SoftNAS Architecture on AWS

Eric Olson, Greg Pellegrino, SoftNAS

Brandon Chavis, Amazon Web Services

May 2015

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

Network Attached Storage (NAS) software is commonly deployed to provide shared file services to users and applications. SoftNAS Cloud, a popular NAS solution that can be deployed from the Amazon Web Services (AWS) Marketplace, is designed to support a variety of market verticals, use cases, and workload types. Increasingly, SoftNAS is deployed on the AWS platform to enable block and file storage services through Common Internet File System (CIFS), NFS, and iSCSI. This paper addresses architectural considerations when deploying SoftNAS Cloud on AWS. It also provides best practice guidance for security, performance, high availability, and backup.

Introduction

NAS enables data and file sharing and is used for business-critical applications and data management. NAS systems are optimized to balance performance, interoperability, data reliability, and recoverability. Although widely deployed by IT in traditional data center environments, NAS software is increasingly used on AWS, a flexible, cost-effective, easy-to-use cloud-computing platform. Deploying NAS on Amazon Elastic Compute Cloud (Amazon EC2) provides a solution for applications that require the benefits of NAS storage in a software form factor.

About SoftNAS Cloud

SoftNAS is a software-defined NAS filer delivered as a virtual appliance running within Amazon EC2. SoftNAS provides NAS capabilities suitable for the enterprise, including cross-zone high availability with automatic failover in the AWS cloud. SoftNAS Cloud, which runs within the customer AWS account, offers business-critical data protection required for non-stop operation of applications, websites, and IT infrastructure on AWS.

This paper does not cover all SoftNAS Cloud features. For more information, see www.softnas.com.

Architecture Considerations

This section provides information critical to a successful SoftNAS installation, including application and data security, performance, interaction with Amazon Simple Storage Service (Amazon S3), and network security.

Application and Data Security

Security and protection of customer data are the highest priorities when working with SoftNAS on AWS. When SoftNAS is used in conjunction with AWS security features, such as Amazon Virtual Private Cloud (Amazon VPC) and Amazon VPC security groups, customers can deploy a secure data storage solution.

SoftNAS uses the CentOS 6.5 Linux distribution, which is managed, updated, and patched as part of a normal release cycle. SoftNAS StorageCenter, the web-accessible SoftNAS administration console, can be used to check the current software revision and apply available updates. For security and compliance reasons, SoftNAS support should approve any custom package before it is installed on a SoftNAS instance.

Web-based administration through StorageCenter is SSL-encrypted and password-protected by default. The Apache web server may support other authentication schemes.

SoftNAS can be administered through SSH and a secure API. On AWS, all SSH sessions use public/private key access control. Logging in as root is prohibited. Administrative access through API and command line interface (CLI) over SSH are SSL-encrypted and authenticated.

Iptables, a commonly used software firewall, is included with SoftNAS and can be customized to accommodate more restrictive and finer-grained security controls. Data access is performed across a private network by NFS, CIFS, and iSCSI. The list or range of clients addresses allowed to perform data access can also be restricted.

SoftNAS offers encryption options for data security. If NFS is used, all Linux authentication schemes are supported, including Network Information Service (NIS), Lightweight Directory Access Protocol (LDAP), Kerberos, and restrictions based on UID and GID. Using CIFS, security is managed through StorageCenter, facilitating basic Windows user and group permissions. Active Directory integration is supported for more advanced user and permissions management in Windows environments.

The SnapReplicate feature provides block-level replication between two SoftNAS instances. SnapReplicate between source and target SoftNAS instances sends all data through SSH and authenticates using RSA PKI. Data is encrypted in transit using industry-standard ciphers. The default cipher for encryption is blowfish-cbc, selected for its speed and security, but you can use any cipher supported by SSH, including aes256-cbc.

SoftNAS uses the AWS Identity and Access Management (IAM) service to control access of the SoftNAS appliance to other AWS services. IAM roles are designed to allow

applications to securely make API calls from an instance without requiring the explicit management of secret and access keys. When an IAM role is applied to an Amazon EC2 instance, the role handles key management, rotating keys periodically and making them available to applications through Amazon EC2 metadata.

Performance

The performance of a NAS system on Amazon EC2 depends on many factors, including the Amazon EC2 instance type, the number and configuration of Amazon Elastic Block Store (Amazon EBS) volumes, the use of Provisioned IOPS with Amazon EBS, and the application workload. Benchmark your application on several Amazon EC2 instance types and storage configurations to select the most appropriate configuration.

SoftNAS provides AMIs that support both paravirtual (PV) and hardware virtual machine (HVM) virtualization. To take advantage of special hardware extensions (CPU, network, and storage) for optimal performance, SoftNAS recommends that you use a current generation instance type and an HVM AMI with SR-IOV support.

To increase the performance of your system, you need to know which of the server's resources is the performance constraint. If CPU or memory limits your system performance, you can scale up the memory, compute, and network resources available to the software by choosing a larger Amazon EC2 instance type. Use StorageCenter dashboard performance charts and Amazon CloudWatch to monitor your performance and throughput results.

Amazon EC2 instances are allocated varying amounts of CPU, memory, and network capabilities. Some instance families have higher ratios of CPU to memory, or higher ratios of memory to CPU. In general, to achieve the best performance from your SoftNAS appliance, select an instance with large amounts of memory, up to 70 percent of which will be dedicated to high-speed dynamic random-access memory (DRAM) cache. If possible, select an instance with advanced networking or 10 Gigabits per second (Gbps) network interfaces because this will significantly improve SoftNAS performance. If available, choose an EBS-optimized instance. For production workloads, SoftNAS does not recommend using T1, T2, or C1 instances, primarily due to memory constraints. At the time of this writing, R3 instances are the best price/performance ratio instance for SoftNAS.

If your performance is limited by disk I/O, you can make configuration changes to improve the performance of your disk resources.

Because Amazon EBS is connected to an Amazon EC2 instance over the network, instances with higher network bandwidth will be able to provide more Amazon EBS performance. Some instance types support the Amazon EBS-optimized flag

(ec2:EbsOptimized), which provides a dedicated network interface for Amazon EBS-bound traffic (storage I/O), is designed to reduce variability in storage performance due to contention with network I/O. Instances with 500 Mbps of throughput can provide roughly 4,000 input/output operations per second (IOPS) at 16 KB I/O size; instances with 1000 Mbps of throughput can provide 8,000 IOPS at 16 KB I/O size; and instances with 2000 Mbps of throughput can provide 16,000 IOPS at 16 KB I/O size.

Amazon EBS measures each I/O operation per second that is 256 KB or smaller as one IOP. Operations larger than 256 KB are counted in 256 KB capacity units. For example, a 1,024 kB I/O would count as four 256 KB IOPs.

Provisioned IOPS Versus General Purpose Volumes

Standard Amazon EBS volumes are able to provide 100 IOPS per volume. Unlike Standard Amazon EBS volumes, which are backed by magnetic disk, Provisioned IOPS (SSD) and General Purpose (SSD) volumes have different performance characteristics, such as higher total IOPS and throughput capabilities.

There are some differences between Provisioned IOPS and General Purpose volumes, however.

General Purpose volumes provide a fixed 1:3 ratio between gigabytes and IOPS provisioned, so a 100 GB General Purpose volume will provide 300 IOPS. General Purpose volumes less than 1 terabyte (TB) in size can also burst for short periods, up to 3,000 IOPS. General Purpose volumes up to 16 TB and 10,000 IOPS can be provisioned.

Provisioned IOPS volumes are intended for workloads that demand consistent performance, such as databases. Provisioned IOPS volumes up to 16 TB and 20,000 IOPS can be created. Over a year, Amazon EBS Provisioned IOPS volumes are designed to deliver within 10 percent of the provisioned IOPS performance 99.9 percent of the time.

There are differences in total throughput capabilities between Provisioned IOPS and General Purpose SSD volumes, too. Provisioned IOPS volumes are designed to provide up to 320 MB/second of throughput; General Purpose SSD volumes are designed to provide up to 160 MB/second.

RAID

If you need more I/O capabilities than a single volume can provide, you can create an array of volumes with redundant array of independent disks (RAID) software to aggregate the performance capabilities of each volume in the array. For example, a stripe of two 4,000 IOPS volumes will allow for a theoretical maximum of 8,000 IOPS.

RAID 0 and RAID 10 are the two RAID levels recommended for use with Amazon EBS. RAID 0, or striping, has the advantage of providing a linear performance increase with every volume added to the array (up to the maximum capabilities of the host instance). Two 4,000 IOPS volumes will provide 8,000 IOPS, three will provide 12,000, and so on. However, because RAID 0 does not provide redundancy, it has less durability than a single volume. It also aggregates the failure rate of each volume in the array. RAID 10 is a good compromise because it provides increased redundancy, aggregates the read performance of all the volumes in the array, and provides a mirror of stripes in the array. However, RAID 10 is not without drawbacks: there is a 50 percent penalty to write performance and a 50 percent reduction in available storage capacity. This penalty is due to half of the disks in the array being reserved for a mirror; RAID 10 has the same write penalty as RAID 1.

RAID 5 and 6 are not recommended because parity calculations incur significant overhead without dramatically increasing the durability of the volume set. Such a large write penalty makes these RAID levels very expensive to run in terms of both dollars and I/O.

In general, RAID using mirroring or parity for increased durability adds extra steps and reduces performance, while not necessarily increasing the durability of the data. Amazon EBS has its own durability mechanisms; it can be supplemented with Amazon S3-based snapshots and SoftNAS replication to more than one Availability Zone.

DRAM cache can dramatically increase read IOPS performance. Choose instances with more memory for the best read IOPS and throughput. For an even larger read cache, choose instance types with ephemeral SSD locally attached disks and attach an SSD cache device to each storage pool. To ensure their availability, attach local SSD ephemeral disks to the SoftNAS instance when you create the instance.

Many instance types provide instance-store or “ephemeral” volumes. Because these volumes are located physically inside the underlying host of the instance, these volumes are not affected by performance variability from network overhead. Although this varies by instance type, most instance-store volumes (especially on newer instance types) are SSD volumes. However, because a stop and start of an instance moves the instance to another underlying host, stopping and starting an instance will cause all data on these volumes to be lost. SoftNAS does not support the use of these volumes for data set storage. They should only be used as a read cache for storage pools.

If you require additional write caching, IOPS, SSD-backed Amazon EBS volumes can be attached to a storage pool. The use of locally attached ephemeral disks for write cache is not recommended.

Consider your workload requirements and priorities. If the amount of storage and cost take priority over speed, Standard Amazon EBS volumes might be the right choice. In

general, General Purpose SSD or Provisioned IOPS volumes offer the best mix of price, performance, and total storage space. With AWS and SoftNAS, you can add more storage or configure a different type of storage on the fly.

Leveraging Amazon S3 with SoftNAS

SoftNAS provides support for a feature known as SoftNAS S3 Cloud Disks, which are abstractions of Amazon S3 storage presented as a block device. By leveraging Amazon S3 storage, SoftNAS can scale cloud storage to practically unlimited capacity. A cloud disk can be provisioned to hold up to four petabytes (PB) of data; if a larger data store is required, RAID can be used to aggregate multiple cloud disks.

Each SoftNAS S3 Cloud Disk occupies a single Amazon S3 bucket in AWS. The administrator chooses in which AWS region the Amazon S3 bucket and cloud disk will be created. For best performance, choose the same region for both the SoftNAS Amazon EC2 instance and its Amazon S3 buckets.

SoftNAS storage pools and volumes using cloud disks have the full, enterprise-grade NAS features (for example, deduplication, compression, caching, storage snapshots, and so on) available and can be readily published for shared access through NFS, CIFS, and iSCSI.

When using a cloud disk, use a block device local to the SoftNAS appliance as a read cache.

Network Security

Amazon VPC is a logically separated section of the AWS cloud that provides customers complete control over the networking configuration, including the provisioning of an IP space, subnet size and scope, access control lists, and route tables. Subnets inside an Amazon VPC can be marked as either public or private. The difference between public and private subnets is that a public subnet has a direct route to the Internet; a private one does not. When you configure an Amazon VPC to use with SoftNAS, consider the level of access required by your use case. If the SoftNAS appliance does not need to be accessed from the public Internet, consider placing it in private Amazon VPC subnets.

To leverage SoftNAS S3 Cloud Disks, the SoftNAS appliance must have a way to access the Internet; if the appliance is in a private subnet, a NAT instance can be used to proxy traffic to and from the Internet.

A VPC security group acts as a virtual firewall for your instance to control inbound and outbound traffic. For each security group, you add rules that control the inbound traffic to

instances and a separate set of rules that control the outbound traffic. Open only those ports that are required for the operation of your application. Restrict access to specific remote subnets or hosts.

For a SoftNAS installation, determine which ports must be opened to allow access to required services. These ports can be divided in three categories: management, file services, and high availability.

Open the following ports to manage SoftNAS through StorageCenter and SSH. As the table indicates, the source should be limited to hosts and subnets where management clients are located.

Type	Protocol	Port	Source
SSH	TCP	22	Management
HTTPS	TCP	443	Management

When providing file services, first determine which services you will provide. The following tables show which ports to open for security group configuration. As the tables indicate, the source should be limited to clients and subnets that will be consuming these services.

NFS

Type	Protocol	Port	Source
Custom TCP Rule	TCP	111	Clients
Custom TCP Rule	TCP	2010	Clients
Custom TCP Rule	TCP	2011	Clients
Custom TCP Rule	TCP	2013	Clients
Custom TCP Rule	TCP	2014	Clients
Custom TCP Rule	TCP	2049	Clients
Custom UDP Rule	UDP	111	Clients

Type	Protocol	Port	Source
Custom UDP Rule	UDP	2010	Clients
Custom UDP Rule	UDP	2011	Clients
Custom UDP Rule	UDP	2013	Clients
Custom UDP Rule	UDP	2014	Clients
Custom UDP Rule	UDP	2049	Clients

CIFS/SMB

Type	Protocol	Port	Source
Custom TCP Rule	TCP	137	Clients
Custom TCP Rule	TCP	138	Clients
Custom TCP Rule	TCP	139	Clients
Custom UDP Rule	UDP	137	Clients
Custom UDP Rule	UDP	138	Clients
Custom UDP Rule	UDP	139	Clients
Custom TCP Rule	TCP	445	Clients
Custom TCP Rule	TCP	135	Clients

Microsoft Active Directory Integration

Type	Protocol	Port	Source
LDAP	TCP	389	Clients

iSCSI

Type	Protocol	Port	Source
Custom TCP Rule	TCP	3260	Client IPs

The following security group configuration is required when you deploy SnapHA, which is discussed later in this paper. As the table indicates, the source should be limited to the IP addresses of the SoftNAS appliance.

High Availability with SnapHA

Type	Protocol	Port	Source
Custom ICMP Rule	Echo Reply	22	SoftNAS IPs
Custom ICMP Rule	Echo Request	443	SoftNAS IPs

Backup Considerations

Creating a comprehensive strategy for backing up and restoring data is complex. In some industries, regularity requirements for data security, privacy, and records retention must be considered. SoftNAS provides multiple capabilities for backup options.

SoftNAS Snapshots

SoftNAS snapshots are volume-based, point-in-time copies of data. StorageCenter provides a rich set of snapshot scheduling and on-demand capabilities. Snapshots consume storage pool capacity, so usage must be monitored for over-consumption.

SoftNAS snapshots are integrated with Microsoft Windows Previous Versions, which is provided through the Microsoft Volume Shadow Copy Service (VSS) API. This feature is

accessible to operating system users through the **Previous Versions** tab, so IT administrators do not need to assist in file recovery. Microsoft server and desktop operating system users can leverage scheduled snapshots to recover deleted files, view or restore a version of a file that has been overwritten, and compare file versions side-by-side. Operating systems supported include Windows 7, Windows 8, Windows Server 2008 and Windows Server 2012.

SoftNAS SnapClones

SnapClones provide read/write clones of SoftNAS snapshots. They are created instantaneously due to the space-efficient, copy-on-write model. Initially, SnapClones take up no capacity and grow only when writes are made to the SnapClone. SnapClones are mountable as external NFS or CIFS shares. They are good for manipulating copies of data too large or complex to be practically copied, for example, testing new application versions against real data and selective recovery of files and folders using the native file browsers of the client operating system.

Amazon EBS Snapshots

SoftNAS has built in the capability to leverage Amazon EBS point-in-time snapshots to back up EBS-based storage pools. The Amazon EBS snapshot copies the entire SoftNAS storage pool, for backup and recovery purposes. Advantages include the ability to use the AWS console to manage the snapshots. Capacity for the Amazon EBS snapshots is not counted against the storage pool capacity. Amazon EBS snapshots can be used for longer-term data retention.

Deployment Scenarios

The design of your SoftNAS installation on Amazon EC2 depends on the amount of usable storage and your requirements for IOPS and availability

High-Availability Architecture

To realize 99.999% uptime for storage infrastructure on AWS, SoftNAS strongly recommends implementing SnapHA in a high-availability configuration. The SnapHA functionality in SoftNAS provides high availability and automatic, seamless failover across Availability Zones.

SnapHA leverages secure block level replication provided by SoftNAS SnapReplicate to provide a secondary copy of data to a controller in another Availability Zone, and provides both automatic and manual failover.

There are two methods for achieving high availability across zones: AWS Elastic IP addresses and SoftNAS private virtual IP-based HA.

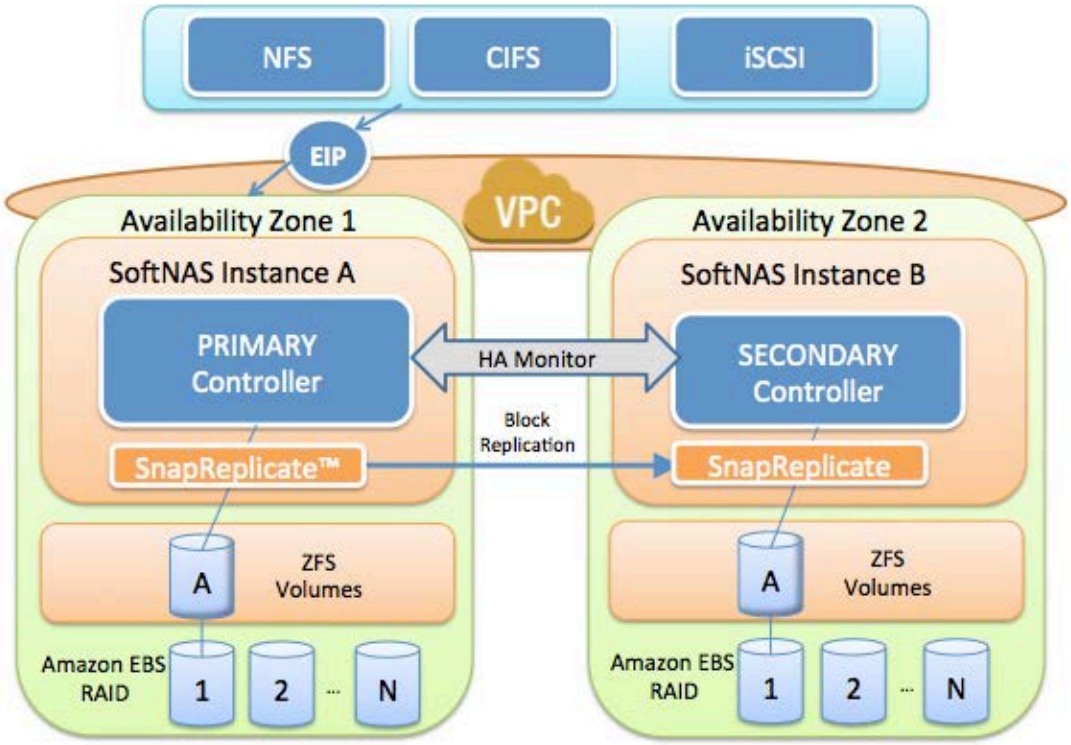

Figure 1: Task Creation and Result Aggregation

Cross-zone HA operates within a VPC. NAS traffic is routed through an enhanced elastic IP address using SoftNAS patent-pending Elastic HA technology; that is, NFS, CIFS, and iSCSI traffic is routed to a primary SoftNAS controller in one zone, and a secondary controller operates in a different Availability Zone. NAS clients can be located in any Availability Zone. SnapReplicate performs block replication from the primary controller, A, to the backup controller, B, keeping the secondary updated with the latest changed data blocks once per minute. In the event of a failure in Availability Zone 1 shown in the preceding figure, the Elastic HA IP automatically fails over to controller B in Availability Zone 2, in less than 30 seconds. Upon failover, all NFS, CIFS, and iSCSI sessions reconnect with no impact on NAS clients (that is, no stale file handles and no need to restart).

HA with Private Virtual IP Addresses

The virtual IP-based HA technology in SoftNAS allows two SoftNAS instances to be deployed inside the private subnet of a VPC. The SoftNAS instances can then be configured with private IP addresses, which are completely isolated from the Internet. This allows for more flexible deployment options and greater control over access to the appliance. In addition, using private IP addresses allows for faster failover because waiting for an EIP to switch instances is no longer required.

For most use cases, cross-zone HA using private virtual IP addresses is the recommend method.

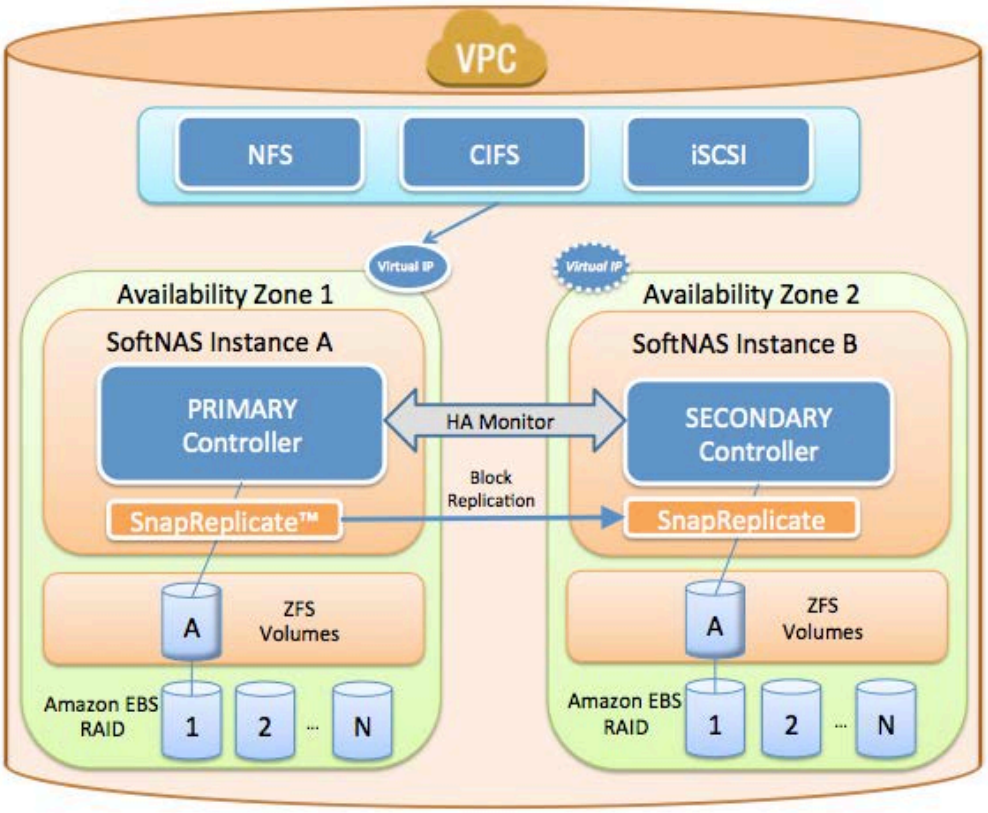

Figure 2: Cross-Zone HA with Virtual Private IP Addresses

For more information about implementation, see SoftNAS High Availability Guide.

Single Controller Architecture

In scenarios where 99.999% availability is not required, you can deploy a single controller.

The following figure shows a basic SoftNAS Cloud instance running within a VPC.

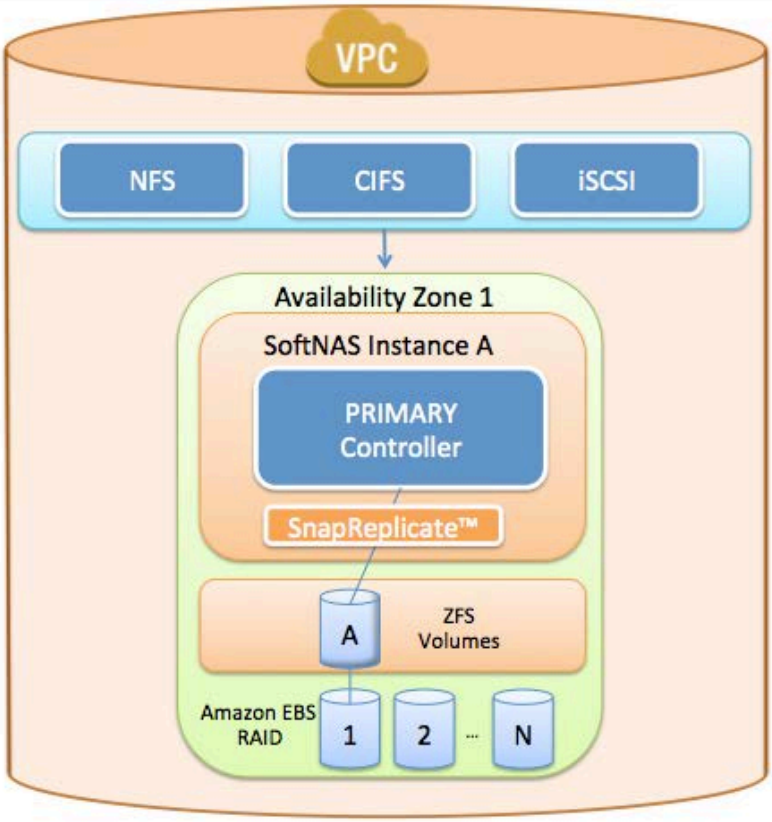

Figure 3: Basic SoftNAS Cloud Instance Running in a VPC

In this example, four EBS volumes are combined into a RAID 10 array for the storage pool on the left to provide 2 terabytes (TB) of usable storage space with no drive failure redundancy. Another storage pool is configured for RAID 0 (striping) for improved performance and IOPS. A third pool has been created using a SoftNAS S3 Cloud Disk.

Volumes are provisioned from the storage pools, and then shared through NFS, CIFS/SMB, or iSCSI.

Hybrid Cloud Architecture

SoftNAS can be deployed in a Hybrid Cloud architecture in which a SoftNAS appliance is installed both in Amazon EC2 and on-premises. This architecture allows for replication of data from on-premises to Amazon EC2 and vice versa, providing synchronized data access to users and applications. Hybrid Cloud architectures are also useful for backup and disaster recovery scenarios, in which AWS can be used as an off-site backup location.

Replication

SoftNAS can be deployed in Amazon EC2 as a replication target using SnapReplicate; this enables scenarios such as backup, disaster recovery, and development environments by copying on-site production data into Amazon EC2, as shown in the following figure.

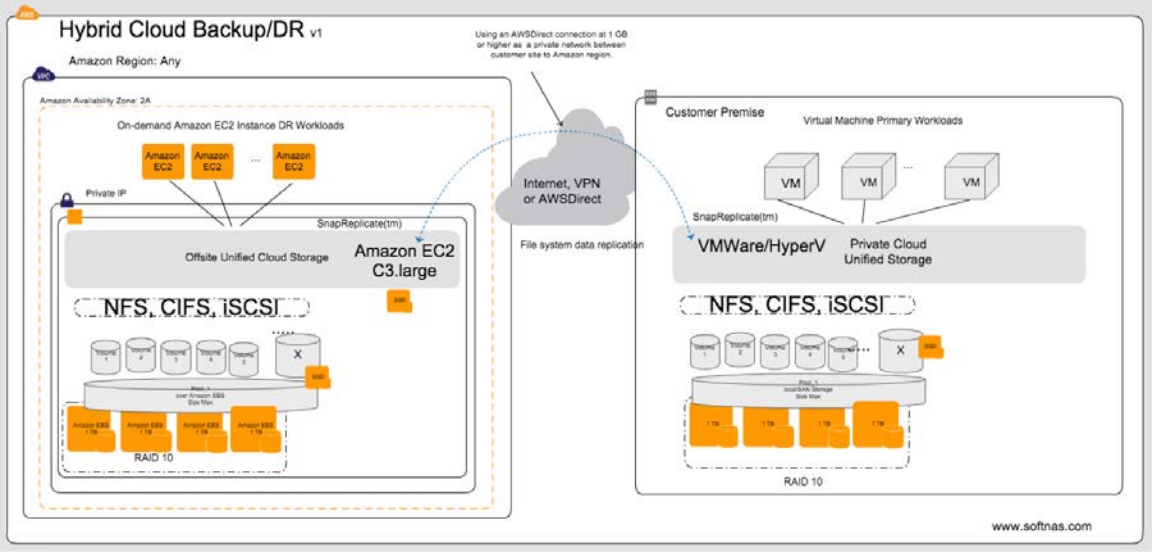

Figure 4: Hybrid Cloud Backup and Disaster Recovery

File Gateway to Amazon S3

SoftNAS Cloud File Gateway is a SoftNAS on-premises product deployed in local data centers on popular hypervisors, such as VMware vSphere and Microsoft Hyper-V. SoftNAS Cloud File Gateway connects to Amazon S3 storage, treating Amazon S3 as a disk device. The Amazon S3 disk device is added to a storage pool where volumes can export CIFS, NFS, iSCSI, and Apple Filing Protocol (AFP). Amazon S3 is cached with block disk devices for read and write I/O. Write I/O is cached at primary storage speeds and then flushed to Amazon S3 at the speed of the WAN. When using Amazon S3-

based volumes with backup software, the write cache will dramatically shorten the backup window.

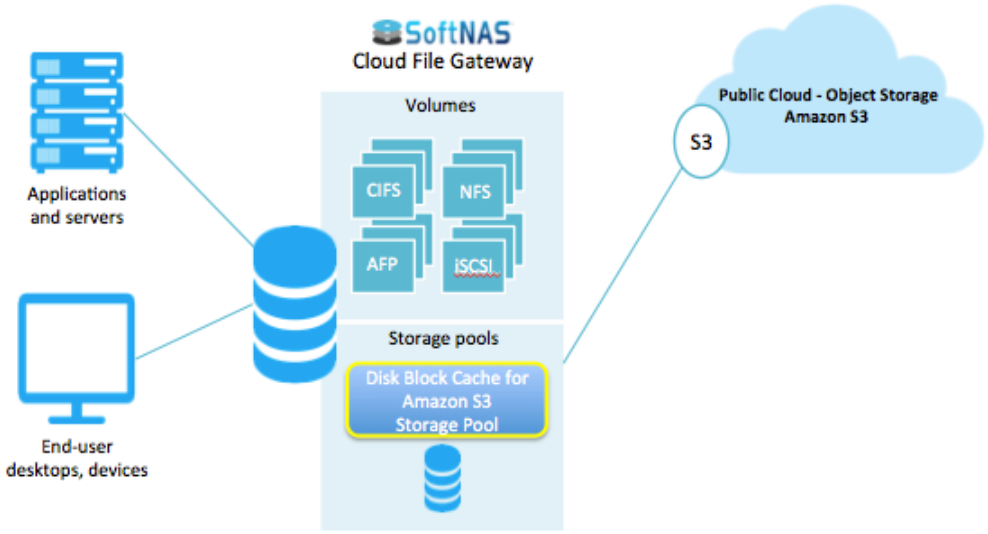

Figure 5: SoftNAS Cloud File Gateway

Automation Options

This section describes how the SoftNAS REST API and CLI and AWS CloudFormation can be used for automation.

API and CLI

SoftNAS provides a secure REST API and CLI. The REST API provides access to the same storage administration capabilities from any programming language using HTTPS and REST verb commands, returning JSON-formatted response strings. The CLI provides command line access to the API set for quick and easy storage administration. Both methods are available for programmatic storage administration by DevOps teams who want to design storage into automated processes. For more information, see SoftNAS API and CLI Guide.

AWS CloudFormation

AWS CloudFormation is a service that lets developers and businesses create a collection of related AWS resources and provision them in an orderly and predictable way.

SoftNAS provides sample CloudFormation templates you can use for automation. These templates can be found here and in the Further Reading section of this paper. When you

work with the AWS CloudFormation templates, pay careful attention to the Instance Type, Mappings, and User Data sections shown in the following examples.

```
    "InstanceType" : {
      "Description" : "SoftNAS EC2 instance type",
      "Type" : "String",
      "Default" : "t1.micro",
      "AllowedValues" : [ "t1.micro", "m1.small",
"m1.medium", "m1.large", "m1.xlarge", "m2.xlarge",
"m2.2xlarge", "m2.4xlarge", "m3.medium", "m3.large",
"m3.xlarge", "m3.2xlarge", "hi1.4xlarge", "hs1.8xlarge",
"c1.medium", "c3.large", "c3.2xlarge", "c3.4xlarge",
"c3.8xlarge", "c1.xlarge" ],
```

List all instance types you want to show up. Edit this section with the latest instance types available.

```
"Mappings" : {
    "RegionMap" : {
      "us-east-1" : { "AMI" : "ami-xxx" },
      "ap-northeast-1" : { "AMI" : "ami-xxx" },
      "ap-southeast-1" : { "AMI" : "ami-xxx" },
      "ap-southeast-2" : { "AMI" : "ami-xxx" },
      "eu-west-1" : { "AMI" : "ami-xxx" },
      "sa-east-1" : { "AMI" : "ami-xxx" },
      "us-west-1" : { "AMI" : "ami-xxxxx" },
      "us-west-2" : { "AMI" : "ami-6e55375e" }
    }
  },
```

Map to the appropriate AMIs here. SoftNAS regularly updates AMIs, so this section must be updated accordingly.

```
"UserData" : { "Fn::Base64" : { "Fn::Join" : ["", [
"#!/bin/bash -v\n",
"# Configure NFS / CIFS Shares \n",
```

```
"/var/www/softnas/scripts/initproc.sh 2>&1 \n",
```

This section is used to pass variables to the SoftNAS CLI for additional configuration.

```
"wget http://www.softnas.com/docs/softnas/v2/api/softnas-
cmd.zip \n",
"unzip softnas-cmd.zip \n",
"mv softnas-cmd /usr/local/bin/ \n",
"chmod 755 /usr/local/bin/softnas-cmd \n",
"INSID=`curl http://169.254.169.254/latest/meta-
data/instance-id` \n",
"/usr/local/bin/softnas-cmd login softnas $INSID --base_url
https://localhost/softnas --pretty_print >> /tmp/cf.tmp
2>&1 \n",
"/usr/local/bin/softnas-cmd createpool /dev/xvdj:/dev/xvdk
pool1 1 on -t >> /tmp/cf.tmp 2>&1 \n",
"/usr/local/bin/softnas-cmd createvolume volume1 pool1
filesystem thin exportNFS=on shareCIFS=on dedup=on
enable_snapshot=on schedule_name=Default hourlysnaps=5
dailysnaps=10 weeklysnaps=0 -t >> /tmp/cf.tmp 2>&1 \n"
```

Conclusion

SoftNAS Cloud is a popular NAS option on the AWS cloud computing platform. By following the implementation considerations and best practices highlighted in this paper, you will maximize the performance, durability, and security of your SoftNAS Cloud implementation on AWS.

For more information about SoftNAS Cloud, see www.softnas.com.

Get a Free 30-day trial of SoftNAS Cloud now.

Further Reading

SoftNAS References

SoftNAS Cloud Installation Guide

SoftNAS Reference Guide

SoftNAS Cloud High Availability Guide

SoftNAS Cloud API and Cloud Guide

AWS CloudFormation Templates for HVM and PV

Amazon Web Services References

Amazon Elastic Block Store

Amazon EC2 Instances

AWS Security Best Practices

Amazon Virtual Private Cloud Documentation