NetApp Verified Architecture

NetApp Private Storage for Cloud

Amazon Web Services (AWS), Microsoft Azure, and Bluemix

Mark Beaupre, NetApp
March 2017 | NVA-0009 | Version 2.3

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Solution Overview

The NetApp® Private Storage (NPS) for Cloud NetApp Verified Architecture 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:

- NPS for Amazon Web Services (AWS)
- NPS for Microsoft Azure
- NPS for IBM Bluemix (formerly IBM SoftLayer)

1.1 Problem Statement

Today's organizations understand the economic and flexibility benefits of the public cloud. Many 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

Simultaneous Connectivity to Multiple Clouds

Customers can use the NPS for Cloud architecture described in this document to help them meet their data stewardship requirements as they move their compute resources to the public cloud.

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 deprovision network links, move data, or create additional copies of data for each cloud. In a network effect that is reminiscent of Metcalfe's Law (which states that a network's value is proportional to the square of the number of connected users), more cloud connection options result in a better IT value proposition.

NetApp's partnership with the colocation provider 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.
- **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, offers 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.

A vast majority of ITaaS users already leverage more than one cloud service provider today. NPS for Cloud builds on that trend and offers IT users even more flexibility to reap the benefits of a multicloud strategy in the enterprise.

1.2 Target Audience

This document is for IT people and decision makers who want to evaluate, sell, or deploy NPS for Cloud solutions that meet or exceed customer expectations and requirements. The following organizations benefit from this solution:

- **Software as a Service (SaaS) providers.** NPS for Cloud enables SaaS providers to diversify the use of public cloud compute and reduce the cost of their services. NPS for Cloud can also help address compliance requirements around data sovereignty.
- **Enterprise customers.** NPS for Cloud provides public cloud connectivity to NetApp storage, which can shift capital expenses to operating expenses while improving service delivery and availability for their business partners.
- **Public sector organizations.** For organizations that must use tax revenue as efficiently as possible, NPS for Cloud helps maximize the availability and security of public data and provides scalable, secure, and cost-efficient services to the citizens they serve.
- **Service providers who leverage public cloud compute to offer secure multi-tenant enterprise-class storage as a service (StaaS).** This new kind of provider connects customer-managed public cloud resources to NetApp storage that the service provider owns and manages.
- **NetApp partners looking to sell and deploy NPS for Cloud solutions to meet customers' business and technical requirements.** It is important for NetApp partners to understand the NPS for Cloud architecture.

1.3 Technology Solution

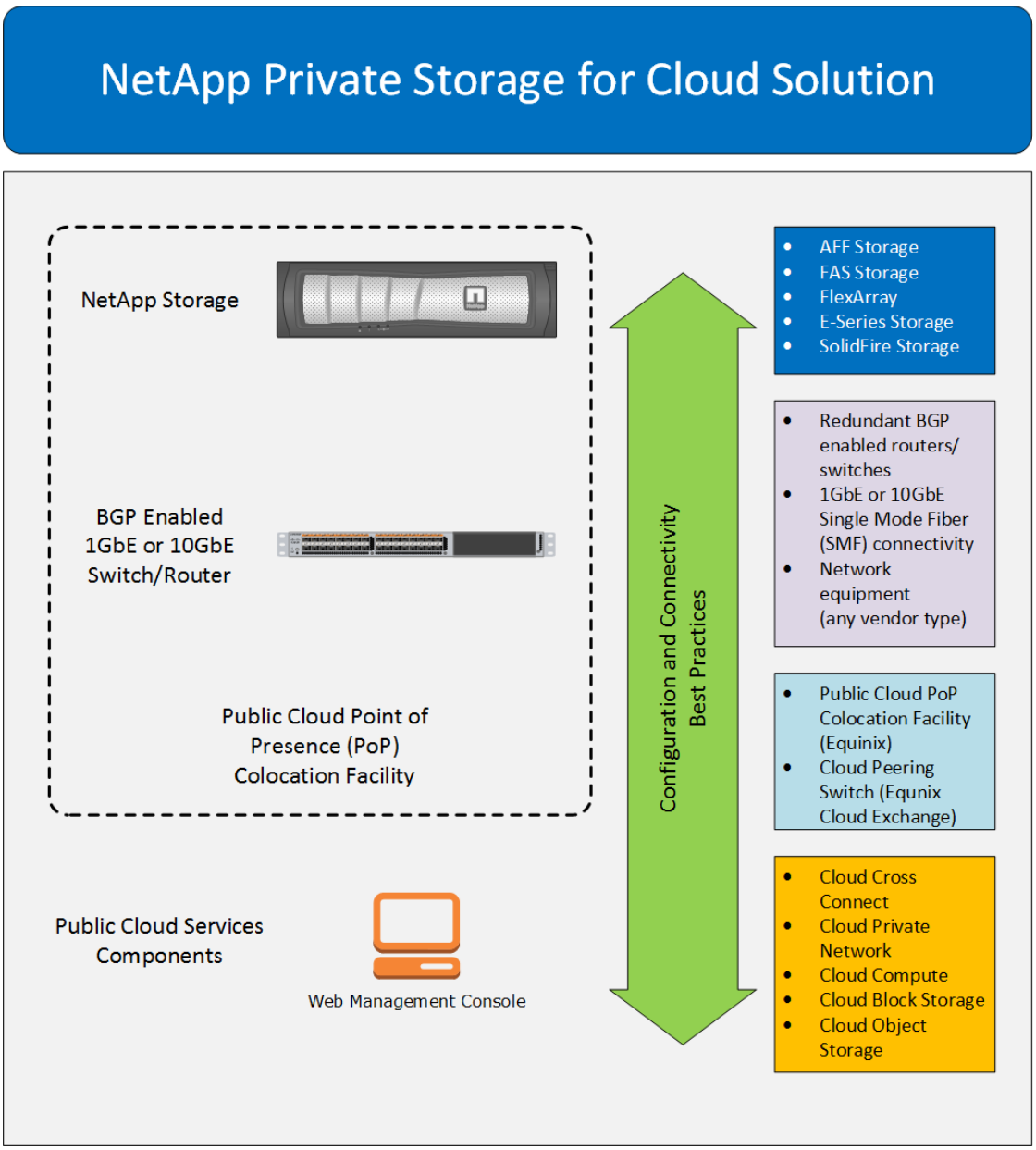
NPS for Cloud is a hybrid cloud architecture that includes the following major components:

- Public cloud virtual machines (VMs)
- Public cloud network
- Layer 3 network connection between NetApp storage and the public cloud
- Colocation facility located near the public cloud
- Colocation cloud exchange/peering switch
- Customer-owned network equipment that supports Border Gateway Protocol (BGP) routing protocols and Gigabit Ethernet (GbE) or 10GbE single-mode fiber (SMF) connectivity
- NetApp storage: AFF, FAS, E-Series, or SolidFire

The components of the solution are connected and configured in keeping with NetApp and public cloud provider best practices to provide a scalable architecture that supports a variety of application workloads. Figure 1 shows the components of the solution.

The NPS for Cloud solution architecture is flexible and can accommodate various customer requirements and application workloads. The flexibility of the architecture is a major strength of this solution.

Figure 1) NetApp Private Storage for Cloud solution components.



1.4 Hardware Requirements

Table 1 lists the hardware components required to implement the solution validated by NetApp. The hardware components used in any particular implementation of the solution might vary based on customer requirements.

Table 1) NetApp Private Storage for Cloud hardware requirements.

Hardware	Quantity
Storage Platform Option	
AFF (All Flash FAS) storage	Minimum of two AFF cluster nodes for high availability (HA)

Hardware	Quantity
	Note: You can use any AFF controller model in the solution. A two-node AFF8080 cluster was used to validate the solution.
FAS storage	Minimum of two FAS cluster nodes for high availability (HA) **Note:** You can use any FAS controller model in the solution. **Note:** You can use NetApp FlexArray® controllers in the solution. **Note:** A four-node FAS8060 cluster was used to validate the solution.
E-Series	Two E-series controllers for high availability (HA) **Note:** You can use any E-series model in the solution. **Note:** You can use Flash or SAS in the solution. **Note:** An EF-560 with two controllers was used to validate the solution.
SolidFire	Minimum of four SolidFire cluster nodes for high availability (HA) **Note:** You can use any SolidFire controller model in the solution. **Note:** A four-node SF19210 cluster was used to validate the solution.
Network	
Layer 3 network switch	• Minimum of one for basic connectivity • Two switches for HA **Note:** NetApp recommends having two switches to provide redundancy for network connectivity. However, the solution is functional with a single switch. **Note:** You can use any switch that supports 1Gbps or 10Gbps optical Ethernet connections in the solution. **Note:** Two Cisco Nexus 5548UP switches with Layer 3 modules were used to validate the solution.
Cross-connect to public cloud service provider or to cloud peering switch • 9/125 LC/SC duplex SMF optic cable	• Minimum of one connection • Two connections for HA **Note:** SMF cross connects are used for 1Gbps and 10Gbps connections. **Note:** Multiple cross connects can be aggregated.
Cloud peering switch • Equinix Cloud Exchange	• Minimum of one connection

Hardware	Quantity
	• Two connections to separate cloud peering switches for HA **Note:** A cloud peering switch is not required for all clouds.

1.5 Software Requirements

Table 2 lists the software components required to implement the specific solution validated by NetApp. The software components used in any particular implementation of the solution might vary based on customer requirements.

Table 2) NPS for Cloud software requirements.

Software	Version
Network	
Layer 3 network switch operating system (OS)	Any network switch OS can be used with the solution as long at the OS can support Layer 3 routing and Single Mode Fiber (SMF) optical cable connectivity. **Note:** Cisco NX-OS 5.2(1)N1(4) was used to validate the solution.
Layer 3 licenses	The Layer 3 software license must support Border Gateway Protocol. **Note:** A Cisco Nexus 5548UP N55-LAN1K9 Layer 3 license and N55-BAS1K9 Layer 3 base licenses were used to validate the solution.
Storage	
NetApp ONTAP® operating system (AFF and FAS)	Any version of ONTAP and both operating modes (7-Mode and clustered ONTAP) can be used with the solution. **Note:** ONTAP 8.3.2 was used to validate the solution with FAS. **Note:** ONTAP 9.0 was used to validate the solution with AFF.
E-Series SANtricity OS Controller Software	Any version of E-Series SANtricity OS Controller Software version 8.30.10.01 or later can be used with the solution. **Note:** E-Series SANtricity OS Controller Software version 8.30.10.01 was used to validate the solution.
SolidFire Element Operating System	Any version of SolidFire Element OS software version 9.0 or later can be used with the solution. **Note:** SolidFire Element OS 9.0 was used to validate the solution.
NetApp ONTAP storage licenses	Cluster, iSCSI, NFS, CIFS, SnapRestore®, FlexClone®, SnapMirror®, SnapVault®, SnapDrive®, SnapManager® suite, SnapCenter® suite **Note:** This solution does not support the Fibre Channel (FC) storage protocol. The solution supports all versions of NetApp host-side software (SnapDrive, SnapManager, and SnapCenter) that are listed in the NetApp Interoperability Matrix Tool.
NetApp OnCommand® software	All versions of the OnCommand suite that are listed in the NetApp Interoperability Matrix Tool work with this solution.

1.6 Storage Considerations

You can use any model of NetApp FAS, AFF, or E-series storage that is listed in the NetApp Interoperability Matrix Tool. SolidFire platforms that support Element OS 9.0 or later can be used.

As noted earlier, only TCP/IP-based storage protocols (NFS, CIFS, iSCSI) can be used to connect cloud VMs or bare metal servers to the NetApp storage.

All best practices for NAS protocols and NetApp storage apply with this solution. All best practices for iSCSI protocol apply, with the following considerations:

- Only guest-connected LUNs can be used with cloud VMs. There is no support for raw device–mapped or pass-through LUNs for cloud VMs.
- There is no benefit to creating multiple iSCSI virtual interfaces on cloud VMs because an administrator cannot guarantee that the virtual interfaces use separate physical adapters.

Note: Bluemix (SoftLayer) Bare Metal servers can be configured to run virtualization software (VMware, Hyper-V, etc.) and in this situation, RDMs, Passthrough LUNs, and SAN booting can be used with NPS.

NetApp Private Storage for Cloud and ONTAP Modes of Operation

The NPS for Cloud solution can be used with both ONTAP operating in 7-Mode and the ONTAP operating mode. Although ONTAP 7-Mode can be used, NetApp recommends using ONTAP. That is because public cloud networks and VMs can be coupled with NetApp storage virtual machines (SVMs), formerly known as Vservers, to provide support for secure multi-tenancy and greater availability than ONTAP 7-Mode can provide.

1.7 Solution Sizing and Performance Considerations

Network latency between the cloud VMs or servers and the NetApp storage must be identified. Certain application workloads are sensitive to latency, and architects must account for this performance factor in the solution.

The network switches in the colocation facility must be sized appropriately to accommodate the network bandwidth, protocol, and routing required by the solution. Network switches are sized according to the methodologies provided by the network switch vendors.

All NetApp storage performance sizing methodologies and tools are used to size the storage performance in this architecture. For assistance in sizing NetApp storage for application workloads used in this solution, consult a NetApp channel partner or a NetApp account team.

1.8 Network Considerations

Network connectivity between a public cloud service provider and NetApp is a critical part of the NPS for Cloud solution. The cross connect to the cloud provider can provide a low-latency, high-performance, dedicated network connection to the public cloud compute; however, customer requirements are met through proper network design.

Network Latency and Choosing the Correct Colocation Facility

Before implementing the solution, architects must determine the environment's application or service latency requirements. Some enterprise applications require no greater than 5ms of latency in the storage stack for certain types of input/output (I/O). Because the NPS for Cloud solution uses only TCP/IP-based storage protocols (NFS, CIFS, iSCSI), knowing the network latency is key to determining the right colocation facility for deploying the NetApp storage.

A major factor in network latency is the distance between the cloud compute and the colocation facility. Contact a NetApp channel partner or a NetApp account team to help determine which colocation facility is right for you.

Note: Network latency is determined by using Internet Control Message Protocol ping or the Traceroute tool.

Network Bandwidth

Architects should also determine the bandwidth requirements of the workloads or services used in the NPS for Cloud solution architecture. Insufficient network bandwidth can cause poor application or service performance.

Note: Saturated network links can be identified by using network monitoring tools or the Traceroute tool.

Network Redundancy

NetApp recommends that architects use redundant network connections and network switches and routers to help avoid an outage if an SMF connection or a network switch or router is lost in the customer colocation facility.

Because of its design, architects cannot control network redundancy within the public cloud. Redundant network connections to cloud VMs do not have a significant effect because it is impossible to control whether the virtual network interfaces use separate physical network interface cards within the cloud.

For the iSCSI protocol, NetApp recommends the following guidelines:

- Create multiple iSCSI logical interfaces (LIFs) on the NetApp SVM.
- Install NetApp MPIO DSM software on the cloud VM connected to the NetApp SVM.
- Establish separate sessions to each iSCSI LIF on the NetApp SVM.

If an iSCSI LIF loses network connectivity, or if an iSCSI session is lost, the NetApp MPIO DSM software maintains the connection to the iSCSI LUNs on the NetApp SVM.

Note: ONTAP iSCSI LIFs do not move to different physical network interfaces when connectivity is lost.

Network Connectivity

Physical connectivity from the customer-provided network equipment to the public cloud is established with a 9/125 duplex SMF optic cable. Architects must verify that the network equipment used in the solution can support this physical connectivity requirement.

Network connections to the cloud service provider network can come in different bandwidth sizes. Multiple connections of the same or different sizes can be used in the same environment. However, architects must verify that the network equipment used can support a mix of 1Gbps and 10Gbps network connections on the same switch or router.

1.9 Management

A variety of management tools are offered by public cloud, NetApp, and network equipment vendors.

Public Cloud

All public cloud providers provide manageability of their resources through an API as well as other tools, such as CLI, scripting languages, and web portals. The type and scope of manageability capabilities vary with each public cloud service provider.

NetApp Storage

The solution works with all NetApp management tools, including NetApp OnCommand, the NetApp PowerShell Toolkit (PSTK), NetApp System Manager, ONTAP CLI, ONTAP APIs, SolidFire Element OS CLI, and the SolidFire Element OS REST API.

Network Equipment

The manageability of the network equipment varies by vendor. At a minimum, all network equipment can be managed through a CLI and monitored through the Simple Network Management Protocol. Some vendors provide GUI-based tools, APIs, and Windows PowerShell cmdlets to manage the network equipment.

1.10 Business Continuity and Data Protection

Almost all NetApp data protection software can be installed on and can function on cloud VMs or servers, as long as the versions used are listed in the NetApp Interoperability Matrix Tool and the SolidFire Element OS documentation.

Note: NetApp, VMware, Xen, and Hyper-V host software does not function with public cloud VM services.

Note: NetApp, VMware, Xen, and Hyper-V host software functions with public cloud physical compute services (i.e. Bluemix Bare Metal Server service).

1.11 Use Case Summary

The NPS for Cloud solution architecture is very flexible; it can be adapted to various customer business and technical requirements. The following use cases are validated for the solution architecture:

- Analytics
- Primary workloads
- Development and test
- Cloudburst for peak workloads
- Disaster recovery (DR)

Note: The NPS for Cloud solution architecture is not limited to the use cases listed here. For detailed use cases, see section 5, “Use Cases for NetApp Private Storage for Cloud Solution.”

2 NetApp Private Storage for AWS

This section describes the solution architecture for the NPS for AWS.

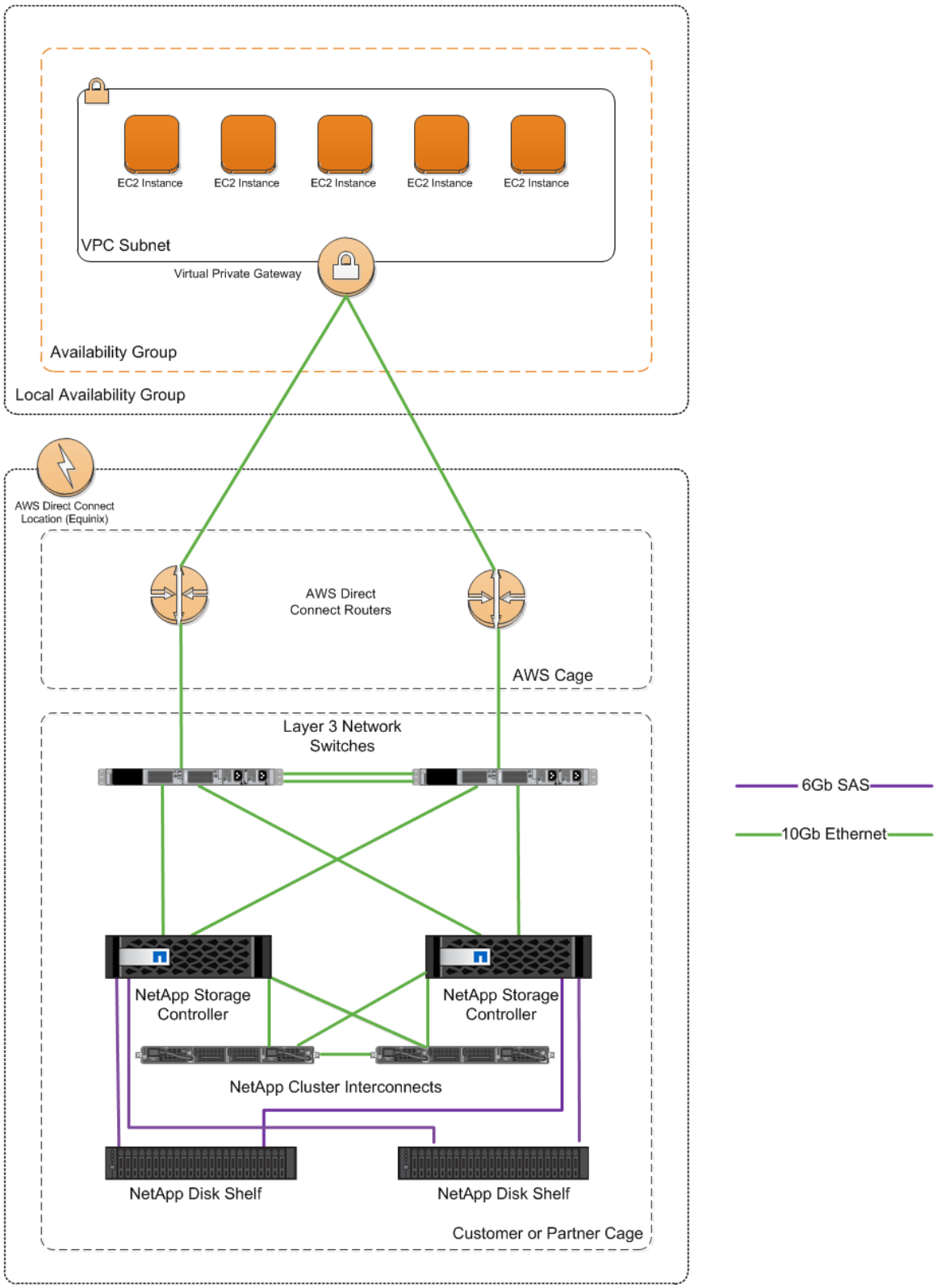
2.1 Solution Architecture Details

The NPS for AWS consists of the following major components:

- AWS Elastic Compute Cloud (EC2) VMs
- AWS Virtual Private Cloud (VPC) network
- AWS Direct Connect
- AWS Direct Connect colocation facility (Equinix)
- Cloud peering switch (Equinix Cloud Exchange) for sub-1Gbps connections
- 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 2 shows the architecture of NPS for AWS using FAS Storage with redundant Direct Connect network connections. Specific implementations will vary, depending on each customer's technical and business requirements.

Figure 2) NetApp Private Storage for AWS.



2.2 Solution Sizing and Performance Considerations

In addition to the general sizing guidelines for NetApp storage and the network for NPS for Cloud documented in section 1, “Solution Overview,” there are also specific guidelines for the sizing of AWS cloud compute resources.

AWS EC2 VMs (CPU, memory, network performance, and elastic block store [EBS] root volume size) must be sized appropriately for the applications and services used in this architecture. For more information about the EC2 sizing methodology, see Amazon Elastic Compute Cloud Documentation.

2.3 Network Considerations

In addition to the general network guidelines for NPS documented in section 1, “Solution Overview,” there are also specific guidelines for the network configuration for AWS.

Network Bandwidth Options

AWS Direct Connect network connections are available in 1Gbps and 10Gbps connection speeds using cross connect. Sub-1Gbps connections are available through the Equinix Cloud Exchange and Amazon network partners. For more information about available bandwidth connections for Direct Connect, see the AWS Direct Connect FAQs.

Network Architecture

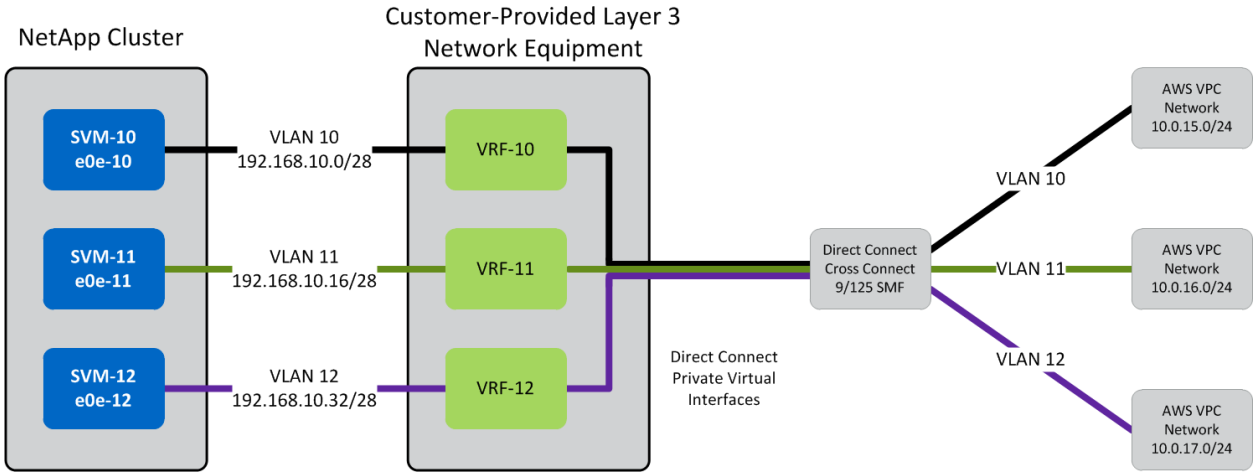
The network architecture for the NPS for AWS can support single tenancy or secure multi-tenancy. 802.1Q virtual local network (VLAN) tags are used by the AWS Direct Connect service to logically connect and route network traffic between the AWS VPC network and the customer network in the colocation facility where the NPS is located.

Secure multi-tenancy is a complicated topic that is not covered in detail in this document. However, if there is a requirement to have multiple AWS VPCs from different AWS accounts connected to the NetApp storage, 802.1Q virtual local area network tags can be used to segregate network traffic between the AWS cloud and the NetApp storage.

An AWS Direct Connect network connection supports multiple Direct Connect private virtual interfaces. Each private virtual interface uses a user-defined VLAN tag and uses BGP routes advertised by the customer network equipment.

Figure 3 illustrates the NPS for AWS network architecture.

Figure 3) NetApp Private Storage for AWS network architecture.



On the network switch, the BGP configuration is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.35 remote-as 64514
    address-family ipv4 unicast
  neighbor 169.254.253.45 remote-as 7224
    password 3 63611e150f52294d04dd44fe
    address-family ipv4 unicast
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to AWS, and the `169.254.253.45` IP address is the AWS peer IP address for the routing.

On the secondary network switch, the BGP configuration (Cisco NX-OS) is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.34 remote-as 64514
    address-family ipv4 unicast
  neighbor 169.254.253.49 remote-as 7224
    password 3 63611e150f52294d04dd44fe
    address
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to AWS, and the `169.254.253.49` IP address is the AWS peer IP address for the routing.

The VLAN network segregation is extended to the NetApp storage by using VLAN interfaces. For example, if the storage has a physical 10GbE interface labeled `e0e`, then a VLAN interface called `e0e-10` is created and an IP address from `192.168.10.0/28` is assigned to the VLAN interface.

AWS Direct Connect Link Aggregation Group

AWS Direct Connect supports the aggregation of up to 4 Direct Connect network connections using the Link Aggregation Control Protocol (LACP). Direct Connect Link Aggregation Groups (LAGs) require that all of the connections in the LAG are in the same Direct Connect location and are the same bandwidth (1Gbps or 10Gbps).

Direct Connect LAGs can be created from exising Direct Connect network connections, and new Direct Connect connections can be added to existing LAGs.

LAGs are used to provide additional throughput above a single Direct Connect network connection. Use cases where a lot of compute is connected to the NPS storage, such as analytics and database workloads, benefit from the increase in available bandwidth.

For more information, please review the AWS Direct Connect LAG documentation.

2.4 Virtual Machine Infrastructure

AWS EC2 VMs support Microsoft Windows, Linux, and Berkeley Software Distribution (BSD) operating systems.

The AWS EC2 hypervisor is a forked version of the Xen hypervisor that is heavily customized to run in the Amazon cloud.

Note: NetApp Xen integration tools do not work with AWS.

AWS offers preconfigured VM images (templates) that are called Amazon Machine Instances (AMIs). AWS also allows users to build their own AMIs, which can be shared with other AWS users. For more information about AMIs, refer to the AWS Marketplace.

AWS EC2 instances are available in different instance types that have different combinations of CPU, memory, and network throughput. In addition to the instance types, there are three different instance categories:

- **Spot instances** are generally the lowest-priced instances. The tradeoff is that the customer bids on how much to pay for an instance, but has little control over when the instance is deployed.
- **On-demand instances** have fixed prices and they generally start when they are deployed.
- **Reserve instances** are lower priced than on-demand instances and are guaranteed to start. These instances are useful when the solution is used for DR or for cloudburst scenarios.

There is no restriction on deploying virtualization infrastructure in the AWS Direct Connect colocation facility where the NetApp storage is located. The use of local virtualization is outside the scope of this document.

2.5 Operating Systems

Windows, Linux, and BSD operating systems can be used in the solution. However, the versions of Windows and Linux used in the solution must be listed in the NetApp Interoperability Matrix Tool.

2.6 Management

All AWS resources can be managed through the AWS Dashboard, Windows PowerShell, Python, and the AWS command line interface (CLI), as well as through APIs. For a list of tools that can be used to manage AWS resources, refer to Tools for Amazon Web Services.

2.7 Business Continuity and Data Protection

Almost all NetApp data protection software can be installed on and can function on AWS VMs, as long as the versions used are listed in the NetApp Interoperability Matrix Tool.

Note: Because AWS does not support nested hypervisors, Hyper-V and VMware do not function in AWS. NetApp hosted software that works with VMware and Hyper-V does not function in AWS.

2.8 AWS GovCloud Region Support

AWS GovCloud is a region completely separated from all other AWS regions. AWS GovCloud is used only by the United States government to run workloads and services in the AWS cloud subject to the strict compliance requirements of the US government. See the AWS GovCloud documentation for more information about the GovCloud region.

Currently, there is only one AWS Direct Connect Point of Presence (PoP) for the AWS GovCloud region using cross connect. The location of this PoP is Equinix SV1/SV5 in San Jose, CA.

The functionality of the Direct Connect service in the GovCloud region is identical to the functionality of Direct Connect in the other commercial AWS regions. There are public and private virtual interfaces and the workflows to create and configure them are the same as the Direct Connect workflows in the other AWS commercial regions.

The compliance program that has the most effect on the NetApp Private Storage for Cloud solution architecture is the US International Traffic in Arms Regulations (ITAR) program. ITAR-regulated data are defense-related articles and services on the United States Munitions List (USML) and related technical data. Due to the nature of the data, only U.S. citizens are authorized to have access.

In the AWS GovCloud Direct Connect User Guide, the ITAR boundary is defined as follows:

Table 3) AWS Direct Connect ITAR boundary.

ITAR-Regulated Data Permitted	ITAR-Regulated Data Not Permitted
• If you are transferring any type of ITAR-regulated data through the AWS Direct Connect connection, you must encrypt the data that is being transferred by using a VPN tunnel.	• AWS Direct Connect metadata is not permitted to contain ITAR-regulated data. This metadata includes all of the configuration data that you enter when creating and maintaining AWS Direct Connect, such as connection names. • Do not enter ITAR-regulated data in the following console fields: – Connection Name – VIF Name

If you are managing ITAR-regulated data, a hardware VPN appliance is required in the cabinet/shared cage at Equinix to encrypt the network traffic between the NetApp storage and the AWS cloud compute. The VPN tunnel connects to the AWS VPC over a Direct Connect public virtual interface.

If you are managing non-ITAR-regulated data with Direct Connect and GovCloud, use a private virtual interface with no hardware VPN appliance.

The Federal Risk and Authorization Management Program (FedRAMP) does not directly affect the technical aspects of the solution, but it does affect the ability of the solution to be deployed and managed.

Note: Currently, NetApp is working to secure FedRAMP certification for the NetApp Private Storage for AWS solution. Contact your NetApp account team for more information about the current status of FedRAMP certification and the availability of partners who have received Agency Authorization to Operate (ATO).

The use cases for NetApp Private Storage for AWS are also valid for NetApp Private Storage in the AWS GovCloud region.

3 NetApp Private Storage for Microsoft Azure

This section describes the solution architecture for NPS for Microsoft Azure.

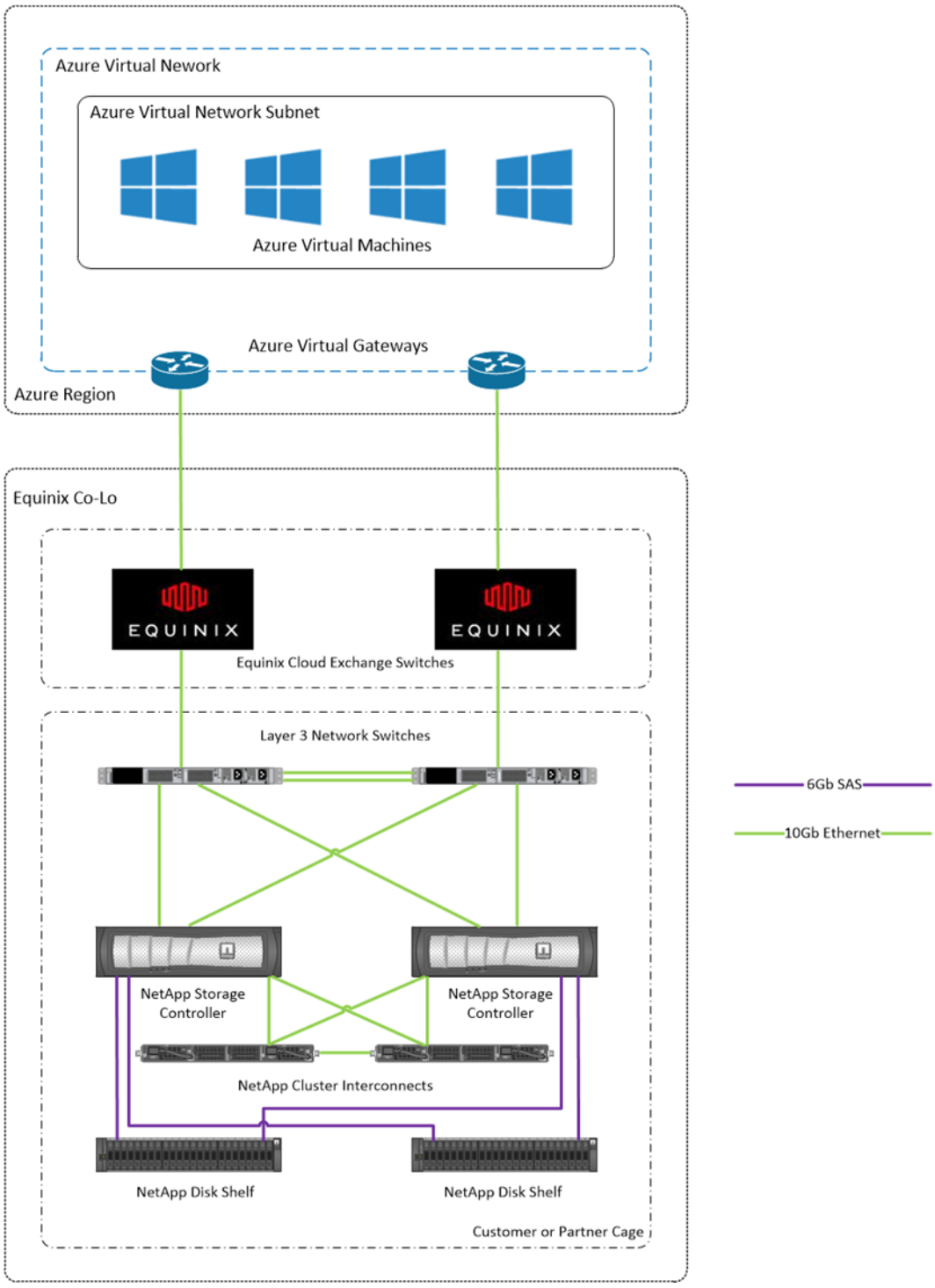
3.1 Solution Architecture Details

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

- Azure Compute VMs
- Azure Virtual Networks
- Azure ExpressRoute
- Azure ExpressRoute colocation facility (Equinix)
- Cloud peering switch (Equinix Cloud Exchange)
- Customer-network equipment that supports BGP routing protocols and 1Gbps or 10Gbps SMF connectivity
- NetApp storage (AFF, FAS, E-Series, or SolidFire platforms)

Figure 4 shows the architecture of NPS for Microsoft Azure using FAS Storage with redundant ExpressRoute connections. Specific implementations will vary, depending on each customer's technical and business requirements.

Figure 4) NetApp Private Storage for Microsoft Azure.



3.2 Solution Sizing and Performance Considerations

In addition to the general sizing guidelines for NetApp storage and the network for NPS for Cloud documented in section 1, “Solution Overview,” there are specific guidelines for the sizing of Azure cloud compute resources.

Azure VMs (CPU, memory, network performance, and root volume size) must be sized appropriately for the applications and services used in this architecture. For more information about the Azure VM sizes, refer to Virtual Machine and Cloud Service Sizes for Azure.

3.3 Network Considerations

In addition to the general network guidelines for NPS documented in section 1, “Solution Overview,” there are also specific guidelines for the network configuration for Bluemix.

Network Bandwidth

Azure ExpressRoute network connections are available in sub-1Gbps, 1Gbps, and 10Gbps network connection speeds. For available bandwidth options, see the Azure ExpressRoute FAQ.

Network Segregation

The network architecture for the NPS for Microsoft Azure can support single tenancy or secure multi-tenancy. 802.1Q VLAN tags are used by the Azure ExpressRoute service to logically connect and route network traffic between the Azure Virtual Network and the customer network in the colocation facility where the NPS is located.

Secure multi-tenancy is a complicated topic that is not covered in detail in this document. If multiple Azure Virtual Networks from different Azure subscriptions connected to the NetApp storage are required, 802.1Q VLAN tags can be used to segregate network traffic between the Azure Virtual Networks and the NetApp storage.

The physical network connection to Azure through Azure ExpressRoute can support multiple Azure ExpressRoute virtual circuits. Each virtual circuit uses a user-defined VLAN tag and uses BGP routes advertised by the customer network equipment.

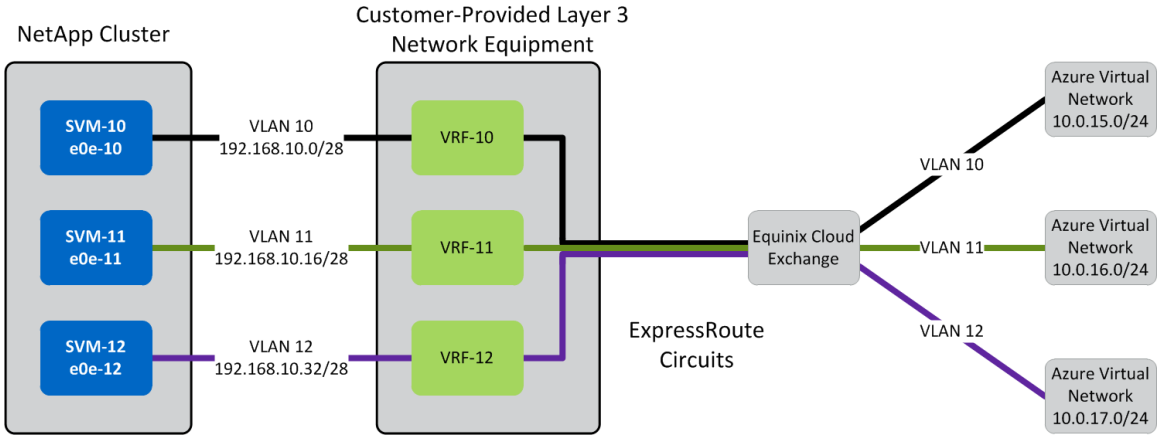
For example:

Tenant A: VLAN 10

Tenant B: VLAN 11

Tenant C: VLAN 12

Figure 5) NetApp Private Storage for Azure network architecture.



The BGP peering for each ExpressRoute virtual circuit consists of two IP addresses: one on the Azure virtual gateway and the other on the customer-provided network switch or router. For example, the following configuration is for the private virtual interface for Tenant A:

```
PS C:\Users\Mark Beaupre> Get-AzureBGPPeering -ServiceKey 2a5f5eef-2291-4ff6-99f8-258bba8d8b85


AdvertisedPublicPrefixes      :
AdvertisedPublicPrefixesState :
AzureAsn                      : 12076
PeerAsn                       : 64514
PrimaryAzurePort              : EQIX-SJC-06GMR-CIS-3-PRI-A
PrimaryPeerSubnet             : 192.168.100.128/30
SecondaryAzurePort            : EQIX-SJC-06GMR-CIS-4-SEC-A
SecondaryPeerSubnet           : 192.168.100.132/30
State                         : Enabled
VlanId                        : 10
```

On the primary network switch, the BGP configuration (Cisco NX-OS) is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.35 remote-as 64514
    address-family ipv4 unicast
  neighbor 192.168.100.130 remote-as 12076
    password 3 63611e150f52294d04dd44fe
    address-family ipv4 unicast
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to Azure, and the `192.168.100.130` IP address is the Azure peer IP address for the routing.

On the secondary network switch, the BGP configuration (Cisco NX-OS) is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.34 remote-as 64514
    address-family ipv4 unicast
  neighbor 192.168.100.134 remote-as 12076
    password 3 63611e150f52294d04dd44fe
    address
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to Azure, and the `192.168.100.134` IP address is the Azure peer IP address for the routing.

The VLAN network segregation is extended to the NetApp storage by using VLAN interfaces. For example, if the storage has a physical 10GbE interface labeled `e0e`, then a VLAN interface called `e0e-10` is created and an IP address from `192.168.10.0/28` is assigned to the VLAN interface.

3.4 Virtual Machine Infrastructure

Azure VMs support Microsoft Windows and Linux operating systems.

The Azure hypervisor is a proprietary hypervisor that runs only in the Azure cloud.

Note: There are no NetApp integration tools with this hypervisor.

Azure offers preconfigured VM images (templates). Azure also allows users to build their own images, which can be shared with other Azure users. For more information about the Azure images available, see the Azure Marketplace.

Azure instances are available in different instance types that have different combinations of CPU, memory, and network throughput.

There is no restriction on deploying virtualization infrastructure in the Azure ExpressRoute facility where the NPS is located. The use of local virtualization is outside the scope of this document.

3.5 Operating Systems

Windows and Linux operating systems can be used in the solution. However, the versions of Windows and Linux used in the solution must be listed in the NetApp Interoperability Matrix Tool.

3.6 Management

A variety of management tools is offered by Azure, NetApp, and network equipment vendors.

Microsoft Azure

All Azure resources can be managed through the Azure Management Portal, Windows PowerShell, Azure command line interface (CLI), Microsoft System Center, as well as through APIs. For a list of tools that can be downloaded and used to manage Azure resources, refer to Azure Downloads.

3.7 Business Continuity and Data Protection

Almost all NetApp data protection software can be installed on and can function on Azure VMs, as long as the versions used are listed in the NetApp Interoperability Matrix Tool.

Note: Because Azure does not support nested hypervisors, Hyper-V and VMware hypervisors do not function in Azure. NetApp hosted software that works with VMware and Hyper-V hypervisors does not function in Azure.

The Azure cloud offers a service called Azure Site Recovery (ASR) that can be used to replicate on-premises VMs to Azure to support DR. Both Microsoft Hyper-V and VMware VMs can be migrated to Azure with ASR.

For more information, see the Azure Site Recovery documentation and the NetApp white paper WP-7215: Azure Site Recovery with SAN Replication to NetApp Private Storage for Microsoft Azure Solution Configuration and Testing.

3.8 Azure Government Region Support

The NetApp Private Storage for Cloud solution can be used with the Azure Government regions.

Azure Government consists of two Azure regions: US Gov Iowa and US Gov Virginia. These regions are completely separated from all other Azure regions. Azure Government is used by United States government agencies to run workloads and services in the Azure cloud subject to the strict compliance requirements of the US government. See the Azure Government documentation for more information.

Azure ExpressRoute connectivity to the Azure government regions are available in Equinix Chicago and Equinix Ashburn (Washington DC) data centers. Customers can also connect to Azure Government from their on-premises data centers using point-to-point network links provided by ExpressRoute Layer 3 service providers. See the Azure Government ExpressRoute documentation for more information.

The functionality of the ExpressRoute service in the Azure Government regions is identical to the functionality of ExpressRoute in the other commercial Azure regions. There are public, private, and Microsoft ExpressRoute circuits and the workflows to create and configure them are the same as the ExpressRoute workflows in the other Azure commercial regions.

NetApp Private Storage for Azure solution architecture can be used with data controlled by the US International Traffic in Arms Regulations (ITAR) program. ITAR-regulated data are defense-related

articles and services on the United States Munitions List (USML) and related technical data. Due to the nature of the data, only U.S. citizens are authorized to have access.

The ITAR boundary for Azure ExpressRoute is not specifically defined in the Using Azure Government with ITAR Controlled Data documentation. If you are planning to use NPS for Azure with ITAR Controlled Data, please contact your NetApp account team for assistance. NetApp will work with Microsoft to help define the ExpressRoute ITAR boundary for your situation. If you are managing non-ITAR-regulated data with ExpressRoute and Azure Governement, use a private ExpressRoute circuit.

Although the Federal Risk and Authorization Management Program (FedRAMP) does not directly affect the technical aspects of the solution, it affects the ability of the solution to be deployed and managed.

Note: Currently, NetApp is working to secure FedRAMP certification for the NetApp Private Storage for Azure solution. Contact your NetApp account team for more information about the current status of FedRAMP certification and the availability of partners who have received Agency Authorization to Operate (ATO).

The use cases for NetApp Private Storage for Azure are also valid for NetApp Private Storage in the Azure Government regions.

4 NetApp Private Storage for Bluemix

This section describes the solution architecture for NPS for IBM Bluemix, formerly known as IBM SoftLayer.

4.1 Solution Architecture Details

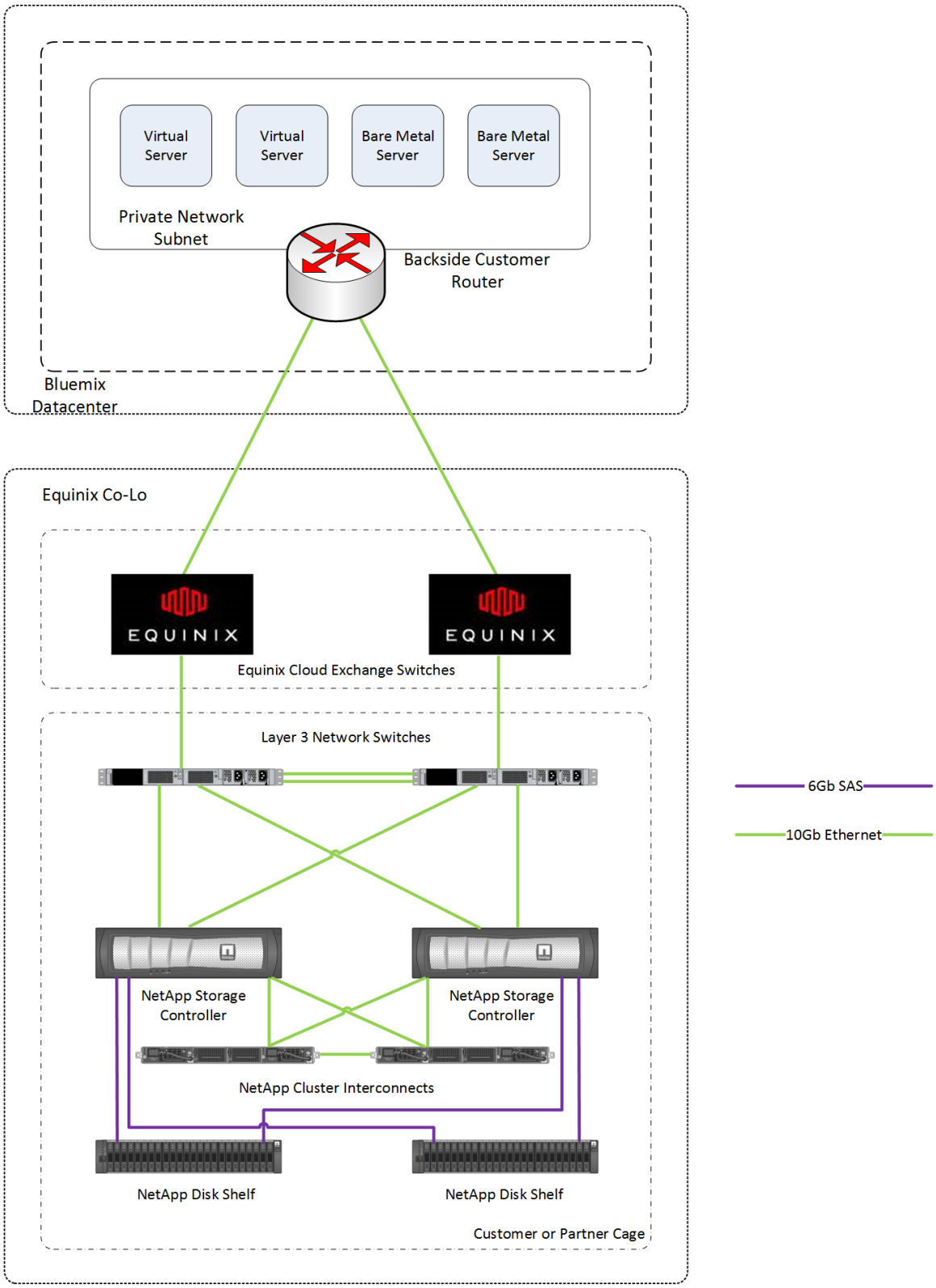
The NPS for Bluemix consists of the following major components:

- Bluemix VMs
- Bluemix Bare Metal Servers
- Bluemix Private Network
- Bluemix Direct Link
- Bluemix Point of Presence colocation facility (Equinix)
- Cloud peering switch (Equinix Cloud Exchange)
- Customer-owned network equipment that supports BGP routing protocols and 1Gbps or 10Gbps SMF connectivity
- NetApp storage (AFF, FAS, E-Series, or SolidFire platforms)

Note: At this time, Bluemix is not participating in the United State government ITAR program. ITAR controlled data should not be used with NPS for Bluemix.

Figure 6 shows the architecture of NPS for Bluemix using FAS storage. Specific implementations will vary depending on each customer's technical and business requirements.

Figure 6) NetApp Private Storage for Bluemix.



4.2 Solution Sizing and Performance Considerations

In addition to the general sizing guidelines for NetApp storage and the network for NPS in Cloud documented in section 1, “Solution Overview,” there are also specific guidelines for the sizing of Bluemix cloud compute resources.

Bluemix VMs (CPU, memory, network performance, and root volume size) and Bare Metal Servers must be sized appropriately for the applications and services used in this architecture.

For more information about Bluemix virtual servers, see the Bluemix Introduction to Virtual Servers website.

For more information about Bluemix Bare Metal Servers, see the Bluemix Bare Metal Server website.

4.3 Network Considerations

In addition to the general network guidelines for NPS documented in section 1, “Solution Overview,” there are also specific guidelines for the network configuration for Bluemix.

Network Bandwidth

Bluemix Direct Link network connections are available in 1Gbps and 10Gbps connection speeds.

Note: You can identify saturated network links by using network monitoring tools or the Traceroute tool.

Network Connectivity

As previously discussed, the network connections for Bluemix Direct Link are in 1Gbps or 10Gbps connection types. The fiber optic network cable used by Bluemix Direct Link is a 9/125 duplex SMF. Architects must verify that the network equipment used in the solution can support this physical connectivity requirement.

1Gbps and 10Gbps Bluemix Direct Link network connections can be used in the same environment. However, architects must verify that the network equipment used can support a mix of 1Gbps and 10Gbps network connections on the same switch or router.

Network Segregation

The network architecture for the NPS for Microsoft Bluemix can support single tenancy or secure multi-tenancy. 802.1Q VLAN tags are used by the Bluemix Direct Link service to logically connect and route network traffic between the Bluemix Private Network and the customer network in the colocation facility where the NPS is located.

Secure multi-tenancy is a complicated topic that is not covered in detail in this document. If multiple Bluemix Private Networks from different Bluemix subscriptions connected to the NetApp storage are required, 802.1Q VLAN tags can be used to segregate network traffic between the Bluemix Private Networks and the NetApp storage.

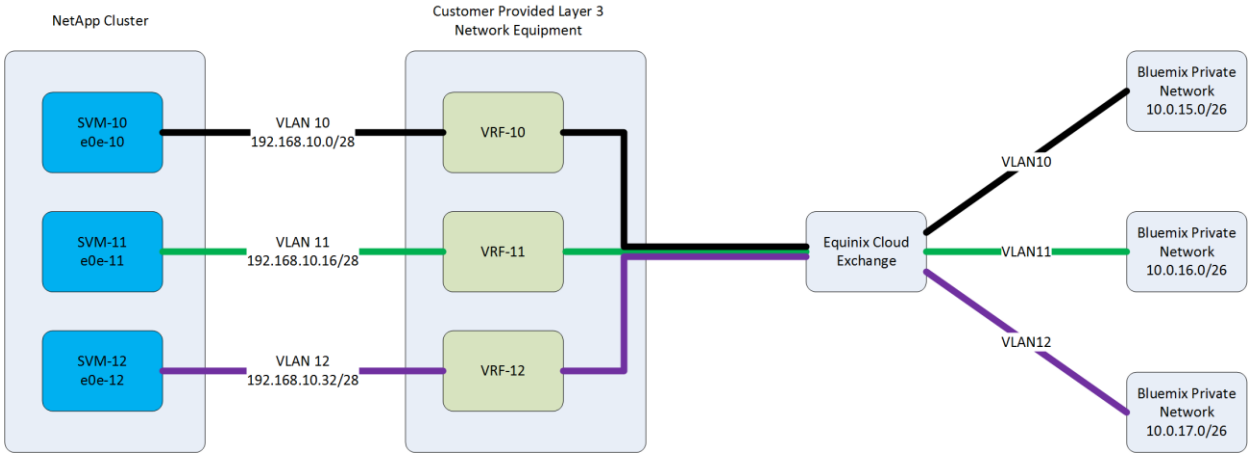
The physical network connection to Bluemix through Bluemix Direct Link can support multiple Bluemix Direct Link connections. Each connection uses a user-defined VLAN tag and uses BGP routes advertised by the customer network equipment.

By using multiple VLANs, customers can partition the Direct Link dedicated connection into multiple Direct Link connections. As Figure 7 shows, each Direct Link private network is associated with a unique VLAN tag.

This network segregation goes from the Bluemix private network across the Direct Link network connection (cross connect) through dedicated virtual routing and forwarding (VRF) instances. It then goes down to VLAN interfaces used by LIFs on the SVMs, on the NetApp storage cluster.

Figure 7 illustrates the Bluemix Direct Link network architecture.

Figure 7) Bluemix Direct Link network architecture.



On the network switch, the BGP configuration is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.35 remote-as 64514
    address-family ipv4 unicast
  neighbor 192.168.100.130 remote-as 13884
    password 3 63611e150f52294d04dd44fe
    address-family ipv4 unicast
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to Bluemix, and the `192.168.100.130` IP address is the Bluemix peer IP address for the routing.

On the secondary network switch, the BGP configuration (Cisco NX-OS) is as follows:

```
router bgp 64514
vrf vrf-10
  address-family ipv4 unicast
    network 192.168.10.0/28
    maximum-paths eibgp 2
  neighbor 192.168.25.34 remote-as 64514
    address-family ipv4 unicast
  neighbor 192.168.100.134 remote-as 13884
    password 3 63611e150f52294d04dd44fe
    address
```

The subnet on which the SVM is located (on the `192.168.10.0/28` address) is advertised to Bluemix, and the `192.168.100.134` IP address is the Bluemix peer IP address for the routing.

The VLAN network segregation is extended to the NetApp storage by using VLAN interfaces. For example, if the storage has a physical 10GbE interface labeled `e0e`, then a VLAN interface called `e0e-10` is created and an IP address from `192.168.10.0/28` is assigned to the VLAN interface.

4.4 Virtual Machine Infrastructure

Bluemix VMs support Microsoft Windows and Linux operating systems.

Bluemix virtual servers are VMs that customers can use to rapidly deploy computing resources. The virtual servers can be fully customized, allowing customers to select CPU, memory, network, storage, operating systems, system add-ons, and monitoring options.

Customers can also select the tenancy of the virtual server. In standard tenancy, the virtual server is deployed to a multi-tenant environment. In private-node tenancy, the virtual server is deployed to a single-tenant environment. Virtual servers deployed onto private nodes are ideal for workloads that have stringent resource requirements.

Bluemix virtual servers connect to NetApp storage in the colocation facility through guest-level connectivity for iSCSI, NFS, or SMB.

Note: There is no support for RDM or pass-through LUNs with Bluemix virtual servers.

For more information about Bluemix virtual servers, refer to the Bluemix Introduction to Virtual Servers website.

There is no restriction on deploying virtualization infrastructure in the Bluemix Direct Link colocation facility where the NetApp storage is located. The use of local virtualization is outside the scope of this document.

4.5 Bare Metal Server Infrastructure

In addition to virtual servers, Bluemix offers the option of deploying Bare Metal Servers or Bare Metal Instances.

A Bare Metal Server is a monthly offering that provides customers with a dedicated server with components they can customize. A Bare Metal Instance is a prebuilt server that comes in different configurations that can be ordered on an hourly or a monthly basis.

Bare Metal Servers can be installed with virtualization software such as VMware or Microsoft Hyper-V in addition to operating systems.

Bluemix Bare Metal Servers and Bare Metal Instances connect to the NetApp storage in the colocation facility by using connectivity for iSCSI (software initiator only), NFS, or SMB.

Note: If the virtualization software is installed on the Bare Metal Instance, RDM LUNs or pass-through LUNs stored on the customer NetApp storage can be used. That configuration is outside the scope of this document.

For more information about Bluemix Bare Metal Servers, refer to the Bluemix Bare Metal Server website.

4.6 Operating Systems

Windows, Linux, and BSD operating systems can be used in the solution. However, the versions of Windows and Linux used in the solution must be listed in the NetApp Interoperability Matrix Tool.

4.7 Management

A variety of management tools is offered by Bluemix, NetApp, and network equipment vendors.

Bluemix

All Bluemix resources can be managed through the Bluemix Customer Portal, the Bluemix CLI, as well as through APIs. For a list of tools that can be used to manage Bluemix resources, refer to the Meet Bluemix website.

4.8 Business Continuity and Data Protection

Almost all NetApp data protection software can be installed on and can function on Bluemix VMs and Bare Metal Servers, as long as the versions used are listed in the NetApp Interoperability Matrix Tool.

5 Use Cases for NetApp Private Storage for Cloud Solution

The flexibility of the NPS for Cloud solution architecture allows it to accommodate various customer business and technical requirements, including the following use cases:

- Analytics
- Multicloud connectivity
- Primary database workloads
- Development and test
- Cloudburst for peak workloads
- Multiregion application continuity
- Disaster Recovery

5.1 Multicloud Connectivity

Having simultaneous connectivity to multiple clouds allows customers to use the cloud resources of their choice based on cost, performance, and features. Applications can be deployed across multiple clouds to help avoid dependency on a single cloud provider and to help protect against an application outage during a service outage in one or more clouds.

Multicloud access relies on using the same VLAN tag, VRF, and NetApp storage VLAN interface to connect to multiple clouds. Transitive network routing between clouds provides the ability for applications (such as Microsoft SQL Server AlwaysOn Failover Clusters) to be deployed across clouds while keeping the data outside of a cloud.

Connectivity to the clouds can be through a cloud-peering switch (for example, Equinix Cloud Exchange) through a cross connect, or through both.

Note: Some clouds block autonomous system numbers and networks from some cloud providers, so be sure to refer to your cloud vendor's network documentation.

Figure 8 shows a multicloud network architecture supported by NetApp Private Storage for Cloud.

Figure 8) NetApp Private Storage multicloud network architecture.

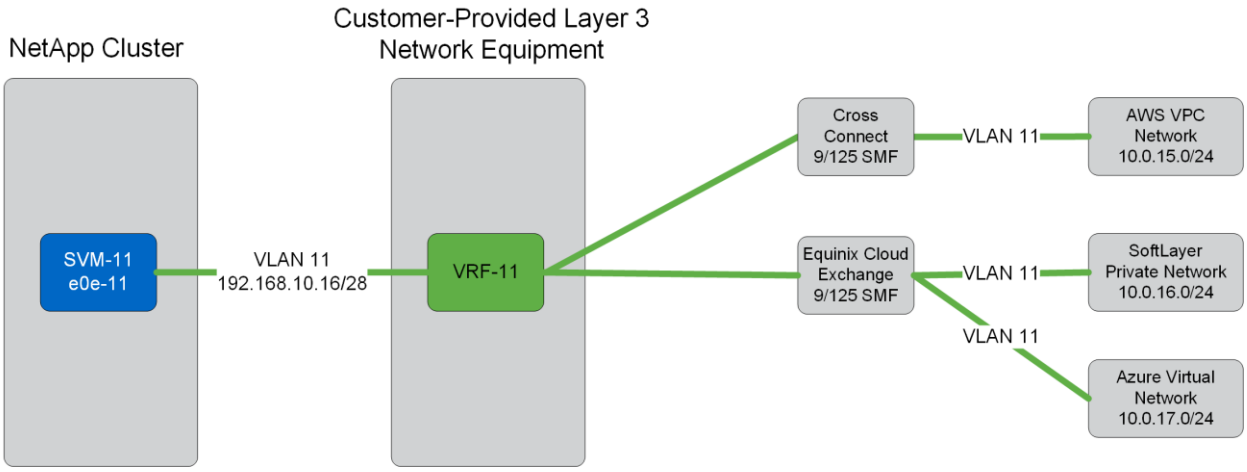
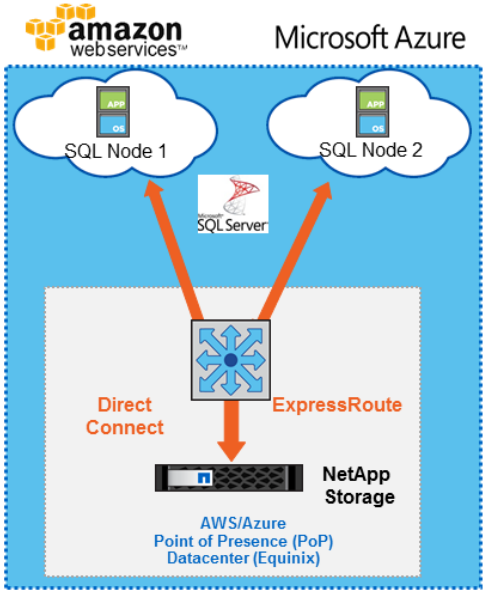


Figure 9 shows a Microsoft SQL Server AlwaysOn Failover Cluster deployed across AWS and Azure. One node of the SQL Server cluster is deployed in AWS, and the other is deployed in Azure. Both cluster nodes are connected to NetApp Private Storage through Direct Connect and ExpressRoute, respectively.

Figure 9) Microsoft SQL AlwaysOn Failover Cluster deployed across AWS and Azure clouds.

- Microsoft AlwaysOn Failover Cluster nodes are deployed in AWS and Azure
- SQL nodes are connected to NetApp storage storage via iSCSI or SMB3
- Transitive routing between AWS and Azure allow for cluster nodes to communicate for cluster failover coordination
- In the event of SQL node failure, Windows Failover Clustering works with SQL to automatically move the SQL workload to the other node in the cloud

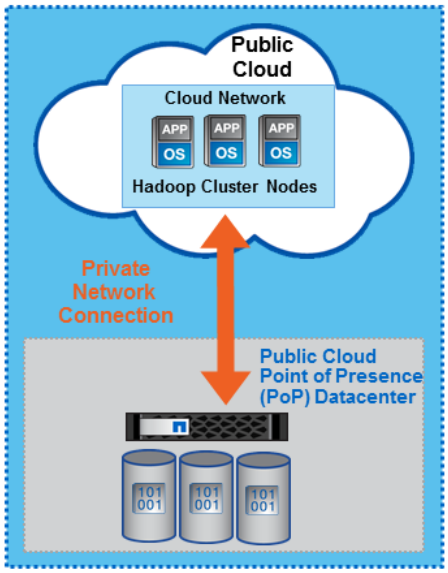


5.2 Analytics Workloads

Analytics workloads can be run on the NPS for Cloud solution, as shown in Figure 10. For Hadoop workloads, Apache Hadoop cluster nodes in the cloud are connected to NetApp Private Storage via Apache Spark, NetApp NFS Connector for Hadoop, and NFS storage protocol.

The NetApp NFS Connector for Hadoop and Apache Spark is installed on each Hadoop cluster node. The NFS Connector configure simplifies the connectivity of the NFS exports hosted on NPS storage. For more information about the NetApp NFS Connector, please refer to TR-4382 NetApp FAS NFS Connector for Hadoop.

Figure 10) Analytics workload with Hadoop.



- Data is stored on NetApp storage located in public cloud point of presence (PoP) datacenter
- Round trip network latency to the cloud must be less than 5ms
- Private Network Connection to the cloud should be 10Gbps or greater
- Spark and the NetApp NFS Connector for Hadoop are installed on each cluster node. Each node is connected to NPS via NFS
- In place analytics jobs are run and the cloud compute can be terminated once the jobs are complete
- Multi-Cloud analytics offer the opportunity for composition of analytics services and APIs from multiple clouds against the same storage

In addition, there are other custom analytics workloads specific to certain industries (Oil and Gas, Geology/Seismic, and Genomics/Pharma) that can be used with NetApp Private Storage. The custom analytics applications are installed on cloud virtual machines that are connected to NetApp Private Storage.

5.3 Primary Database Workloads

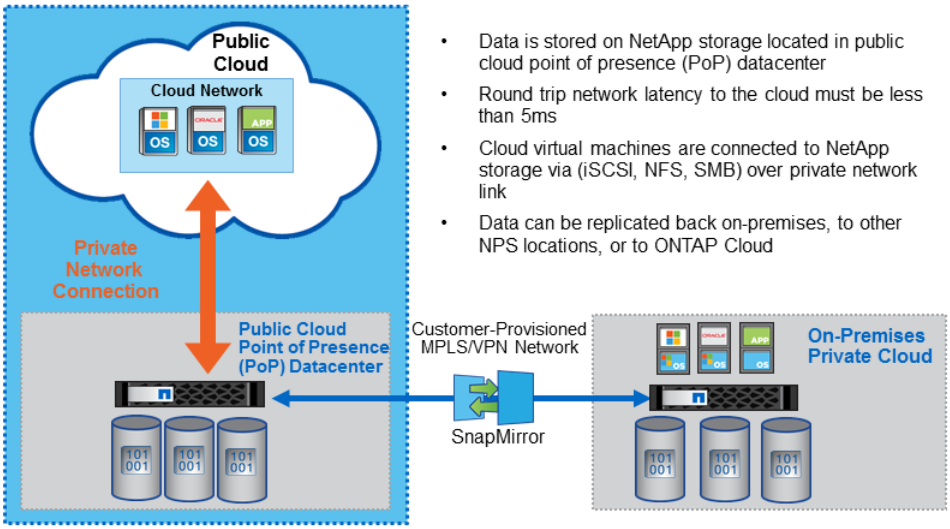
Primary database workloads can be run on the NPS for Cloud solution, as shown in Figure 11. NetApp storage and public cloud compute can be integrated to provide a scalable and elastic infrastructure with the performance needed by enterprise applications such as Oracle, Microsoft SQL Server, and SAP.

Almost all enterprise applications can be installed on public cloud compute. The same design principles and best practices apply for these applications when they are deployed on this solution.

Note: Although many database and enterprise applications are available to run in the public cloud, please refer to your database and enterprise application vendor for the technical and support requirements around the use of public cloud compute.

Applications that require block-level access to storage must use public cloud compute that are configured with guest-connected LUNs through the iSCSI protocol. Applications that require file-level access to storage (NFS, SMB) must use public cloud VMs that are configured to support the protocol required by the application.

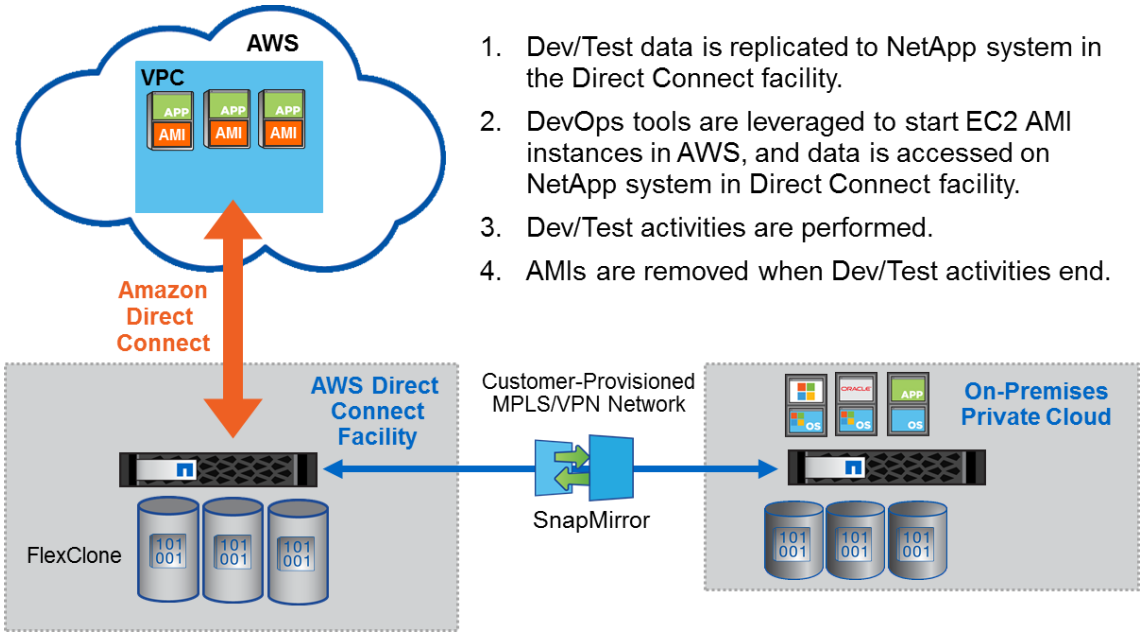
Figure 11) Production workloads.



5.4 Development and Test

The NPS for Cloud solution is well-suited to supporting DevOps workflows, as shown in Figure 12. NetApp storage and AWS can be integrated into DevOps tools such as Ansible, Puppet, Chef, or Visual Studio for development. They can also be integrated into QA automation scripts for testing.

Figure 12) Development and test information.



5.5 Disaster Recovery

In this solution, SnapMirror is used to support DR. The way SnapMirror is implemented in the solution depends on the DR requirements of the application deployed on the solution. There are different ways to support this replication:

- The SnapMirror replication can occur over site-to-site virtual private network (VPN) links between an on-site location and the Equinix colocation facility.

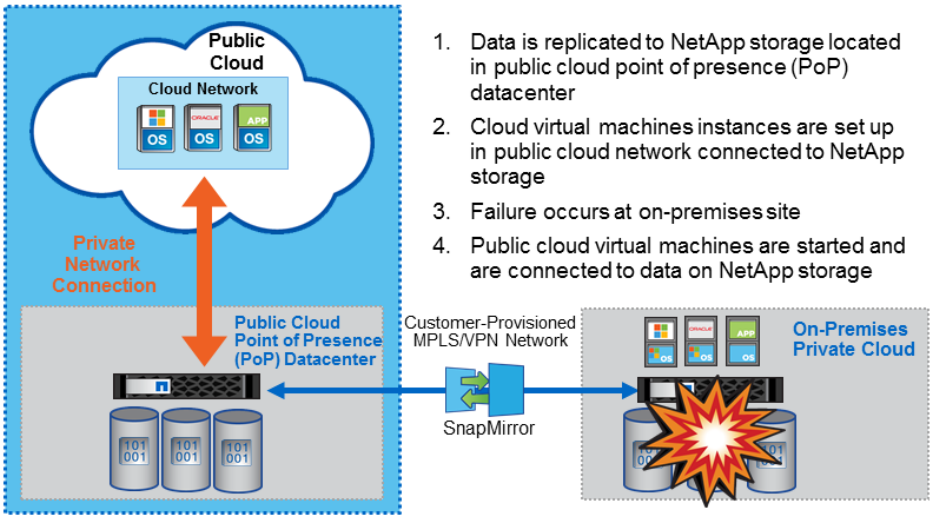
  To support this replication, network security equipment that can support a site-to-site VPN must be deployed in both the primary and the secondary locations, and an Internet connection must exist between both of the locations.
- The SnapMirror replication can occur over a Multiprotocol Label Switching (MPLS) dedicated network connection (that is, “dark fiber”) between an on-site location and the Equinix colocation facility.

  To support this replication, network equipment that can support this connection must be deployed in both the primary and the secondary locations.
- The SnapMirror replication can also occur between two Equinix colocation facilities through the use of either a site-to-site VPN or an MPLS connection. The same requirements apply to this scenario.

Note: SnapMirror is only available on FAS and AFF storage systems.

Figure 13 shows a general disaster reocovery use case.

Figure 13) General Disaster Recovery use case.



6 Specific Use Cases for Azure

6.1 Disaster Recovery/Virtual Machine Migration with Azure Site Recovery

The Azure cloud offers a service called ASR that can be used to migrate on-premises VMs to Azure. Both Microsoft Hyper-V and VMware VMs can be migrated to Azure with ASR.

Microsoft System Center Virtual Machine Manager (VMM) integrates with the NetApp storage SMI-S provider to manage NetApp storage and SnapMirror replication as part of VM and data protection groups. ASR relies on the Hyper-V replica service to perform block-level replication of VMs to Azure VMs.

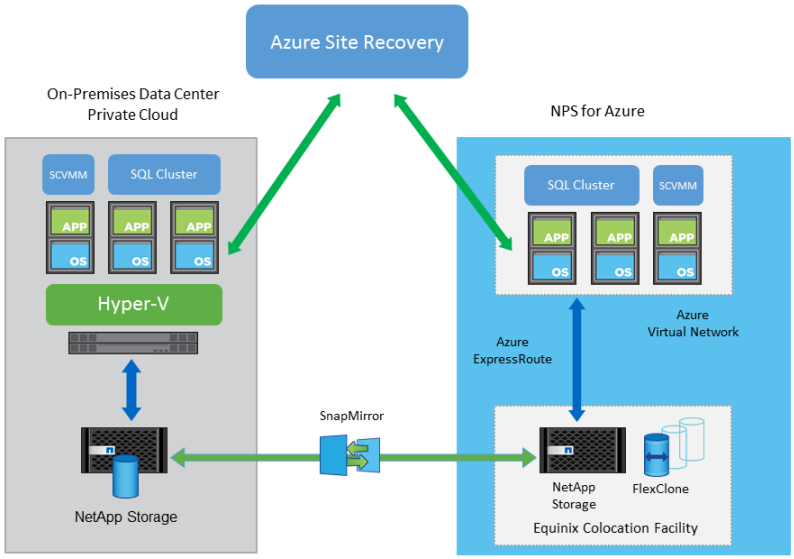
In the case of DR, VMs and the storage in the primary location are offline. System Center VMM running in Azure or in the NPS colocation facility does the following:

- Issues commands to the NetApp SMI-S 5.2 provider to break SnapMirror replication
- Brings the Azure VMs online
- Creates iSCSI sessions to NPS
- Maps the LUNs on NPS to the Azure VMs

ASR can also be used to migrate on-premises VMs and data to NPS for Azure in a controlled fashion.

Note: This use case was validated with ONTAP which is only available on AFF and FAS storage systems.

Figure 14) ASR with NPS for Cloud solution for Microsoft Azure.



7 Specific Use Cases for Bluemix

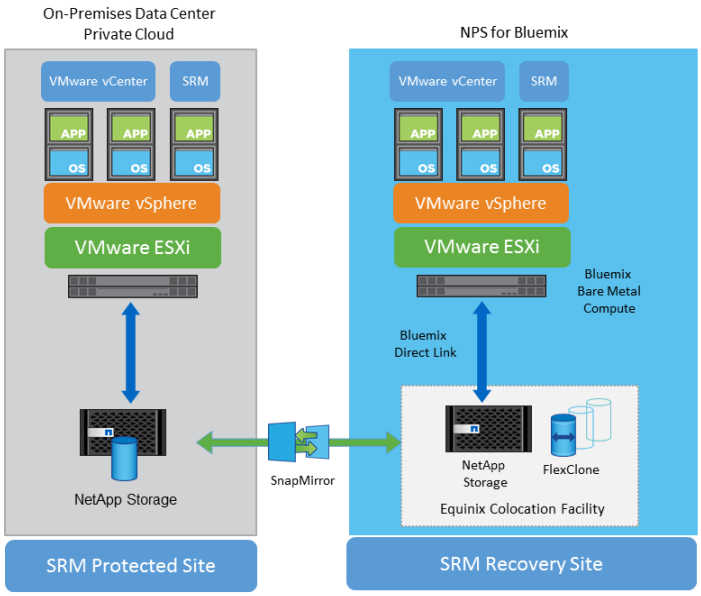
7.1 Disaster Recovery Using VMware Site Recovery Manager

Bluemix differs from Azure and AWS by offering physical compute resources in addition to its virtual compute services. What this means is that customers can install their own hypervisor onto Bluemix Bare Metal Servers, including the VMware ESXi hypervisor.

This capability provides administrators with the ability to leverage NetApp SnapMirror and VMware Site Recovery Manager with NPS for Bluemix as a way to provide DR protection for VMs and application data.

Figure 15 illustrates the solution architecture for VMware Site Recovery Manager with the NPS for Cloud solution for Bluemix.

Figure 15) VMware Site Recovery Manager with NPS for Cloud solution for the Bluemix solution architecture.



8 Design Validation

The NPS for Cloud solution has been deployed successfully. For further information about the following success stories, contact your NetApp account team.

8.1 Success Stories

Software as a Service Provider: Achieve Higher SLAs While Lowering Costs

Australia's largest publicly traded software company has expertise in seven key markets and delivers integrated, preconfigured solutions that provide proven practice, streamline implementations and reduce time, cost and risk.

The firm faced increased customer demand to buy software as a service instead of buying a traditional software subscription. By the end of 2015, the firm had moved "all in" to AWS, but the costs from AWS EBS storage threatened their SaaS business model. When the Australian government authorized the use of Azure, the firm needed to be able to become multi-cloud without adding cost or complexity.

In addition, the performance and availability SLAs of AWS storage did not meet the requirements of the firm's largest customers.

Faced with all of these challenges, the firm decided to deploy a four node NetApp MetroCluster connected to both AWS and Azure simultaneously. Two nodes were deployed in two different Equinix datacenters approximately 3 kilometers apart and all four nodes were connected to AWS and Azure.

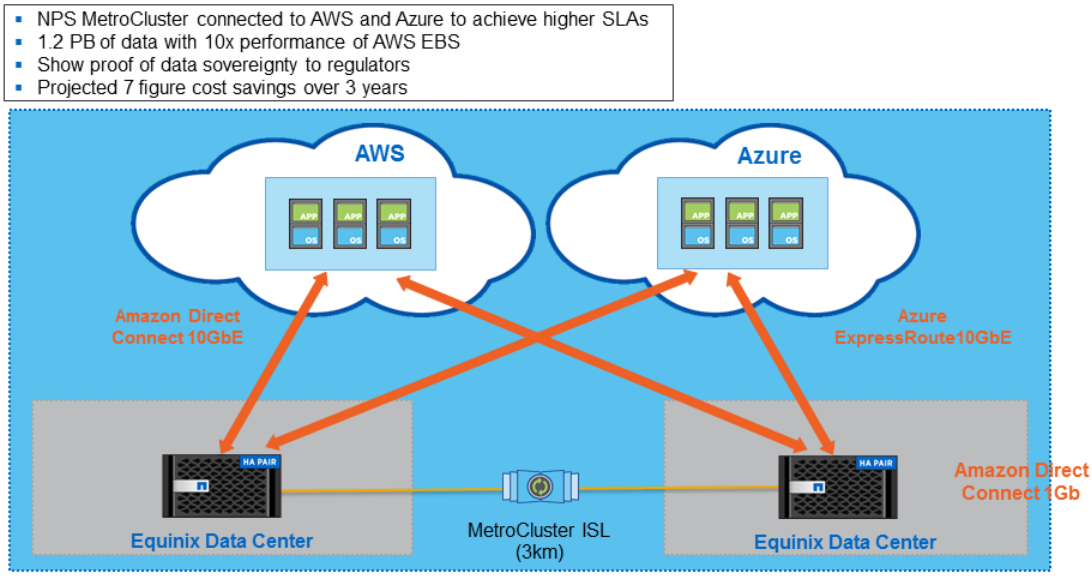
The move to NetApp Private Storage with MetroCluster resulted in the following:

- Lower customer acquisition costs and better customer experience
- Lower storage costs by leveraging NetApp storage efficiency. Only 220TB of storage is consumed while providing 1.2PB of effective data capacity to customers.
- Improved ability to meet SLA guarantees, which ensures better customer experience and the avoidance of fines paid for missed SLA's

- Achieving ten times the performance of AWS EBS fastest storage tier
- Multi-cloud capabilities, which reduces risk by removing single cloud dependency.It can fail over to other clouds when the primary cloud is unavailable.
- Satisfying Australian regulators by enabling government and financial customers to prove where data resides at all times

Figure 16 shows the SaaS provider's use of the solution.

Figure 16) SaaS company using solution for production.



Major Oil and Natural Gas Exploration and Production Firm: Disaster Recovery for Critical Data

After the completion of a corporate risk assessment, a major oil and natural gas exploration company headquartered in the United States determined that they were exposed to unacceptable risks by having only one offsite copy of company data.

This assessment provided the impetus for the firm to rethink their datacenter strategy more broadly. The customer traditionally operated in a 100% on-premises datacenter model. Data was bi-directionally replicated between datacenters located in the Denver and Houston metropolitan areas.

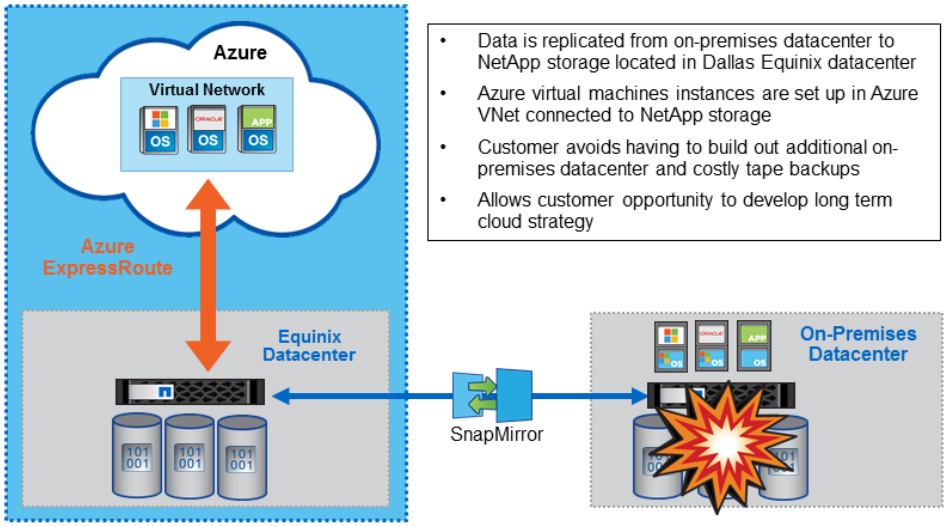
The firm decided to set up a tertiary copy of their data in an Equinix datacenter in Dallas, TX using NetApp Private Storage and Microsoft Azure.

The move to NetApp Private Storage allowed the firm to:

- Eliminate costly tape backups
- Maintain control of company data while connected to the Azure cloud
- Develop their long term cloud strategy

Figure 17 shows the Oil and Gas firm's use of the solution.

Figure 17) Major Oil and Gas exploration and production firm using solution for disaster recovery.



Public Sector: Managed NPS For Production and Disaster Recovery

A major agency of the United States government was looking to more efficiently manage the budget allocated to them by using the cloud. However, they needed to ensure that they had control over their data at all times due to federal regulation and laws concerning the management of their data.

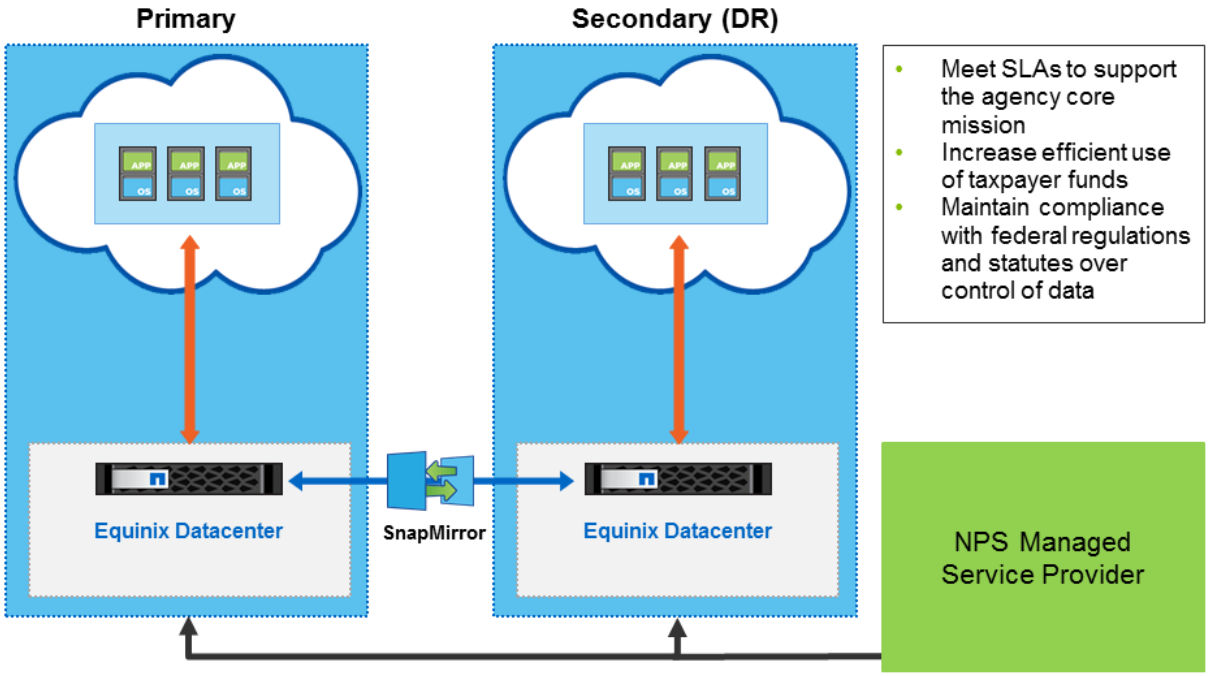
The agency decided to use a managed NetApp Private Storage solution that was connected to the cloud for production (primary site) and disaster recovery (secondary site). Using a managed service allowed the agency to focus on its core mission instead of having to build and operate NPS infrastructure.

The move to a managed NetApp Private Storage solution allowed the agency to:

- Meet their SLAs to support the agency core mission
- Increase efficient use of taxpayer funds
- Maintain compliance with federal regulations and statutes

Figure 18 shows the agency's use of managed NetApp Private Storage.

Figure 18) Managed NPS for production and disaster recovery.



9 Conclusion

NPS for Cloud is an agile hybrid cloud solution that allows customers to balance public cloud and private resources to optimize business outcomes.

The solution allows customers to:

- Adjust cloud resources on demand and dynamically optimize both operational and capital expenses.
- Easily move data between private resources and the public cloud.
- Improve cost efficiencies for a variety of performance workloads.
- Maintain complete control, compliance, and mobility of data.
- Implement a disaster recovery strategy that achieves a substantial cost savings by paying for computing power only when it is needed.

References

The following recommended documents support this NetApp Verified Architecture:

- NetApp TR-4133: NetApp Private Storage for Amazon Web Services (AWS) Solution Architecture and Deployment Guide
  www.netapp.com/us/media/tr-4133.pdf
- AWS Documentation
  http://aws.amazon.com/documentation
- NetApp TR-4316: NetApp Private Storage for Microsoft Azure Solution Architecture and Deployment Guide
  www.netapp.com/us/media/tr-4316.pdf
- Azure Documentation
  azure.microsoft.com/en-us/

- NetApp TR-4326: NetApp Private Storage for SoftLayer Solution Architecture and Deployment Guide www.netapp.com/us/media/tr-4326.pdf
- Bluemix Documentation knowledgelayer.softlayer.com

Version History

Version	Date	Document Version History
Version 1.0	March 2014	Initial release.
Version 2.0	July 2015	Updated for Azure, SoftLayer, and the Equinix Cloud Exchange. Reorganized content layout for readability.
Version 2.1	April 2016	Added information for AWS GovCloud
Version 2.2	August 2016	Added information for Azure Government
Version 2.3	March 2017	Added additional storage platforms; Updated Bluemix (SoftLayer) branding; Updated Bluemix Direct Link with Equinix Cloud Exchange

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.