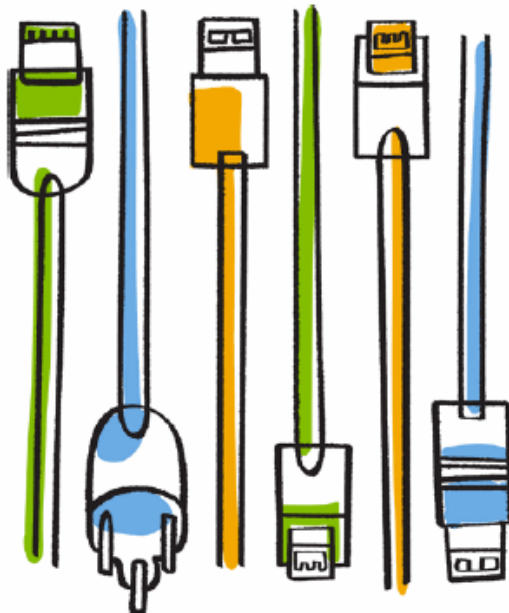




NetApp® AltaVault® Cloud Integrated Storage 4.1

Installation and Service Guide for Cloud Appliances



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: + 1 (408) 822-4501
Support telephone: +1(888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-10480_A0
November 2015

Contents

Contents	3
Chapter 1 - Introducing AltaVault cloud-based appliances	5
Overview of Amazon EC2	5
Cloud backup and disaster recovery	5
Cloud-based workload protection.....	6
Cloud disaster recovery	6
Chapter 2 - Deploying an Amazon Machine Image	7
AltaVault AMI user scenarios.....	7
Supported AltaVault cloud-based appliance AMI models.....	8
Deploying AltaVault cloud-based appliances.....	8
Accessing the AltaVault AMI and choosing a launch method	8
Storage configuration	14
Configuring the SSH console for AltaVault cloud-based appliance access	14
Configuring AltaVault account access.....	17
Configuring networking	17
How to achieve optimal performance using best practices	19
Using best practices for deploying AMI instances.....	19
Best practices for connecting an AMI instance to the network.....	19
Troubleshooting AltaVault AMI instance problems.....	19
Next steps	20
Chapter 3 - Performing AltaVault AMI upgrades.....	21
Overview of AltaVault AMI upgrades.....	21
Plan an AltaVault AMI upgrade	22
AltaVault AMI upgrades.....	22
Saving and exporting the original AltaVault AMI configuration	23
Stopping the original AltaVault AMI and detaching the data volumes	24
Launching and configuring the new AltaVault AMI instance upgrade	26
Importing the Configuration File.....	33
Attaching data volumes to the new upgrade instance	34
Rebooting the new AltaVault AMI upgrade	35
Cleaning up after the upgrade.....	36
Accessing community support.....	36

Chapter 4 - Deploying a Microsoft Azure virtual machine37

 Overview of Microsoft Azure.....37

 Creating an AltaVault virtual machine37

 Log in to AltaVault VM.....45

 Initialize the datastore.....45

 Next steps46

Copyright information47

Trademark information.....49

How to send your comments.....51

Index53

CHAPTER 1 **Introducing AltaVault cloud-based appliances**

Use this solution guide to deploy and configure an AltaVault cloud-based appliance using Amazon Web Services™ Marketplace.

This chapter includes the following sections:

- [“Overview of Amazon EC2” on page 5](#)

Overview of Amazon EC2

Amazon’s computing infrastructure is provided in the form of the EC2 offering that is a fully scalable, elastic cloud compute environment where virtual machines (VMs) can run. Amazon EC2 provides reliable and re-sizable compute capacity in the cloud that can be accessed and managed using a simple Web service interface. It provides you with complete control of your computing resources and lets you run on Amazon’s proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Deploying an Amazon AMI into the EC2 infrastructure is as simple as selecting the AMI template and deploying it, configuring the security and network capabilities of the VM, and linking it to storage and other infrastructure as needed.

Cloud backup and disaster recovery

AltaVault cloud-based appliances deliver complete cloud backup and disaster recovery. NetApp and Amazon are tackling the next generation of backup and resiliency challenges by introducing the industry’s first enterprise-class cloud-based backup appliances. An AltaVault cloud-integrated appliance, also known as an AltaVault AMI instance, launched in the Amazon Web Services (AWS) Marketplace gives users flexibility in protecting their critical business data. Not only can cloud workloads be protected and archived for long term retention on cheaper storage, but both virtual and physical workloads can also be recovered. AltaVault cloud-based appliances allow you to select whether you want to recover at traditional secondary sites, or in the EC2 compute environment that is managed and secured by Amazon. Utilizing EC2 gives smaller companies the ability to have a DR solution, at a much smaller cost than maintaining the infrastructure, security, and management of a physical DR site.

Cloud-based workload protection

AltaVault cloud-based appliance AMI instances offer an efficient and secure approach to backing up cloud-based workloads. Using your existing backup software, AltaVault cloud-based appliance AMI deduplicates, encrypts, and rapidly migrates data to Amazon S3 or Glacier, which reduces the long term costs of protecting the data. Since Amazon Glacier, for example, offers storage costs of \$.01/GB/month, this represents a 10 fold reduction in costs vs. performing and maintaining Amazon Elastic Block Store (EBS) snapshots. Users can effectively tier their data protection requirements adaptively by having an AltaVault cloud-based appliance AMI instance to offload data based on data usage and retention requirements. As an example, long term email data can be directed to Amazon Glacier for audit/compliance/regulatory reasons, higher priority user data can be stored on Amazon S3 for quicker recovery, and critical database or application data be maintained in Amazon EBS snapshots that are retained for shorter periods of time for quick point in time recovery.

Cloud disaster recovery

For organizations without a secondary disaster recovery location, or for companies looking for extra protection with a low-cost tertiary site, AltaVault cloud-based appliance AMI instances are the key to enabling cloud disaster recovery. Using on-premise AltaVault physical or virtual appliances, data is seamlessly and securely protected in the cloud. If the primary site is unavailable, customers can quickly spin-up an AltaVault cloud-based appliance AMI and recover data to Amazon EC2.

Businesses that want to have a complete DR solution traditionally have been forced into spending large sums of money, time and resources to build out, maintain, and secure a secondary site location. Whether this is at an existing site owned by a company or at a collocation facility where space is rented, the cost is significant because the computing and storage resources are always on premise and must be available 24x7x365. The benefits of cloud compute and storage have significantly altered the perceptions and reality of DR because of the scale, elasticity, and pay as you go model that cloud infrastructure provides. Instead of paying for resources that are in standby mode 99% of the time, you pay for resources that are powered on for the 1% of the time that you have to perform Disaster Recovery. The elastic model that Amazon services provide make it possible such that you no longer have to pay excessive amounts of money for resources that are on stand by a majority of the time. Because an AltaVault cloud-based appliance AMI instance is like any other AltaVault appliance, you can effectively make the cloud computing infrastructure your DR site to your physical site, as well as any virtualized site (either on premise or within a compute cloud).

CHAPTER 2 Deploying an Amazon Machine Image

Use this solution guide to deploy and configure an AltaVault cloud-based appliance using the Amazon Web Services Marketplace. The AltaVault Amazon Machine Image (AMI) is an AltaVault cloud-based appliance built specifically for deployment within the Amazon EC2 compute environment. Leveraging the capabilities of Amazon's scalable, elastic compute cloud, AltaVault cloud-based appliance can now be deployed within the EC2 environment to deliver cloud protection and Disaster Recovery (DR) capabilities of virtual and physical environments.

This chapter includes the following sections:

- [“AltaVault AMI user scenarios” on page 7](#)
- [“Supported AltaVault cloud-based appliance AMI models” on page 8](#)
- [“Deploying AltaVault cloud-based appliances” on page 8](#)
- [“How to achieve optimal performance using best practices” on page 19](#)
- [“Troubleshooting AltaVault AMI instance problems” on page 19](#)

AltaVault AMI user scenarios

You can use the AltaVault AMI in the following scenarios:

- **Media server in the cloud:** If your backup media server in AWS is an EC2 instance, the AltaVault cloud-based appliance AMI runs in the same AWS account. The backup media server backs up data to the AltaVault in EC2.
- **Media server on site:** AltaVault runs in EC2, but the backup media server and software are on site. The uncompressed data goes to the EC2 AltaVault that deduplicates the data and stores it in the cloud.
- **Disaster recovery:** You have a physical AltaVault with the backup software on site that stores the backup data in the Amazon cloud, and you want the capability to create an EC2-based AltaVault cloud-based appliance with the backup images in EC2 in the event of a disaster at the primary site. This setup enables you to recover your data if your entire primary site network is down.
- **NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Cloud Appliances**

Supported AltaVault cloud-based appliance AMI models

There are three supported versions of AMI:

- AVA-c4: 4 TB of local disk cache

Note: The AVA-c4 has been designed and optimized for deployment on the DS3 instance. NetApp strongly recommends deploying the AVA-c4 with the DS3 instance only.

- AVA-c8: 8 TB of local disk cache
- AVA-c16: 16 TB of local disk cache

For the AVA-c16 model, there are two methods of deployment:

- 1-Click Launch: Provides a 1 GbE infrastructure for communication with other EC2 instances.
- Manual Launch: Use the manual launch method if you are deploying an AVA-c16 AMI instance that will be used as a target by the backup application server instance. This method provides a 10 GbE infrastructure for communication with other EC2 instances. Both the AVA-c16 and the back-up application instance should be in the same placement group.

Deploying AltaVault cloud-based appliances

Deploying an AltaVault cloud-based appliance AMI instance into an Amazon EC2 infrastructure involves the following steps:

- [“Accessing the AltaVault AMI and choosing a launch method” on page 8](#)
- [“Storage configuration” on page 14](#)
- [“Configuring the SSH console for AltaVault cloud-based appliance access” on page 14](#)
- [“Configuring AltaVault account access” on page 17](#)
- [“Configuring networking” on page 17](#)

Accessing the AltaVault AMI and choosing a launch method

Log in to the Amazon Web portal and choose an AMI model to launch.

To access the AltaVault AMI

1. Login to the Amazon Web Services portal and browse to the Amazon Marketplace at <https://aws.amazon.com/marketplace>.
2. Search AWS Marketplace for AltaVault.

3. Select the NetApp AltaVault cloud-based appliance version that you want to use from the following:

- AVA-c4
- AVA-c8
- AVA-c16

The AVA-c16 for AWS is selected in the example below.

The screenshot shows the AWS Marketplace product page for NetApp AltaVault (formerly SteelStore) AVA-c16 for AWS. The page includes the AWS Marketplace logo, a search bar, and navigation links. The product details section shows the NetApp logo and a description of the appliance. The pricing details section shows the region set to US East (N. Virginia) and a table of hourly fees for EC2 instance types and EBS Magnetic volumes.

AltaVault (formerly SteelStore) AVA-c16 for AWS
Sold by: NetApp, Inc.

The NetApp AltaVault cloud-based appliances for AWS can be used for two primary purposes: to recover on-premises workloads in the cloud or to efficiently protect cloud-based workloads. For organizations without a secondary disaster recovery location, or for companies looking for extra protection with a low-cost tertiary site, AltaVault cloud-based appliances are the key to enabling cloud-based disaster recovery. Using on-premises AltaVault physical or virtual appliances, data is seamlessly and securely protected in the cloud. If the primary site is unavailable, customers can quickly spin-up a ... [Read more](#)

Customer Rating Be the first to review this product

Latest Version 4.1 (Other available versions)

Base Operating System Linux/Unix, Other 4.1

Delivery Method 64-bit Amazon Machine Image (AMI) ([Learn more](#))

Support [See details below](#)

AWS Services Required Amazon EC2, Amazon EBS, Amazon S3

Highlights

- Open & Efficient: Integrates with ease into your existing backup architecture and uses inline deduplication and compression for up to 30:1 data-reduction ratios
- Secure: Offers end-to-end security for data at rest and in flight using FIPS 140-2 level 1-compliant encryption
- Simple: Takes you from zero to protected in less than 30 minutes

Pricing Details

For region: **US East (N. Virginia)**

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	EC2 Usage	Software	Total
c3.xlarge	\$1.68/hr	\$1.54/hr	\$3.22/hr

EBS Magnetic volumes

- \$0.05 per GB-month of provisioned storage
- \$0.05 per 1 million I/O requests

Assumes On-Demand EC2 pricing

4. Click **Continue**.

5. Enter your AWS credentials to sign in to your account.

The screenshot shows the AWS Sign In or Create an AWS Account page. It includes the Amazon Web Services logo and a form for signing in or creating an account. The form asks for an email or mobile number and a password. There are radio buttons for 'I am a new user' and 'I am a returning user and my password is:'. A 'Sign in using our secure server' button is present, along with a 'Forgot your password?' link. On the right, there is a promotional banner for AWS re:Invent 2015.

Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

☐ I am a new user.

☒ I am a returning user and my password is:

[Sign in using our secure server](#)

[Forgot your password?](#)

Announced at
AWS re:Invent 2015
Explore the next generation of AWS cloud capabilities

[See what's new](#)

Learn more about [AWS Identity and Access Management](#) and [AWS Multi-Factor Authentication](#), features that provide additional security for your AWS Account. View full [AWS Free Usage Tier](#) offer terms.

6. Choose one of the following launch methods:

- 1-Click Launch: Preferred method
- Manual Launch: Select this launch method if the target instance will be used in conjunction with the backup application server instance. This method provides a 10 GbE infrastructure for communication with other EC2 instances. Both the AVA-c16 and the back-up application instance should be in the same placement group.

Launch on EC2:

AltaVault (formerly SteelStore) AVA-c16 for AWS

The screenshot shows the AWS Marketplace launch page for AltaVault (formerly SteelStore) AVA-c16 for AWS. The page is divided into two main sections: '1-Click Launch' and 'Manual Launch'. The '1-Click Launch' section is active, showing a 'Launch with 1-Click' button. The 'Manual Launch' section is inactive, showing 'With EC2 Console, APIs or CLI'. The page also displays pricing information, including a cost estimator and software charges.

1-Click Launch
Review, modify, and launch

Manual Launch
With EC2 Console, APIs or CLI

Click "Launch with 1-Click" to launch this software with the settings below

The default settings are provided by the software seller and AWS Marketplace.

Version
4.1, released 11/05/2015

Region
US East (N. Virginia)

EC2 Instance Type

c3.8xlarge	Memory	60 GB
	CPU	108 EC2 Compute Units (32 virtual cores with 3.375 Compute Units each)
	Storage	2 x 320 GB SSD
	Platform	64-bit
	Network performance	Very High (10 Gigabit Ethernet)
	API Name	c3.8xlarge

VPC Settings
Will launch into: subnet-e3238994

Price for your selections:

\$3.22 / hour
\$1.68 c3.8xlarge EC2 Instance usage fees +
\$1.54 hourly software fee

\$0.05 / GB / month
EBS Magnetic Storage

\$0.05 / 1 million I/O requests
EBS Magnetic Storage

Launch with 1-Click

Cost Estimator

\$2,318.40 / month
c3.8xlarge EC2 Instance usage fees
Assumes 24 hour use over 30 days

Software Charges

\$1,108.80 / month
\$1,108.80 hourly software fees for c3.8xlarge

AWS Infrastructure Charges

\$1,209.60 / month

To deploy an AltaVault AMI instance using the 1-Click Launch method

1. From the launch page, select 1-Click Launch.
2. Chose a Region in which to create the AltaVault cloud based appliance AMI instance.
Region - Determines the geographical region to create and place the AltaVault cloud-based appliance AMI instance. The default selection is US East (Virginia).

Note: EC2 Instance Type: This selection determines an EC2 instance type and is not adjustable.

3. Chose a Security Group for the AltaVault cloud based appliance AMI instance.

Security Group - Determines a Security Group for the AltaVault cloud-based appliance AMI instance. By default, a preselected security group displays as seen in the figure below. If one is not present, it automatically creates the group during the deployment process. The security group describes which ports and IPs the AltaVault cloud-based appliance AMI instance uses to communicate with other VMs.

▼ Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. [Learn more about Security Groups.](#)

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

Create new based on seller settings ▼

Description:

A new security group will be generated by AWS Marketplace. It is based on recommended settings for AltaVault (formerly SteelStore) AVA-c4 Cloud-Based Appliance for AWS version 4.0.0 provided by NetApp Inc..

Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22 - 22	Anywhere ▼ 0.0.0.0/0
HTTP	tcp	80 - 80	Anywhere ▼ 0.0.0.0/0
	tcp	111 - 111	Anywhere ▼ 0.0.0.0/0
HTTPS	tcp	443 - 443	Anywhere ▼ 0.0.0.0/0
	tcp	445 - 445	Anywhere ▼ 0.0.0.0/0
	tcp	2049 - 2049	Anywhere ▼ 0.0.0.0/0
	tcp	4001 - 4001	Anywhere ▼ 0.0.0.0/0
	tcp	4002 - 4002	Anywhere ▼ 0.0.0.0/0
	udp	111 - 111	Anywhere ▼ 0.0.0.0/0
	udp	2049 - 2049	Anywhere ▼ 0.0.0.0/0
	udp	4002 - 4002	Anywhere ▼ 0.0.0.0/0
RDP	tcp	3389 - 3389	Anywhere ▼ 0.0.0.0/0

Warning

Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.

4. Chose a Key Pair.

Key Pair - Determines a Key Pair to authenticate to the AltaVault cloud-based appliance AMI instance for performing operations, using either the AltaVault CLI or the GUI interface. Creating a key pair is a prerequisite requirement.

For instructions on creating a key pair, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#having-ec2-create-your-key-pair>.

5. Click **Accept Terms & Launch with 1-Click**.

6. Continue to the next step, “[Storage configuration](#)” on page 14.

Note: To connect to the AltaVault cloud-based appliance AMI instance using the external SSH tool, PuTTY, you must configure the key pair file in a format that is accepted by PuTTY. Refer to the following Amazon document for converting the key pair file into a PuTTY friendly form: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>.

Note: For Unix SSH, you must ensure the permissions on the key pair file is set at 400. You can change permissions using the command, `chmod 400 <key-pair.pem>`.

To deploy an AltaVault AMI instance in Amazon EC2 using the Manual Launch method

1. From the AltaVault Launch page, select Manual Launch for the AVA-c16 model.

Launch on EC2:

AltaVault (formerly SteelStore) AVA-c16 for AWS

1-Click Launch
Review, modify, and launch

Manual Launch
With EC2 Console, APIs or CLI

Launching Options

- You can click the "Launch with EC2 Console" buttons below and following the instructions to launch an instance of this software
- You can also find and launch these AMIs by searching for the AMI IDs (shown below) in the "Community AMIs" tab of the [EC2 Console](#) [Launch Wizard](#)
- You can view this information at a later time by visiting the Your Software page. For help, see [step-by-step instructions](#) [for launching Marketplace AMIs from the AWS Console](#).

[Usage Instructions](#)

Select a Version

4.1, released 11/05/2015

Region	ID	
US East (N. Virginia)	ami-558ded30	Launch with EC2 Console
US West (Oregon)	ami-0b988b3b	Launch with EC2 Console
US West (N. California)	ami-23699267	Launch with EC2 Console
EU (Ireland)	ami-95c3e4e2	Launch with EC2 Console
Asia Pacific (Singapore)	ami-ae8e3fc	Launch with EC2 Console
Asia Pacific (Sydney)	ami-73703c49	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-8a87098a	Launch with EC2 Console
South America (Sao Paulo)	ami-ebbc36f6	Launch with EC2 Console

Pricing Details

For region
US East (N. Virginia)

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	Software	EC2	Total
c3.8xlarge	\$1.54/hr	\$1.68/hr	\$3.22/hr

EBS Magnetic volumes

- \$0.05 per GB-month of provisioned storage
- \$0.05 per 1 million I/O requests

Assumes On-Demand EC2 pricing; prices for [Reserved](#) and [Spot](#) instances will be lower. See [pricing details](#).

Data transfer fees not included.

[Learn about instance types](#)

2. Select Launch with EC2 Console for the corresponding Region where you intend to deploy the AMI instance.

The selection, Launch with EC2 Console, automatically provides a 10 GbE interface. Ensure that you choose a placement group while launching the AMI. The 10 GbE capabilities are only realized when the AMI and the backup server in the same placement group.

3. Scroll down to the Compute optimized section and select the instance type, c3.8xlarge.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Instance Type	Instance Class	VCPU	Memory (GiB)	Storage	EBS only	Yes	High
<input checked="" type="radio"/> Compute optimized	c4.xlarge	16	30	EBS only	Yes	High	
<input type="radio"/> Compute optimized	c4.8xlarge	36	60	EBS only	Yes	10 Gigabit	
<input type="radio"/> Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate	
<input type="radio"/> Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate	
<input type="radio"/> Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High	
<input type="radio"/> Compute optimized	c3.4xlarge	16	30	2 x 160 (SSD)	Yes	High	
<input checked="" type="radio"/> Compute optimized	c3.8xlarge	32	60	2 x 320 (SSD)	-	10 Gigabit	
<input type="radio"/> Compute optimized	c1.medium	2	1.7	1 x 350	-	Moderate	
<input type="radio"/> Compute optimized	c1.xlarge	8	7	4 x 420	Yes	High	
<input checked="" type="radio"/> Compute optimized	cc2.8xlarge	32	60.5	4 x 840	-	10 Gigabit	
<input checked="" type="radio"/> Compute optimized	cc1.4xlarge	16	23	2 x 840	-	10 Gigabit	
<input checked="" type="radio"/> GPU instances	g2.2xlarge	8	15	1 x 60 (SSD)	Yes	High	
<input checked="" type="radio"/> GPU instances	g2.8xlarge	32	60	2 x 120 (SSD)	-	10 Gigabit	

Cancel Previous **Review and Launch** Next: Configure Instance Details

4. Click **Next: Configure Instance Details**.

5. From the Placement group drop-down menu, select the placement group to which the backup application server instance belongs.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

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 the instance, and more.

Number of instances

Purchasing option ☐ Request Spot Instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group
☒ New placement group

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

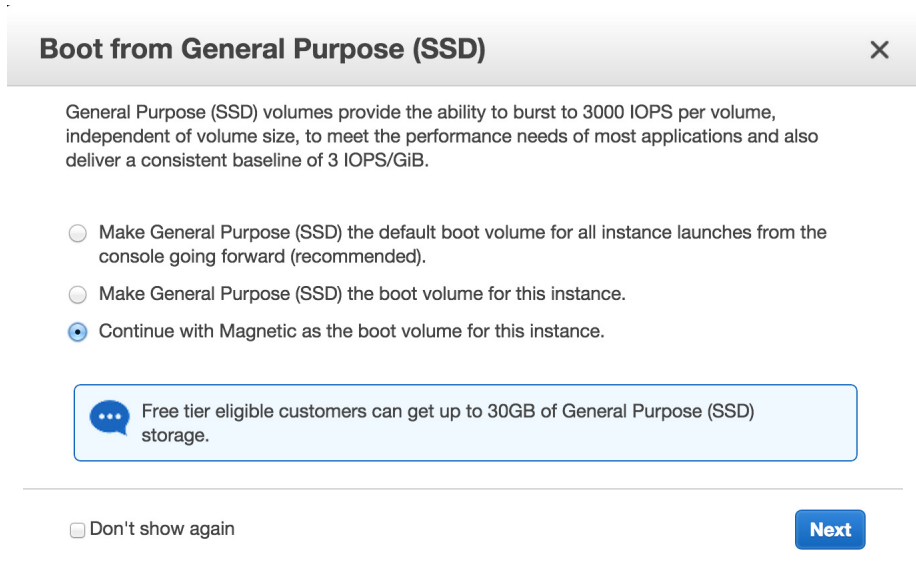
Monitoring ☐ Enable CloudWatch detailed monitoring
 Additional charges apply.

Tenancy
 Additional charges will apply for dedicated tenancy.

Cancel Previous **Review and Launch** Next: Add Storage

6. Click **Review and Launch**.

7. From the Boot from General Purpose (SSD) page, select Continue with Magnetic as the boot volume for this instance.



Boot from General Purpose (SSD) ✕

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

☐ Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).

☐ Make General Purpose (SSD) the boot volume for this instance.

☒ Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

☐ Don't show again **Next**

8. Click **Next**.
9. Review the launch instance details and click **Launch**.

Storage configuration

An AltaVault cloud-based appliance AMI instance deploys with an automatically provisioned 100GB disk that contains the AltaVault OS install image and a preconfigured second set of disks used for storing the data AltaVault cloud-based appliance received from your backup application. The size and number of disks are based on the model of appliance that you previously selected to launch and cannot be configured.

Note: In Amazon EC2, volumes can be attached as either disk or as instance store volumes. An AltaVault cloud-based appliance AMI only supports EBS volumes, and as such, EBS volumes are created and associated with the AltaVault AMI appliance.

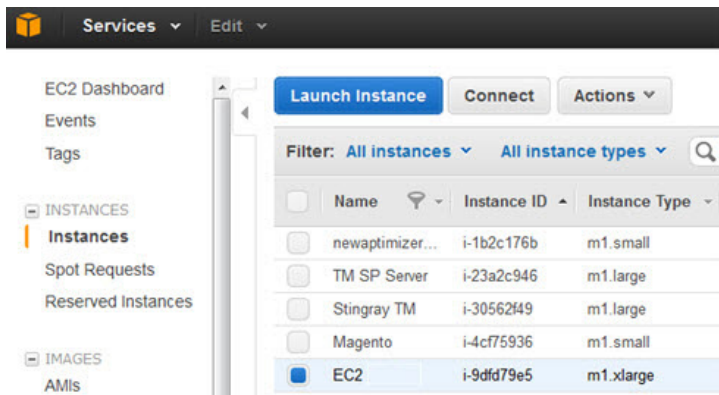
Configuring the SSH console for AltaVault cloud-based appliance access

You can access the AltaVault cloud-based appliance in one of two ways:

- Use the Amazon provided Web browser SSH interface
- Use a native SSH client of your own

To access your AltaVault cloud-based appliance instance using the Amazon Web browser

1. Select the instance name of the AltaVault cloud-based appliance AMI instance.
2. From the top menu, select Connect.



3. Select the radio button, A Java SSH client directly from my browser (Java required).



4. Enter the User name, admin.
5. To begin the session, click **Launch SSH Client**.

Configuring your native SSH client

To configure console access using your own SSH client, you must have the following items:

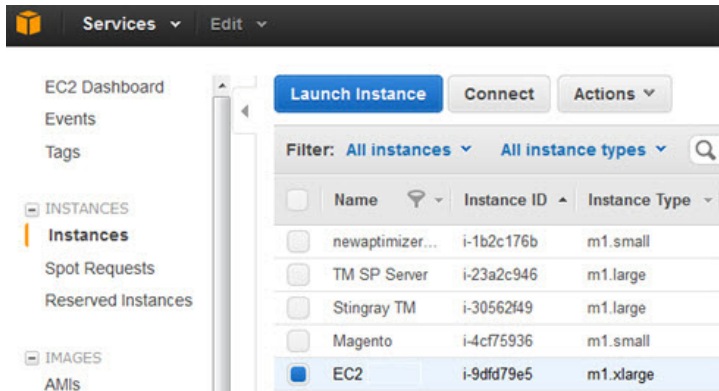
- SSH Client - Available (Linux includes a native SSH client, and Windows users can use PuTTY).
- AMI Instance name of the AltaVault cloud-based appliance
- Public DNS name of the instance
- Private key (.pem) file associated with this AMI from your Amazon account

Configuring Linux

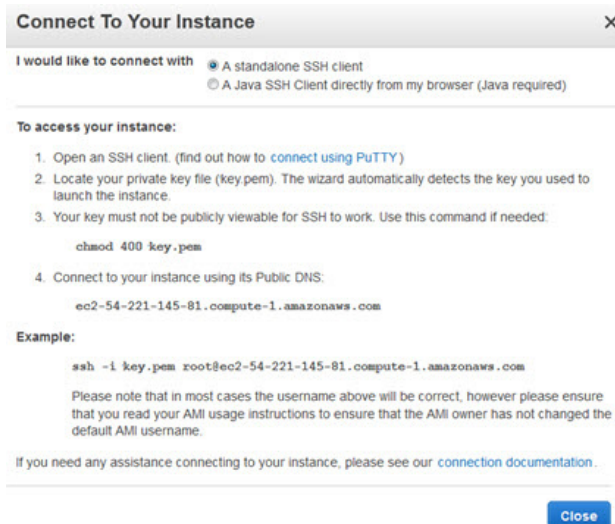
The SSH command needed is provided from the Amazon Web browser.

To access your AltaVault cloud-based appliance instance using Linux

1. Select the AMI instance name of the AltaVault cloud-based appliance.
2. From the top menu, select Connect.



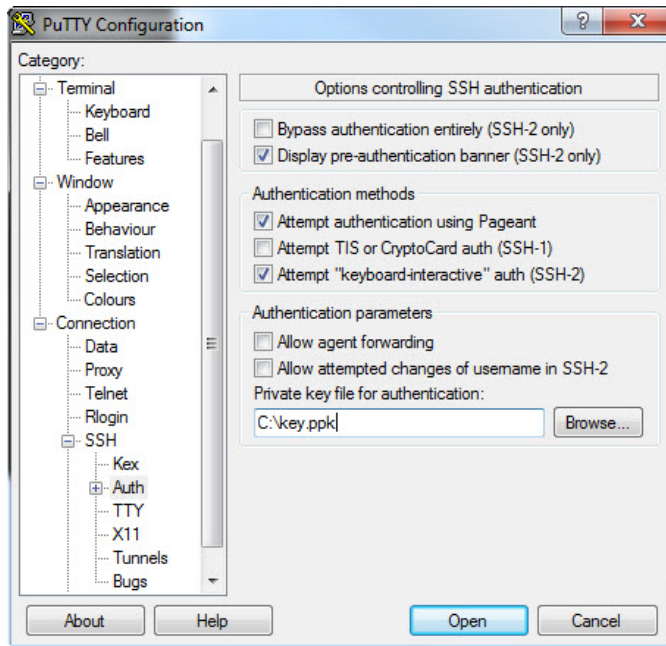
3. Select the radio button, A standalone SSH client.



4. Use the admin account to connect to the AltaVault cloud-based appliance AMI instance. You cannot use the root account.

Configuring Windows using PuTTY

If you use PuTTY, you must start by converting the private key from the .pem file format provided by Amazon to the .ppk file format used by PuTTY.



PuTTY does not accept .pem files directly as a private key file. Refer to the following Amazon document to set up an SSH connection using PuTTY: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>.

Configuring AltaVault account access

The AltaVault cloud-based appliance AMI instance does not initially come configured with a password configured for the default admin account. When you first connect to the AltaVault cloud-based appliance using an SSH session you are automatically logged in as admin. To set the initial account password for admin, issue the following commands:

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config)# username admin password 0 <your-new-password>
amnesiac (config)# write memory
```

Configuring networking

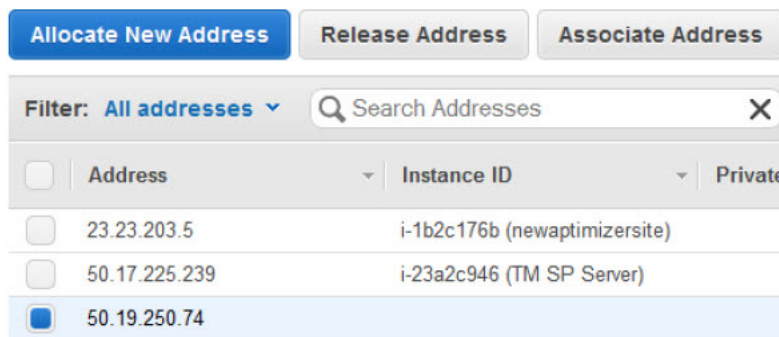
An AltaVault cloud-based appliance AMI instance comes with a single network adapter. The network adapter is used to receive and send all traffic from the device. By default, the AltaVault cloud-based appliance AMI instance provides an OpenDNS address that changes each time you restart the AltaVault cloud-based appliance. However, you can manually configure this as an Elastic IP address after initially deploying the appliance.

To manually configure an Elastic IP address

1. From the left menu of the EC2 Dashboard page, under NETWORK & SECURITY, select Elastic IPs.



2. If an Elastic IP address is available, select it from the list, and select Associate Address. If none is available, allocate a new Elastic IP address by selecting Allocate New Address.



3. Select the AltaVault cloud-based appliance AMI instance from the drop down list and click **Associate**.



How to achieve optimal performance using best practices

The following recommendations and best practices are intended to guide you to achieving optimal performance while reducing configuration and maintenance requirements.

Using best practices for deploying AMI instances

The following table displays best practices recommendations for deploying the AltaVault cloud-based appliance AMI Instance.

Best Practice	Description
Region	For general DR purposes, it is recommended to deploy the AltaVault cloud-based appliance in a geographically different region within Amazon than where your physical production environment resides. This provides you the best chance of recovering your production environment in to the Amazon EC2 environment should an entire region go down, say due to an electrical grid failure or natural event such as a hurricane. However, if your production environment is cloud based in Amazon EC2, then your AltaVault cloud-based appliance could be located in the same region.
Security Group	It is recommended to place the AltaVault cloud-based appliance AMI instance in the same media group as the backup or media server VMs so the VMs can communicate with the AltaVault cloud-based appliance AMI instance. Refer to AWS documentation for further details on how to configure security group settings.
Key Pair	The key pair is used to authenticate to the AltaVault cloud-based appliance AMI instance for performing operations, either using the AltaVault CLI or the GUI interface. Creating a key pair is a prerequisite requirement before deploying an AltaVault cloud-based appliance AMI instance.

Best practices for connecting an AMI instance to the network

To reliably connect to the AltaVault cloud-based appliance AMI instance without having to first refer to the AWS EC2 instance dashboard interface, associate the AltaVault cloud-based appliance AMI instance with an Elastic IP address. This guarantees that the AltaVault cloud-based appliance AMI instance is always reachable from the SSH or Web browser at the same URL address, regardless of whether the instance has been rebooted.

Do not attempt to set a static IP address using the AltaVault UI. This could cause the AltaVault cloud-based appliance to become unreachable by EC2, forcing you to redeploy and recover the AltaVault cloud-based appliance AMI instance.

Troubleshooting AltaVault AMI instance problems

AltaVault cloud-based appliance AMI instance does not start - If an AltaVault cloud-based appliance AMI instance does not start, confirm that you have properly deployed two EBS volumes and assigned them to the AltaVault cloud-based appliance AMI instance as described in the section, [“Storage configuration” on page 14](#).

AltaVault cloud-based appliance AMI instance is critical - Verify that the EBS volumes have been attached to the AltaVault cloud-based appliance AMI instance after it boots.

Issue the following commands to attach the /data partition using those EBS volumes previously created as shown in the figure below.

```
admin@ec2-54-242-126-236.compute-1.amazonaws.com's password:
Last login: Wed Oct  2 22:24:06 2013 from 216.200.161.6
amnesiac > en
amnesiac # conf t
amnesiac (config) # no service enable
Terminating optimization service...
.
amnesiac (config) # aws setup data partition
Data partition setup complete.
amnesiac (config) # service restart
% The optimization service is not running.
Starting optimization service...
.....
Storage Optimization Service: ready
amnesiac (config) #
```

These commands take a few minutes to complete because they format all EBS volumes and create a RAID0 /data partition.

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config)# no service enable
amnesiac (config)# aws setup data partition
```

Cannot login to the AltaVault Web GUI - If this is an initial deployment, confirm that the admin account was assigned a password. Refer to the section “[Configuring AltaVault account access](#)” on page 17. If this is a subsequent login access, confirm the user name and password being provided. For details regarding set up of user accounts, refer to the *NetApp AltaVault Cloud Integrated Storage User’s Guide*.

Next steps

After you log in to AltaVault virtual appliance, the configuration wizard displays and allows you to do the following:

- Specify system settings, including time zone and DNS.
- Configure cloud settings, including cloud credentials, licenses, and data encryption.
- Configure data interfaces that are used to receive data from the backup application.
- Configure CIFS shares or NFS exports that the backup application can access.
- Optionally, configure peer monitoring, email alerts, SNMP, and additional login security.
- Export the Virtual AltaVault configuration for safe keeping in the event of a disaster.
- To manage Virtual AltaVault using the command-line interface, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
- To complete configurations, go to the *NetApp AltaVault Cloud Integrated Storage Deployment Guide*.

CHAPTER 3 Performing AltaVault AMI upgrades

This chapter describes how to perform AMI upgrades. It includes the following sections:

- [“Overview of AltaVault AMI upgrades” on page 21](#)
- [“Plan an AltaVault AMI upgrade” on page 22](#)
- [“AltaVault AMI upgrades” on page 22](#)
- [“Cleaning up after the upgrade” on page 36](#)
- [“Accessing community support” on page 36](#)

Overview of AltaVault AMI upgrades

Data protection is an ever-increasing burden on the enterprise. Storage growth, security and compliance requirements, performance, and ultimately costs are all increasing. This causes organizations to potentially incur significantly increased risk. Cloud storage has quickly evolved and helps to mitigate some of these concerns, specifically around data growth, security, and costs. By leveraging highly elastic and scalable cloud storage at pennies per gigabyte per month, businesses can reduce the risks and costs associated with data protection.

NetApp AltaVault storage enables customers to securely back up data to any cloud at up to 90% less cost compared to on-premises solutions. AltaVault gives customers the power to tap into cloud economics while preserving investments in existing backup infrastructure and meeting backup and recovery Service Level Agreements (SLAs). AltaVault appliances simply act as a network attached storage target within a backup infrastructure, enabling organizations to eliminate their reliance on tape infrastructure and all of its associated capital and operational costs, while improving backup windows and disaster recovery capabilities.

It is simple to set up AltaVault appliance and start moving data to the cloud in as quickly as 30 minutes, compared to setting up tape or other disk replication infrastructures which can take days. Leveraging industry leading deduplication, compression and WAN optimization technologies, AltaVault appliances shrink data set sizes by 10 to 30x substantially reducing cloud storage costs, accelerating data transfers and storing more data within the local cache, speeding recovery.

Security is provided by encrypting data on-site, in-flight, as well as in the cloud using 256-bit AES encryption and SSL v3/TLS v1. AltaVault appliances provide a dual layer of encryption that ensures that any data moved into the cloud is not compromised, and it creates a complete end-to-end security solution for cloud storage.

Since an AltaVault appliance is an asymmetric solution, you can recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances provide flexibility to scale cloud storage as the business requirements change. All capital expenditure planning required with tape and disk replication based solutions is avoided, saving organizations up to 90%.

With AltaVault now supported in Amazon's AWS Marketplace as an Amazon machine image (AMI), organizations are further enabled by being able to recover on-premises workloads in the cloud and efficiently protect cloud-based workloads. Customers can quickly spin up an AltaVault AMI to recover data to Amazon EC2 and restore business-critical operations.

Plan an AltaVault AMI upgrade

AltaVault AMI upgrades are a disruptive process, and no operations to or from an AltaVault AMI may be performed while an upgrade is in progress. Upgrades can take upward of an hour to perform, depending on the version of AltaVault AMI appliance deployed. Upgrades can only be to the same model as currently deployed. For example, an AVA-c8 AMI can only be upgraded to a newer AVA-c8 AMI version and cannot be upgraded to a AVA-c16 AMI.

Make sure that all operations to and from AltaVault are complete or suspended. This includes operations such as backup, recovery, or replication. Review the AltaVault reports for information regarding ongoing activity and work with the backup administrator to schedule downtime.

Administrative login credentials for the Amazon Web Services (AWS) console are required to perform the upgrade actions, which include working with EBS volumes, altering the existing AltaVault AMI, and creating a new AltaVault AMI instance.

AltaVault AMI upgrades

To perform the upgrade, follow the steps exactly as described in the following sections. Carefully note the information that is required in each step because this information is carried forward to subsequent steps.

An AltaVault AMI upgrade takes place in the following distinct phases:

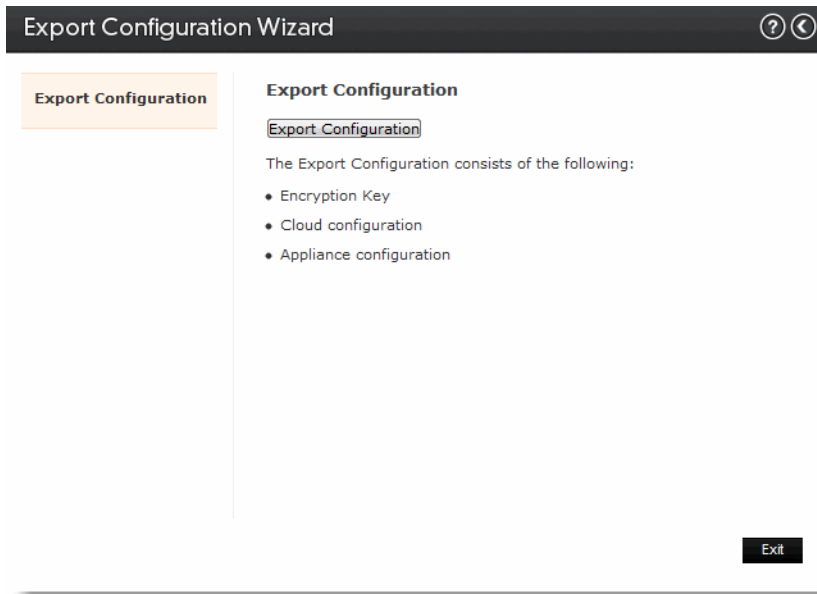
- [“Saving and exporting the original AltaVault AMI configuration” on page 23](#)
- [“Stopping the original AltaVault AMI and detaching the data volumes” on page 24](#)
- [“Launching and configuring the new AltaVault AMI instance upgrade” on page 26](#)
- [“Importing the Configuration File” on page 33](#)
- [“Attaching data volumes to the new upgrade instance” on page 34](#)
- [“Rebooting the new AltaVault AMI upgrade” on page 35](#)

Saving and exporting the original AltaVault AMI configuration

You must export your current configuration file from your older version of AltaVault, `altavault_config_(HOSTNAME)_(DATETIME).tgz`, and store it in a safe place, such as with your business continuity plans.

To export your configuration file

1. Choose Settings > Setup Wizard.
2. From the AltaVault wizard dashboard, click **Export Configuration**.



3. Type the password for the encryption key in the password field.
The password field appears only if you specified a password for your encryption key when you generated it in the cloud settings wizard page.
4. Click **Export Configuration** to download the current AltaVault configuration file, `AltaVault_config_(HOSTNAME)_(DATETIME).tgz`.
5. Click **Exit** to close the Export Configuration Wizard page and go back to the dashboard.
6. Click **Exit** to close the dashboard.

Stopping the original AltaVault AMI and detaching the data volumes

You must stop the original AltaVault AMI and record the instance information before detaching the original AltaVault AMI data volumes.

To stop the original AltaVault AMI and detach the data volumes

1. Log in to the AWS console.
2. Locate your AltaVault AMI launch instance.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Key Name	Monitoring	Launch Time	Security Group	Security Groups
2	i-775984a5	m3.xlarge	us-east-1d	running	2/2 checks ...	None	sh	disabled	August 5, 2015 at 1:51:14 P...	open	open
1	i-06a7b9d5	m3.xlarge	us-east-1d	running	2/2 checks ...	None	af	disabled	July 27, 2015 at 1:05:29 PM ...	open	open
store	i-9308d641	m3.xlarge	us-east-1d	running	2/2 checks ...	None	sha	disabled	August 5, 2015 at 9:00:15 P...	open	open

3. Record the Instance ID, Region, and Availability zone where the AltaVault AMI instance is located.

Instance items	Record instance values
Instance ID	
Region	
Availability zone	

4. Stop the original AltaVault AMI instance by selecting Actions > Instance State > Stop.

Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status
2	i-775984a5		running	2/2 checks ...	None
1	i-06a7b9d5		running	2/2 checks ...	None
store	i-9308d641		running	2/2 checks ...	None

5. Identify the volumes that are associated with the original AltaVault AMI instance:
 - a. Go to the Volumes selection and identify the volumes that are associated with the original AltaVault AMI instance that was stopped in the preceding step.

b. From the Attachment information field, locate the 100 GiB volume that has the value /dev/sda and /dev/sdk as shown below.

<input checked="" type="checkbox"/>	vol-78bb0c3c	100 GiB	standard	snap-fb1db044	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...
<input type="checkbox"/>	vol-19bb0c5d	1024 GiB	standard	snap-8c399433	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...
<input type="checkbox"/>	vol-1abb0c5e	1024 GiB	standard	snap-bc02af03	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...
<input type="checkbox"/>	vol-1bbb0c5f	100 GiB	standard	snap-ca399475	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...

Size	100 GiB	Snapshot	snap-fb1db044
Created	November 19, 2014 4:38:14 PM UTC-8	Availability Zone	us-east-1a
State	in-use	Encrypted	Not Encrypted
Attachment information	i-b1408d5d (Store) /dev/sda1 (attached)	KMS Key ID	
Volume type	standard	KMS Key Aliases	
Product codes	marketplace: 6ejkxeaj1fxpgj0ifqmi62e	KMS Key ARN	
IOPS	-		

These volumes will NOT be part of the upgrade, however, all other volumes will be part of the upgrade.

6. Select all the volumes attached to the original AltaVault AMI instance ID **except** the two volumes identified in Step 5.
7. Select the operation, Actions > Detach Volumes.

Name	Volume Type	Snapshot	Created	Availability Zone	State	Alarm Status	Attachment Information	Monitoring
vol-78bb0c3c	standard	snap-fb1db044	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...	
vol-19bb0c5d	standard	snap-8c399433	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...	
vol-1abb0c5e	standard	snap-bc02af03	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...	
vol-1bbb0c5f	standard	snap-ca399475	November 19, 2014 ...	us-east-1a	in-use	None	i-b1408d5d (OldSteel...	


Volumes: vol-f3bc0bb7, vol-84bc0bd0, vol-b5bc0bf1, vol-b6bc0bf2, vol-babc0bfe, vol-57bb0c13, vol-19bb0c5d, vol-1abb0c5e, vol-1bbb0c5f

Launching and configuring the new AltaVault AMI instance upgrade

Upgrade the AltaVault AMI to a custom installation of a new AltaVault AMI.

To launch and configure the new AltaVault AMI instance

1. Find the newer version of your AltaVault AMI model in the AWS Marketplace and click **Continue**.



AltaVault (formerly SteelStore) AVA-c4 for AWS

Sold by: [NetApp Inc.](#)

The NetApp AltaVault cloud-based appliances for AWS can be used for two primary purposes: to recover on-premises workloads in the cloud or to efficiently protect cloud-based workloads. For organizations without a secondary disaster recovery location, or for companies looking for extra protection with a low-cost tertiary site, AltaVault cloud-based appliances are the key to enabling cloud-based disaster recovery. Using on-premises AltaVault physical or virtual appliances, data is seamlessly and securely protected in the cloud. If the primary site is unavailable, customers can quickly spin-up a ... [Read more](#)

Customer Rating [Be the first to review this product](#)

Latest Version 4.1 [\(Other available versions\)](#)

Base Operating System Linux/Unix, Other 4.1

Delivery Method 64-bit Amazon Machine Image (AMI) [\(Learn more\)](#)

Support [See details below](#)

AWS Services Required Amazon EC2, Amazon EBS, Amazon S3

Highlights

- Open & Efficient: Integrates with ease into your existing backup architecture and uses inline deduplication and compression for up to 30:1 data-reduction ratios
- Secure: Offers end-to-end security for data at rest and in flight using FIPS 140-2 level 1-compliant encryption
- Simple: Takes you from zero to protected in less than 30 minutes

Continue You will have an opportunity to review your order before launching or being charged.

Pricing Details

For region **US East (N. Virginia)**

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	EC2 Usage	Software	Total
m3.xlarge	\$0.266/hr	\$0.67/hr	\$0.936/hr

EBS Magnetic volumes ⓘ
\$0.05 per GB-month of provisioned storage
\$0.05 per 1 million I/O requests

Assumes On-Demand EC2 [pricing](#)

2. Select the Manual Launch tab, and click the **Launch with EC2 Console** button that corresponds to the same region as the original AltaVault AMI.

Launch on EC2:

AltaVault (formerly SteelStore) AVA-c4 for AWS

1-Click Launch
Review, modify, and launch

Manual Launch
With EC2 Console, APIs or CLI

Launching Options

- You can click the "Launch with EC2 Console" buttons below and following the instructions to launch an instance of this software
- You can also find and launch these AMIs by searching for the AMI IDs (shown below) in the "Community AMIs" tab of the [EC2 Console](#) [Launch Wizard](#)
- You can view this information at a later time by visiting the Your Software page. For help, see [step-by-step instructions](#) [for launching Marketplace AMIs from the AWS Console](#).

Usage Instructions

Select a Version

4.1

Region	ID	
US East (N. Virginia)	ami-43f52028	Launch with EC2 Console
US West (Oregon)	ami-f7e9eac7	Launch with EC2 Console
US West (N. California)	ami-9f1fecdb	Launch with EC2 Console
EU (Ireland)	ami-064a0571	Launch with EC2 Console
Asia Pacific (Singapore)	ami-a8686bfa	Launch with EC2 Console
Asia Pacific (Sydney)	ami-55a9ee6f	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-c0fd56c0	Launch with EC2 Console
South America (Sao Paulo)	ami-972da18a	Launch with EC2 Console

Security Group

The vendor recommends using the following security group policies. You will be able to select these settings or configure your own when launching this software.

Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22 - 22	0.0.0.0/0
HTTP	tcp	80 - 80	0.0.0.0/0
	tcp	111 - 111	0.0.0.0/0
HTTPS	tcp	443 - 443	0.0.0.0/0
	tcp	445 - 445	0.0.0.0/0

Pricing Details

For region
US East (N. Virginia)

Hourly Fees

Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	Software	EC2	Total
m3.xlarge	\$0.67/hr	\$0.266/hr	\$0.936/hr

EBS Magnetic volumes

\$0.05 per GB-month of provisioned storage
\$0.05 per 1 million I/O requests

Assumes On-Demand EC2 pricing; prices for [Reserved](#) and [Spot](#) instances will be lower. See [pricing details](#).

Data transfer fees not included.

[Learn about instance types](#)

3. Select the appropriate instance type.

The instance type must match the original AltaVault AMI instance type, for example:

- AVA-c4 is m3.xlarge
- AVA-c8 is m3.2xlarge
- AVA-c16 is c3.8xlarge

4. After you select the appropriate instance type, click **Next: Configure Instance Details**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	Micro instances	t1.micro <small>Free tier eligible</small>	1	0.613	EBS only	-	Very Low
<input checked="" type="radio"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input checked="" type="radio"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m1.small	1	1.7	1 x 160	-	Low
<input type="checkbox"/>	General purpose	m1.medium	1	3.7	1 x 410	-	Moderate

Cancel Previous Review and Launch Next: Configure Instance Details

5. Configure the subnet to the same availability zone as the original AltaVault AMI and click **Next: Add Storage**.

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 the instance, and more.

Number of instances: 1

Purchasing option: ☐ Request Spot Instances

Network: vpc-c39c16a6 (172.31.0.0/16) (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: ☐ No preference (default subnet in any Availability Zone)

IAM role: **subnets-ec2-elastic-1c** (172.31.0.0/20) [Default in us-east-1c]

Shutdown behavior: ☐ Protect against accidental termination

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring

EBS-optimized instance: ☐ Launch as EBS-optimized instance

Tenancy: Shared tenancy (multi-tenant hardware)

Cancel Previous Review and Launch Next: Add Storage

6. Delete all the default EBS volumes in the list by selecting the X icon next to each volume, as shown below.

- Note that you should not delete the volume /dev/sdk, which will be 100GB in size.
- Also, you cannot delete the volume, /dev/sda1.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-fb1db044	100	Magnetic	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdf	snap-9b399424	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdh	snap-811db03e	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sde	snap-8039943f	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdd	snap-8c399433	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdg	snap-bc02a03	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdi	snap-80399430	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdk	snap-ca399475	100	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	snap-ef1db050	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdc	snap-61db047	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted

Cancel Previous **Review and Launch** Next: Tag Instance

7. After the EBS volumes are deleted, click **Next: Tag Instance**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-fb1db044	100	Magnetic	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdf	snap-9b399424	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdh	snap-811db03e	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sde	snap-8039943f	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdd	snap-8c399433	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdg	snap-bc02a03	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdi	snap-80399430	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdk	snap-ca399475	100	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	snap-ef1db050	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdc	snap-61db047	1024	Magnetic	N/A	<input type="checkbox"/>	Not Encrypted

Cancel Previous **Review and Launch** Next: Tag Instance

8. Give the newly upgraded AltaVault AMI a name value in the Value field, and click **Next: Configure Security Group**.

Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	NewSteelStoreAM

Create Tag (Up to 10 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

9. Configure the security group:

- Select an existing security group radio button
- Match the Security Group ID with the original AltaVault AMI.

Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description	Actions
sg-bf938eda	default	default VPC security group	Copy to new
sg-e69c7982	open	open	Copy to new
sg-e69c7982	AltaVault - formerly SteelStore- AVA-c4 for AWS-4-0-1-AutogenByAWSMP-	This security group was generated by AWS Marketplace and is base...	Copy to new

Inbound rules for sg-e69c7982 (Selected security groups: sg-e69c7982)

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	445	0.0.0.0/0
Custom UDP Rule	UDP	111	0.0.0.0/0
Custom TCP Rule	TCP	111	0.0.0.0/0

Cancel Previous **Review and Launch**

10. Click **Review and Launch**.

11. Select the option, **Continue with magnetic as the boot volume for this instance.**

Boot from General Purpose (SSD)

General Purpose (SSD) volumes provide the ability to burst to 3,000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

- ☐ Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).
- ☐ Make General Purpose (SSD) the boot volume for this instance.
- ☒ Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

☐ Don't show again

Next

12. Click **Next**.

13. Review your selections to make sure all the fields are correct.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Your instance configuration is not eligible for the free usage tier


To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#)

Improve your instance's security. Your security group, AltaVault (formerly SteelStore) AVA-c8 Cloud-Based Appliance for AWS

Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ **AMI Details** **AVA-c8-m18-GA** [Edit AMI](#)

 **AVA-c8-m18-GA-6c2bd4fa-5216-4b9e-b846-19e14e6b34f6-ami-3c0e9a54**

Root Device Type: ebs Virtualization type: paravirtual

▼ **Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m3.2xlarge	26	8	30	2 x 80	Yes	High

▼ **Security Groups** [Edit security groups](#)

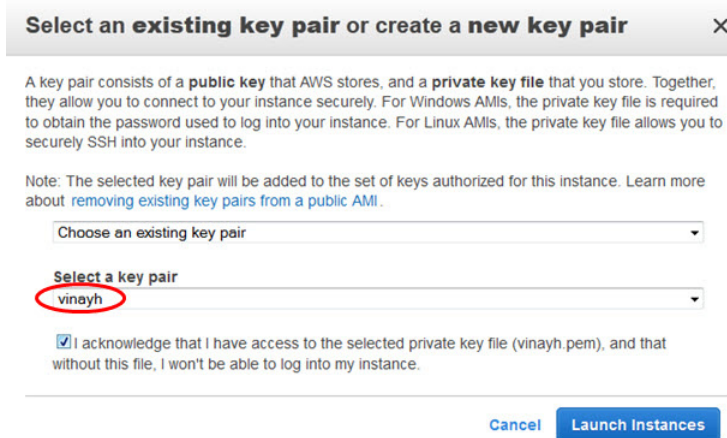
Cancel

Previous

Launch

14. Click **Launch**.

15. Select the existing key pair that the original AltaVault AMI was using and click **Launch Instances**.



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

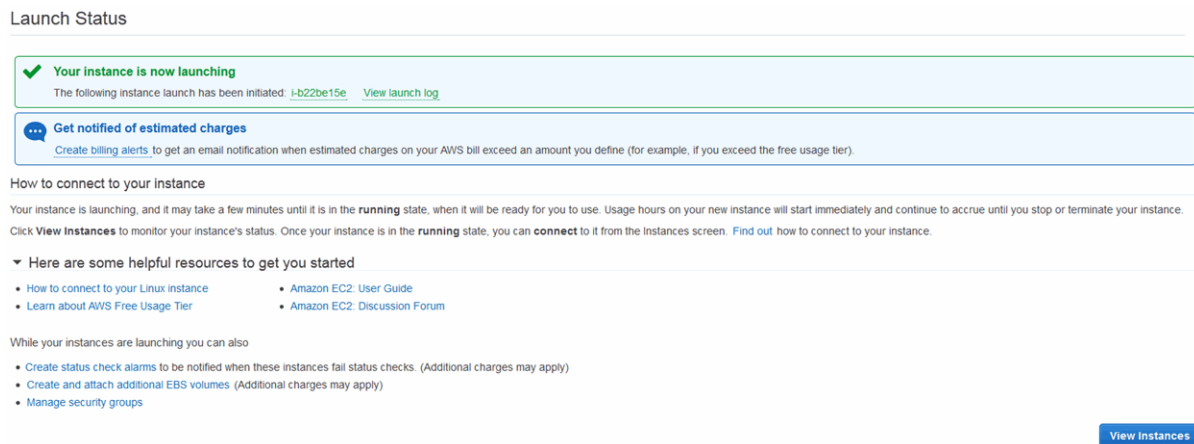
Choose an existing key pair ▼

Select a key pair
vinayh ▼

☒ I acknowledge that I have access to the selected private key file (vinayh.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

16. When the new AltaVault AMI upgrade instance launches, note the new instance ID.



Launch Status

✓ **Your instance is now launching**
The following instance launch has been initiated: [i-b22be15e](#). [View launch log](#)

⋮ **Get notified of estimated charges**
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instance
Your instance is launching, and it may take a few minutes until it is in the **running** state, when it will be ready for you to use. Usage hours on your new instance will start immediately and continue to accrue until you stop or terminate your instance. Click **View Instances** to monitor your instance's status. Once your instance is in the **running** state, you can **connect** to it from the Instances screen. [Find out](#) how to connect to your instance.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

17. Click **View Instances**

Login to AMI and set the admin account password

Login to the new AMI instance as admin using ssh with the key-pair that was used to launch the AMI. You must set a password for the AMI admin account. You can set the same password that was used in the older AMI.

To set the password for the AMI admin account

1. Run the following commands:

```
enable
configure terminal
```

2. Enter the following commands:

```
amnesiac (config)# username admin password 0 <password>
amnesiac (config)# write memory
```


Importing the Configuration File

This process imports the older AMI configuration into the new AMI instance.

To import the older AMI Configuration into the new AMI instance

1. Click **Import Configuration** in the wizard dashboard.

The screenshot shows the 'Import Configuration Wizard' window. The title bar is dark grey with a question mark icon. The main window has a light grey background. On the left, there is a sidebar with the text 'Import Configuration'. The main area has a title 'Import Configuration' and a subtitle 'This will allow you to import a previously saved AltaVault configuration'. Below this, there are two radio buttons: 'Local File' (selected) and 'URL'. The 'Local File' option has a 'Browse...' button and the text 'No file selected.'. The 'URL' option has a text field containing 'admin'. Below these, there is a checked checkbox labeled 'Import Shared Data Only (when to enable?)'. At the bottom of the main area, there is a 'Key Phrase:' label and a text field with six dots. A blue 'Import Configuration' button is positioned below the key phrase field. At the bottom right of the window, there is a dark grey 'Exit' button.

2. Import the configuration exported from the older AMI to the newer AltaVault.
3. Select Local File and click **Choose a File** to select a local configuration file from your computer.
4. Select the check box, Import Shared Data Only, to ensure that only shared data gets imported.
5. Select the Password protect the Encryption Key check box to specify a password for the encryption key.
If you select this option, you must enter the same password when you import or export the encryption key.
6. Click **Import Configuration**.

Caution: After this process completes, the system displays a prompt to restart the storage optimization service. Do not click the restart service button to restart the storage optimization service.

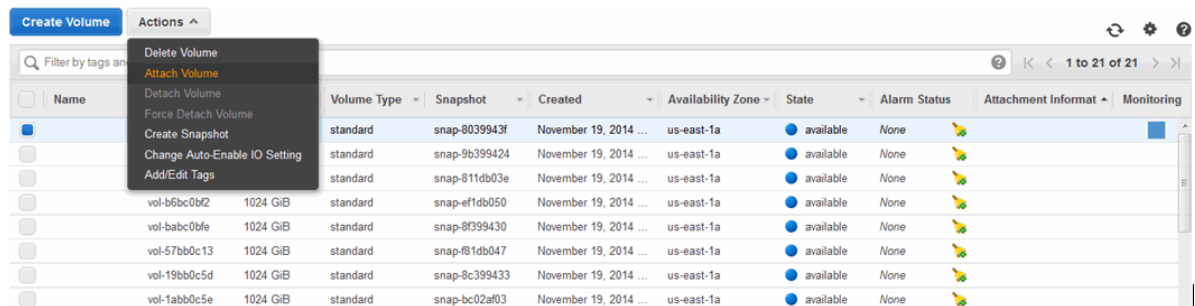
Attaching data volumes to the new upgrade instance

You must attach all the original AltaVault AMI data volumes (EBS volumes) to the newly created AltaVault AMI instance.

Caution: Failure to correctly attach all of the volumes results in the loss of the entire AltaVault AMI. Ensure that you attach all data volumes to the AltaVault AMI to prevent data loss.

To attach the original AltaVault AMI data volumes

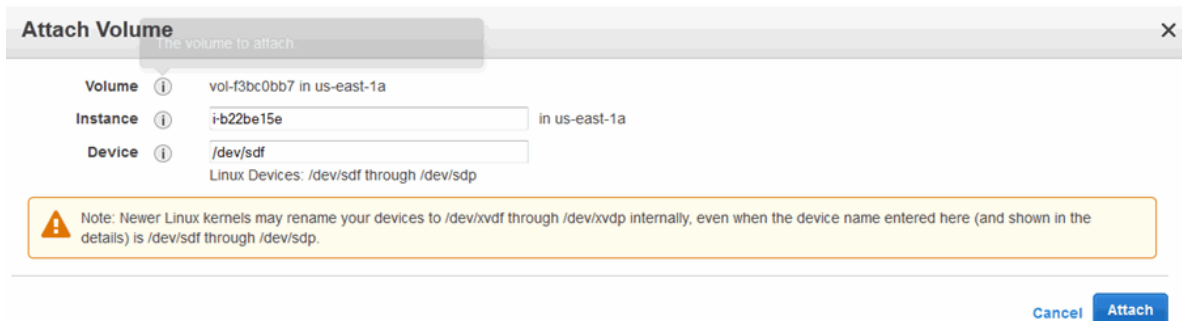
1. Go to AWS EC2 web console.
2. Navigate to Volumes in the left navigation tree.
3. Attach the EBS volumes from the original AltaVault AMI to the new upgraded AltaVault AMI.



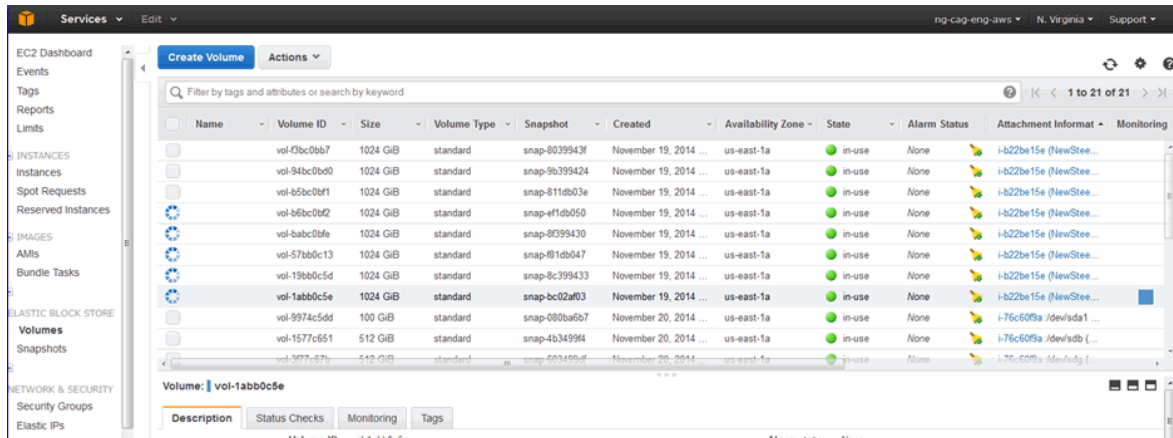
There should be a total of 8 volumes for the AltaVault AMI AVA-c4/AVA-c8 and a total of 16 volumes for the AltaVault AMI AVA-c16.

4. For each EBS volume added, check to ensure that the correct AltaVault AMI instance name is selected.

The device value can acquire any default value Amazon selects as shown in the figure below.



- Confirm that all the volumes are attached.

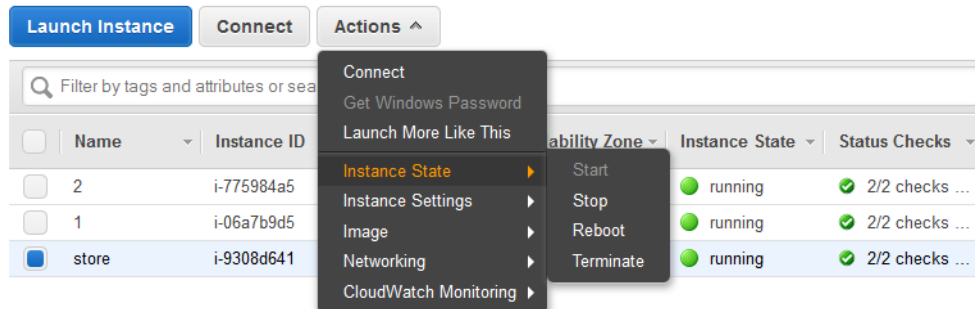


Rebooting the new AltaVault AMI upgrade

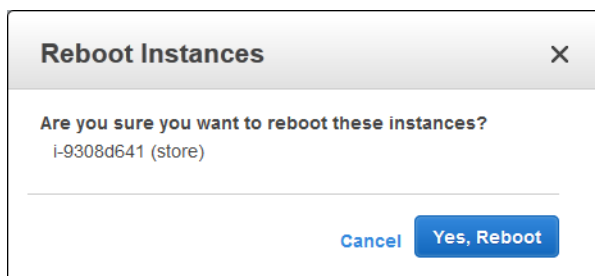
You must reboot the new AltaVault AMI upgrade instance and associate it with the original cloud storage bucket.

To reboot the newly upgraded AltaVault AMI instance

- From the Instances page, select Actions > Instance State > Reboot.



- To confirm the reboot, click **Yes, Reboot**.



After the reboot completes, use a Web browser to connect to the new AltaVault AMI public IP.

The new AltaVault AMI upgrade detects a serial mismatch when it attempts to acquire cloud storage bucket ownership. When this occurs, the AltaVault AMI state becomes critical.

3. To correct a serial mismatch, SSH to the AltaVault command-line interface (CLI) and issue the following commands:

```
enable
configure terminal
no service enable
megastore guid reset
service enable
```

The AltaVault AMI indicates a healthy state with a green check mark.



4. Save the configuration of the new AMI.

Cleaning up after the upgrade

When the upgrade process is complete and operations have resumed using the new AltaVault AMI upgrade, you can terminate the original AltaVault AMI to stop incurring operating charges for its use.

To terminate the original AltaVault AMI, select it from the Instances page of the AWS console and select Actions > Terminate.

Note: After you terminate the original AltaVault AMI, it cannot be recovered.

Accessing community support

AltaVault AMI is supported through the NetApp Community portal. Access the portal by selecting: <http://community.netapp.com/t5/forums/filteredbylabelpage/board-id/hybrid-cloud-discussions/label-name/AltaVault>.

CHAPTER 4 Deploying a Microsoft Azure virtual machine

This chapter describes how to deploy the AltaVault cloud-based appliance within the Microsoft® Azure environment. It includes the following sections:

- “Overview of Microsoft Azure” on page 37
- “Creating an AltaVault virtual machine” on page 37
- “Next steps” on page 46

Overview of Microsoft Azure

Microsoft Azure is an open and flexible cloud platform that enables you to quickly build, deploy and manage applications across a global network of Microsoft-managed data centers. You can build applications using any language, tool or framework. And you can integrate your public cloud applications with your existing IT environment.

Microsoft Azure enables you to easily scale your applications to any size. It is a fully automated self-service platform that allows you to provision resources within minutes. Elastically grow or shrink your resource usage based on your needs. You only pay for the resources your application uses. Microsoft Azure is available in multiple data centers around the world, enabling you to deploy your applications close to your customers.

It allows for virtual machines to provision on-demand, scalable computer infrastructure when flexible resources are needed. You can create VMs that run Windows, Linux, or enterprise applications.

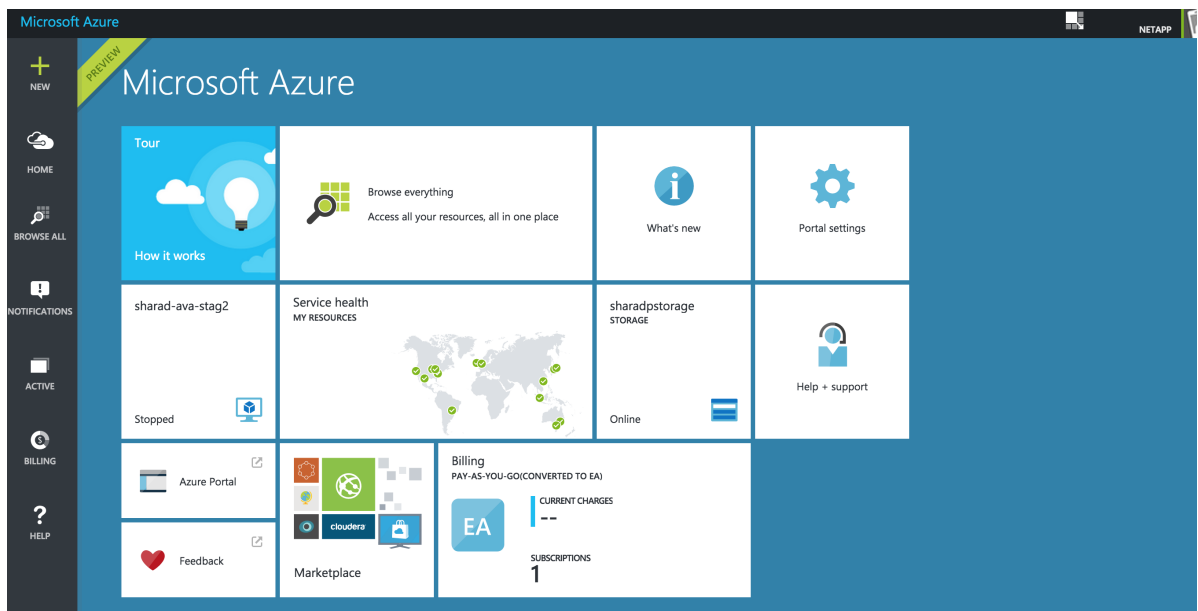
Creating an AltaVault virtual machine

Before you create a virtual machine on Microsoft Azure, ensure that you have a login account for Windows Azure. For more details, see <https://portal.azure.com>.

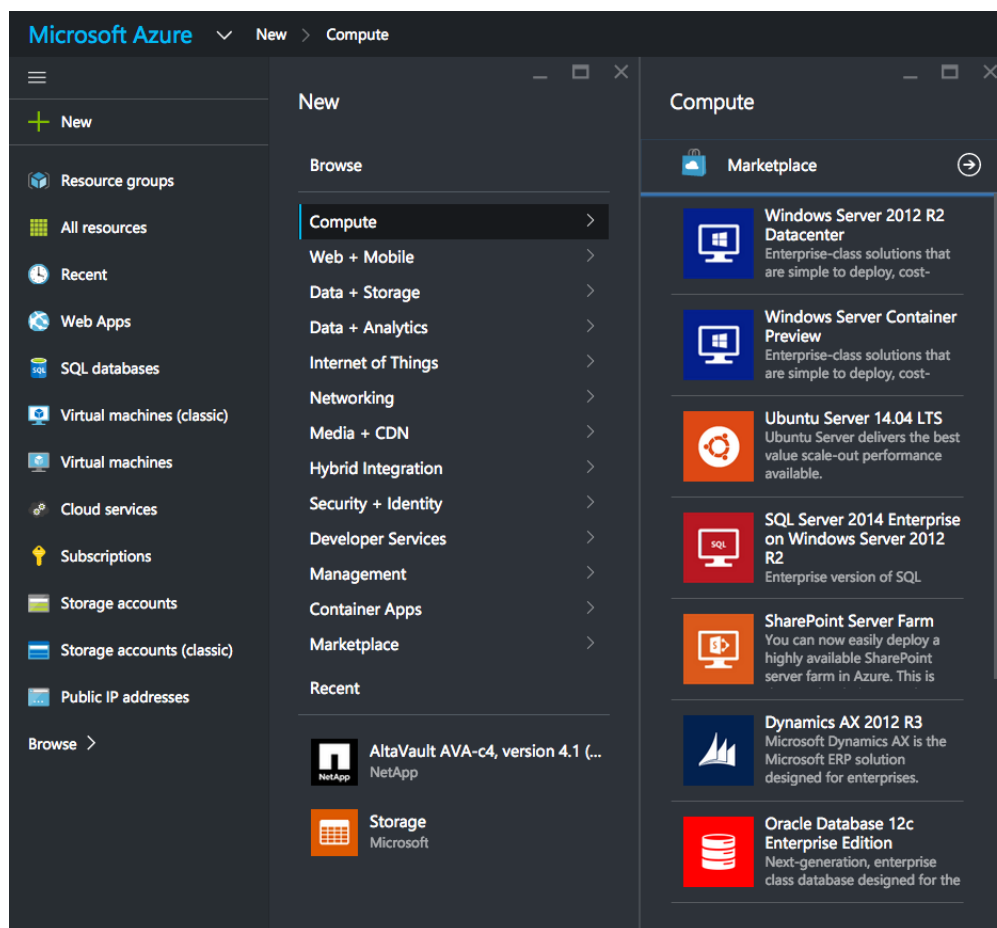
To create a virtual machine

1. Log in to the Microsoft Azure portal at <https://portal.azure.com>.

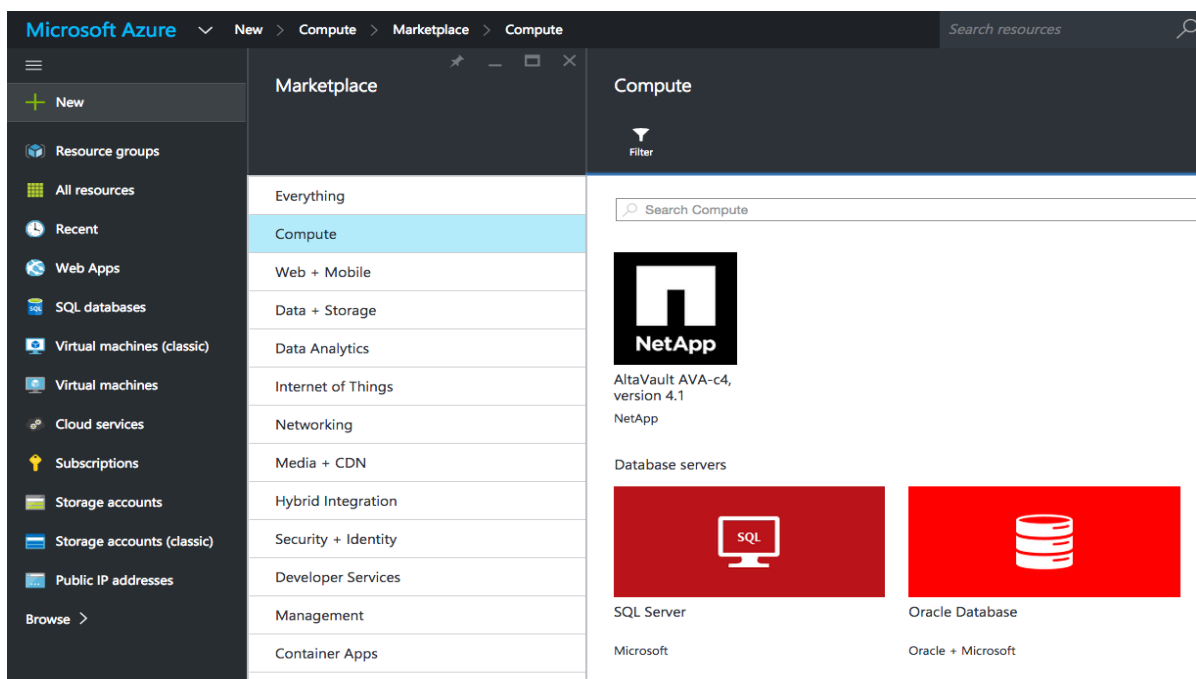
2. Select New (+) in the upper-left corner of the screen.



3. Select Compute, then, select the Marketplace icon to the right.

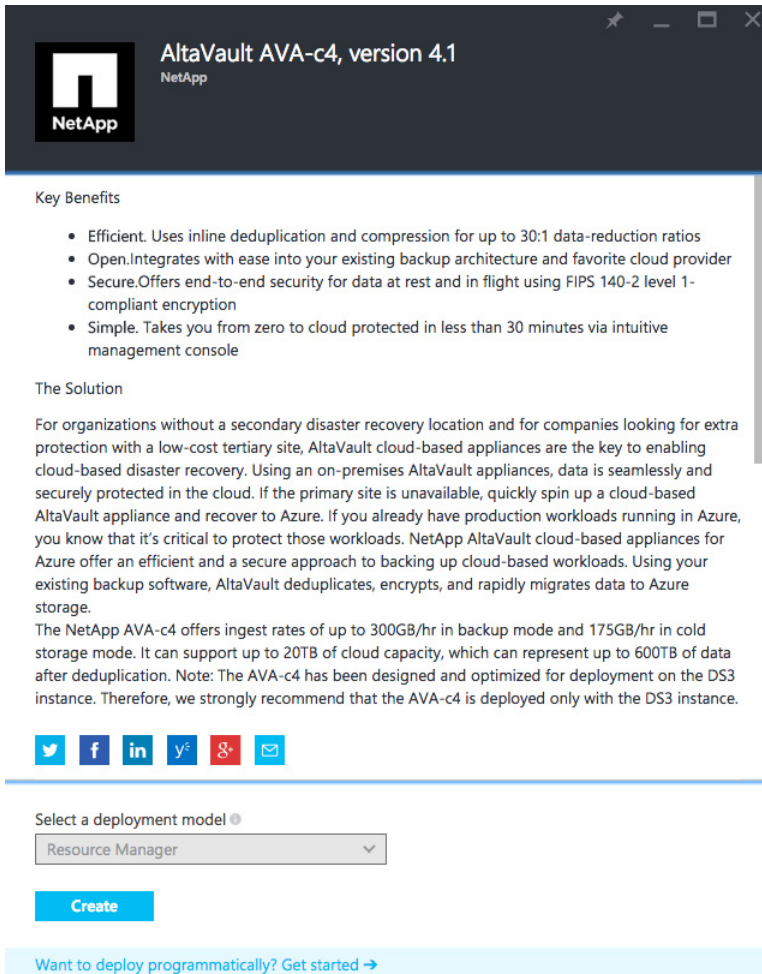


4. Perform a search on AltaVault to find the NetApp AltaVault cloud-based appliance.



5. Select the appliance from the search results.

6. Scroll down and click **Create**.



AltaVault AVA-c4, version 4.1
NetApp

Key Benefits


- Efficient. Uses inline deduplication and compression for up to 30:1 data-reduction ratios
- Open. Integrates with ease into your existing backup architecture and favorite cloud provider
- Secure. Offers end-to-end security for data at rest and in flight using FIPS 140-2 level 1-compliant encryption
- Simple. Takes you from zero to cloud protected in less than 30 minutes via intuitive management console


The Solution

For organizations without a secondary disaster recovery location and for companies looking for extra protection with a low-cost tertiary site, AltaVault cloud-based appliances are the key to enabling cloud-based disaster recovery. Using an on-premises AltaVault appliances, data is seamlessly and securely protected in the cloud. If the primary site is unavailable, quickly spin up a cloud-based AltaVault appliance and recover to Azure. If you already have production workloads running in Azure, you know that it's critical to protect those workloads. NetApp AltaVault cloud-based appliances for Azure offer an efficient and a secure approach to backing up cloud-based workloads. Using your existing backup software, AltaVault deduplicates, encrypts, and rapidly migrates data to Azure storage.

The NetApp AVA-c4 offers ingest rates of up to 300GB/hr in backup mode and 175GB/hr in cold storage mode. It can support up to 20TB of cloud capacity, which can represent up to 600TB of data after deduplication. Note: The AVA-c4 has been designed and optimized for deployment on the DS3 instance. Therefore, we strongly recommend that the AVA-c4 is deployed only with the DS3 instance.

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)

Select a deployment model 

Resource Manager 

Create

[Want to deploy programmatically? Get started →](#)

7. Step 1, configure basic settings for the virtual machine:

The screenshot shows the 'Create virtual machine' wizard in the Azure portal. The 'Basics' step is selected, and the following settings are visible:

- Name:** (empty text box)
- User name:** (empty text box)
- Authentication type:** Password, **SSH public key** (selected)
- SSH public key:** (empty text box)
- Subscription:** Pay-As-You-Go(Converted to EA)
- Resource group:** (empty text box)
- Location:** East US 2

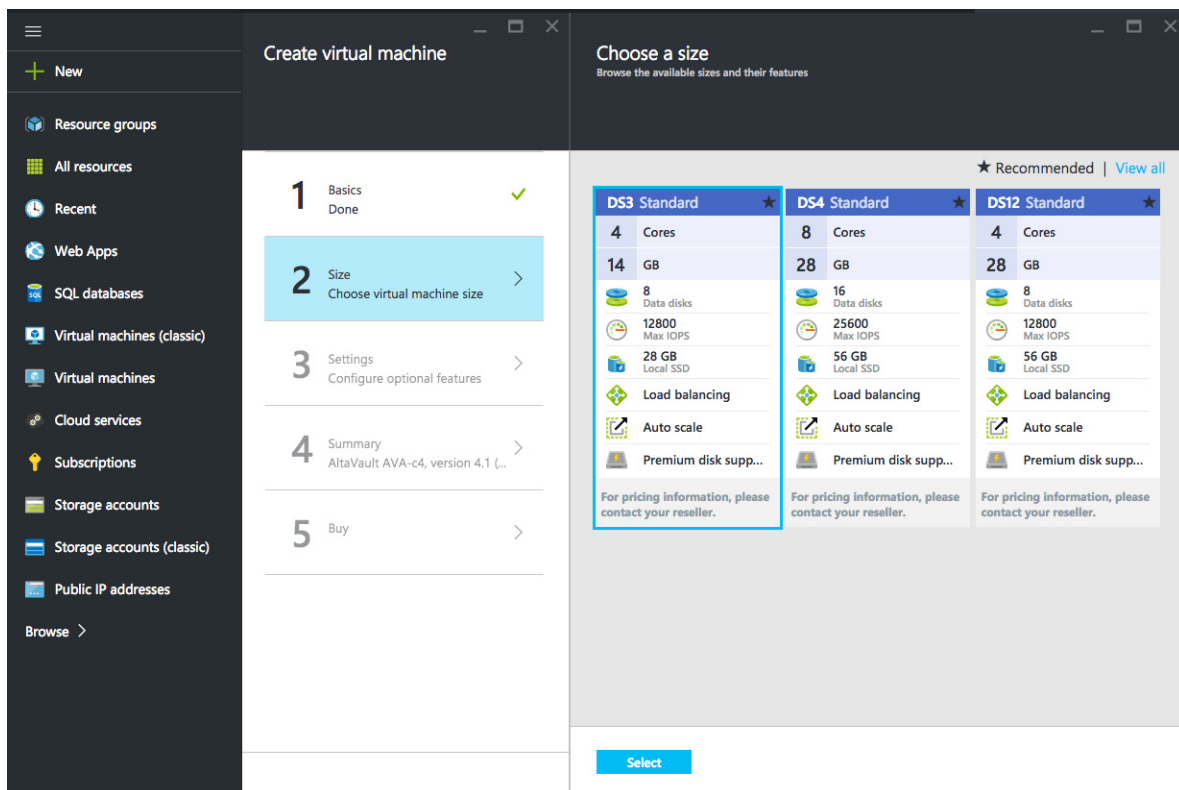
An 'OK' button is located at the bottom right of the 'Basics' section.

a. Configure basic settings as described in the following table:

Basic settings	Description
Name	Specify the virtual machine name that is easy to remember and describes what it is used for.
User name	Specify a user name. This user name is used as a placeholder and is not used upon a login; you log in to the virtual machine with the user name, <i>admin</i> .
Authentication type	Specify SSH Public key, the supported authentication type.
Note: Only SSH public key is supported; password is not a supported authentication type.	
SSH public key	Specify an open SSH public key that can be generated with tools like ssh-keygen, etc.
Resource group	Specify a resource group for AltaVault.
Location	Specify a location for the AltaVault virtual machine.

b. Click **OK**.

8. Step 2, choose the virtual machine size:



- For the virtual machine size, select DS3 Standard, the only supported selection.
- From the bottom of the screen, click **Select**.

9. Step 3, configure optional features:

The screenshot shows the 'Create virtual machine' wizard in the Azure portal. The 'Settings' step is selected, showing configuration options for Storage, Network, and Monitoring. The 'Disk type' is set to 'Premium (SSD)'. The 'Storage account' is 'avaeastus2'. The 'Virtual network' is 'avaresource', and the 'Subnet' is 'default (10.10.0.0/24)'. The 'Public IP address' is '(new) ava', and the 'Network security group' is '(new) ava'. The 'Diagnostics' are set to 'Disabled'. An 'OK' button is at the bottom.

a. Configure optional settings as described in the following table:

Optional features	Description
Disk type	Specify Premium SSD disk type
Storage account for (new) AVA storage	Create a new storage account or specify an existing one.
Network	Virtual network: Create a new virtual network or specify an existing one. Subnet: Create a new subnet or specify the default. Public IP address: Create a public IP address or specify an existing one. Network security group: Use the default settings.
Monitoring	Disable or enable monitoring.

b. Click **OK**.

10. Step 4, confirm the summary settings by clicking **OK**.

Summary	
Subscription	Pay-As-You-Go(Converted to EA)
Resource group	avaresource
Location	East US 2
Computer name	avademo
User name	avademo
Size	Standard DS3
Disk type	Premium (SSD)
Storage account	avaeastus2
Virtual network	avaresource
Subnet	default (10.10.0.0/24)
Public IP address	(new) ava
Network security group	(new) ava
Availability set	None
Diagnostics	Disabled

OK

11. Step 5, accept the terms of the agreement and click **Create**.

Offer details

AltaVault AVA-c4, version 4.1
by NetApp

Standard DS3
[Legal terms](#) and [privacy policy](#)

For pricing information, please contact your reseller. Please note that your reseller may not permit monetary commitment funds or other subscription credits to be used to purchase the above offering(s). If any Microsoft products are included in the above offering(s) (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Legal terms

By clicking "Create," I (a) agree to the legal terms and privacy statement(s) associated with each offering above, and (b) agree that Microsoft may share my contact information and these transaction details with any third-party vendors, if listed above. Microsoft does not provide rights for non-Microsoft products or services. See the [Azure Marketplace Terms](#) for additional details.

Create

The newly provisioned virtual machine displays in the Microsoft Azure preview page.



Log in to AltaVault VM

Log in to the AltaVault virtual machine (VM) using the public IP and private SSH key.

To log in to AltaVault

1. Get the Public IP from the Virtual Machine settings.
2. Use the private SSH key to login to the CLI.

```
ssh -i <path to SSH private key> admin@<Public IP>
```

Initialize the datastore

Use the following commands to format all data disks required to create a datastore. It may take some time for the commands to complete.

To create the datastore

Run the following commands in the command line interface (CLI):

```
amnesiac> enable
amnesiac# configure terminal
amnesiac (config)# no service enable
amnesiac (config)# azure setup data partition
```

Next steps

After you log in to AltaVault virtual appliance, the configuration wizard displays and allows you to do the following:

- Specify system settings, including time zone and DNS.
- Configure cloud settings, including cloud credentials, licenses, and data encryption.
- Configure data interfaces that are used to receive data from the backup application.
- Configure CIFS shares or NFS exports that the backup application can access.
- Optionally, configure peer monitoring, email alerts, SNMP, and additional login security.
- Export the Virtual AltaVault configuration for safe keeping in the event of a disaster.
- To manage Virtual AltaVault using the command-line interface, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
- To complete configurations, go to the *NetApp AltaVault Cloud Integrated Storage Deployment Guide*.

Copyright information

Copyright © 1994-2015 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark information

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

How to send your comments

Index

A

- admin account
 - password set 32
- AltaVault
 - scenarios 7
 - supported versions 8
- Amazon
 - EC2 7
- AMI instance configuration 26

C

- cloud
 - disaster recovery 6
- configuration
 - exporting 23
 - importing 33

D

- data volumes
 - attaching 34
- detaching the data volumes 24

E

- EBS volumes 34
- EC2 7
 - overview 5
- exporting
 - configuration file 23

M

- Microsoft Azure 37
 - prerequisites 37

N

- next steps 20, 46

O

- Overview
 - backup 5
 - disaster recovery 5

P

- password set for AMI 32

U

- upgrade cleanup 36

