Abstract

FlexPod® forms a flexible, open, integrated foundation for running multihypervisor cloud environments such as enterprise-grade OpenStack and VMware private cloud. Platform9 Managed OpenStack is the fast, easy, and enterprise-grade path to hybrid cloud due to the simplicity of its SaaS-managed delivery model. By combining support for existing VMware vSphere environments, Platform9 provides a single management plane for your Managed OpenStack and Amazon cloud resources. The FlexPod Hybrid Cloud Solution with Platform9 Managed OpenStack combines best-in-class infrastructure and software to provide a hybrid cloud platform for virtualized and cloud-native workloads.
TABLE OF CONTENTS

1 Solution Overview .................................................................................................................. 3
  1.1 Use Case Summary ........................................................................................................... 3
  1.2 Solution Technology ........................................................................................................ 3

2 Deployment and Management of Platform9 OpenStack on FlexPod ....................................... 14
  2.1 Technology Requirements ............................................................................................... 14
  2.2 Deployment Procedures ................................................................................................ 15
  2.3 Solution Validation .......................................................................................................... 21

3 Managing AWS Resources with Platform9 Clarity UI .............................................................. 30
  3.1 Technology Requirements ............................................................................................. 30
  3.2 Deployment Procedures ................................................................................................. 31
  3.3 Solution Validation ......................................................................................................... 32

4 Managing VMware vSphere Resources with Platform9 Clarity UI ........................................... 32
  4.1 Technology Requirements ............................................................................................. 32
  4.2 Deployment Procedures ................................................................................................. 33
  4.3 Solution Validation ......................................................................................................... 34

5 OpenStack Upgrade .............................................................................................................. 34

Conclusion .............................................................................................................................. 34

References .................................................................................................................................. 35

LIST OF TABLES
Table 1) FlexPod OpenStack hardware requirements .................................................................... 15
Table 2) FlexPod OpenStack software requirements ................................................................... 15
Table 3) FlexPod OpenStack hardware requirements .................................................................. 32
Table 4) FlexPod OpenStack software requirements .................................................................. 32

LIST OF FIGURES
Figure 1) FlexPod Datacenter components .............................................................................. 4
Figure 2) Cisco UCS components ............................................................................................. 5
Figure 3) ONTAP ..................................................................................................................... 9
Figure 4) KVM host vNIC and network segmentation ................................................................. 17
Figure 5) OpenStack upgrade notification .................................................................................. 34
1 Solution Overview

Cloud computing models have changed the way IT organizations operate, and many enterprises are turning to public cloud resources to offset traditional IT capital expenses. However, there are many workloads that must remain on site due to performance, security, or other reasons. For workloads that remain on the premises, customers would still like to manage those resources with the same simplicity as their public cloud environments. Platform9’s software-as-a-service (SaaS) platform allows enterprises to deploy an OpenStack private cloud in minutes and provides visibility into every layer of the infrastructure stack. Customers can also integrate other public and private cloud platforms into the Platform9 management plane, such as Amazon Web Services and VMware vSphere, allowing customers to manage their entire hybrid cloud estate from a single management plane.

FlexPod converged infrastructures utilize Cisco UCS Servers, Cisco Nexus switches, and NetApp® All Flash FAS storage systems to deliver the most flexible, scalable, and reliable infrastructure on the market. FlexPod allows organizations to build an infrastructure that supports almost any operating system or application with enterprise-class performance and reliability. FlexPod also supports nondisruptive scaling of any resource and dynamic reallocation of resources, providing organizations the agility to react to changing business requirements with minimal impact. This eliminates application silos and streamlines IT operations by creating a standardized infrastructure that supports API-based administration for innovative private cloud deployments. By leveraging the NetApp Data Fabric, FlexPod becomes the on-site component of a highly efficient hybrid cloud.

This document describes the benefits and technical details of Platform9 Managed OpenStack running on the FlexPod Datacenter converged infrastructure. This document also includes validation of AWS and VMware vSphere management from the Platform9 Clarity user interface.

1.1 Use Case Summary

This solution provides customers with an onsite OpenStack infrastructure, which is managed in the same manner as public cloud resources. Platform9 deploys OpenStack storage, networking, and compute resources on the customer-provided hardware using a management plane located in Platform9 cloud. In addition to managing the OpenStack environment through the Platform9 Clarity UI, this solution provides true hybrid cloud management capabilities by integrating Amazon EC2 (and other public cloud providers in future) and VMware vSphere management capabilities into the UI as well.

This solution applies to the following use cases:

- Deployment and management of OpenStack on FlexPod converged infrastructure through Platform9 Managed OpenStack
- Connectivity and management of Amazon Web Services resources through Platform9’s Managed OpenStack drivers for hybrid and multicloud environments
- Connectivity and management of VMware vSphere resources through Platform9 Managed OpenStack integration with vSphere

1.2 Solution Technology

FlexPod Converged Infrastructure

FlexPod is a prespecified, best practice data center architecture that is built on the Cisco Unified Computing System (Cisco UCS), the Cisco Nexus family of switches, and NetApp FAS and AFF storage systems. FlexPod is a suitable platform for running a variety of virtualization hypervisors as well as bare-metal operating systems (OSs) and enterprise workloads. FlexPod delivers a baseline configuration and can also be sized and optimized to accommodate many different use cases and requirements. Figure 1 depicts the component families of the FlexPod solution.
FlexPod provides a uniform approach to IT architecture, offering a well-characterized and documented shared pool of resources for application workloads. FlexPod delivers operational efficiency and consistency with the versatility to meet a variety of SLAs and IT initiatives, including the following:

- Application rollouts or migrations
- Business continuity and disaster recovery (DR)
- Desktop virtualization
- Cloud delivery models (public, private, and hybrid) and service models (IaaS, PaaS, and SaaS)
- Asset consolidation and virtualization
- Data center consolidation and footprint reduction

Cisco and NetApp have thoroughly validated and verified the FlexPod solution architecture and its many use cases. In addition, they have created a portfolio of detailed documentation, information, and references to assist customers in transforming their data centers to this shared infrastructure model. This portfolio includes, but is not limited to, the following items:

- Best practice architectural design
Cisco and NetApp have also built a robust and experienced support team focused on FlexPod solutions, from customer account and technical sales representatives to professional services and technical support engineers. This support alliance provides customers and channel services partners with direct access to technical experts who collaborate with cross vendors and have access to shared lab resources to resolve potential issues.

FlexPod supports tight integration with virtualized and cloud infrastructures, making it the logical choice for long-term investment.

**Cisco UCS**

The Cisco UCS is a next-generation data center platform that unites computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce the total cost of ownership and increase business agility. The system integrates a low-latency, lossless 10 Gigabit Ethernet (10GbE) unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain.

*Figure 2) Cisco UCS components.*
The main components of the Cisco UCS are as follows:

- **Compute.** The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers based on Intel Xeon 2600 v2 series processors.
- **Network.** The system is integrated onto a low-latency, lossless, 10Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks that are typically configured as separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables and by reducing power and cooling requirements.
- **Virtualization.** This system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access.** The system provides consolidated access to both SAN storage and NAS over the unified fabric. By unifying storage access, the Cisco UCS can access storage over Ethernet (SMB 3.0 or iSCSI), FC, and FCoE. This provides customers with storage choices and investment protection. In addition, server administrators can preassign storage access policies to storage resources for simplified storage connectivity and management, which lead to increased productivity.
- **Management.** The system integrates all system components so that the entire solution can be managed as a single entity by Cisco UCS Manager. Cisco UCS Manager has an intuitive GUI, a CLI, and a powerful scripting library module for Microsoft PowerShell built on a robust API. These different methods can manage all system configuration and operations.

Cisco UCS fuses access layer networking and servers. This high-performance, innovative server system provides a data center with a high degree of workload agility and scalability.

**Cisco UCS 6248UP Fabric Interconnects**

The fabric interconnects provide a single point of connectivity and management for the entire system. Typically deployed as an active-active pair, the system’s fabric interconnects integrate all components into a single, highly available management domain controlled by Cisco UCS Manager. The fabric interconnects manage all I/O efficiently and securely at a single point, resulting in deterministic I/O latency independent of the topological location of a server or VM in the system.

Cisco UCS 6200 Series fabric interconnects support the system’s 10Gbps unified fabric with low-latency, lossless, cut-through switching that supports IP, storage, and management traffic with a single set of cables. The fabric interconnects feature virtual interfaces that terminate both physical and virtual connections equivalently, establishing a virtualization-aware environment in which blades, rack servers, and VMs are interconnected by the same mechanisms. The Cisco UCS 6248UP is a 1RU fabric interconnect that features up to 48 universal ports that can support 10GbE, FCoE, or native FC connectivity.

**Cisco UCS 5108 Blade Server Chassis**

The Cisco UCS 5100 Series blade server chassis is a crucial building block of the Cisco UCS, delivering a scalable and flexible chassis. The Cisco UCS 5108 blade server chassis is 6RU high and can mount in an industry-standard, 19-inch rack. A single chassis can house up to eight half-width Cisco UCS B-Series blade servers and can accommodate both half-width and full-width blade form factors.

Four single-phase, hot-swappable power supplies are accessible from the front of the chassis. These power supplies are 92% efficient and can be configured to support nonredundant, N + 1 redundant configurations and grid-redundant configurations. The rear of the chassis contains eight hot-swappable fans, four power connectors (one per power supply), and two I/O bays for Cisco UCS 2200 XP fabric extenders. A passive midplane provides up to 40Gbps of I/O bandwidth per server slot and up to 80Gbps of I/O bandwidth for two slots.
Cisco UCS 2204XP Fabric Extenders

The Cisco UCS 2204XP has four 10GbE, FCoE-capable, enhanced small form-factor pluggable (SFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2204XP has 16 10GbE ports connected through the midplane to the half-width slot in the chassis. When configured in pairs for redundancy, two 2204XP fabric extenders provide up to 80Gbps to the chassis.

Cisco UCS B200 M4 Blade Servers

The enterprise-class Cisco UCS B200 M4 blade server extends the capabilities of the Cisco UCS portfolio in a half-width blade form factor. The Cisco UCS B200 M4 is powered by the latest Intel Xeon E5-2600 v4 Series processor family CPUs. This server contains up to 1536GB of RAM (using 64GB DIMMs), two solid-state drives (SSDs) or hard disk drives (HDDs), and up to 80Gbps throughput connectivity. The Cisco UCS B200 M4 blade server mounts in a Cisco UCS 5100 Series blade server chassis or a Cisco UCS Mini blade server chassis. It supports one connector for Cisco’s Virtual Interface Card (VIC) 1340 or VIC 1240 adapter, which provides Ethernet and FCoE.

Cisco UCS Manager

Cisco UCS Manager provides unified, centralized, embedded management of all Cisco UCS software and hardware components across multiple chassis and thousands of VMs. Administrators use this software to manage the entire Cisco UCS as a single logical entity through an intuitive GUI, a CLI, or an XML API.

The Cisco UCS Manager resides on a pair of Cisco UCS 6200 Series fabric interconnects in a clustered, active-standby configuration for high availability. The software provides administrators with a single interface for performing server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection. Cisco UCS Manager service profiles and templates support versatile role-based and policy-based management.

Key elements managed by Cisco UCS Manager include the following:

- Cisco UCS Integrated Management Controller (IMC) firmware
- RAID controller firmware and settings
- BIOS firmware and settings, including server universal user ID (UUID) and boot order
- Converged network adapter firmware and settings, including MAC addresses, worldwide names (WWNs), and SAN boot settings
- Virtual port groups used by VMs, with Cisco Data Center VM-FEX technology
- Interconnect configuration, including uplink and downlink definitions, MAC address and WWN pinning, virtual local area networks (VLANs), virtual storage area networks, quality of service (QoS), bandwidth allocations, Cisco Data Center VM-FEX settings, and EtherChannels to upstream LAN switches

For more information, see the Cisco UCS Manager site.

Cisco Nexus 9000 Series Switches

The Cisco Nexus 9000 Series is designed for data center environments with cut-through switching technology that enables consistent low-latency Ethernet solutions. With front-to-back or back-to-front cooling, the Cisco Nexus 9000 Series possesses data ports in the rear, which brings switching into close proximity with servers and makes cable runs short and simple. This switch series is highly serviceable, with redundant, hot-pluggable power supplies and fan modules. It uses data center–class Cisco NX-OS software for high reliability and ease of management.

The Cisco Nexus 9000 platform extends the industry-leading versatility of the Cisco Nexus Series purpose-built, 10GbE data center–class switches and provides innovative advances toward higher density, lower latency, and multilayer services. The Cisco Nexus 9000 platform is well suited for enterprise data center deployments across a diverse set of physical, virtual, and high-performance
computing (HPC) environments. Cisco Nexus 9000 switches provide 40Gb switching capability and can participate in Cisco Application Centric Infrastructure.

The switch used in the validation of this FlexPod architecture is the Cisco Nexus 9396PX. This switch has the following specifications:

- A two-rack unit, 1/10/40GbE switch
- Forty-eight fixed 1/10GbE ports on the base chassis and one expansion slot supporting up to 12 fixed 40GbE ports
- Throughput of up to 1.92Tbps

Other Cisco Nexus 9000 switches, such as the Cisco Nexus 9372, are also suitable for this architecture. Cisco Nexus 9396PX switches were used for this validation due to inventory availability. However, their use is not a specific requirement for this solution.

For more information, see the Cisco Nexus 9000 Series Switches site.

NetApp FAS/AFF Storage Systems

A product of more than 20 years of innovation, ONTAP® has evolved to meet the changing needs of customers and help drive their success. ONTAP provides a rich set of data management features and clustering for scale-out, operational efficiency, and nondisruptive operations. This storage software offers customers one of the most compelling value propositions in the industry. The IT landscape is undergoing a fundamental shift to IT as a service (ITaaS), a model that requires a pool of compute, network, and storage resources that serve a wide range of applications and deliver a wide range of services. Innovations such as ONTAP are fueling this revolution.

NetApp solutions are user friendly, easy to manage, and quick to deploy and offer increased availability while consuming fewer IT resources. This means that they dramatically lower lifetime TCO. Whereas others manage complexity, NetApp eliminates it. A NetApp solution includes hardware in the form of controllers and disk storage and the NetApp ONTAP software.

NetApp offers the NetApp Unified Storage Architecture. The term "unified" refers to a family of storage systems that simultaneously support SAN and NAS across many operating environments such as VMware, Windows, and UNIX. This single architecture provides access to data by using industry-standard protocols, including NFS, CIFS, iSCSI, FCP, and FCoE. Connectivity options include standard Ethernet (100/1000 or 10GbE) and FC (2, 4, 8, or 16Gbps).

This FlexPod Datacenter solution includes the NetApp FAS8000 series unified scale-out storage systems. Powered by ONTAP, the FAS series unifies SAN and NAS storage infrastructures. The FAS8000 features a multiprocessor Intel chipset and leverages high-performance memory modules, NVRAM to accelerate and optimize writes, and an I/O-tuned PCIe gen3 architecture that maximizes application throughput. The FAS8000 series comes with integrated UTA2 ports that support 16Gb FC, 10GbE, or FCoE.

NetApp storage solutions provide redundancy and fault tolerance through clustered storage controllers, hot-swappable redundant components (such as cooling fans, power supplies, disk drives, and shelves), and multiple network interfaces. This highly available and flexible architecture enables customers to manage all data under one common infrastructure while achieving mission requirements. The NetApp Unified Storage Architecture allows data storage with higher availability and performance, easier dynamic expansion, and greater ease of management than any other solution.

ONTAP 9

With ONTAP 9, NetApp provides the next generation of enterprise-ready, unified scale-out storage. Developed from a solid foundation of proven ONTAP technology and innovation, ONTAP 9 is the basis for large virtualized shared storage infrastructures, which are architected for nondisruptive operations over the lifetime of the system. Controller nodes are deployed in HA pairs that participate in a single storage domain or cluster.
NetApp ONTAP scale-out is one way to respond to growth in a storage environment. All storage controllers have physical limits to their expandability. The number of CPUs, number of memory slots, and amount of space for disk shelves dictate the maximum capacity and controller performance. If more storage or performance capacity is needed, it might be possible to add CPUs and memory or install additional disk shelves, but ultimately the controller becomes completely populated, with no further expansion possible. At this stage, the only option is to acquire another controller.

**Scale-Out**

The use of scale-out means that as the storage environment grows, additional controllers are added seamlessly to the resource pool residing on a shared storage infrastructure. Host and client connections as well as datastores can move seamlessly and nondisruptively anywhere in the resource pool. Therefore, existing workloads can be easily balanced over the available resources, and new workloads can be easily deployed. Technology refreshes (replacing disk shelves or adding or completely replacing storage controllers) are accomplished in an environment that remains online and continues serving data.

The benefits of scale-out include the following:

- Nondisruptive operations
- The ability to add additional workloads with no effect on existing services
- Operational simplicity and flexibility

Although scale-out products have been available for some time, these products were typically subject to one or more of the following shortcomings:

- Limited protocol support (NAS only)
- Limited hardware support (supported only a particular type of storage controller or a very limited set)
- Little or no storage efficiency (thin provisioning, deduplication, and compression)
- Little or no data replication capability

Although these products are well positioned for certain specialized workloads, they are less flexible, less capable, and not robust enough for broad deployment throughout the enterprise.

As is depicted in Figure 3, ONTAP is the first product to offer a complete scale-out solution with an adaptable, always-available storage infrastructure for today’s highly virtualized environment. An ONTAP system can scale up to 24 nodes, depending on platform and protocol, and can contain different disk types and controller models in the same storage cluster.

**Figure 3) ONTAP.**
Note: Storage virtual machines (SVMs) were formerly known as Vservers.

Nondisruptive Operations

The move to a shared infrastructure has made it nearly impossible to schedule downtime to accomplish routine maintenance. ONTAP is designed to eliminate the planned downtime needed for maintenance operations and lifecycle operations as well as the unplanned downtime caused by hardware and software failures.

Three standard tools make this elimination of downtime possible:

- **NetApp DataMotion™ for Volumes (vol move).** Allows data volumes to be moved from one aggregate to another on the same or a different cluster node.
- **Logical interface (LIF) migrate.** Allows the physical Ethernet interfaces in ONTAP to be virtualized. LIF migrate also allows LIFs to be moved from one network port to another on the same or a different cluster node.
- **Aggregate relocate (ARL).** Allows complete aggregates to be transferred from one controller in an HA pair to the other without data movement.

Used individually and in combination, these tools enable customers to nondisruptively perform a full range of operations, from moving a volume from a faster to a slower disk all the way up to a complete controller and storage technology refresh.

As storage nodes are added to the system, all physical resources—CPUs, cache memory, network I/O bandwidth, and disk I/O bandwidth—can easily be kept in balance. NetApp ONTAP systems enable users to:

- Add or remove storage shelves (over 23PB in an 8-node cluster and up to 69PB in a 24-node cluster).
- Move data between storage controllers and tiers of storage without disrupting users and applications.
- Dynamically assign, promote, and retire storage while providing continuous access to data as administrators upgrade or replace storage.

These capabilities allow administrators to increase capacity while balancing workloads and can reduce or eliminate storage I/O hot spots without the need to remount shares, modify client settings, or stop running applications.

Availability

Shared storage infrastructure provides services to thousands of virtual desktops. In such environments, downtime is not an option. The NetApp AFF solution eliminates sources of downtime and protects critical data against disaster through two key features:

- **High availability.** A NetApp HA pair provides seamless failover to its partner in case of hardware failure. Each of the two identical storage controllers in the HA pair configuration serves data independently during normal operation. During an individual storage controller failure, the data service process is transferred from the failed storage controller to the surviving partner.
- **NetApp RAID DP® data protection technology.** During any virtualized desktop deployment, data protection is critical because any RAID failure might disconnect hundreds to thousands of end users from their desktops, resulting in lost productivity. RAID DP provides performance comparable to that of RAID 10, and yet it requires fewer disks to achieve equivalent protection. In contrast to RAID 5, RAID DP provides protection against double disk failure, which can protect against only one disk failure per RAID group. Therefore, RAID DP provides RAID 10 performance and protection at a RAID 5 price point.
NetApp Advanced Data Management Capabilities

This section describes the storage efficiencies, multiprotocol support, and replication capabilities of the NetApp AFF solution.

Storage Efficiencies

The NetApp ONTAP solution includes built-in thin provisioning, inline and postprocess data deduplication, inline and postprocess data compression, inline data compaction, and zero-cost cloning with NetApp FlexClone® data replication technology. These features offer multilevel storage efficiency across virtual desktop data, installed applications, and user data. This comprehensive storage efficiency package enables a significantly reduced storage footprint for virtualized desktop implementations, with a capacity reduction of up to 10:1, or 90%. This analysis is based on existing customer deployments and NetApp solutions lab verification.

Several features make this level of storage efficiency possible:

- **Thin provisioning.** Allows multiple applications to share a single pool of on-demand storage. This feature eliminates the need to provision more storage for an application if another application still has plenty of allocated but unused storage.

- **Deduplication.** Saves space on primary storage by removing redundant copies of blocks in a volume that hosts hundreds of virtual desktops. This process is transparent to the application and the user, and it can be enabled and disabled on the fly. With Data ONTAP® 8.3.2 and later, inline deduplication of in-memory data is enabled by default, and postprocess deduplication is also available. To eliminate any potential concerns about postprocess deduplication causing additional wear on the SSDs, NetApp provides up to a five-year warranty for all SSDs (three-year standard plus an additional two-year extended warranty), with no restrictions on the number of drive writes.

- **Inline compression.** Data compression reduces the disk space required, regardless of storage protocol, application, or storage tier. Inline compression also reduces the data that must be moved to SSDs, thereby reducing the wear on SSDs.

- **Data compaction.** Data compaction enables even greater space savings on certain types of data. When data writes from the host are smaller than the default 4k block size on the storage system, ONTAP can compact multiple sub-4k writes into a single physical block on disk, producing significant capacity savings.

- **FlexClone.** Because NetApp Snapshot® copies are created at the FlexVol® volume level, they cannot be directly leveraged within an OpenStack context. This is because a Cinder user requests a Snapshot copy be taken of a Cinder volume (not the containing FlexVol volume). Because a Cinder volume is represented as either a file on NFS or an iSCSI LUN, the way that Cinder snapshots are created is through the use of NetApp FlexClone technology. By leveraging the FlexClone technology to provide Cinder snapshots, it is possible to create thousands of Cinder snapshots for a single Cinder volume.

NetApp ONTAP provides several additional features that can be leveraged in a private cloud environment. Some of these features are:

- **NetApp Snapshot copies.** Manual or automatically scheduled point-in-time copies that write only changed blocks, with no performance penalty. Snapshot copies consume minimal storage space because only changes to the active file system are written. Individual files and directories can easily be recovered from any Snapshot copy, and the entire volume can be restored back to any Snapshot state in seconds.

- **LIF.** A logical interface that is associated with a physical port, interface group (ifgrp), or VLAN interface. More than one LIF can be associated with a physical port at the same time. There are three types of LIFs:
  - NFS LIF
  - iSCSI LIF
FC LIF

LIFs are logical network entities that have the same characteristics as physical network devices but are not tied to physical objects. LIFs used for Ethernet traffic are assigned specific Ethernet-based details such as IP addresses and iSCSI-qualified names and are then associated with a specific physical port capable of supporting Ethernet. LIFs used for FC-based traffic are assigned specific FC-based details such as worldwide port names and are then associated with a specific physical port capable of supporting FC or FCoE. NAS LIFs can be nondisruptively migrated to any other physical network port throughout the entire cluster at any time, either manually or automatically (by using policies). SAN LIFs rely on multipath input/output (MPIO) and Asymmetric Logical Unit Access (ALUA) to notify clients of any change in the network topology.

- **Storage virtual machine.** An SVM is a secure virtual storage server that contains data volumes and one or more LIFs through which it serves data to the clients. An SVM securely isolates the shared virtualized data storage and network and appears as a single dedicated server to its clients. Each SVM has a separate administrator authentication domain and can be managed independently by an SVM administrator.

### Multiprotocol Support

By supporting all common NAS and SAN protocols on a single platform, NetApp Unified Storage enables the following functions:

- Direct access to storage by each client
- Network file sharing across different platforms without the need for protocol-emulation products such as SAMBA, NFS Maestro, or PC-NFS
- Simple and fast data storage and data access for all client systems
- Fewer storage systems
- Greater efficiency from each system deployed

ONTAP 9 can support several protocols concurrently on the same storage system. Unified storage is important in private cloud deployments, where servers may utilize SAN protocols for boot volumes or high-performance data LUNs and NAS protocols for shared file system access, all within the same application stack. The following protocols are supported on NetApp ONTAP systems:

- NFS v3, v4, and v4.1 (including pNFS)
- iSCSI
- FC
- FCoE
- CIFS

### Platform9 Managed OpenStack

Platform9 Managed OpenStack is a fully SaaS-managed offering from OpenStack. Version 2.6 of Platform9 Managed OpenStack is based on the Newton release of OpenStack.

### SaaS-Managed Solution

OpenStack is the de-facto open-source private cloud computing standard with open APIs and is defined by enormous support from the open-source community. At the core of Platform9’s Managed OpenStack solution is a fully SaaS-managed architecture, eliminating the need to install, configure, troubleshoot, or upgrade the OpenStack cloud management plane. It can be simply paired and configured with the FlexPod infrastructure. Because it is a SaaS solution, Platform9 Managed OpenStack includes proactive 24x7 monitoring of the OpenStack control plane, with proactive 24x7 support for rapid issue detection and remediation. A unified management experience is provided across FlexPod, legacy hardware and virtualized infrastructure, and public clouds such as AWS and GCE, all with the OpenStack API and UI.
Platform9 Managed OpenStack with FlexPod simplifies the implementation of cloud, offering the following advantages:

- Platform9’s SaaS-managed architecture eliminates the need to install, configure, or upgrade any complex management software. Simply add and configure FlexPod in a few simple steps, drastically decreasing reducing time to value.
- SaaS deployment means proactive 24x7 monitoring of OpenStack by Platform9, with proactive 24x7 support for rapid issue detection and remediation built into the solution.
- Seamless and nondisruptive rolling upgrade of OpenStack components
- Significantly reduced operational cost, complexity, and TCO, with a simplified yet feature-rich user experience.
- Single-interface management across FlexPod and public clouds such as AWS, all with the OpenStack API and UI, enabling a true hybrid cloud experience.

**DevOps Agility**

DevOps and IT teams can both utilize Platform9 Managed OpenStack’s open and programmatic access to infrastructure for a true DevOps environment. Tenants can be created for individual teams, such as dev/test, QA, and more. Quotas and VM leases enable teams to self-serve, while optimizing the use of compute and storage resources.

Developers are likely to use the Platform9 user interface to get started and for ad-hoc operations. However, beyond the initial use of the Platform9 user interface, they are more likely to utilize the APIs to quickly and programmatically automate the development, test, and release pipeline. Platform9 simplifies this process and with intuitive DevOps test automation:

- Platform9 Managed OpenStack’s functionality is available using OpenStack’s REST APIs, which are documented here: [http://docs.platform9.com/](http://docs.platform9.com/).
- Being based on OpenStack enables DevOps teams to use libraries such as jclouds or Libcloud to integrate their development pipeline with Platform9 hybrid cloud.
- Development teams can reuse existing support in virtually any major automation framework to integrate the development pipeline with Platform9. These include Puppet OpenStack Provisioner, Chef’s knife CLI, Ansible’s Nova Compute Module, and SaltStack’s OpenStack Module.

Self-service is at the core of all DevOps and advanced IT ops teams. Platform9 Managed OpenStack provides a self-service portal, enabling on-demand access to shared infrastructure. Platform9 has an extremely friendly user interface, making it easy for IT teams to provide:

- Rapid provisioning for the creation and deployment of virtual machines instantaneously
- Web-based access to your virtual machines from anywhere using the web interface
- Collaboration for the capture and sharing of virtual machine configurations easily, both within a team and across teams
- VM configuration manager for customization of virtual machine instances to perform operations such as injecting a script, starting an agent, injecting security keys, and so on, using cloud-init

Platform9 Managed OpenStack provides agility to DevOps and IT teams and makes it easy to provide simple, yet policy-based access to resources:

- Quota-based allocation portions out different pools of capacity to different tenants, so teams have access to the resources they need while IT maintains overall control.
- Role-based access makes it easy to assign users with privileges based on their role.

As a SaaS-managed solution, Platform9 Managed OpenStack is an enterprise-grade, highly available managed offering of OpenStack. Platform9’s unique architecture hosts the OpenStack control plane from a Platform9-hosted cloud as a SaaS solution. The control plane consists of all the API endpoints such as nova-api, cinder-api, and glance-api. Organizations looking to use Platform9 Managed OpenStack with
FlexPod simply need to register their servers with the SaaS OpenStack control plane. This simple registration process takes only a few minutes and eliminates the cost and complexity of installing, configuring, and maintaining OpenStack.

After being registered, Platform9 Managed OpenStack transforms FlexPod into a fully functional OpenStack cloud by configuring compute, storage, and network nodes on Cisco UCS servers based on administrator-defined policies. The solution features several benefits:

- **Time to value.** The FlexPod OpenStack cloud can be fully deployed and operational within an hour, instead of days or weeks.
- **SaaS management for lower TCO.** Unlike do-it-yourself or shrink-wrapped software, Platform9’s offering is fully SaaS managed: the cloud platform is monitored 24x7 for issues, problems are proactively detected and communicated, and patches and upgrades are delivered as SaaS. The result is a cloud that is dramatically easier to operate and scale, with up to 80% reduced TCO.
- **Single-interface hybrid cloud.** Platform9 Managed OpenStack includes fully integrated support for Omni, which allows OpenStack to manage both private and public clouds through a single interface. Omni, which is a big-tent OpenStack project, fully supports integration with AWS with upcoming integrations for Google Cloud Platform and Microsoft Azure. This solution enables single-interface management across public and private infrastructure, with a unified self-service portal and unified policy management for capacity allocation and quota management.
- **Enterprise readiness.** Platform9 Managed OpenStack is fully integrated with common enterprise solutions. Single sign-on systems such as Active Directory, Okta, or other SAML-based solutions are ready to configure. Multiple data centers or regions can be managed from a single interface. Lease policies enable more efficient use of capacity, and audit/notification integrations enable integration with any enterprise NOC.
- **No lock-in.** All of these benefits are provided through refstack-compatible OpenStack APIs and UI, which means that there is zero vendor lock-in. In addition, it also means a variety of DevOps tools such as configuration management (puppet, chef, salt, ansible), CI/CD (Jenkins), and integration libraries (jcloud, libcloud, fog, knife) are all compatible straight out of the box.

**Container Ready**

In the same user interface and open-source framework, Platform9 also offers Managed Kubernetes for enterprise teams working with containers. Kubernetes is the leading open-source framework for container orchestration and was built with solving large-scale enterprise application problems in mind. In the same philosophy as Managed OpenStack, Platform9 offers SaaS-managed Kubernetes, where deployment, maintenance, and monitoring are handled by Platform9.

### 2 Deployment and Management of Platform9 OpenStack on FlexPod

This solution provides customers with the benefits of OpenStack as a dedicated private cloud, with none of the risks associated with OpenStack administration. Installation, management, and monitoring are provided as a service by Platform9, and the customer simply manages the virtual infrastructure through a web-based management portal.

#### 2.1 Technology Requirements

This section covers the technology requirements for the deployment of Platform9 OpenStack on FlexPod converged infrastructure.
Hardware Requirements

Table 1 lists the hardware components that are required to implement the use case.

Table 1) FlexPod OpenStack hardware requirements.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS 6200 Series fabric interconnects</td>
<td>FI 6248UP</td>
</tr>
<tr>
<td>Cisco UCS B200 blades</td>
<td>B200 M3 using Cisco UCS VIC 1240</td>
</tr>
<tr>
<td>Cisco UCS 5108 chassis</td>
<td>Cisco UCS-IOM 2208XP</td>
</tr>
<tr>
<td>Cisco Nexus 9000</td>
<td>Cisco Nexus 9396PX</td>
</tr>
<tr>
<td>NetApp FAS/AFF storage system</td>
<td>AFF8040</td>
</tr>
<tr>
<td>NetApp DS2246 disk shelves</td>
<td>Disk shelves populated with 400GB SSD</td>
</tr>
</tbody>
</table>

Software Requirements

Table 2 lists the software components that are required to implement the use case. The software components used in an implementation of the solution might vary based on customer requirements.

Table 2) FlexPod OpenStack software requirements.

<table>
<thead>
<tr>
<th>Software/Firmware</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td></td>
</tr>
<tr>
<td>Cisco UCS Manager</td>
<td>3.1(1e)</td>
</tr>
<tr>
<td>Networking</td>
<td></td>
</tr>
<tr>
<td>Cisco NX-OS</td>
<td>7.0(3)i2(2a)</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
</tr>
<tr>
<td>ONTAP</td>
<td>9</td>
</tr>
<tr>
<td>NetApp ONTAP licenses</td>
<td>Cluster base, NFS, iSCSI, FlexClone</td>
</tr>
<tr>
<td>NetApp Unified Cinder driver</td>
<td>OpenStack Liberty</td>
</tr>
<tr>
<td>Hypervisor/Operating System Software</td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>7.2</td>
</tr>
</tbody>
</table>

2.2 Deployment Procedures

Platform9 Installation Prerequisites

Verify that the following prerequisites are in place before beginning the installation:

- Request an account with Platform9. Each Platform9 customer receives a unique Platform9.net subdomain to be used as the OpenStack endpoint and management portal. In this validation, the subdomain is netapp-flexpod.platform9.net.
- The servers are installed with RHEL 7.2 and are updated with the latest patches.
The servers can reach the HTTPS management plane at netapp-flexpod.platform9.net:443. Modify network routing and firewall configurations as required.

For details about the Platform9 installation prerequisites, go to:


**FlexPod Deployment Procedures**

The basic infrastructure setup for this solution was completed using the deployment procedure found in the FlexPod Datacenter with Cisco UCS 6300 Fabric Interconnect and VMware vSphere 6.0 U1 Deployment Guide.

**Note:** This is an IP-based solution. It does not require the configuration of the FC or FCoE protocol described in the deployment guide. Specific configurations for this solution are documented in the sections that follow.

In addition to the basic infrastructure deployment, the following details were configured:

- Cisco Nexus configuration
- Cisco UCS configuration
- NetApp ONTAP configuration

**Cisco Nexus Configuration**

The basic configuration of the Cisco Nexus switch was completed using the FlexPod Datacenter with Cisco UCS 6300 Fabric Interconnect and VMware vSphere 6.0 U1 Deployment Guide. The following VLANs are configured to support this solution:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI A and iSCSI B</td>
<td>Supports boot LUNs for servers</td>
</tr>
<tr>
<td>NFS</td>
<td>Supports OpenStack Cinder block storage services and NFS backend for Glance</td>
</tr>
<tr>
<td>OOB-Management</td>
<td>Provides management connectivity for all devices</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Acts as underlay network for neutron tenant networks</td>
</tr>
<tr>
<td>External</td>
<td>Provides external connectivity from nova instances</td>
</tr>
</tbody>
</table>

**Cisco UCS Configuration**

The basic configuration of Cisco UCS was completed using the FlexPod Datacenter with Cisco UCS 6300 Fabric Interconnect and VMware vSphere 6.0 U1 Deployment Guide. The following specific configurations were performed to support this solution:

- The service profiles for the Linux servers are configured for SAN boot using the iSCSI protocol.
- VLAN tagging is used to achieve network segmentation among different VLAN types.
- This solution is validated using individual vNICs dedicated to each VLAN with Cisco UCS fabric failover enabled for resiliency.
- Each service profile is configured with the vNICs associated with the fabric interconnects, as shown in Figure 4.
NetApp AFF8040 Configuration

The NetApp storage cluster configuration was completed using the FlexPod Datacenter with Cisco UCS 6300 Fabric Interconnect and VMware vsphere 6.0 U1 Deployment Guide. The following specific configurations were performed to support this solution:

1. Create VLANs for iSCSI boot and NFS traffic for Cinder and Glance. Add them to the appropriate broadcast domain.

```bash
network port modify -node <st-node01> -port a0a -mtu 9000
network port modify -node <st-node02> -port a0a -mtu 9000
network port vlan create -node <st-node01> -vlan-name a0a-<iscsi-a-vlan-id>
network port vlan create -node <st-node02> -vlan-name a0a-<iscsi-a-vlan-id>
network port vlan create -node <st-node01> -vlan-name a0a-<iscsi-b-vlan-id>
network port vlan create -node <st-node02> -vlan-name a0a-<iscsi-b-vlan-id>
network port vlan create -node <st-node01> -vlan-name a0a-<nfs-vlan-id>
network port vlan create -node <st-node02> -vlan-name a0a-<nfs-vlan-id>
broadcast-domain add-ports -broadcast-domain Jumbo <st-node01>:a0a-<nfs-vlan-id>,<st-node01>:a0a-<iscsi-a-vlan-id>,<st-node02>:a0a-<iscsi-b-vlan-id>,<st-node02>:a0a-<iscsi-a-vlan-id>,<st-node02>:a0a-<iscsi-b-vlan-id>
```

2. Create an infrastructure SVM.

```bash
vserver create -vserver infra-svm -rootvolume rootvol -aggregate aggr1_node01 -rootvolume-security-style unix
```

3. Create an operational SVM that provides FlexVol volumes corresponding to Cinder and Glance storage.

```bash
vserver create -vserver openstack-svm -rootvolume rootvol -aggregate aggr1_node01 -rootvolume-security-style unix
```

4. Add the data aggregates to the infra-svm aggregate list.

```bash
vserver modify -vserver infra-svm -aggr-list aggr1_node01,aggr1_node02
```

5. Add the data aggregates to the openstack-svm aggregate list.

```bash
vserver modify -vserver infra-svm -aggr-list aggr1_node01,aggr1_node02
```

6. Add the iSCSI data protocol for infrastructure SVM (for boot LUNs).

```bash
vserver remove-protocols -vserver infra-svm -protocols nfs cifs fcp ndmp
```

7. Add NFS data protocol for operational SVM.

```bash
vserver remove-protocols -vserver infra-svm -protocols iscsi cifs fcp ndmp
```
8. Enable iSCSI service on the infrastructure SVM.
   ```bash
vserver iscsi start -vserver infra-svm
   ```

9. Enable NFS protocol on the operational SVM.
   ```bash
nfs create -vserver openstack-svm -udp disabled
   ```

10. Enable advanced NFS options on the operational SVM.
    ```bash
vserver nfs modify -vserver openstack-svm -v4.0 enabled -v4.1 enabled -v4.1-pnfs enabled -vstorage enabled
   ```

11. Create a new rule for the infrastructure subnet in the default export policy.
    ```bash
vserver export-policy rule create -vserver openstack-svm -policyname default -ruleindex 1 -protocol nfs -clientmatch <nfs-subnet-cidr> -rorule sys -rwrule sys -superuser sys -allow-suid false
   ```

12. Assign the export policy to the operational SVM root volume.
    ```bash
volume modify -vserver openstack-svm -volume rootvol -policy default
   ```

13. Modify the default UNIX user’s group ID for the SVM’s root user from 1 to 0.
    ```bash
unix user-modify -vserver openstack-svm -user root -primary-gid 0
   ```

    ```bash
volume create -vserver infra-svm -volume iscsi_boot -aggregate aggr1_node01 -size 500GB -state online -policy default -space-guarantee none -percent-snapshot-space 0
volume create -vserver openstack-svm -volume cinder1 -user 1000 -group 1000 -aggregate aggr01_node01 -size 500GB -state online -policy default -junction-path /cinder1 -space-guarantee volume -percent-snapshot-space 0
volume create -vserver openstack-svm -volume cinder2 -user 1000 -group 1000 -aggregate aggr01_node02 -size 500GB -state online -policy default -junction-path /cinder2 -space-guarantee volume -percent-snapshot-space 0
volume create -vserver openstack-svm -volume cinder3 -user 1000 -group 1000 -aggregate aggr01_node03 -size 500GB -state online -policy default -junction-path /cinder3 -space-guarantee volume -percent-snapshot-space 0
volume create -vserver openstack-svm -volume glance -user 1000 -group 1000 -aggregate aggr01_node04 -size 500GB -state online -policy default -junction-path /glance -space-guarantee volume -percent-snapshot-space 0
   ```

   **Note:** The user and the group permissions for Cinder and Glance FlexVol volumes should match the `pf9user` and `pf9group` created on the KVM hosts. Although the default value is set to 1000, it can be modified later by checking the KVM hosts.

    ```bash
create efficiency on -vserver openstack-svm -volume glance
   ```

16. Create igroups for the boot LUNs.
    ```bash
igroup create -vserver infra-svm -igroup server01 -protocol iscsi -ostype linux -initiator <<<initiator-server01-a>>,<<initiator-server01-b>>
igroup create -vserver infra-svm -igroup server02 -protocol iscsi -ostype linux -initiator <<<initiator-server02-a>>,<<initiator-server02-b>>
igroup create -vserver infra-svm -igroup server03 -protocol iscsi -ostype linux -initiator <<<initiator-server03-a>>,<<initiator-server03-b>>
igroup create -vserver infra-svm -igroup server04 -protocol iscsi -ostype linux -initiator <<<initiator-server04-a>>,<<initiator-server04-b>>
   ```

17. Create boot LUNs for the Linux hosts.
1. To maintain stateless compute, RHEL 7.2 servers are booted from ONTAP LUNs using the iSCSI protocol, which requires configuration of boot options during initial installation.

2. To install RHEL 7.2, complete the following steps:

   1. Map the RHEL 7.2 server DVD ISO image file to the virtual media of the service profile. Boot the server and press the Tab key to prevent the default boot configuration.
2. Remove the Quiet option by pressing the backspace key and entering `rd.iscsi.ibft=1`.
3. Select the installation destination and click Done in the upper-right corner.
4. In the Network & Host Name pane, enter the host name and static management IP to be assigned for the server.
5. Click Begin Installation and set root password.
6. Click Reboot after the system has completed installation.
7. After the reboot, configure the network interfaces on all nodes with IP addresses on the appropriate network for each interface. Configure typical network settings such as DNS servers and domain names, default gateways, and so on.

Configuring Prerequisites for Platform9 OpenStack Installation

1. To install packages, subscribe to the Red Hat Subscription Manager tool for Platform9 agent.
   ```
   sudo subscription-manager register --username=userName --password
   ```
2. Attach to the Red Hat Enterprise Linux pool.
   ```
   subscription-manager attach --pool=myPool
   ```
3. Disable the repositories that are currently enabled.
   ```
   sudo subscription-manager repos --disable=
   ```
4. Enable the following repositories.
   ```
   sudo subscription-manager repos --enable=rhel-7-server-rpms --enable=rhel-7-server-extras-rpms --enable=rhel-7-server-rh-common-rpms
   ```
5. Update to the latest packages. Platform9 agents download any required package dependencies and install them to prepare each server to be part of OpenStack. This includes any libvirt/KVM package dependencies.
   ```
   yum -y update
   ```
6. Install and configure NTP on the servers. The hosts fail to authenticate with Platform9 services if the date/time settings are incorrect.
sudo yum -y install ntp

7. Substitute the NTP server to time.netapp.com in the /etc/ntp.ntp.conf.

    server time.netapp.com

8. Allow NTP outbound through the firewall and start the NTP daemon.

    sudo firewall-cmd --add-service=ntp -permanent
    sudo firewall-cmd --reload
    sudo systemctl start ntpd
    sudo systemctl enable ntpd

Platform9 Managed OpenStack Installation

After the infrastructure and host operating systems prerequisites are met, deployment of OpenStack is simple and can be performed with some assistance from Platform9 professional services personnel. Specific details of the installation are out of scope for this document, but the following basic tasks are completed:

- Platform9 OpenStack host agent is installed on each physical server. This agent registers with the Platform9 OpenStack management plane to make the host available for further configuration.

- Host roles are configured. This includes:
  - Glance image repository. Three hosts are configured to support Glance image library services in an HA configuration.
  - Cinder storage hosts. Three hosts are configured to support Cinder volume services in an HA configuration.

Cinder is configured with the NetApp unified driver for ONTAP with NFS during deployment. The NetApp copy offload tool is also configured for efficient instance creation.

- Neutron networking:
  - Routing mode: distributed virtual routing (DVR) or legacy mode. The default mode is DVR, in which each hypervisor is L3 capable and both east-west traffic and north-south traffic using floating IPs are handled directly at the hypervisor.
  - Configuration of DNS domain and forwarding
  - Number of DHCP servers
  - Network type: VXLAN based
  - Create mappings between virtual networks (VXLAN) and physical networks (VLAN)
  - Other customer-specific network configurations based on the preceding selections

- Hypervisor: All hosts are typically configured as hypervisor hosts, which allows them to support general VM workloads.

After the host roles and networks are configured, the Platform9 Managed OpenStack implementation is ready for production VM deployment.

2.3 Solution Validation

After deployment of the Platform9 Managed OpenStack solution on FlexPod, several tasks were performed to validate the correct operation and integration of the various services.

Creating a Tenant and User

This section describes the procedure to create a tenant and a user for the tenant created.

1. Log in to the Clarity UI using the public endpoint and administrator account set up by Platform9.

2. Verify that the KVM hosts are registered. Verify the roles by clicking the Infrastructure tab in the left pane and viewing the Assigned Roles column for the hosts.
**Note:** To make sure of highly available Cinder volume service and Glance image library, three instances of the services are deployed across three KVM hosts.

3. **Click Tenants & Users** in the navigation pane and follow the instructions to create a new tenant.

4. **Set the quotas for cores, RAM, and network.**

   **Note:** Quotas can be set to enforce limits on resource utilization specific to a region. For example, the quota for AWS region can be set to zero to prevent any AWS resource utilization.
5. Select the networks, flavors, and users associated with the tenant and then click Create Tenant.

6. Click Tenants & Users in the navigation pane and click the Users tab. Configure the user name and password, select the tenants, and then click Create User.
Uploading Image to Glance

To upload the image, complete the following steps:

1. Click Images in the navigation pane and then click the Download Prebuilt Images tab.
   This validation uses a prebuilt Centos 7.1 image with a cloud-init user.
2. Click Add New Image.
3. Log in to one of the nodes hosting the image library.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>IP Address</th>
<th>Path to Image Library Watch Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>kvm02.rtp.netapp.com</td>
<td>172.21.11.152</td>
<td>/var/lib/glance/images</td>
</tr>
<tr>
<td>kvm04.rtp.netapp.com</td>
<td>172.21.11.154</td>
<td>/var/lib/glance/images</td>
</tr>
<tr>
<td>kvm03.rtp.netapp.com</td>
<td>172.21.11.153</td>
<td>/var/lib/glance/images</td>
</tr>
</tbody>
</table>

4. Navigate to the Image Library folder and download the images.

    cd /var/lib/glance/images

    After the image is downloaded, it appears under the Images tab.
5. Click the Images tab and verify that the image listed has the correct size.

Creating an External Network for Outbound Internet Access

1. Click Networks in the navigation pane and then click Create New Network.

2. Enter details for creating the network.

   - **Network Type**: External Network
     - External Networks generally correspond to the physical networks in your Datacenter that are publicly routable/are enabled with access to Internet.
     - As an Administrator, you would want to supply one or more External Networks to Neutron so that:
       - Your Virtual Machines can route packets from the internal network to the internet (so they can ping google.com for eg)
       - You can assign Floating IPs to your Virtual Machine and have them publicly addressable from the internet (so you can run a web server that can be accessed from the internet for eg)
     - Refer to this [article](#) for more information.
   - **Network Name**: floating
   - **Admin state to start the network in**: UP
   - **Tenant**: service
   - **External Network Type**: VLAN (Tagged)
   - **VLAN ID**: 3274
   - **Physical Network**: external

3. Enter details about the subnet.
4. Create the network.

**Creating Tenant Network and Router**

As a tenant user (nonadmin), we need to configure the tenant with a network and routing to the external network.

1. Log in to Clarity as a nonadmin user created in the previous step (NetApp tenant).
2. Click Networks and then click Create New Network.
3. **Edit the subnet credentials.**

4. **Review the configuration and create the network.**
5. **Click Networks > Routers > Create New Router.**
6. **Associate it with the external network created in the previous step (floating) and create the router.**
7. Click Router, Interfaces, Create New Interface.
8. Select the tenant network created in the previous step.

This enables outbound connectivity to your instances through the router.

Creating a Bootable Cinder Volume for Persistent Instances

Most virtual machines in OpenStack use ephemeral storage, typically direct-attached storage. However, it is possible to use the storage provider, in this case NetApp, to provide base disks for the instances.

1. Click Volumes and Snapshots in the navigation pane and click Create New Volume.
2. In the Volume Source section, select Image from the “Create from” options. Select the image and click Next.
3. Enter a name and size for the volume. Select the Bootable option.

4. Create the volume. This volume can now be used to boot the virtual machines.

**Importing an SSH Key for Logging In to the Instance**

1. Click Access & Security in the navigation pane and click Import Key.
2. Name the key, copy the SSH public key into the text box, and import the key.

**Note:** Instructions for creating a new SSH key pair are provided on the right side.
Creating an Instance

1. Click Instances in the navigation pane and click New VM Instance.
2. Select the image source for Volume and select the bootable volume.

3. Assign m1.small flavor, tenant network, and SSH key created in section Importing an SSH Key for Logging In to the Instance.

4. (Optional) To log in using console, you need to create a cloud-init user.
   To do this, navigate to the Customize page, select Use cloud-init, and enter the following script:

   ```
   #cloud-config
   password: winterwonderland
   chpasswd: { expire: False }
   ssh_pwauth: True
   disable_yc2_metadata: True
   runcmd:
     - ['sh', '-c', 'echo "Hello World from PF9" > /tmp/pf9.txt']
   ```

5. Click Next and create an instance.

3  Managing AWS Resources with Platform9 Clarity UI

In addition to managing on-site OpenStack resources, the Platform9 Clarity UI can also manage AWS public cloud resources.

3.1  Technology Requirements

This use case requires an Amazon Web Services account with permissions to create and manage AWS virtual infrastructure.
3.2 Deployment Procedures

Adding an AWS Region to the Clarity UI

To add an AWS region to the Clarity UI, complete the following steps:

1. Submit the customer’s support request for a new region to Platform9.
   Platform9 creates the new region, which appears in the Region drop-down list on the top-right corner of the UI.

2. After the region is added, all included resources can be managed from the Clarity UI.

Configuring the AWS Region

To configure the newly added AWS region, complete the following steps:

1. Select the new AWS region from the Region drop-down list.
2. Click Infrastructure in the left pane.
3. Click Edit AWS Credentials.
4. Enter the access key ID and secret key associated with the AWS account.

Platform9 detects the resources that already exist in your AWS account and populates these items in the Clarity UI. For example, existing AMI, VMs, and networks are visible in the Clarity UI.

5. An external network is created by default.
3.3 Solution Validation

After the AWS region is added and configured, several tasks need to be performed to validate the correct operation and integration of the various services:

- A private network was created using the Clarity UI using the preceding instructions for creating a tenant network. The AWS console was checked to verify that a new VPC is created with the corresponding subnets.
- An instance was created using the Clarity UI, and the AWS console was checked to verify the new instance.
- A volume was created, and a new EBS volume was confirmed in the AWS console.

4 Managing VMware vSphere Resources with Platform9 Clarity UI

VMware vSphere is the industry-leading server virtualization platform, and many customers already leverage vSphere in their data centers. In addition to OpenStack and AWS, Platform9 supports managing vSphere environments from the Platform9 Clarity UI. This allows customers to manage several different hypervisor/virtualization environments from the same management plane and provides the ability to deploy workloads across any platform from the same interface.

4.1 Technology Requirements

VMware vSphere integration with Platform9 was validated using additional blades in the same FlexPod infrastructure used to validate the Platform9 OpenStack deployment. This further shows the flexibility of FlexPod, with both OpenStack and vSphere running in the same physical infrastructure.

Hardware Requirements

Table 3 lists the hardware components used to validate the use case. The hardware components used in any implementation of the solution might vary based on customer requirements.

Table 3) FlexPod OpenStack hardware requirements.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS 6200 Series fabric interconnects</td>
<td>FI 6248UP</td>
</tr>
<tr>
<td>Cisco UCS B200 blades</td>
<td>B200 M3 using Cisco UCS VIC 1240</td>
</tr>
<tr>
<td>Cisco UCS 5108 chassis</td>
<td>Cisco UCS-IOM 2208XP</td>
</tr>
<tr>
<td>Cisco Nexus 9000</td>
<td>Cisco Nexus 9396PX</td>
</tr>
<tr>
<td>NetApp FAS/AFF storage system</td>
<td>AFF8040</td>
</tr>
<tr>
<td>NetApp DS2246 disk shelves</td>
<td>Disk shelves populated with 400GB SSD</td>
</tr>
</tbody>
</table>

Software Requirements

Table 4 lists the software components that were used to validate the use case. The software components used in any implementation of the solution might vary based on customer requirements.

Table 4) FlexPod OpenStack software requirements.

<table>
<thead>
<tr>
<th>Software/Firmware</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td></td>
</tr>
</tbody>
</table>
### 4.2 Deployment Procedures

The basic infrastructure setup for this solution was completed by using the deployment steps found in the *FlexPod Datacenter with Cisco UCS 6300 Fabric Interconnect and VMware vSphere 6.0 U1 deployment guide*.

**Platform9 Installation Prerequisites**

For the purposes of this validation, a basic HA and DRs-enabled cluster was created according to the Platform9 installation prerequisites.

Specific details regarding Platform9 installation prerequisites for VMware vSphere can be found at [https://platform9.com/support/pre-requisites-platform9-openstack-vmware-vsphere/](https://platform9.com/support/pre-requisites-platform9-openstack-vmware-vsphere/).

**Adding a vSphere Region to the Clarity UI**

1. The customer requests a new region to manage by submitting a support request to Platform9.
2. Platform9 creates the new region, which appears in the Region drop-down list in the top-right corner of the UI.
3. After the region is added, all included resources can be managed from the Clarity UI.

**Configuring the vSphere Region**

To complete configuration of the vSphere region, the following steps were completed:

1. A `pf9_user` was created in vSphere with the appropriate roles as listed in the prerequisites. This user was used to log in to the vSphere environment to perform the remaining steps.
2. Similar to downloading Platform9 agent in case of Linux/KVM. A Platform9 OVA for managing vSphere was downloaded and deployed as a VM (available from Platform9's clarity UI, under Manage VMware Gateway). The OVA configuration includes:
   a. Configuring the vSphere endpoint (vCenter)
   b. Supplying vSphere authentication credentials
   c. Specifying the external and private VM networks to be used

**Note:** Platform9 managed vSphere also supports the use of additional storage optimization features such as the use of VAAI plug-in.

### 4.3 Solution Validation

After the Platform9 OVA is successfully deployed, all existing vSphere resources are visible in the Clarity UI. To validate the integration, several tasks were performed:

- A VM was created from the Clarity UI, and its outbound network connectivity was confirmed.
- The vSphere console was checked to confirm the new VM and its network configuration.
- The VM console was accessed through the Clarity UI interface.

### 5 OpenStack Upgrade

Platform9 Managed OpenStack provides the best-in-class maintenance and support for OpenStack. Platform9 Managed OpenStack goes through extensive testing for each major and minor version upgrade of both OpenStack and Platform9 components.

The Platform9 operations team will reach out to your designated team members about maintenance window and upgrade details, including bug fixes and features releases. Upon agreement, the Platform9 operations team will schedule an upgrade, depending on the number of servers and regions in an environment, Platform9 will do a rolling upgrade of OpenStack and its components. The experience is hassle free and doesn't affect the running workloads. A Platform9 control plane that includes OpenStack API components is temporarily unavailable for 10 to 30 minutes during the upgrade window. After the upgrade is completed, a notification displays, as shown in Figure 5.

Figure 5) OpenStack upgrade notification.

```
Hello,

Your Platform9 cloud platform has been scheduled for an upgrade to release 2.6. Maintenance will take place on *[DATE]*. Your cloud platform will be unavailable for 30 minutes. If you need to reschedule, please reply to this email.
```

### Conclusion

FlexPod with Platform9 Managed OpenStack provides customers with a robust and flexible private cloud framework that is managed like a public cloud. When VMware vSphere and Amazon Cloud resources are integrated, applications can be managed across public and private clouds by using a single management plane.
References

Additional information about this solution can be found in the following documents:

- Browser-based sandbox: https://platform9.com/sandbox/
- Platform9 Managed OpenStack for VMware vSphere: https://platform9.com/vmware
- Platform9 Managed OpenStack for Linux/KVM: https://platform9.com/kvm/
Refer to the **Interoperability Matrix Tool (IMT)** on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

**Copyright Information**

Copyright © 2017 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

**THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

**Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at [http://www.netapp.com/TM](http://www.netapp.com/TM) are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4595-DEPLOY-0517