Technical Report

VMware Cloud Infrastructure and Management on NetApp

Jack McLeod and Matt Robinson, NetApp and Wen Yu, VMware

Version 1.0
August 2011 | TR-3948

ABSTRACT

Storage infrastructure is a key element of the infrastructure layer. Storage efficiency, unified architecture, high availability, multiprotocol capability, ease of management, integration with VMware® vSphere™ and VMware vCloud™ Director (vCD), and enterprise backup and disaster recovery ability are all earmarks of cloud-enabled storage. NetApp® unified storage extends all the efficiencies and flexibility already available for VMware vSphere virtualized environments to VMware vCD, enabling companies to more efficiently realize the full benefits of cloud computing. This report covers the best practices and detailed procedures for designing storage for the VMware vCloud infrastructure.
TABLE OF CONTENTS

1 EXECUTIVE SUMMARY ............................................................................................................. 6
  1.1 IMPLEMENTING BEST PRACTICES ................................................................................... 6
  1.2 AUDIENCE ....................................................................................................................... 7
  1.3 SCOPE ............................................................................................................................... 7

2 KEY TERMINOLOGIES AND COMPONENTS ........................................................................... 7

3 VMWARE VCLOUD DIRECTOR BEST PRACTICES ................................................................. 9
  3.1 VMWARE VSPHERE BEST PRACTICES ............................................................................. 9
  3.2 VCLOUD NETWORK DESIGN BEST PRACTICES .......................................................... 10
  3.3 MANAGEABILITY AND CHARGEBACK ........................................................................... 10

4 NETAPP SOLUTIONS AND COMPONENTS ........................................................................... 11
  4.1 HIGH-LEVEL ARCHITECTURE ......................................................................................... 11
  4.2 NETAPP STORAGE SYSTEM BEST PRACTICES ........................................................... 12
  4.3 NETWORK ARCHITECTURE ............................................................................................ 15
  4.4 UNIFIED ARCHITECTURE ............................................................................................... 15
  4.5 STORAGE EFFICIENCY .................................................................................................... 16
  4.6 RAPID PROVISIONING ................................................................................................... 18
  4.7 PERFORMANCE ............................................................................................................... 18
  4.8 NETAPP VSPHERE INTEGRATION .................................................................................. 19
  4.9 VIRTUAL STORAGE CONSOLE ....................................................................................... 21
  4.10 NETAPP VCLOUD INFRASTRUCTURE INTEGRATION ............................................... 21

5 SOLUTION IMPLEMENTATION PROCEDURES .................................................................... 24
  5.1 PURPOSE ......................................................................................................................... 24
  5.2 THE DEPLOYMENT SCENARIO ....................................................................................... 25
  5.3 THE ENVIRONMENT ....................................................................................................... 25
  5.4 SOFTWARE NEEDED FOR DEPLOYMENT ..................................................................... 25

6 NETWORK SETUP .................................................................................................................. 25
  6.1 NETWORK SETUP OF CISCO NEXUS NETWORK SERIES ............................................. 26

7 INSTALL AND CONFIGURE VSPHERE AND VCLOUD DIRECTOR ...................................... 27
  7.1 INSTALL VSPHERE .......................................................................................................... 27
  7.2 INSTALL VMWARE VCENTER SERVER ......................................................................... 27
  7.3 CONFIGURE SERVICE CONSOLE FOR REDUNDANCY ............................................... 27
  7.4 CONFIGURE VMWARE KERNEL NFS PORT ................................................................. 30
  7.5 CONFIGURE VMOTION .................................................................................................. 31
  7.6 CONFIGURE VMWARE VSPHERE HOST NETWORK ..................................................... 32
  7.7 TRANSITION NETWORK TO DISTRIBUTED SWITCHING ............................................. 32
LIST OF TABLES
Table 1) Deployment mix for each organization ................................................................. 25
Table 2) Configure the service console for redundancy........................................................ 27
Table 3) Configure VMware kernel NFS port ........................................................................ 31
Table 4) Configure vMotion .................................................................................................. 31
Table 5) Transition network to distributed switching .............................................................. 32
Table 6) Set up network for both storage controllers .............................................................. 40
Table 7) Configure NFS trunk ............................................................................................... 41
Table 8) Configure storage controller SSH configuration ..................................................... 45
Table 9) Configure FlexScale for Flash Cache ..................................................................... 45
Table 10) Configure vCloud Director datastore aggregate .................................................. 46
Table 11) Modify the aggregate Snapshot reserve for the VMware vCloud aggregate .......... 47
Table 12) Configure VSC 2.1 ................................................................................................. 48
Table 13) Create initial vCloud volume for operating system templates ............................... 51
Table 14) Host volumes in template virtual machine ............................................................ 54
Table 15) Create volume to host virtual machine swap files ............................................... 57
Table 16) Configure volume ................................................................................................. 58
Table 17) Configure location of virtual swap file datastore .................................................. 58
Table 18) Configure optimal performance for VMDKs on NFS .............................................. 61
Table 19) Set up resource pools .......................................................................................... 61
Table 20) Set up provisioning policies .................................................................................. 64
Table 21) Set up dataset provisioning .................................................................................... 70
Table 22) Install and configure VMware vCenter Orchestrator ............................................ 76
Table 23) Set up provider VDC ............................................................................................ 79
Table 24) Add storage containing template VMs for provider vDC ......................................... 84
Table 25) Set up gold organization ....................................................................................... 85
Table 26) Add additional storage to provider VDC .............................................................. 90
Table 27) Install Snap Creator ............................................................................................. 94
Table 28) Configure Snap Creator ....................................................................................... 99
Table 29) Backup execution ................................................................................................ 110
Table 30) Validate solution. ........................................................................................................ 111
Table 31) Revision history. ........................................................................................................ 112

LIST OF FIGURES
Figure 1) vCD self-service network architecture (graphic provided by VMware). ......................... 10
Figure 2) High-level architecture: vCloud Director on NetApp integration...................................... 12
Figure 3) Traditional provisioning and thin provisioning. .............................................................. 16
Figure 4) Thin provisioning allocation (graphic obtained from Oliver Wyman study). ................... 17
Figure 5) NetApp deduplication. .................................................................................................. 17
Figure 6) Operations Manager .................................................................................................... 22
Figure 7) SANscreen VM Insight. ................................................................................................ 23
Figure 8) VMware vSphere host configuration example. .............................................................. 32
Figure 9) NetApp storage controller disk configuration. ............................................................... 45
1 EXECUTIVE SUMMARY

Cloud computing improves efficiency by enabling pooling and on-demand consumption of IT resources so that businesses can meet their needs in a more agile and cost-effective manner. Cloud computing provides a set of virtualized services from which the users can consume compute, storage, and network resources only when needed, often paying only upon usage, and often allowing the consumer to deploy their environments at their leisure. Cloud computing can exist as an internal cloud, meaning it is built inside an enterprise firewall, or as an external cloud, meaning it is hosted externally by a service provider who specializes in providing cloud services.

VMware provides a full suite of products and solutions for service providers and enterprises to build cloud services. These products include VMware vCloud Director (vCD), vCloud Service Manager, vCenter™ Chargeback, vShield™ Edge, vCenter Orchestrator, and vSphere. A service provider or enterprise customer who is building a vCloud infrastructure as a service (IaaS) today would use all of these products.

Building an IaaS offering based on vCloud requires the following considerations:

- Efficiency and high performance
- High availability
- Service automation and analytics
- Agility
- Nonstop operations

The storage infrastructure is a key element at the infrastructure layer. The earmarks of cloud-enabled storage are:

- Storage efficiency
- Unified architecture
- High availability
- Multiprotocol capability
- Ease of management
- Integration with vSphere and vCD
- Enterprise backup
- Disaster recovery

NetApp unified storage extends all the efficiencies and flexibility already available for VMware vSphere virtualized environments to VMware vCD, enabling companies to more efficiently realize the full benefits of cloud computing. This report describes the best practices for designing NetApp storage for the vCloud infrastructure and provides step-by-step examples.

1.1 IMPLEMENTING BEST PRACTICES

The recommendations and practices presented in this document should be considered as deployment requirements unless otherwise stated. NetApp and VMware provide support even if these best practices are not all implemented. However, disregarding any of these practices commonly results in the need to implement them at a later date, in a much larger environment, and often with the requirement of application downtime. For these reasons, NetApp recommends implementing all of the best practices as defined within this document as a part of the initial deployment or migration.

All recommendations in this document apply specifically to deploying vSphere on NetApp.

Note: Data ONTAP® Version 7.3.1P2 or greater is required to implement the NetApp vSphere plug-ins.
NetApp and our partners offer professional services to architect and deploy the designs contained within this document. These services help our customers achieve an optimal virtual storage architecture for their virtual data centers.

1.2 AUDIENCE

The target audience for this paper is familiar with concepts pertaining to VMware vSphere, including VMware ESX® 5, VMware vCenter Server 5, VMware vCloud Director 1.5, VMware vShield, vCloud Service Manager, VMware Chargeback, and NetApp Data ONTAP 7.3.1.P2 or greater.

1.3 SCOPE

The solution described in this document is applicable to either a service provider building an external cloud or an enterprise building an internal cloud solution with VMware vCloud Director and NetApp unified storage. This report details the best practices and implementation related to creating a cloud environment using VMware vCloud Director working in conjunction with NetApp cloud-enabled storage to create an ITaaS environment quickly and efficiently.

This report also focuses on the solution design best practices and provides step-by-step instructions for the underlying infrastructure layer.

- Refer to sections 2-4 for a discussion of the overview and best practices.
- Refer to sections 5-16 for implementation guidelines.

The software as a service (SaaS), automation and extension, service portal, and compliance areas are not in the scope of this document.

2 KEY TERMINOLOGIES AND COMPONENTS

This section describes the VMware vCloud Director terminology used throughout this document. For more information, refer to the VMware vCloud Director documentation on www.vmware.com/products/vcloud-director.

INFRASTRUCTURE AND OPERATIONS

This report references the following VMware infrastructure and operations components:

- **vSphere.** vSphere resources include the vCenter Servers, ESX hosts, resource pools, datastores, vNetwork Distributed Switches, and port groups that are used to provision cloud resources in VMware vCloud Director.

- **Chargeback.** VMware vCenter Chargeback allows cost models to be customized to the process and policies of different organizations. [VMware vCenter Server](http://www.vmware.com/products/vcenter-server) collects virtual machine resource consumption data to provide the most complete and accurate tabulation of resource costs. Integration with VMware vCloud Director and vShield also enables automated chargeback for private and public cloud environments.

- **vShield.** VMware vShield Edge provides perimeter security enforcement and isolation for each tenant in the vCloud environment. vShield Manager provides the single-pane-of-glass firewall rules for configuration and enforcement. The latest version of vShield Manager 5.0 is fully integrated with Cisco Nexus® 1000v for network service orchestration.

- **vCenter Orchestrator (vCO).** VMware vCenter Orchestrator provides out-of-the-box workflows that can help administrators automate existing manual tasks. Administrators can use sample workflows from VMware vCenter Orchestrator's workflow library to provide a blueprint for creating additional workflows. NetApp fully integrates with vCO to provide a storage provisioning plug-in, based on Operations Manager.
• Hyperic. VMware Hyperic® provides performance monitoring capability to the virtualized infrastructure. Hyperic monitors infrastructure resource utilization to verify that infrastructure resource capacity is in compliance with the enterprise and service provider’s predefined threshold.

• Update Manager. VMware Update Manager, an integrated vSphere host patching solution, upgrades, patches, and installs third-party components on ESXi™ server hosts.

CLOUD RESOURCES
This report uses the following VMware vCloud Director terms:

• Cloud cells. Cloud cells are the Red Hat Enterprise Linux® 5 (RHEL5) servers that run the VMware vCloud Director software. Multiple cloud cells form the VMware vCloud Director cluster.

• Provider vDC. A provider vDC is a group of compute, memory, and storage resources from one vCenter. You can allocate portions of a provider vDC to your organizations using VMware vCloud Director.

• External network. An external network uses a network in vSphere to connect to a network outside your cloud. The network can be a public network such as the Internet or an external VPN network that connects to a given organization.

• Organization. An organization is the fundamental grouping in VMware vCloud Director. An organization contains users, the vApps they create, and the resources the vApps use. An organization can be a department in your own company or an external customer to whom you are providing cloud resources.

• Organization vDC. An organization vDC provides an organization with the compute, memory, storage, and network resources required to create vApps.

• Network pool. A network pool is a collection of VM networks that are available to be consumed by vDCs to create vApp networks and by organizations to create organization networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

• vApp. A vApp is a virtual application that contains one or more VMs.

• Catalog. A catalog is a virtual repository that allows you to share vApp templates and media images with other users in your organization or with other organizations in VMware vCloud Director.

STORAGE RESOURCES
This report uses the following NetApp storage terms:

• NetApp FlexClone®. A NetApp storage technology that instantly replicates data volumes and datasets as transparent, virtual copies without requiring additional storage space or compromising performance.

• NetApp FlexShare®. A Data ONTAP software feature that provides workload prioritization for a storage system. It prioritizes processing resources for key services when the system is under heavy load.

• NetApp Snapshot™ technology. A NetApp point-in-time copy technology that enables data protection with no performance impact and minimal consumption of storage space.

• NetApp SnapProtect™. This software combines high-speed Snapshot copies and replication with tape to significantly reduce risk of downtime and data loss.

• NetApp SnapMirror®. A NetApp data replication solution that provides disaster-recovery protection of business-critical data and enables a DR site for other business activities.

• NetApp SnapVault®. A NetApp disk-to-disk backup solution that fully integrates with Data ONTAP, Snapshot technology, and FAS deduplication to provide point-in-time backup copies in native format.

• VIF. A virtual network interface (VIF) or EtherChannel is a mechanism that supports aggregation of network interfaces into one logical interface unit. Once created, a VIF is indistinguishable from a physical network interface. VIFs are used to provide fault tolerance of the network connection and in some cases higher throughput to the storage device.
- **Virtual Storage Console (VSC).** This plug-in to VMware vCenter is available for all vSphere clients that connect to that vCenter, and it provides storage configuration and monitoring using VSC 2.1 capability, datastore provisioning, virtual machine cloning using the provisioning and cloning capability, and backup and recovery of virtual machines and datastores using the backup and recovery capability.

3 **VMWARE VCLOUD DIRECTOR BEST PRACTICES**

Storage infrastructure is a key element of the infrastructure layer. Storage efficiency, unified architecture, high availability, multiprotocol capability, ease of management, integration with VMware vSphere and vCD, and enterprise backup and disaster recovery ability are all earmarks of cloud-enabled storage. NetApp unified storage extends all the efficiencies and flexibility already available for VMware vSphere virtualized environments to VMware vCD, enabling companies to more efficiently realize the full benefits of cloud computing. The following sections cover the best practices for designing storage for the vCloud infrastructure.

3.1 **VMWARE VSPHERE BEST PRACTICES**

vCloud Director builds on top of the vSphere platform to create a new resource abstraction layer for enablement of secure multi-tenancy and to define the SLA-based policy needed for cloud mobility. Therefore, the vSphere platform layer must be highly available and highly scalable, with a clear separation of management and raw tenant resources.

**SEPARATION OF RESOURCES**

Two ESX Server clusters should be created: one dedicated as a management cluster and the other dedicated as a resource group. The management cluster hosts all the infrastructure and management virtual machines, such as vCenter Server and its database, vCD cell and its database, vCenter Chargeback and its database, vShield Manager, or any other VMs serving the ITSM functions. The resource group cluster provides raw compute resources for end tenants, either individual business units, teams, departments within a private cloud of an enterprise, or individual tenants of a vCloud service provider cloud. This level of physical separation provides independent scalability for each cluster, minimizing the impact of tenant operations. When unexpected failures occur, this design also helps with problem isolation and troubleshooting.

**HIGH AVAILABILITY**

Follow these best practices to achieve high availability:

- **Enable VMware HA for both the management cluster and resource group cluster.**
- **Set the admission control to Enable to provide sufficient virtual machine resource reservations.**
- **Use the Percentage of cluster resources reserved as failover spare capacity admission control policy for the management cluster because the infrastructure VMs might have vastly different levels of resource reservations set. Initially, a cloud administrator can set the failover capacity at 25%. As the environment reaches steady state (that is, all the required infrastructure VMs are put in place and running with the correct reservation values), the percentage of resource reservation can be modified to a value that is greater than or equal to the average resource reservation size or amount per ESX host.**
- **Consider using the Number of Host Failure admission control policy for the resource group cluster because cloud workloads are bursty in nature. A minimum of one host failure must be specified for this admission control policy.**

vSphere5 HA has an enhanced fault domain manager (FDM) architecture:
The primary and secondary node architecture has been decommissioned and replaced by the enhanced master/slave implementation. Staggering the addition of the first five ESX hosts to the cluster when the vCloud implementation spans more than one blade server chassis is no longer required.

FDM in vSphere5 has a secondary heartbeat monitoring mechanism. A shared datastore can be used to monitor the heartbeat of ESX Server nodes in the event of management network failure. For both management and resource group clusters, more than two datastores must be presented to each cluster before enabling HA so that the HA automatically chooses the two datastores to serve as the secondary heartbeat monitoring storage. If needed, the default can be changed.

3.2 VCLOUD NETWORK DESIGN BEST PRACTICES

vCloud Director provides a new layer of abstraction for network resources. VM port groups service different roles in this layer. VMware highly recommends that customers use the VMware vNetwork Distributed Switch, or the Cisco Nexus 1000v, in vCD deployments. For a given network pool in vCloud Director, the built-in integration of the VMware vDS and Cisco Nexus 1000v allows for the creation of VM port groups dynamically, thereby eliminating mistakes and inconsistencies from normal virtual switch provisioning. Figure 1 shows how service providers and enterprise customers implement a vCD self-service network architecture.

Figure 1) vCD self-service network architecture (graphic provided by VMware).

3.3 MANAGEABILITY AND CHARGEBACK

Manage user behavior by providing transparency into actual resource usage and by quantifying the metrics in financial terms. Metering involves measuring and reporting the consumption units appropriate
to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, reported, and accounted for appropriately, providing transparency for both the provider and the consumer of the utilized service. VMware handles these tasks through the use of several technologies, including VMware vCloud Director and vCenter Chargeback.

VMware vCenter Chargeback provides the capability to account, monitor, and report the costs associated with the virtual infrastructure. The key benefits are:

- **Improved resource utilization.** Associating costs to VMs eliminates many of the "unused" VMs, which frees resources for higher priorities.
- **Optimized budgets.** Business units can determine how much they are paying for resources and can monitor resource utilization, including unused resources, allowing them to optimize resource consumption and costs.

The key features are:

- Fixed, allocation, and utilization-based costing
- Ability to charge different amounts for tiers of infrastructure
- Ability to schedule reports and e-mail results

For more information, refer to the documentation on [www.vmware.com](http://www.vmware.com).

4 NETAPP SOLUTIONS AND COMPONENTS

4.1 HIGH-LEVEL ARCHITECTURE

NetApp storage enables backup and recovery, storage analytics, storage orchestration, storage services management, and storage policy management inside of vCloud Director. With this tight-knit integration with vCloud Director, a storage as a service (StaaS) offering can be created that integrates into the VMware IT as a service (ITaaS) model. At each level of integration, manageability and control are further gained over the environment, complexity is reduced, and time and effort are saved. These efficiencies directly affect the bottom line of a cloud service provider for both public providers and private organizations that provide cloud services to organizations within their own infrastructures. Figure 2 shows the high-level architecture of the vCloud Director on NetApp storage.
4.2 NETAPP STORAGE SYSTEM BEST PRACTICES

This section provides a high-level overview of the components and features that should be considered when deploying a VMware vCloud Director environment on NetApp storage. For detailed information on storage resiliency, refer to the following NetApp technical reports:

- TR-3437: Storage Subsystem Resiliency Guide
- TR-3450: Active-Active Controller Overview and Best Practices Guidelines

BUILDING A RESILIENT STORAGE ARCHITECTURE

The NetApp highly resilient storage environment for vCloud Infrastructures provides maximum uptime and reliability. By allowing maximum operations of vCloud Infrastructures, NetApp further increases return on investment (ROI) and total cost of ownership (TCO) for the entire environment. NetApp uses the following technologies to provide a resilient vCloud Infrastructure:

- **Active-active NetApp controllers.** If the controller in a storage system is not designed correctly, it can be a single point of failure. Active-active controllers provide controller redundancy and simple automatic transparent failover in the event of a controller failure to deliver enterprise-class availability. Providing transparent recovery from component failure is critical because all desktops rely on the shared storage. For more information, refer to [www.netapp.com/us/products/platform-os/active-active.html](http://www.netapp.com/us/products/platform-os/active-active.html).

- **Multipath HA.** Multipath HA storage configuration further enhances the resiliency and performance of active-active controller configurations. Multipath HA—configured storage enhances storage resiliency by reducing unnecessary takeover by a partner node due to a storage fault, improving overall system availability, and promoting higher performance consistency. Multipath HA provides added protection against various storage faults, including HBA or port failure, controller-to-shelf cable failure, shelf module failure, dual intershel1 cable failure, and secondary path failure. Multipath HA helps provide consistent performance in active-active configurations by providing larger aggregate storage loop bandwidth. For more information, refer to TR-3437: Storage Subsystem Resiliency Guide.
**RAID data protection.** Data protection against disk-drive failure using RAID is a standard feature of most shared storage devices. However, with the capacity and subsequent rebuild times of current hard drives, where exposure to another drive failure can be catastrophic, protection against double-disk failure is now essential. NetApp RAID-DP®, an advanced RAID technology, is provided as the default RAID level on all FAS systems. RAID-DP provides performance that is comparable to that of RAID 10, with much higher resiliency. It provides protection against double-disk failure as compared to RAID 5, which can only protect against a single disk failure in a RAID group. NetApp strongly recommends using RAID-DP on all RAID groups that store VMware View™ data. For more information on RAID-DP, refer to TR-3298: RAID-DP: NetApp Implementation of Double-Parity RAID for Data Protection.

**SnapProtect.** SnapProtect software integrates with NetApp Snapshot technology to provide a seamless and centralized backup and recovery software solution. Whether you have a traditional or a shared IT infrastructure, SnapProtect software in your VMware environment can help meet backup windows and rapidly restore data while reducing administrative costs. With its single management console, you can create, catalog, and manage application-aware Snapshot copies across disk to disk to tape. With SnapProtect software, you can build a single backup and recovery solution that spans traditional and shared IT infrastructures in both traditional virtual environments and in vCloud Director environments.

**Remote LAN management (RLM) card.** The RLM card improves storage system monitoring by providing secure out-of-band access to the storage controllers, which can be used regardless of the state of the controllers. The RLM offers a number of remote management capabilities for NetApp controllers, including remote access, monitoring, troubleshooting, logging, and alerting features. The RLM also extends AutoSupport™ capabilities of the NetApp controllers by sending alerts or a down storage system notification with an AutoSupport message when the controller goes down, regardless of whether the controller can send AutoSupport messages. These AutoSupport messages also provide proactive alerts to NetApp to help provide faster service. For more information on RLM, refer to http://now.netapp.com/NOW/download/tools/rlm_fw/info.shtml.

**Networking infrastructure design (FCoE, FC, or IP).** A network infrastructure (FCoE, FC, or IP) should have no single point of failure. An HA solution includes having two or more FC, FCoE, or IP network switches; two or more CNAs, HBAs, or NICs per host; and two or more target ports or NICs per storage controller. In addition, if using Fibre Channel, two independent fabrics are required to have a truly redundant architecture.

For additional information on designing, deploying, and configuring vSphere SAN and IP networks, refer to TR-3749: NetApp and VMware vSphere Storage Best Practices.

**TOP RESILIENCY BEST PRACTICES**

Follow these top resiliency best practices:

- Use RAID-DP, the NetApp high-performance implementation of RAID 6, for better data protection.
- Use multipath HA with active-active storage configurations to improve overall system availability and to promote higher performance consistency.
- Use the default RAID group size (16) when creating aggregates.
- Allow Data ONTAP to select disks automatically when creating aggregates or volumes.
- Use the latest Data ONTAP general deployment release available on the NetApp Support site.
- Use the latest storage controller, shelf, and disk firmware available on the NetApp Support site.
- Take advantage of disk drive differences: FC, SAS, SATA disk drive types, disk size, and rotational speed (RPM).
- Maintain two hot spares for each type of disk drive in the storage system to take advantage of Maintenance Center.
- Do not put user data into the root volume.
- Replicate data with SnapMirror or SnapVault® for disaster recovery (DR) protection.
- Replicate to remote locations to increase data protection levels.
- Use an active-active storage controller configuration (clustered failover) to eliminate single points of failure (SPOFs).
- Deploy NetApp SyncMirror® and RAID-DP for the highest level of storage resiliency.

For more information, refer to TR-3437: Storage Subsystem Resiliency Guide.

BUILDING A HIGH-PERFORMANCE STORAGE ARCHITECTURE

A VMware vCloud Director workload can have a varying rate of input/output (I/O) intensity because of the different workloads that each customer might deploy. A storage array with multiple customers on it can experience a host of issues. Simultaneous boot up (boot storm), login (login storm), and virus scan within the virtual machines are all issues that can be faced by storage in a cloud. A boot storm, depending on how many ESX Servers and guests are attached to the storage, can create a significant performance effect if the storage is not sized properly. A boot storm can affect both the speed in which the virtual machines are available to the customer and the overall customer experience. A virus scan storm is similar to a boot storm in I/O but might last longer and can significantly affect the customer experience. A virus scan storm is when a virus scan within the guest is initiated on all the clients at once.

Design the storage architecture to eliminate or decrease the effect of these events.

- **Aggregate sizing.** An aggregate, the NetApp virtualization layer, abstracts physical disks from logical datasets, which are referred to as flexible volumes. Aggregates are the means by which the total IOPS available to all of the physical disks are pooled as a resource. This design is well suited to meet the needs of an unpredictable and mixed workload. Whenever possible, NetApp recommends using a small aggregate as the root aggregate. This aggregate stores the files required for running and providing GUI management tools for the storage system. The remaining storage should be placed into a small number of large aggregates. The overall disk I/O from VMware environments is traditionally random by nature; therefore, this storage design gives optimal performance because a large number of physical spindles are available to service I/O requests. On smaller storage systems, having more than a single aggregate might not be practical because of the restricted number of disk drives on the system. In these cases, it is acceptable to have only a single aggregate.

- **Disk configuration summary.** When sizing your disk solution, consider the number of virtual machines being served by the storage controller and disk system and the number of IOPS per virtual machine to calculate the number and size of the disks needed to serve the given workload. Keep the aggregates large, the spindle count high, and the rotational speed fast. When one factor needs to be adjusted, Flash Cache can help eliminate potential bottlenecks to the disk.

- **Flexible volumes.** Flexible volumes contain either LUNs or virtual disk files that are accessed by VMware ESX Servers. NetApp recommends a one-to-one alignment of VMware datastores to flexible volumes. This design offers an easy means to understand the VMware data layout when viewing the storage configuration from the storage system. This mapping model also makes it easy to implement Snapshot backups and SnapMirror replication policies at the datastore level, because NetApp implements these storage side features at the flexible volume level.

- **LUNs.** LUNs are units of storage provisioned from a NetApp storage controller directly to the ESX Servers. The LUNs presented to the ESX Server are formatted with the VMware File System (VMFS). This shared file system is capable of storing multiple virtual desktops and is shared among all ESX Servers within the HA/DRS cluster. This method of using LUNs with VMFS is referred to as a VMFS datastore.

- **Flash Cache.** Flash Cache enables Virtual Storage Tiering and improves read performance. In turn, it increases throughput and decreases latency. It provides greater system scalability by removing IOPS limitations due to disk bottlenecks and lowers cost by providing the equivalent performance with fewer disks. Leveraging Flash Cache in a dense (deduplicated) volume allows all the shared blocks to be accessed directly from the intelligent, faster Flash Cache versus disk. Flash Cache provides great benefits in a VMware vCloud environment, especially during a boot storm, login storm, or virus storm, because only one copy of deduplicated data needs to be read from the disk (per volume). Each
subsequent access of a shared block is read from Flash Cache and not from disk, increasing performance and decreasing latency and overall disk utilization.

4.3 NETWORK ARCHITECTURE

IP storage connectivity is very effective in vCD environments because of its ease of configuration, management, and implementation. In this vCD architecture, we use NFS for connectivity of the vSphere environment to the NetApp storage infrastructure. For IP network connectivity of storage, NetApp recommends using switches that support cross-stack EtherChannel trunking or virtual port channels (VPCs). As a best practice, NetApp also recommends using a design similar to Fibre Channel (FC) connectivity by separating IP-based storage traffic from public IP network traffic by implementing separate physical network segments or logical network segments using VLANs. If a VLAN is used, NetApp recommends using private, nonroutable VLANs to increase security. Provided the switches in the environment use cross-stack EtherChannel trunking, each storage controller needs only one physical connection to each switch. The two ports connected to each storage controller are then combined into one multimode LACP VIF with IP load-balancing enabled.

Also, it is extremely important to have at least two physical Ethernet switches for proper network redundancy in your VMware vCloud Director environment. Carefully plan the network layout for your environment, and develop detailed visual diagrams that display the connections for each port.

When connecting a datastore to the ESX Servers, the administrator configures the connection to use the IP addresses on a private nonroutable VLAN assigned to the NetApp storage controller. When NFS datastores are used, this is accomplished by specifying the IP address when mounting the datastore. Unlike iSCSI datastores (detailed in TR-3749: NetApp and VMware vSphere Storage Best Practices), each NFS datastore should be connected only once from each ESX/ESXi Server using the same NetApp target IP address on each ESX/ESXi server.

When creating a VMware vCloud Director environment that contains several hundred or several thousand virtual machines, be sure to create a large enough DHCP scope inside the cloud to cover the number of IP addresses that will be needed by the clients. This step should be planned well before implementation. Furthermore, a range of static IP addresses will also be needed. These should be set aside on the DHCP server as well.

4.4 UNIFIED ARCHITECTURE

The NetApp Unified Storage Architecture enables customers to deploy an agile and scalable shared storage infrastructure that can meet all the VMware vCloud Director storage requirements from a single storage array:

- VMware vCloud Director tenant data (vApps, VMs, catalogs with vApp templates, and media files) hosted on NFS or VMFS (FC, FCoE, or iSCSI) datastores
- SaaS (guest-connected storage) for tenant vApps and VMs (for example, shared NFS mounts or iSCSI LUNs directly connected inside the VMs in a vApp)
- VMware vCloud Director infrastructure VMs hosted on NFS or VMFS (FC, FCoE, or iSCSI) datastores
- NFS shared storage mounted on all VMware vCloud Director server hosts as the transfer area required for uploading/downloading vApp templates and media files to and from local computers

All NetApp storage systems use the Data ONTAP operating system to provide SAN (FC, FCoE, and iSCSI), NAS (CIFS and NFS), and HTTP capabilities from the same storage array. This provides a significant cost savings for building a scalable VMware vCloud Director environment on a scalable storage array.
4.5 STORAGE EFFICIENCY

NetApp storage in a VMware vCloud Director environment provides enhanced storage efficiency at the datastore level by using primary storage deduplication in conjunction with NetApp thin provisioning. These savings are achievable for both VMware vCloud Director tenant data (VMs, vApps, catalogs with vApp templates, and media files) and VMware vCloud Director infrastructure VMs deployed on any of the storage protocols (FC, FCoE, iSCSI, and NFS).

As a statement of confidence in our ability to provide storage saving in virtual environments, NetApp provides a 50% virtualization storage savings guarantee as well.

THIN PROVISIONING

Thin provisioning is a way of logically presenting more storage to hosts than physically available. With thin provisioning, the storage administrator can utilize a pool of physical disks (known as an aggregate) and create logical volumes for different applications to use without having to preallocate space to those volumes. The space gets allocated only when the host needs it. The unused aggregate space is available for the existing thinly provisioned volumes to expand or to create new volumes. For more information on thin provisioning, refer to NetApp TR-3563: NetApp Thin Provisioning Increases Storage Utilization with On-Demand Allocation.

Figure 3) Traditional provisioning and thin provisioning.

---

NETAPP DEDUPLICATION

NetApp deduplication saves space on primary storage by removing redundant copies of blocks within a volume hosting hundreds of virtual desktops. This process is transparent to the application and user and can be enabled and disabled on the fly. In a vCloud environment, deduplication can provide significant space savings, because each VM can be an identical copy of the OS, applications, and patches. Deduplication is also ideal for user and personal (profile) data stored in CIFS home directories. However, not all data within a vCloud environment is ideal for deduplication. Data such as swap and other transient data should not be deduplicated. For more information on NetApp deduplication, refer to NetApp TR-3505: NetApp Deduplication for FAS and V-Series Deployment and Implementation Guide.
4.6 RAPID PROVISIONING

Cloud tenants demand a very elastic and scalable environment that allows multiple VMs to be rapidly provisioned on demand and also allows self-serviced VM provisioning for individual tenants as needed.

VMware vCloud Director and NetApp provide the capability to meet both these requirements with agility and high levels of storage efficiency. By using VMware vCloud Director administrator-directed VM provisioning, the VMware vCloud Director administrator provisions the desired number and types of VMs as requested by the tenant. The VMs are created in VMware vCenter and imported as vApps into the tenant organization vDCs.

In a VMware vCloud Director environment built on traditional storage arrays, this operation in the past would result in a VMware full clone operation. However, because of the nature of VMware full cloning, each method provisioned by VM/vApp consumed time and required a distinct amount of storage for each VM that essentially had the same or a similar type of data.

However, with vCloud Director 1.5, fast provisioning of virtual machines is now available. This feature functions similarly to the VMware View linked clone feature and allows for rapid provisioning of virtual machines with a small storage footprint.

In addition to fast provisioning, the NetApp FlexClone capability can be leveraged by VMware vCloud Director by using the NetApp Rapid Cloning Utility (RCU) ability. RCU allows for the rapid creation of tens, hundreds, or thousands of VMs into a vSphere or vCloud environment while simultaneously increasing storage efficiency by achieving storage savings of up to 90% in some environments. By leveraging VMware vCloud Connector, you can then import these VMs into the appropriate tenants.

4.7 PERFORMANCE

Cloud providers might face performance issues associated with hosting thousands of VMs on shared storage, specifically performance associated with events that produce a large influx of simultaneous I/O such as login storms, boot storms, and antivirus operations. With vCloud Director, significant performance issues might arise during these critical operations. This essentially means the solution would require a large number of additional spindles to meet the performance requirements, resulting in an increased overall cost for the solution.

To solve this problem, the NetApp solution contains Virtual Storage Tiering, which is a core component of Data ONTAP and is extended with Flash Cache (formerly PAM II). These solution components save customers money by:

- Requiring far less disks and cache
- Not requiring tiers of SSD disk to alleviate boot and login storms
- Serving read data from cache freeing up disk I/O to perform writes
- Providing better throughput and system utilization
- Providing faster response times and a better overall end user experience

Also, performance SLAs can be achieved with the NetApp deduplication-aware Flash Cache and FlexShare capabilities. These capabilities strongly complement the NetApp storage efficiency capabilities by accelerating the performance of deduped data and by providing performance QoS on a per-datastore basis.

VIRTUAL STORAGE TIERING

Virtual Storage Tiering (VST) allows customers to benefit from NetApp storage efficiency while at the same time significantly increasing I/O performance. VST is natively built into the Data ONTAP operating system and works by leveraging block-sharing technologies such as NetApp primary storage deduplication and file/volume FlexClone to reduce the amount of cache required and eliminate duplicate disk reads. Only one instance of any duplicate block is read into cache, thereby requiring less cache than
traditional storage solutions. One clear example of this deduplicated read cache advantage is in the deployment of VMware View virtual desktop implementations, where customers can see as great as 99% initial space savings (validated in the NetApp solutions lab during a 50,000-seat buildout) using NetApp space-efficient cloning technologies. This translates into higher cache deduplication and high cache hit rates. VST is especially effective in addressing the simultaneous system boot or boot storm and login of hundreds to thousands of virtual desktop systems that can overload a traditional legacy storage system.

VST offers the following benefits:

- **Increased performance.** When VST is combined with FlexClone and deduplication, latencies decrease significantly by a factor of 10x versus serving data from the fastest spinning disks available, giving submillisecond data access. Decreasing the latency results in higher throughput and lower disk utilization, which directly translate into fewer disk reads.

- **Lower TCO.** Requiring fewer disks and getting better performance allow customers to increase the number of virtual machines on a given storage platform, resulting in a lower total cost of ownership.

- **Green benefits.** Power and cooling costs are reduced because the overall energy needed to run and cool the Flash Cache module is significantly less than even a single shelf of Fibre Channel disks. A standard DS14mk4 disk shelf of 300GB 15K RPM disks can consume as much as 340 watts (W)/hr and generates heat up to 1394Btu/hr. In contrast, the Flash Cache module consumes only a mere 18W/hr and generates 90Btu/hr. Deploying one less shelf can lead to power savings alone of as much as 3000kWh/year. In addition to the environmental benefits of heating and cooling, each shelf that is not used saves 3U of rack space. For a real-world deployment, a NetApp solution (with Flash Cache as a key component) would typically replace several such storage shelves; therefore, the savings could be considerably higher.

**FLASH CACHE**

NetApp Flash Cache is a hardware device that extends the native Data ONTAP VST capabilities. Flash Cache increases the amount of available cache, which helps to reduce virtual machine storm activities. For more information on NetApp Flash Cache technology, visit [http://www.netapp.com/us/products/storage-systems/flash-cache/flash-cache-tech-specs.html](http://www.netapp.com/us/products/storage-systems/flash-cache/flash-cache-tech-specs.html).

**FLEXSHARE**

NetApp FlexShare provides performance QoS by granting up to five priority levels to control workload prioritization, making it possible to create a VMware vCloud Director environment with multiple tiers of storage services specifically based on the granted QoS levels. For more information on FlexShare, refer to NetApp [TR-3459: FlexShare Design and Implementation Guide](http://www.netapp.com/us/products/storage-systems/flash-cache/flash-cache-tech-specs.html).

**FLEXIBLE VOLUMES AND AGGREGATES**

Flexible volumes (also known as FlexVol® volumes) and aggregates provide pools of storage. This storage virtualization allows the performance and capacity to be shared by all desktops in the volume or aggregate. Similar to the way that VMware virtualizes computing resources, NetApp virtualizes the storage resources.

### 4.8 NETAPP VSPHERE INTEGRATION

**vStorage API for Array Integration (VAAI)**

vStorage API for Array Integration (VAAI) is a VMware vStorage initiative that enables I/O offload from the hypervisor layer to the storage controllers. The key value proposition for this integration with storage partners is to improve the scalability and performance of the infrastructure. NetApp is fully integrated with VAAI primitives, for both block and NFS storage. Because vCloud Director builds on top of vSphere, VAAI offload benefits are leveraged at the vCloud Director layer, without any manual user intervention.
VAAI FOR BLOCK STORAGE

The following primitives for VMFS storage provide benefits at the vCloud Director layer:

- **Copy offload.** When a vApp is deployed from the catalog or a vApp is being cloned as a vApp template to catalog, the copying operations (read from storage array, write to storage array) are offloaded to the storage controller. Additionally, for fast provisioning of vApps using VMware redo log-based linked clones, when the destination datastore does not have a copy of the source vApp template base disk, a copying operation is required to create a shadow VM that serves as the new base for the destination datastore. This copy operation is offloaded to the storage controller to provide better efficiency.

- **Hardware-assisted locking.** vCloud Director 1.5 provides stateless scale-up and scale-out architecture to support the elastic nature of cloud workloads. It supports multiple vCenter Servers and aggregate compute, networking, and storage resources into a new layer of abstraction (provider vDC). A typical deployment involves a large number of ESX Servers sharing a common set of VMFS volumes. Hardware-assisted locking is imperative to enhance the scalability of the large environment by eliminating the need for SCSI-2 reservation to lock up the entire LUN. Instead, it offloads the lock to the array with the automatic test and set operation to lock metadata regions at the disk sector level.

- **Thin provisioning: space reclamation.** Cloud workloads are often bursty in nature, meaning vApps are instantiated and then decommissioned after specifically defined periods of usage. With this new primitive in vSphere 5 VAAI, vApp deletion triggers an UNMAP command to be sent to the storage controller. This command frees up the associated blocks of the vApps, which return free disk capacity back to the VMFS volumes. Additionally, Storage vMotion® can be programmatically invoked at the vCD layer (relocate_vm vCloud API). When this VMDKs migration takes place between datastores, the source datastore incurs dead space, which is unused blocks that belong to the moved VMDKs. Space reclamation in vSphere 5 VAAI reclaims this dead space and returns it to the pool of available capacity.

- **Thin provisioning: out-of-space monitoring.** Thin provisioning is a common and key storage feature that enables cloud providers to overcommit storage allocation (because bursty workloads frequently have varying levels of space allocation and deallocation). However, use this feature carefully because overcommitment can cause exhaustion of physical disk capacity. With this new primitive in vSphere 5 VAAI, the NetApp storage controller alerts the ESX Server when the thin-provisioned flexible volume runs out of disk capacity (where auto_grow can no longer grow the volume automatically due to exhaustion of physical capacity). The out-of-space condition populates in the vCenter Server UI, and the ESX storage stack halts and suspends all I/O operations for all virtual machines affected. In addition, an alert window is generated to recommend administrative actions to increase the storage capacity and allow a retry of the failed writes.

VAAI FOR NFS STORAGE

vSphere5 has introduced VAAI primitives for the NFS storage protocol. The following primitive provides benefits at the vCloud Director layer:

- **Full file copy.** Similar to the copy offload block primitive, full file copy enables the ESX Server to offload copying operations resulting from a vApp template deployment from the catalog or a clone of a vApp into the catalog as a vApp template. Additionally, for fast provisioning of vApps using VMware redo log-based linked clones, a copy operation is required to create a shadow VM that serves as the new base for the destination datastore when the destination datastore does not have a copy of the source vApp template base disk. This copying operation is offloaded to the NFS storage controller to provide better efficiency.

VSTORAGE API FOR STORAGE AWARENESS

vStorage API for storage awareness (VASA) integration provides transparency of storage provisioned to ESX clusters. Finding LUN or NFS volume protection attributes, state, and the policies for protection and replication is not easy at the vCenter Server or vCloud Director layers. VASA integration provides this information, out of band, to the vCenter Server. Although not directly propagated to the vCloud Director...
layer at the current state, VASA integration still provides benefits for vCloud Director deployments. vCD builds on top of vSphere; therefore, all compute, network, and storage resources must be preconfigured by the provider and or the cloud administrator. If the provider vDC is differentiated based on storage type, then the cloud administrator must know the capabilities, the protection/replication schedules, and the disk types when the flexible volume/NFS exports are presented to the ESX Server. VASA integration makes this information readily available in vCenter Server, thereby enabling the cloud administrators to create meaningful datastore naming conventions. These conventions make it easier to associate the right storage type, for the right level of resource allocation, during the provider vDC creation.

4.9 VIRTUAL STORAGE CONSOLE

NetApp Virtual Storage Console (VSC) is a VMware vCenter plug-in that enables cloud administrators to centrally perform storage operations such as monitoring, provisioning datastores, VM cloning, deduplication, backup and recovery, and data replication without requiring coordinated support from storage administrators. In addition, the plug-in includes real-time discovery, health monitoring, capacity management, and enhanced toolsets for storage I/O performance for a more efficient environment. This combination of unique capabilities provides VMware administrators with the necessary tools to improve server and storage visibility and efficiencies while still enabling storage administrators to own and control storage policies. For more information on NetApp VSC, refer to http://www.netapp.com/us/products/management-software/vsc/virtual-storage-console.html.

4.10 NETAPP VCLOUD INFRASTRUCTURE INTEGRATION

VMWARE VCENTER ORCHESTRATOR PLUG-IN FOR NETAPP

The NetApp vCenter Orchestrator (vCO) plug-in offers an integrated approach to storage creation and management inside of vCloud Director. With the ability to create organizations, configure storage, and create vFiler® units for secure-multi tenancy (SMT) integration with vCloud Director, the NetApp vCO plug-in enables administrators to easily manage their cloud environment without having to touch the storage controller. This plug-in integrates into Operations Manager, which is part of the NetApp OnCommand® core package, and uses the Storage Catalog Services to provision storage based on set parameters that could include types of disk drives, storage performance, and backup and recovery policies. By having integrated policies that can be driven from within a VMware framework, a cloud administrator can deploy, configure, and remove storage when necessary.

OPERATIONS MANAGER

SANSCREEN VM INSIGHT

Also available as a VMware vCenter plug-in, NetApp SANscreen® VM Insight, which is part of the NetApp OnCommand core package, provides multi-tenant visibility from the VM to the shared storage, allowing both storage and server administration teams to more easily manage their VMware vCloud Director storage and server infrastructure. VM Insight provides service-level information for virtual servers, physical servers, and storage devices, as well as VM volume, allocated capacity, and datastore information from VMware vCenter. Based on this visibility, VM Insight shows the actual service paths and server performance information to allow end-to-end monitoring. The enterprise-class data warehouse provides IT the ability to access, query, and analyze VM data; and, when deployed with SANscreen Capacity Manager, it enables capacity planning and chargeback for VM environments.

For more information, refer to SANscreen VM Insight.
The NetApp Snap Creator™ Framework addresses the needs and challenges that administrators and developers face by providing a centralized and consistent solution for backing up critical information: a solution that integrates with existing application environments to reduce costs and enable a higher ROI.

Snap Creator integrates with vCloud Director and provides granular-level backup and recovery of the cloud architecture. Virtual machines, organizations, and vApps can be backed up and restored as needed using Snap Creator.

Follow these best practices and recommendations when using the Snap Creator Framework:

- Review the NetApp Snap Creator for 3.4.0 Installation and Configuration Guide for information on how to use features within Snap Creator Framework. A significant number of configuration options are available to facilitate both simple and complex backup configurations.
- Create configuration files through the GUI so that default options are created properly (even if the configuration files can be created and executed through a CLI interface). The configuration can then be edited to add additional enhancements.
- Verify each backup configuration separately before testing both of them together when creating configurations to support vApp and application-consistent backups. By using this method, issues with the application-consistent backup and the vApp-consistent backup can be confirmed independently.
• Use the Snap Creator Framework agent in conjunction with the Snap Creator Framework server when using the VMware plug-in for vCloud because of the potential Java® timeout conditions during long-running restore operations.
• Use HTTP for NetApp controller connectivity when creating a new Snap Creator Framework 3.4 configuration. This requirement will change in later releases of Snap Creator Framework.
• When using the Snap Creator Framework agent, set an agent timeout to a value sufficient for the backup configuration to run to completion. A general recommendation is a minimum of 300 seconds. However, this value can be increased as needed depending on the number of objects being backed up as well as the size of the vCloud environment.
• Select the backup objects based on the service provided to tenants when backing up multiple vApps, vDCs, or organizations. For example, if the entire organization represents a single-service policy or tier, one configuration file might be sufficient. However, if different service levels are provided across vDCs or specific vApp names, change the vCloud backup objects to group backups based on the service-level agreements (SLAs) provided to each tenant.
• Verify that the metadata associated to the vApp and VM exist in vCD and vSphere respectively when performing restore operations with Snap Creator Framework. Snap Creator Framework cannot currently restore VM and vApp objects if the metadata does not exist. This also applies if the VM or vApp has moved from its original location and a backup was not completed.
• Take vApp backups before every maintenance operation to provide rollback capability, especially if an application is changing within the vApp.
• Use the vSphere restore capabilities within the VMware plug-in to perform the restore operation so other VMs associated to the vApp are not affected if a single VM within a vApp must be restored. When Snap Creator Framework performs a restore of a vApp, all VMs associated to the vApp will be restored. In addition, create a backup for rollback purposes in advance of the restore.
• Verify that sufficient Snapshot space exists on the volumes holding the datastores and resource pools. In addition, verify that the NetApp best practices have been applied to the ESX hosts, clusters, datastores, and VMs, including alignment, for newly deployed vApps to be backed up.
• Adjust the number of logs saved in the configuration file if a longer retention time is needed for logs. If backup policies include vDC or organizations, all vApps underneath will be backed up. However, because the Snap Creator Framework does not have a database or catalog, a record of what is backed up is not stored except in the log files for the backed-up vApps.
• Change the `VIBE_VMWARE_SNAPSHOT` variable in the configuration file from Y to N if VMware snapshots are not desired. By default, the VMware plug-in for vCloud and vSphere environments creates VMware snapshots for each VM associated to a vApp being backed up. This change can be made using a text file editor.

5 SOLUTION IMPLEMENTATION PROCEDURES

5.1 PURPOSE

This section provides a step-by-step guide on how to deploy VMware vCloud Director 1.5 on NetApp FAS series active-active controller configurations. It covers the deployment of a multiorganization environment in a vCloud Director environment.

This section is intended as an instructional guide and does not attempt to explain why certain steps are taken. For more detailed information on some of the steps included in this document, refer to TR-3749: NetApp and VMware vSphere Storage Best Practices.

These directions focus on achieving multiple levels of storage efficiency and performance acceleration for each of the deployment scenarios in these organizations. Although steps for only three different types of organization models are detailed, the principles for storage layout, efficiency, performance acceleration, and operational agility can be used for every type of deployment.
This section does not focus on maximizing the number of virtual machines that can be placed on a storage controller. Instead, it focuses on the methodology needed to deploy the given scenario of virtual machines in a vCloud environment in a step-by-step approach. The methodology demonstrated in this section can be scaled up for larger deployments and down for smaller deployments. Each vCloud environment should have a sizing exercise performed as part of the planning phase for each deployment.

5.2 THE DEPLOYMENT SCENARIO

This section demonstrates a deployment scenario for three different organizations in a vCloud Director environment. The first organization is a pure virtual server environment and has only Microsoft® Windows® 2008 servers. The second has Microsoft Windows 7 desktops exclusively. The third and final environment has a mix of servers and desktops. Table 1 summarizes the organizations and their operating platforms.

Table 1) Deployment mix for each organization.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Type of Storage</th>
<th>Number of VMs</th>
<th>Servers and Desktops</th>
<th>Type of Backup and Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>FC</td>
<td>20</td>
<td>20 servers</td>
<td>Hourly, daily, and weekly Snapshot copies and nightly DR</td>
</tr>
<tr>
<td>Silver</td>
<td>FC</td>
<td>30</td>
<td>20 desktops</td>
<td>Hourly, daily, and weekly Snapshot copies and weekly DR</td>
</tr>
<tr>
<td>Bronze</td>
<td>SATA</td>
<td>30</td>
<td>10 servers 10 desktops</td>
<td>Hourly and daily Snapshot copies</td>
</tr>
</tbody>
</table>

This configuration can be used with NetApp FAS series active-active controller configurations as well as NetApp V-Series controllers. By detailing this representative VMware vCloud Director 1.5 environment, deployment methodologies for larger or smaller environments can be derived. The design can be easily altered to suit any combination and number for each deployment type. Use these guidelines to assist in setting up environments ranging from proof of concepts (POCs) to production deployments.

5.3 THE ENVIRONMENT

Proper licensing for the NetApp controllers, VMware products, Windows 2008, and Windows 7 must be obtained to use these features. Where appropriate, trial licenses can be used for many of the solution components to test the configuration.

5.4 SOFTWARE NEEDED FOR DEPLOYMENT

- NetApp System Manager 1.1
- VMware vSphere (ESX 5.0 and vCenter Server 5.0)
- VMware vCloud Director 1.5
- VMware vCenter Orchestrator
- NetApp Virtual Storage Console (VSC) 2.1
- NetApp Snap Creator 3.4
- VMware vCenter Orchestrator plug-in for NetApp

6 NETWORK SETUP

Because of the complexity and variety of each organization’s network environment, it is very difficult to provide a single network configuration topology. For this solution design, we focused on using a network
environment that takes advantage of cross-stack EtherChannel switching. For more detailed information on additional network configuration options and on the following topics, refer to TR-3749: NetApp and VMware vSphere Storage Best Practices:

- Traditional Ethernet switch designs
- Highly available storage design with traditional Ethernet switches
- vSphere networking with multiple virtual machine kernel ports
- vSphere with multiple virtual machine kernel, traditional Ethernet, and NetApp networking with single-mode VIFS
- vSphere with multiple virtual machine kernel, traditional Ethernet, and NetApp networking with multilevel VIFS
- Cross-stack EtherChannel switch designs
- Highly available IP storage design with Ethernet switches that support cross-stack EtherChannel
- EtherChannel vSphere networking and cross-stack EtherChannel
- vSphere and NetApp with cross-stack EtherChannel
- Datastore configuration with cross-stack EtherChannel

### 6.1 NETWORK SETUP OF CISCO NEXUS NETWORK SERIES

We used a network design with two switches capable of cross-stack EtherChannel and VLAN segmentation for the purpose of this deployment. We then cross-linked these two switches to two core switches, with both downstream switches connected to each core switch, to provide failover redundancy.

**Note:** When implementing switch configurations, follow the switch vendor’s best practices.

The goal of using cross-stack EtherChannel in conjunction with VLAN segmentation is to provide logical separation of public IP traffic from storage IP traffic. In doing this, the chance of issues developing from changes made to a portion of the network is mitigated, and security of data traveling across the nonroutable storage VLAN is protected.

Cross-stack EtherChannel deployment also provides a high level of redundancy and fault tolerance by enabling multiple parallel paths between nodes and load balancing traffic where alternate paths exist. This solution uses a 10GbE environment.

When creating the network:

- Make sure that both switches have at least one connection to both core switches.
- Make sure that the cross-stack EtherChannel has been enabled and configured.
- Create the public VLAN, service console VLAN*, NFS VLAN, and the vMotion VLAN.
- Configure the NFS and vMotion networks as private and nonroutable VLANs.

**Note:** *This configuration is optional. If you do not use this configuration or have this option available, use the public VLAN for the service console.

If you are using cross-stack EtherChannel switches, configure a nonroutable VLAN for the NFS storage traffic to pass to and from the NetApp storage controllers to the vSphere hosts. With this setup, the NFS traffic is kept completely contained, and security is more tightly controlled.

Also, it is extremely important to have at least two physical Ethernet switches for proper network redundancy in your VMware vCloud Director environment. Carefully plan the network layout for your environment and develop visual diagrams that detail the connections for each port.
7 INSTALL AND CONFIGURE VSphere AND VCloud DIRECTOR

7.1 INSTALL VSphere

For information on the installation and configuration of vSphere, refer to the ESX and vCenter Server Installation Guide published by VMware.

7.2 INSTALL VMware vCenter Server

For information on the installation and configuration of VMware vCenter Server, refer to the ESX and vCenter Server Installation Guide published by VMware.

To obtain licenses for VMware, contact your VMware sales representative.

7.3 CONFIGURE SERVICE CONSOLE FOR REDUNDANCY

Follow the steps in Table 2 to configure the service console for redundancy.

Table 2) Configure the service console for redundancy.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Make sure that the primary service console vSwitch has two NICs assigned to it. <strong>Note:</strong> The network ports that the NICs use must exist on the administrative VLAN and be on separate switches to provide network redundancy.</td>
</tr>
<tr>
<td>2</td>
<td>Open VMware vCenter.</td>
</tr>
<tr>
<td>3</td>
<td>Select a vSphere host.</td>
</tr>
<tr>
<td>4</td>
<td>In the right pane, click the Configuration tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Hardware box under the Configuration tab, click Networking.</td>
</tr>
<tr>
<td>6</td>
<td>In the Networking section, click the Properties section of vSwitch1.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>7</td>
<td>In the Properties section, click the Network Adapters tab. Click Add.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Network Adapters tab" /></td>
</tr>
<tr>
<td>8</td>
<td>Select the vmnic that will act as the secondary NIC for the service console. Click Next.</td>
</tr>
</tbody>
</table>
9. In the following screen, verify and click Next.

10. Click Finish.
7.4 CONFIGURE VMWARE KERNEL NFS PORT

Follow the steps in Table 3 to configure the VMware kernel NFS port.
Table 3) Configure VMware kernel NFS port.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>For each vSphere host, create a separate NFS VMkernel network in the existing virtual switch. The VMkernel will be set up on the private, nonroutable NFS VLAN created in previous steps. This example uses VLAN 350.</td>
</tr>
</tbody>
</table>
| 2    | Use the following assignments for your NFS storage traffic VMware kernel IP addresses.  
**Note:** The storage network uses the private subnet of 192.168.0.xxx.  
vSphere Host 1: 192.168.0.11  
vSphere Host 2: 192.168.0.12  
vSphere Host 3: 192.168.0.13 |
| 3    | For the vSwitch for the NFS VMware kernel, set the load balancing policy to **Route based on IP hash**. |

7.5 **CONFIGURE VMOTION**

Follow the steps in Table 4 to configure vMotion.

Table 4) Configure vMotion.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>For each vSphere host, create a separate vMotion VMkernel network in the existing virtual switch. The VMkernel will be set up on the private, nonroutable vMotion VLAN created in previous steps. This example uses VLAN 350.</td>
</tr>
</tbody>
</table>
| 2    | Use the following assignments for your vMotion VMware kernel IP addresses.  
**Note:** The storage network uses the private subnet of 192.168.1.xxx. |
7.6 CONFIGURE VMWARE VSPHERE HOST NETWORK

Figure 8 depicts how a fully configured network environment looks after the previous networking steps are completed.

Figure 8) VMware vSphere host configuration example.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6</td>
<td>CONFIGURE VMWARE VSPHERE HOST NETWORK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Before beginning this process, make sure that one vmnic is available to create the dvSwitch. Open vCenter and click Home.</td>
</tr>
</tbody>
</table>
2 Click Networking.

3 At the Networking screen, right-click the data center that houses your vCloud infrastructure and select New vSphere Distributed Switch.

4 Choose vSphere Distributed Switch Version: 5.0.0 and select Next.
5  Enter a name for the dvSwitch and select the number of uplink ports you need. Click Next.

6  Choose Add now and then select the hosts that you want to add to the dvSwitch. Also, select the
Step 7

Verify that **Automatically create a default port group** is checked and that all information is correct and click Finish.
8 Convert the current vSwitch settings to the new dvSwitch.

9 Right-click the new dvSwitch and select Manage Hosts.
10 Select the hosts that you want to manage and click Next.

11 Chose all of the vmnics. By doing this, you will import the current vmnic that is being used by the vSwitch to the dvSwitch and regain your network redundancy. Make sure to choose the correct uplink port group for the vmnic being imported. Click Next.
12 Verify that each VMkernel is being transitioned to the correct dvPortGroup. This will import all the VMkernels that do vMotion, NFS connectivity, and management from your vSwitch to the dvSwitch. All IP settings are also transitioned during this process. Click Next.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Unless you have virtual machines to migrate, click Next at this screen.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Screenshot of the VMware Cloud Infrastructure and Management on NetApp interface for migrating virtual machine networking from vSwitch to dvSwitch." /></td>
</tr>
<tr>
<td>14</td>
<td>Verify the settings for the migration and click Finish. You have now migrated all of your settings from the vSwitch to the dvSwitch.</td>
</tr>
</tbody>
</table>
7.8 INSTALL AND CONFIGURE VCLOUD DIRECTOR 1.5

Refer to the VMware “vCloud Director Installation and Configuration Guide” for directions on how to install vCloud Director 1.5. For vCloud Director, you must also install and configure a vShield Manager appliance. Follow all of the VMware best practices and recommendations for performing the install.

8 STORAGE CONFIGURATION

Perform all of the steps listed in this section on both controllers of the NetApp system. A failure to do so could result in inconsistencies and performance problems within the environment.

8.1 NETWORK SETUP OF NETAPP STORAGE CONTROLLER

To achieve optimal performance, maximize the number of Ethernet links for both controllers in the NetApp active-active controller configuration. Follow the steps in Table 6 to set up the network for both storage controllers.

Table 6) Set up network for both storage controllers.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to the NetApp storage controllers using System Manager.</td>
</tr>
</tbody>
</table>
### 2. Use the previous diagrams as a reference on how to configure the cabling for the FAS storage controller.
- For 10GbE connections, determine the interface from each of the two dual-port NICs that will separate the Cisco Nexus 5020 switches. In total, two connections should go to Cisco Nexus 5020 A and two should go to Cisco Nexus 5020 B.
- Use this setup on both FAS storage controllers in the active-active controller configuration.

### 3. The ports that connect these interfaces to the switches must meet the following criteria:
- They must be on the nonroutable VLAN created for the NFS network traffic.
- They must be configured into a trunk, either manually as a multimode VIF or as an LACP VIF.
- If LACP is used, then the VIF type must be set to static LACP instead of multimode on the NetApp storage controller.

**Note:** For the purposes of this document, we use the 192.168.0.0/24 network for the private subnet for NFS and the 192.168.1.0/24 network for the private subnet for vMotion.

- The NetApp storage controller IP address range is from 192.168.0.2 through 192.168.0.10.
- The vSphere NFS VMware kernel IP address range is from 192.168.0.11 through 192.168.0.254.
- The address range of the VMware kernel IP enabled by VMware vMotion is from 192.168.1.11 through 192.168.1.254.

### 8.2 CONFIGURE NFS TRUNK

Complete the steps in Table 7 to configure the NFS trunk.

**Table 7  Configure NFS trunk.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to the NetApp storage controllers using System Manager.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP Address</th>
<th>Partner</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0a</td>
<td>Ethernet</td>
<td>192.168.11.118</td>
<td>NA</td>
<td>Enabled</td>
</tr>
<tr>
<td>e0b</td>
<td>Ethernet</td>
<td>192.168.11.1184</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>e0M</td>
<td>Ethernet</td>
<td>NA</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>e0a</td>
<td>Ethernet</td>
<td>NA</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>e0b</td>
<td>Ethernet</td>
<td>NA</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>e0a</td>
<td>Ethernet</td>
<td>NA</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>e0b</td>
<td>Ethernet</td>
<td>NA</td>
<td>NA</td>
<td>Disabled</td>
</tr>
<tr>
<td>lb</td>
<td>Loopback</td>
<td>127.0.0.1</td>
<td>NA</td>
<td>Enabled</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Click Next in the Create VIF Wizard screen.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Enter the name of the VIF, select the four 10GbE interfaces, choose the LACP option, and click Next.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Select IP based as the load-balancing type and click Next.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Load balancing type**

Load balancing type determines how the network packets are transmitted for multimode and LACP VIF.

- **IP based**
  - Outgoing interface is selected on the basis of file's and client's IP address
- **MAC based**
  - Outgoing interface is selected on the basis of file's and client's MAC address

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>In the VIF Interface Parameters screen, enter the IP address and the subnet mask and click Next.</td>
</tr>
</tbody>
</table>
6. Click Finish to build the VIF.

![Create VIF Wizard]

Completing the Create VIF Wizard

You have successfully completed the steps needed to create the VIF with the following properties:

- Name: "vif"
- Interface links: e0b, e0c, e2a, e3b
- Trunk mode: UACP
- Load balancing mode: "IP"
- IP address: 192.168.1.2
- Net mask: 255.255.255.0
- Gateway: NA
- MTU size: "1500"
- Trusted: "Yes"
- VINS: "Yes"

Click Finish to create the VIF interface and close this wizard.

7. Verify that the VIF is enabled. The VIF created should display as an entry similar to the one below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP Address</th>
<th>Gateway</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vif</td>
<td>VIF</td>
<td>192.168.2.2</td>
<td>NA</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Note:** Repeat these steps for the two remaining ports. Make sure that one NIC is on switch A and the other is on switch B. These ports will be used for CIFS and management traffic and should be set up using VLAN tagging.

### 8.3 OVERVIEW OF THE NETAPP STORAGE CONTROLLER DISK CONFIGURATION

Figure 9 shows the disk layout for production data on both of the NetApp storage controllers. Aggr0 is only used for the root file system and is typically three drives. To meet the performance and capacity needs of this configuration, each controller has one data aggregate (Aggr1 for hosting production virtual machines) with the required number of spindles and enough spare disks that can be easily added later to the aggregates to deal with unknowns.
8.4 CONFIGURE NETAPP STORAGE CONTROLLER SSH CONFIGURATION

Follow the steps in Table 8 to configure the SSH configuration for both NetApp storage controllers.

Table 8) Configure storage controller SSH configuration.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to the NetApp storage controller’s console (by using either the telnet or console connection).</td>
</tr>
</tbody>
</table>
| 2    | Run the following commands and follow the setup script:  
  - `secureadmin setup ssh`  
  - `options ssh.enable on`  
  - `options ssh2.enable on` |

8.5 CONFIGURE FLEXSCALE FOR FLASH CACHE

Flash Cache is an intelligent read cache that reduces storage latency and increases I/O throughput by optimizing performance of random read-intensive workloads. As a result, disk performance is increased, and the amount of storage needed is decreased.

Follow the steps in Table 9 to configure NetApp FlexScale™ for Flash Cache.

Table 9) Configure FlexScale for Flash Cache.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to the NetApp storage controller’s console (using either SSH, telnet, or console connection).</td>
</tr>
</tbody>
</table>
| 2    | Run the follow commands to enable and configure FlexScale:  
  - `options flexscale.enable on` |
8.6 CONFIGURE VCLOUD DIRECTOR DATASTORE AGGREGATE

Follow the steps in Table 10 for both storage controllers to configure the vCloud Director datastore aggregate.

**Note:** The data aggregate should have a RAID group size no smaller than 12.

Table 10) Configure vCloud Director datastore aggregate.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open NetApp System Manager, right-click Aggregates, and select Create.</td>
</tr>
<tr>
<td>2</td>
<td>The Create Aggregate Wizard launches. Click Next.</td>
</tr>
<tr>
<td>3</td>
<td>Name the aggregate <strong>vCloud_Production</strong>, and choose Dual parity for the RAID type.</td>
</tr>
</tbody>
</table>
For the aggregate size, choose 19 of the available 21 drives. This provides 17 data drives, 2 parity drives, and 2 spares. Click Next.

Review the settings, click Next, and click Finish to build the new data aggregate.

8.7 MODIFY THE AGGREGATE SNAPSHOT RESERVE FOR THE VMWARE VCLOUD AGGREGATE

Follow the steps in Table 11 for both storage controllers to modify the aggregate Snapshot reserve for the VMware vCloud aggregate.

Table 11) Modify the aggregate Snapshot reserve for the VMware vCloud aggregate.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to the controller’s console, using either SSH, telnet, or the serial console.</td>
</tr>
</tbody>
</table>
| 2    | Set the aggregate Snapshot schedule:  
  `snap sched -A <aggregate-name> 0 0 0` |
| 3    | Set the aggregate Snapshot reserve:  
  `snap reserve -A <aggregate-name> 0` |
| 4    | Delete existing Snapshot copies:  
  `snap list -A <vol-name>`  
  `snap delete <vol-name> <snap-name>` |
| 5    | Press CTRL+D to log out of the NetApp console. |
9 NETAPP STORAGE AND SOFTWARE SETUP

The steps in this section demonstrate how to create NetApp volumes and VMware datastores through the use of VSC 2.1.

9.1 CONFIGURE VSC 2.1

Follow the steps in Table 12 to configure VSC 2.1.

Table 12) Configure VSC 2.1.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To begin provisioning storage with VSC 2.0.1P1, the storage controllers must be added to vCenter through the VSC 2.0.1P1 plug-in. Log in to vCenter, click the Home link, and then click the NetApp icon listed under Solutions and Applications.</td>
</tr>
<tr>
<td>2</td>
<td>On the left pane, click Provisioning and Cloning, Storage controllers, Add…</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>3</td>
<td>Enter the host name or IP address, user name, and password, and select SSL if it is currently configured on the storage controller. Click Next.</td>
</tr>
<tr>
<td>4</td>
<td>Select the interfaces, volumes, and aggregates that will be available to VSC 2.0.1P1. Click Next.</td>
</tr>
</tbody>
</table>
5. The following screen provides advanced settings and shows the defaults that have been chosen. Click Next.

6. Review the selections and click Apply. Repeat the process for all storage controllers that the VSC 2.0.1P1 will use.
9.2 CREATE AN INITIAL VCLOUD VOLUME FOR OPERATING SYSTEM TEMPLATES

Follow the steps in Table 13 to create an initial vCloud volume for operating system templates.

Table 13) Create initial vCloud volume for operating system templates.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To provision datastores across multiple ESX hosts in a data center, in vCenter right-click a data center, select NetApp, and then select Provision datastore.</td>
</tr>
</tbody>
</table>

![Image of vSphere Client window](image1.png)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Click the storage controller to deploy the datastore to use.</td>
</tr>
</tbody>
</table>

![Image of Storage Controller details](image2.png)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Specify the datastore type. This example uses NFS.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 4    | Complete the wizard:  
|      | • Set the size of the volume as 100GB.  
|      | • Name the volume `vcloud_datastore_1`.  
|      | • Place the `vcloud_datastore_1` volume on the `vCloud_Production` aggregate.  
|      | • Enable thin provisioning.  
|      | • Enable `auto-grow`.  
|      | • Enter a grow increment of 5.  
|      | • Enter a maximum datastore size of 150.  
|      | • Click Next when all information is entered.  |

**Select the datastore type you would like to create**

Which of the 2 types of datastores would you like to use?

<table>
<thead>
<tr>
<th>Storage Controller details</th>
<th>Datastore type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NFS</td>
</tr>
<tr>
<td></td>
<td>VMFS</td>
</tr>
</tbody>
</table>

**Datastore details**

<table>
<thead>
<tr>
<th>Datastore details</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 Verify that all information is correct and click Apply.
6. Select one of the ESX hosts on which the new datastore was created, click the Configuration tab, right-click the new datastore, select NetApp, Deduplication Management. Make sure that the deduplication state is set to Enabled.
9.3 CONFIGURE SNAPSHOT COPIES AND OPTIMAL PERFORMANCE

Follow the steps in Table 14 to host volumes in the template virtual machine.

Table 14) Host volumes in template virtual machine.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into System Manager.</td>
</tr>
<tr>
<td>2</td>
<td>To configure Snapshot copies, highlight the rcu_gold volume, click Snapshot, and then click Configure.</td>
</tr>
<tr>
<td>3</td>
<td>Set the Snapshot reserve (%) to 0 and clear the Enable scheduled snapshots option. Click Apply and then OK to return to the System Manager main screen.</td>
</tr>
</tbody>
</table>
To set optimal performance, highlight `vcloud_datastore_1`, right-click the directory, and select `Edit` from the drop-down list.
5. Click the Auto Size tab and make sure that both the Allow volume to grow automatically and Delete snapshots automatically boxes are checked. Click Apply.

6. Click the Deduplication tab and make sure that the Enable deduplication on volume is selected. Set the deduplication schedule according to your business needs.
### 9.4 CONFIGURE VMS FOR VCLOUD INFRASTRUCTURE

Set up two template VMs to be used for vCloud Director and place them in the newly created datastore. One Windows 2008 VM and one Windows 7 VM are required. Verify that these VMs are ready for deployment and are configured using the VMware best practices. After the VMs are created, power them off. In a later step, the newly created storage will be added to vCloud Director, which will make these VMs available for import and use.

### 10 STORAGE CONTROLLERS ADDITIONAL SETUP AND CONFIGURATION

Follow the steps in this section for both storage controllers.

**CREATE THE VOLUME TO HOST VIRTUAL MACHINE SWAP FILES**

Follow the steps in Table 15 to create the volume to host the virtual machine swap files.

**Table 15** Create volume to host virtual machine swap files.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In vCenter, right-click cluster and click NetApp, and then select Provision datastores. This will provision datastores across multiple ESX hosts in a data center.</td>
</tr>
<tr>
<td>2</td>
<td>At the next screen, select the storage controller to which you would like to deploy the datastore.</td>
</tr>
</tbody>
</table>
3 Complete the wizard using the following and click Next:
- Make the size of the volume 100GB.
- Name the volume vCloud_swap.
- Place the vCloud_swap volume on the vCloud_Production aggregate.
- Enable thin provisioning.
- Enable autogrow.
- Enter a grow increment of 5.
- Enter a maximum datastore size of 150.

Note: The size of the vCloud_vswap varies depending on the size of the vCloud environment that is being deployed.

4 In the next screen, verify that all information is correct and click Apply.

5 Select one of the ESX hosts on which the new datastore was created, click the Configuration tab, right-click the new datastore, select NetApp, Deduplication Management, and verify that the deduplication state is set to Enabled.

### CONFIGURE THE VOLUME

Follow the steps in Table 16 to configure the volume.

Table 16) Configure volume.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into System Manager.</td>
</tr>
<tr>
<td>2</td>
<td>To configure Snapshot copies, highlight the vCloud_swap volume, click Snapshot, and then click Configure.</td>
</tr>
<tr>
<td>3</td>
<td>Set the Snapshot reserve (%) to 0 and clear the Enable scheduled snapshots option. Select Apply and then OK to return to the System Manager main screen.</td>
</tr>
<tr>
<td>4</td>
<td>To set optimal performance, highlight and right-click vCloud_swap, and click Edit from the drop-down list.</td>
</tr>
<tr>
<td>5</td>
<td>Click the Auto Size tab and make sure that both the Allow volume to grow automatically and Delete snapshots automatically boxes are selected. Click Apply.</td>
</tr>
<tr>
<td>6</td>
<td>Click the Deduplication tab and set the deduplication schedule according to your business needs.</td>
</tr>
<tr>
<td>7</td>
<td>Select the Advanced tab. Make sure that the No access time updates option is selected. Also make sure that the No automatic Snapshot copy box is selected. Click Apply and then OK to return to the main System Manager screen.</td>
</tr>
</tbody>
</table>

### 10.1 CONFIGURE LOCATION OF VIRTUAL SWAP FILE DATASTORE

Follow the steps in Table 17 to configure the location of the virtual swap file datastore.

Table 17) Configure location of virtual swap file datastore.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open VMware vCenter.</td>
</tr>
<tr>
<td>2</td>
<td>Select a vSphere host.</td>
</tr>
<tr>
<td>3</td>
<td>In the right pane, click the Configuration tab.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>In the Software box, select Virtual Machine Swapfile Location.</td>
</tr>
<tr>
<td>5</td>
<td>In the right pane, click Edit. The virtual machine Swapfile Location Wizard opens.</td>
</tr>
<tr>
<td>6</td>
<td>Click vCloud_swap datastore and click OK.</td>
</tr>
<tr>
<td>7</td>
<td>Repeat steps 2 through 7 for each vSphere host in the vSphere cluster.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Note:</strong> If the vSphere hosts are part of a cluster, the swap file location must be changed first in the cluster configurations. In vCenter, right-click the cluster and click Edit Settings.</td>
</tr>
</tbody>
</table>
9  Select Swapfile Location and select Store the swapfile in the datastore specified by the host. Click OK and proceed editing the individual vSphere hosts.

10.2 CONFIGURE OPTIMAL PERFORMANCE FOR VMDKS ON NFS

Follow the steps in Table 18 for all the volumes with NFS exports configured for controller A.
Table 18) Configure optimal performance for VMDKs on NFS.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the NetApp console.</td>
</tr>
<tr>
<td>2</td>
<td>From the storage appliance console, run: options nfs.tcp.recvwindowsize 64240</td>
</tr>
</tbody>
</table>

11 CONFIGURE OPERATIONS MANAGER

11.1 INSTALL OPERATIONS MANAGER

Install and license the following to install operations manager:

- **DataFabric® Manager Server.** The installation and configuration guide can be found at [http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/upgrade.pdf](http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/upgrade.pdf).

- **Operations Manager.** The administration and configuration guide can be found at [http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/opsmgr.pdf](http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/opsmgr.pdf).

- **Provisioning Manager and Protection Manager.** The workflow guide for both Provisioning Manager and Protection Manager can be found at [http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/workflow.pdf](http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel402/pdfs/workflow.pdf).

11.2 SET UP RESOURCE POOLS

After Operations Manager is configured and installed, log in and perform the steps in Table 19 to configure a resource pool to provision storage from the VMware vCenter Orchestrator plug-in for NetApp.

Table 19) Set up resource pools.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open Operations Manager, click the Data tab, and then click Resource Pools. Click Add.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the relevant information at the next screen, choose the correct time zone, and click Next.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>3</td>
<td>Select the aggregate or aggregates that will be used for the resource pool and click Next.</td>
</tr>
<tr>
<td>4</td>
<td>Enter a label for the resource pool and click Next.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>5</td>
<td>Select the space thresholds and the aggregate overcommit thresholds appropriate for your organizations policies and click Next.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that all of the information is correct and click Finish.</td>
</tr>
</tbody>
</table>
### 11.3 SET UP PROVISIONING POLICIES

Follow the steps in Table 20 to set up the provisioning policies.

Table 20) Set up provisioning policies.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open Operations Manager and click the Policies tab. Click Add to create a new provisioning policy.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>2</td>
<td>Click Next at the following screen.</td>
</tr>
<tr>
<td></td>
<td><img src="image1.png" alt="Add Provisioning Policy Wizard" /></td>
</tr>
<tr>
<td>3</td>
<td>At the next screen, choose the appropriate availability options that are consistent with your organizations policies and click Next.</td>
</tr>
<tr>
<td></td>
<td><img src="image2.png" alt="Add Provisioning Policy Wizard" /></td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>Select the resource label created in the previous section. Then click Next.</td>
</tr>
</tbody>
</table>
5. Select your deduplication options and click Next.

6. Select your space utilization properties and click Next.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Select your space thresholds and click Next.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Space Thresholds" /></td>
</tr>
<tr>
<td>8</td>
<td>If you have a provisioning script path, enter it at this screen. If not, leave this blank. Click Next.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Provisioning Script" /></td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>9</td>
<td>Verify that the information you entered is correct and click Finish.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add Provisioning Policy Wizard" /></td>
</tr>
</tbody>
</table>

10 The main screen displays along with the provisioning policy that you just created.

11.4 SET UP DATASET PROVISIONING

Follow the steps in Table 21 to set up dataset provisioning.
Table 21) Set up dataset provisioning.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open Operations Manager and click the Data tab. Click Datasets and then click Add to create a new provisioning policy.</td>
</tr>
<tr>
<td>2</td>
<td>Click Next.</td>
</tr>
<tr>
<td>3</td>
<td>At the General Properties screen, enter a name for the dataset and all other relevant information.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>Select the group to which to add the dataset and click Next.</td>
</tr>
<tr>
<td>5</td>
<td>Select Provision and attach resources using a policy and click Next.</td>
</tr>
</tbody>
</table>
6 Choose the provisioning policy created in a previous step.

7 At the same screen, click NFS Export Settings and turn this setting on.
8

On the same screen, click the Resource Pools tab and choose the resource pool created in the previous steps. Click Next.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>A vFiler instance has not been created for this specific setup; therefore, click Next to advance to the next screen.</td>
</tr>
<tr>
<td>10</td>
<td>Select No and click Next.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>11</td>
<td>Click Next after the conformance results are successfully completed.</td>
</tr>
<tr>
<td>12</td>
<td>Verify that the information on this screen is correct and click Finish.</td>
</tr>
</tbody>
</table>
### 12 INSTALL AND CONFIGURE VCENTER ORCHESTRATOR PLUG-IN

In order to use the VMware vCenter Orchestrator plug-in for NetApp, the vCenter Orchestrator must be installed and configured for use with your vCloud environment. Refer to the “vCenter Orchestrator Installation and Configuration Guide” from VMware for information on how to install and configure vCenter Orchestrator.

Follow the steps in Table 22 to install and configure VMware vCenter Orchestrator.

**Table 22) Install and configure VMware vCenter Orchestrator.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>The main screen displays, and the dataset that you just created will be visible.</td>
</tr>
<tr>
<td>14</td>
<td>Repeat these steps to create both silver and bronze provisioning services.</td>
</tr>
</tbody>
</table>

### Step 1

**Open VMware vCenter Orchestrator Configuration.**

1. Open VMware vCenter Orchestrator Configuration.

### Step 2

**Verify that the network, LDAP, and database are configured correctly.**

2. Verify that the network, LDAP, and database are configured correctly. Also, verify that the environment has been properly licensed. Finally, make sure that the vCloud Director plug-in has been installed and configured.

### Step 3

**Click the Plug-ins tab.**

3. Click the Plug-ins tab. Click the search icon under **Install new plug-in** and browse to the NetApp plug-in.

### Step 4

**Click Upload and Install.**

4. Click **Upload and Install.** After the plug-in has been uploaded, click **Apply Changes.**
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Go to Startup Options and click Restart Service.</td>
</tr>
<tr>
<td>6</td>
<td>The plug-in loads after the service restarts. Click the new NetApp tab.</td>
</tr>
<tr>
<td>7</td>
<td>Configure the NetApp plug-in with the IP address of the Operations Management server. Also, configure the credentials for the administrator name and password for the Operations Management server.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>8</td>
<td>Log in to the vCenter Orchestrator client and verify that the NetApp workflows are present.</td>
</tr>
</tbody>
</table>
**13 CONFIGURE VCLOUD DIRECTOR**

**13.1 SET UP PROVIDER VDC**

Follow the steps in Table 23 to set up the provider VDC.

Table 23) Set up provider VDC.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open the VMware vCenter Orchestrator plug-in for NetApp.</td>
</tr>
</tbody>
</table>
2. Select the Workflows tab and then expand the NetApp Workflows section. Expand the vCloud Provisioning section. Right-click Provision Provider vDC with ONTAP Datastore and select Start Workflow.
### Step 3

**Action**

The following screen displays.

<table>
<thead>
<tr>
<th>Resource Pool Provisioning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Provisioned in ESX Cluster</td>
</tr>
<tr>
<td>ESX Cluster</td>
</tr>
<tr>
<td>New Resource Pool</td>
</tr>
<tr>
<td>New Resource Pool Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Datastore Provisioning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Provision to access ESX</td>
</tr>
<tr>
<td>Storage Service for new Datastore</td>
</tr>
<tr>
<td>Datastore Name</td>
</tr>
<tr>
<td>Size of Datastore (GB)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provider vDC Provisioning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>vCloud Host</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Enable this provider vDC</td>
</tr>
</tbody>
</table>

*3 errors - [Datastore Name], Mandatory field not set*

### Step 4

**Action**

Click **Not set listed** next to ESX Cluster. At the screen that displays, drill down under the desired cluster. Under the host folder, click the cluster to which you want to provision. Click **Select**.

### Step 5

**Action**

When the main screen displays and your cluster is selected, enter a name for the resource pool that you will create.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6</strong></td>
<td>Under Datastore Provisioning, click <strong>Not set</strong> next to Storage Service for new Datastore. Then drill down at the next screen until you can select the storage service that was created in a previous step. <strong>Click Select.</strong></td>
</tr>
</tbody>
</table>

**Datastore Provisioning**

<table>
<thead>
<tr>
<th><strong>Datastore</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision to secure vFilier</td>
<td>○ Yes ○ No</td>
</tr>
<tr>
<td>Storage Service for new Datastore</td>
<td><strong>Not set</strong></td>
</tr>
<tr>
<td>Datastore Name</td>
<td></td>
</tr>
<tr>
<td>Size of Datastore (GB)</td>
<td><strong>2.0</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Select (NetApp) Storage Service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetApp</strong></td>
</tr>
<tr>
<td><strong>vCloud Host</strong></td>
</tr>
<tr>
<td><strong>Physical Storage Systems</strong></td>
</tr>
<tr>
<td><strong>Virtual Storage Systems</strong></td>
</tr>
<tr>
<td><strong>Storage Service Catalog</strong></td>
</tr>
<tr>
<td><strong>Gold Datastore Provisioning Storage Services</strong></td>
</tr>
</tbody>
</table>

**vCloud Hosts**

<table>
<thead>
<tr>
<th><strong>vCloud Hosts</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>XYZ-Corp Provider1-vCloud-Host</strong></td>
</tr>
</tbody>
</table>

| **7** | When the storage service is selected under Datastore Provisioning, enter the datastore name and size. |

**Datastore Provisioning**

<table>
<thead>
<tr>
<th><strong>Datastore</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision to secure vFilier</td>
<td>○ Yes ○ No</td>
</tr>
<tr>
<td>Storage Service for new Datastore</td>
<td><strong>Gold Datastore Provisioning Storage Services</strong></td>
</tr>
<tr>
<td>Datastore Name</td>
<td><strong>XYZ-Corp Provider1-vCloud-Host-Gold</strong></td>
</tr>
<tr>
<td>Size of Datastore (GB)</td>
<td><strong>500</strong></td>
</tr>
</tbody>
</table>

| **8** | Under Provider vDC Provisioning, click **Not set** next to vCloud Host. At the vCloud Host screen, drill down and select the vCloud Director environment. |

---

82 VMware Cloud Infrastructure and Management on NetApp
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 9    | After the vCloud Director environment is selected:  
- Name the provider vDC  
- Enter a description  
- Enable the vDC  
- Choose whether you would like it to be elastic  
- Choose if you want to enable HA  
- Enter the CPU and memory amounts you would like the provider vDC to have from the resources available |
| 10   | Click Submit to create the provider vDC. |
### 13.2 ADD STORAGE CONTAINING TEMPLATE VMS FOR PROVIDER VDC

Follow the steps in Table 24 to add storage containing the template VMs for the provider vDC.

**Table 24** Add storage containing template VMs for provider vDC.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open vCloud Director, go to the Manage and Monitor tab, and then to Provider vDCs, and select your provider. Select the Datastores tab. Click the add datastore button.</td>
</tr>
</tbody>
</table>

![Add/Remove Datastores window](image)

- Select the vCloud_datastore_1 datastore, click Add, and click OK.

2 | At the Add/Remove Datastores window, select the vCloud_datastore_1 datastore, click Add, and click OK. |

![Add/Remove Datastores window](image)

3 | Your Provider vDC screen should now contain the newly added datastore. |

---

---

---
14 SET UP ORGANIZATIONS AND VAPPS IN VCLOUD DIRECTOR

The following sections contain generic steps to set up the vCloud Director 1.5 environment. Not all screens are shown for each step. Refer to the “VMware Install and Configuration Guide for vCloud Director 1.5” for specific instructions.

14.1 SET UP THE GOLD ORGANIZATION

The gold organization has a high level of backup and recovery, and it exists on the fastest disk drives. Follow the steps in Table 25 to set up the gold organization.

Table 25) Set up gold organization.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open a Web page to your vCloud Director environment and log in.</td>
</tr>
<tr>
<td>2</td>
<td>Create an external network for your vCloud Infrastructure.</td>
</tr>
</tbody>
</table>
3. Create a network pool for your vCloud infrastructure.

4. Create an organization for your vCloud environment.
5  Allocate resources to the organization that you created.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Add network resources to the organization that you created. This requires the creation of both an internal network and an external network.</td>
</tr>
</tbody>
</table>
14.2 ADD ADDITIONAL STORAGE TO THE PROVIDER VDC

Use the VMware vCenter Orchestrator plug-in for NetApp to provision additional storage to the provider vDC. Follow the steps in Table 26 to add additional storage to an existing provider vDC.

Table 26) Add additional storage to provider VDC.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open the VMware vCenter Orchestrator plug-in for NetApp.</td>
</tr>
<tr>
<td>2</td>
<td>Select Not set next to the ESX host.</td>
</tr>
<tr>
<td>3</td>
<td>Drill down until an ESX host is in the data center to which you deployed the PvDC in the previous steps.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>Select Not set next to Storage Service, and drill down until you find the storage service to which you would like to deploy the PvDC.</td>
</tr>
<tr>
<td>5</td>
<td>For the purposes of this scenario, select the silver storage service and click Select.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>6</td>
<td>Enter the datastore name and size.</td>
</tr>
</tbody>
</table>
| ![Image](image1.png) **ESX Cluster**
| **ESX Cluster**
| ESX Host | 10.81.177.222 |
| Storage Service | Silver Datostore Provisioning Storage Services |
| Datastore Name | OrganizationSilver-1 |
| Datastore Size (GB) | 500 |
| 7    | Under the vCloud section, click *Not set* next to Provider vDC. |
| ![Image](image2.png) **vCloud**
| **vCloud**
| Provider vDC | Not set |
| 8    | On the next screen, drill down until you find the provider vDC to which you want to deploy additional storage. Highlight the provider vDC and click Select. |
After all the steps have been completed, click Submit.

### 14.3 SET UP THE SILVER ORGANIZATION

The silver organization is set up using a moderate level of backup and disaster recovery capability, and it is set up to use fast disk shelves. Perform steps 4 through 6 in Table 25 to set up the organization in vCloud Director. Point this organization at the storage created for silver-level environments.

### 14.4 SET UP THE BRONZE ORGANIZATION

The bronze organization is set up using a low level of backup and no disaster recovery capability. It is also set up to use slower disk shelves and relies on the NetApp Flash Cache technology to enhance speeds for the individual VMs. Perform steps 4 through 6 in Table 25 to set up the organization in vCloud Director. Point this organization at the storage created for bronze-level environments.
14.5 SET UP VAPP

The next step is to import the Microsoft Windows 2008 VM created in a previous step into vCloud Director and the organization Gold vDC.

Create the vApps in the individual organizations that were previously created by adding 20 Windows 2008 VMs into the gold organization, 20 Windows 7 VMs into the silver organization, and 10 of each operating system into the bronze organization.

Refer to the VMware “vCloud Director Administrator’s Guide” for directions on how to create a vApp within an organization.

15 INSTALL AND CONFIGURE SNAP CREATOR

The backup solution for vCloud Director uses the Snap Creator Framework. For information on how to install and configure Snap Creator, refer to the “Snap Creator 3.2 Installation and Administration Guide.”

Snap Creator Framework 3.4 supports the backup and restore of vApps within a vCloud environment. The following two sections walk through the installation and configuration process for the Snap Creator Framework.

15.1 INSTALL SNAP CREATOR FRAMEWORK

Follow the steps in Table 27 to install Snap Creator Framework.

Table 27) Install Snap Creator.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | • Download the Snap Creator Framework 3.4 (or newer) Windows installation package from the NetApp Support (formerly NOW®) site under Software Downloads: [https://now.netapp.com/NOW/cgi-bin/software](https://now.netapp.com/NOW/cgi-bin/software).  
• You will need a NOW account to access the software. In addition, select the appropriate x86 or x64 version to download based on the 32-bit or 64-bit Windows version running on the server hosting Snap Creator Framework. The vCloud backups with Snap Creator Framework 3.4 are currently supported for Windows environments only. Refer to the NetApp Interoperability Matrix Tool at [http://now.netapp.com/matrix](http://now.netapp.com/matrix) for more information.  
• Additional requirements include installation of Java Runtime Environment (JRE) 1.6 for the Windows platform (32-bit or 64-bit). Disk space and memory requirements are documented in the NetApp Snap Creator Framework 3.4.0 release notes. The documentation for Snap Creator Framework is located at: [https://now.netapp.com/NOW/knowledge/docs/snapcreator/rel340/index.shtml](https://now.netapp.com/NOW/knowledge/docs/snapcreator/rel340/index.shtml). |
2. Install the Snap Creator Framework on a physical or virtual Windows server from where the backups will be managed. The server must have network access to both the vCloud Director server as well as the vCenter instances being managed. The first step is launching the installation package. Review the welcome screen and click the Next button to continue.

3. Review the license agreement on the next screen, and if you accept the terms of the agreement, click the I Agree button to continue.
4 The next screen displays the install type for Snap Creator Framework. For vCloud environments, both the Snap Creator Framework agent and server installation types must be checked. In addition, the Snap Creator Framework server and agent service should be installed so that Snap Creator Framework services start each time Windows starts. Changing the default server and agent ports is not required unless the environment requires a more complex port mapping or if a port conflict exists with the listed ports on the server.

After checking the appropriate options, click Next to continue.

5 Under the Profile setup window, enter the serial number of a NetApp controller that is being used for Snapshot copies. Only one serial number is required. In addition, a GUI user name and password must be created. This will be the user name for managing Snap Creator Framework through the GUI interface, and it is not associated with any Active Directory® user name or password. Select a user name and password that are easy to remember, and click Next to continue.
In the Install Location window, select a path to install Snap Creator Framework on the local Windows server. Change the path if necessary and click Next to continue.

In the Start Menu Folder window, select the menu folder to use. If other NetApp management software is available on the local Windows server, click the NetApp folder in the list of folders and verify the folder path displays NetApp\Snap Creator. Click the Install button to start the installation process.
The Installation window displays the files being copied into place. If either the server or agent was selected to start as a service, new services will be created after the Next button is clicked. After the installation is completed, click Finish to exit the installer.

15.2 CONFIGURE SNAP CREATOR

Follow the steps in Table 28 to configure Snap Creator.
Table 28) Configure Snap Creator.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open a Web browser to the following URL on the Windows server where the Snap Creator Framework is installed: <a href="http://localhost:8080/">http://localhost:8080/</a>. If Java is properly installed and the Snap Creator Framework server service is running, the following window displays in the browser:</td>
</tr>
</tbody>
</table>

Enter the user name and password created during the installation process and click Connect to continue.
If Snap Creator Framework is properly installed, the following screen displays in the Web browser:

Click the green plus button in the Management Configuration window under Backup Profiles. A new dialog box displays. Enter a new profile name, enter the name `vcloud_backups`, and click Ok.
Create a new configuration by right-clicking the `vcloud_backups` profile and selecting the New Configuration option.

A new Configuration dialog box displays that allows users to create a new Snap Creator configuration file. This file represents the vCloud backup. Click Next to continue.
In the Configuration dialog box, enter the configuration file name to use to store the vCloud backup configuration information. This example uses `vapp_backup` as the configuration file name. Click Next to continue.

In the Plug-ins dialog box, select the VMware vCloud Director plug-in and click Next to continue.
In the Backup Type dialog box, select the type of consistent backup to create. Snap Creator Framework provides two types of consistent backup: One is a standard vApp backup within a vCloud environment, and the other is a vApp- and application-consistent backup. For the purposes of this example, a vApp-consistent backup is created. More complex Snap Creator Framework configurations might include quiesce and unquiesce of applications within a vApp, which is provided with the section option. Click Next to continue.

In the VMware vCloud Director authentication dialog box, enter the URL associated to the vCloud environment. This is generally formatted as https://<IP>/cloud. In addition, enter the user name and password for system credentials. Currently, Snap Creator supports tenant-based backups, which require entering credentials at the system level rather than at the organization level. After entering the appropriate credentials, click Next to continue.
After authentication to the vCloud Director, a list of organizations, vDCs, and vApps appears. Select either the organizations, vDCs, or vApps to back up by checking the boxes next to the name of each object. If an organization or vDC is selected for backup, all vApps within that organization or vDC will be backed up. For this example, vApp_Win2k8 will be backed up. Click Next to continue.

In the VMware vSphere dialog box, enter the vCenter user name and password credentials. In order to create vApp-consistent backups, the vCloud plug-in takes VMware snapshots of each VM associated to the vApps selected in the backup configuration. To take VMware snapshots, commands must be issued to the vCenter server to create and delete snapshots of the VMs during the backup workflow. Therefore, vCenter credentials are required. Click Next to continue.
In the Agent Configuration dialog box, enter the local Snap Creator Framework agent settings. The IP address can be `localhost` or `127.0.0.1`, and the port will be `9090`, or the value entered during the install process. Set the timeout value to a number that provides a sufficient amount of time to run the entire backup configuration, and click `Test agent connection`.

If agent connection is working, a small dialog confirmation box displays. If the box does not appear or an error occurs, verify that the agent service is running on the local Windows server. After confirming the agent is running properly, click `Ok` and `Next` to continue.
13. In the Filer Login Credentials dialog box, enter the storage controller information. HTTP must be used for vCloud instead of HTTPS, and the Windows server running Snap Creator Framework must be able to reach the storage controller on the IP address listed. Click Next to continue.

![Configuration dialog box with Filer Login Credentials](image)

14. In the Snapshot Action dialog box, enter the snapshot information. Select a snapshot name based on the configuration as well as a policy name, snapshot retention, and retention age. A description of the field displays when you hover the mouse over each field. In addition, select the naming convention to use for snapshots. NetApp recommends using the Recent snapshot naming convention if multiple vApps across multiple datastores are backed up. Click Next.

![Configuration dialog box with Snapshot Action](image)
In the Data Protection dialog box, if SnapMirror or SnapVault is configured for the volumes associated to the VMware datastores where the vApps are stored, Snap Creator Framework triggers a SnapMirror and/or SnapVault operation after the backup workflow is completed. Check the appropriate boxes if applicable and click Next to continue.
In the Operations Manager dialog box, enter the Operations Manager host, user name, password, and port information to send Operations Manager alerts when backups are completed. If Protection Manager is in use, click the Protection Manager checkbox. Click Next to continue.

If Protection Manager is selected, a new Protection Manager dataset is created. Place the appropriate resource pools with vCloud data into the newly created dataset and define the protection policy to use.
Click the Finish button to create the configuration file. After the configuration file is created, close the configuration tab by clicking the x button next to the vapp_backup configuration. Click the Refresh button under the Backup Profiles section. Reopen the vapp_backup configuration by clicking the configuration file name in the Backup Profiles section.

Review the settings in the Management Configuration window for completeness. If vApps are stored across multiple NetApp storage controllers, click the green plus button in the Configuration window under Filer Login Credentials to add new controllers and credentials as needed.

15.3 EXECUTE BACKUP

Backups can be scheduled through the Schedules option under the Management menu, or they can be triggered on a one-time basis in advance of a scheduled maintenance activity. To perform a one-time backup, follow the steps in Table 29.
Table 29) Backup execution.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Configurations under the Management section and click the <code>vapp_backup</code> configuration file under the <code>vcloud_backups</code> profile. Select the Actions button under the configuration file.</td>
</tr>
</tbody>
</table>

1. A dialog box requesting information about which policy to use displays. Select the policy used when creating the configuration file. If this is the first time creating a backup with the configuration file, select the Debug Mode checkbox to see the output during the operation of the backup job. Click Ok to start the backup job. |
In the Console section at the bottom of the Management Configurations window, debug output displays that shows the status of the backup operation. As an agent is utilized, each phase of the backup needs to complete before the log results are returned. The console screen looks similar to the following:

```
[Date] DEBUG: Exiting with error code - 0
```

If the backup operation completes successfully, the following message displays:

If a nonzero error code is listed, look for red error messages in the console output to see what the error condition is. Review the “Snap Creator Framework Installation and Administration Guide” on the NOW site for the specific error message and the cause.

If the backup is successful, review the set of snapshots on the volumes of the NetApp controllers where the vApps are stored. If new snapshots are created and the timestamp of the snapshots match, then the backup is working as expected. If snapshots do not exist, review the Snap Creator Framework logs to see where snapshots were created and correct the configuration file to reflect the correct storage controllers and/or vCenter servers.

### 16 VALIDATE SOLUTION

Table 30 includes a checklist designed to determine if your environment is set up correctly. Run these tests as appropriate for your environment and document the results.

**Table 30) Validate solution.**

<table>
<thead>
<tr>
<th>Item</th>
<th>Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Test Ethernet connectivity for VMware vSphere servers and NetApp. If using NIC teams or VIFs, pull network cables or down the interfaces and verify network functionality.</td>
</tr>
<tr>
<td>2</td>
<td>If running in a cluster, test SAN multipathing by performing a cable pull or by disabling a switch port (if applicable).</td>
</tr>
<tr>
<td>3</td>
<td>Verify that datastores are seen as clusterwide resources by creating a custom map of the hosts and datastores and verifying connectivity.</td>
</tr>
<tr>
<td>4</td>
<td>Test vCenter functionality for appropriate access control, authentication, and VI clients.</td>
</tr>
<tr>
<td>5</td>
<td>Perform NetApp active-active controller configuration failover testing for NAS and verify that datastores remain connected.</td>
</tr>
<tr>
<td>6</td>
<td>Test performance and IOPs to determine that the environment is behaving as expected.</td>
</tr>
<tr>
<td>7</td>
<td>Test vCloud Director by logging into the environment and having other accounts log into the environment.</td>
</tr>
</tbody>
</table>
17 REFERENCES

This report referenced the following NetApp documentation:

- Flash Cache
- High Availability
- Installation and Upgrade Guide: For Use with DataFabric® Manager Server 4.0 Supporting Operations Manager, Protection Manager, and Provisioning Manager Operations Manager
- NetApp Interoperability Matrix Tool
- NetApp Snap Creator Framework 3.4.0 Installation and Configuration Guide
- Operations Manager Administration Guide: For Use with DataFabric® Manager Server 4.0
- Provisioning Manager and Protection Manager: Guide to Common Workflows for Administrators For Use with DataFabric® Manager Server 4.0
- Remote LAN
- SANscreen VM Insight
- Snap Creator
- TR-3437: Storage Subsystem Resiliency Guide
- TR-3450: Active-Active Controller Overview and Best Practices Guidelines
- TR-3459: FlexShare™ Design and Implementation Guide
- TR-3505: NetApp Deduplication for FAS Deployment and Implementation Guide
- TR-3563: NetApp Thin Provisioning Increases Storage Utilization With On Demand Allocation
- TR-3749: NetApp and VMware vSphere Storage Best Practices
- TR-3808: VMware vSphere and ESX 3.5 Multiprotocol Performance Comparison Using FC, iSCSI, and NFS
- TR-3841: Snap Creator 3.2 Installation and Administration Guide
- Virtual Storage Console

This report referenced the following VMware documentation:

- ESX Configuration Guide
- ESX and vCenter Server Installation Guide
- Guest Operating System Installation Guide
- Private Cloud Computing
- VMware Infrastructure Documentation
- VMware vCenter Server
- VMware vCloud Director
- vSphere Virtual Machine Administration Guide

18 REVISION HISTORY

Table 31) Revision history.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>August 2011</td>
<td>Original document</td>
</tr>
</tbody>
</table>
19 ACKNOWLEDGMENTS

The authors thank the following people for their contribution to this report:

- Scott Baker, Virtualization Manager, NetApp
- Shekhar Borde, Software Engineer, NetApp
- Prakash Buddhiraja, Member of Technical Staff, NetApp
- Julian Cates, Solutions Architect, NetApp
- Chris Gebhardt, Reference Architect, NetApp
- Neil Glick, Solutions Architect, NetApp
- Nick Howell, Solutions Architect, NetApp
- Simon Mijolovic, vCloud Architect, VMware
- Vaughn Stewart, Director of Virtualization and Cloud Computing, NetApp
- Vinod Talati, Software Engineer, NetApp

20 FEEDBACK

For questions or comments concerning this document, send an e-mail to xdl-vgibutmeymtr@netapp.com.
NetApp provides no representations or warranties regarding the accuracy, reliability or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer’s responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.