops reports

Reports in vC Ops provide a more formal reporting structure for the various views and summaries available. Each report can have a specific schedule attached or can be run manually.

When a report is successfully run, it can be downloaded in either PDF or CSV format along with previously run instances of the same report.

The scope of reporting with vC Ops in this EMC Enterprise Hybrid Cloud solution includes the cloud management platform and the cloud resources used by vCAC.

## Metering

The hybrid cloud environment requires flexible metering and costing models that can account for the utilization of all resources within the environment. VMware ITBM Suite Standard Edition is a valuable business management tool in VMware's cloud management portfolio. It is designed for customers looking for a simplified management solution that will help provide them with focused cloud infrastructure costing. ITBM provides the costs for virtual machines and utilization of shared resources to help better manage demand, budget for the future, and view capital and operating expenditures, while driving accountability over cloud resources to lower TCO.

As shown in Figure 84, the ITBM Suite is integrated as part of vCAC to provide business management and cost transparency capabilities in a virtual infrastructure.





Figure 84. ITBM overview

ITBM enables the cloud administrator to:

- Determine the pricing of vCAC blueprints by using the current cost and utilization levels of virtual machines as a reference.
- Make decisions related to the placement of workloads based on the cost and services that are available in the hybrid cloud environment.
- Provide chargeback cost of virtual machine and blueprints based on the business unit and application group in the hybrid cloud environment.
- Manage costs based on capital and operating expenditures.
- Get an accurate cost of virtual machines without performing financial configurations.

The charts displayed on the dashboard, as shown in Figure 84, are fully interactive. The dashboard displays with projected information for the current month. ITBM performs monitoring of the environment, collects new usage statistics, recalculates the displayed data over time, and updates the graphics, as necessary.

More detailed information for each topic is available as you navigate the ITBM Suite. More detailed reports with breakdowns of machine quota, memory, and storage usage by business group, virtualization compute resources, and blueprints are available in **Reports**.





**Metering analysis** ITBM is integrated with VMware vCenter and can import existing resource hierarchies, folder structures, and vCenter tags to organize hybrid cloud resource usage with business units, departments, and projects.

ITBM contains a number of analysis views containing information:

- Operational analysis
- Demand analysis

### Operational analysis

Operational analysis enables the cloud administrator to analyze the costs of the underlying service resources of your hybrid cloud. These resources include CPU, RAM, storage, and operating system (license and labor).

The operational analysis module accepts the total monthly operating cost in the cloud infrastructure, as modeled by using the cost driver component as input, and arrives at the base rate for CPU and RAM, expressed in terms of dollars per gigahertz and dollars per gigabytes of CPU and RAM respectively. The derived base rates for CPU, memory, and storage configured in the cost driver are used to calculate the total monthly operating cost. Certain costs are directly attributed to the virtual machines, for example, desktop operating system licenses and labor costs are classified under the heading of **OS (License and Labor)**.

As shown in Figure 85, this dashboard enables the user to visualize the total loaded cost of CPU, RAM, storage, OS, and virtual machines running on different generations of servers and costs.

This information enables the cloud administrator to optimize workload placements based on the generation of hardware (for example, virtual machines on older servers might cost more than the virtual machines on new servers) and get visibility of how costs for CPU and RAM are trending over time.

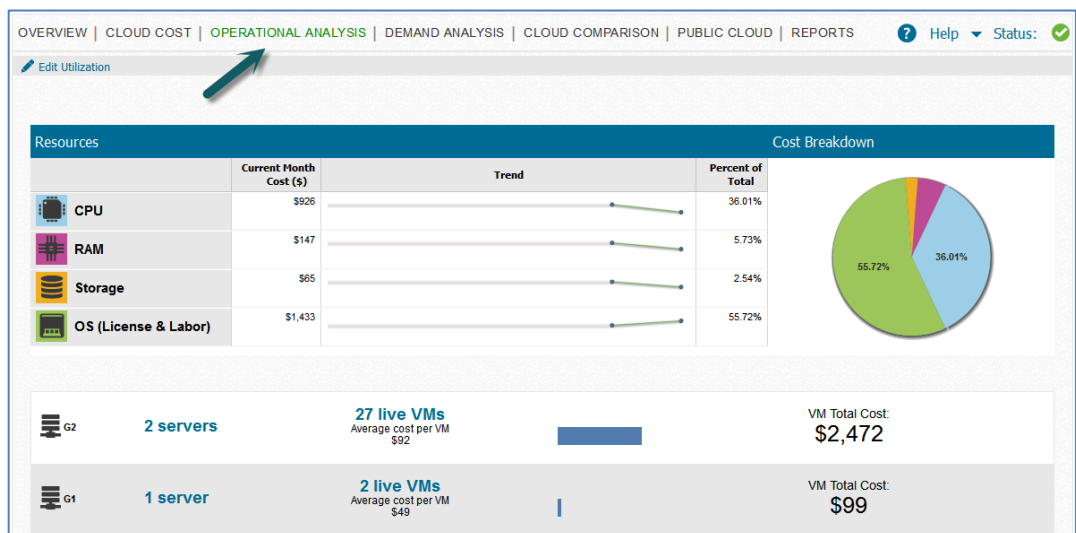


Figure 85. ITBM operational analysis of a hybrid cloud environment



The cloud administrator can adjust how the cost allocation occurs in the virtual infrastructure. The total loaded cloud cost includes hardware, operating systems, maintenance, network, labor, and facility costs. These costs are allocated on the virtual infrastructure. To compute the loaded unit cost of CPU and RAM, the administrator can specify the expected CPU value and memory utilization, as shown in Figure 86.

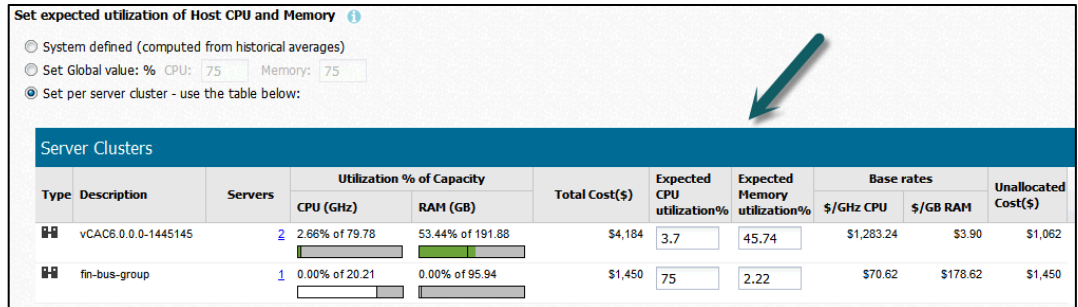


Figure 86. ITBM: Set expected utilization of CPU and RAM

The utilization levels of clustered and unclustered hosts are derived from the average monthly usage data from vCenter. This enables the cloud administrator to understand the loaded costs by cluster and to manage unallocated costs based on utilization levels.

### Demand Analysis

Through Demand Analysis, the VMware ITBM Suite Standard Edition enables the user to easily identify their cloud resource consumers, the purpose for which they are being consumed, and the costs associated with running those resources.

Figure 87 shows a list of cost centers that provides cost and usage of CPU, RAM, and storage of virtual machines for the current month, categorized based on the application, and the business unit. It also shows the monthly usage trend in a linear graphical manner. The data is displayed at the beginning of the month based on the previous month's averages. It is updated throughout the month as utilization varies.

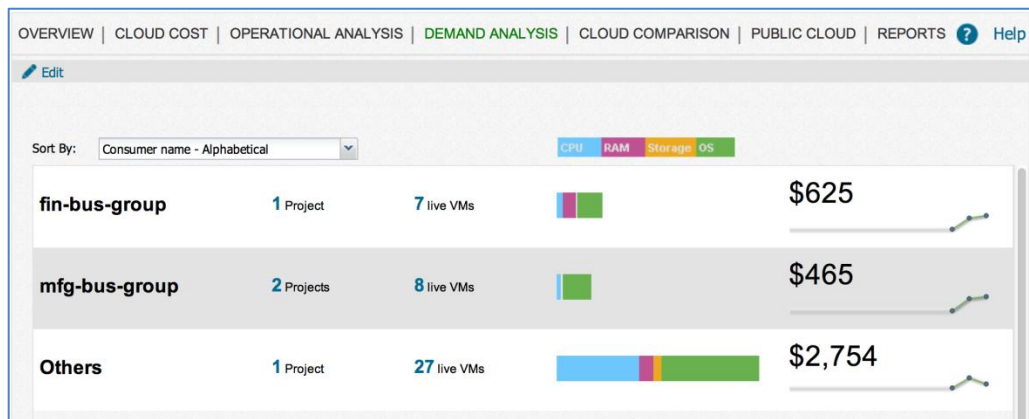
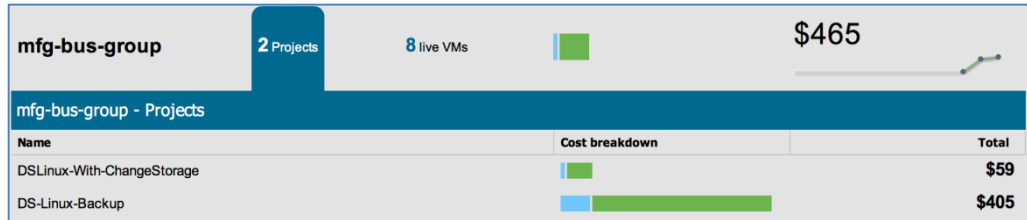


Figure 87. ITBM Demand Analysis of hybrid cloud

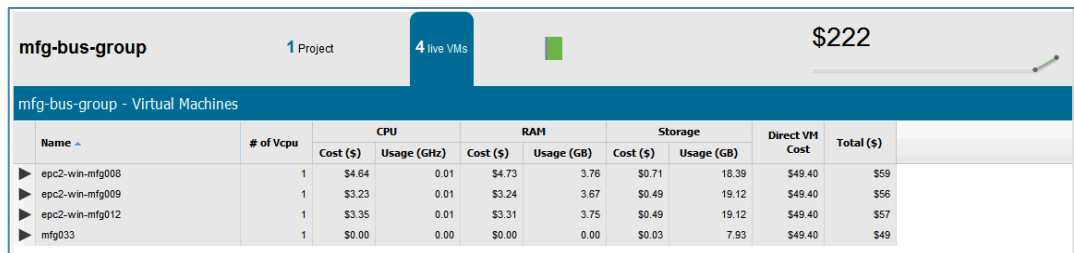


ITBM provides intuitive navigation to detailed information. By clicking **Projects**, the cloud administrator can view a breakdown of applications and the total cost of virtual machines for each of the applications, as shown in Figure 88. This also provides a visual view of cost and usage of CPU, RAM, and storage for virtual machines, categorized based on the application in that business unit.



**Figure 88. ITBM Demand Analysis: Application costs**

Click **live VMs** to show a detailed breakdown of cost and usage data for each cloud resource, as shown in Figure 89. This view provides a list of virtual machines and usage by CPU, RAM, storage, OS, and costs for each component. Click each virtual machine to show the virtual machine resource cost history chart.



**Figure 89. ITBM Demand Analysis: Virtual machine costs**

### Metering reporting

ITBM Standard Edition has a powerful reporting engine that provides information about various system objects such as servers, datastores, virtual machines, virtual machines of the public cloud, and clusters, to visualize capital expenditure (CAPEX) and operational expenditure (OPEX) costs. ITBM reports allow this information to be exported in CSV format for further analysis.

ITBM provides the user with the following reports containing detailed information for the selected topics:

- **Servers:** Provides details about all servers that run your hybrid cloud and is expandable to provide details for each cost driver
- **Datastores:** Provides details about each of the datastores seen by vCenter Servers that ITBM is monitoring
- **VMs:** Provides details about all virtual machines running in the environment
- **Clusters:** Provides details about the servers within the clusters of the virtual environment



The **Servers** report, shown in Figure 90, has details for all servers hosted in the hybrid cloud. You can add more server information by selecting cost drivers such as server hardware, OS licensing, maintenance, physical server labor, network, facilities, other costs, and allocation costs. ITBM Standard Edition also displays the total loaded costs of servers.

Servers							
Server Details							
Server ID	vCenter Server ID	Host Name	Description	CPU GHz	RAM GB	CPUs	Cores per CPU
45	5	vcac6-beta02.dts.lab.esg.local	Intel(R) Xeon(R) CPU X5680 @ 3.33GHz	3.30GHz	96GB	2	12
24	5	vcac6-beta01.dts.lab.esg.local	Intel(R) Xeon(R) CPU X5680 @ 3.33GHz	3.30GHz	96GB	2	12
204	5	fin-bus01.dts.lab.esg...	Intel(R) Xeon(R) CPU E5540 @ 2.53GHz	2.50GHz	96GB	2	8

Figure 90. ITBM Server report: Part I

The **Servers** report displays details such as server ID, vCenter Server ID, host name, description, CPU, RAM, and various other useful details. ITBM appends color-coded sections to the report for every cost driver metric that is selected in each report. The cost drivers can be configured as appropriate.

The server hardware detail, shown in Figure 91, contains information relating to the purchase date of the server, the original price, the depreciated value, the current reference price, and the total monthly cost.

Servers						
Server Hardware						
Cluster Name	Cluster ID	Launch Date	Purchase			
			Purchase Date	Original Purchase Price	Depreciated value	Current Reference Price
vcac6.0.0.0-1445145	213	2010 Q1	06/01/2012	\$10,616	\$4,883	\$10,616
vcac6.0.0.0-1445145	213	2010 Q1	06/01/2012	\$10,616	\$4,883	\$10,616
fin-bus-group	214	2009 Q1	01/01/2014	\$8,135	\$8,135	\$8,135

Figure 91. ITBM Server report: Part II Server Hardware

Figure 92 shows the licensing cost metrics selected in the **Servers** view. The metrics show the licensing cost amortized monthly and by operating system, the number of sockets being licensed, and the associated per-socket costs.

Servers						
OS Licensing						
Server OS						
Sockets	Cost per socket	Operating Systems	Windows Server Cost	Redhat Cost	Suse Cost	Other Operating Systems Cost
2	\$400	3	\$400	\$0	\$200	\$200
2	\$400	3	\$400	\$0	\$200	\$200
2	\$100	1	\$0	\$200	\$0	\$0

Figure 92. ITBM Server report: Part III OS Licensing

The **VMs** report, shown in Figure 93, has details for all virtual machines running in the hybrid cloud. The report can be viewed in a grid view or in a vCenter Server folder



structure. This report contains all of the virtual machine specifications and usage and utilization details that contribute to the total price.

VMs					
VM Name	Entity ID	vCenter Server ID	vCPUs	CPU GHz (Configured)	RAM GB (Co
vcac6svr - 10.110.76.101	21	5	4	3.30GHz	
vipr1	23	5	4	3.30GHz	
nsx-nsxm01	25	5	4	3.30GHz	
vcac6-srv - 10.110.76.80-OLD	27	5	4	3.30GHz	

**Figure 93. ITBM VMs report**

The reports show the various cost drivers such as storage cost, compute cost, OS labor, OS licensing, OS maintenance, VI labor, and direct cost. A total monthly cost is displayed at the end of each row, as shown in Figure 94.

VI Labor		Direct Cost	Tags	Monthly Uptime		Total VM Monthly Cost
Hourly Rate	Total			Hours	%	
\$49.40	\$4.4460	\$49.40		24	7.14%	<b>\$113.63</b>
\$49.40	\$4.4460	\$49.40		23	6.85%	<b>\$172.73</b>
\$49.40	\$4.4460	\$49.40		24	7.14%	<b>\$118.46</b>
\$49.40	\$4.4460	\$49.40		17	5.06%	<b>\$117.68</b>

**Figure 94. ITBM VMs report with Total VM Monthly Cost**

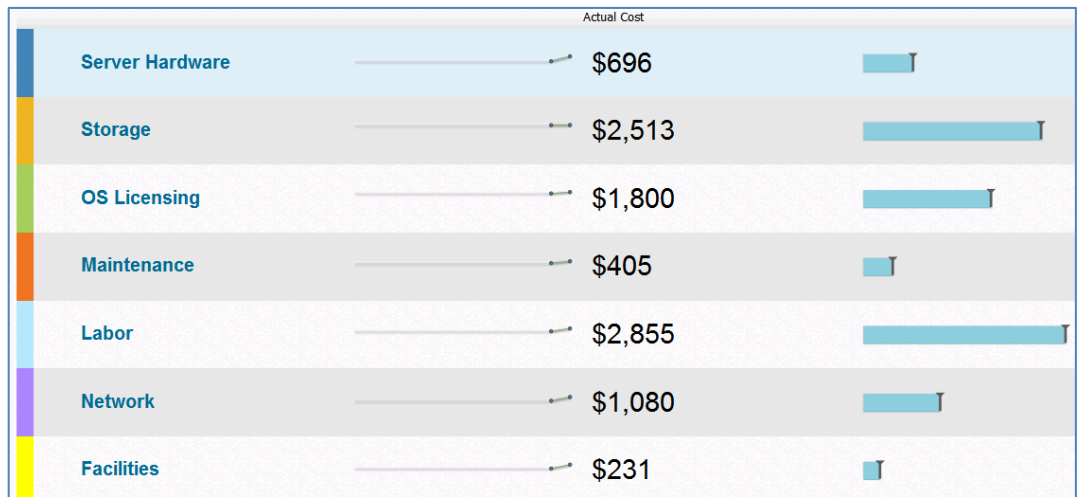
The report can be sorted based on consumers, applications, and vCenter tags. As with the other reports, this report can be exported into a CSV format to be used with other applications.

### Cost drivers

Cost drivers are the costs that are incurred in managing a data center. The Business Management Administrator can manually input the cost drivers. If cost drivers are not input, the values are obtained from the reference database included with the ITBM Standard Edition.

ITBM Standard Edition categorizes the cost drivers into **Server Hardware, Storage, OS Licensing, Maintenance, Labor, Network, Facilities**, and **Other Costs**, as shown in Figure 95. The cost driver data that you provide is the monthly cost, except for the server hardware cost.

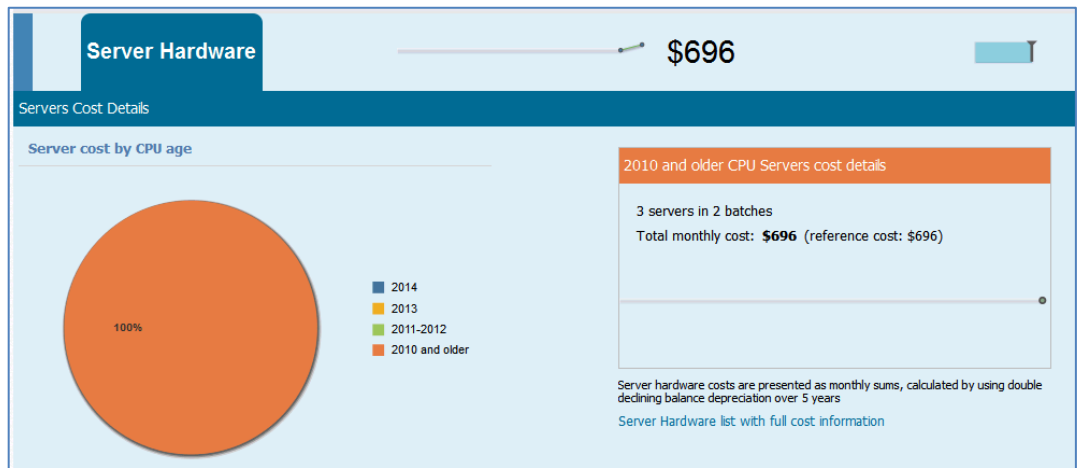




**Figure 95. ITBM cloud cost overview**

These costs can be displayed as percentage value or unit rate and might not always show the actual cost. The final amounts of cost drivers are calculated by the user's inputs. If the inputs are not provided for cost drivers, the default values are taken from the reference database, which is part of the ITBM Standard Edition product.

The cloud cost view enables the user to visualize all of the factors that affect the cost of the environment. Figure 96 shows an example of this view.



**Figure 96. ITBM cloud cost: Server Hardware details**

In addition to breaking down the costs into categories, the ITBM cloud cost displays the chart view of the monthly costing trends, the actual cost, and the reference cost. The costs have been calculated using the default cost drivers from the ITBM reference database. The information in the database is derived from industry standards data and vendor-specific data.

Figure 97 shows the edit screen. The administrator can manually edit the monthly cost of all eight cost drivers from the current month and onward. The configuration



used for cost drivers determines how ITBM Standard Edition calculates and displays the cost.

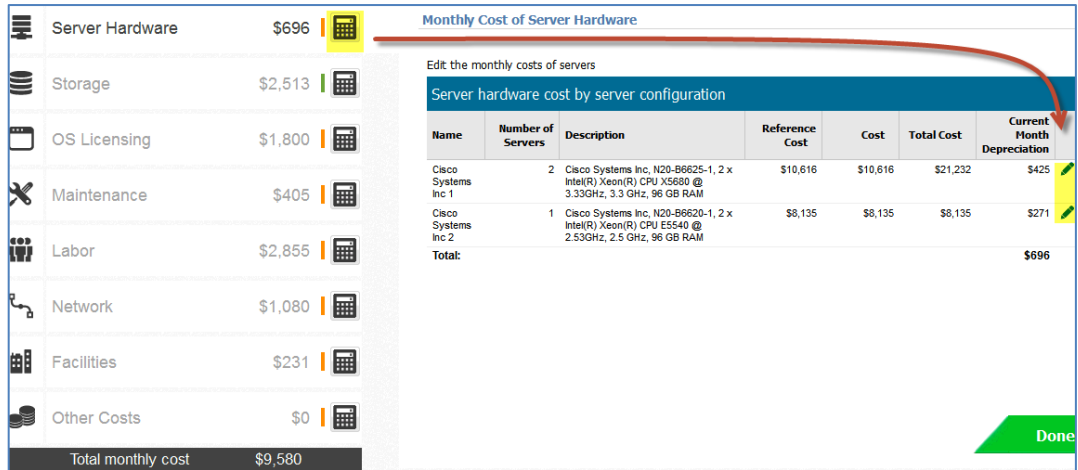


Figure 97. ITBM cloud cost: Edit monthly costs of server hardware

### Cost profiles

VMware ITBM Standard Edition uses the reference database, which is preloaded with industry standards data and vendor-specific data to generate the base price for vCPU, RAM, and storage values. These prices, which show the default cost of CPU, RAM, and storage, are automatically used by the vCAC, as shown in Figure 98. This feature eliminates the need to manually configure cost profiles in vCAC and assign them to compute resources, as shown for storage resources.

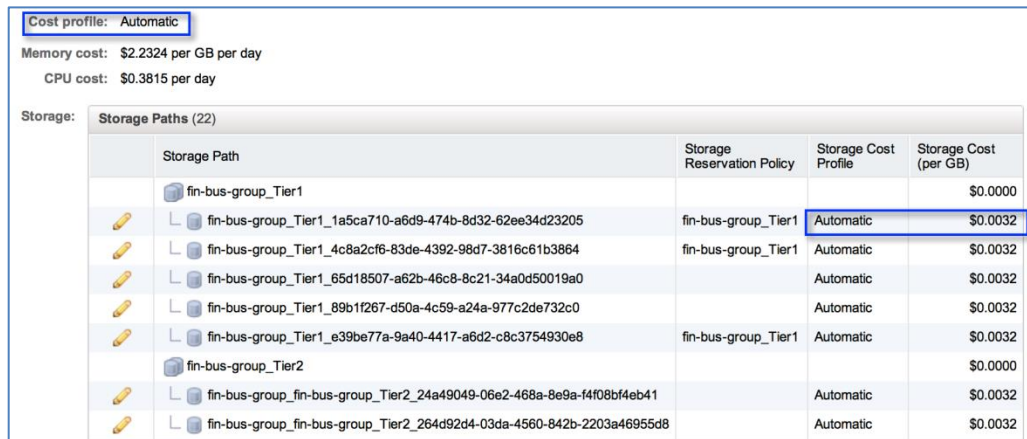


Figure 98. ITBM Automatic cost profile for storage resources in vCAC

Through its integration with VMware vCenter and vCAC, ITBM enables the cloud administrator to automatically monitor the utilization of storage resources provided by EMC ViPR.

Storage profiles are created and based on the storage capabilities of each type of storage presented to the storage service offerings. This integration enables ITBM to automatically discover, group, and meter datastores in line with their storage profile.



Figure 99 shows that the storage profiles created in vCenter are discovered by ITBM where appropriate storage cost profiles are applied. This enables the business management administrator to group tiered datastores provisioned with ViPR and set the monthly cost per GB as needed.

Edit the total monthly cost per GB for storage based on:

Storage Profile     Storage Type

Storage monthly costs by storage profile					
Profile	Datastores	Total GB	Reference Cost	Monthly Cost Per GB	Monthly Cost
Tier-2	2	999.5	\$0.10	\$0.07	\$70
Tier-3	2	999.5	\$0.10	\$0.05	\$50
Uncategorized	28	47344.05	\$0.10	\$0.10	\$4,734
<b>Total:</b>					<b>\$4,854</b>

**Figure 99. VMware ITBM chargeback based on storage profile of datastore**

If the predefined price points are not appropriate, the ITBM administrator can manually configure the price of the vCPU, RAM, and storage values. This enables the administrator to:

- Select **Set Default prices**, where price is the cost for CPU, RAM, and storage
- Manually set the prices for each of the clusters and unclustered hosts
- Manually set the price for each of the datastores

**ITBM integration with vCAC and vCenter**

ITBM Standard Edition is integrated as part of vCAC and is displayed as a screen in the vCAC self-service portal. This solution uses VMware vCenter Server as its endpoint, so ITBM is configured to manage that vCenter Server.

After entering the appropriate administrative credentials for the vCenter Server and establishing a connection, ITBM can monitor the vCenter inventory.

**Summary**

This solution, using VMware vCenter Operations Manager and EMC ViPR SRM, provides comprehensive visibility of cloud infrastructure and applications, with proactive SLA management, automated operations management for maximum utilization, and operational efficiency.

With an integrated cloud operations management approach, VMware vCenter Log Insight provides the operational intelligence and enterprise-wide visibility needed to proactively ensure service levels and operational efficiency in this EMC Enterprise Hybrid Cloud solution.

With the integration of ITBM into the self-service portal for the cloud administrator, VMware vCAC addresses the metering and chargeback of all resources assigned and used within the vCAC-managed hybrid cloud in this solution.





## Chapter 6 Security

This chapter presents the following topics:

<b>Overview of cloud security challenges .....</b>	<b>106</b>
<b>Public key infrastructure X.509 integration.....</b>	<b>107</b>
<b>Converged authentication .....</b>	<b>109</b>
<b>Role-based access control .....</b>	<b>113</b>
<b>Centralized log management .....</b>	<b>115</b>
<b>Security configuration and management .....</b>	<b>119</b>
<b>Multitenancy.....</b>	<b>123</b>
<b>Summary.....</b>	<b>128</b>



## Overview of cloud security challenges

While many organizations have successfully introduced virtualization as a core technology within their data center, some have not experienced the benefits of cloud computing, such as increased agility, mobility, and control. Many organizations are now under pressure to provide secure and compliant cloud services to address these evolutionary needs. As a result, IT departments need to create cost-effective alternatives to public cloud services that do not compromise enterprise security features such as data protection, disaster recovery, and guaranteed service levels.

Security challenges must be addressed for organizations to maintain or improve their security posture while enabling the business. Some of the challenges addressed in the EMC Enterprise Hybrid Cloud are:

- Lack of trust
- Disjointed authentication mechanisms
- Lack of coordinated event tracking
- Inconsistent application and server configurations
- Difficulty in maintaining multitenancy

EMC Enterprise Hybrid Cloud implements a variety of security features to control network access, monitor system access, monitor user activity, and support the transmission of encrypted data. The security features related to EMC Enterprise Hybrid Cloud are implemented on EMC and VMware components that constitute the solution.

This chapter provides feature information and configuration options available for secure system operation. It explains when to use security features and why they are relevant. It includes the following sections:

- Public key infrastructure X.509 integration
- Converged authentication
- Centralized log management
- Security configuration management
- Multitenancy



## Public key infrastructure X.509 integration

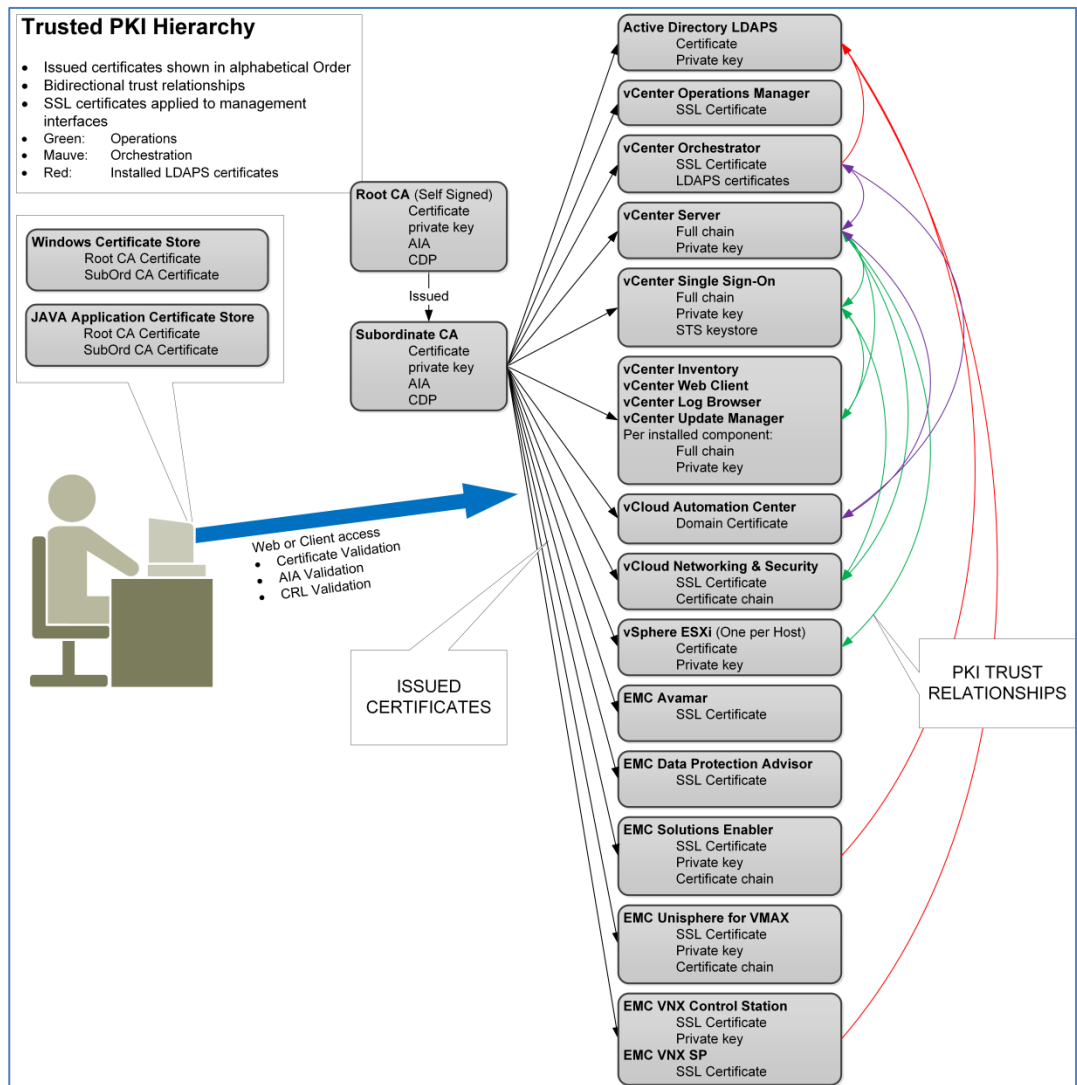
Integrating a PKI infrastructure in a multitenant EMC Enterprise Hybrid Cloud environment ensures that all the components that make use of X.509 certificates and technology are trusted. By default, components are installed or factory shipped with self-signed X.509 certificates. These are considered untrusted because the authenticity of who issued or signed them cannot be verified and, by extension, the application or device cannot be trusted. In such an environment, an attacker could impersonate a device or application to perform man-in-the-middle attacks or harvest administrative credentials for subsequent use in compromising other systems on the network. A successful administrative attack is more serious because of the elevated privileges usually given to systems administrators to fulfill their duties. Certain regulated industries and governments, such as the U.S. Department of Defense, only use trusted certificates.

Integration with a trusted PKI addresses this problem by establishing a chain of trust from the trusted X.509 certificate installed on the device or application through the issuing certification authority (CA) to the root CA. In addition, it provides a means to validate this trust by publishing Authority Information Access (AIA) and Certificate Revocation Lists (CRLs).

### Enterprise PKI architecture

Figure 100 shows the hierarchal relationship of the PKI environment with the root self-signed certificate, the issuing CA certificate, and the end-entity-issued certificates. Figure 100 also shows the trust relationship between the end-entity certificates used in the EMC Enterprise Hybrid Cloud and the end user.





**Figure 100. PKI hierarchy for EMC Enterprise Hybrid Cloud solution stack**

All issuing CA and end-entity certificates have URLs where the root and subordinate CA certificates are located defined for the AIA, in addition to the location for the CRL Distribution Point (CDP) that contains a list of revoked certificate serial numbers. The end-entity certificates were issued by the subordinate CA and requested with a Subject Alternative Name that consists of a fully qualified domain name (FQDN), hostname, and IP address.

**Enterprise PKI solution integration**

Part of hardening the infrastructure is to replace the self-signed X.509 certificates with valid signed certificates from a trusted CA. Some organizations may choose to use an external entity for this.

The EMC Enterprise Hybrid Cloud is configured with an internal CA using a hierarchical structure, as shown in Figure 100. This shows the CA architecture with the root at the top level, which is either offline or air-gapped. Subordinate CAs are tiered in the Active Directory forest.



Safeguards should be put in place to protect the private keys used by the CAs. A virtualized environment can use using network-based hardware security modules (HSMs), to store the CAs' private keys in a secure manner with tamper protection. HSMs can also provide offloading of certain cryptographic processing for symmetric or asymmetric needs where performance is a requirement.

The PKI used in the EMC Enterprise Hybrid Cloud is based on the deployment of the Active Directory Certificate Services. You must follow best practices when designing your organization's PKI infrastructure and take additional security measures to ensure protection of the private keys in use by the CAs.

### **Microsoft Active Directory—LDAP over SSL certificates**

LDAP is the protocol by which many applications submit authentication or authorization requests. LDAP introduces a significant security risk because credentials (username and password) are passed over the network unencrypted.

We can significantly strengthen the security of these authentication and authorization communications by encrypting the entire LDAP session with SSL, known as LDAP over SSL or LDAPS. By default, Active Directory is not configured to support LDAPS, so certain steps must be taken to integrate Active Directory with a trusted PKI to enable LDAPS.

The Active Directory LDAP over SSL (LDAPS) certificate is issued by the subordinate CA and requested on each participating domain controller using the certificate's Microsoft Management Console (MMC). The certificate is installed in the domain controller certificate store and is used by Active Directory Domain Services to apply to the LDAP protocol to secure authentication and authorization communications.

For more information about integrating PKI and centralized authentication in a cloud environment, complete with configuration procedures, refer to *EMC Integration of PKI and Authentication Services for Securing VMware vCloud Suite 5.1 Environments Proven Solution Guide*.

## **Converged authentication**

This section introduces integration of authentication mechanisms with a centralized directory and includes the following sections:

- Microsoft Active Directory LDAPS
- Windows authentication and service accounts
- VMware vCenter SSO
- Terminal Access Controller Access Control System Plus (TACACS+) authentication integration



**Secure authentication**

A significant challenge in securing any environment is controlling access to the solution's resources. This is addressed in part through PKI by implementing trusted certificates that allow the authenticity of applications and devices to be verified, and that encrypt administrator access to the management interfaces.

Another challenge is the use of disparate authentication containers and policies across distributed hardware and software components. EMC Enterprise Hybrid Cloud relies on secure services from Active Directory to centralize authentication services for VMware, EMC, and Cisco components.

In the EMC Enterprise Hybrid Cloud, Active Directory provides a single point of control for account management and policy enforcement. In addition, it provides Kerberos and LDAPS authentication, and authorization services. TACACS+ has been integrated with Active Directory to support devices that do not provide direct integration with Active Directory.



Figure 101 shows the hierarchy of authentication communication paths used in the EMC Enterprise Hybrid Cloud.

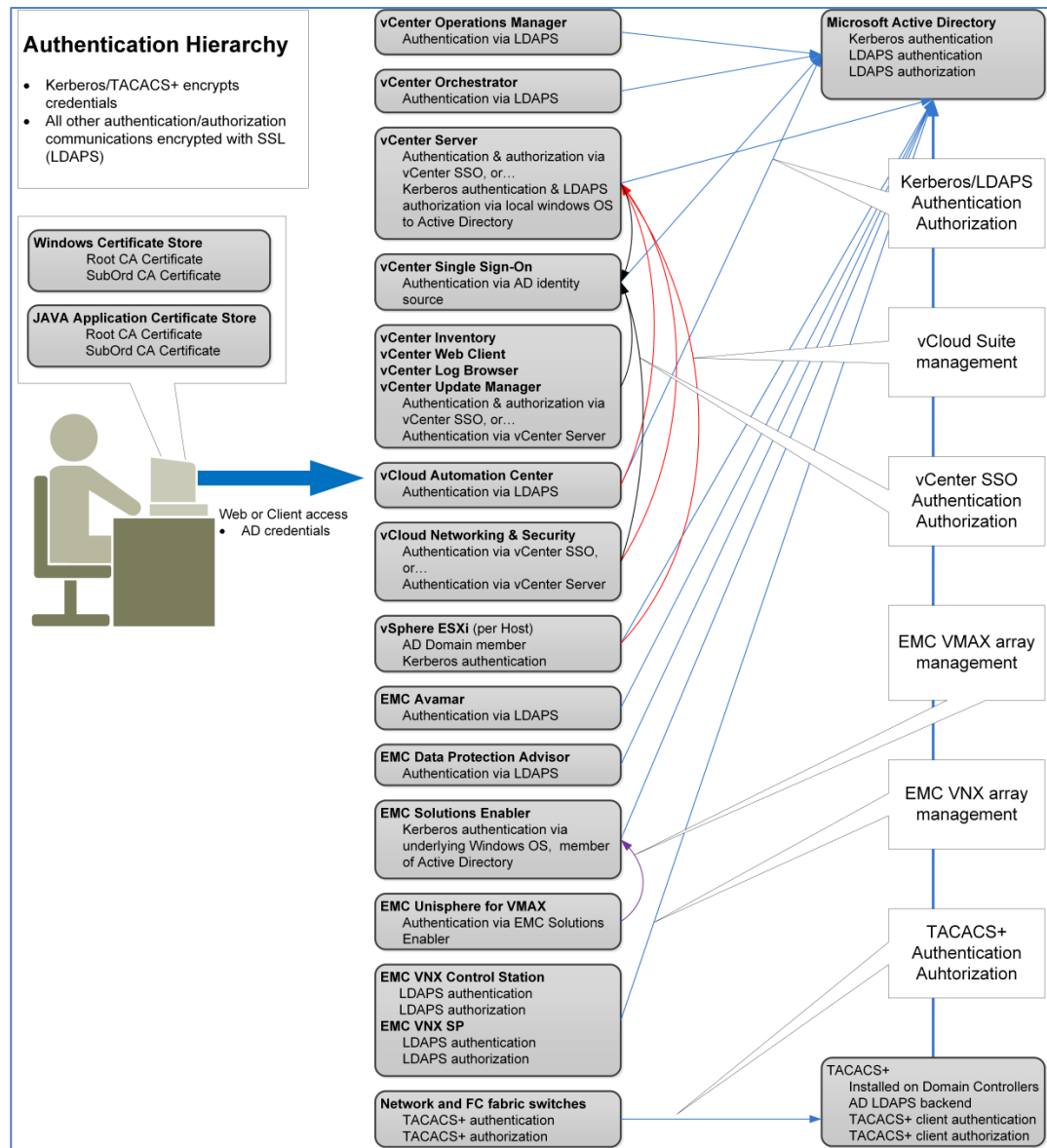


Figure 101. Authentication relationships between the solution components



## Microsoft Active Directory

Encrypt the authentication session to avoid exposing clear text account credentials when an application or system authenticates users using a simple BIND request to the directory.

To enable LDAPS, an authentication certificate issued by a trusted CA is installed on each domain controller that will service authentication requests.

### Windows authentication and service accounts

In a production environment, use service accounts to track and control applications, and to mitigate the impact of a potential systems compromise.

### Integrated Windows authentication

The integrated Windows authentication feature in Microsoft SQL Server provides better security than SQL Server authentication by taking advantage of Active Directory user security and account mechanisms. When an application connects through an Active Directory user account, SQL Server validates the account name and password using the Active Directory principal token in the operating system. This means that Active Directory confirms the user identity. SQL Server does not ask for the password and does not perform the identity validation.

Integrated Windows authentication uses the Kerberos security protocol, and provides a centralized mechanism for password policy enforcement with regard to complexity validation for strong passwords, support for account lockout, and password expiration. Integrated Windows authentication offers additional password policies that are not available for SQL Server logins.

### Windows service accounts

Microsoft recommends isolating critical services under separate, low-rights Active Directory or local user accounts to reduce the risk that one compromised service could be used to compromise other services.

The hierarchy of accounts (from least privileged to most privileged) that can be used is:

1. Domain user (non-administrative)
2. Local user (non-administrative)
3. Network service account
4. Local system account
5. Local user (administrative)
6. Domain user (administrative)

Account types 1 and 2 are preferred as they best encompass the principle of least privilege. Local system is a very high-privileged built-in account. It has extensive privileges on the local system and acts as the computer on the network. Account types 5 and 6 are less secure, since they grant too many unneeded privileges.

The following products can be directly integrated with Active Directory:

- vCenter Log Insight





- vCenter Operations Manager
- vSphere ESXi hypervisor
- EMC Unisphere
- EMC ViPR

### VMware vCenter SSO

vCenter provides Single-Sign On (SSO) capability for vCloud Automation Center users. SSO is an authentication broker and security token exchange that interacts with the enterprise identity store (Active Directory or OpenLDAP) to authenticate users.

These solution components can be indirectly integrated with Active Directory through vCenter SSO:

- vCenter Orchestrator
- vCenter Server
- vCloud Application Director
- vCloud Automation Center
- ITBM

VMware vCloud Application Director and ITBM integrate directly with vCAC and use vCAC configured authentication providers, that is, Active Directory through SSO.

---

**Note:** The VMware Identity Appliance can be used in place of vCenter SSO.

---

### TACACS+ authentication integration

The EMC Enterprise Hybrid Cloud relies on TACACS+ to provide Active Directory authentication integration for network and storage switch infrastructure. TACACS+ provides an increased level of security through authentication, authorization, and accounting services, and is a publicly documented protocol over TCP/IP. It encrypts credentials passed from the client device to the TACACS+ system and can be configured to use Active Directory as its authentication directory to enable centralized authentication.

## Role-based access control

Throughout each element of the solution, local roles are mapped to Active Directory groups for the purposes of administration, operation, and auditing. However, the vCAC portal is exposed to infrastructure administrators and end users to perform requests from the service catalog and manage their provisioned resources.

vCAC is built to work with existing infrastructures. It supports the different requirements of the many business units in an enterprise and integrates with a wide variety of existing IT systems and best practices.

User roles and responsibilities are defined and used in the structure of vCAC. The administration of users and compute resources in vCAC is managed through the vCAC console, which is the administrative portal.



The primary groups, users, and roles that this solution focuses on are:

- IaaS administrator
- Fabric group administrator
- Business group administrator
- Business group support
- Business group user

### **Infrastructure administrator**

The infrastructure administrator role is responsible for configuring resource endpoints and fabric groups, where fabric group administrators and their respective compute resources need to be defined.

A primary task of the cloud administrator is to configure the endpoints used by vCAC for provisioning compute resources and operations.

In this solution, two endpoints were required:

- vSphere (vCenter): Used by vCAC for compute resources
- vCenter Orchestrator: Used by vCAC for additional configuration

The compute resources available for each fabric group are assigned when the cloud administrator edits the fabric group.

### **Tenant administrator**

The tenant administrator role is responsible for configuring tenant-specific branding and user management. The tenant administrators create business groups and assign the business group manager, support, and user roles to Active Directory or OpenLDAP users and groups. Administrators are also responsible for catalog management, configuring catalog services, entitlements, approval policies, and shared blueprints within the context of their tenant. They also track resource usage by tenant users and initiate reclamation requests for decommissioning unused virtual machines.

### **Fabric group administrator**

Fabric groups can be used to segregate resources used by one organizational group from another. Limited to their respective fabric group, fabric administrators can manage cloud resources as defined by the IaaS administrator. Fabric group administrators are responsible for configuring resource reservations to be consumed by each business group. They also define network, storage, compute, and cost profiles. The fabric administrators can also define approval groups and policies.



**Business group**

Users in business groups are the consumers of the infrastructure provided to them by their fabric group administrator:

- **Business group manager role:** Can access all virtual machines, create and publish blueprints for end users, manage approval requests, and work on behalf of other users in their group
- **Business group support role:** Help desk users whose role enables them to work on behalf of other group users where required for troubleshooting and support
- **Business group user role:** End users, in the context of vCAC, who can deploy from the blueprints made available to them by the business group manager

Users assigned the user role are the primary consumers of the vCAC self-service portal. They can provision and manage their virtual machines. The deployment of machine blueprints may be subject to approval by the business group manager. The business group manager sets this approval policy per blueprint.

vCAC is configured to use Active Directory as an identity so the above roles can also be mapped to Active Directory groups corresponding to existing enterprise teams, as described in the *vCloud Automation Center Installation Guide*. Additional user groups can be created in Active Directory and assigned to support the various roles in vCAC.

**Entitlements**

Entitlements are a vCAC construct designed to provide user and group access controls to machine and service blueprints. Entitlements can also restrict access to specific machine actions enabling or restricting actions available to certain users. In addition, entitlements are the implementation point for approval policies. vCAC entitlements can be used to restrict certain users to a defined view of the service catalog, limiting access to the machine and service blueprints that users require to fulfill their function.

**Centralized log management**

Most hardware systems and applications support recording audit and operational events in a local log and, optionally, remote log servers. However, remote logging is not enabled by default. The lack of a centralized log collection and management system introduces a significant challenge for organizations, not just in troubleshooting operational issues, but also in detecting and investigating security incidents. In addition, it makes meeting regulatory and industry compliance requirements extremely difficult if not impossible.

Some of the challenges are:

- Many log sources
- Inconsistent log content
- Inconsistent timestamps
- Inconsistent log formats



**VMware vCenter Log Insight**

To address these challenges the EMC Enterprise Hybrid Cloud uses VMware vCenter Log Insight to deliver real-time log management and log analysis with machine learning-based Intelligent Grouping, high performance search, and better troubleshooting capabilities across the entire EMC Enterprise Hybrid Cloud solution.

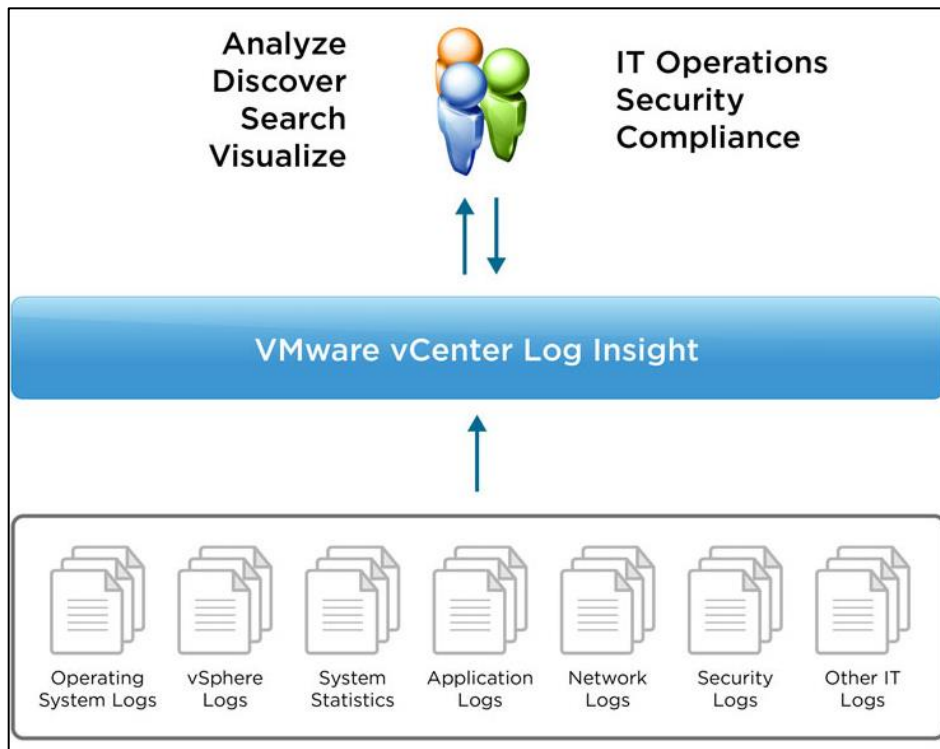
Some of the benefits of Log Insight as they relate to security are:

- Install Log Insight easily by deploying an Open Virtualization Format (OVF) package and providing network configuration details.
- Can be integrated with PKI and Active Directory to provide secure role-based access for security and operation administrators.
- Tightly integrated with vCenter Server and ESXi and comes with built-in knowledge and native support for vCenter Operations Manager.

The Log Insight administrative web UI is used to:

- Deploy and configure Windows agents
- Integrate with vCenter and vC Ops
- Configure ESXi hosts to forward logs

Other systems such as Linux servers, virtual appliances, arrays, switch gear, and data center systems that include syslog functionality can be easily configured to forward syslog events to Log Insight, as shown in Figure 102.



**Figure 102. Overview of vCenter Log Insight log collection types**



One of the biggest challenges to any organization deploying a log management system is getting all their different systems' events into the log server properly. vCenter Log Insight can plug in vendor-provided content packs and enable an organization to create its own content packs. Content packs already exist on the [vCenter Log Insight Solution Exchange](#) for many vendors such as EMC, HyTrust, Cisco, Puppet, and Microsoft.

Unlike many syslog implementations, Log Insight supports receiving syslog formatted events over UDP, TCP, and SSL protocols. In high volume environments, the inclusion of TCP support provides a significant performance improvement over a UDP-only based system, because more events can be channeled through fewer connections. This ensures that events are not lost as they could be with UDP based log servers. Additionally, support for receiving syslog events over SSL ensures that the event details are transmitted over the network in a confidential manner.

Log Insight consolidates and archives all log data in the EMC Enterprise Hybrid Cloud and creates a historical record that enables:

- Storage of events in sufficient detail and with accuracy
- Audit logs to be retained for a determined period of time consistent with enterprise security policy
- Identification of security incidents and policy violations as they occur
- Performance of auditing and forensic analysis
- Establishment of baselines that can be used to detect anomalous behavior

Authorized users can use Log Insight to perform ad-hoc searches across all event data, as illustrated in the failed login query shown in Figure 103. Commonly used queries can be saved and reused when needed.

vCenter Log Insight integration with vCenter Operations Manager enables you to build a security dashboard, correlating events across the EMC Enterprise Hybrid Cloud solution and beyond.



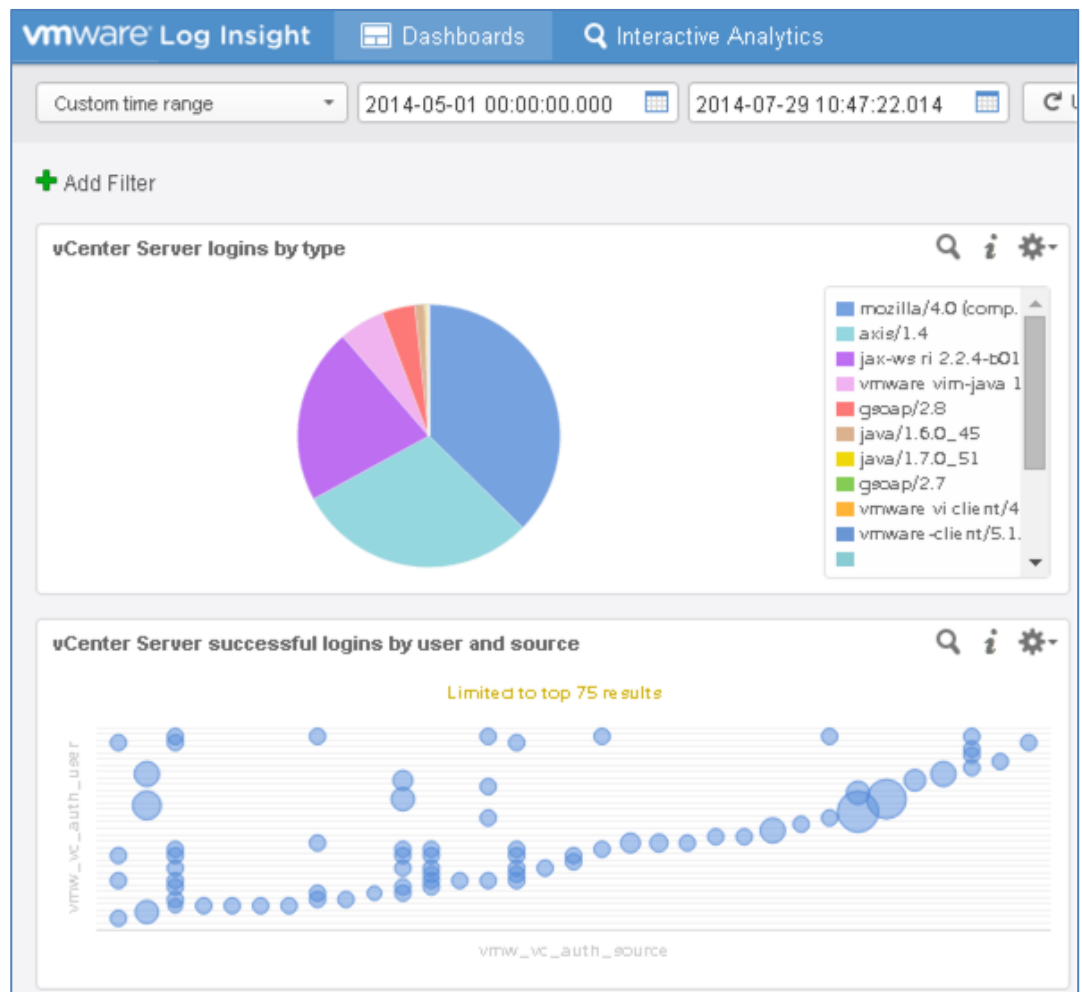


Figure 103. Example of a vCenter Log Insight dashboard showing logins



## Security configuration and management

In the EMC Enterprise Hybrid Cloud, we applied the recommendations contained in the *vSphere 5.5 Security Hardening Guide*, along with security configuration recommendations from other vendors. This raises the challenge of how to apply these hardening recommendations and operational configurations consistently across all affected components in the hypervisor and virtualization plane.

Configuration management is a vital element of implementing secure systems consistently and in accordance with your security policies. It comprises a collection of steps focused on establishing a configuration baseline to maintain the integrity of the EMC Enterprise Hybrid Cloud and the resources it supports.

Many organizations' IT and security groups face a significant challenge in gaining visibility into configuration management and compliance in their environments. To address this challenge, the EMC Enterprise Hybrid Cloud uses a number of native capabilities such as:

- **vCenter host profiles.** Ensure that a configuration set is applied consistently across all ESXi hosts. Host profiles also enable many vSphere Hardening Guidelines to be centrally applied. They provide a means to perform ad-hoc scans for validate host profile compliance and displays alerts within the vSphere Web Client.
- **vSphere Update Manager.** Enables patch management across virtual appliances and ESXi hosts. Provides a means to install and update third-party software on ESXi hosts. Organizations can establish a baseline and audit compliance.
- **vCenter Configuration Manager.** Extends the capabilities of vCenter host profiles and vSphere Update Manager to provide scheduled compliance scans and reports. In addition, it enables patch management configuration management of Windows and Linux guest operating systems and can audit the entire virtualized environment against many industry or regulatory frameworks and standards.

You should not underestimate the importance of the visibility, management, and compliance that these three components bring to the secure operation of the EMC Enterprise Hybrid Cloud solution.

### vCenter host profiles

vCenter host profiles ensure that a consistent configuration is applied across all vSphere ESXi hosts when the EMC Enterprise Hybrid Cloud is initially deployed and as new hosts are added to the environment. Specifically, host profiles:

- Ensure consistency for compliance
- Reduce the deployment time for new hosts
- Apply the same change to multiple hosts

Configuration settings that are shared by a group of vSphere ESXi hosts are stored in a host profile. When a host profile is created, it is attached to one or more vSphere



hosts or clusters. Once attached, the host configuration is compared against the host profile and any deviations are reported. Administrators associate host profiles with other hosts and clusters, ensuring consistency. Any drift in configurations can be corrected automatically.

New hosts that are added to vCenter Server can be configured by applying the host profile. Using this configuration management feature, administrators can create a profile once, and then use it for multiple vSphere hosts, providing fast setup. This automation feature eliminates the need to set up specialized scripts or manually configure hosts.

When firmware upgrades or other events happen that require storage, network, or security configuration changes on multiple hosts in a cluster, administrators can edit the host profile and apply it across the cluster for consistent configuration updates. In addition, the administrator can remove any settings that must be excluded from the host profile check.

### **vSphere Update Manager**

Organizations that are unable to patch systems effectively are susceptible to compromises that are easily preventable. It is important to carefully consider patch management in the context of security, because it is important in establishing and maintaining a solid security baseline. In addition, patch management is a core requirement of various security compliance standards such as Payment Card Industry Data Security Standard (PCI DSS). This standard requires that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

To address patch management in the EMC Enterprise Hybrid Cloud, VMware vSphere Update Manager (VUM) is used to keep vSphere hosts and virtual appliances up-to-date. VUM automates patch management and eliminates manual tracking and patching of vSphere hosts and virtual appliances. It compares the state of vSphere hosts with baselines, and then updates and patches to enforce compliance.

VUM includes these core features:

- A compliance dashboard to provide visibility into the patch and upgrade status of hosts and virtual appliances for compliance to static or dynamic baselines
- Stage and schedule patching for remote sites
- Deployment of patches that are downloaded directly from a vendor website, including drivers, Common Information Model (CIM), and other updates from hardware vendors for VMware vSphere hosts

Patching can lead to compatibility errors that require remediation. VUM can eliminate the most common patching problems before they occur, ensuring that the time you save in batch processing automation is not wasted later in performing rollbacks and dealing with one-offs. Benefits of VUM include:

- Store snapshots for a user-defined period, so that administrators can roll back the virtual machine if necessary





- Securely patch offline virtual machines without exposing them to the network, reducing the risk of non-compliant virtual machines
- Ensure the most current version of a patch is applied with automatic notification services

## vCenter Configuration Manager

The security status of each cloud system changes dynamically. These changes may be caused by a cloud administrator operation introducing risk into the environment, cloud components that are susceptible to a vulnerability or an external environment change such as a new attack method. Therefore, it is important to continuously monitor the security status of the EMC Enterprise Hybrid Cloud, mitigate the potential risk, and keep the system compliant to a security baseline.

In this solution, VMware vCenter Configuration Manager (VCM) is integrated with VMware vCenter Operations Manager (vC Ops) to build a configuration compliance audit and management system.

VCM provides a unified dashboard for managing configuration compliance. It integrates with vSphere to perform configuration data collection, which enables the vSphere infrastructure and its dependent components to be audited, flagging exceptions to policy, and performing remediation. Preset rules and templates are available that enable you to begin monitoring system compliance to regulatory (Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), industry (PCI DSS), and Microsoft standards.

Examples of elements that can be tracked for compliance are:

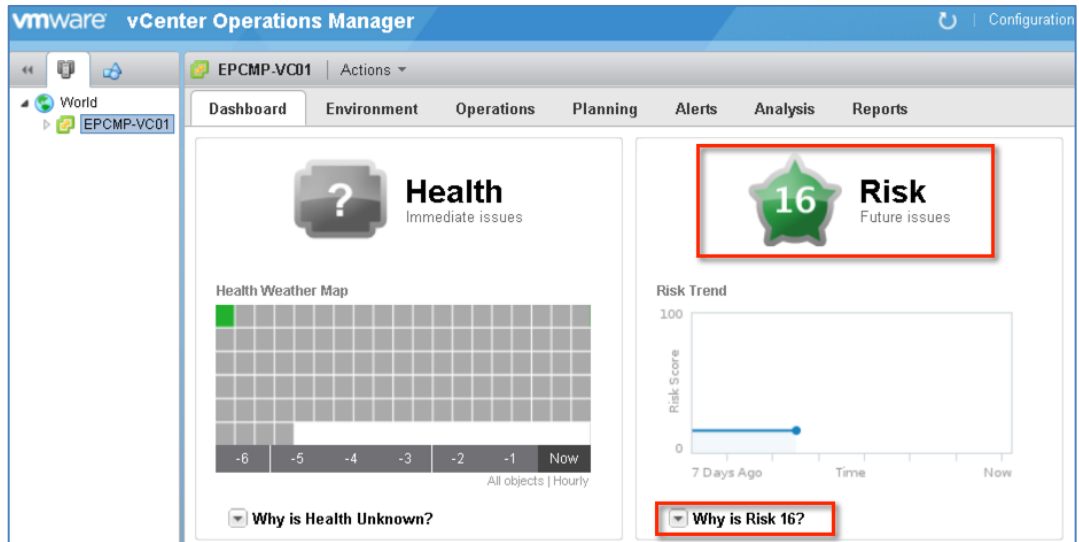
- Hypervisor configuration through vCenter host profiles
- Hypervisor and virtual appliance patch management through VUM baselines
- Linux and Windows guest OS configuration
- Regulatory and industry standards through default compliance toolkits

Configuration compliance can be maintained against internal standards, security best practices, vendor hardening guidelines, and regulatory mandates such as:

- Security best practices developed by the Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS), and many more
- Hardening guidelines from VMware and Microsoft
- Regulatory mandates such as SOX, the PCI standard, HIPAA, and FISMA

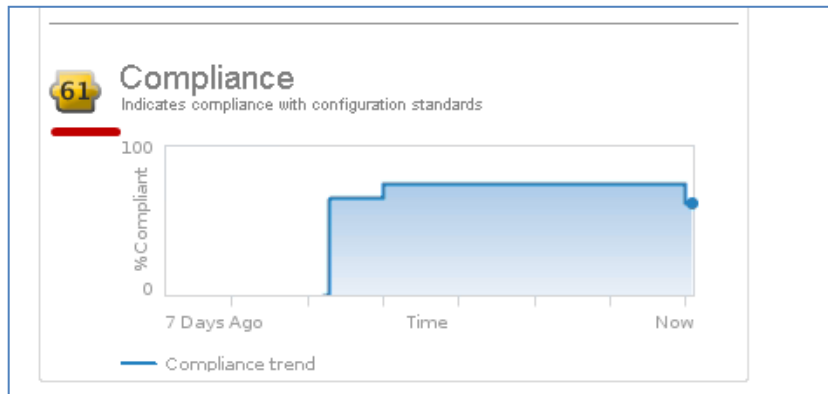
You can also use VCM to build your own IT standard to enforce best practices in your environment. The integration between vCenter Operations Manager and VCM includes using the VCM compliance template results to contribute to the Risk badge score in vCenter Operations Manager, as shown in Figure 104.





**Figure 104. vC Ops dashboard displaying Risk badge score**

The compliance templates are included in badge mappings that are run in VCM against objects in vCenter Server instances that are managed by both VCM and vCenter Operations Manager. These objects include virtual machines, host systems, clusters, vCenter Server instances, and datastores. The compliance mapping results determine the compliance score. Expanding the risk status table in Figure 104 shows the compliance status summary, as shown in Figure 105.



**Figure 105. vC Ops dashboard displaying compliance status summary**

vCenter Operations Manager pulls the scores into the formulas used to calculate the Risk badge scores. When you review the standards compliance in vCenter Operations Manager, you can navigate back to VCM to view the detailed results and identify any configuration changes that you must make to bring an object that is noncompliant back to compliance.



## Multitenancy

Consumers of provisioned resources need to operate in a dedicated environment and benefit from infrastructure standardization, without having concerns about information leakage and unauthorized access on a shared network infrastructure.

To address these concerns, the EMC Enterprise Hybrid Cloud solution was designed with multitenancy in mind, through a defense-in-depth perspective, which is demonstrated through:

- Implementation of VLANs to enable isolation at Layer 2 in the cloud management pod and where the solution intersects with the physical network
- Use of VXLAN overlay networks to segment tenant and business group traffic flows
- Integration with firewalls functioning at the hypervisor level to protect virtualized applications and enable security policy enforcement in a consistent fashion throughout the solution
- Deployment of tenant Edge firewalls to protect tenant resources at the tenant perimeter

The vCNS and NSX for vSphere deployment options not only add network virtualization capabilities through the implementation of VXLAN, but also add rich security feature sets. Both solutions offer a single interface for managing the virtual network and protecting business group assets.

The solution was validated using hybrid cloud environments that implement network and security virtualization using vCNS and NSX for vSphere in each environment.

---

**Note:** The architecture can be supplemented at the physical switch layer with private VLANs (PVLANS) and VRF tables to provide segmentation at Layers 2 and 3, although doing so is outside the scope of this chapter.

---

### Network security

The logical topology is designed to address the requirements of enabling multitenancy and securing separation of the tenant resources. The topology is also designed to align with the VMware security best practice of segmenting networks according to the purpose or traffic type. For example, configuring an isolated network segment for vMotion traffic between VMware vSphere ESXi hosts helps prevent attacks where the unencrypted data transfer can be intercepted by an attacker and reconstructed to gain access to sensitive data.

In validation testing, we configured trunks on the physical network infrastructure to enable only the VLANs and PVLANS required for operations within the hybrid cloud environment. As well as being a security best practice, this helps to conserve valuable resources such as Spanning Tree Protocol (STP) logical interfaces. Each switch supports a limited number of STP logical interfaces, which can be used up before the VLAN limit is reached, especially in a multitenant environment. Therefore, pruning and carrying only the necessary VLANs can be of critical importance.



Figure 106 shows the logical topology of the physical and virtual networks defined in the EMC Enterprise Hybrid Cloud solution. VLANs provide segmentation of the networks at Layer 2 in the cloud management pods, as that environment is likely to be static and an extension of existing management networks.

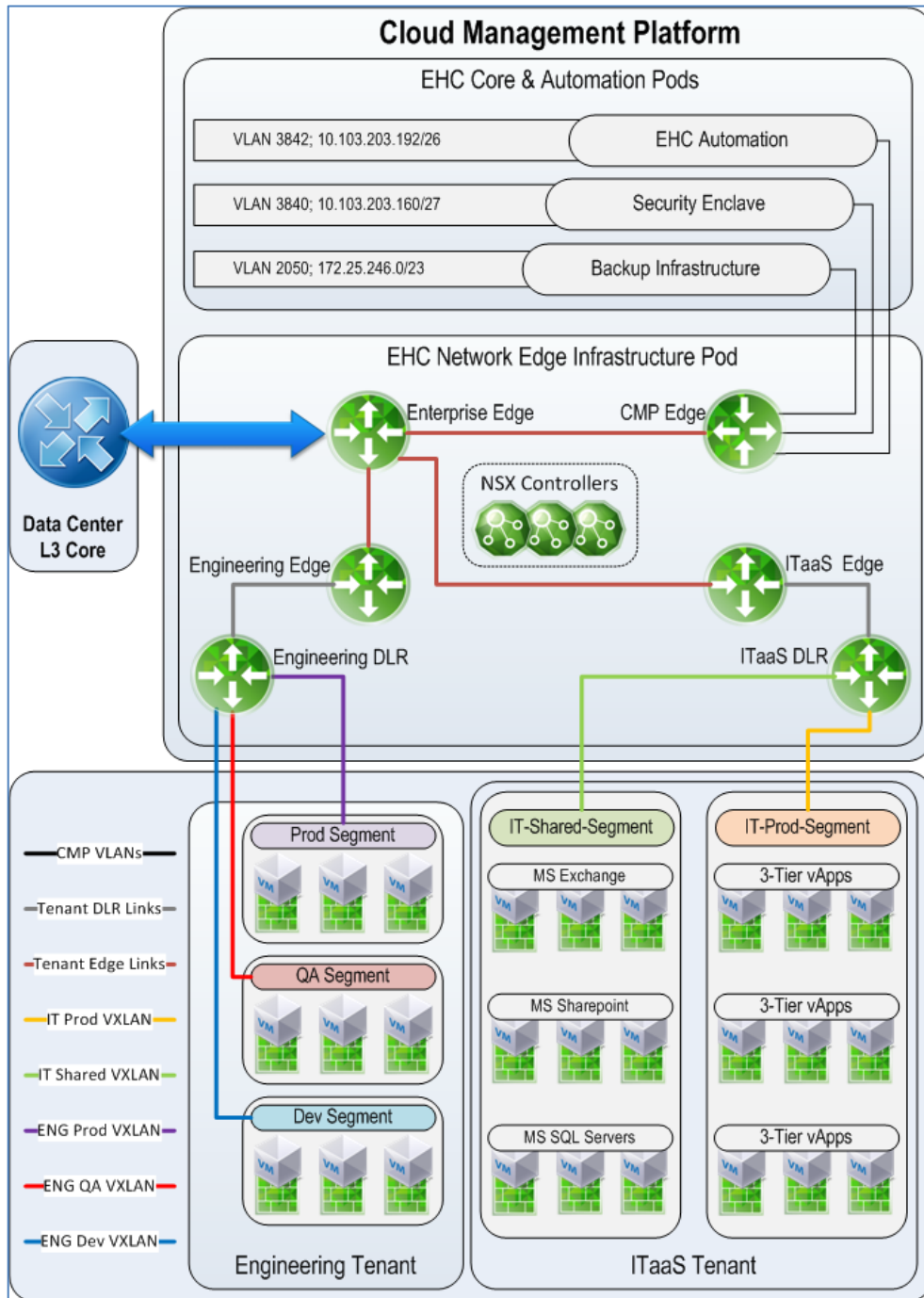


Figure 106. EMC Enterprise Hybrid Cloud network architecture



### Tenant and enterprise Edge routers

To enable connectivity between the physical network core and the tenant resources, we deployed an enterprise NSX Edge router and a tenant NSX Edge router in HA mode for each tenant.

An Edge appliance was configured as an enterprise router to act as a perimeter gateway for the EMC Enterprise Hybrid Cloud tenants, on which we could apply a perimeter security policy. This allowed security policies for the entire EMC Enterprise Hybrid Cloud environment to be managed from a single interface.

---

**Note:** An existing Layer 3 core could provide the function of the enterprise Edge router used in our example. The use of an NSX Edge appliance for this function is not prescriptive.

---

## Security virtualization

Two options are currently available for security virtualization in the EMC Enterprise Hybrid Cloud; vCloud Networking and Security, and the premium deployment option, NSX for vSphere. In this section, we focus on their security features.

### vCloud Networking and Security

vCNS Manager is a single management and control appliance for vCNS operations and provides the interface to manage network virtualization in the solution. This enables the cloud administrator to prepare the vSphere ESXi hosts, configure VXLAN, and create VXLAN networks.

---

**Note:** The term “prepare” in this context is used to mean the installation of the necessary kernel modules on each ESXi host to enable VXLAN. While initiated by the administrator, the installation is executed directly by vCNS Manager.

---

In addition, vCNS Manager is the point from which vCNS App and vCNS Edge appliances are deployed and security policies managed. Integration with vCAC is achieved through the vCAC endpoint where the vCNS Manager URL and enterprise administrator credentials are specified when configuring the endpoint for vCenter. This enables vCAC to make calls to vCNS Manager to retrieve inventory, create VXLAN networks, and provision vCNS Edge routers.

vCNS Manager enables the use of security groups to provide logical containers that can be populated with related objects to streamline security policies. As an example, if you create a security group for web servers you can then apply a security policy to that security group to permit access over port 80 and block all other access. Security policies can be configured on vCNS Edge appliances to protect perimeters and vCNS App Firewall at the datacenter and cluster levels in the vCenter hierarchy, enabling consistent protection to be applied across the data center.



### **vCNS App Firewall**

vCNS App Firewall provides virtual networking security for virtual machines through segmentation and zoning down to the vNIC level. vCNS App Firewall is a hypervisor-based application firewall that:

- Interrogates all the traffic flows between the virtual machines on a vSphere ESXi host
- Provides detailed visibility into network flows and communications
- Enforces granular policies with security at the virtual network interface card (vNIC) level by using a loadable kernel module to inspect and monitor traffic and enforce the security policy

Adaptive trust zones with Layer 2 firewalling protect against password sniffing, DHCP snooping, or poisoning attacks, and Address Resolution Protocol (ARP) spoofing. Application-aware firewalling improves security by opening session (ports) only when needed for common applications, such as Oracle Database, Microsoft Exchange, and Microsoft RPC.

Implementing vCNS App Firewall provides further granularity by enabling policies to be applied to individual virtual machines, vApps, or logical groups of resources called security groups. Security groups enable enterprise administrators to logically group various resources such as IP addresses, MAC addresses, resource pools, virtual machines, and vNICs in their datacenter when creating firewall rules, thus simplifying administration and reducing complexity. The architecture enables a single management point for networking and security to protect a relatively large number of resources. This advances the flexibility of security beyond the traditional, physical gateway model to a model that protects from the perimeter down to the vNIC level.

vCNS App Firewall is an important tool for implementing security policies to protect virtualized applications across the data center and monitoring inter-virtual machine traffic to demonstrate compliance when customers are trying to meet regulatory requirements. All virtual machine traffic flows can be easily monitored, rules can be defined and enforced regardless of virtual machine location, and rules can be set to log to a centralized log repository.

### **vCNS Edge appliance**

The vCNS Edge appliances provide a rich set of integrated gateway services for protecting virtual data centers and optimizing resource utilization. This virtual appliance includes services such as stateful firewall, network address translation (NAT), load balancing, DHCP, and VPN. Edge high availability protects against network, host, and software failures to deliver reliable network communications and connectivity within each business group's networks. In addition, vCNS Edge acts as a fully fledged Layer 3/Layer 4 stateful firewall, enabling security at the business group edge and between internal networks.

### **NSX for vSphere**

VMware NSX is the next generation of network virtualization and offers additional functionality and improved performance over vCNS. This additional functionality includes distributed logical routing and SSL off-loading, distributed virtual



firewalling, logical load balancing, and support for routing protocols such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Open Shortest Path First (OSPF).

NSX also provides substantial performance improvements in throughput, with logical routing and firewalling providing line-rate performance distributed across many hosts instead of being limited to a single virtual machine or physical host. VMware NSX extensibility provides VMware- and partner-integrated services to help customers optimize the deployment of their virtual networks. The NSX platform uses a distributed service framework that allows service composition at multiple points in the network and enables easy insertion of partner services through the NSX API. This provides a framework for third-party security integrations such as intrusion detection, intrusion prevention, anti-virus, and vulnerability management. These integrations enable further workload behavioral analysis and workflows to protect the environment.

### **NSX distributed firewall**

Another key feature is the NSX distributed firewall, which is implemented in the hypervisor kernel and eliminates the need to route traffic through vCNS Edge or physical firewalls for inspection. Traffic is analyzed by the hypervisor when it leaves the source virtual machine vNIC and before it enters the vNIC of the destination virtual machine. Because the NSX is integrated with vCenter Server, it can use the vCenter inventory and filter on more than just source and destination IP addresses or ports.

Rules can be applied to virtual machines, security groups, clusters, and data centers. Security groups can also have dynamic membership, which can apply rules based on virtual machine attributes such as guest OS, virtual machine name, or security tags, enabling rapid deployment of new virtual machines or additional capacity to existing applications that automatically inherit all applicable security rules. Because this inspection is performed at the hypervisor level, traffic does not have to be steered through and analyzed by another device or virtual machine on the network.

Flow monitoring can also be used to see historical and real-time traffic flows. These flows can be shown in aggregate, by service, or by virtual machine. The data can be used for troubleshooting performance issues, firewall misconfigurations, or rogue traffic on the network.

### **NSX Edge**

It is important to highlight differences between the NSX Edge that is deployed by vCAC as part of a blueprint and what can be deployed directly from the Networking & Security web client.

Through the Networking & Security web client, an NSX Edge is deployed as either an Edge gateway or a distributed logical router (DLR). This appears in the Networking & Security web client as an NSX Edge 6.0. However, when vCAC provisions an on-demand Edge, a vCNS 5.5 Edge, which does not have as rich a feature set as the NSX Edge 6.0, is deployed. This vCNS Edge appears in the Networking & Security web client as an NSX Edge 5.5.



A comparison of the Edge features when deployed by vCAC based on the blueprint deployment model is shown in Table 3.

**Table 3. Comparison of the NSX Edge features supported by vCAC**

Feature	Pre-created	On demand
Logical switch	Y	Y
Provider Edge (distributed logical router)	Y	N
NSX Edge 6.0	Y	N
NSX Edge 5.5	Y	Y
Edge load balancer	Y	Y
Edge load balancer SSL termination	Y	N
Edge load balancer application rules	Y	N
Firewall Edge gateway	Y	Y
Logical DHCP	Y	Y

## Summary

The infrastructure solutions stack required to deliver EMC Enterprise Hybrid Cloud services must provide a trusted means of centralized management, bringing together the software and hardware components that form the complete solution so that they can be securely managed and enforced.

This chapter demonstrated that an EMC Enterprise Hybrid Cloud solution stack can be integrated with an enterprise PKI to ensure authenticity, strengthen authentication, and encrypt administrative communications. In addition, this shows how integration with a common directory can be achieved to support LDAPS, Kerberos, and TACACS+ authentication services, streamline administration and policy enforcement, and provide tighter control. In addition, we showed that the native capabilities of the solution can be used to provide centralized log management and analytics, patch management, configuration management, and security compliance enabling considerable visibility into the operation and security posture of the cloud environment.





# Chapter 7 Conclusion

This chapter presents the following topic:

**Conclusion .....130**



## Conclusion

The EMC Enterprise Hybrid Cloud empowers IT to be a broker of cloud services, providing the control and visibility that IT organizations need, and the on-demand self-service that developers and application users expect.

Users can easily provision standardized services directly from an application marketplace portal, with upfront pricing. Delivery of these resources from private and public clouds, whatever the workload calls for, is built on policies set by IT. This ensures application workloads are placed in the right cloud, with the right cost, security, and performance.

The EMC Enterprise Hybrid Cloud is also the bridge between today's applications (Platform 2) and the social, mobile, analytics and cloud applications of the future (Platform 3).



EMC<sup>2</sup>

Pivotal™

RSA

vmware®

# Chapter 8 References

This chapter presents the following topic:

**EMC documentation .....132**  
**Other documentation .....132**



## EMC documentation

The following documents, available on EMC Online Support or EMC.com, provide additional and relevant information. If you do not have access to a document, contact your EMC representative.

- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Foundation Infrastructure Reference Architecture*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Backup Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Continuous Availability Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center: Data Protection Disaster Recovery Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Hadoop Applications Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Pivotal CF Platform as a Service Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Security Management Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5, Federation Software-Defined Data Center: Public Cloud Integration Guide*
- *Using the EMC VMAX Content Pack for VMware vCenter Log Insight White Paper*
- *EMC Integration of PKI and Authentication Services for Securing VMware vCloud Suite 5.1 Environments Proven Solution Guide*
- *EMC Avamar—Technical Deployment Considerations for Service Providers*

## Other documentation

For additional information, see the following document, available on the [VMware documentation](#) website:

- *vCloud Automation Center Installation Guide*

