AltaVault Cloud Integrated Storage 4.4.1

Installation and Service Guide for Cloud Appliances

March 2018 | 215-13006_A0
doccomments@netapp.com

NetApp®

Contents

Introduction to AltaVault cloud-based appliances

For organizations without a secondary disaster recovery location or for companies looking for extra protection with a low-cost tertiary site, cloud-based AltaVault appliances on Amazon Web Services (AWS) and Microsoft Azure are the key to enabling cloud-based recovery.

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.

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. Using 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 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. If the local AltaVault becomes unavailable, users 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 AVA-c4, AVA-c8, and AVA-c16 models. For Microsoft Azure Virtual Machine (AVM), AltaVault is available in the AVA-c4 model.

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

Installing an AltaVault Amazon Machine Image

Installing an AltaVault cloud-based instance is accomplished using an Amazon Machine Image (AMI) available through AWS Marketplace. It requires deploying the instance, setting up access to the appliance, and configuring a static IP address.

About this task

You must complete the following tasks in the order presented:

Steps

1. Accessing the AltaVault AMI on page 5
2. Deploying an AltaVault AMI instance using the 1-Click Launch method on page 6
3. Deploying an AltaVault AMI instance in Amazon EC2 using the Manual Launch method on page 6
4. Configuring access to the AltaVault cloud-based appliance using a web browser on page 7
5. Configuring access to the AltaVault cloud-based appliance using a native SSH client on page 7
6. Configuring a static IP address for an AltaVault AMI instance on page 8
7. Best practices for achieving optimal performance on page 9

Accessing the AltaVault AMI

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

Steps

1. Log in to the “Amazon Web Services” portal, and then browse to the Amazon Marketplace.

   Amazon Web Services (AWS) Marketplace

2. Search AWS Marketplace for AltaVault.

3. Select the NetApp AltaVault cloud-based appliance model that you want to use.

   You can choose AVA-c4, AVA-c8, or AVA-c16.

4. Click **Continue**.

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

6. Choose a launch method:

   - 1-Click Launch
     This is the preferred method for AVA-c4 and AVA-c8 models.

   - Manual Launch
     Select this launch method when the AVA-16c instance is used in conjunction with the backup application server instance. This method provides a 10 GbE infrastructure for communication with other EC2 instances.

Deploying an AltaVault AMI instance using the 1-Click Launch method

The 1-Click Launch is the preferred method for deploying AVA-c4 and AVA-c8 appliances. For AVA-c16 instances, you must use the Manual Launch method.

Steps

1. From the launch page, select **1-Click Launch**.
2. Select a region in which to create the AltaVault cloud-based appliance AMI instance.

   The default selection is US East (Virginia).
3. Select a security group for the AltaVault cloud-based appliance AMI instance.

   The security group describes which ports and IP addresses the AltaVault cloud-based appliance AMI instance uses to communicate with other VMs.
4. Select a Key Pair.

   This key pair provides the mechanism for communicating with the AltaVault AMI instance. The Amazon documentation contains instructions for creating a key pair.

   Amazon Web Services (AWS) Documentation: Amazon EC2 Key Pairs
5. Click **Accept Terms & Launch with 1-Click**.

   Amazon displays the software installation details.

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

The Manual Launch method is required to deploy AVA-c16. It sets up a 10 GbE infrastructure between an AVA-c16 instance and a backup application in the same AWS EC2 placement group.

Steps

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 **Launch with EC2 Console** selection automatically provides a 10 GbE interface. Be sure to choose a placement group while launching the AMI. The 10 GbE capabilities are only realized when the AMI and the backup server are in the same placement group.
3. Choose an Instance Type by scrolling to the Compute optimized section and selecting the `c4.8xlarge` instance type.
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 then click **Next: Configure Security Group**.
9. Choose a Security Group for the AltaVault.

   The security group describes which ports and IP addresses 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 then 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.

Configuring access to the AltaVault cloud-based appliance using a web browser

You can configure access to the AltaVault AMI instance using a web browser. Alternatively, you can access the cloud-based appliance using a native SSH client.

Steps

1. Select the instance name of the AltaVault AMI instance.
2. From the top menu, click **Connect**.
3. Select the **A Java SSH client directly from my browser (Java required)** radio button.
4. Enter the user name **admin**.
5. Begin the session by clicking **Launch SSH Client**.

Result

When the AltaVault connection is established for the first time, you are presented with the AltaVault CLI configuration wizard.

Configuring access to the AltaVault cloud-based appliance using a native SSH client

You can configure SSH access to the AltaVault AMI instance using either the built-in Linux SSH client or, in Windows environments, the PuTTY tool.

Before you begin

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

- SSH client (Linux or 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 that the permissions on the key pair file is set at `400`. You can change permissions using the `chmod 400` *`key-pair.pem`*command.

An SSH connection to the AltaVault AMI instance using PuTTY requires a configured key pair file in a format that is accepted by the PuTTY tool. The Amazon documentation contains details about converting the key pair file into a PuTTY friendly form.

Amazon Web Services (AWS) Documentation: Connecting to Your Linux Instance from Windows Using PuTTY

Choices

- Accessing 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 **A standalone SSH client** radio button.

     A command is displayed 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.
- Accessing your AltaVault AMI instance using Windows PuTTY
  1. If you use PuTTY, 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. You can set up an SSH connection using PuTTY.

     Amazon Web Services (AWS) Documentation: Connecting to Your Linux Instance from Windows Using PuTTY
  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* into the **Private key file for authentication** field.

Result

When the AltaVault connection is established for the first time, you are presented with the AltaVault CLI configuration wizard.

Configuring a static IP address for an AltaVault AMI instance

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. You can manually configure this as a static IP address after initially deploying the appliance using an Elastic IP address from AWS.

Steps

1. From the left menu of the EC2 Dashboard page, select **NETWORK & SECURITY > Elastic IPs**.
2. If an Elastic IP address is available, select it from the list, and then 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 then click **Associate**.

Best practices for achieving optimal performance

When deploying an AltaVault AMI instance, you should follow the best practices regarding security group, key pair, placement group, and network settings. Doing so helps to in delivering optimal performance from the appliance.

Best practices for deploying AMI instances

Security Group

For general disaster recovery purposes, it is recommended that you 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.

It is recommended that you place the AltaVault AMI instance in the same media group as the backup or media server virtual machines so that the virtual machines can communicate with the AltaVault AMI instance.

Key Pair

The key pair is used to authenticate the AltaVault AMI instance. Creating a key pair is a requirement before deploying an AltaVault AMI instance.

Placement Group

Both the AVA-c16 and the backup application instance should be in the same placement group to take advantage of using the 10 GbE infrastructure for communications.

MTU

It is recommended that you 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. The AWS documentation contains more information.

Amazon Web Services (AWS) Documentation: Network Maximum Transmission Unit (MTU) for Your EC2 Instance

Best practices for connecting an AMI instance to the network

Elastic IP address

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

Static IP address

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

Installing an AltaVault Microsoft AVM

Deploying an AltaVault Azure virtual machine (AVM) is provided through the Microsoft Azure portal. It requires installing and configuring the AVM instance, and providing an SSH connection.

About this task

You must complete the following tasks in the order presented:

Steps

1. Deploying an AltaVault AVM instance on page 10
2. Connecting to the AltaVault AVM on page 11

Deploying an AltaVault AVM instance

You can launch an AltaVault cloud-based appliance (AVA-c4 model only) from the Microsoft Azure portal using the AVM wizard.

Steps

1. Log in to the Microsoft Azure portal.

   Microsoft Azure Dashboard

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 of the AVM wizard, configure basic settings for the virtual machine, and then click **OK**.

Basic setting	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 “admin” user name.
Authentication type	Specify SSH Public key, the supported authentication type. **Note:** Only SSH public key is supported. The “password” authentication type is not supported.
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 the AltaVault.

Basic setting	Description
Location	Specify a location for the AltaVault virtual machine.

7. In Step 2 of the AVM wizard, select the virtual machine size by clicking **Select**.

   DS3 Standard is the only supported selection. The location where you deploy AltaVault AVM determines whether the DS3 Standard is available. The Microsoft Azure website has more information about locations.

   https://azure.microsoft.com/en-us/regions/services

8. In Step 3 of the AVM wizard, configure optional features, and then click **OK**.

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

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

10. In Step 5 of the AVM wizard, review the terms of the agreement, and then 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

You connect to the AltaVault Azure-based cloud appliance using the public IP address and the private SSH key.

Step

1. Power on the AVM and connect to it using SSH, using the public IP address and private SSH key:

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

   .

   When you start the AltaVault AVM for the first time, the initial boot process can take a few minutes. During this time, the system does not display any debugging message on the console, and might seem like it has stopped responding. Be patient, and do not hard power reset the appliance during the initial boot process. Doing so corrupts the file system on the cache disks and logs 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 boot process, you need to delete and then add the cache disk again, and wait until the system completes the boot process.

Result

When the AltaVault connection is established for the first time, you are presented with the AltaVault CLI configuration wizard.

AltaVault cloud-based appliance upgrades

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.

Follow the upgrade procedure for your cloud-based appliance instance type:

- *Upgrading AltaVault AMI instances* on page 13
- *Upgrading AltaVault AVM Instances* on page 18

Upgrading AltaVault AMI instances

Upgrading AltaVault AMI cloud-based appliance software includes actions on the AltaVault instance to save existing configuration information and on the AWS Marketplace portal to deploy new software and attach data volumes.

Before you begin

- All operations to and from AltaVault must be complete or suspended.
- You must have the administrative login credentials for the Amazon Web Services (AWS) console. The credentials 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.

About this task

You must complete the tasks in the order presented.

Steps

1. Saving and exporting the original AltaVault AMI configuration on page 13
2. Stopping the original AltaVault AMI instance and detaching the data volumes on page 14
3. Launching and configuring the new AltaVault AMI instance upgrade on page 14
4. Logging in to the AMI instance and setting the admin account password on page 15
5. Importing the configuration file on page 16
6. Attaching data volumes to the new upgrade instance on page 16
7. Rebooting the new AltaVault AMI instance on page 17

Saving and exporting the original AltaVault AMI configuration

Prior to upgrading your AltaVault AMI instance, you need to export your current configuration file from your existing AltaVault, `altavault_config_`*`HOSTNAME_DATETIME`*`.tgz`, and store it in a safe place.

Steps

1. Select **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 `AltaVault_config_`*`HOSTNAME_DATETIME`*`.tgz` configuration file .
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 instance 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.

Steps

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. From the **Volumes** selection, identify the volumes that are associated with the original AltaVault AMI instance.

   b. From the **Attachment information** field, locate the volumes associated with your appliance version. For versions prior to 4.3, locate two 100 GiB volumes that have the values `/dev/sda` and `/dev/sdk`, respectively. For version 4.3 and later, locate the 92 GiB volume with the value /dev/xvda.

   These volumes are not part of the upgrade. All other volumes are part of the upgrade.
6. Select all of the volumes attached to the original AltaVault AMI instance ID except for the volumes listed in the prior step.
7. Select **Actions > Detach Volumes**.
8. Save the private IP address and the VPC name of the original, older version of the AltaVault AMI appliance.
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.

Steps

1. Find the newer version of your AltaVault AMI model in the AWS Marketplace, and then click **Continue**.
2. Select the **Manual Launch** tab, and then 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. 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 enables the backup application to 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 then click **Next: Add Storage**.

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

   Note: Do not delete the `/dev/xvda` volume.

8. Click **Next: Tag Instance**.

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

10. Configure the security group:

    a. Select an existing security group radio button.

    b. Match the Security Group ID with the original AltaVault AMI.

11. Click **Review and Launch**.

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

13. Click **Next**.

14. Review your selections to make sure that all of the fields are correct.

15. Click **Launch**.

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

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

18. Click **View Instances**.

Logging in to the AMI instance and setting the admin account password

As part of the process for upgrading an AMI instance, you must configure the password for the AMI admin account.

Steps

1. Log in to the new AMI instance as admin using SSH with the key-pair that was used to launch the AMI.

2. Set a password for the AMI admin account.

   You can set the same password that was used in the older AMI.

3. Enter the following commands as shown in this screen:

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

4. Enter the following commands:

   ```
   hostname (config)# username admin password 0 password
   hostname (config)# write memory
   ```

Importing the configuration file

Use this procedure to import the older AMI configuration into the new AMI instance.

Steps

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 then click **Choose a File** to select a local configuration file from your computer.
4. Select the **Import Shared Data Only** check box so 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 **Import Shared Data Only** option. You must reconfigure the DNS server settings using the DNS Settings section in the **Settings > Networking > Host Settings** page, and then 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.

   > **Attention:** After this process is complete, 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 of the original AltaVault AMI data volumes (EBS volumes) to the newly created AltaVault AMI instance.

About this task

You must attach all original volumes to the new AltaVault instance.

> **Attention:** Failure to correctly attach all of the volumes results in the loss of the entire AltaVault AMI.

Steps

1. Go to the 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 eight volumes for the AltaVault AMIs AVA-c4 and AVA-c8. There should be a total of 16 volumes for the AltaVault AMI AVA-c16.
4. For each EBS volume added, verify that the correct AltaVault AMI instance name is selected.

   Note: The device value can acquire any default value Amazon selects.
5. Confirm that all of 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.

Steps

1. Use SSH to access the AltaVault command-line interface (CLI), and reboot the appliance.

   Example

   ```
   hostname> enable
   hostname# configure terminal
   hostname (config)# reload
   ```
2. After the reboot is complete, use SSH to access the AltaVault CLI again, and then stop Service Optimization, reset the metastore GUID, and restart Service Optimization.

   Example

   ```
   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.

After you finish

When the upgrade process is complete and operations have resumed using the new AltaVault AMI upgrade, you should 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 then select **Actions > Terminate**.

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

Upgrading AltaVault AVM Instances

Upgrading an AltaVault AVM instance requires downloading and installing the latest upgrade image from the NetApp Support Site.

Before you begin

All operations to and from AltaVault must be complete or suspended.

About this task

The software upgrade procedure for AltaVault AVM is the same as for physical and virtual AltaVault appliances and is described in the AltaVault administration documentation.

NetApp AltaVault Cloud Integrated Storage Administration Guide

Steps

1. Follow the procedure for upgrading AltaVault software in the *AltaVault Cloud Integrated Storage Administration Guide*.
2. When the upgrade process is complete and operations have resumed using the new AVM instance, select **Maintenance > Software Upgrade** and verify the booted version.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

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.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

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