
Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint

AWS Whitepaper



Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint: AWS Whitepaper

Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint	1
Abstract	1
Introduction	1
About AWS Marketplace	3
About SoftNAS Cloud NAS	5
Architecture Considerations	6
Capacity Planning	6
Storage Performance	6
Fault Tolerance	6
High Availability	6
High-Level Architecture	7
Deployment	8
SoftNAS IAM Policy and Role	8
Marketplace AMI Deployment with EC2 Console	9
Limited Access Security Group	11
Configuration	13
Administrative Setup	13
Active Directory Membership	17
SoftNAS Snap Replication	19
SoftNAS SNAP HA	20
Conclusion	23
Resources	24
Document Details	25
Contributors	25
.....	25
AWS Glossary	26

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint

Publication date: **January 2018** ([Document Details](#) (p. 25))

Abstract

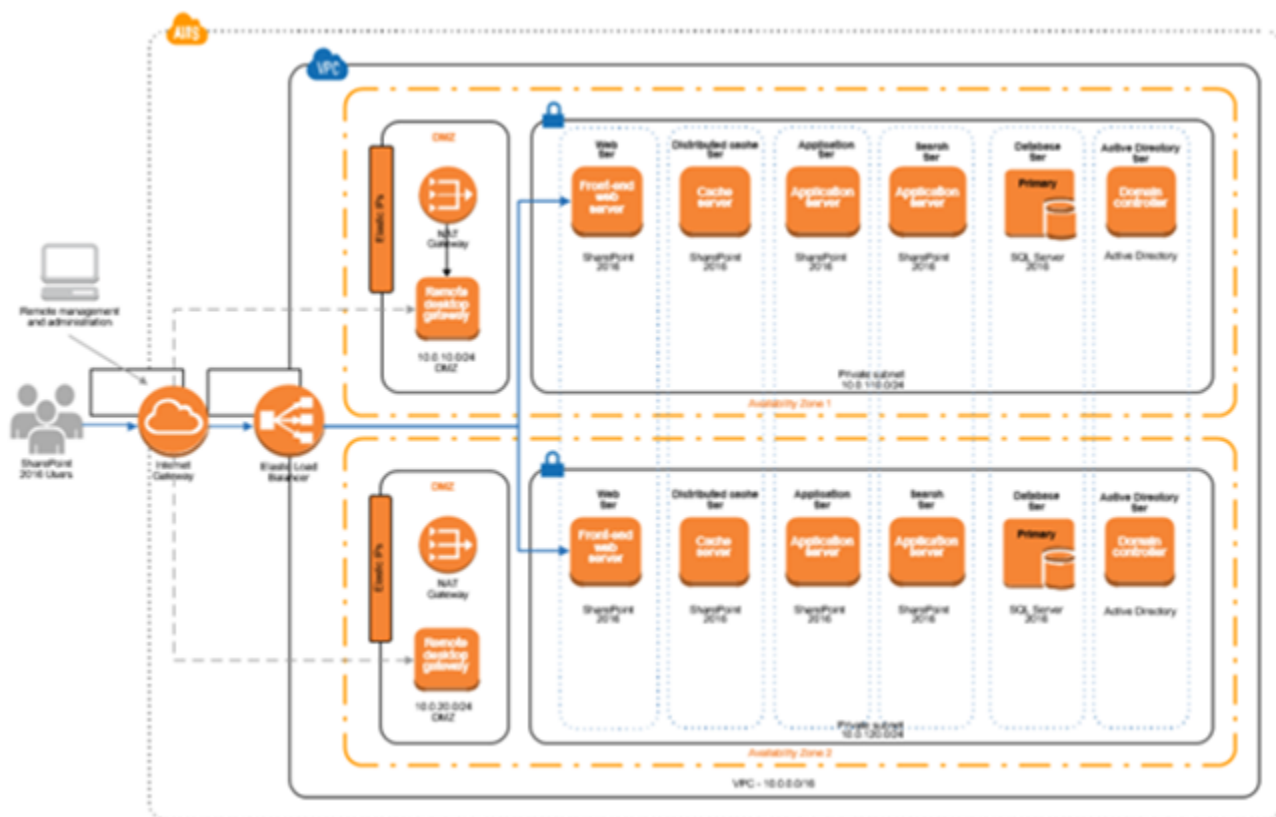
Designing a cloud storage solution to accommodate traditional enterprise software such as Microsoft SharePoint can be challenging. Microsoft SharePoint is complex and demands a lot of the underlying storage that's used for its many databases and content repositories. To ensure that the selected storage platform can accommodate the availability, connectivity, and performance requirements recommended by Microsoft you need to use third-party storage solutions that build on and extend the functionality and performance of Amazon Web Services (AWS) storage services.

An appropriate storage solution for Microsoft SharePoint needs to provide data redundancy, high availability, fault tolerance, strong encryption, standard connectivity protocols, point-in-time data recovery, compression, ease of management, directory integration, and support. The focus of this paper is to walk through the deployment and configuration of SoftNAS Cloud NAS, an AWS Marketplace third-party storage product that provides secure, highly available, redundant, and fault-tolerant storage to the Microsoft SharePoint collaboration suite.

Introduction

Successful Microsoft SharePoint deployments require significant upfront planning to understand the infrastructure and application architecture required. A successful deployment would ensure performance, scalability, high availability, and fault tolerance across all aspects of the application. The primary component of a successful Microsoft SharePoint architecture is the proper understanding and sizing of the storage system used by the SQL Server databases that store, analyze, and deliver content for the SharePoint application.

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint AWS Whitepaper Introduction



Microsoft SharePoint requires storage for several key aspects of its architecture to include a quorum for the Windows Services Failover Cluster (WSFC), WSFC witness server CIFS file share, Microsoft SQL Server Always On clustered database storage, Remote Blob Storage (RBS), and Active Directory integration.

Microsoft provides detailed guidance on SharePoint storage architecture and capacity planning in the Storage and SQL Server capacity planning and configuration (SharePoint Server) documentation on TechNet at [https://technet.microsoft.com/en-us/library/cc298801\(v=office.16\).aspx](https://technet.microsoft.com/en-us/library/cc298801(v=office.16).aspx). This guidance, described in the [Architecture Considerations](#) (p. 6), provides details about how you can use a SharePoint implementation, the types and numbers of objects that you can store, the performance required for object storage and retrieval, and the storage design that best fits the requirements for a SharePoint implementation. This guidance drives how you can use the underlying storage provisioned with AWS in conjunction with AWS Marketplace third-party storage products to provide a successful storage architecture for deploying Microsoft SharePoint on AWS.

About AWS Marketplace

AWS Marketplace is a curated digital catalog that provides a way for customers around the globe to find, buy, and immediately start using software that runs on AWS. The storage software products available on AWS Marketplace are provided and maintained by industry newcomers with born-in-the-cloud solutions as well as existing industry leaders. They include many mainstream storage products that are already familiar and commonly deployed in enterprises.

AWS Marketplace provides value in several ways: saving money with flexible pricing options, access to easy 1-click deployments of preconfigured and optimized Amazon Machine Images (AMIs), software as a service (SaaS), AWS CloudFormation templates, and ensures that products are scanned periodically for known vulnerabilities, malware, default passwords, and other security-related concerns.

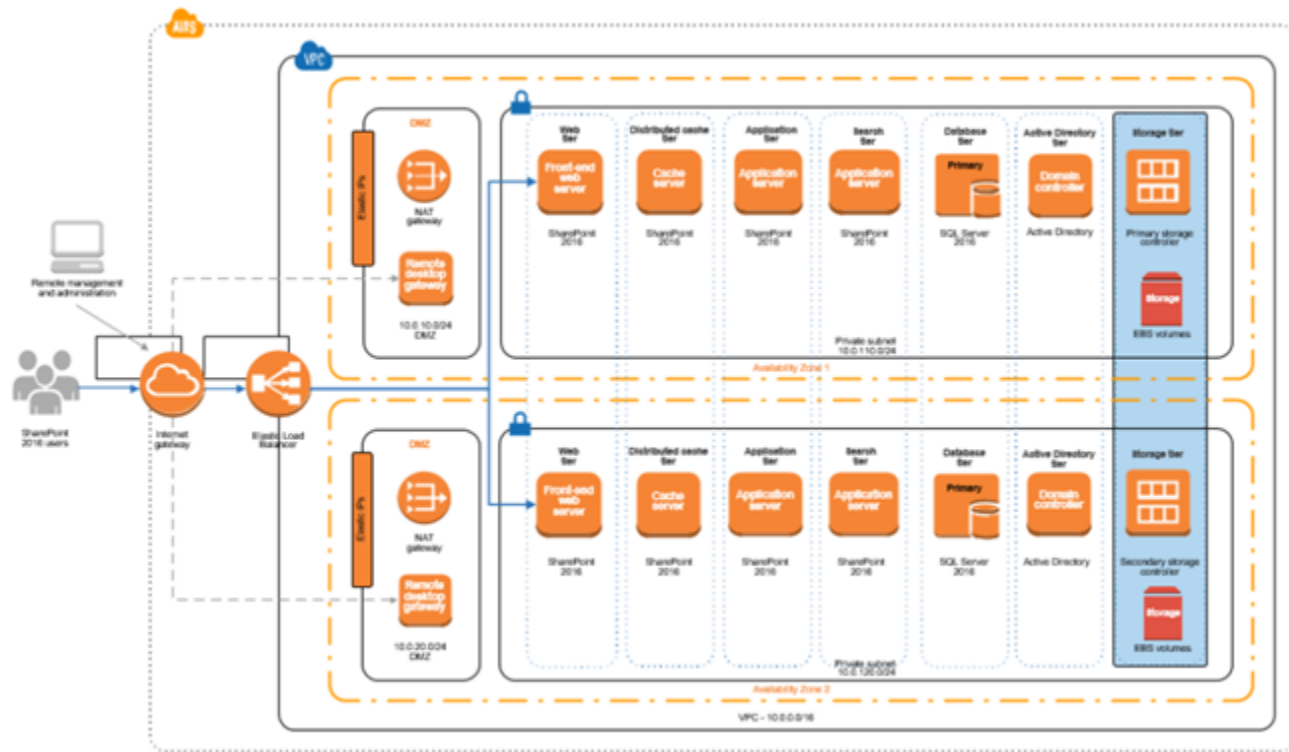
Several solutions from AWS Marketplace can provide appropriately available and scaled storage for SharePoint implementations. You should consider the following when choosing a product:

- High availability (HA) – Multiple Availability Zone failover and multiple region failover
- Fault tolerance – Multiple availability zone and multiple region replication
- Performance – RAID mapping complementary to Amazon Elastic Block Store (Amazon EBS) and instances sized for high IO
- Encryption – Integration with AWS Key Management Service (KMS) or built-in data encryption capability
- Compression – Proprietary or industry-adopted compression capability
- Standard connectivity protocols – iSCSI and CIFS
- Point-in-time data recovery – Proprietary or industry-adopted data recovery capability
- Active Directory integration – Domain membership with user, group, and computer controls

AWS Marketplace Products for SharePoint integration

Product Vendor	Product Name	Link
Datoma	Datomizer S3NAS	https://aws.amazon.com/marketplace/seller-profile?id=e5778de2-bea7-48d1-96c9-9bc9e6611458
NetApp	ONTAP Cloud for AWS	https://aws.amazon.com/marketplace/seller-profile?id=ba83fe1c-57eb-4bac-93a5-5f5d7da7e2f2
SoftNAS	SoftNAS Cloud NAS	https://aws.amazon.com/marketplace/seller-profile?id=28ae3a2c-9300-4a7c-898f-6f6df5692092
StarWind	StarWind Virtual SAN	https://aws.amazon.com/marketplace/seller-profile?id=395b939f-9b80-4d40-bb58-d099abdb342f

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint AWS Whitepaper



The solution proposed in this paper uses the AWS Marketplace SoftNAS Cloud NAS product, however you can use other AWS Marketplace storage products to provide similar functionality.

About SoftNAS Cloud NAS

Secure, redundant, and highly-available storage for content is a critical requirement for any collaboration suite. SharePoint can accumulate significant amounts of data over time, increasing the size and scope of the infrastructure required to serve this data with the continued expectations around performance and availability.

Additional details about SoftNAS Cloud NAS capabilities and features are available on the SoftNAS AWS Marketplace product webpage at <https://aws.amazon.com/marketplace/pp/B00PJ9FGVU>.

Architecture Considerations

Topics

- [Capacity Planning \(p. 6\)](#)
- [Storage Performance \(p. 6\)](#)
- [Fault Tolerance \(p. 6\)](#)
- [High Availability \(p. 6\)](#)
- [High-Level Architecture \(p. 7\)](#)

Capacity Planning

SharePoint uses storage in several ways and selecting the appropriate configuration is a key aspect in the overall performance of the SharePoint collaboration suite. AWS Marketplace storage product provides storage for the Microsoft SQL Server 2016 databases and for SharePoint Remote BLOB Storage (RBS) which stores larger binary objects (for example, Visio diagrams, PowerPoint presentations) within a file system outside the SharePoint Microsoft SQL database. Microsoft provides detailed guidance related to SharePoint capacity planning in Storage and SQL Server capacity planning and configuration (SharePoint Server) on TechNet that takes into account the type and number of artifacts you plan to store in your SharePoint environment (see [https://technet.microsoft.com/en-us/library/cc298801\(v=office.16\).aspx](https://technet.microsoft.com/en-us/library/cc298801(v=office.16).aspx)). This guidance helps you select and size the appropriate Amazon EC2 instances you need to provide database and content storage capacity, and necessary I/O performance to meet your needs.

Storage Performance

Your storage configuration varies based on the requirements you gather from the SharePoint capacity planning guidance. Amazon EBS volumes can be configured in a variety of ways (for example, RAID striping, different volume sizes, etc.) to yield different performance characteristics. For high I/O scenarios, you can create and attach additional Amazon EBS volumes, and stripe using RAID software to increase the total number of I/O operations per second (IOPS). Each Amazon EBS volume is protected from physical drive failure through drive mirroring, so using a RAID level higher than RAID 0 is unnecessary.

Fault Tolerance

For multi-AZ fault tolerance, SoftNAS instances need to be deployed independently because each instance must reside in a separate Availability Zone. When you configure SnapReplicate, the SoftNAS replication component, the Availability Zone of replication source and target are validated to ensure that the instances are not in the same Availability Zone.

High Availability

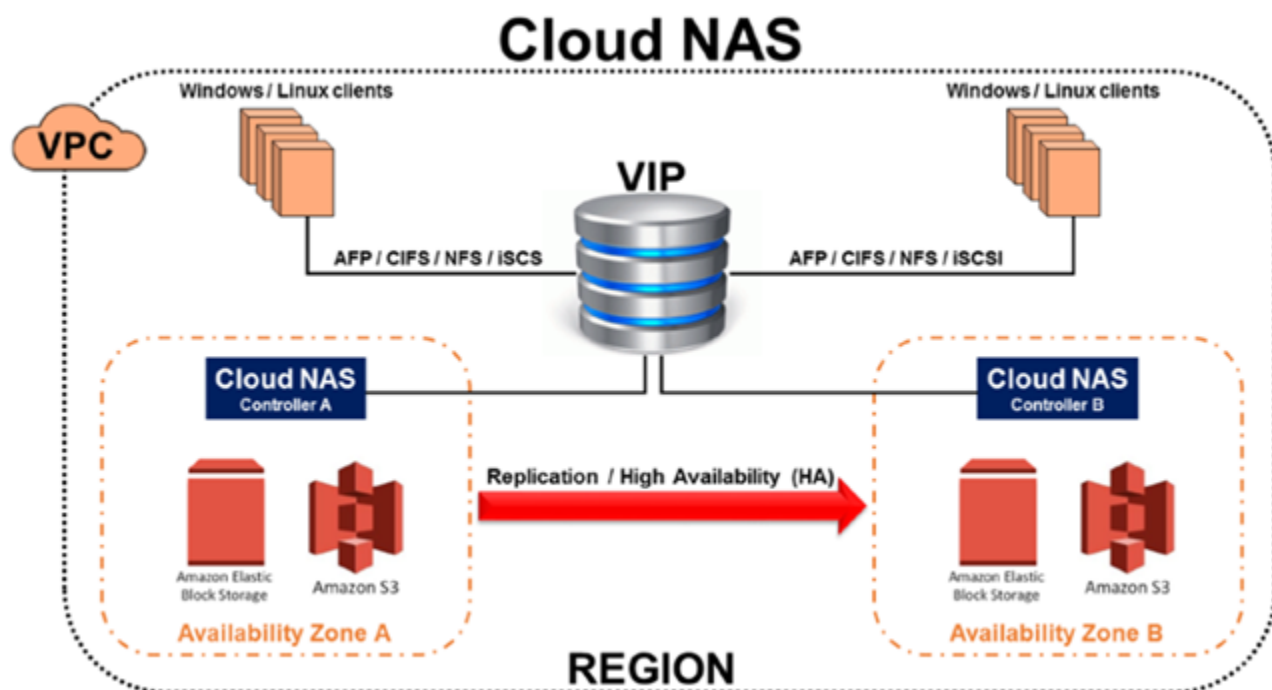
You need to configure each SoftNAS instance with a second network interface that you'll use later to establish connectivity for high availability. The secondary interface is used to create a virtual IP address within the Amazon Virtual Private Cloud (Amazon VPC). The virtual IP address is used as the target for

iSCSI and CIFS storage clients and enables continued connectivity to the SoftNAS Cloud NAS in the event that the primary instance fails. You can add the secondary network interface when you create the instance or at a later time prior to enabling SoftNAS SnapHA.

High-Level Architecture

To implement the Microsoft SharePoint solution described in this paper includes the following components:

- Two AWS Marketplace SoftNAS Cloud NAS instances
- Each instance deployed in separate Availability Zones
- Each instance deployed with two network interfaces
- Each instance deployed with the appropriate number and configuration of Amazon EBS volumes
- SoftNAS Snap Replicate to replicate the source instances to the target instance
- SoftNAS SnapHA to provide high availability and failover capability between instances
- Virtual IP address to provide SoftNAS SnapHA cluster connectivity (VIP is allocated from an address range outside the scope of the CIDR block for VPC of each instance)



Deployment

Topics

- [SoftNAS IAM Policy and Role \(p. 8\)](#)
- [Marketplace AMI Deployment with EC2 Console \(p. 9\)](#)
- [Limited Access Security Group \(p. 11\)](#)

SoftNAS IAM Policy and Role

Prior to deploying the SoftNAS Cloud NAS instances you need to create a custom IAM role that allows the setup and configuration of SoftNAS Snap high availability (HA). You must use the name **SoftNAS_HA_IAM** for the role because the IAM role is hard coded in the SoftNAS Snap HA application.

Create the **SoftNAS_HA_IAM** role with the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1444200186000",
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2:DeleteVolume",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",

        "aws-marketplace:MeterUsage",

        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReplaceRoute",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",

        "s3:CreateBucket",
        "s3:Delete*",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
    }
  ],
}
```

```
"Resource": [
  "*"
]
}
```

The IAM policy grants users permissions to access APIs for Amazon EC2, Amazon S3, and AWS Marketplace.

- Amazon EC2 permissions allow for management of instance attributes, volumes, tags, snapshots, route tables, routes, network attributes, and IP addresses.
- Amazon S3 permissions allow for the setup of SoftNAS Snap Replication and SnapHA.
- AWS Marketplace permissions allow for metered billing.

Marketplace AMI Deployment with EC2 Console

You can deploy the SoftNAS Cloud NAS using the Amazon EC2 console. To do this, open the console, select **Launch Instance**, choose **AWS Marketplace**, type **SoftNAS** in the search box, and then select the appropriate SoftNAS storage configuration from the results list.

The screenshot displays the AWS Management Console interface for selecting an Amazon Machine Image (AMI). The top navigation bar shows 'Services' and 'Resource Groups'. The main content area is titled 'Step 1: Choose an Amazon Machine Image (AMI)' with a 'Cancel and Exit' link. Below the title, a search bar contains the text 'softnas'. The search results list three SoftNAS products:

- SoftNAS Cloud Express - Cloud NAS (HVM/SRV-IO/1TB)**: Starting from \$0.00/hr or from \$156/yr (20% savings) for software + AWS usage fees. Linux/Unix, CentOS 6.5 | 64-bit Amazon Machine Image (AMI) | Updated: 3/12/17. Includes a 'Free Trial' badge and a 'Select' button.
- SoftNAS Cloud Standard - High-Performance Cloud NAS (HVM/SRV-IO/20TB)**: Starting from \$0.00/hr or from \$710/yr (up to 31% savings) for software + AWS usage fees. Linux/Unix, CentOS 6.5 | 64-bit Amazon Machine Image (AMI) | Updated: 3/12/17. Includes a 'Free Trial' badge and a 'Select' button.
- SoftNAS Cloud NAS (HVM/SRV-IO) (Consumption)**: Starting from \$0.12 per TB for software usage + AWS usage fees. Linux/Unix, CentOS 6.5 | 64-bit Amazon Machine Image (AMI) | Updated: 3/23/17. Includes a 'Select' button.

The left sidebar shows filters for 'Categories' (Software Infrastructure, Business Software), 'Operating System' (All Linux/Unix, CentOS), and 'Software Pricing Plans' (Hourly, Annual, By Data).

After you choose a SoftNAS Cloud NAS configuration you can complete the rest of the process to deploy and configure the SoftNAS Cloud NAS instance. You need to deploy two SoftNAS Cloud NAS instances to configure fault tolerance and high-availability, but you need to deploy each instance independently so that you can select separate Availability Zones.

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to 1

Number of instances 1 A free trial only applies to a single instance. Additional instances will be charged the standard software fee.
[Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network vpc-34f60c52 | islawnson-online-collaboration-VPCs [Create new VPC](#)

Subnet subnet-b70c22fe | islawnson - Private subnet 1A | us- [Create new subnet](#)
8181 IP Addresses available

Auto-assign Public IP Disable

Placement group No placement group

IAM role SoftNAS_HA_IAM [Create new IAM role](#)

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

EBS-optimized instance ☒ Launch as EBS-optimized instance

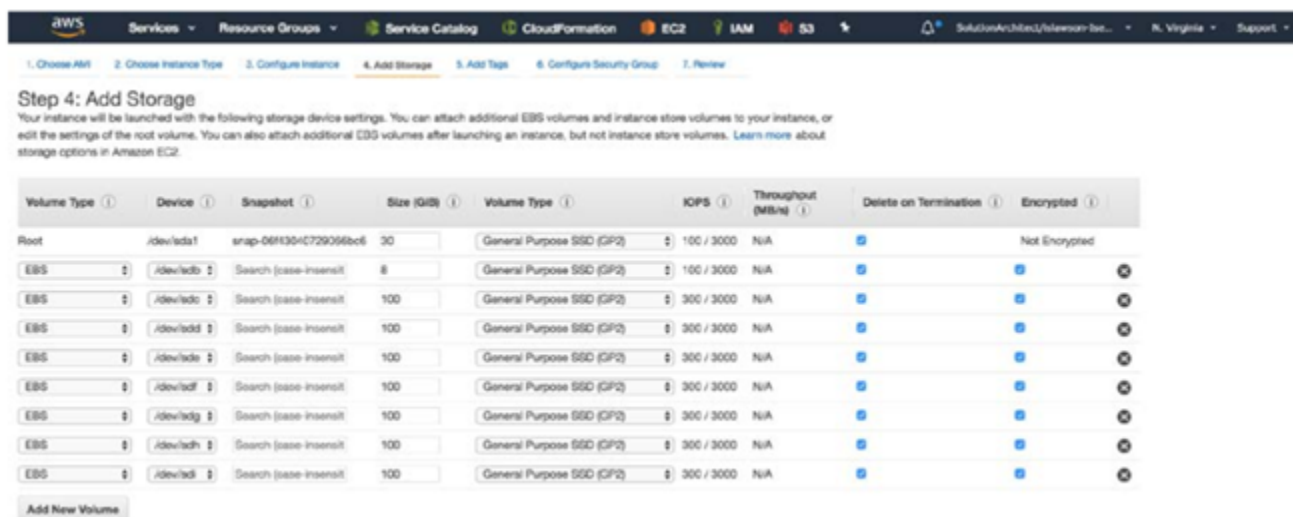
Tenancy Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-b70c22fe	Auto-assign	Add IP	
eth1	New network interface	subnet-b70c22fe	Auto-assign	Add IP	Add IP

For this implementation you add instance storage to accommodate the WSFC quorum majority disk, SharePoint databases (for example, tempdb, content, usage, search, transaction logs), a Microsoft WSFC witness file share, and SharePoint RBS Storage using separate Amazon EBS volumes for each database as recommended by Microsoft for optimal performance. You can also add initial or additional storage from the SoftNAS GUI after deployment. For more information, see Storage and SQL Server capacity planning and configuration (SharePoint Server 2013) at <https://technet.microsoft.com/en-us/library/cc298801.aspx>.

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint AWS Whitepaper Limited Access Security Group



To complete the instance deployment, follow the Amazon EC2 launch wizard, providing the appropriate input for instance type, instance configuration details, addition of storage, tags, and security group configuration. After you review the launch configuration, you need to select a key pair to use for post-deployment administration prior to launching the SoftNAS Cloud NAS instance. Select the appropriate key pair and then launch the instance.

Limited Access Security Group

SoftNAS Cloud NAS instances require access for administration on ports TCP 22 and TCP 443, and access for iSCSI connectivity on port TCP 3260. SoftNAS Snap Replicate and Snap HA require SSH between instances as well as the additional ICMP Echo Request and Echo Reply configuration. Configure inbound security group rules to accommodate this connectivity and to limit inbound traffic from authorized sources.

You can limit access to the SoftNAS storage to accept only traffic from authorized sources by adding the appropriate sources in the configuration. Management access on ports 22 and 443 is required only from the jump server instances, iSCSI and CIFS access is required only from the Microsoft SQL Server database instances and WSFC file share witness. ICMP and SSH connectivity are required between the subnets used by the SoftNAS Cloud NAS instances.

Security Group	Inbound Source	Type	Ports
SoftnasAdmin	Jump Servers and RDGW Servers	SSH HTTPS	TCP 22 TCP 443
SoftnasISCSI	Microsoft SQL Servers	ISCSI	TCP 3260
SoftnasCIFS	WSFC Witness Server	CIFS CIFS CIFS AD	UDP 137 & 138 TCP 139 & 445 TCP 389
SoftnasCluster	SoftNAS Replication and HA members	SSH ICMP	TCP 22 Echo Request

Leveraging AWS Marketplace Storage Solutions
for Microsoft SharePoint AWS Whitepaper
Limited Access Security Group

Security Group	Inbound Source	Type	Ports
		ICMP	Echo Reply

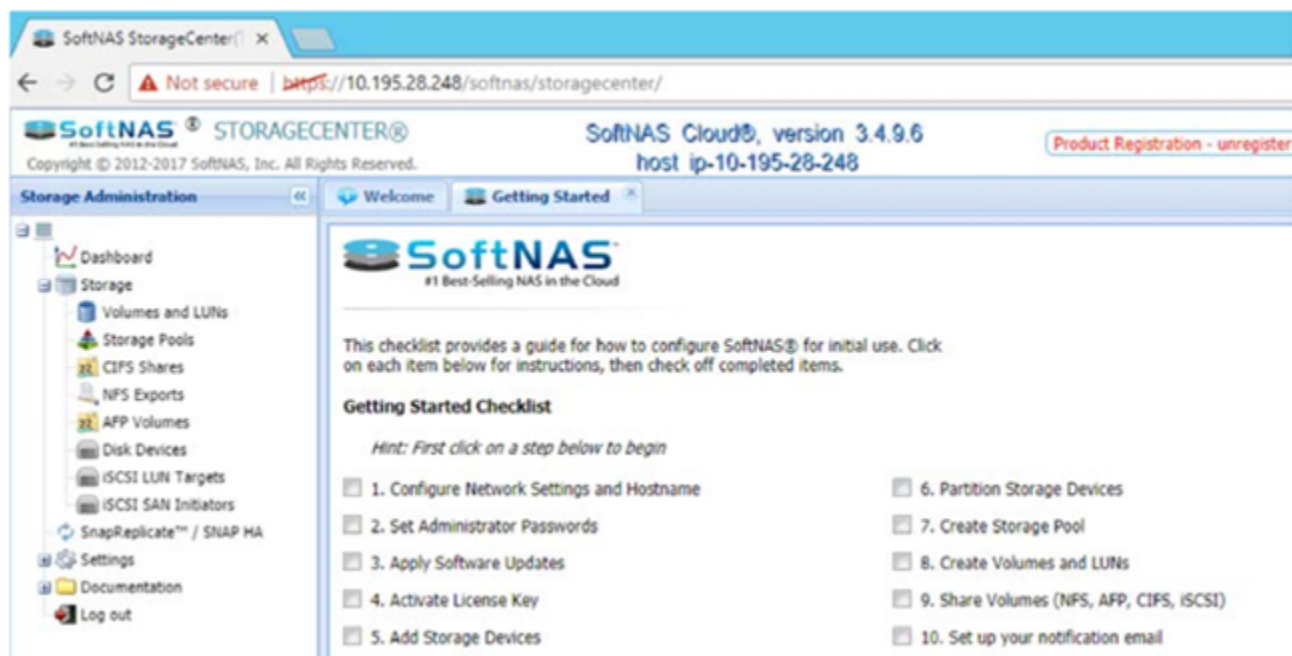
Configuration

Topics

- [Administrative Setup \(p. 13\)](#)
- [Active Directory Membership \(p. 17\)](#)
- [SoftNAS Snap Replication \(p. 19\)](#)
- [SoftNAS SNAP HA \(p. 20\)](#)

Administrative Setup

After you provision your SoftNAS Cloud NAS instances, you access the instances using the Amazon EC2 console. Because the SoftNAS EC2 instance is deployed into a private subnet within the Amazon VPC, access is restricted through a [bastion host](#) or remote desktop gateway server with access to the SoftNAS Cloud NAS security group. For more information, see [Controlling Network Access to EC2 Instances Using a Bastion Server](https://aws.amazon.com/blogs/security/controlling-network-access-to-ec2-instances-using-a-bastion-server/) on the AWS Security Blog at <https://aws.amazon.com/blogs/security/controlling-network-access-to-ec2-instances-using-a-bastion-server/>. The default user name is **softnas** and the default password is set as the instance ID, which you can find in the Amazon EC2 console. After you log in, you see a Getting Started Checklist that you can use to configure your SoftNAS storage. By following the checklist, you can set up and present your storage targets quickly.



The Amazon EBS storage volumes that you added during deployment are available to each SoftNAS Cloud NAS instance as a device that needs a partition. Using the SoftNAS administration interface, you need to partition all appropriate devices.

Optionally, you can partition devices using the SoftNAS command line interface (CLI).

```
ec2-user@ip-10-0-133-229:~$ /usr/local/bin/softnas-cmd parted_command  
partition_all -t  
{
```



```
"result": {
  "msg": "All partitions have been created successfully.",
  "records": {
    "msg": "All partitions have been created successfully."
  },
  "success": true,
  "total": 1
},
"session_id": "8756",
"success": true
}
```

After partitioning is complete the devices are available and you can assign them to a storage pool.

Create storage pools that accommodate the storage capacity and performance requirements required. For this solution, you create separate storage pools for each Amazon AWS EBS storage device. When you configure the storage pool, you can set up an additional layer of encryption that allows SoftNAS Cloud NAS to encrypt data. You can use an encryption password or the AWS Key Management Service (KMS) to implement encryption key management. For more information, see the AWS KMS website at <https://aws.amazon.com/kms/>.

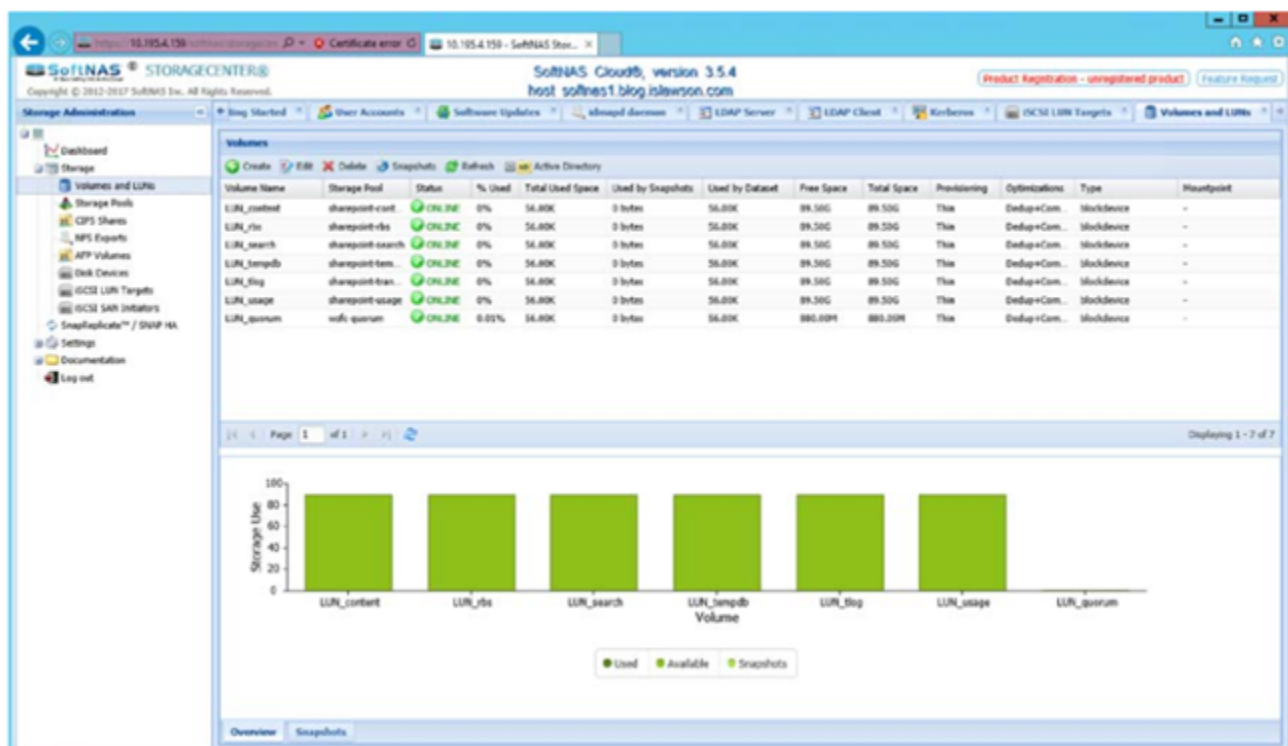
Optionally, you can create storage pools using the SoftNAS CLI.

```
ec2-user@ip-10-0-133-229:~$ /usr/local/bin/softnas-cmd createpool
/dev/xvdb quorum 0 on LUKSpasword123 standard off on -t
{
  "result": {
    "msg": "Create pool 'quorum' was successful.",
    "records": {
      "Available": 7.0996566768736002,
      "Used": 0.00034332275390625,
      "compression": "on",
      "dedup": "off",
      "dedupfactor": "1.00x",
      "free_numeric": 7623198310,
      "free_space": "7.1G",
    },
    "no_disks": 5,
    "optimizations": "Compress",
    "pct_used": "0%",
    "pool_name": "quorum",
    "pool_type": "Standard",
    "provisioning": "Thin",
    "request_arguments": {
      "cbPoolCaseinsensitive":
"off",
      "cbPoolTrim": "on",
      "forcedCreation": "on",
      "opcode": "createpool",
      "pool_name": "quorum",
      "raid_abbr": "0",
      "selectedItems": [
        {
          "disk_name":
"/dev/xvdb"
        }
      ],
      "sync": "standard",
      "useLuksEncryption": "on"
    },
    "status": "ONLINE",
    "time_updated": "Oct 16, 2017"
  }
}
```

Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint AWS Whitepaper Administrative Setup

```
15:43:01",
  "total_numeric": 7623566950,
  "total_space": "7.1G",
  "used_numeric": 368640,
  "used_space": "360.0K"
},
"success": true,
"total": 21
},
"session_id": "8756",
"success": true
}
```

After you create the storage pools, you must allocate the capacity in each storage pool to SoftNAS volumes to enable remote connectivity as iSCSI LUNs and CIFS shares.



Optionally, you can create volumes with the SoftNAS CLI.

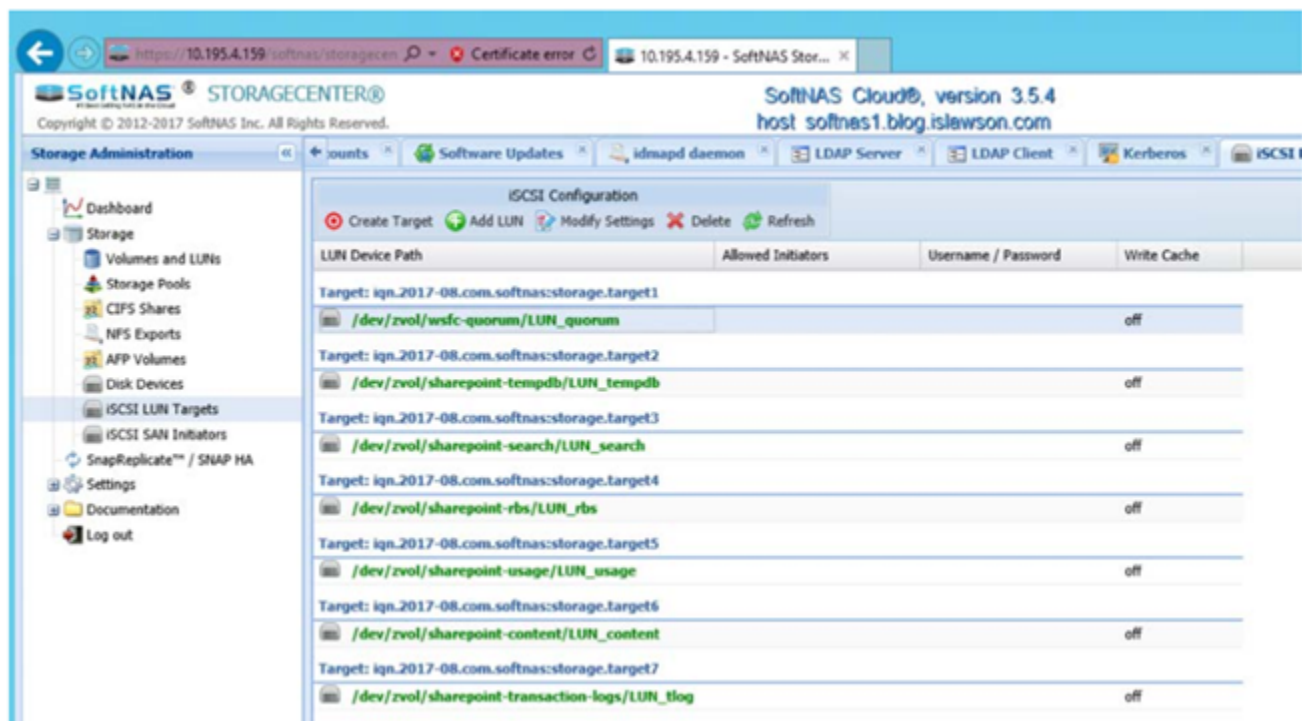
iSCSI volume example:

```
ec2-user@ip-10-0-133-229:~$ /usr/local/bin/softnas-cmd createvolume
vol_name=quorum pool=quorum vol_type=blockdevice provisioning=thin
exportNFS=off shareCIFS=off ShareISCSI=on dedup=on
enable_snapshot=off schedule_name=Default hourlysnaps=0
daily snaps=0 weeklysnaps=0 sync=always --pretty_print
{
  "result": {
    "msg": "Volume 'LUN_quorum'
created.",
    "records": {
      "Available": 7.0999999999999996,
      "Snapshots": 0,
```

```
    "Used": 5.340576171875e-05,  
    "cbSnapshotEnabled": "1",  
    "compression": "off",  
    "compressratio": "1.00x",  
    "dailysnaps": 0,  
    "dedup": "on",  
    "free_numeric": 7623566950.3999996,  
    "free_space": "7.1G",  
    "hourlysnaps": 0,  
    "logicalused": "0.0G",  
    "minimum_threshold": "0",  
    "nfs_export": null,  
    "optimizations": "Dedup",  
    "pct_used": "0%",  
    "pool": "quorum",  
    "provisioning": "Thin",  
    "replication": false,  
    "request_arguments": {  
      "cbSnapshotEnabled": "on",  
      "dailysnaps": "0",  
      "dedup": "on",  
      "exportNFS": "off",  
      "hourlysnaps": "0",  
      "opcode": "createvolume",  
      "pool": "quorum",  
      "provisioning": "thin",  
      "schedule_name": "Default",  
      "shareCIFS": "off",  
      "sync": "always",  
      "vol_name": "quorum",  
      "vol_type": "blockdevice",  
      "weeklysnaps": "0"  
    },  
    "reserve_space": 7.1000534057616997,  
    "reserve_units": "G",  
    "schedule_name": "Default",  
    "status": "ONLINE",  
    "sync": "always",  
    "tier": false,  
    "tier_disabled": null,  
    "tier_name": null,  
    "tier_order": null,  
    "tier_uuid": null,  
    "time_updated": "Oct 16, 2017 15:52:59",  
    "total_numeric": 7623624294.3999996,  
    "total_space": "7.1G",  
    "used_numeric": 5.340576171875e-05,  
    "used_space": "0.0G",  
    "usedbydataset": "56K",  
    "usedbysnapshots": "0B",  
    "vol_name": "LUN_quorum",  
    "vol_path": "-",  
    "vol_type": "blockdevice",  
    "weeklysnaps": 0  
  },  
  "success": true,  
  "total": 40  
},  
"session_id": "8756",  
"success": true  
}
```

When you create the iSCSI LUNs, the associated iSCSI targets are also created. The initial iSCSI target is set up with open connectivity. However, you can update the configuration for each iSCSI target

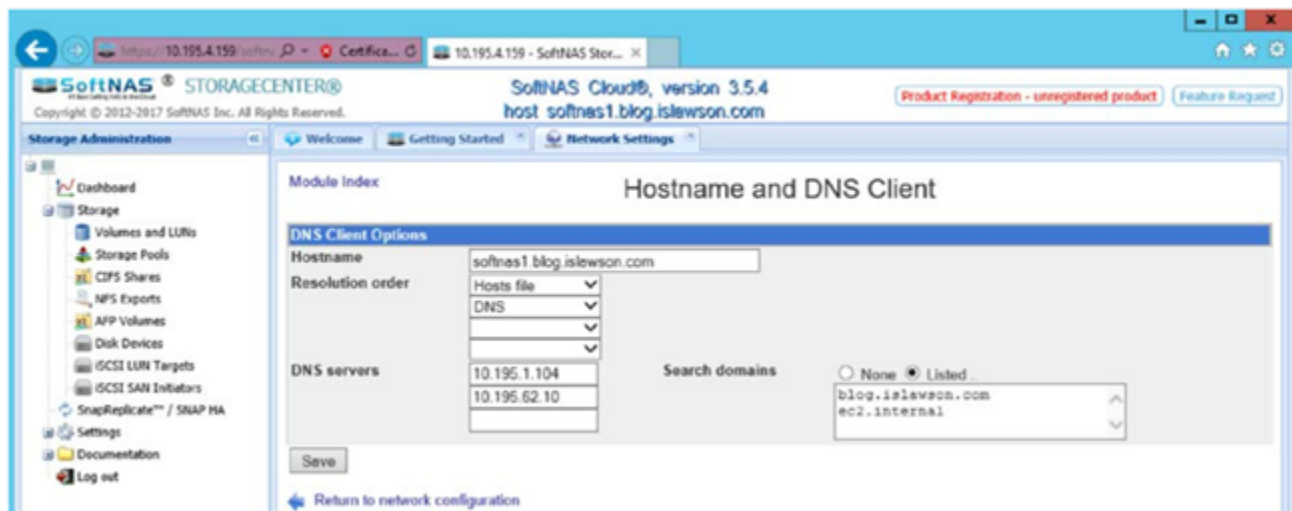
with the IQN for each iSCSI initiator as well as a user name and password that can be used for CHAP authentication between the iSCSI initiators and targets.



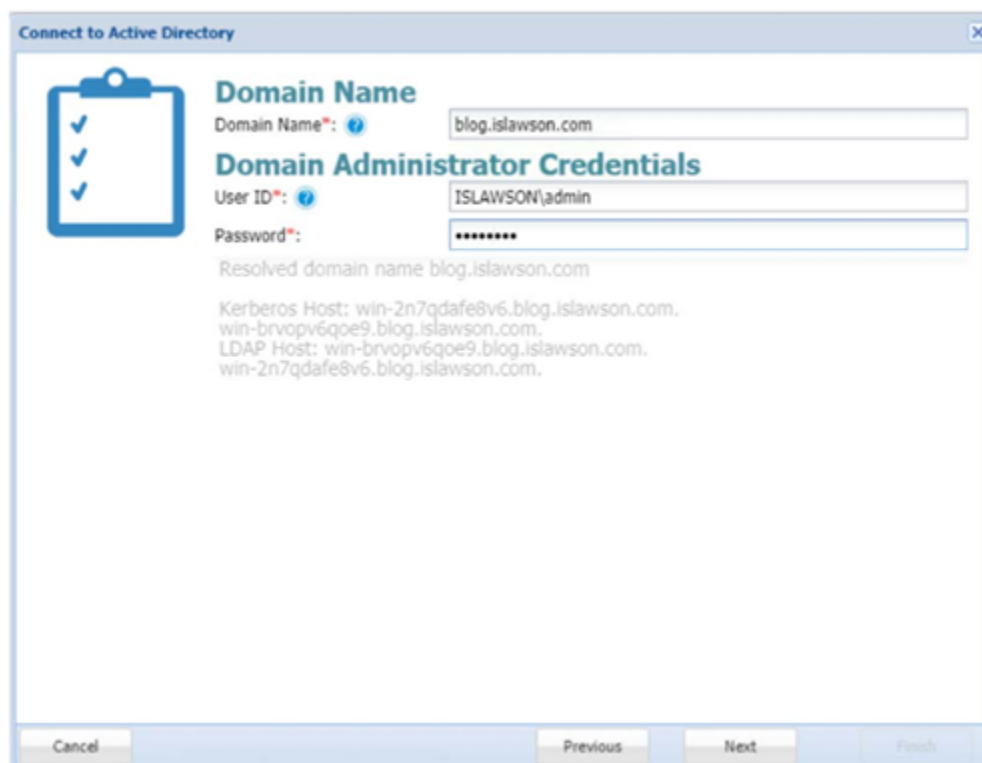
You can't create the iSCSI targets or add IQN and CHAP details using the SoftNAS CLI.

Active Directory Membership

Before you can join the SoftNAS Cloud NAS instances to the Active Directory domain, you need to update the hostname of each instance (that is, the hostname used by the SoftNAS management interface, not the hostname of the EC2 instance). The default hostname is based on the IP address of the EC2 instance. Depending on the IP address, the hostname might contain too many characters to be a valid NETBIOS name, which is required for you to add it to Active Directory. Update the hostname as appropriate in the SoftNAS web management console to a NETBIOS compliant name. For more information, see the Naming conventions in Active Directory for computers, domains, sites, and OUs article on the Microsoft website at <https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and->.



You attach the SoftNAS instance to Active Directory by navigating to the volume configuration page and selecting **Active Directory** from the top-level menu. After you select the interface, you are prompted for the Active Directory domain name, enter a domain user name and password with appropriate domain join permissions to join it to the domain. If the NETBIOS hostname is too long, a prompt appears and explains what actions you need to take to correct the error before proceeding.



Optionally, you can use the SoftNAS CLI to attach the SoftNAS Cloud NAS instance to Active Directory.

```
ec2-user@ip-10-0-133-229:~$ # kinit -p admin-user@EXAMPLE.COM
```

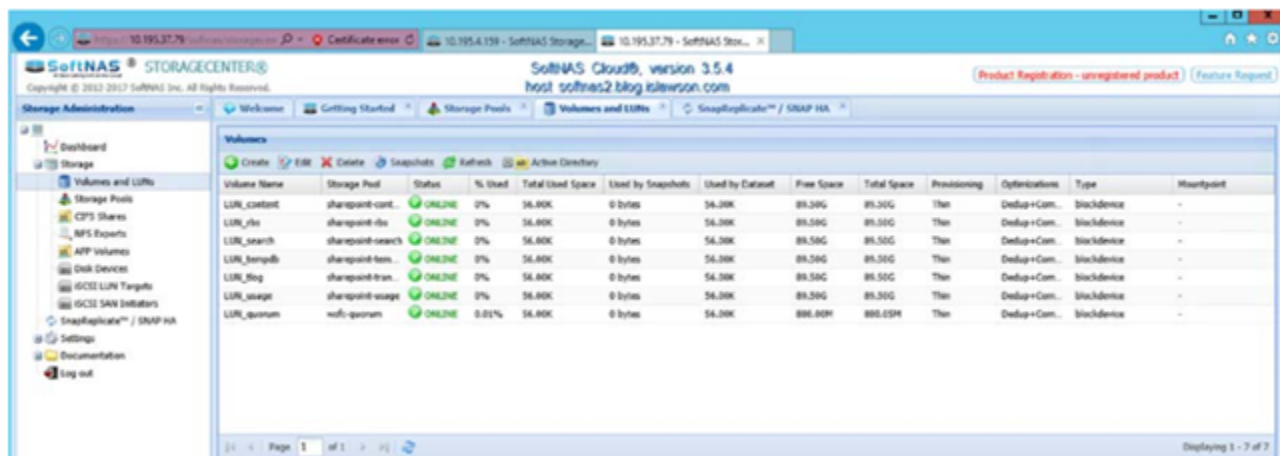
At this point, you've finished configuring the primary SoftNAS Cloud NAS instance. Now, you need to configure the secondary failover instance so that you can configure SNAP Replicate and SNAP HA. For the first step, follow the instructions in the previous section to set up the secondary node, but stop before you create any volumes because these are created during the replication process.

The secondary instance should only be configured to include disk partitioning and storage pool creation. The replication setup process creates all appropriate volumes, CIFS shares, and iSCSI targets as a mirror of the source instance.

After you have configured both the primary and secondary SoftNAS Cloud NAS instances, connect to the SoftNAS administration console of the primary instance and navigate to the **SnapReplicate / Snap HA** menu. First, you set up replication between the primary and secondary SoftNAS Cloud NAS instances. You need to do this from the primary instance. You need to use the IP address, administrative user name, and password of the secondary instance as input. After you complete the setup wizard, SnapReplicate begins replicating each iSCSI LUN from the primary instance to the secondary. After the replication process finishes, the SnapReplicate replication control plan indicates that **Current State** for each LUN is **SNAPREPLICATED-COMPLETE** and the secondary instance now has the replicated LUNs created and visible within the **Volume and LUNs** dashboard.



Leveraging AWS Marketplace Storage Solutions for Microsoft SharePoint AWS Whitepaper SoftNAS SNAP HA



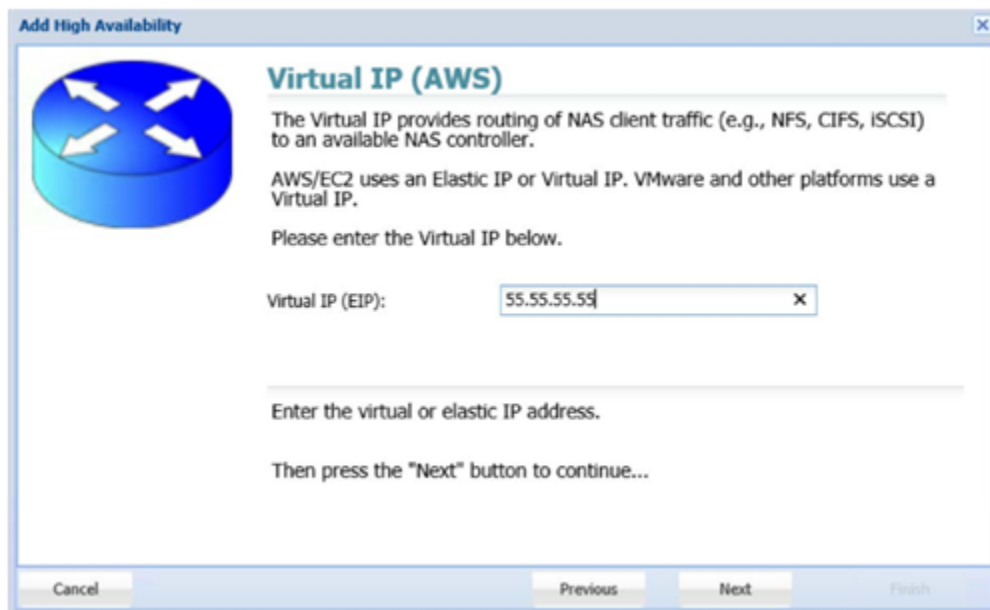
Optionally, you can set up SoftNAS SnapReplicate using the SoftNAS CLI.

```
ec2-user@ip-10-0-133-229:~$ # softnas-cmd snaprepcommand  
initsnapreplicate remotenode="REMOTENODEIP" userid=softnas  
password="PASSWORD" type=target -t
```

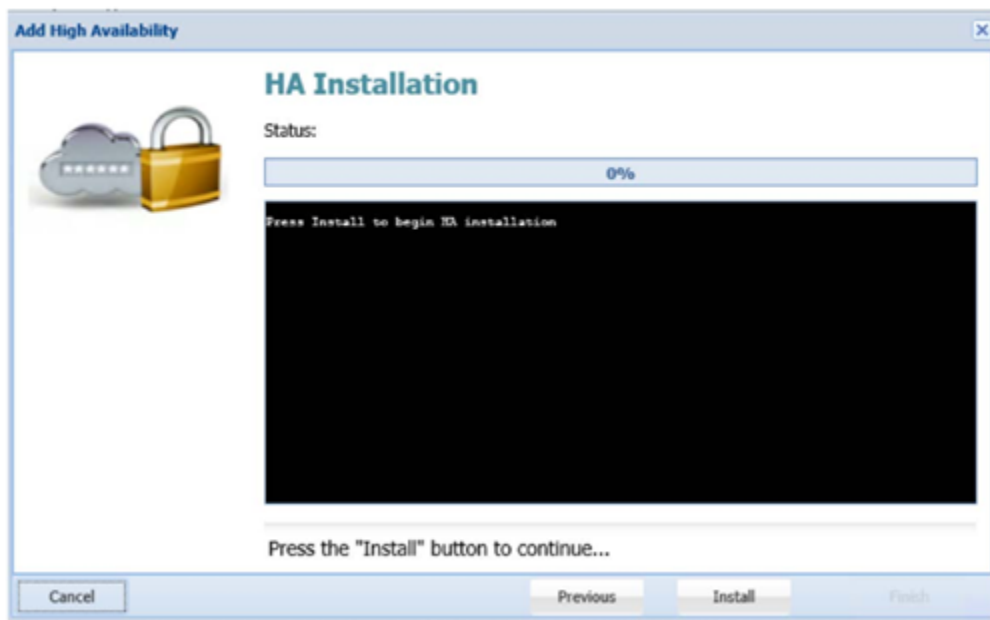
SoftNAS SNAP HA

After SnapReplicate replication has been established, you can set up Snap HA to enable high availability and failover capability for the SoftNAS Cloud NAS. In the **SnapReplicate / Snap HA** control panel choose **Add Snap HA** to begin the setup process.

During the setup process, select the Virtual-IP mode. You need to use a virtual IP address outside of the VPC CIDR block to set up Snap HA communication on the secondary network interface. When requested, enter an IP address that is not addressable within your VPC CIDR range. For instance, if the VPC CIDR block is 10.195.0.0/16, select any other address that doesn't start with 10.195 can work as the virtual IP address required to set up Snap HA. It's important to ensure that the IP address you choose doesn't belong to another VPC or CIDR range that's routed to from this VPC.



After you provide a virtual IP address, you need to enter an AWS Access Key ID and Secret Key. These options are greyed out if the **SoftNAS_HA_IAM** IAM role was attached to each instance. Choose **Next** to confirm that the appropriate permissions are associated with the attached IAM role. If the permissions aren't correct, an error appears and the setup process fails. If the permissions are correct, Choose **Start Install** to begin the Snap HA installation and configuration.



After preparation and configuration are complete, choose **Next**. The Snap HA process completes the installation, and then places the SoftNAS Cloud NAS instances in high availability mode. After the SnapHA setup is complete, choose **Finish**.

Optionally, you can use the SoftNAS CLI to set up SoftNAS SnapHA.

Leveraging AWS Marketplace Storage Solutions
for Microsoft SharePoint AWS Whitepaper
SoftNAS SNAP HA

```
ec2-user@ip-10-0-133-229:~$ # softnas-cmd hacommand add  
YOUR_AWS_ACCESS_KEY YOUR_AWS_SECRET_KEY VIP 1.1.1.1 --pretty_print
```

Conclusion

The solution is complete and configured as follows:

- The primary and secondary SoftNAS Cloud NAS instances are configured.
- The primary instance replicates to the secondary instance.
- Both instances are configured in an active-passive high availability failover cluster.
- SoftNAS Cloud NAS storage is ready to be used by Microsoft SharePoint and SQL Server.
- Connectivity from client iSCSI initiators and CIFS clients is established using the cluster virtual IP address.

AWS has a powerful set of tools that you can use to build your next solution. In addition to AWS services, you can use the software available in AWS Marketplace to build and extend solutions using familiar products from reputable software vendors.

Resources

SoftNAS Resources

- AWS Getting Started Guide at <https://docs.softnas.com/pages/viewpage.action?pageId=3604488>
- AWS Design and Configuration Guide at <https://www.softnas.com/wp/support/aws-cloud-nas-design-configuration-guide/>
- AWS Instance Size Guide at <https://www.softnas.com/wp/products/instance-size-recommendations/#aws>
- AWS Backend Storage Selection Guide at <https://www.softnas.com/wp/support/aws-storage-guide/>
- High Availability: Amazon Web Services at <https://docs.softnas.com/display/SD/High+Availability%3A+Amazon+Web+Services>
- Cloud Formation Template at <https://www.softnas.com/docs/softnas/v3/api/Softnas-AWSCloudTemplateHVM.json>

Microsoft SharePoint SQL Server Resources

- Overview of SQL Server in a SharePoint Server 2016 environment at [https://technet.microsoft.com/en-us/library/ff945791\(v=office.16\).aspx](https://technet.microsoft.com/en-us/library/ff945791(v=office.16).aspx)
- Storage and SQL Server capacity planning and configuration (SharePoint Server) at [https://technet.microsoft.com/en-us/library/cc298801\(v=office.16\).aspx](https://technet.microsoft.com/en-us/library/cc298801(v=office.16).aspx)
- SharePoint Server 2016 Databases – Quick Reference at [https://technet.microsoft.com/en-us/library/cc298801\(v=office.16\).aspx#section1a](https://technet.microsoft.com/en-us/library/cc298801(v=office.16).aspx#section1a)
- Database Types and Descriptions in SharePoint Server at [https://technet.microsoft.com/en-us/library/cc678868\(v=office.16\).aspx](https://technet.microsoft.com/en-us/library/cc678868(v=office.16).aspx)

AWS Resources

- AWS SoftNAS Whitepaper at <https://d0.awsstatic.com/whitepapers/softnas-architecture-on-aws.pdf>
- AWS Bastion Host Blog Post at <https://aws.amazon.com/blogs/security/controlling-network-access-to-ec2-instances-using-a-bastion-server/>

Document Details

Contributors

The following individuals and organizations contributed to this document:

- Israel Lawson, Solutions Architect, AWS
- Kevin Brown, Solutions Architect, SoftNAS
- Ross Ethridge, Technical Support Manager, SoftNAS

Date	Description
January 2018	First publication

AWS Glossary

For the latest AWS terminology, see the [AWS Glossary](#) in the *AWS General Reference*.