White Paper

NetApp IT Approach to NetApp Private Storage and Amazon Web Services in Enterprise IT Environment

Sanjay Nighojkar, Enterprise Cloud Services, NetApp IT

October 2014 | WP-7206

TABLE OF CONTENTS

1 Abstract

The NetApp cloud strategy is based on the value of giving customers the ability to seamlessly move data and workloads between clouds: private cloud (for example, FlexPod®), public cloud providers (for example, IBM Softlayer), and hyperscale cloud providers (for example, Amazon Web Services). These different clouds are the endpoints for a NetApp cloud data fabric.

NetApp IT plays a vital role as "customer 1" and an early adopter of NetApp® solutions. NetApp IT is one of the largest enterprise customers of NetApp solutions and provides feedback to the NetApp product teams as they define future strategies to meet the business challenges of today's enterprise IT customers. The use of NetApp products and solutions for application workloads, both on the premises and with external cloud providers, allows NetApp IT to better support its own employees and partners.

NetApp IT's hybrid cloud includes a mix of on-premises and external cloud resources, one of which is Amazon Web Services (AWS). AWS, in conjunction with NetApp Private Storage (NPS), is used for workloads including development, test, and production applications that meet the criteria for off-premises hosting based on our IT cloud governance framework.

This document provides the NetApp IT story from a practitioner's viewpoint on NetApp IT hybrid cloud architecture, including the usage of (1) native AWS storage; (2) NPS; and (3) on-premises data center storage, including future plans to use Cloud ONTAP that bring the NetApp feature set to AWS storage.

The document also covers different AWS deployment models within our hybrid cloud landscape and provides architectural considerations and solution guidance for operationalizing a hybrid cloud using NPS. This document is to provide an IT practitioner's viewpoint so that other enterprise IT organizations can benefit.

Key Takeaways

- Guiding principles and architectural considerations for deployment and operations of a hybrid cloud environment, including details around colocation, multi-tenancy, security, segmentation, automation, and orchestration.
- Governance and best practices for aligning application workloads with the correct cloud services based on various factors, including risk, security, performance, data privacy, compliance, and cost.
- Hybrid cloud strategy, use cases, and benefits of using NPS.

2 Background

NetApp IT began its cloud journey in late 2010 to address the sprawl of shadow IT workloads. These application workloads were important to NetApp's business, but increased the potential of security risk and operating costs and provided little structured operational and infrastructure support. The original goal of the IT cloud offering and its service model was to rein in shadow IT and those under-the-desk systems by providing elastic compute infrastructure as a service (IaaS) to the business. This was achieved through the successful cloud service brokering with CenturyLink. In 2011 NetApp IT deployed nCloud as an IT service offering.

Today NetApp IT has a multicloud provider strategy and in 2013 embarked on an initiative to onboard AWS given its strategic partnership and leadership position (source: Gartner Magic Quadrant for cloud IaaS, August 2013). AWS became even more relevant with NetApp's announcement for NPS.

In order to onboard applications and simplify the decision process, IT created a cloud decision framework that provides an evaluation mechanism and guidance on determining "cloud-fit" applications.

The goal within NetApp IT is to become a true service broker and adopt an IT-as-a-service (ITaaS) model. This will involve the continuous enhancement and evolution of our:

- Cloud decision framework
- Cloud governance processes

- Cloud security approach
- Cloud service management framework

3 NPS Relevance for NetApp IT

As the IT industry changes, the use of multicloud or hybrid cloud is becoming an obvious choice for enterprise IT organizations. IT organizations want to drive business value by playing a role of service broker by adopting ITaaS. The subsequent sections in this document provide details around NetApp IT's evolution and transformation to hybrid cloud. This document is to provide an IT practitioner's viewpoint so that other enterprise IT organizations can benefit.

Some of the business drivers for NetApp IT to use NPS in hybrid cloud are:

- **Enterprise IT versus retail IT for cloud.** Both of these want highest return on investment (ROI), lowest total cost of ownership (TCO), full data protection, and optimal use of resources. When it comes to data protection, typical enterprise IT shops have strict auditing regulations, follow global trade and compliance laws (maybe even regional and/or country-specific regulations), and use protected global customer trade and business contracts. With retail IT, regulated governance is absent. There are no strict policies and enforcement because the goals are quick turnaround and speed to market. Retail IT providers often overlook the fact that data has inertia and is difficult to migrate after it is established.
- **Compliance**. NetApp IT strictly complies with corporate legal policies, Sarbanes-Oxley, and data privacy obligations to protect NetApp's intellectual property and business interests. Compared to retail IT options, most of these factors are flexible, tailored as needed, and change over time.
- **Security responsibility.** Typically hyperscalers and public colocated service providers (CSPs) refer to a "shared security model" that puts onus on the customer to make sure of data privacy, compliance, and legal obligations. Unless an IT organization is mature enough to manage risk, CSP storage services cannot provide 100% accountability for an organization's enterprise data (at least not initially).
- **Data mobility across cloud**. Cloud is attractive and appealing, and yet, big bang migrations and all-or-nothing approaches often fail. NetApp IT has adopted a phased approach with a selective workload migration strategy using a cloud decision framework. NetApp IT finds that large applications and data transfers using traditional data migration methods such as rsync, SSH (or secure) file transfer protocol (sFTP,) physical tape ship, export/import, and tar/untar from current state to cloud are challenging.
- **NPS as an enabler for data mobility.** NetApp IT finds that NPS acts as central data hub to give application mobility across clouds, regardless if a public, private, or storage-as-a-service (SaaS) storage platform such as Box.net or ShareFile. NPS helps to effectively manage data movement across clouds, retention, deduplication, compression, backup and recovery, optimization, and demand forecasting.
- **Standardization**. Gain process and platform services standardization across public and private cloud with a unified service delivery model.

4 NetApp IT's Strategic Goals for NPS/AWS

- Align with NetApp IT cloud adoption strategy by driving to a "cloud first" mentality while creating a hybrid IT cloud service broker and provider approach.
- Lay ground for high availability/disaster recovery (HA/DR) and hybrid cloud while making cloud services ready for enterprise-class applications through improved security and performance.
- Enable shift in application architecture to take advantage of cloud characteristics such as elasticity, cloud bursting, automation, and orchestration.
- Define standard operational processes and governance for managing hybrid cloud services.

5 NetApp IT Methodology and Approach

5.1 NPS for AWS Prerequisites

- An Amazon account with an associated payment method must be created, and this account must be associated with AWS (http://aws.amazon.com).
- Amazon AWS region in which Amazon Elastic Compute Cloud (EC2) virtual machines (Amazon Machine Images, or AMI) will be stored must be designated.
- Availability zones in the designated AWS region where AMI virtual machines will be created must be identified.
- IP address plan for virtual private cloud (VPC) (IP Classless Inter-Domain Routing Block and subnet information) must be created.
- NetApp storage controller must be installed in the colocation facility for the designated Amazon AWS region.
- IT-provided network switches and routers must be installed in the colocation facility for the designated Amazon AWS region.
- IT-provided network routers must have Border Gateway Protocol (BGP) support enabled.
- Which type of AMI virtual machine will be deployed in EC2 for the solution must be determined.
- NetApp storage system network interfaces must be connected to the customer-provided network switches.
- NetApp storage system network interfaces must be enabled and configured.

5.2 NPS Journey for NetApp IT

As NetApp IT began its journey to NPS, project phases were defined along with a corresponding checklist. Below is a sample of the phases and tasks.

Tactical Phases	Sample Tasks
Planning and sizing	• Identify use cases • Identify apps, get current capacity, and estimate growth • Apply IT standards • Make sure of on-premises storage compatibility • Size your cloud: storage and bandwidth forecast • Start small (for example, 50TB FAS6290) • Engage with CSP
Contract and costing	• Prepare bill of materials (BOM) • Establish contract with CSP • Engage with Vendor Management and legal for contract negotation/review • Consider remote management, service-level agreements (SLAs), bandwidth, and costs (monthly and non-recurring) and expand on-demand terms in contract • Make sure of exit strategy and review renewal terms (month to month)

Tactical Phases	Sample Tasks
Procurement and setup	• Consider 10GB direct connect between AWS and CSP; 1GB point-to-point virtual private network (VPN) between CSP and on-premises storage • Start with one cage and dedicated racks for business units (BUs) • Set up remote management of devices and VPN • Provide cabling for VPC • Do failover test
Design and configuration	• Follow established IT standard design and operational framework • Review network design (corporate, demilitarized zone [DMZ], public zones, storage virtual machine [SVM], and virtual routing and forwarding/virtual LANs • Provide direct connect • Manage storage (Windows® 2012R2) NetApp Oncommand Insight instance in AWS • Configure cluster interconnect switch • Configure storage cluster node install and base cluster • Provide security and access • Provision storage volume • Test system
Deployment and testing	• Set up application environment: EC2, Relational Database Services (RDS), Elastic Block Store (EBS) • Lay out disk and provision LUN • Migrate data using SnapMirror® or S3, rsync, and so on • Connect EC2, RDS with NPS volume • Test integration • Test performance and function • Launch readiness checklist validation

6 NetApp IT Solution Architecture

6.1 Overview

The following section details NetApp's internal corporate IT setup. The configuration for other organizations might vary depending on region, infrastructure, and/or business requirements.

NPS for AWS solution is a hybrid cloud architecture where NetApp FAS storage system is connected to the AWS public cloud compute and storage resources using a dedicated, high-bandwidth, low-latency network connection called Amazon Direct Connect (DX).

6.2 Solution Components

The major components of the NPS for AWS solution are the following:

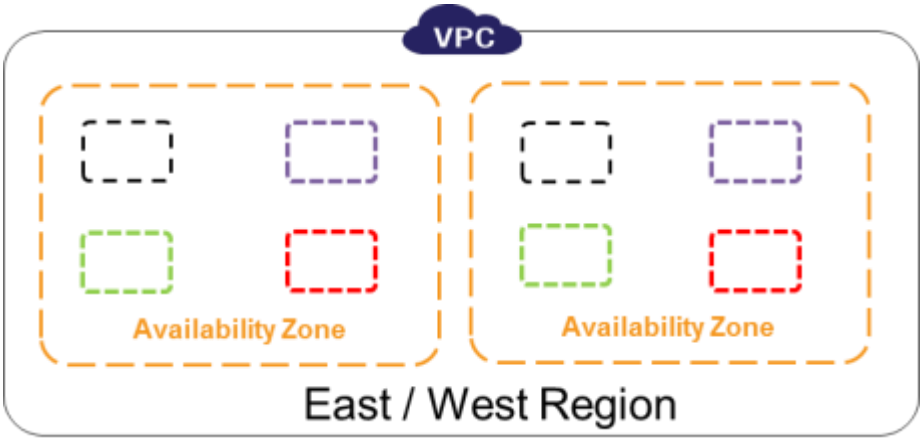
- AWS EC2 virtual machines
- Amazon DX network connection
- Amazon DX colocation facility
- NetApp FAS storage

- Network switch or router capable of supporting Layer 3 network routing (BGP and Open Shortest Path First [OSPF])

6.3 Amazon VPC and EC2 Instance

NetApp IT has set up AWS East (WV) and West (OR) regions with two availability zones.

Figure 1) VPC with two Availability Zones



The VPC has a direct connection with the NetApp data center in Research Triangle Park, North Carolina, and has these characteristics:

- Ability to traverse availability zones in a region
- Creation of our own logical network (corporate or intranet, DMZ, public or Internet) zones
- Use of NetApp internal private IP address
- Segmentation using concept of VLANs and subnet
- Provisioning of enough addresses for expansion in each VPC and region (no restriction based on broadcast domain)
- Network-based access-control lists (ACLs) that can be used to control network layer (stateless)
- Routing between subnets that can be controlled
- Routing to 0.0.0.0/0 that will be based on VPC placement
- Tagging of resource attributes

The network segmentation was done to match NetApp IT data center network design for the normalization and standardization needed for a hybrid IT Infrastructure. For the VPC, NetApp IT established security policies and standards guidelines to make sure of consistent security governance and operation.

Each VPC is divided into three network zones to host various types of workloads based on their need for exposure, access, and security requirements:

- **Intranet zone:**
  - Includes a VPN connection and has access to all corporate resources.
  - Access to Internet is only for AWS resources (for example, EC2, S3, Dynamo, API). This can be achieved through Network Access Translation or a proxy setting.
  - Firewall on corporate side allows everything inbound and outbound, except RDP/SSH from VPC back into corporate. This is to prevent security vulnerabilities and unauthorized access.
  - Default route points back to corporate.
- **DMZ zone:**

- Has access to the Internet and intranet corporate resources. Access into the Intranet is limited to specific resources.
- Intranet into DMZ resources should be accessible.
- Is default route to Internet, DMZ firewall subnet route back to corporate.

- **Public zone:**
  - Access is only to Internet; VPN connection is for authentication and administrative purposes.
  - Intranet users have access into public zone through jump host using SSH to manage servers.

Each zone can host AWS EC2 instances that eventually would connect to NPS storage volume to access NetApp business data. The EC2 instance provides cloud compute through virtual machines hosted in the AWS U.S. East region with two availability zones. Amazon EC2 supports Windows and Linux® virtual machines.

EC2 instances connect to NetApp storage using TCP/IP-based storage protocols (iSCSI, NFS, CIFS, NDMP) over the AWS DX network connection. Note that the solution architecture does not support Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) protocols.

6.4 AWS DX Colocation

NetApp IT has established a contract with Equinix IBX® occupying a starter capacity with one 19" cage equipped with 2.4 kVA power capacity and two fiber cross-connect interconnects to host NetApp storage gears. The yearly contract allows NetApp IT to expand incrementally based on need.

The colocation facility provides a set of services related to the management and support of the NetApp storage devices. Although services vary from provider to provider, Equinix will:

- Deliver parts to the cage or cabinet where the hardware is located provided Equinix is notified of any inbound shipment
- Provide access to the cage or cabinet for field support engineering assistance provided Equinix is notified of the visit beforehand

6.5 NetApp FAS Storage

All versions of NetApp FAS storage systems located in the AWS DX colocation facility can be used in this solution as long as the storage controllers are licensed for any of the TCP/IP-based storage protocols such as NFS, CIFS, iSCSI, and NDMP.

The colocation cage is installed with a NetApp IT standard storage controller FAS6290 HA pair with four DS4246 shelves using 2TB SATA disks.

NetApp IT has configured an Internet connection to the corporate network in the colocation facility for AutoSupport™ to function normally. Keeping the location and contact information for the storage controllers current to make sure that replacement parts will arrive at the correct location is important.

The support process for colocation-based FAS systems in this solution is the same as the process for standard on-premises NetApp Support for FAS systems.

6.6 Network Switches and Routers

Specific network switches and routers are not explicitly certified for use in this solution. The only requirements for the network equipment are that it must support Layer 3 network routing protocols BGP and OSPF. NetApp IT standard network gears are Cisco Nexus® 5K and 881W routers.

The network equipment is also able to support 1GbE or 10GbE connectivity to the DX network connection The physical media used for the DX network connection is single-mode fiber (SMF) cable (9/125nm SC connector type).

6.7 AWS DX Network Connection

The AWS DX network connection is a dedicated, high-bandwidth, low-latency network connection that connects AWS EC2 compute resources to the NetApp storage system in the colocation facility.

AWS DX network connections are connected to customer-provided network equipment using SMF connections. The connections can be provisioned as 1GbE or 10GbE connections. NetApp IT can connect up to 12 DX network connections for up to 120GbE of bandwidth to the NetApp FAS storage.

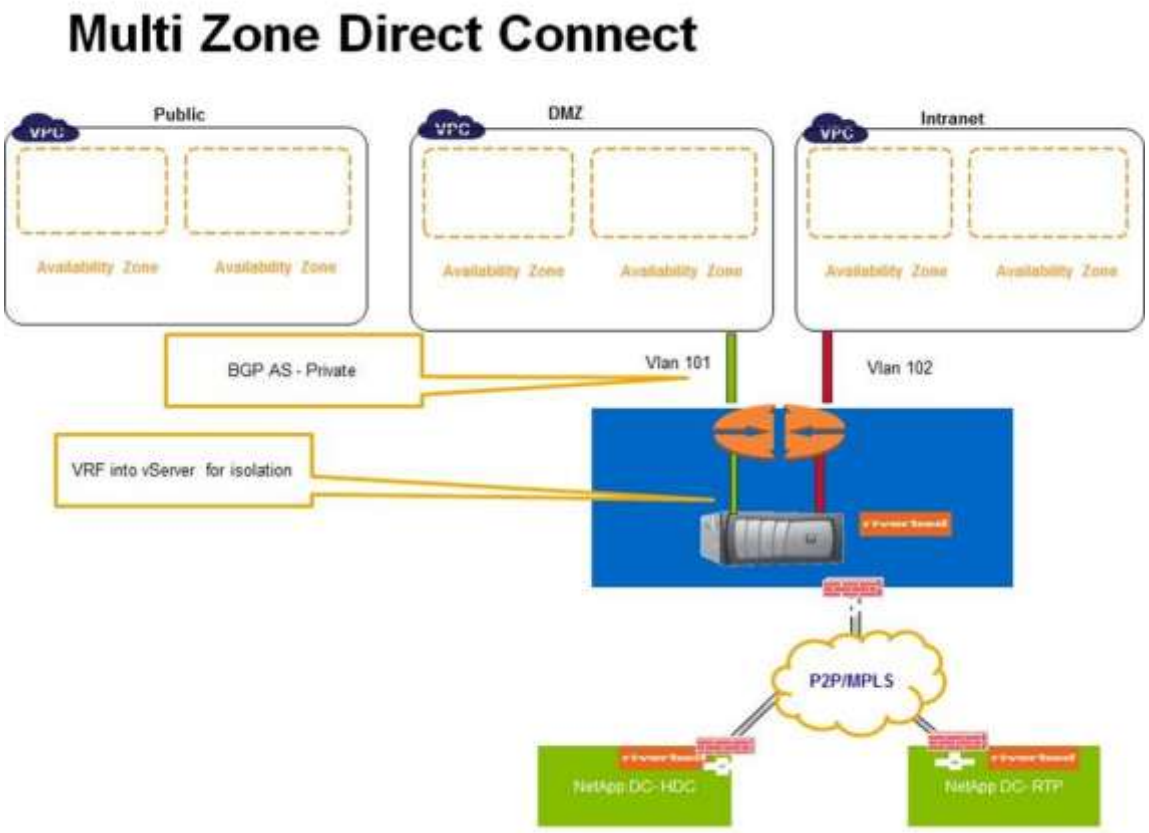
One end of the DX network connection is an AWS virtual private gateway (VGW), and the other end of the DX network connection is the NetApp IT-provided network equipment in the colocation facility.

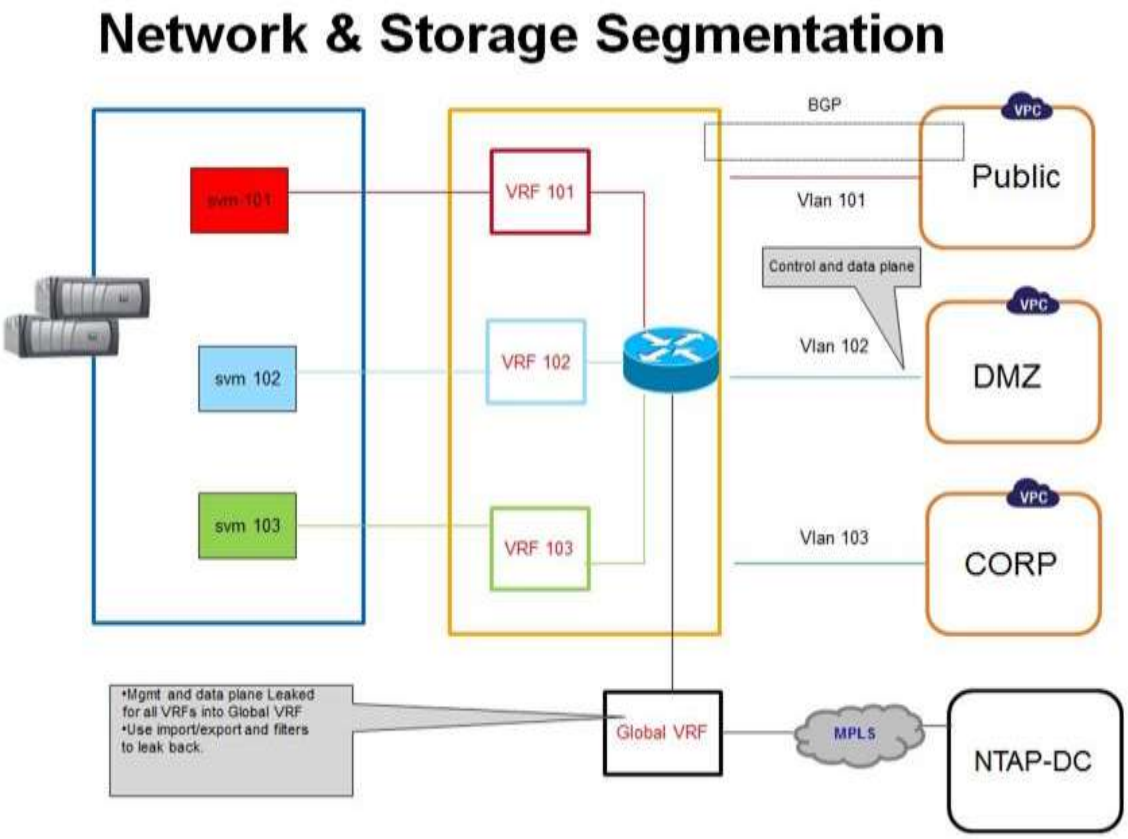
The AWS VGW is attached to a VPC network. The VPC is a virtual network in the AWS cloud that is used by the EC2 virtual machines. The VPC can be configured with subnets, routing, Internet gateways (IGWs) for EC2 virtual machine connectivity to the internet, VGWs, and network firewall functionality.

Each VGW is mapped to an AWS virtual interface. The virtual interface is configured with an 802.1Q VLAN so that the network traffic for that VGW/VPC is isolated from other VGW/VPC network traffic. The NetApp storage can be configured with VLAN interfaces on the same VLAN as the virtual interface to provide end-to-end network isolation of network traffic from VPC to NetApp.

6.8 NetApp IT AWS/NPS Solution Design

The following pictures show that the NPS is accessed only through DMZ and Intranet virtual LAN to ensure security of NetApp data and corporate services inside the IT data centers.





BGP is used to support network routing between the VPC and NetApp IT rack in the Equinix colocation facility over the DX network connection. The BGP configuration advertises local network routes and also receives the BGP advertisements from the virtual network over the network connection.

7 NetApp IT Use Cases for NPS/AWS

7.1 Use Case 1: Web Portals (Persistent and Nonpersistent Contents)

- Nonpersistent websites with HTML/front-end web server to render static contents in on-premises storage systems.
- Shared web folders to host and launch static contents by internal users to allow them to build blog sites or personal profile pages or even deploy a proof of concept/demo app on which they are working. The contents are stored on internal global storage systems that are closed to the user.
- Organization and departmental sites based on open source content management systems (for example, WordPress, Joomla, Drupal) on a cloud-based LAMP (Linux, Apache, MySQL and PHP), an open-source Web development platform. Such portals are informative, have SSO, and use IT DNS and mail services. The portals have actionable forms and static contents coming from cloud-based storage. The MySQL database is on EC2 with NPS mount.

7.2 Use Case 2: High-Performance Business Analytics Applications

- IT business analytics platform that needs high performance and high input/output per second (IOPS). Business analytics data mart for BU management reporting. The current technologies used include Pentaho BA and data integration 64 bit, OBIEE, and Oracle® 11g. Currently hosted on a single Oracle DB instance and a cloud VM with apache and Pentaho. In the future, AWS EC2 apache front-loaded with ELB and Pentaho installed connected with OBIEE and Oracle RDS on a high-IOPS performance-optimized EC2 with data/log disks mounted on NPS.

- IT dashboard to show operational metrics from IT help desk system (ServiceNow).The integration and data push from ServiceNow (SaaS) to NPS is a classic use case to validate cross-cloud data transfer performance.
- Data on demand (DoD) and BI reporting applications. Business users periodically need enterprise data from on-premises enterprise applications to generate custom management and analytical reports. Current DoD delivery vehicle is a Pentaho-/OBIEE-based platform or traditional sFTP, Excel, and/or NAS storage system–based solution. These traditional modes of data transfer are very slow and usually not secure while data is in transit. The NPS solution can provide a secure, controlled environment to deliver corporate data to business users at high speed.

7.3 Use Case 3: Application Backup Hub

NPS can be used as cloud-based storage option in lieu of using service provider's storage. This low-cost, secure, unlimited, and central storage hub can be connected to multiple public (including SaaS) and private clouds to allow scheduled application backup use NPS. In a true ITaaS model, IT can choose to meter the storage usage and either show back or charge back to the consumers. The data can be backed up on NPS through secure FTP, through IT-monitored bastion hosts, or by directly mounting the NPS volume on the source servers.

7.4 Use Case 4: Self-Service Provisioning of Dev/Test Environment

Using IT's cloud management platform and self-service portal, internal users can request and self-provision nonproduction, dev/test/stage environments with cloud compute attached to NPS storage. Self-service and reduced time to provision will provide business agility and improved time to capabilities. This is useful for consumers needing short-duration lab-on-demand resources for test and automation or proof-of-concept and demo purposes.

7.5 Use Case 5: HA/DR Using Data Mobility Across Clouds

- NPS as "storage broker" for multiple dispersed clouds, including SaaS
- Application data SnapMirror from NPS to on the premises
- Migrate application layer from one cloud to another (recreate instances) and change the storage pointers to same NPS volumes (when on-premises storage is not NetApp)
- Restore from on the premises to NPS as true hybrid storage to be used in HA/DR cases

8 NetApp IT Practitioner View of Tactical and Technical Goals

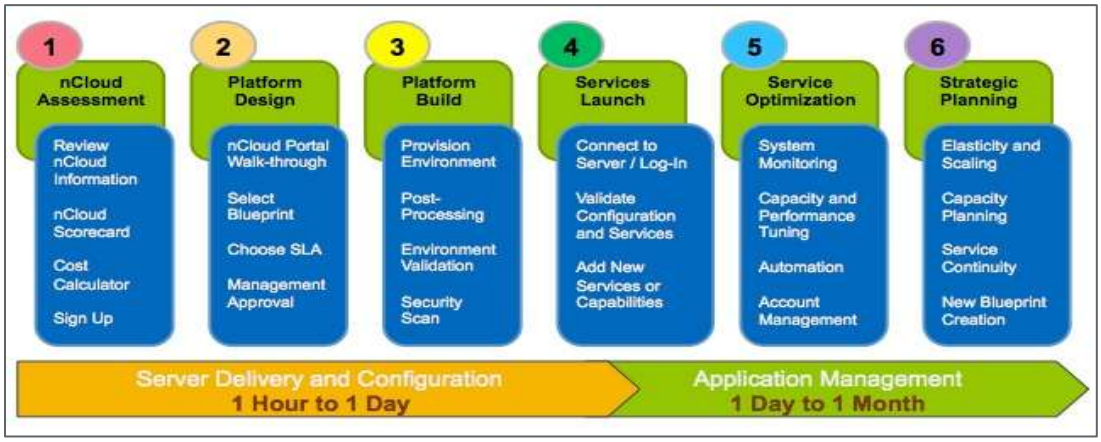
NetApp IT set up its first NPS at an Equinix colocation facility and initially started the implementation as a proof of concept to get firsthand experience. These goals helped keep the team focused on driving this innovative engineering project and demonstrates the use of NPS to maintain control and mobility of data.

- Create repeatable process to set up NPS at any location from beginning.
- Show ability to expand and procure additional colocation space (racks/cages) quickly.
- Ability to move from "shared cage model" to "dedicated cage model" through modular network and storage design.
- Create a storage metering and billing model; demonstrate pay-as-you-go chargeback/showback model for hybrid cloud services that use NPS, public cloud, and on-premises storage.
- Validate NetApp cloud capabilities in enterprise IT environment.
- Demonstrate improved security, SLA, performance, and stability in hybrid cloud environment.
- Perform detail cost and ROI analysis to get IT cloud platform TCO due to hybrid storage. Take cloud storage cost savings into account.
- Demonstrate reduced latency due to colocation/DX compared to SaaS storage services.

- Capture and validate data transfer, bandwidth, application response time, throughput, and overall resource utilization requirements for IT use cases.
- Provide ability to incrementally add resources (pay as you go).
- Provide ability to encrypt data in transit and at rest.
- Demonstrate creation of disk volume, storage scaling, thin provisioning, deduplication, compression, and other standard IT storage management and operational tasks.
- Provide ability to mount disk volume from NPS on AWS EC2 instances for static content provisioning and content management.
- Provide ability to use SnapMirror and data replication between on-premises storage and NPS.
- Provide ability to restore application data on AWS from Equinix disk volume or NetApp locations for gold/silver SLA applications.
- Demonstrate application performance in hybrid cloud:
  a. Show application running on local AWS storage.
  b. Show storage provisioning through IT cloud management platform (CMP)/policies.
  c. Mirror and migrate the application data to NPS.
  d. Show consistence application performance through CMP dashboard, reports, and AWS cloud watch monitoring service, Splunk logging, and alerts/notifications.
  e. Demonstrate storage cluster failover and seamless migration to another node.
  f. Show application running on NetApp FAS NPS.
- Demonstrate application portability between clouds:
  a. Show application running on AWS EC2 with flexible volume on NPS.
  b. Migrate the app to a new VM on private cloud through CMP.
  c. Point the NPS volume to new private cloud instance and bring up the app.
  d. Now, use SnapMirror NPS to on-premises storage on private cloud.
  e. Change the storage pointer for new private cloud VM to on-premises storage.

9 Roadmap Used by NetApp IT

Below is a six step, governance-light process to guide business users when assessing their needs. Solutions can be delivered as early as one day to one month depending on the platform design, build, and complexity of the application architecture.



Summary and Lessons Learned

The following are a few of the lessons learned and outcomes of NPS/AWS implementation in NetApp IT:

- Make sure that the Master Service Agreement MSA and contract/statement of work are signed with colocation and AWS to cover the business engagement, legal and regulatory compliance, security and data privacy policy compliance, service levels, price, and other terms and conditions (for example, tax, insurance, indemnity, and so on)
- Develop internal expertise in setting up NPS, network, DX, and AWS as you set up one location. Templatize the process for future repetition for other locations.
- Always keep in mind the upfront costs and investments made. Track monthly recurring costs and nonrecurring costs for all the services. This is required to calculate TCO and determine ROI. Make sure ROI works for your business model.
- Enable use of SnapMirror on day one to keep a copy of the data on the premises.
- Use NPS to onboard critical and high-performance apps to the cloud.
- Reengineer and redesign applications before migrating to gain the most benefits of the hybrid cloud model. Use AWS (and CSP) services and best practices as much as possible. For example:
    a. Use content delivery network (CDN) for content delivery.
    b. Use elastic load balancer (ELB) for availability and load distribution.
    c. Make the web layer as stateless as possible. Use autoscale on day one.
    d. Size the servers (EC2 instances) based on performance.
    e. Use caching (memcache and redis) as much as possible.
    f. The app layer should be optimized and innovate as much as possible. Use queuing, parallel processing, threading, memory and CPU usage optimization, locking, transactional process prioritization, and process dependency layout.
    g. Choose the right storage volume (I/O optimized, IOPS, and high performance) based on performance requirements.
    h. Use as many standard AMIs and CSP-provided services as possible.
    i. Drive usage of object store for log archiving. Use NPS for backup, Snapshot® copies, and data/application/code/content backup.
- Keep security in mind at all times. Secure data at rest and in motion by applying standard data protection measures.
- For data escrow coverage, make a copy of data on the premises.
- Make sure the operational activities are tested in a new NPS/AWS location.
- Test, test, and test to make sure promised SLA can be provided in the hybrid IT environment.

References

The following references were used in this document:

- TR-4133: NetApp Private Storage for AWS Solution Architecture and Deployment Guide www.netapp.com/us/media/tr-4133.pdf
- Amazon AWS Documentation http://aws.amazon.com/documentation

Disclaimer

This document does not intend to provide the best practices or method of installation, deployment, and usage of NetApp Private Storage. The purpose of this document is to share the NetApp IT experience using NPS in its ecosystem in conjunction with its hybrid cloud strategy, use cases, methodologies, and polices. For more information, refer to NetApp Private Storage for Amazon Web Services (AWS) or contact your sales representative for details.

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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

www.netapp.com