NetApp® AltaVault™ Cloud Integrated Storage 4.4

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:215-12479_A0
November 2017

Contents

CHAPTER 1

Introducing AltaVault cloud-based appliances

Use this guide to deploy an AltaVault cloud-based appliance using Amazon Web Services™ Marketplace or Microsoft Azure™.

Cloud backup and disaster recovery

AltaVault cloud-based appliances provide users flexibility in protecting compute environments running in Amazon Web Services (AWS) or Microsoft Azure as well as provide users an alternative solution to performing traditional disaster recovery using secondary sites. Utilizing compute from a cloud gives companies the ability to have a disaster recovery solution at a much lower cost than maintaining the infrastructure, security, and management of a physical disaster recovery site.

Cloud-based workload protection

AltaVault cloud-based appliance instances offer an efficient and secure approach to backing up cloud-based workloads. Using your existing backup software, AltaVault cloud-based appliance deduplicates, encrypts, and rapidly replicates data to object storage, reducing the long-term costs of protecting the data. Users can add an additional data protection tier to a cloud provider's existing data protection features by having an AltaVault cloud-based appliance instance.

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 instances are the key to enabling cloud-based disaster recovery. Using on-premise AltaVault physical or virtual appliances, data is seamlessly and securely protected in the cloud in cases where the local AltaVault becomes unavailable, customers can quickly spin-up an Amazon or Azure cloud-based AltaVault and recover their data.

Supported AltaVault cloud-based appliance models

For Amazon Machine Images (AMI), AltaVault is available in the following models: AVA-c4, AVA-c8, AVA-c16.

For Microsoft Azure Virtual Machine (AVM), AltaVault is available in the following model: AVA-c4.

Models vary by local storage capacity, which ranges from 4 TB to 16 TB.

CHAPTER 2

Installing an AltaVault Amazon Machine Image

The AltaVault Amazon Machine Image (AMI) is an AltaVault cloud-based appliance instance built specifically for deployment within the Amazon EC2 compute environment.

Deploying an AltaVault AMI

This section describes deploying an AltaVault cloud-based appliance from the AWS marketplace.

Accessing the AltaVault AMI

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 model that you want to use: AVA-c4, AVA-c8, AVA-c16.
4. Click **Continue**.
5. Enter your AWS credentials to sign in to your account.

6. Choose one of the following launch methods:
   - 1-Click Launch: Preferred method for AVA-c4 and AVA-c8.
   - Manual Launch: Select this launch method if the AVA-16c 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.

Deploying 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.

   The default selection is US East (Virginia).
3. Chose a Security Group for the AltaVault cloud based appliance AMI instance.

   Security Group - The security group describes which ports and IPs the AltaVault cloud-based appliance AMI instance uses to communicate with other VMs.
4. Chose a Key Pair. This key pair provides the mechanism for communicating with the AltaVault AMI instance.

   For instructions on creating a key pair, see the following information:
   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**.

   Amazon displays the software installation details.
6. Continue to "Configuring the SSH console for AltaVault cloud-based appliance access" on page 9 in this guide.

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.

Deploying 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.
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. Choose an Instance Type by scrolling down to the Compute optimized section and selecting the instance type, c4.8xlarge.
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.
6. Click **Next: Add Storage**.

   The Add Storage page appears. Do not change any values on this page.
7. Click **Next: Tag Instance**.
8. In Tag Instance page, optionally provide a value for the key name, and click **Next: Configure Security Group**.
9. Chose a Security Group for the AltaVault.

   The security group describes which ports and IPs the AltaVault uses to communicate with other VMs.
10. Click **Review and Launch**.
11. From the Boot from General Purpose (SSD) page, select "Continue with Magnetic as the boot volume for this instance."
12. Click **Next**.
13. Review the launch instance details and click **Launch**.
14. From the Select an existing key pair or create a new key pair page, select an existing key pair.
15. Click **Launch**. Amazon displays the Launch Status.
16. Click **View Instance** to display your AltaVault instance.
17. Continue to "Configuring the SSH console for AltaVault cloud-based appliance access" on page 9 in this guide.

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

Configure access to the AltaVault cloud-based appliance using the Amazon Web browser

1. Select the instance name of the AltaVault 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**.

Configure access to the AltaVault cloud-based appliance using a 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 may use PuTTY)
- AMI Instance name of the AltaVault
- Public DNS name of the instance
- Private key (.pem) file associated with this AMI from your Amazon account

---

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 connect to the AltaVault 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.

To access your AltaVault AMI instance using Linux

1. From the Amazon EC2 web console page, select the AMI instance name of the AltaVault.
2. From the top menu, select **Connect**.
3. Select the radio button, **A standalone SSH client**. A command displays on the console page.
4. Copy the command resulting from step 3 into your Linux console prompt to begin an SSH session.
5. Use the admin account to connect to the AltaVault AMI instance. You cannot use the root account.

To access your AltaVault AMI instance using Windows PuTTY

1. 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.
2. In the PuTTY session pane, enter the public name to the AltaVault AMI instance into the Host name field.
3. In the PuTTY Connection > SSH > Auth pane, enter the path and file name of the converted private key file from Step 1 above into the Private key file for authentication textbox.

Connecting to the AltaVault AMI and next steps

When the AltaVault connection is established for the first time, you will be presented with the AltaVault CLI configuration wizard. Refer to Chapter 3 in the *AltaVault Cloud Integrated Storage Administration Guide* for details on completing this wizard and performing further configuration of AltaVault.

Configuring a static IP address for AltaVault

An AltaVault AMI instance comes with a single network adapter. By default, the AltaVault AMI instance is given a public IP address that changes each time you restart the AltaVault. However, you can manually configure this as a static IP address after initially deploying the appliance using an Elastic IP address from AWS.

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 AMI instance from the drop down list and click **Associate**.

Best practices for achieving optimal performance

Best practices for deploying AMI instances

Best Practice	Description
Security Group	For general disaster recovery purposes, it is recommended to deploy the AltaVault AMI in a different region within Amazon than where your physical or virtual production environment resides. However, if your production environment is cloud based in Amazon EC2, then your AltaVault AMI could be located in the same region and placement group.
Security Group	It is recommended to place the AltaVault AMI instance in the same media group as the backup or media server virtual machines so the virtual machines can communicate with the AltaVault 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 AMI instance. Creating a key pair is a prerequisite requirement before deploying an AltaVault AMI instance.
Placement Group	Both the AVA-c16 and the back-up application instance should be in the same placement group in order to take advantage of use the 10 GbE infrastructure for communications.
MTU	It is recommended to set the MTU size to 9000 to optimize the network interface performance with AltaVault. Although an MTU size of 9000 is not supported by all environments, it is supported by AWS. It is important that both the AltaVault appliance and client MTU sizes match. For more information, refer to the following AWS link: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html

Best practices for connecting an AMI instance to the network

Optionally, to connect to the AltaVault AMI instance without having to first refer to the AWS dashboard, associate the AltaVault instance with an Elastic IP address.

Do not attempt to set a static IP address using the AltaVault UI as this can cause the appliance to become unreachable by EC2, and result in a redeployment and recovery of the AltaVault AMI instance.

CHAPTER 3

Installing AltaVault Microsoft Azure Virtual Machine

This chapter describes how to install the AltaVault cloud-based appliance within the Microsoft® Azure environment.

Deploying an AltaVault AVM

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. Perform a search on AltaVault to find the NetApp AltaVault cloud-based appliance.
4. Select the appliance from the search results.
5. Scroll down and click **Create**. A screen appears with steps for creating the virtual machine.
6. In Step 1, configure basic settings for the virtual machine:
   a. Configure basic settings as described in the following table:

Basic settings	Description
Name	Specify the virtual machine name.
VM disk type	Specify SSD disk type.
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, *admin*.
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.
Subscription	Select the subscription for your environment.
Resource group	Specify a resource group for AltaVault.
Location	Specify a location for the AltaVault virtual machine.

b. Click **OK**.

7. In Step 2, choose the virtual machine size. For the virtual machine size, DS3 Standard is the only supported selection. Click **Select.**

   The location where you deploy AltaVault AVM will determine if the DS3 Standard is available. For more information, go to https://azure.microsoft.com/en-us/regions/#services.

8. In Step 3, configure optional features:

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

Optional features	Description
Storage	Use managed disks: No. Storage account: Create new or specify an existing Premium storage account to be used for AltaVault local cache.
Network	Virtual network: Create new or specify an existing one. Subnet: Create new or specify the default. Public IP address: Create or specify an existing one. Network security group: Use the default settings.
Extensions	Not used.
High Availability	None
Monitoring	Disable monitoring options.

   b. Click **OK**.

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

10. In Step 5, review the terms of the agreement and click **Purchase**.

11. After deployment, select the newly deployed AltaVault AVM in the Azure portal to display the Public IP address required to log in to the AltaVault.

Connecting to the AltaVault AVM and next steps

1. Power on the AVM and connect to it using the Public IP address and private SSH key. For example, using SSH enter the following command:

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

   When you start the AltaVault AVM for the first time, the initial boot-up process can take a few minutes. During this time, the system does not display any debugging message on the console, and you might incorrectly interpret that the system has stopped responding. Do not hard power reset the appliance during initial boot-up; this will corrupt the file system on the cache disks and log the following errors in the system logs:

   ```
   Jul 21 15:55:40 localhost rbtinit: mount: can't find /data in /etc/fstab or /etc/mtab
   ```

```
Jul 21 15:55:50 altavault statsd[3083]: [statsd.NOTICE]: Alarm triggered for rising error for
event datastore_disk
```

Note: If you inadvertently interrupted the AltaVault AVM boot process (described above), you will need to delete and then add the cache disk again and wait until the system completes its boot process.

---

2. When the AltaVault connection is established for the first time, you will be presented with the AltaVault CLI configuration wizard. Refer to Chapter 3 in the *AltaVault Cloud Integrated Storage Administration Guide* for details on completing this wizard and performing further configuration of AltaVault.

APPENDIX A Performing AltaVault AMI and AVM software upgrades

This chapter describes how to perform AltaVault cloud-based appliance upgrades. The information in this chapter applies to both the AMI and AVM AltaVault appliance models.

Plan an AltaVault cloud-based appliance upgrade

AltaVault upgrades are a disruptive process and can take up to an hour to complete. During the upgrade, no operations to or from an AltaVault can be performed. Upgrades are limited to new versions of AltaVault and are not intended to migrate from one version of a cloud appliance to another. For example, an AVA-c8 cannot be upgraded to an AVA-c16.

Prior to initiating the upgrade, ensure that all operations to and from AltaVault are complete or suspended.

Note: The software upgrade procedure for AltaVault AMI is different from the software upgrade process for other AltaVault appliances. 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. Use the procedure in this chapter to upgrade the AltaVault AMI.

AltaVault AMI upgrades

To perform the upgrade, follow the steps 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

You must export your current configuration file from your existing AltaVault, altavault_config_(HOSTNAME)_(DATETIME).tgz, and store it in a safe place.

To export your configuration file

1. Choose Configure > 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.
3. Record the Instance ID, Region, Placement Group, and Availability zone where the AltaVault AMI instance is located.
4. Stop the original AltaVault AMI instance by selecting Actions > Instance State > Stop.
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.

Note: There are two 100 GiB volumes for AMI instances prior to AltaVault 4.3. For AltaVault 4.3 and later releases, there is one 92 GiB volume for AMI instances that has the value /dev/xvda.

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 5b.

7. Select the operation, Actions > Detach Volumes.

8. Save the private IP address and the VPC name of the original, older version of the AltaVault AMI appliance, for example, in a notepad.

9. Terminate the old appliance.

Launching and configuring the new AltaVault AMI instance upgrade

The process to perform a software upgrade of the AltaVault AMI requires you to deploy a custom installation of a new AltaVault AMI and move the existing AMI instance data volumes to this new instance.

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**.

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.

3. Select the appropriate instance type.

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

   - AVA-c4 is m4.xlarge
   - AVA-c8 is m4.2xlarge
   - AVA-c16 is c4.8xlarge

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

5. In the Network Interfaces section, set the Primary IP field to the private IP address of the original AltaVault appliance that you saved earlier. This ensures that the backup application will continue to talk to the new appliance using the same IP address.

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

7. Delete all the default EBS volumes in the list by selecting the X icon next to each volume.

Note: Do not delete volume /dev/xvda.

---

8. After the EBS volumes are deleted, click **Next: Tag Instance**.
9. Give the newly upgraded AltaVault AMI a name value in the Value field, and click **Next: Configure Security Group**.
10. Configure the security group:
    - Select an existing security group radio button.
    - Match the Security Group ID with the original AltaVault AMI.
11. Click **Review and Launch**.
12. Select the option, **Continue with magnetic as the boot volume for this instance**.
13. Click **Next**.
14. Review your selections to make sure all the fields are correct.
15. Click **Launch**.
16. Select the existing key pair that the original AltaVault AMI was using and click **Launch Instances**.
17. When the new AltaVault AMI upgrade instance launches, note the new instance ID.
18. Click **View Instances**

Log in 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:

```
hostname> enable
hostname# configure terminal
```

2. Enter the following commands:

```
hostname (config)# username admin password 0 <password>
hostname (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.
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**.

Note: Import Configuration does not import the DNS settings when you use the option, *Import Shared Data Only.* You must reconfigure the DNS server settings using the *DNS Settings* section in the Settings > Networking > Host Settings page and rejoin the domain.

---

7. From the Web interface, select Configure > Host Settings to reconfigure the DNS server settings.

8. Select Configure > SMB to rejoin the domain.

   For more information on reconfiguring the DNS server settings and rejoining the domain, see "Modifying general host settings" in the *NetApp AltaVault Cloud Integrated Storage Administration Guide*.

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

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.

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 AMIs AVA-c4 and 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. Note that the device value can acquire any default value Amazon selects.

5. Confirm that all the volumes are attached.

Rebooting the new AltaVault AMI instance

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

1. SSH to the AltaVault command-line interface (CLI) and issue the following commands:

```
hostname> enable
hostname# configure terminal
hostname (config)# reload
```

2. After the reboot completes, SSH to the AltaVault command-line interface (CLI) again and issue the following commands:

```
hostname> enable
hostname# configure terminal
hostname (config)# no service enable
hostname (config)# megastore guid reset
hostname (config)# service enable
```

3. Connect to the Web user interface.

   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.

AltaVault Azure Virtual Machine Upgrades

The software upgrade procedure for AltaVault AVM is the same as for physical and virtual AltaVault appliances. Follow the software upgrade instructions in the section *Upgrading your software* in the *NetApp AltaVault Cloud Integrated Storage Administration Guide*.

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.

Copyright information

Trademark information

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

Index