



# FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage

## Design Guide

**Last Updated:** August 14, 2017



# About the Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit

<http://www.cisco.com/go/designzone>.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2017 Cisco Systems, Inc. All rights reserved.

# Table of Contents

Executive Summary .....	5
Solution Overview .....	7
Introduction .....	7
Audience .....	7
<b>What's New?</b> .....	7
Solution Summary.....	8
Technology Overview .....	9
FlexPod Datacenter with ACI – Private Cloud .....	9
NetApp All Flash FAS and ONTAP 9 .....	10
Storage Efficiency.....	11
RAID-TEC.....	11
Root-Data-Data Disk Partitioning.....	12
SnapMirror.....	13
FlexClone .....	14
Hybrid Cloud Management System: Cisco CloudCenter.....	14
NetApp Private Storage for Cloud.....	16
Equinix Hosting.....	17
Public Cloud .....	18
Equinix Cloud Exchange .....	19
Solution Design.....	20
FlexPod Datacenter with ACI – Private Cloud .....	21
Cisco CloudCenter – Setting up the Hybrid Cloud Management.....	23
CloudCenter Manager (CCM).....	24
CloudCenter Orchestrator.....	24
AMQP and Guacamole.....	24
Bundle Store.....	25
Package Store .....	25
Management Agent and Base OS Images.....	25
Component Deployment .....	25
Network Rule Configuration .....	26
Private Cloud Configuration .....	27
Amazon Web Services (AWS).....	29
Microsoft Azure Resource Manager (MS Azure RM).....	33

NetApp Private Storage .....	35
NPS to FlexPod Private Cloud VPN connectivity.....	36
NPS for AWS Design Overview .....	37
NPS for Azure Design Overview.....	40
Application Setup .....	44
Application Overview.....	44
Application Data Handling.....	45
OpenCart Application Blue Print.....	45
Cloud Selection .....	46
Deploying Production Instance of Application .....	47
Making Data Available using NetApp Private Storage.....	47
Automating the Data Replication Process .....	49
Application Blue Print – Global Parameters .....	50
Configuration Scripts .....	50
Data Repatriation – Using NPS to Migrate Application(s) to the Private Cloud .....	51
ACI Integration.....	52
Deployment Hardware and Software .....	54
Hardware and Software Revisions .....	54
Validation.....	55
Test Plan .....	55
VPN Connectivity Validation.....	55
Private Cloud Validation.....	55
Public Cloud Validation .....	55
Summary .....	56
References .....	57
Products and Solutions .....	57
Interoperability Matrixes.....	58
About the Authors.....	59
Acknowledgements .....	59

## Executive Summary

---

Cisco Validated Designs (CVDs) deliver systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of the customers and to guide them from design to deployment.

Customers looking to deploy applications using a shared data center infrastructure face a number of challenges. A recurrent infrastructure challenge is to achieve the required levels of IT agility and efficiency that can effectively meet the company's business objectives. Addressing these challenges requires having an optimal solution with the following key characteristics:

- **Availability:** Help ensure applications and services availability at all times with no single point of failure
- **Flexibility:** Ability to support new services without requiring underlying infrastructure modifications
- **Efficiency:** Facilitate efficient operation of the infrastructure through re-usable policies
- **Manageability:** Ease of deployment and ongoing management to minimize operating costs
- **Scalability:** Ability to expand and grow with significant investment protection
- **Compatibility:** Minimize risk by ensuring compatibility of integrated components

Cisco and NetApp have partnered to deliver a series of FlexPod solutions that enable strategic data center platforms with the above characteristics. FlexPod solution delivers an integrated architecture that incorporates compute, storage and network design best practices thereby minimizing IT risks by validating the integrated architecture to ensure compatibility between various components. The solution also addresses IT pain points by providing documented design guidance, deployment guidance and support that can be used in various stages (planning, designing and implementation) of a deployment.

Cloud computing has clearly been one of the most disruptive IT trends of recent times. With the undeniable benefits of cloud computing, many enterprises are now moving aggressively towards a cloud first strategy. While the benefits of public cloud have been proven for certain workloads and use cases, there is growing acknowledgement of its trade-offs in areas such as availability, performance, customization and security. To overcome these public cloud challenges, organizations are adopting hybrid cloud models that offer enterprises a more cohesive approach to adopt cloud computing. A hybrid cloud model gives organizations the flexibility to leverage the right blend of public and private cloud services, while addressing the availability, performance, and security challenges

FlexPod Datacenter for Hybrid Cloud delivers a validated Cisco ACI based FlexPod infrastructure design that allows customers to utilize resources in the public cloud based on the organization workload deployment policies or when the workload demand exceeds the available resources in the Datacenter. The FlexPod Datacenter for Hybrid Cloud showcases:

- A fully programmable software defined networking (SDN) enabled DC design based on Cisco ACI
- An application-centric hybrid cloud management platform: Cisco CloudCenter
- High-speed cloud to co-located storage access: NetApp Private Storage in Equinix Datacenter

- Multi-cloud support: AWS and Azure

## Solution Overview

---

### Introduction

FlexPod solution is a pre-designed, integrated and validated architecture for data center that combines Cisco UCS servers, Cisco Nexus family of switches, Cisco MDS fabric switches and NetApp Storage Arrays into a single, flexible architecture. FlexPod is designed for high availability, with no single points of failure, while maintaining cost-effectiveness and flexibility in the design to support a wide variety of workloads.

FlexPod design can support different hypervisor options, bare metal servers and can also be sized and optimized based on customer workload requirements. FlexPod design discussed in this document has been validated for resiliency (under fair load) and fault tolerance during system upgrades, component failures, and partial as well as total power loss scenarios.

The FlexPod solution for hybrid cloud is based on a Cisco ACI based FlexPod infrastructure design that allows customers to utilize resources in the public cloud when the workload demand exceeds the available resources in the Datacenter. This new FlexPod solution will allow customers to seamlessly extend compute and storage resources from an on-premises FlexPod to major cloud providers such as Amazon and Azure using Cisco CloudCenter and NetApp Private Storage.

### Audience

The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

### What's New?

The following design elements distinguish this version of FlexPod from previous models:

- Integration of Cisco CloudCenter with FlexPod Datacenter with ACI as the private cloud
- Integration of Cisco CloudCenter with Amazon Web Services (AWS) and Microsoft Azure Resource Manager (MS Azure RM) public clouds
- Providing secure connectivity between the FlexPod DC and the public clouds for secure Virtual Machine (VM) to VM traffic
- Providing secure connectivity between the FlexPod DC and NetApp Private Storage (NPS) for data replication traffic
- Ability to deploy application instances in either public or the private clouds and making up-to-date application data available to these instances through orchestration driven using Cisco CloudCenter
- Setting up, validating and highlighting operational aspects of a development and test environment in this new hybrid cloud model

For more information about previous FlexPod designs, see: <http://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html>

## Solution Summary

The FlexPod solution for Hybrid Cloud showcases a development and test environment for a sample open source e-commerce application, OpenCart. Utilizing an application blue-print defined in Cisco CloudCenter, the solution allows customers to deploy new application instances for development or testing on any available cloud within minutes. Using the NetApp Data Fabric combined with automation driven by the Cisco CloudCenter, new dev/test instances of the application, regardless of the cloud location, are pre-populated with up-to-date customer data. When the application instances are no longer needed, the compute resources in the cloud are terminated and data instances on the NetApp storage are deleted. Cisco CloudCenter is also integrated with Cisco ACI to provide both network automation and data segregation within the private cloud deployments. This makes an ACI based FlexPod an ideal platform for this new hybrid environment.

This validated solution is delivered using following core design components:

- Cisco CloudCenter (formerly CliQr) effortlessly deploys and manages applications across both public and private clouds
- Secure connectivity is established from the FlexPod based private cloud to NetApp Private Storage (NPS), Amazon Web Services (AWS) and Microsoft Azure
- Application data is replicated from on-premise FlexPod storage array to NetApp Private Storage and cloned copies are made available to new application dev/test instances on demand
- NetApp Private Storage, hosted in Equinix DC, allows customers to store and access critical data across multiple clouds while maintaining strict access control
- Deleting an application instance deletes the data associated with the application instance for additional security
- The solution allows customers to move their workloads and associated critical user data to on-premise FlexPod private cloud

## Technology Overview

---

The FlexPod Datacenter with Hybrid Cloud comprises of following four design areas:

- Private Cloud: FlexPod Datacenter with ACI
- Hybrid Cloud Management System: Cisco CloudCenter
- NetApp Private Storage for Cloud
- Public Cloud

The technologies and solutions covered in each of these areas is described below.

### FlexPod Datacenter with ACI – Private Cloud

FlexPod is a data center architecture built using the following infrastructure components for compute, network and storage:

- Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus and Cisco MDS Switches
- NetApp Storage Systems (FAS, AFF, etc.)

These components are connected and configured according to best practices of both Cisco and NetApp and provide an ideal platform for running a variety of workloads with confidence. The reference architecture covered in this document leverages the components covered in the following reference design:

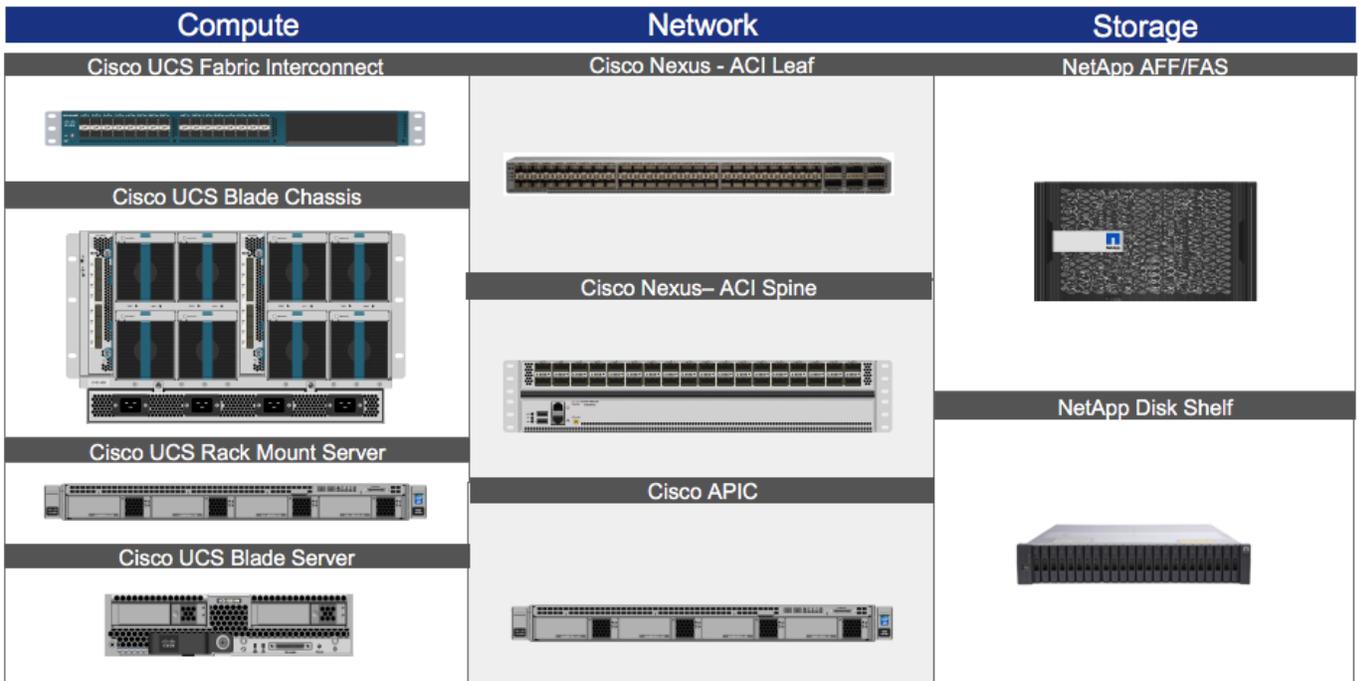
[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/UCS\\_CVDs/flexpod\\_esxi60u1\\_n9k\\_aci\\_design.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi60u1_n9k_aci_design.html)



While the current design guide utilizes FlexPod DC with ACI design referenced in the URL above, customers can choose any supported FlexPod configuration as the private cloud including traditional non-ACI FlexPod designs

---

Figure 1 FlexPod DC with Cisco ACI – Components



One of the key benefits of FlexPod is the ability to maintain consistency at both scale-up and scale-out models. FlexPod can scale-up for greater performance and capacity. In other words, you can add compute, network, or storage resources as needed; or it can also scale-out where you need multiple consistent deployments like rolling out additional FlexPod modules. Each of the component families shown in Figure 1, Cisco Unified Computing System, Cisco Nexus Switches, and NetApp storage arrays offer platform and resource options to scale the infrastructure up or down while supporting the same features and functionality.

For technical and design overview of the compute, network, storage and management components of the FlexPod with ACI solution, see:

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/UCS\\_CVDs/flexpod\\_esxi60u1\\_n9k\\_aci\\_design.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi60u1_n9k_aci_design.html)

## NetApp All Flash FAS and ONTAP 9

NetApp AFF addresses enterprise storage requirements with high performance, superior flexibility, and best-in-class data management. Built on ONTAP software, AFF accelerates business processing without compromising the efficiency, reliability, or flexibility of your IT operations.

NetApp ONTAP 9 is used in the FlexPod DC as well as NetApp Private Storage. With NetApp ONTAP 9, enterprises can quickly integrate the best of traditional and emerging technologies, incorporating flash, the cloud, and software-defined architectures to build a data-fabric foundation across on-premises and cloud resources. ONTAP 9 software is optimized for flash and provides many features to improve performance, storage efficiency, and usability. For more information about ONTAP 9, see the ONTAP 9 documentation center: <http://docs.netapp.com/ontap-9/index.jsp>

Some of the key NetApp ONTAP features utilized in the current FlexPod for Hybrid Cloud design are covered in the sections that follow.

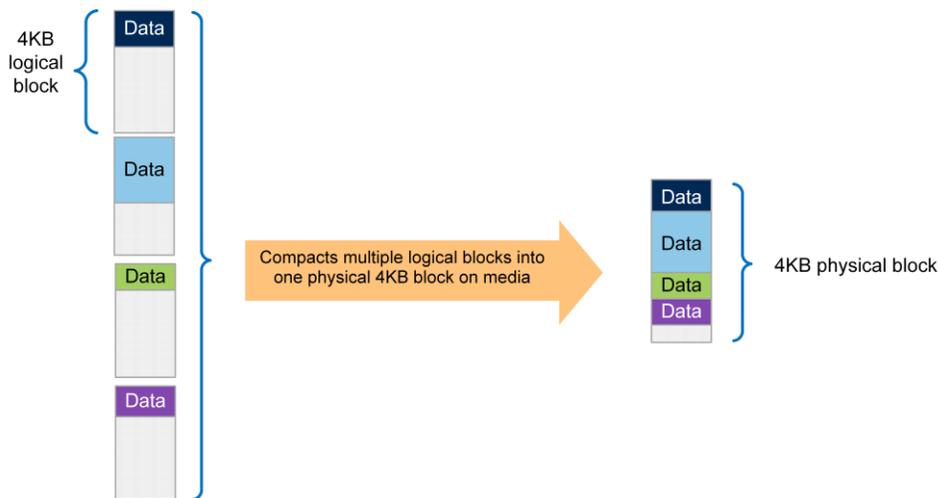
## Storage Efficiency

Storage efficiency has always been a primary architectural design point of ONTAP. A wide array of features allow businesses to store more data using less space. In addition to deduplication and compression, businesses can store their data more efficiently by using features such as unified storage, multi-tenancy, thin provisioning, and NetApp Snapshot™ copies.

Starting with ONTAP 9, NetApp guarantees that the use of NetApp storage efficiency technologies on AFF systems reduce the total logical capacity used to store customer data by 75%, a data reduction ratio of 4:1. This space reduction is a combination of several different technologies, such as deduplication, compression, and compaction, which provide additional reduction to the basic features provided by ONTAP.

Compaction, which is introduced in ONTAP 9, is the latest patented storage efficiency technology released by NetApp. In the ONTAP WAFL file system, all I/O takes up 4KB of space, even if it does not actually require 4KB of data. Compaction combines multiple blocks that are not using their full 4KB of space together into one block. This one block can be more efficiently stored on the disk-to-save space. This process is illustrated in Figure 2.

Figure 2 ONTAP 9 - Compaction



For more information about compaction and the 3-4-5 Flash promotion in ONTAP 9, see:

- <http://www.netapp.com/us/media/tr-4476.pdf>
- <http://www.netapp.com/us/forms/sales-inquiry/flash-3-4-5-promotion.aspx>

## RAID-TEC

With ONTAP 9, NetApp became the first storage vendor to introduce support for 15.3TB SSDs. These large drives dramatically reduce the physical space it takes for rack, power, and cool infrastructure equipment. Unfortunately, as drive sizes increase, so does the time it takes to reconstruct a RAID group after a disk failure. Although the NetApp RAID DP® storage protection technology offers much more protection than RAID 4, it is more vulnerable than usual to additional disk failure during reconstruction of a RAID group with large disks.

To provide additional protection to RAID groups that contain large disk drives, ONTAP 9 introduces RAID with triple erasure encoding (RAID-TEC™). RAID-TEC provides a third parity disk in addition to the two that are present in RAID DP. This third parity disk offers additional redundancy to a RAID group, allowing up to three disks in the RAID group to fail. Because of the third parity drive present in RAID-TEC RAID groups, the size of the RAID group can be increased. Because of this increase in RAID group size, the percentage of a RAID group taken up by parity drives is no different than the percentage for a RAID DP aggregate.

RAID-TEC is available as a RAID type for aggregates made of any disk type or size. It is the default RAID type when creating an aggregate with SATA disks that are 6TB or larger, and it is the mandatory RAID type with SATA disks that are 10TB or larger, except when they are used in root aggregates. Most importantly, because of the WAFL format built into ONTAP, RAID-TEC provides the additional protection of a third parity drive without incurring a significant write penalty over RAID 4 or RAID DP.

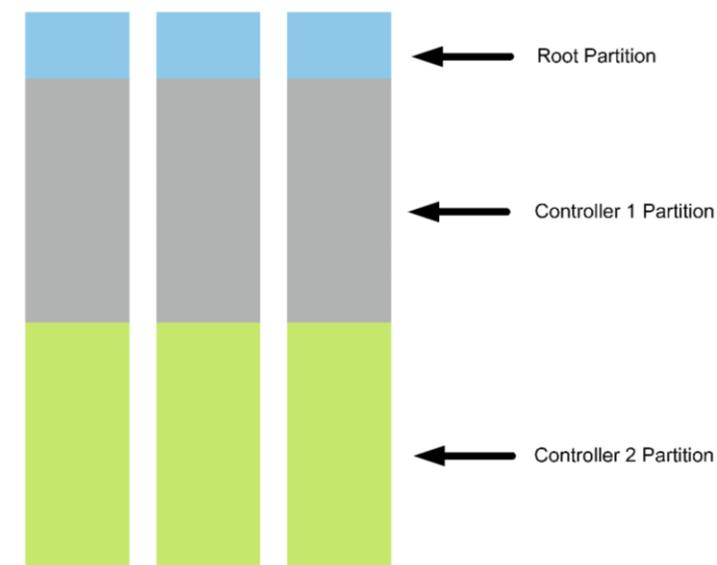
For more information on RAID-TEC, see the Disks and Aggregates Power Guide:

[https://library.netapp.com/ecm/ecm\\_download\\_file/ECMLP2496263](https://library.netapp.com/ecm/ecm_download_file/ECMLP2496263)

## Root-Data-Data Disk Partitioning

Starting with ONTAP 8.3.2, aggregates in entry-level and AFF platform models can be composed of parts of a drive rather than the entire drive. This root-data partitioning conserves space by eliminating the need for three entire disks to be used up in a root aggregate. ONTAP 9 introduces the concept of root-data-data partitioning. Creating two data partitions enables each SSD to be shared between the two nodes in the HA pair.

Figure 3 Root-Data-Data Disk Partitioning



Root-data-data partitioning is usually enabled and configured by the factory. It can also be established by initiating system initialization using option 4 from the boot menu. Note that system initialization erases all data on the disks of the node and resets the node configuration to the factory default settings.

The size of the partitions is set by ONTAP, and depends on the number of disks used to compose the root aggregate when the system is initialized. The more disks used to create the root aggregate, the smaller the root partition. The data partitions are used to create aggregates. The two data partitions created in root-

data-data partitioning are of the same size. After system initialization, the partition sizes are fixed. Adding partitions or disks to the root aggregate after system initialization increases the size of the root aggregate, but does not change the root partition size.

For root-data partitioning and root-data-data partitioning, the partitions are used by RAID in the same manner as physical disks. If a partitioned disk is moved to another node or used in another aggregate, the partitioning persists. You can use the disk only in RAID groups composed of partitioned disks. If you add a non-partitioned drive to a RAID group consisting of partitioned drives, the non-partitioned drive is partitioned to match the partition size of the drives in the RAID group and the rest of the disk is unused.

## SnapMirror

There are several approaches to increasing data availability in the face of hardware, software, or even site failures. Backups provide a way to recover lost data from an archival medium (tape or disk). Redundant hardware technologies also help mitigate the damage caused by hardware issues or failures. Mirroring provides a third mechanism to facilitate data availability and minimize downtime. NetApp SnapMirror® technology offers a fast and flexible enterprise solution for replicating data over local area networks (LANs) and wide area networks (WANs). SnapMirror is a key component in enterprise data protection (DP) strategies.

DP capabilities are integrated within the ONTAP software. NetApp SnapMirror is integrated with NetApp Snapshot technology, which provides a method for quickly and efficiently creating on-disk replicas or point-in-time copies of data that do not require an actual copy operation to create. NetApp integrated data protection can be used to create an on-disk, quickly accessible history of application-consistent Snapshot copies that eliminates the concept of traditional backup windows. NetApp SnapMirror then replicates the history of Snapshot copies to the destination volumes that can be used for backup, DR, or test and development.

SnapMirror replication is efficient because it only replicates the 4KB blocks that have changed or have been added since the previous update. Additional efficiency is gained when SnapMirror is combined with NetApp storage-efficiency technologies. When deduplication is used on the primary storage, only unique data is replicated to the DR site. If compression is enabled on the source, then compression is maintained on the destination. Data is not uncompressed because it is replicated. These technologies can result in telecommunication savings and significant storage capacity savings.

SnapMirror offers various use cases and benefits:

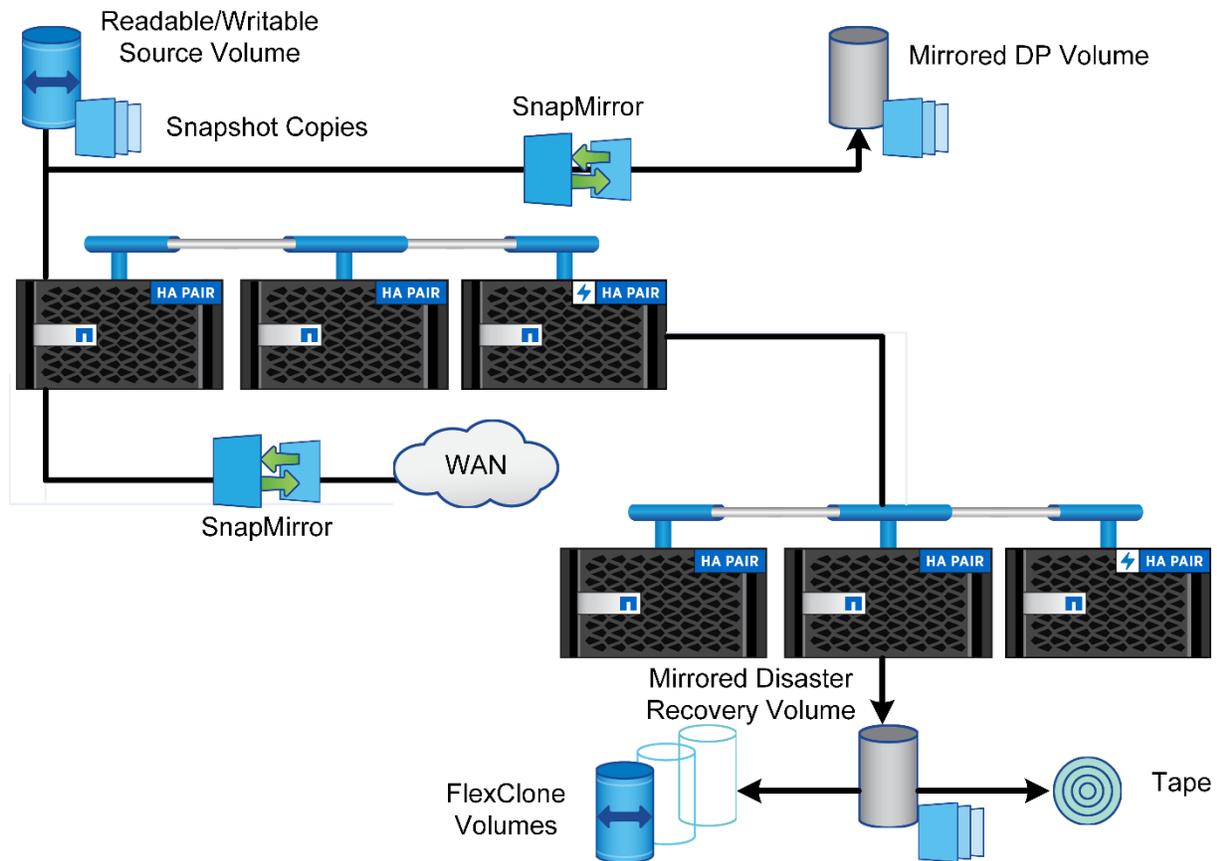
- Integrated data protection
- SnapMirror for disaster recovery
- NetApp FlexClone® technology for disaster recovery testing and application development/test
- Data distribution and remote data access
- Backup offloading and remote tape archiving
- Unified architecture flexibility

See TR-4015 (<https://www.netapp.com/us/media/tr-4015.pdf>) for detailed SnapMirror configuration and best practices.

## FlexClone

FlexClone technology can be used to quickly create a space-efficient read-write copy of a SnapMirror destination FlexVol® volume, eliminating the need for additional copies of the data. For example, a 10GB FlexClone volume does not require another 10GB FlexClone volume; it requires only the metadata needed to define the FlexClone volume. FlexClone volumes only store data that is written or changed after a clone is created. Figure 4 provides an overview of ONTAP replication, and how FlexClone is used to quickly create a cloned volume from the SnapMirror destination for testing in the cloud.

Figure 4 NetApp FlexClone

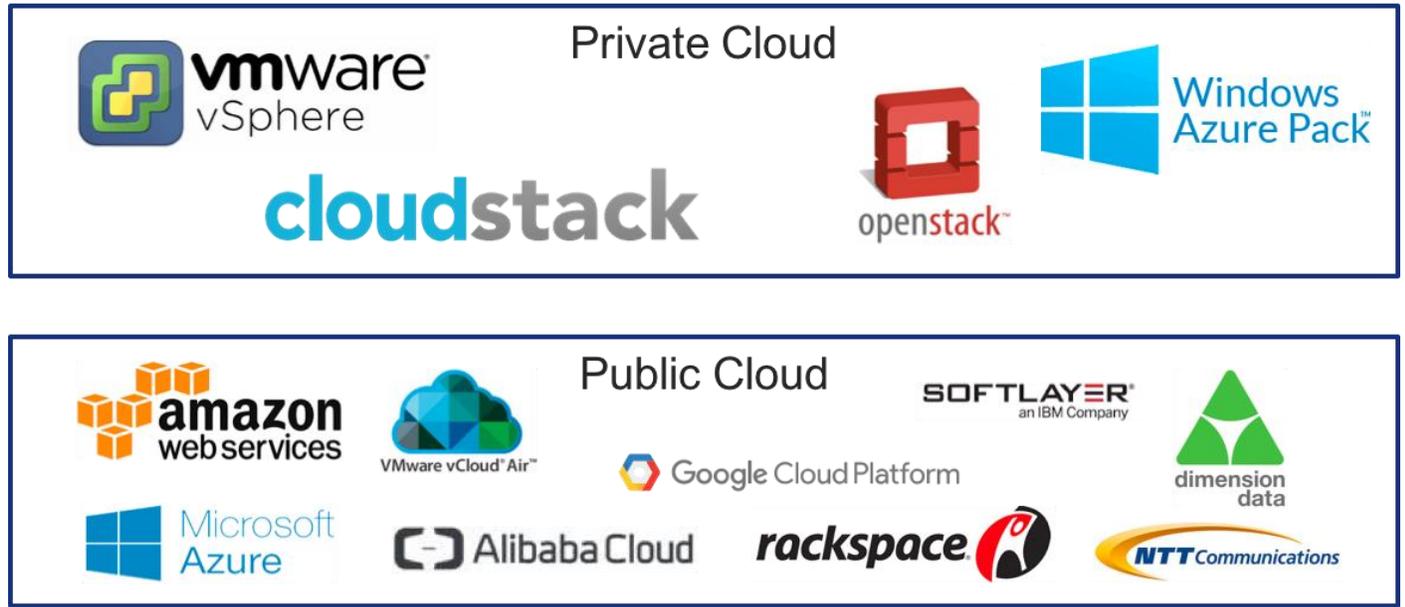


The FlexPod for Hybrid Cloud solution uses NetApp FlexClone technology to create copies of production data for application development and test instances.

## Hybrid Cloud Management System: Cisco CloudCenter

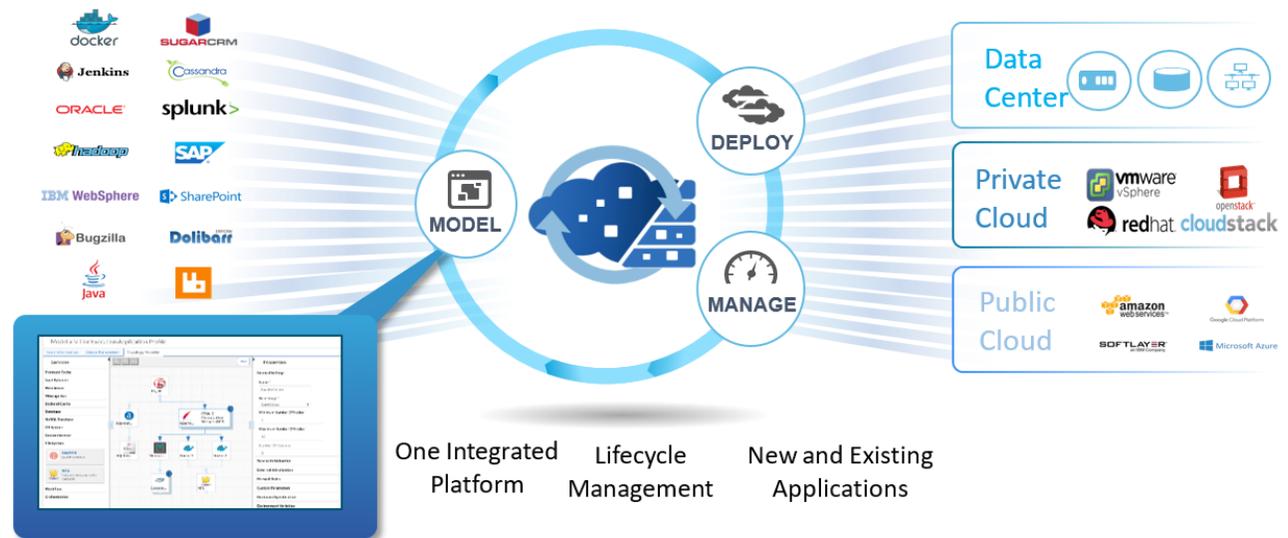
Cisco CloudCenter™ is an application-centric hybrid cloud management platform that securely provisions infrastructure resources and deploys applications across more than 20 data centers, private and public cloud environments. Some of the supported cloud options are highlighted in Figure 5.

Figure 5 Cisco CloudCenter Supported Clouds



Cisco CloudCenter provides a single-platform solution with unique hybrid cloud technology that abstracts the application from the underlying cloud environment and helps ensure that the infrastructure adapts to meet the deployment and management needs of each application. With Cisco CloudCenter, IT organizations can deploy with one application in one cloud or manage multiple applications across multiple environments. It works with a simple virtual machine or with complex, multi-tier application stacks. With an application-centric management platform, enterprise IT organizations can pursue a range of powerful use cases such as on-demand hybrid IT as a service (ITaaS), automated DevOps and continuous delivery, capacity augmentation including bursting, high availability and disaster recovery, and permanent application migration across the clouds.

Figure 6 Cisco CloudCenter; Model, Deploy, and Manage Applications Across the Clouds



Cisco CloudCenter provides organizations with the process and tools to build and manage a cloud-agnostic application profile. One profile can be used in any environment without modifying deployment scripts or

changing application code. The application profile defines the deployment and management requirements for the application in five key areas:

- Application topology and dependencies
- Infrastructure resource and cloud service requirements
- Description of deployment artifacts, consisting of packages, binaries, scripts, and optional data
- Orchestration procedures needed to deploy, configure, and secure
- Run-time policies that guide ongoing management

After applications are deployed, Cisco CloudCenter helps organizations to manage deployments and perform ongoing operations. Users can monitor the applications and use a range of lifecycle management actions, or specify automated responses using preconfigured policies. Unlike many cloud management platforms that are focused on managing infrastructure, Cisco CloudCenter application-centric management integrates the management of the application with management of the underlying cloud resources.

For more information on Cisco CloudCenter, see: <http://www.cisco.com/c/en/us/products/cloud-systems-management/cloudcenter/index.html>

## NetApp Private Storage for Cloud

The NetApp Private Storage (NPS) for Cloud solution enables enterprise customers to leverage the performance, availability, security, and compliance of NetApp storage with the economics, elasticity, and time-to-market benefits **of the public cloud**. **NPS for Cloud is available with a growing number of today's** industry-leading clouds, including two covered in this design:

- NPS for Amazon Web Services (AWS)
- NPS for Microsoft Azure

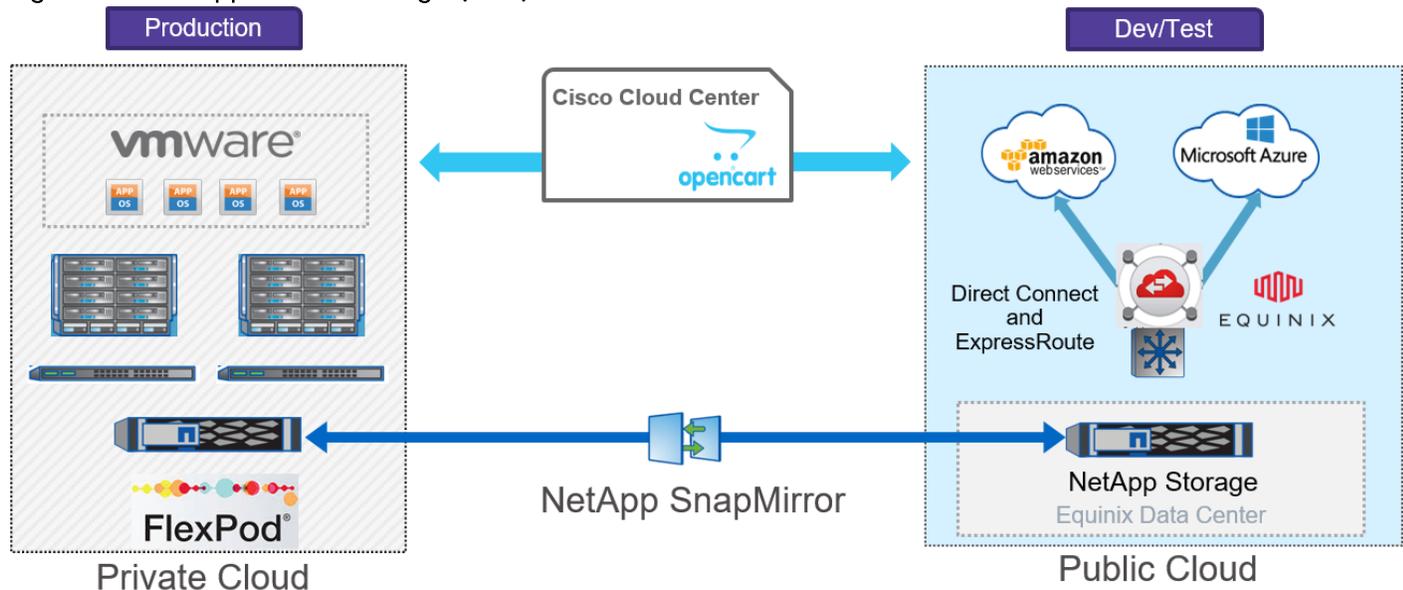
Today, many organizations have top-down mandates to move a percentage of workloads into the cloud. However, cloud customers still have stringent operational and business requirements for their data, such as:

- Performance
- Compliance
- Availability and protection
- Efficient application data replication
- Rapid cloning of application data for development, test, and QA

NetApp storage, that is privately connected to a single public cloud, offers the benefits described in the solution overview; however, additional benefits are accrued when the same storage device and data sets can be quickly connected to multiple clouds without having to provision and de-provision network links, move data, or create additional copies of data for each cloud. When combined with FlexPod Datacenter as an on-premise infrastructure, **customers can position data wherever it's needed, and deploy applications in** the location that makes the most sense for the business. Figure 7 illustrates how application data that is

deployed on premise for production use can be replicated to the NPS system for testing or development using cloud compute resources.

Figure 7 NetApp Private Storage (NPS) Overview



## Equinix Hosting

Equinix Cloud Exchange allows customers to host physical equipment in a location that is logically close to **multiple cloud services providers**. **NetApp's partnership with Equinix and the integration with the Equinix Cloud Exchange** enable dedicated private connectivity to multiple clouds almost instantly and provide the following expanded set of benefits for enterprise users:

- Connect to new clouds quickly and switch clouds at any time. An organization can start with its preferred cloud and add or jump to new clouds in minutes. After an **organization's** NetApp storage is situated next to one cloud (for example, when it is placed in select Equinix data centers), it can establish a dedicated network connection to more clouds in minutes by using the Equinix Cloud Exchange. This will enable customers to connect to multiple cloud providers seamlessly and simultaneously – AWS, Azure, SoftLayer etc.
- Eliminate lock-in and costly data migrations. The major cloud service vendors continually innovate price and feature sets. Organizations that want to switch cloud vendors for any reason can do so without having to deal with the time-consuming, costly obstacles of traditional data migration. They can turn off connectivity to the first cloud and spin up connectivity to the second cloud in minutes, and they can do so without having to move data.
- Diversify risk. Customers can now easily run applications in more than one cloud to diversify risk. For example, if the first cloud does not respond or is slow because of a performance problem, an application can instead be run instantly and securely through the alternate second cloud.
- Enable an organization to expand its cloud choices. By keeping its data close to multiple clouds, **an organization is free to connect to an expanding portfolio of selected clouds**. **NetApp's enlarged**

network of cloud service provider partners, including industry leaders, offer NPS for Cloud customers even more options moving forward.

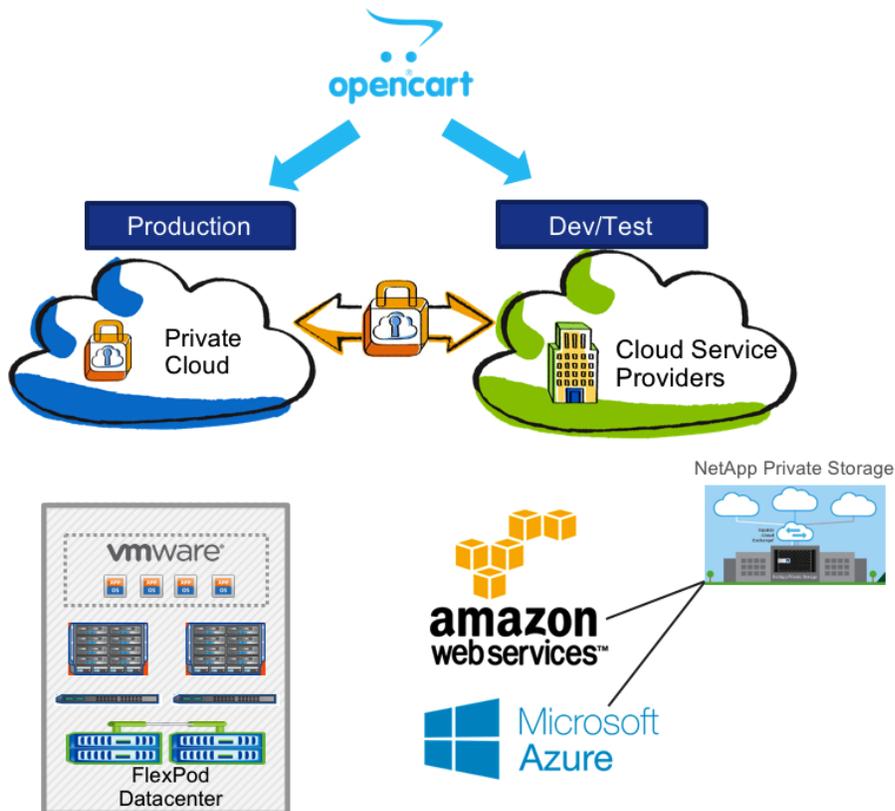
- Maximize an organization’s cloud buying power and flexibility.** Using NPS for Cloud with multiple clouds gives organizations more control and potentially even more bargaining power to get the cloud services and capabilities they need under favorable terms.

## Public Cloud

IT organizations moving toward a hybrid IT strategy need flexibility in how and where the applications are deployed. A vast majority of ITaaS users already leverage more than one cloud service provider today. Both Cisco CloudCenter and NetApp Private Storage for cloud builds on this trend and offer IT users extreme flexibility to benefit from a multi-cloud strategy in the enterprise. CloudCenter supports multitudes of combinations of private and public cloud resources by keeping applications consistent regardless of the placement. NetApp Private Storage integration with Equinix Cloud Exchange also enables dedicated, on-demand private connectivity to multiple clouds.

This design guide covers two of **today’s** leading public cloud providers, Amazon Web Services (AWS) and Microsoft Azure. The document guides users through setting up a true multi-cloud development and test environment for an open source e-commerce application, OpenCart. In this solution, an end user can instantiate and deploy an application easily in any of the available clouds (public or private) while maintaining the control of the critical customer data using FlexPod or the NetApp Private Storage.

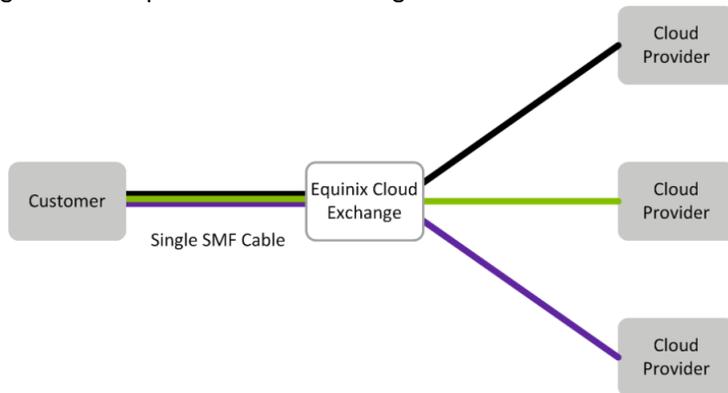
Figure 8 Multi-Cloud Solution Design



## Equinix Cloud Exchange

The Equinix Cloud Exchange is an Amazon Virtual Private Cloud Direct Connect and an Azure ExpressRoute Exchange and provider. Figure 9 shows how the Equinix Cloud Exchange allows customers to rapidly connect to multiple network and cloud service providers over an optical cable. The Cloud Exchange portal is utilized by customers to request connectivity to Microsoft Azure through Azure ExpressRoute and AWS through Direct Connect.

Figure 9 Equinix Cloud Exchange



Border Gateway Protocol (BGP) is used to support network routing between the cloud virtual networks and the customer network in the Equinix co-location facility. The customer network in the Equinix co-location data center is directly connected to the customer-provided Layer-3 network equipment. The BGP configuration advertises local network routes to the cloud virtual networks and receives the BGP advertisements from the cloud virtual networks over the Equinix Cloud Exchange network connection. Specific details on AWS and Microsoft Azure network topologies can be found in the sections that follow.

## Solution Design

---

The FlexPod DC for the Hybrid Cloud solution targets deploying e-commerce application in the Hybrid Cloud to provide an application development and test environment. The solution has been verified in a multi-cloud environment. The two public clouds utilized for this validation are:

- Amazon Web Services (AWS)
- Microsoft Azure Resource Manager (MS Azure RM\*)



**\* To simplify the deployment and management of resources, Microsoft recommends that Azure Resource Manager should be used for new cloud based deployments.**

---

The NetApp Private Storage, used for solution validation, is hosted in Equinix DC on the west coast. A high speed, low latency, link from Equinix datacenter is established to both AWS and MS Azure public clouds. Cloud zones on the US west coast (for example, AWS West) are selected for validating the solution to keep compute geographically close to the NetApp Private Storage (NPS) and therefore maintain low network latency. The solution:

- Allows the end user to instantiate and deploy an application easily in any available cloud including the private cloud
- Allows customers to maintain the control of the critical data while utilizing resources in public cloud by keeping the critical user data on the FlexPod storage or the NPS
- Makes data available consistently across all the clouds and keep the data in-sync across various deployments
- Allows customer to deploy a distributed application such that applications tiers utilize different clouds (e.g. web servers in public cloud and DB servers in private cloud)
- Allows automated data replication and availability for new instances of the application

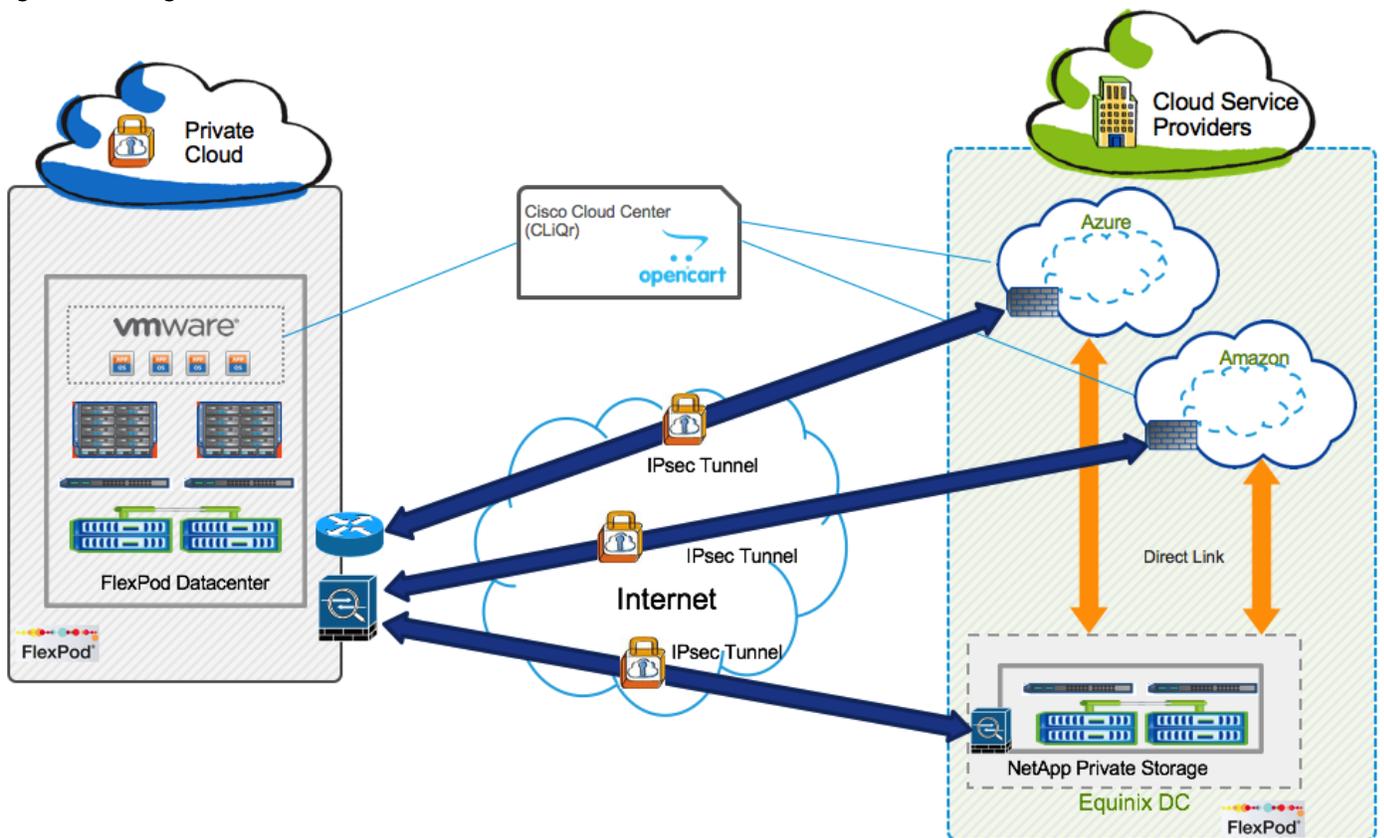
Various components used in developing the hybrid cloud solution extend great flexibility to the customers for defining a solution suitable for their individual organizational needs. The design highlighted in this document satisfies the customer requirements listed below. However, it must be noted that the design can be easily modified to support additional customer requirements.

- Primary workload for FlexPod has been pre-provisioned within the FlexPod DC, for example, the production version of the application is already up and running within the FlexPod DC and contains the production data which needs to be made available to development or test instances of the applications
- Application blueprint in Cisco CloudCenter, combined with callout scripts, is used to configure the storage system when deploying applications at any cloud location
- Development and Test instances of the application are deployed at any available public or the private cloud. Since this solution supports a multi-cloud environment, customers can enforce the deployment environment selection based on policy tags

- NetApp SnapMirror functionality is used to sync the production user data to NetApp Private Storage and make up-to-date customer data available to the new application instances across the clouds
- NPS combined with dedicated direct links to both AWS and Azure makes secure data accessible to the application instances in both public cloud
- Removing the development and test application instances also destroys the volumes and mount points associated with the deployed instance for additional security
- Data repatriation; allows customers, who have deployed production apps in the public cloud, to move the application and the user data back to on-premise FlexPod to meet any SLA requirements or other corporate control directives

Figure 10 shows high-level solution architecture utilized to deliver the solution functionality outlined above.

Figure 10 High-Level Solution Architecture



The following design subsections discuss the design requirements and components (Figure 10) in greater detail.

## FlexPod Datacenter with ACI – Private Cloud

FlexPod DC with Cisco ACI, used as the private cloud, aligns with the converged infrastructure configurations and best practices. The system includes hardware and software compatibility support between all components and aligns to the configuration best practices for each of these components. All the

core hardware components and software releases are listed and supported on both the Cisco compatibility list:

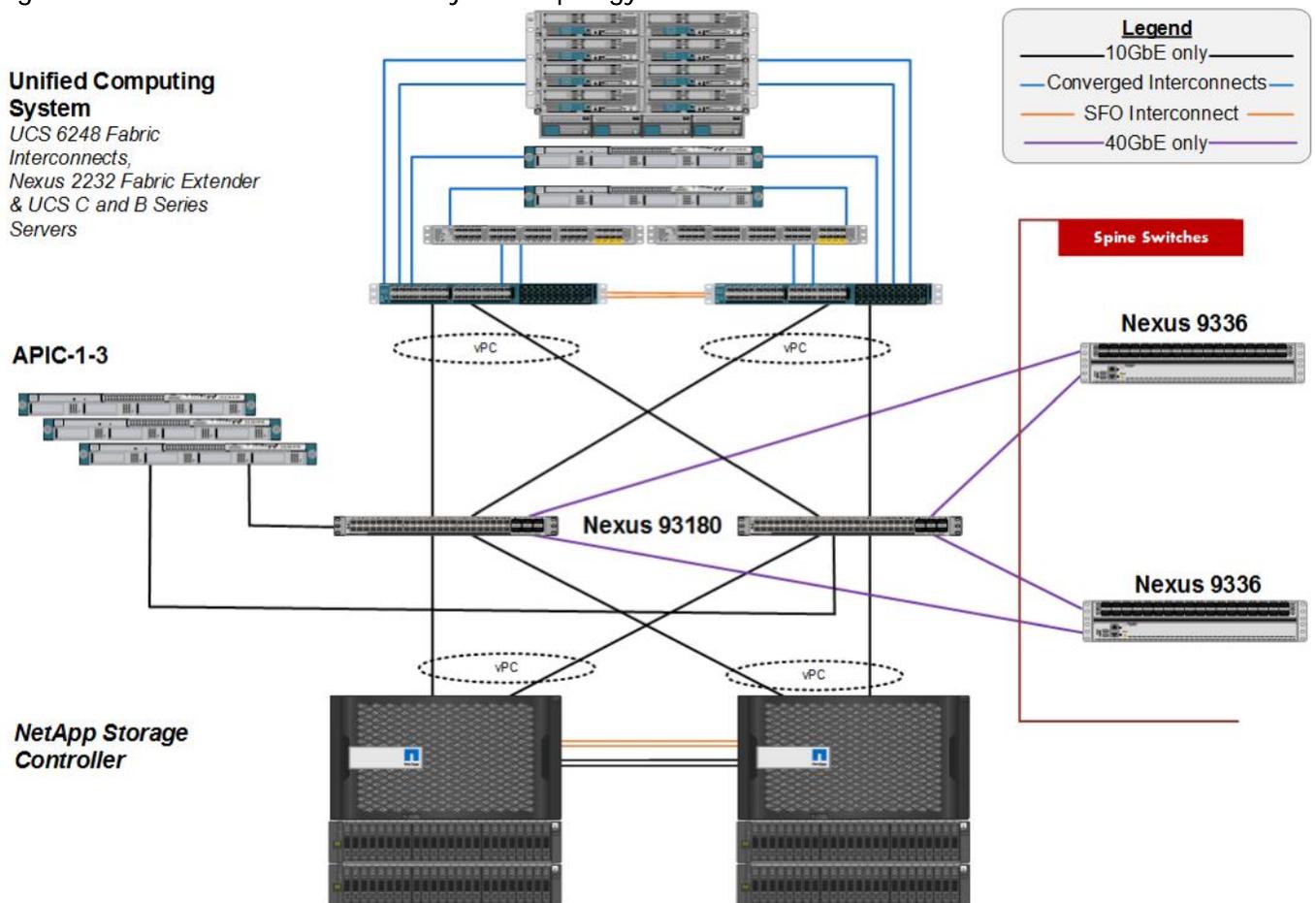
<http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>

and NetApp Interoperability Matrix Tool:

<http://mysupport.netapp.com/matrix/>

The system supports high availability at network, compute and storage layers such that no single point of failure exists in the design. The system utilizes 10 and 40Gbps Ethernet jumbo-frame based connectivity combined with port aggregation technologies such as virtual port-channels (VPC) for non-blocking LAN traffic forwarding. Figure 11 shows the physical connectivity of various components of the FlexPod DC design.

Figure 11 FlexPod DC with ACI – Physical Topology



Some of the key features of the private cloud solution are highlighted below:

- The system is able to tolerate the failure of compute, network or storage components without significant loss of functionality or connectivity
- The system is built with a modular approach thereby allowing customers to easily add more network (LAN or SAN) bandwidth, compute power or storage capacity as needed

- The system supports stateless compute design thereby reducing time and effort required to replace or add new compute nodes
- The system provides network automation and orchestration capabilities to the network administrators using Cisco APIC GUI, CLI and restful API
- The systems allow the compute administrators to instantiate and control application Virtual Machines (VMs) from VMware vCenter
- The system provides storage administrators a single point of control to easily provision and manage the storage using NetApp System Manager
- The solution supports live VM migration between various compute nodes and protects the VM by utilizing VMware HA and DRS functionality
- The system can be easily integrated with optional Cisco (and third party) orchestration and management application such as Cisco UCS Central and Cisco UCS Director
- The system showcases layer-3 connectivity to the existing enterprise network

For an in-depth discussion of the FlexPod DC with ACI design components, refer to the following design guide:

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/UCS\\_CVDs/flexpod\\_esxi60u1\\_n9k\\_aci\\_design.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi60u1_n9k_aci_design.html)

## Cisco CloudCenter – Setting up the Hybrid Cloud Management

Cisco CloudCenter provides organizations with the process and tools to build and manage a cloud-agnostic application profile. An application profile can be used in any environment without modifying deployment scripts or changing application code. Cisco CloudCenter comprises of various components as outlined in the CloudCenter documentation: <http://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/cloud-management/cloudcenter/v47/installation-guide/cloudcenter47-installationguide.pdf>

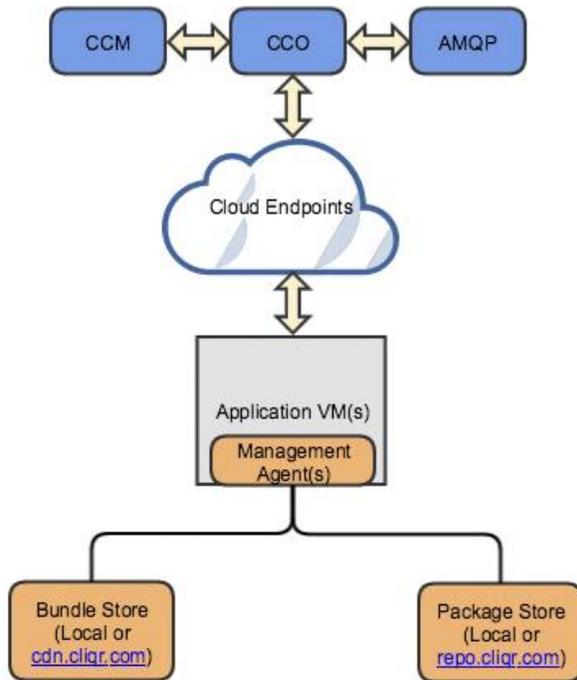
However, not all the CloudCenter components need to be deployed under all the circumstances. The components utilized in the FlexPod DC for Hybrid Cloud are shown in 0.



This design guide does not cover installation procedures and design for CloudCenter HA. Customers and partners are encouraged to engage Cisco CloudCenter Technical Marketing or Cisco Advanced Services teams to design a robust CloudCenter deployment

---

Figure 12 FlexPod DC for Hybrid Cloud – Cisco CloudCenter Components



## CloudCenter Manager (CCM)

The CloudCenter Manager (CCM) is a centralized management tier that acts as a dashboard for users to model, migrate, and manage deployments. It provides for the unified administration and governance of clouds and users. The CCM interacts directly with each CloudCenter Orchestrator (CCO) based on the deployment's application profile(s). Users can access the CloudCenter features by either through the CCM UI or REST APIs.

In this design, a single CCM instance is deployed on the FlexPod private cloud using the CCM VMware appliance downloaded from [cisco.com](http://cisco.com).

## CloudCenter Orchestrator

CloudCenter Orchestrator (CCO) is deployed in every supported cloud region. The CCO is a backend server that interacts with cloud endpoints to handle application deployment and runtime management. CCO decouples an application from its underlying cloud infrastructure in order to reduce the cloud deployment complexity. A single CCO can manage up to 10,000 Virtual Machines (VMs) in a cloud region.

In this design, a CCO server is required for each cloud, including private cloud.

## AMQP and Guacamole

The CloudCenter platform features Advanced Message Queuing Protocol (AMQP) based communication between the CCO and the Agent VM. The CloudCenter platform incorporates RabbitMQ as the open source message broker for AMQP implementation. If the application VM (worker) runs in isolated networks (like

Amazon's VPC or Firewall protected private cloud), ensure that the application VM has outbound connectivity to the AMQP server. The Guacamole component is embedded, by default, in the AMQP server. Guacamole server is used to enable web based SSH/VNC/RDP to application VMs launched during the application lifecycle process.

In this design, an AMQP/Guacamole server is deployed for each cloud, including private cloud.

## Bundle Store

The bundle store hosts agent bundles and service bundles and is used by the application VMs to bootstrap, install, and start the agent on the application VM (worker). A bundle store can also be installed locally for a CloudCenter deployment. In the current FlexPod DC for Hybrid Cloud design, an Internet connection is required so that the application VM can reach the default bundle store on CDN (cdn.cliqr.com).

## Package Store

The package store is a repository that contains binaries for all third-party application services (out-of-box services) as well as binaries for several components required for the CloudCenter installation itself. The default package store is hosted at [repo.cliqrtech.com](http://repo.cliqrtech.com) and the current design requires CloudCenter components and VMs Internet access to use the default package store. Customers can also choose to install a local package store and register it with the CCO.

## Management Agent and Base OS Images

CloudCenter installations require installation of a management agent in the application VMs. Cisco provides Base OS images with the management agent already installed for a number of operating systems and on a number of Public and Private clouds. A complete list of the supported Base OS Images can be found at:

<http://docs.cloudcenter.cisco.com/display/CCD46/Base+OS+Images>

For some clouds (e.g. Azure Resource Manager cloud) where a Base OS image is not provided, the CloudCenter management agent can be dynamically installed on the VMs at the launch time. The list of clouds and images supporting dynamic bootstrapping can be found at:

<http://docs.cloudcenter.cisco.com/display/CCD46/Dynamic+Bootstrapping+Support>



Customer can choose to create their own private images for various clouds to customize the Base OS Image.

## Component Deployment

Cisco CloudCenter components have specific deployment requirements and installation procedures. Cisco provides both an appliance based deployment for certain clouds (e.g. VMware and AWS) and manual installation for most other clouds (for example, MS Azure RM). A customer typically requires one CCM deployed in-house (FlexPod environment in this case) to manage various clouds. Components such as CCO and AMQP servers are deployed for every available cloud (or cloud zone) and are registered with the CCM. Table 1 shows the deployment location and VM requirements for various CloudCenter components used in the FlexPod DC for Hybrid Cloud design.

**Table 1** Component Requirements

Component	Per Cloud Region	Deployment Mode	VM Requirement	Deployment Location
-----------	------------------	-----------------	----------------	---------------------

Component	Per Cloud Region	Deployment Mode	VM Requirement	Deployment Location
CCM	No	Appliance for VMware	2 CPU, 4GB memory, 50GB storage*	FlexPod
CCO	Yes	Appliance for VMware and AWS  Manual installation for Azure RM	2 CPU, 4GB memory, 50GB storage*	FlexPod, AWS, Azure RM
AMQP/Guacamole	Yes	Appliance for VMware and AWS  Manual installation for Azure RM	2 CPU, 4GB memory, 50GB storage*	FlexPod, AWS, Azure RM
Base OS Image	Yes	Customized Image created in each cloud	CentOS 6; Smallest CPU and Memory instances selected for solution validation	FlexPod, AWS, Azure RM

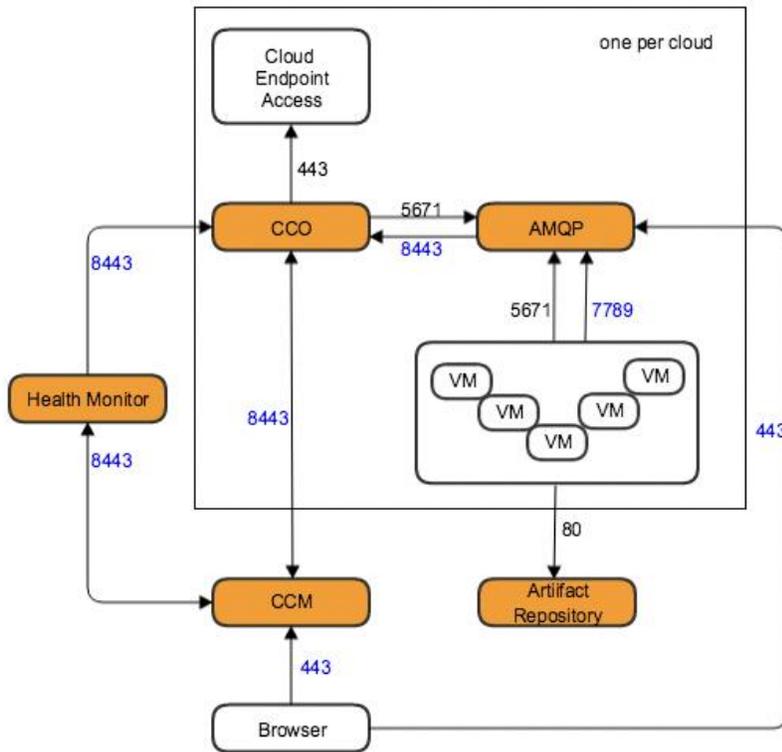
\* VMware appliances auto-select the VM size. The VM size provided above is based on support for less than 500 application VMs. For complete sizing details, see:

<http://docs.cloudcenter.cisco.com/display/CCD46/Phase+1%3A+Prepare+Infrastructure>

### Network Rule Configuration

0 shows various TCP ports that need to be enabled between various CloudCenter components and between the application VMs for the CloudCenter to work correctly. When deploying CCO and AMQP in AWS and Azure, these ports must be enabled on the VM security groups. Similarly, if various CloudCenter components are separated by a firewall in the private cloud, the TCP ports should be allowed in the firewall rules.

Figure 13 Network Port Requirements



The list of required network rules for various components can be found here:

<http://docs.cloudcenter.cisco.com/display/CCD46/Phase+2%3A+Configure+Network+Rules>

## Private Cloud Configuration

As shown in Table 1, in the FlexPod DC for Hybrid Cloud design, CCM, CCO and AMQP servers are deployed in the FlexPod based private cloud. These three appliances are downloaded from cisco.com and deployed in the management cluster within the FlexPod environment. For deployment details for these components, see: <http://docs.cloudcenter.cisco.com/display/CCD46/VMware+Appliance+Setup>.

These components need to be added to DNS and should be setup with Internet access to be able to reach the CloudCenter repositories for upgrade and maintenance. CCM, in particular, needs to be able to reach CCOs running in public clouds and be able to communicate on port 443 and port 8443. Additionally, the application VMs also need access to the CloudCenter components using both IP and DNS information.

## ACI Setup

For setting up the private cloud as a deployment environment, a dedicated ACI tenant named App-A is created to host all the application instances. The application tenant creation is covered in detail in the FlexPod with ACI Design Guide:

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/UCS\\_CVDs/flexpod\\_esxi60u1\\_n9k\\_aci\\_design.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi60u1_n9k_aci_design.html)

To successfully deploy an application, the following requirements need to be met:

1. An application profile and EPGs need to be pre-provisioned

2. A DHCP server needs to be setup to assign IP addresses to the VMs
3. The DNS server should be able to resolve the IP addresses for the CloudCenter components
4. An L3-Out or Shared L3-Out needs to be setup and VMs should be able to access Internet

### vCenter Setup

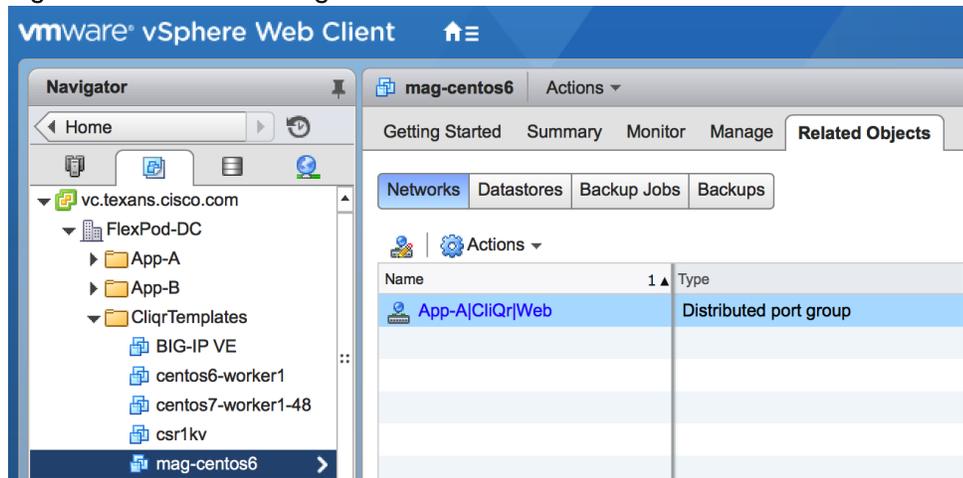
To add VMware vCenter as a deployment environment, a VMware datacenter and cluster needs to be identified. Figure 14 shows the datacenter and cluster information defined in VMware vCenter.

While not required, setting up a VMware folder for application VM deployment is also recommended for ease of grouping application VMs together. For detailed information about setting up the VMware based cloud, see: <http://docs.cloudcenter.cisco.com/pages/viewpage.action?pagelid=5540210>.

### Base OS Image

In a VMware environment, the base OS image is a VM Snapshot. The VM is added to a folder called CliqrTemplates and is referenced using its snapshot name. For the OpenCart application deployment, the base image in use is the CentOS6 image. A VM called mag-centos6 is copied to CliqrTemplates folder and a snapshot named Snap1 is created:

Figure 14 Base OS Image



As shown in Figure 14, the VM NIC is assigned to the distributed port-group created by APIC. 0 shows the VM template to Base OS image mapping in the CloudCenter:

Figure 15 CloudCenter - VMware Image Mapping

## Edit Cloud Mapping

Image Name

CentOS 6.x

Cloud

FlexPod-Private

Cloud Image ID \*

mag-centos6/Snap1

Every cloud stores this information in different places. Please login to your cloud provider to find your Image ID.

## Amazon Web Services (AWS)

Integrating AWS with the FlexPod DC for Hybrid Cloud solution is a three-step process:

1. Integrate AWS with Cisco CloudCenter
2. Setup secure connectivity between FlexPod private cloud and AWS
3. Configure AWS Direct Connect with NPS

### Integration with Cisco CloudCenter

To successfully integrate an AWS account with Cisco CloudCenter and to be able to deploy applications in AWS, CCO and AMQP need to be deployed in the customer AWS account. Cisco provides both CCO and AMQP appliances for AWS deployments which need to be enabled for the customer AWS account.

See <http://docs.cloudcenter.cisco.com/display/CCD46/Amazon+Appliance+Setup> for details on requesting CloudCenter image sharing. The URL above also guides customers on how to deploy the CCO and AMQP appliances.

AWS to CloudCenter integration can be easily accomplished using the default customer Virtual Private Cloud (VPC) and therefore the FlexPod DC for Hybrid Cloud utilizes default VPC for CCO, AMQP and application VM deployments.

After CCO and AMQP are successfully deployed and configured according to the URL above, an AWS cloud can be added to CCM as detailed in:

<http://docs.cloudcenter.cisco.com/pages/viewpage.action?pageId=5540210>

When an AWS cloud is setup, all the available AWS instance types become available in the CloudCenter. Customers can choose to limit the instance type to one or many instances depending on the organizational preferences.

Figure 16 CloudCenter - AWS Instance Types

Instance Type CLEAR ALL SETTINGS

Select which instance type(s) you would like to make available for your end-users

All Instance Types **Multiple Instance Types** Single Instance Type

Filter Instance Types / Show

AVAILABLE INSTANCE TYPES (58) / 4 SELECTED

Instance Type	Virtual CPU	Memory	Storage	Hourly Price	Monthly Price (approx)
T2.MICRO	1	1 GB	0 GB	\$ 0.017 /hour	approx 12.41/month
ELASTIC LOAD BALANCER	0	0.000 GB	0 GB	\$ 0.025 /hour	approx 18.25/month
T1.MICRO	1	0.599 GB	0 GB	\$ 0.025 /hour	approx 18.25/month

HARDWARE INFO

PRICING INFO

Cisco CloudCenter also allows customers to select VPC and subnet information for the deployment. CloudCenter allows customers to upload their own public key to be assigned to the AWS deployed VMs. This setting can be accessed during the cloud setup procedure. **For this design, “Persist Private Key” option** was selected to enable a Cloud VM (Web VM) to SSH to another VM (DB VM) for storage configurations.

Figure 17 CloudCenter - AWS Settings

The screenshot displays the 'Cloud Settings' configuration page in CloudCenter. At the top left, there are icons for visibility (an eye) and a lock. The main title is 'Cloud Settings'. Below this, the 'INSTANCE PROFILE ARN' field is populated with a masked AWS ARN. The '\* VPC' dropdown menu is set to 'vpc-e1c91e84 | CIDR 172.31.0.0/16'. The 'ASSIGN PUBLIC IP' toggle is turned 'ON'. Under 'NIC 1', the '\* NETWORK' dropdown is set to 'subnet-... us-west-1a | CIDR 172.31.0.0/20'. The '\* PRIVATE IP ALLOCATION' dropdown is set to 'DHCP'. A blue plus icon and the text 'NETWORK INTERFACE CONTROLLER' are visible below. The 'ENABLE RESOURCE VALIDATION' toggle is set to 'NO'. At the bottom, the 'SSH Options' section shows three buttons: 'No Preference', 'Assign Public Key', and 'Persist Private Key' (which is highlighted in blue). Below these buttons is the text: 'Select to persist the private key in the instance SSH configuration'.

### Base OS Image

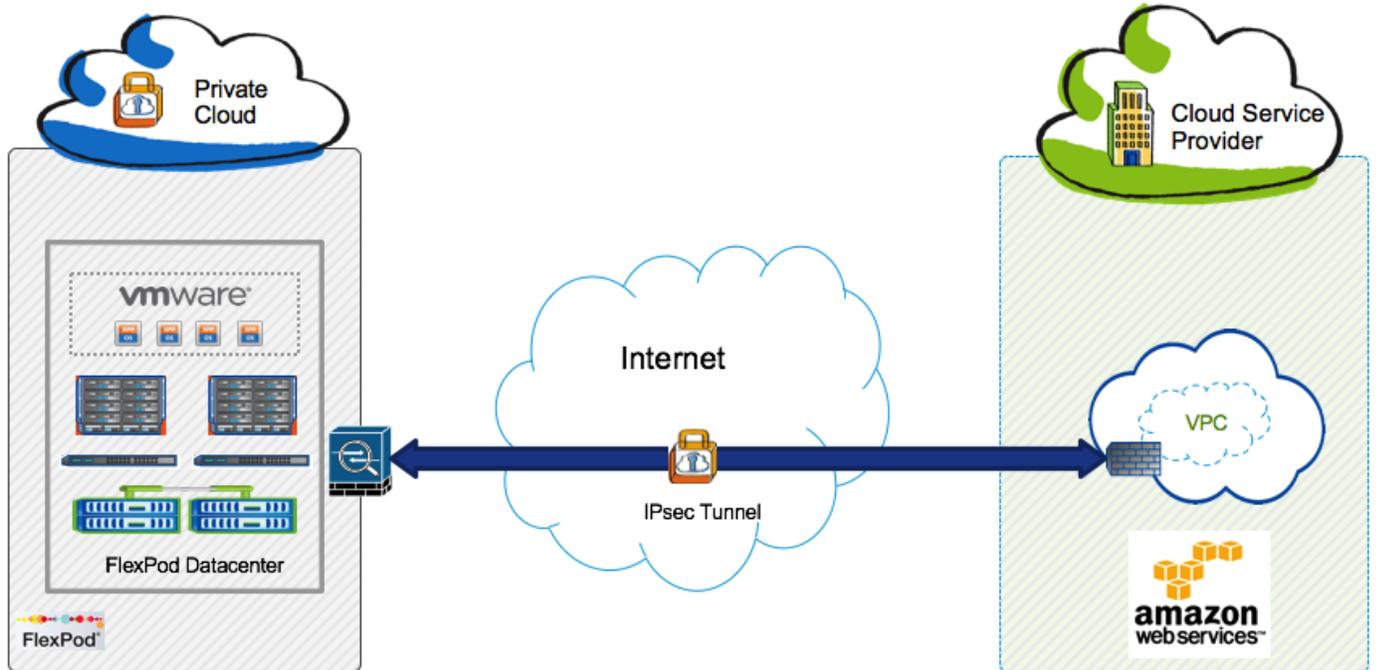
During AWS environment setup, various base OS images are automatically mapped to appropriate AMIs. For the OpenCart application deployment, the CentOS6 base image is used. A custom AMI is created and mapped for application usage.

### FlexPod to AWS VPN Connectivity

The FlexPod based private cloud is connected to the Internet using Cisco ASA firewalls. The ASA firewalls allow customers to establish site-to-site VPN connections for secure connectivity between the private cloud and the public cloud(s). This secure site to site VPN tunnel allows application VMs at the customer location (private cloud) to securely communicate with the VMs hosted in AWS. If an organization needs to deploy

distributed applications where one tier of the application (e.g. DB servers) is hosted in the private cloud while another tier (e.g. web servers) is deployed in the public cloud, the VPN connection provides required secure connection.

Figure 18 FlexPod to AWS VPN Connectivity



The IPsec tunnel parameters utilized in the current design are listed in Table 2

**Table 2** IPsec Tunnel Details for AWS

Parameter	Value
IKE (Phase 1)	
Authentication	Pre-Shared
Encryption	AES 128
Hash	SHA
DH Group	2
Lifetime	28800 seconds
IPsec (Phase 2)	
Network	Source and Destination depend on deployment
PFS	On
Peers	Provided by AWS
Transform Set	AES-128, SHA-HMAC

Parameter	Value
IPsec SA Lifetime	3600 seconds



An IPsec tunnel to AWS can only be established by initiating data traffic from the private cloud. Customers need to ensure there is a continuous data exchange between the FlexPod and AWS clouds to keep the tunnel up at all times.

### AWS Direct Connect Connectivity

AWS Direct Connect is used to establish a dedicated network connection between the customer-provided network switch or router in the AWS Direct Connect data center (Equinix) and the Amazon VPC. The AWS direct connect setup is covered in detail in section [NPS for AWS](#).

### Microsoft Azure Resource Manager (MS Azure RM)

Integrating MS Azure RM with the FlexPod DC for Hybrid Cloud solution is a three-step process:

1. Integrate Azure RM with Cisco CloudCenter
2. Setup secure connectivity between FlexPod private cloud and Azure RM
3. Configure Azure ExpressRoute service with NPS

### Integration with Cisco CloudCenter

To successfully integrate an Azure RM account with Cisco CloudCenter and to be able to deploy applications in Azure, CCO and AMQP need to be deployed in the customer Azure RM account. Cisco does not provide the CCO and AMQP appliances for Azure deployments which means customers need to proceed with a manual installation procedure to deploy these two components. For details about the manual installation procedures for the various clouds, see

<http://docs.cloudcenter.cisco.com/display/CCD46/Installation+Approach>.

After CCO and AMQP are successfully deployed and configured according to the URL above, an Azure RM cloud can be added to CCM as shown here:

<http://docs.cloudcenter.cisco.com/pages/viewpage.action?pagelid=5540210>. Before adding Azure Cloud to CCM, define a resource group in the appropriate zone of Azure RM.

Similar to AWS setup, when Azure RM Cloud is added to CloudCenter, all the available instance types become available and customers can make one or more instance types available to end users for application deployments. Mapping the cloud settings are also similar to AWS but require additional fields such as Resource Group, Storage Account and Diagnostics information.



If an organization requires VPN connectivity between private cloud and MS Azure RM, a Virtual network should be defined with a large enough subnet so that adequate IP address sub-ranges are available for VPN connectivity as well as VM deployments.

### FlexPod to Azure RM VPN Connectivity

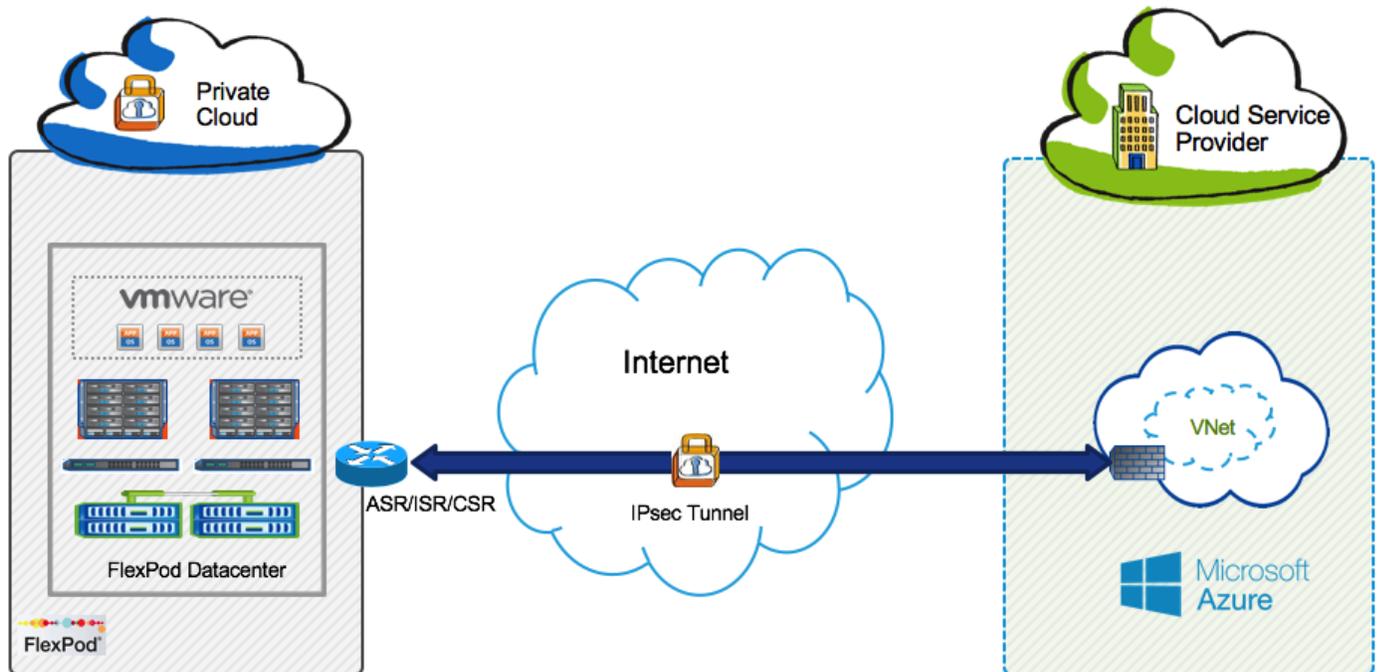
A secure site to site VPN tunnel allows application VMs at the customer location (private cloud) to securely communicate with the VMs hosted in Azure RM. According to Microsoft documentation: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>, route-based VPN connection needs to be configured when using both Express Route and VPN GW at the same time. Since VPN connectivity to MS Azure is configured along with Express Route configuration in this scenario, a Cisco CSR is deployed to setup the VPN connectivity.

---

 <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices> provides a list of validated VPN devices on the customer premise and the appropriate configuration.

---

Figure 19 FlexPod to MS Azure RM VPN Connectivity



The IPsec tunnel parameters utilized in the current design are listed in Table 3

**Table 3** IPsec Tunnel Details for MS Azure RM

Parameter	Value
IKEv2 (Phase 1)	
Authentication	Pre-Shared
Encryption	AES 256
Hash	SHA
DH Group	2
Lifetime	86400 seconds
IPsec (Phase 2)	

Parameter	Value
Network	0.0.0.0/0 to 0.0.0.0/0 (Interface Tunnel)
PFS	Off
Peer(s)	Provided by Azure
Transform Set	AES-256, SHA-HMAC
IPsec SA Lifetime	3600 seconds

### Azure ExpressRoute Connectivity

Azure ExpressRoute is used to establish a dedicated network connection between the customer-provided network switch or router in the Azure Direct Connect data center (Equinix) and the Azure Vnet. The Azure ExpressRoute setup is covered in detail in section [NPS for Azure](#).

### NetApp Private Storage

The NetApp Private Storage (NPS) architecture is flexible and can accommodate various customer requirements and application workloads. NPS supports all supported cluster configurations and variety of controller and/or disk configurations can be implemented to meet specific customer requirements. NPS for Hybrid Cloud solution is comprised of the following major components:

- Virtual machines (VMs) running in the Public Cloud
- Layer 3 network connection between NetApp storage and the public cloud
- Colocation facility located near the public cloud (Equinix)
- Colocation cloud exchange/peering switch
- Customer-owned network equipment that supports BGP routing protocols and 1 Gigabit Ethernet (GbE) or 10GbE connectivity
- NetApp storage: AFF, FAS, E-Series, or SolidFire®

The components of the solution are connected and configured to provide a scalable architecture that supports a variety of application workloads.

For the FlexPod DC for Hybrid Cloud solution validation, NetApp FAS was utilized in the Equinix colocation. The system was configured as per NetApp storage system best practices, including a separate aggregate for each controller. Separate volumes are created to host SnapMirror source and destination data, and on-demand volume clones are created by Cisco CloudCenter during application deployment operations.

Network configuration of the storage system also follows NetApp best practices where two 10Gbps Ethernet connections from each controller terminate at a pair of Cisco Nexus 5000 switches using LACP link aggregation. Separate VLANs are created on the interface groups to provide connectivity from the storage system to AWS and Azure Virtual Network.

## NPS to FlexPod Private Cloud VPN connectivity

Cisco ASA provides VPN capabilities to NPS so that VPN connectivity can be established between the storage controllers in NPS and the storage controllers in FlexPod for SnapMirror operations. The VPN link can also be utilized for managing the storage controllers or specific Storage Virtual Machines (SVM).

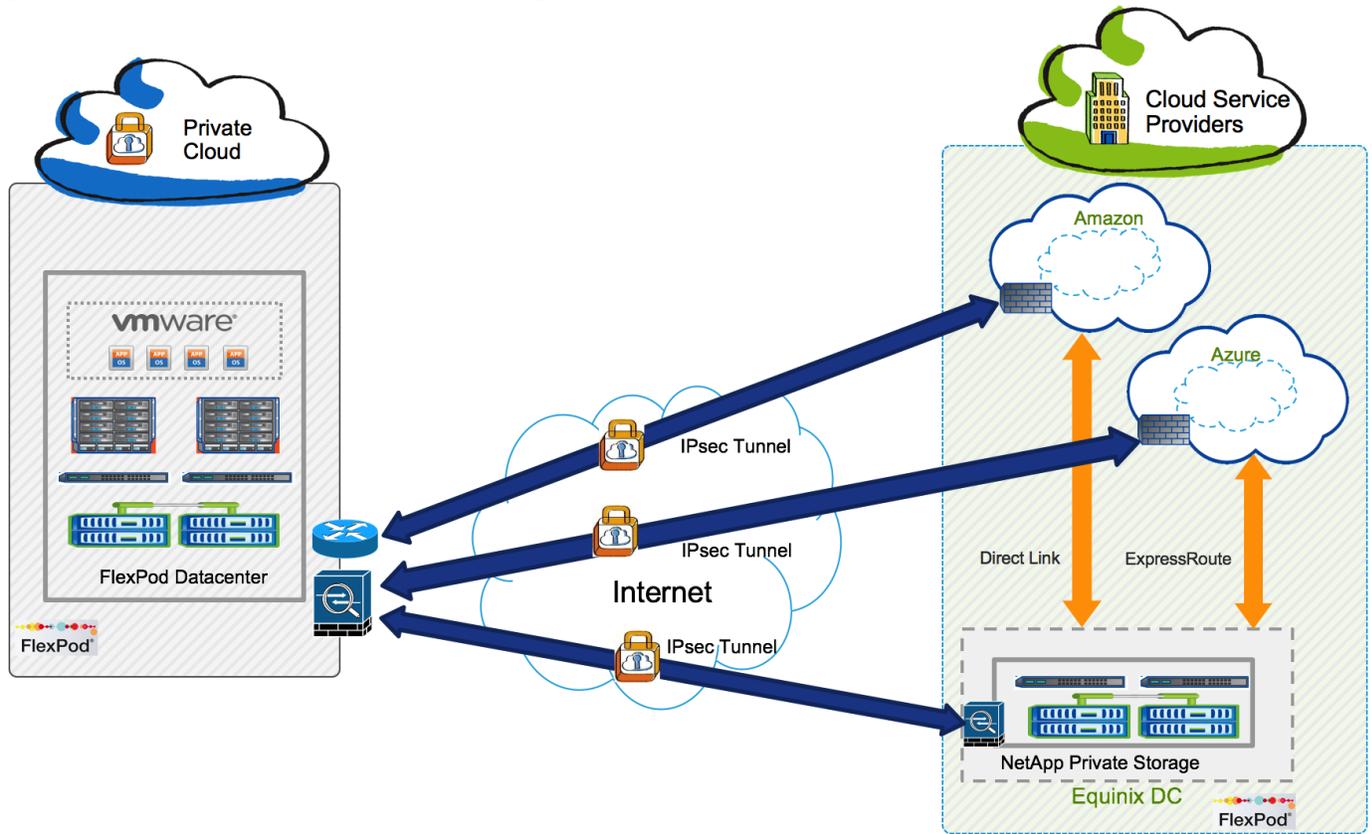
The IPsec tunnel parameters to setup this connectivity in the current design are listed in Table 4

**Table 4** IPsec Tunnel Details for NPS Connectivity

Parameter	Value
IKE (Phase 1)	
Authentication	Pre-Shared
Encryption	AES 128
Hash	SHA
DH Group	2
Lifetime	28800 seconds
IPsec (Phase 2)	
Network	Source and Destination depend on deployment
PFS	On
Peers	IP addresses of FlexPod and NPS ASAs
Transform Set	AES-128, SHA-HMAC
IPsec SA Lifetime	3600 seconds

0 shows the resulting network connectivity when the VPN tunnels are successfully established between FlexPod private cloud, public clouds and NPS.

Figure 20 FlexPod to NPS VPN Connectivity



## NPS for AWS Design Overview

The NetApp Private Storage for AWS solution combines computing resources from AWS with NetApp storage deployed at AWS Direct Connect data centers. In the AWS Direct Connect data center (Equinix), the customer provides network equipment (switch or router) and NetApp storage systems. VMs in the AWS cloud connect to the NetApp storage through IP-based storage protocols (iSCSI, CIFS, or NFS).

The NPS for AWS includes the following major components:

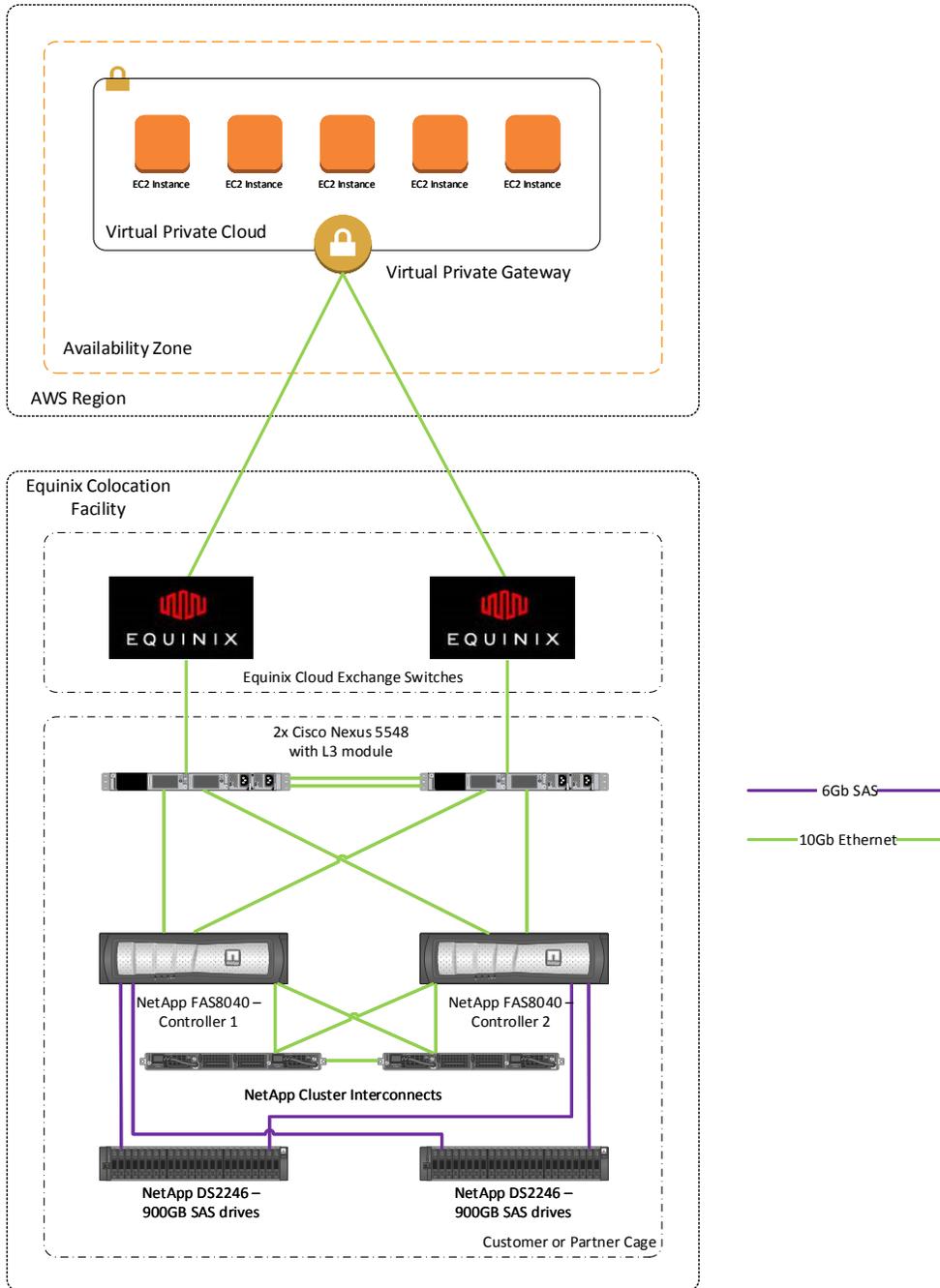
- AWS Elastic Compute Cloud (EC2) VMs
- AWS Virtual Private Cloud (VPC) network
- AWS Direct Connect
- Equinix colocation data center (AWS Direct Connect data center)
- Equinix Cloud Exchange (cloud peering switch for sub-1Gbps connections)
- Border Gateway Protocol—customer-owned network equipment that supports BGP routing protocols and 1Gbps or 10Gbps SMF connectivity
- NetApp storage (AFF, FAS, E-Series, or SolidFire platforms)

Figure 21 shows the architecture of NPS for AWS using FAS storage with redundant Direct Connect network connections using Equinix cloud exchange.



Specific customer implementations will vary, depending on each customer's technical and business requirements.

Figure 21 NPS to AWS Connectivity



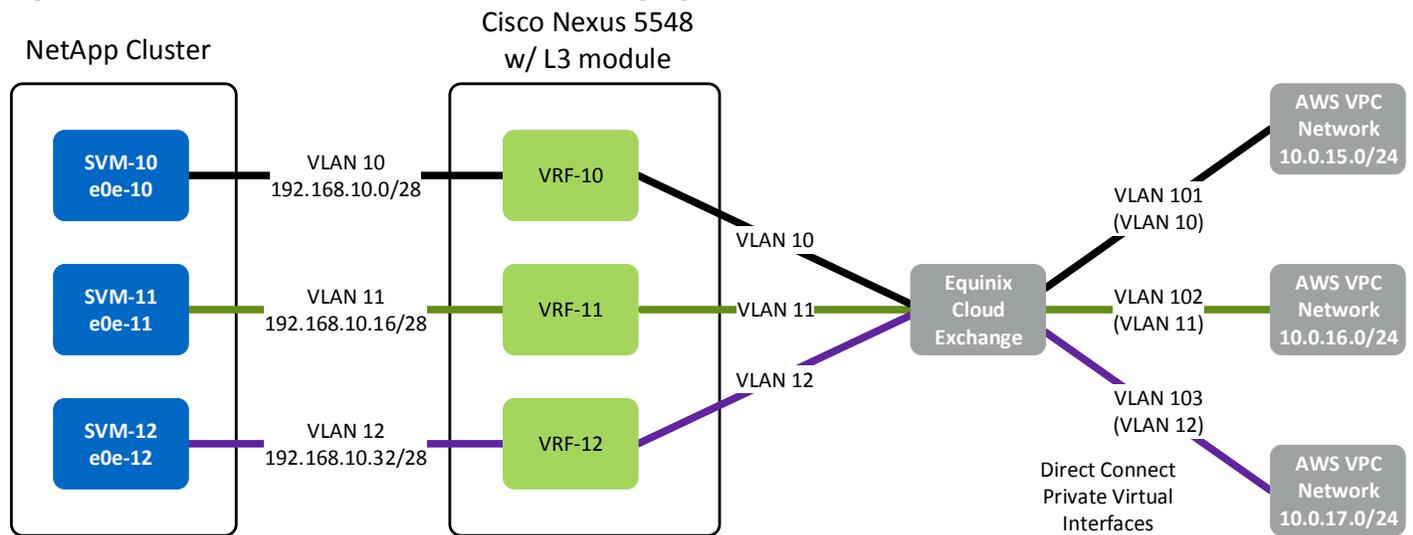
Connectivity from the NetApp storage to the AWS cloud is made possible by the AWS Direct Connect network service. The current design was validated using the cross-connect solution to connect NPS to AWS at link speed of 1Gbps.

## AWS Direct Connect

AWS Direct Connect is used to establish a dedicated network connection between the customer-provided network switch or router in the AWS Direct Connect data center (Equinix) and the Amazon VPC. Direct Connect supports the use of 802.1Q virtual local area networks (VLANs). By using multiple VLANs, customers can partition the Direct Connect dedicated connection into multiple Direct Connect private virtual interfaces. As shown in Figure 22, each Direct Connect private virtual interface is associated with a unique VLAN tag.

Using dedicated virtual routing and forwarding (VRF) instances, VLANs and LIFs on the SVMs on the NetApp storage cluster, this network segregation is maintained from the AWS VPC across the direct connect network connections and (cross connect) through the Direct Connect private virtual interfaces.

Figure 22 AWS Direct Connect – VLAN based segregation



Direct Connect connections come in two types: 1Gb Ethernet and 10Gb Ethernet. The connection from the VPC to the network switch (or router) in the Equinix colocation data center is a layer 2 connection from each AWS VGW used by the VPC. A cross-connect cable is patched from the AWS point of presence (PoP) in the Direct Connect data center to the customer network demarcation panel in the Direct Connect data center.

BGP is used to support network routing between the AWS VPC and the network in the Direct Connect data center over the AWS Direct Connect network connection. The network in the Equinix colocation data center is directly connected to the customer-provided layer 3 network equipment. The BGP configuration advertises local network routes to the VPC network over the Direct Connect network connection. It also receives the BGP advertisements from the VPC network over the Direct Connect network connection.

The customer-provided network equipment is in the same AWS Direct Connect data center as the NetApp storage. The network equipment must support the following features:

- Border Gateway Protocol. BGP is used to route network traffic between the local network in the Direct Connect data center and the AWS VPC network.

- At least one 9/125 SMF (1Gb/sec or 10Gb/sec) port. Direct Connect requires a minimum of one physical connection (9/125 SMF) from the customer-owned network equipment to AWS (or to the Equinix Cloud Exchange).
- 1000BASE-T Ethernet ports. The 1000BASE-T network ports on the switch provide network connectivity from the NetApp storage cluster. Although these ports can be used for data, NetApp recommends using 1GbE ports for node management and out-of-band management.
- 802.1Q VLAN support. The 802.1Q VLAN tags are used by Direct Connect private virtual interfaces (and the Equinix Cloud Exchange) to segregate network traffic on the same physical network connection
- The FlexPod DC for Hybrid Cloud utilized a pair of Nexus 5548 switches with L3 routing modules.



TR-4133 (<https://www.netapp.com/us/media/tr-4133.pdf>) provides detailed solution architecture and in-depth deployment details for NPS/AWS connectivity.

## NPS for Azure Design Overview

The NetApp Private Storage for Microsoft Azure solution combines computing resources from Microsoft Azure VM with NetApp storage deployed at Equinix colocation facilities. Connectivity from the NetApp storage to the Azure cloud is made possible by the Equinix Cloud Exchange and the Microsoft Azure ExpressRoute service. In the Equinix colocation data center, the customer provides network equipment (switch or router) and NetApp storage systems. VMs in the Azure cloud connect to the NetApp storage through IP-based storage protocols (iSCSI, CIFS, or NFS).



FlexPod DC for Hybrid Cloud utilizes the same equipment hosted in Equinix for connectivity to both AWS and MS Azure.

The NPS for Microsoft Azure consists of the following major components:

- Azure virtual machines (VMs) service
- Azure virtual network (VNet) service
- Azure ExpressRoute service
- Equinix colocation data center
- Equinix Cloud Exchange
- Border Gateway Protocol–customer-provided layer 3 network equipment that supports BGP routing protocols and 1Gbps or 10Gbps SMF connectivity
- NetApp storage (AFF, FAS, E-Series, or SolidFire platforms)

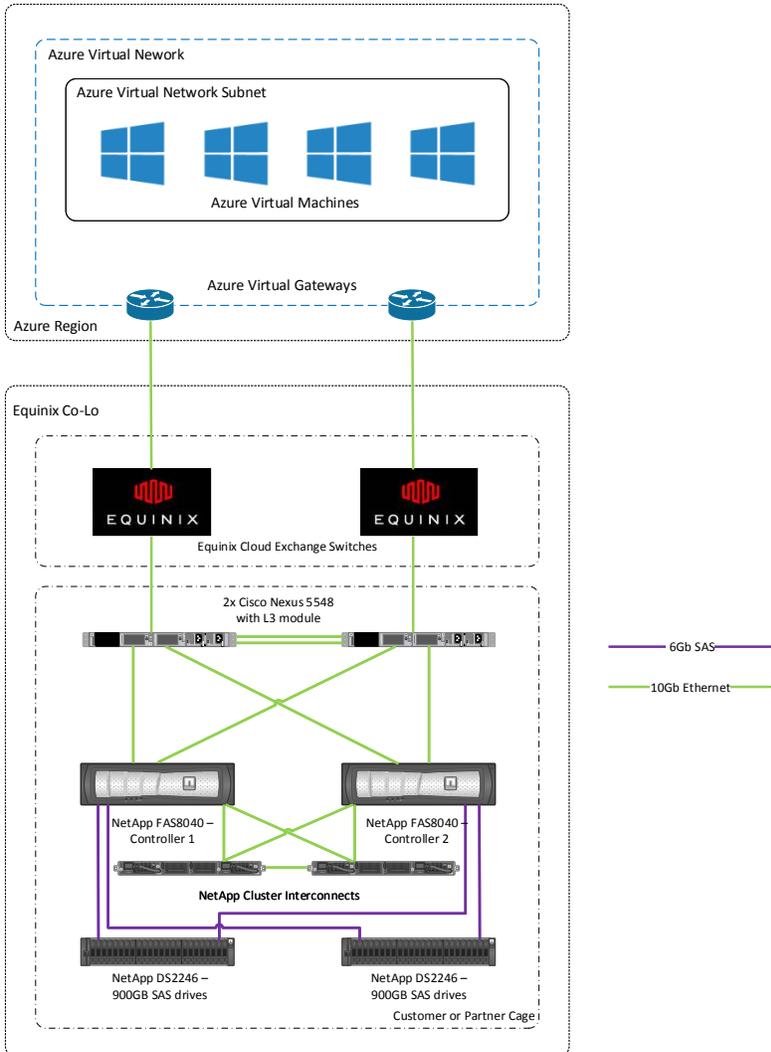
Figure 23 shows the architecture of NPS for Microsoft Azure using FAS storage with redundant ExpressRoute connections.



Specific customer implementations will vary, depending on each customer's technical and business requirements.



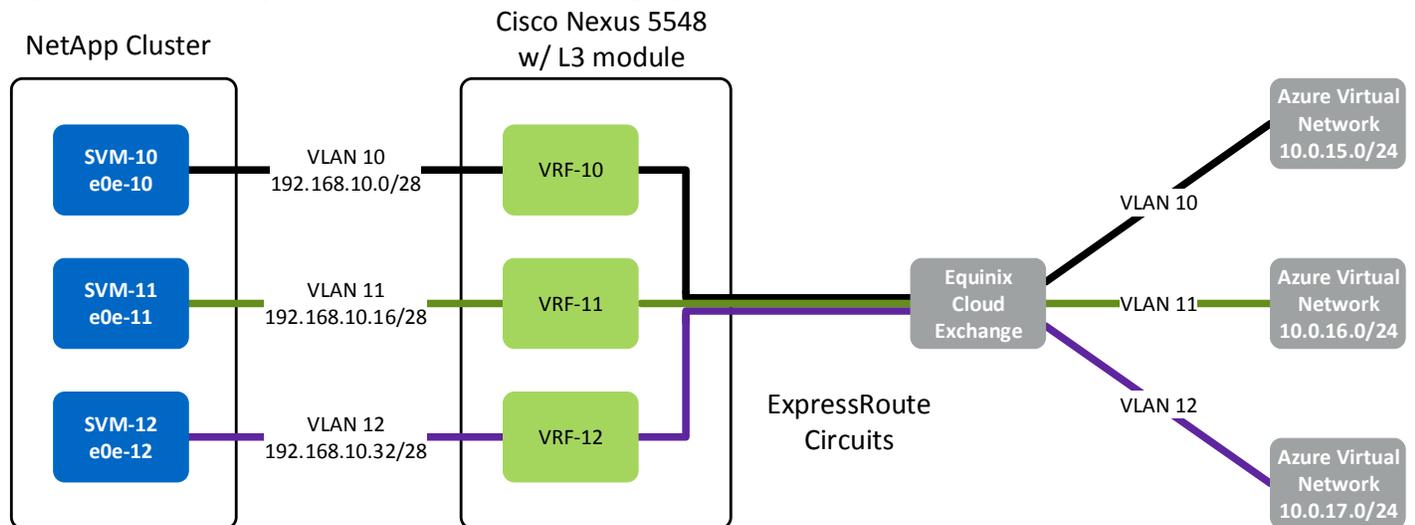
Figure 23 NPS to Azure Connectivity



### Azure ExpressRoute

Azure ExpressRoute is used to establish private dedicated network connections between the customer-provided network equipment in the Equinox data center and the Azure VNet. ExpressRoute supports the use of 802.1q VLANs. By using multiple VLANs, customers can partition the Azure ExpressRoute dedicated connection into multiple ExpressRoute circuits. As shown in Figure 24, each Azure ExpressRoute circuit is associated with a unique VLAN tag.

Figure 24 Azure ExpressRoute – VLAN based segregation



Azure ExpressRoute requires two physical network connections to the customer-provided network equipment in the colocation facility. It is recommended to patch each of these connections into redundant network switches so that if one switch or network connection fails, the network connectivity to Azure is maintained.

Border Gateway Protocol (BGP) is used to support network routing between the Azure VNETs and the customer network in the Equinix colocation facility over the Azure ExpressRoute network connection. The customer network in the Equinix colocation data center is directly connected to the customer-provided layer 3 network equipment. The BGP configuration advertises local network routes to the Azure VNet over the ExpressRoute network connection and also receives the BGP advertisements from the Azure VNet over the Azure ExpressRoute network connection.

The customer-provided network equipment is in the same Equinix colocation facility as the NetApp storage. The network equipment must support the following features:

- Border Gateway Protocol. BGP is used to route network traffic between the local network in the Equinix data center and the Azure VNet
- Virtual Router Redundancy Protocol (VRRP) or HSRP. Azure ExpressRoute requires two physical connections (9/125 SMF) from the customer network equipment to the Cloud Exchange. Redundant physical connections protect against potential loss of ExpressRoute service caused by a failure in the physical link
- Two layer-3 network switches/routers, for redundancy
- At least one 9/125 SMF (1Gbps or 10Gbps) port per switch. Minimum of one physical connection (9/125 SMF) from the customer-owned network equipment to Equinix Cloud Exchange
- At least one 1000BASE-T Ethernet port per switch. The 1000BASE-T network ports on the switch provide network connectivity from the NetApp storage cluster. Although these ports can be used for data, NetApp recommends using 1GbE ports for node management and out-of-band management

- 802.1q VLAN support. The 802.1q VLAN tags are used by the Equinix Cloud Exchange and Azure ExpressRoute to segregate network traffic on the same physical network connection

The FlexPod DC for Hybrid Cloud utilized a pair of Cisco Nexus 5548 switches with L3 routing modules.



TR-4316 (<https://www.netapp.com/us/media/tr-4316.pdf>) provides detailed solution architecture and in-depth deployment details for NPS/Azure connectivity.

---

## Application Setup

The FlexPod solution for Hybrid Cloud models a development and test environment for a sample open source e-commerce application, OpenCart. Utilizing an application blue-print defined in Cisco CloudCenter, the solution allows customers to deploy new application instances for development or testing at any available cloud within minutes. Using the NetApp Data Fabric combined with automation driven by the Cisco CloudCenter, new dev/test instances of the application regardless of the cloud location are pre-populated with up-to-date customer data. When the application instances are no longer required, the compute resources in the cloud are released and data instances on the NetApp storage are deleted.

## Application Overview

OpenCart is a free open source ecommerce platform for online merchants. The application is deployed using two separate CentOS 6 VMs; a catalog front end built on apache and PHP and a database backend based on MySQL DB.

Figure 25 OpenCart Application Overview



## Application Data Handling

Once the OpenCart application is deployed, a fully functional e-commerce application is available to customers where new user accounts can be easily added to the e-commerce site using the web GUI. If a user adds **items to his or her cart**, **these items are saved along with user's ID** in the database. The cart information can be later retrieved just like any other e-commerce website. OpenCart uses the following directory on the DB server to save all the user order and **cart information**: **"/data/mysql/opencart"**. This directory information will be used to setup data migration in the upcoming data handling section.

## OpenCart Application Blue Print

Cisco CloudCenter team has developed a blue print for the OpenCart application which can be requested through the CloudCenter technical marketing or sales teams. The blue print defines both the application tiers, their dependencies and software package locations.

Figure 26 OpenCart Blue Print

Edit "OpenCart Base" Application Profile

Version: [2.0](#) (Revision: 3)

Basic Information   Global Parameters   **Topology Modeler**

**Services**

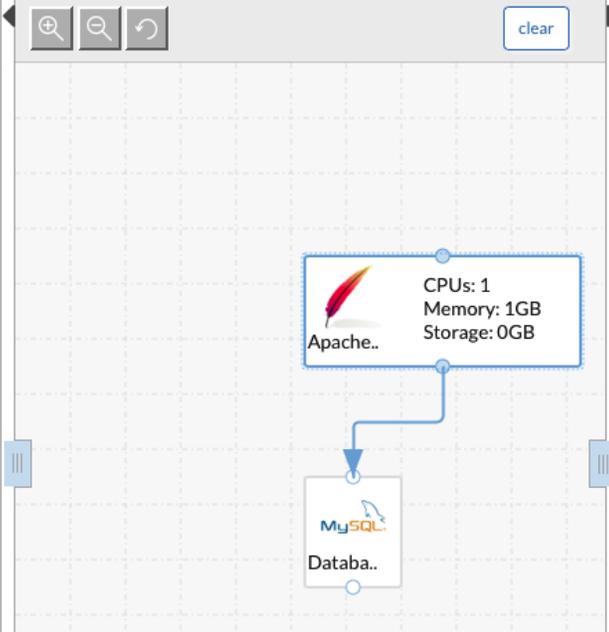
- OS Service
- Custom Service
- File System
- Workflow
- Frontend Cache
- Load Balancer
- Web Server



**Apache2**  
Open-source HTTP server for OS



**Geronimo3**  
Open source application server



**Properties**

**General Settings**

Name \*

Base Image \*

Minimum Number Of Nodes \*

Maximum Number Of Nodes \*

Number Of Volumes

**Service Initialization**

## Cloud Selection

Cisco CloudCenter allows system tags to be defined and assigned to various deployment options. In this design, three system tags were defined:

- Production
- Development
- Hybrid

The three system tags defined above are tied to various clouds as follows:

- Production: FlexPod/VMware Cloud
- Public: AWS or Azure Clouds
- Hybrid: AWS, Azure or Private Clouds

Based on the tags and their associations, the system has been validated where application can be deployed in any available cloud or can be deployed in a distributed fashion where DB server runs on FlexPod while the Web tier runs on the public cloud.

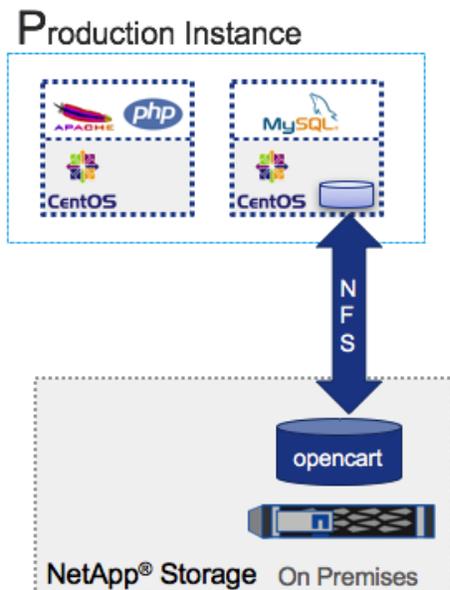
## Deploying Production Instance of Application

Using the application blue print for OpenCart and selecting the FlexPod as deployment locations (Tag: Private), first instance of the application is deployed. This instance is named OC-Production (or something similar) to identify it as production instance of the application. When the application is successfully deployed, customers can access the OpenCart application by pointing their browsers to the IP address or DNS name for the OpenCart Web VM.

To integrate the production copy of the application with NPS, following changes need to be made to the DB server:

- Create a Volume (opencart) and set up appropriate NFS mount-point (/opencart) on FlexPod Storage
- Mount the volume on the database VM using NFS (/mnt/opencart); add the mount information to /etc/fstab
- Shutdown the MySQL services
- Move the OpenCart data from its current location to the recently mounted directory
- Create a soft link at the previous directory location (/data/mysql/) to point to new location
- Restart the MySql services

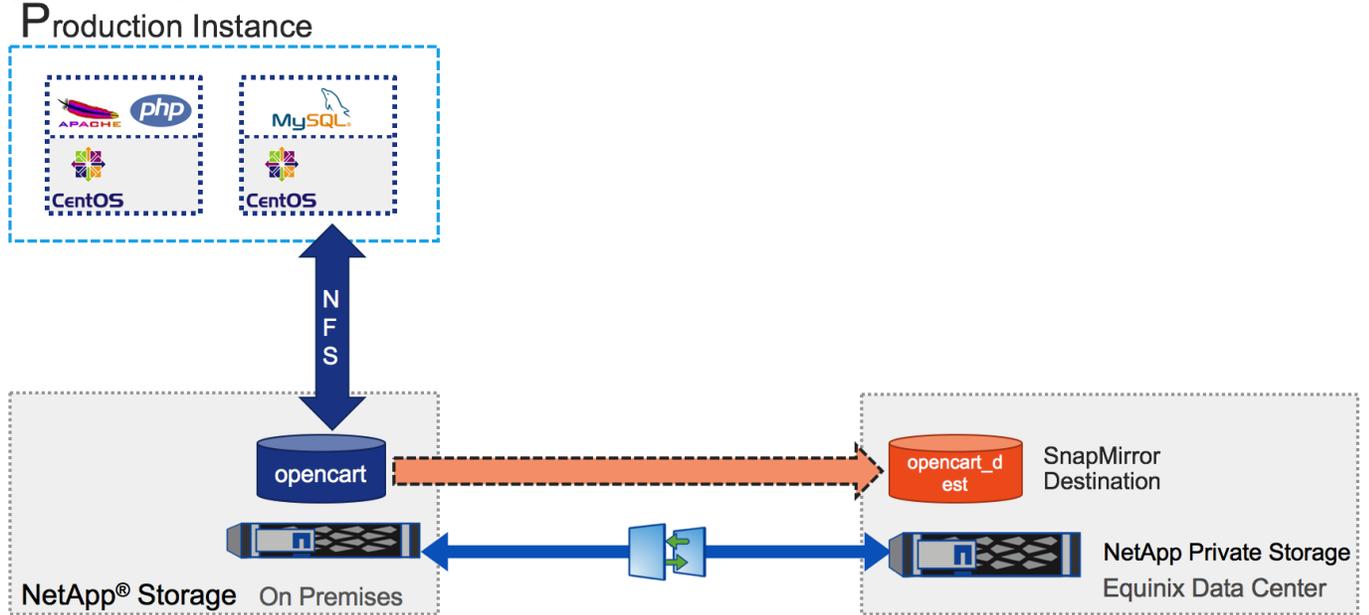
Figure 27 OpenCart – Production Application Instance



## Making Data Available using NetApp Private Storage

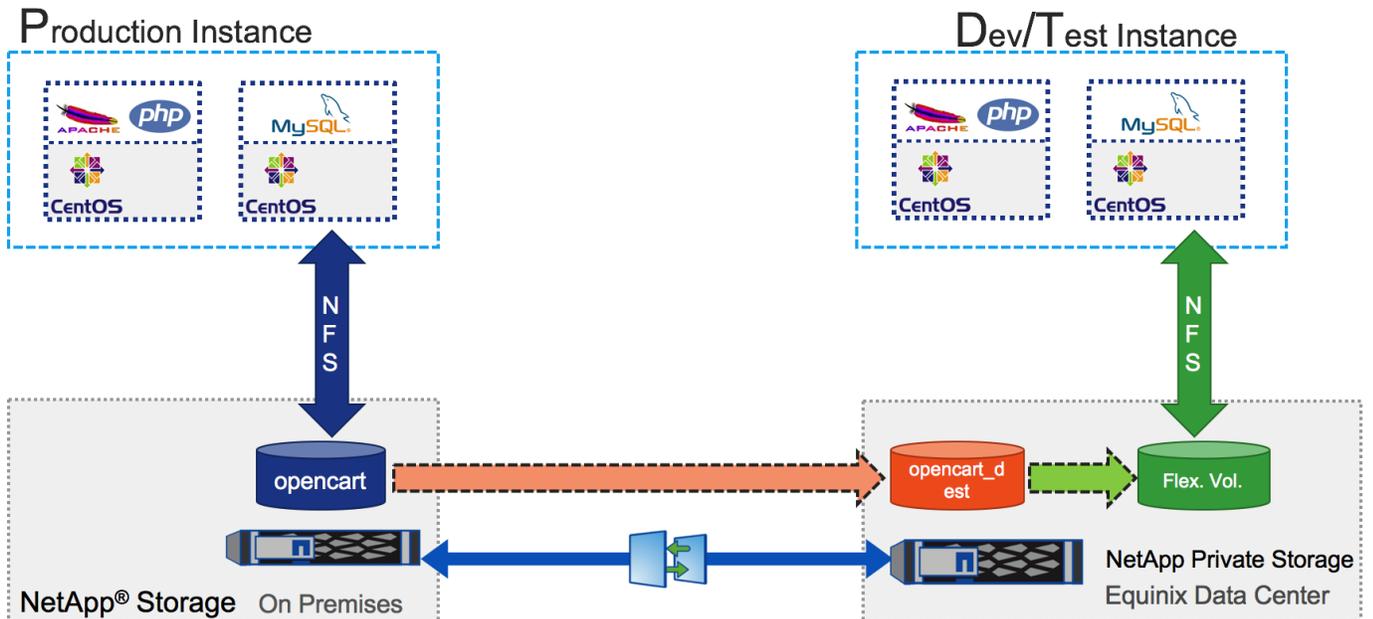
In the FlexPod DC for Hybrid Cloud, SnapMirror is used to replicate primary workload data from the on-premises production site to NPS (connected to both AWS and Azure). SnapMirror enables consistent data availability across all the clouds, keeps the data in sync, and automates data replication. The data is kept in sync by using a SnapMirror schedule, enabling the availability of up-to-date customer data for the new application instances across the clouds.

Figure 28 SnapMirror between FlexPod and NPS



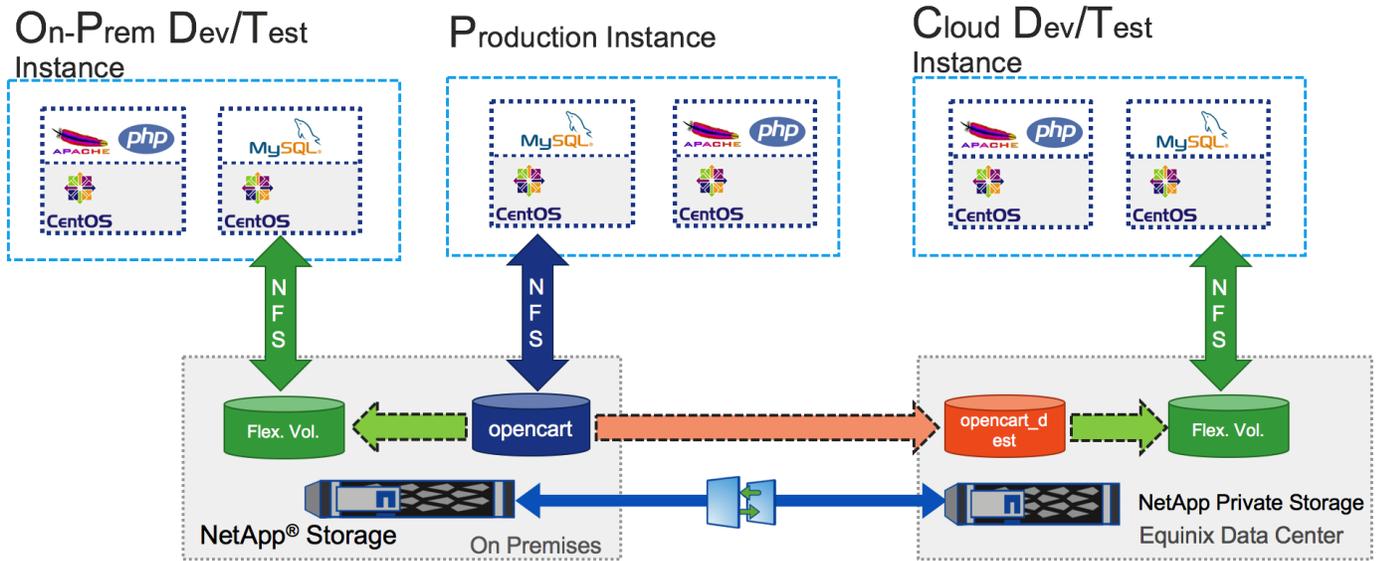
When an instance of the application is deployed in the public cloud, the SnapMirror destination volume is then cloned to provide multiple storage-efficient data instances. The destination volumes are cloned in NPS which has direct links to both AWS and Azure to make secure data accessible to the application instances in both the public clouds.

Figure 29 Cloning the SnapMirror Destination Volume during application deployments



If a customer chooses the private cloud to deploy the application development or test instance, there is no need to setup SnapMirror. A copy of the main data volume, opencart, is created on the FlexPod storage and mounted to the on-premise application instance.

Figure 30 Cloning the Volume for on-premise deployment

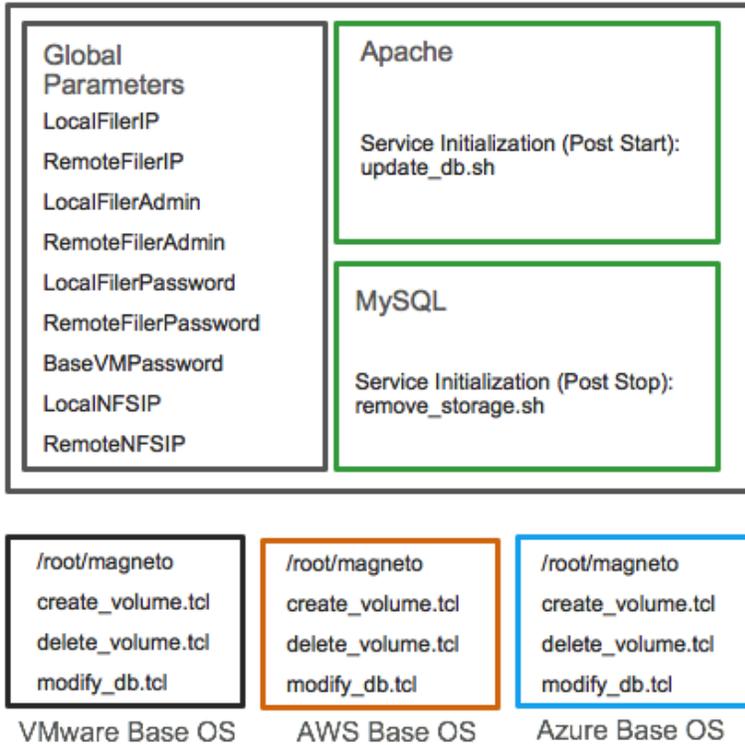


## Automating the Data Replication Process

The above sections covered setting up the hybrid cloud environment using CloudCenter, public and private clouds and using NPS to setup data replication and synchronization across various clouds. The final step in delivering a fully automated Dev-Test environment is to automate the data creation and deletion process for all future application instances. This process is completed using shell and TCL/expect scripts. Figure 31 shows how various scrips are positioned in the environment.

Figure 31 Script Framework for Data Automation

### OpenCart Blue Print



### Application Blue Print – Global Parameters

The application blue print for OpenCart is modified and the required connectivity and authentication information is stored as global parameters. The configuration scripts utilize this information to connect to storage devices (and VMs in some cases) and issue CLI commands to create flexible volumes, etc.

### Configuration Scripts

To successfully create the volume clones in FlexPod and the cloud environment, two types of scripts are utilized:

- Scripts common to all deployments hosted in an HTTP repository: update\_db.sh and remove\_storage.sh. These shell scripts are called from the CloudCenter at the time of setting up or terminating an application instance
- Scripts unique to individual deployments are positioned in the base OS image templates for various cloud platforms. These TCL/expect scripts are setup with commands specific to the individual cloud requirements.

When an application instance is launched, the scripts perform the following actions:

- Determine the location of the deployment based on the deployment tag information
- Log into the storage system using the correct global parameter information

- For Private Cloud deployments, a FlexClone of the data volume is created and an NFS mount point configured
- For Public Cloud deployments, the SnapMirror relationship is updated before creating a FlexClone volume and an NFS mount point
- DB services are stopped and the data from newly created FlexClone volume is mounted and made available to the MySQL server
- DB services are restarted and as a result, OpenCart application is populated with latest user data

When an application instance is terminated the scripts perform following actions:

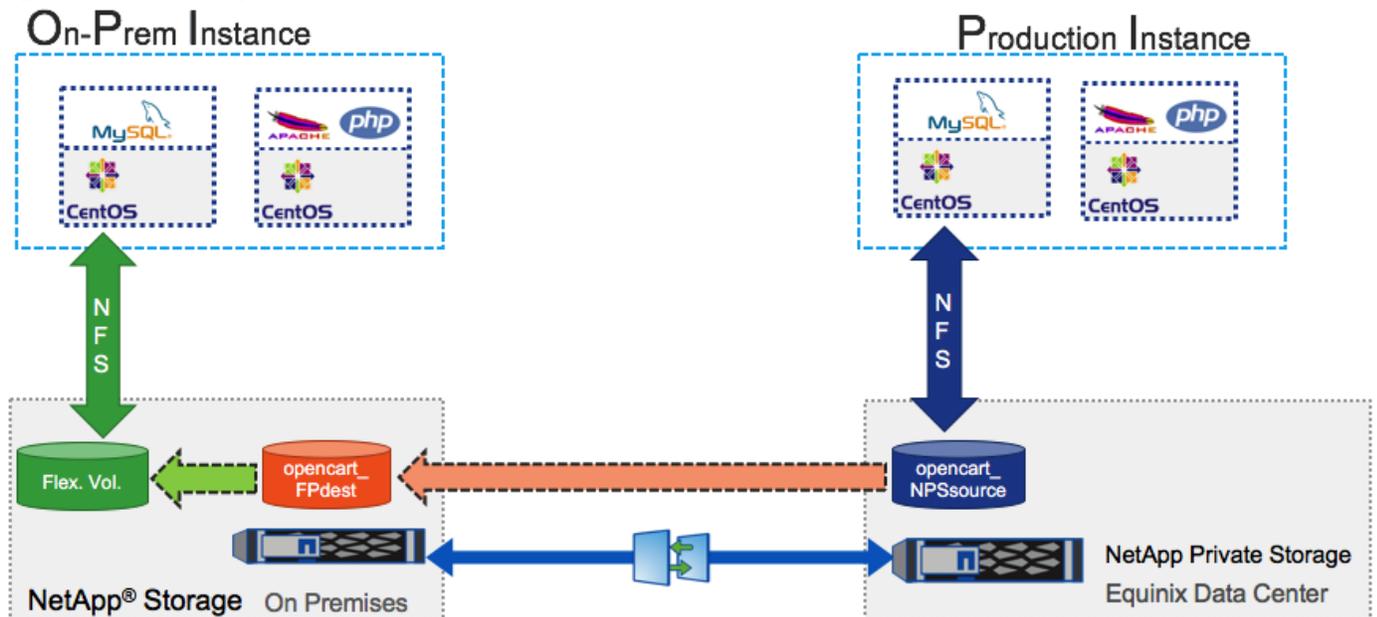
- Determine the location of the deployment based on the deployment tag information
- Log into the correct storage system using the global parameters information
- Delete the FlexClone volume associated with the application instance

## Data Repatriation – Using NPS to Migrate Application(s) to the Private Cloud

Public Cloud provides a great platform for various types of workloads. However, running an application permanently in the public cloud can become very expensive over time. Many a times, cost is not the only reason customers might want to move the applications back to private cloud. Corporate data control requirements, data security needs and enhanced SLA requirements can be some of the other factors under consideration. One of the major challenges that many organizations face when trying to bring an application back to their on-premise infrastructure (private cloud) is the challenge of user data migration from the public cloud. Using the design highlighted above combined with reverse SnapMirror i.e. mirroring data from NPS to FlexPod DC, customers can easily migrate the applications back to their on-premise infrastructure.

FlexPod DC for hybrid cloud design has been verified to support the data repatriation use case. In this scenario, an OpenCart production instance is deployed in AWS. Using the methodology outlined above, the data from the production DB server is **moved to a volume called “opencart\_NPSsource”** hosted on NPS storage. This volume is then replicated to a volume named **“opencart\_FPdest” on the FlexPod private** storage. When the data automation is combined with the application blue print, future application instances deployed in Private cloud utilize up to date data replicated from the public cloud. When the customers are satisfied with the local instance of the application and local copy of the data, the application instance from the Public Cloud can be shut down and removed.

Figure 32 Data Repatriation



## ACI Integration

CloudCenter and Cisco ACI are application-centric platforms which integrate seamlessly for application delivery. Because CloudCenter is tightly integrated with the APIC, the network and security requirements are easily satisfied during the execution phase. When an application is deployed by CloudCenter in an ACI fabric, the conventional APIC objects and policies are dynamically created and applied to the respective virtual machines.

The FlexPod DC for Hybrid Cloud design details covered so far required a destination EPG to be provisioned for deploying OpenCart application. All the contracts to allow communication to the storage system as well as to utilize L3-Out for accessing Internet also needed to be pre-configured. One shortcoming of this design is that all new Dev/Test instances are deployed using the same EPG and therefore are not be isolated from each other at the network layer. Integrating CloudCenter with ACI overcomes this limitation and depending on customer requirement, CloudCenter offers various deployment models for an ACI-enabled private cloud.

Details of various design options can be accessed here:

<http://docs.cloudcenter.cisco.com/display/CCD46/ACI>.

For the ACI integration in the current design, the following items have been pre-provisioned using FlexPod DC with ACI design options:

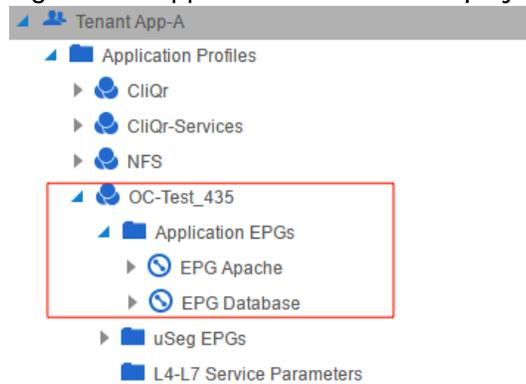
- Tenant (App-A)
- Virtual Machine Manager (vCenter-VDS)
- Bridge Domain (App-A/BD-Internal)
- Existing Contracts (App-A/Allow-NFS, common/Allow-Shared-L3-Out)

Using these settings, when a new application instance is deployed on the private cloud, the following items are automatically created:

- Application Profile
- Web EPG
- DB EPG
- Contract allowing communication between Web and DB EPGs
- Pre-existing contracts consumed by application tiers to enable communication to storage and L3 network

Figure 33 shows how a new application profile for an OpenCart application instance looks like on APIC:

**Figure 33 Application Profile for deployment names OC-Test**



The name of the application profile is derived using the deployment name provided in CloudCenter. Any new application instance will result in creation of new application profile.

## Deployment Hardware and Software

### Hardware and Software Revisions

**Table 5** below outlines the hardware and software versions used for the solution validation. It is important to note that Cisco, NetApp, and VMware have interoperability matrices that should be referenced to determine support for any specific implementation of FlexPod. Please refer to the following links for more information:

- <http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>
- <http://mysupport.netapp.com/matrix/>
- <http://www.vmware.com/resources/compatibility/search.php>

**Table 5** Hardware and Software Revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6200 Series, Cisco UCS B-200 M4, Cisco UCS C-220 M4	3.1(2b)	Includes the Cisco UCS-IOM 2208XP, Cisco UCS Manager, and Cisco UCS VIC 1340
Network	Cisco Nexus Switches	12.1(2e)	iNXOS
	Cisco APIC	2.1(2e)	ACI release
Storage	NetApp AFF	9.1P2	Software version
	NetApp VSC	6.2P2	Software version
Software	VMware vSphere ESXi	6.0 update 1	Software version
	VMware vCenter	6.0 update 1	Software version
	CloudCenter	4.7.3	Software version

## Validation

---

### Test Plan

The FlexPod DC for Hybrid Cloud solution was validated by deploying OpenCart application in a multi-cloud environment. The system was validated for successful application deployment, data availability across the clouds, and secure communication between various application tiers when configured in a distributed manner. The types of tests executed on the system are detailed in the following subsections.

#### VPN Connectivity Validation

- Secure communication across the FlexPod to NPS VPN tunnel
- Secure communication across the FlexPod to AWS VPN tunnel
- Secure communication across the FlexPod to Azure VPN tunnel

#### Private Cloud Validation

- Application deployment and data offload to NetApp volume
- Persistent NFS mount across VM reboots
- Updating and provisioning the Base OS template
- Automatic FlexClone volume provisioning and deletion
- Automated ACI Application Profile and EPG configuration
- Application security and access using ACI contracts
- Script validation

#### Public Cloud Validation

- Application deployment and data offload to NetApp Private Storage from AWS and Azure
- Persistent NFS mount across VM reboots
- Updating and provisioning the Base OS template
- Automatic FlexClone volume provisioning and deletion
- SnapMirror validation for data replication
- Application security and access using cloud based VM access control

## Summary

---

FlexPod Datacenter for Hybrid Cloud delivers a validated Cisco ACI based FlexPod infrastructure design that allows customers to utilize resources in the public cloud based on the organization workload deployment policies or when the workload demand exceeds the available resources in the Datacenter. This new FlexPod solution allows customers to seamlessly extend compute and storage resources from an on-premises FlexPod to major cloud providers such as Amazon and Azure using Cisco CloudCenter and NetApp Private Storage. The FlexPod Datacenter for Hybrid Cloud showcases:

- A fully programmable software defined networking (SDN) enabled DC design: Cisco ACI
- An application-centric hybrid cloud management platform: Cisco CloudCenter
- High-speed cloud to co-located storage access: NetApp Private Storage in Equinix Datacenter
- Multi-cloud support: AWS and Microsoft Azure

## References

---

### Products and Solutions

Cisco Unified Computing System:

<http://www.cisco.com/en/US/products/ps10265/index.html>

Cisco UCS 6200 Series Fabric Interconnects:

<http://www.cisco.com/en/US/products/ps11544/index.html>

Cisco UCS 5100 Series Blade Server Chassis:

<http://www.cisco.com/en/US/products/ps10279/index.html>

Cisco UCS B-Series Blade Servers:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/index.html>

Cisco UCS C-Series Rack Servers:

<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html>

Cisco UCS Adapters:

[http://www.cisco.com/en/US/products/ps10277/prod\\_module\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html)

Cisco UCS Manager:

<http://www.cisco.com/en/US/products/ps10281/index.html>

Cisco Nexus 9000 Series Switches:

<http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html>

Cisco Application Centric Infrastructure:

<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html>

Cisco CloudCenter

<http://www.cisco.com/c/en/us/products/cloud-systems-management/cloudcenter/index.html>

Amazon Web Services

<https://aws.amazon.com>

Microsoft Azure

<https://azure.microsoft.com>

VMware vCenter Server:

<http://www.vmware.com/products/vcenter-server/overview.html>

VMware vSphere:

[https://www.vmware.com/tryvmware\\_tpl/vsphere-55\\_evalcenter.html](https://www.vmware.com/tryvmware_tpl/vsphere-55_evalcenter.html)

NetApp Data ONTAP

<http://www.netapp.com/us/products/platform-os/ontap/index.aspx>

NetApp FAS8000:

<http://www.netapp.com/us/products/storage-systems/fas8000/>

NetApp VSC:

<http://www.netapp.com/us/products/management-software/vsc/>

## Interoperability Matrixes

Cisco UCS Hardware Compatibility Matrix:

<http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>

VMware and Cisco Unified Computing System:

<http://www.vmware.com/resources/compatibility>

NetApp Interoperability Matrix Tool:

<http://mysupport.netapp.com/matrix/>

## About the Authors

---

Haseeb Niazi, Technical Marketing Engineer, Computing Systems Product Group, Cisco Systems, Inc.

Haseeb Niazi has over 17 years of experience at Cisco in the Data Center, Enterprise and Service Provider solutions and technologies. As a member of various solution teams and Advanced Services, Haseeb has helped many enterprise and service provider customers evaluate and deploy a wide range of Cisco solutions. As a technical marketing engineer at Cisco UCS solutions group, Haseeb currently focuses on network, compute, virtualization, storage and orchestration aspects of various Compute Stacks. Haseeb holds a master's degree in Computer Engineering from the University of Southern California and is a Cisco Certified Internetwork Expert (CCIE 7848).

David Arnette, Technical Marketing Engineer, Converged Infrastructure Group, NetApp.

David Arnette is a Sr. Technical Marketing Engineer with NetApp's Converged Infrastructure group, and is responsible for developing reference architectures for application deployment using the FlexPod converged infrastructure platform from NetApp and Cisco. He has over 18 years of experience designing and implementing storage and virtualization infrastructure, and holds certifications from Cisco, NetApp, VMware and others. His recent work includes FlexPod solutions for Docker Enterprise Edition, Platform9 Managed OpenStack, and Continuous Integration/Continuous Deployment using Apprenda PaaS and CloudBees Jenkins with Docker containers.

## Acknowledgements

- John George, Technical Marketing Engineer, Cisco Systems, Inc.
- Matthew Baker, Technical Marketing Engineer, Cisco Systems, Inc.
- Ganesh Kamath, Technical Marketing Engineer, NetApp