NetBackup™ 11.2.0.1 Application Guide

For NetBackup Flex Appliance 8.0

COHESITY

NetBackup™ Application Guide

Last updated: 2026-10-19

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Product overview 7

Introduction to NetBackup applications for Flex Appliance 7
About the Flex Appliance documentation 8

Chapter 2 Release notes 9

NetBackup 11.2.0.1 application new features, enhancements, and changes 9
Supported upgrade paths to this release 9
Operational notes 9

Chapter 3 Geting started 11

Prerequisites before you can create NetBackup application instances 11
Installing the NetBackup client packages 11

Chapter 4 Creating NetBackup application instances 13

Creating application instances 13
Creating a NetBackup primary server instance 14
Creating a NetBackup media server instance 16
Creating a NetBackup WORM storage server instance 21

Chapter 5 Managing NetBackup application instances 27

Managing application instances from Flex Appliance and NetBackup 27
Accessing NetBackup primary and media server instances for management tasks 28
Managing users on a primary or a media server instance 28
Managing multifactor authentication on a primary or a media server instance 37
Running NetBackup commands on a primary or a media server application instance 40
Monitoring NetBackup services on a primary or a media server instance 44

Mounting an NFS share on a NetBackup primary server instance 45
Setting environment variables on primary and media server instances 46
Storing custom data on a primary or a media server instance 47
Modifying or disabling the nbdeployutil utility on a primary server instance 47
Disabling SMB server signing on a media server instance 48
Enabling extra OS STIG hardening on a primary or a media server instance 48
Using a login banner on a primary or a media server instance 49
Using a primary server instance for disaster recovery 50
Authorizing a primary or a media server instance for deletion 52
Accessing NetBackup WORM storage server instances for management tasks 52
Managing users from the deduplication shell 53
Managing multifactor authentication on a WORM storage server 58
Managing VLAN interfaces from the deduplication shell 60
Viewing the lockdown mode on a WORM storage server 61
Managing the retention policy on a WORM storage server 61
Managing images with a retention lock on a WORM storage server 62
Auditing WORM retention changes 63
Protecting the NetBackup catalog on a WORM storage server 64
Managing certificates from the deduplication shell 64
Managing FIPS mode from the deduplication shell 68
Managing post-quantum cryptography (PQC) mode from the deduplication shell 69
Encrypting backups from the deduplication shell 70
Configuring an isolated recovery environment using the web UI 71
Tuning the MSDP configuration from the deduplication shell 75
Setting the MSDP log level from the deduplication shell 78
Managing NetBackup services from the deduplication shell 79
Monitoring and troubleshooting NetBackup services from the deduplication shell 89
Managing S3 service from the deduplication shell 96
Authorizing a WORM storage server for deletion 98

Chapter 6 Creating and using a NextGen malware scanner instance 99

Creating a NextGen malware scanner instance 99
Malware scanning workflow for MSDP backup images using Flex application as the scan host 102
Authorizing a malware scanner instance for deletion 105

Chapter 1

Product overview

This chapter includes the following topics:

- Introduction to NetBackup applications for Flex Appliance
- About the Flex Appliance documentation

Introduction to NetBackup applications for Flex Appliance

Flex Appliance is a customizable data management solution that lets you consolidate multiple applications on a single hardware platform. An application is a software program that can be installed on Flex Appliance. You can use these applications to create multiple, concurrent application instances, or single deployments of applications that were historically standalone servers.

The following applications are available for NetBackup release 11.2.0.1:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.
  - AdvancedDisk
- NetBackup WORM storage server version 21.2.0.1
  The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 21.2.0.1 requires a version 11.2.0.1 primary server and media server.

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Support website:

Flex Appliance supported applications and usage information

About the Flex Appliance documentation

The following documents contain information about the Flex Appliance and application software:

- The *NetBackup Flex Appliance Getting Started and Administration Guide*
  Refer to this guide to configure and manage the Flex Appliance software, as well as for general information about creating and managing application instances.
- The *NetBackup Application Guides*
  Refer to these guides for more specific information about the NetBackup applications, including detailed instructions on how to create application instances of each supported version.

The following documents contain information about the appliance hardware:

- The *Hardware Installation Guide* for your particular model
- The *Product Description* for your particular model
- The *Appliance Safety and Maintenance Guide*

Flex Appliance also uses AutoSupport to monitor the appliance. You can find additional information about AutoSupport in the *Appliance AutoSupport Reference Guide*.

You can find the latest documentation on the Cohesity Documentation page. Select the release version and platform in the drop-down.

API documentation is also available from the **Knowledge Base** page on SORT.

Chapter 2

Release notes

This chapter includes the following topics:

- NetBackup 11.2.0.1 application new features, enhancements, and changes
- Supported upgrade paths to this release
- Operational notes

NetBackup 11.2.0.1 application new features, enhancements, and changes

This release does not include any new features, enhancements, or changes that are specific to the NetBackup 11.2.0.1 application. It does include the new features from NetBackup unless they are called out as exceptions in this guide or the NetBackup documentation. See the *NetBackup Release Notes* for more information.

Supported upgrade paths to this release

You can upgrade directly from any previous NetBackup application version to version 11.2.0.1.

Operational notes

This topic explains important aspects of the NetBackup 11.2.0.1 application that may not be documented elsewhere in the documentation.

The following list contains the notes and the known issues that apply for this release:

- Upgrades to this release from versions 10.1.1 and earlier require SQL Anywhere binaries to perform database migration from SQL Anywhere to PostgreSQL. You must install an EEB to make the SQL Anywhere binaries available to the

NetBackup instance during upgrade. The EEB is available at the following location:

https://support.cohesity.com/s/

Chapter 3

Geting started

This chapter includes the following topics:

- Prerequisites before you can create NetBackup application instances
- Installing the NetBackup client packages

Prerequisites before you can create NetBackup application instances

Before you begin working with NetBackup application instances, make sure that you have fully reviewed the *NetBackup Flex Appliance Getting Started and Administration Guide* and have performed all of the following tasks:

- Completed the initial configuration
- Verified that you can access the Flex Appliance Console
- Configured at least one network interface
- Added at least one tenant
- Added the application that you want to use to the repository

You also need access to the NetBackup web UI and the NetBackup client software. See "Installing the NetBackup client packages" on page 11.

Installing the NetBackup client packages

To create and manage NetBackup instances, you need access to the NetBackup client software so that you can install it on the computers that you want to back up.

The NetBackup client packages are included with the Electronic Software Distribution (ESD) images for NetBackup product installation. You can download the NetBackup ESD images from the **Downloads** page on the Support website.

For more information about installing the client software, refer to the *NetBackup Installation Guide*, which is accessible from the NetBackup page on the Support website.

Chapter 4

Creating NetBackup application instances

This chapter includes the following topics:

- Creating application instances

Creating application instances

You can create application instances from the **System topology** page of the Flex Appliance Console. Navigate to the **Application instances** section and click **Create instance** to open a new page that lets you create instances of the following applications for NetBackup release 11.2.0.1:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.
  - AdvancedDisk
- NetBackup WORM storage server version 21.2.0.1
  The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 21.2.0.1 requires a version 11.2.0.1 primary server and media server.

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Support website:

Flex Appliance supported applications and usage information

When you create a NetBackup instance, you need to complete additional configuration steps from within NetBackup. Use the following procedures as a guide and refer to the NetBackup documentation for additional details.

See "Creating a NetBackup primary server instance" on page 14.

See "Creating a NetBackup media server instance" on page 16.

See "Creating a NetBackup WORM storage server instance" on page 21.

Creating a NetBackup primary server instance

Use the following procedure to create a NetBackup primary server instance on Flex Appliance.

To create a NetBackup primary server instance

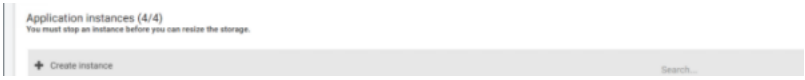
1. Make sure that the NetBackup primary server application you want to use is located in the repository on the Flex Appliance Console.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
3. Gather the following information for the new instance:

   Note: The hostname and IP address must not be in use anywhere else in your domain.

   - Tenant that you want to assign it to
   - Hostname (maximum of 63 characters including the domain name)
   - IP address
   - Network interface
   - Domain name
   - Name servers
   - Search domains

- Administrator password for the `appadmin` account (minimum 8 characters, re-entered for confirmation)

4 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.



5 Click **Create instance**.

6 Select the appropriate primary server application from the repository list that appears, making sure to verify the version number. Click **Next**.

7 Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the media servers and any other NetBackup hosts that you want to communicate with the instance.

---

8 Once the instance has been created, open an SSH session to the instance and log in as `appadmin` using the password that you set in the **Create Instance** wizard. No default password ships with the image, and no password change is required on first login.

9 (Optional) If you want to use an external Certificate Authority (CA), see the topic "Configuring the primary server to use an external CA-signed certificate" in the *NetBackup Security and Encryption Guide*.

Note: Do not configure AdvancedDisk storage on a NetBackup primary server instance. NetBackup lets you create an AdvancedDisk storage server on a primary server instance, but Flex Appliance does not support storage configuration on primary server instances. Create a separate NetBackup media server instance if you want to use AdvancedDisk storage.

See “Managing application instances from Flex Appliance and NetBackup” on page 27.

Creating a NetBackup media server instance

Use the following procedure to create a NetBackup media server instance on Flex Appliance.

To create a NetBackup media server instance

1. Make sure that the NetBackup media server application you want to use is located in the repository on the Flex Appliance Console.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
3. Gather the following information for the new instance:

   Note: The hostname and IP address must not be in use anywhere else in your domain.

   - Tenant that you want to assign it to
   - Hostname (maximum of 63 characters including the domain name)
   - IP address
   - Network interface
   - Domain name
   - Name servers
   - Search domains
   - Primary server hostname

     Note: The Flex Appliance Console does not prevent entering the same hostname in both the **Hostname for NetBackup Media Server** and the **Primary server hostname** fields, but that configuration is not supported. You must have a preexisting primary server with a different hostname.

   - Certificate Authority (CA) information for one of the following:

     For a NetBackup CA:

     - CA SHA-1 or SHA-256 certificate fingerprint
       If the primary server is a Flex instance, you can locate this information from the instance details page of the primary server instance. Click on

the instance name under **Application instances** on the **System topology** page.

If the primary server is not a Flex instance, see the *NetBackup Security and Encryption Guide* for the steps to locate this information from NetBackup.

- (Optional) Token for host ID-based certificate

  Depending on the primary server security level, the host may require an authorization or a reissue token. If you do not specify a token when you create the instance, the wizard attempts to automatically obtain the certificate.

For an external CA:

- Trust store, in PEM format
- Host certificate, in PEM format
- Private key, in PEM format
- (Optional) Passphrase of the private key

  A passphrase is required if the key is encrypted.
- (Optional) Custom CRL files

- (Optional) Password for host name-based certificate

  A host name-based certificate is mandatory if Enhanced Auditing is enabled on the primary server. You can specify the password when you create the instance, or you can deploy the certificate from the primary server later.
- Administrator password for the `appadmin` account (minimum 8 characters, re-entered for confirmation)

4 Add the hostname for the new instance to the **Media servers** list or the **Additional servers** list on the primary server, as follows:

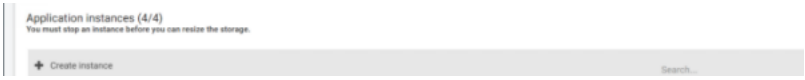
- Sign in to the NetBackup web UI. On the left, click **Hosts** > **Host properties**.
- Select **Primary server** from the list.
- If necessary, click **Connect**.
- Click **Edit primary server**.
- Click one of the following:
  - If you want MSDP storage on the instance, click **Servers**. Then click the **Additional servers** tab.
  - If you want AdvancedDisk storage on the instance, click **Servers**. Then click the **Media servers** tab.

- Click **Add** and enter the host name for the new instance. The host name should appear in the list.
- Click **Save**.

5 If a firewall exists between the primary server and the new instance, open the following ports on the primary server to allow communication:

- `vnetd: 13724`
- `bprd: 13720`
- `PBX: 1556`
- If the primary server is a NetBackup appliance that uses TCP, open the following ports:
  443, 5900, and 7578.

6 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.



7 Click **Create instance**.

8 Select the appropriate media server application from the repository list that appears, making sure to verify the version number. Click **Next**.

9 Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the primary server and any other NetBackup hosts that you want to communicate with the instance.

---

10 Once the instance has been created, open an SSH session to the instance and log in as `appadmin` using the password that you set in the Create Instance wizard. No default password ships with the image, and no password change is required on first login.

11 Create the storage servers for your selected storage, as follows:

- Sign in to the NetBackup web UI. On the left, click **Storage** > **Disk storage**. Navigate to the **Storage servers** tab and then click **Add**.
- In the **Storage type** list, select **Disk storage servers**.
- From the **Category** options, select **AdvancedDisk** or **Media Server Deduplication Pool (MSDP, MSDP Cloud)** and follow the prompts to create the storage servers. Enter the following storage information for AdvancedDisk and MSDP:
  - AdvancedDisk storage volume: `/mnt/advanceddisk/vol*`
  - MSDP storage path: `/mnt/msdp/vol0`

  Note: If the MSDP disk pool spans multiple volumes, only select vol0. Also note that the wizard shows only a portion of the storage, but the remaining storage displays after the storage server is configured.

See the following guides for more information on NetBackup storage configuration:

- The *NetBackup AdvancedDisk Storage Solutions Guide*
- The *NetBackup Deduplication Guide*

12 (Optional) If you need to upload custom CRL files for an external CA, perform the following steps:

- Run the following command on the instance to create a directory for the files:

  ```
  sudo mkdir -p /mnt/nbdata/hostcert/crl/
  ```

- Use an SCP tool to copy the files to the new `/mnt/nbdata/hostcert/crl/` directory.
- Run the following commands on the instance to enable the CRL check using the custom files:

  ```
  sudo nbsetconfig ECA_CRL_CHECK = CHAIN
  sudo nbsetconfig ECA_CRL_PATH = /mnt/nbdata/hostcert/crl/
  ```

See the *NetBackup Security and Encryption Guide* for more information on the CRL configuration options.

13 If you plan to create or already have multiple instances with deduplication storage, you must adjust the deduplication cache sizes so that the total memory of all instances does not exceed 75% of the physical RAM on the appliance.

The default cache sizes are as follows:

- `MaxCacheSize`: 50%
- `MaxPredictiveCacheSize`: 20%
- `MaxSamplingCacheSize`: 5%

To tune the cache sizes on this instance:

- Run the following command to tune the `MaxCacheSize`:

  ```
  sudo /usr/openv/pdde/pdag/bin/pdcfg --write
  /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section CACHE
  --option MaxCacheSize --value <percent>%
  ```

  Where <*percent*> is the percentage of the appliance RAM to use for the cache on the instance.

- Run the following command to tune the `MaxPredictiveCacheSize`:

  ```
  sudo /usr/openv/pdde/pdag/bin/pdcfg --write
  /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section Cache
  --option MaxCacheSize --value <percent>%
  ```

  Where <*percent*> is the percentage of the appliance RAM to use for the predictive cache.

- Run the following command to tune the `MaxSamplingCacheSize`:

  ```
  sudo /usr/openv/pdde/pdag/bin/pdcfg --write
  /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section Cache
  --option MaxSamplingCacheSize --value <percent>%
  ```

  Where <*percent*> is the percentage of the appliance RAM to use for the sampling cache.

- Restart the `pdde-storage` process with the following commands:

  ```
  sudo /etc/init.d/pdde-storage force-stop
  sudo /etc/init.d/pdde-storage start
  ```

14 If you selected MSDP storage for the instance, log in to the instance. Run the following command to create a backup policy to protect the MSDP catalog:

```
sudo /usr/openv/pdde/pdcr/bin/drcontrol --new_policy --residence
<storage unit> [--policy <policy name>] [--client<instance
hostname>]
```

Where *<storage unit>* is the name of the storage unit on which to store the MSDP catalog backups, and [--policy *<policy name>*] and [--client *<instance hostname>*] are optional.

See the *NetBackup Deduplication Guide* for the other options that are available with the `drcontrol` utility.

15 (5250 appliances only) If you selected MSDP storage for the instance, use the following procedure to tune the MSDP parameters. Tuning the parameters increases backup and restore performance on the 5250 hardware.

To tune the parameters on a 5250 appliance:

- Log in to the instance as the **appadmin** user and run the following commands:
  - `sudo /usr/openv/pdde/pdag/bin/pdcfg --write /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section CRDataStore --option MaxFileSize --value 256Mib`
  - `sudo /usr/openv/pdde/pdag/bin/pdcfg --write /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section CRDataStore --option WriteBufferSize --value 65536`
- From the `home` or `tmp` directory, restart the `pdde-storage` and `mtstrmd` processes with the following commands:
  - `sudo /etc/init.d/pdde-storage force-stop`
  - `sudo /etc/init.d/pdde-storage start`

See "Managing application instances from Flex Appliance and NetBackup" on page 27.

Creating a NetBackup WORM storage server instance

NetBackup WORM (Write Once Read Many) storage server instances prevent your data from being encrypted, modified, or deleted. Any data that is saved on these instances is protected with the following security measures:

- Immutability
  This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.

- Indelibility
  This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

See the *NetBackup Administrator's Guide, Volume I* for more information about WORM storage.

Use the following procedure to create a NetBackup WORM storage server instance on Flex Appliance.

Note: Your appliance must be in lockdown mode before you can create a WORM storage instance.

See the topic "Changing the lockdown mode" in the *NetBackup Flex Appliance Getting Started and Administration Guide* for the steps to enable lockdown mode.

To create a NetBackup WORM storage server instance

1. Make sure that the NetBackup WORM storage server application you want to use is located in the repository.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
   - Verify that the appliance is in lockdown mode. You can check or change the lockdown mode from the **Lockdown mode** page on the Flex Appliance Console. See the topic "Changing the lockdown mode" in the *NetBackup Flex Appliance Getting Started and Administration Guide* for details.
3. Gather the following information for the new instance:

   Note: The hostname and IP address must not be in use anywhere else in your domain.

   - Tenant that you want to assign it to
   - Hostname (maximum of 63 characters including the domain name)
   - IP address
   - Network interface
   - Domain name
   - Name servers

- Search domains
- Primary server hostname (must be version 8.3.0.1 or later)
- Media server hostname if applicable (must be version 8.3.0.1 or later)
- Username for storage
  NetBackup requires this username to connect to the deduplication storage. The username must be between 4 and 30 characters and can include uppercase letters, lowercase letters, and numbers.
- Password for storage
  NetBackup requires this password to connect to the deduplication storage. The password must be between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~={}?!).
- KMS key group
- KMS passphrase
- Certificate Authority (CA) information for one of the following:

  For a NetBackup CA:

  - CA SHA-1 or SHA-256 certificate fingerprint
    If the primary server is a Flex instance, you can locate this information from the instance details page of the primary server instance. Click on the instance name under **Application instances** on the **System topology** page.
    If the primary server is not a Flex instance, see the *NetBackup Security and Encryption Guide* for the steps to locate this information from NetBackup.
  - (Optional) Token for host ID-based certificate
    Depending on the primary server security level, the host may require an authorization or a reissue token. If you do not specify a token when you create the instance, the wizard attempts to automatically obtain the certificate.

  For an external CA:

  - Trust store, in PEM format
  - Host certificate, in PEM format
  - Private key, in PEM format
  - (Optional) Passphrase of the private key
    A passphrase is required if the key is encrypted.
- (Optional) Password for host name-based certificate

A host name-based certificate is mandatory if Enhanced Auditing is enabled on the primary server. You can specify the password when you create the instance, or you can deploy the certificate from the primary server later.

- Administrator password for the `msdpadm` account

  Password must be between 15 and 32 characters and must include at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9), and one special character (_.+~@={}?!).

4 On the primary server, use the `nbsetconfig` command or manually edit the NetBackup backup configuration file (`bp.conf` on Linux and UNIX, or the Windows registry) to add the following entry:

```
MSDP_SERVER=<MSDP hostname>
```

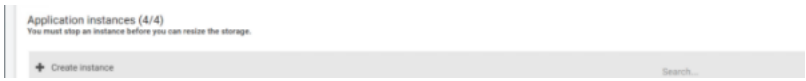
Where *<MSDP hostname>* is the hostname of the new WORM storage server instance.

5 If a firewall exists between the primary server and the new instance, open the following ports on the primary server to allow communication:

- `vnetd: 13724`
- `bprd: 13720`
- `PBX: 1556`
- If the primary server is a NetBackup appliance that uses TCP, open the following ports:

  443, 5900, and 7578.

6 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.



7 Click **Create instance**.

8 Select the appropriate storage server application from the repository list that appears, making sure to verify the version number. Click **Next**.

9 Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the primary server and any other NetBackup hosts that you want to communicate with the instance.

---

10 Once the instance has been created, open an SSH session to the instance and log in as `msdpadm` using the password that you set in the Create Instance wizard. No default password ships with the image, and no password change is required on first login.

11 If you plan to create or already have multiple instances with deduplication storage, you must adjust the deduplication cache sizes so that the total memory of all instances does not exceed 75% of the physical RAM on the appliance.

The default cache sizes are as follows:

- `MaxCacheSize`: 512 MiB
- `MaxPredictiveCacheSize`: 40%
- `MaxSamplingCacheSize`: 20%

To tune the cache sizes on this instance:

- Run the following command to tune the `MaxCacheSize`:

  `setting set-MSDP-param max-cache-size value=<value>`

  Where <*value*> is the amount of the appliance RAM to use for the cache on the instance, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.

- Run the following command to tune the `MaxPredictiveCacheSize`:

  `setting set-MSDP-param max-predictive-cache-size value=<value>`

  Where <*value*> is the amount of the appliance RAM to use for the predictive cache, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.

- Run the following command to tune the `MaxSamplingCacheSize`:

  `setting set-MSDP-param max-sampling-cache-size value=<value>`

  Where <*value*> is the amount of the appliance RAM to use for the sampling cache, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.

- Restart the `pdde-storage` process with the following commands:

  ```
  sudo /etc/init.d/pdde-storage force-stop
  sudo /etc/init.d/pdde-storage start
  ```

12 The appliance automatically creates a **PureDisk** storage server for the WORM storage instance that has the same name as the instance. Use the following steps to create a disk pool on that storage server:

From the NetBackup web UI, click **Storage**, click the **Disk pools** tab, and then click **Add**. Follow the prompts to configure the disk pool.

13 Use the following steps to create a deduplication storage unit for your instance:

From the NetBackup web UI, click **Storage**, navigate to the **Storage Units** tab, and then click **Add**. Follow the prompts and make sure that the **Enable WORM** option is activated.

You are ready to create a backup policy and start using your WORM storage instance. See the NetBackup documentation for more information.

See "Managing application instances from Flex Appliance and NetBackup" on page 27.

Chapter 5

Managing NetBackup application instances

This chapter includes the following topics:

- Managing application instances from Flex Appliance and NetBackup
- Accessing NetBackup primary and media server instances for management tasks
- Accessing NetBackup WORM storage server instances for management tasks

Managing application instances from Flex Appliance and NetBackup

After you have created your instances, the instance management is divided between Flex Appliance and NetBackup, depending on the type of operation. In general, use Flex Appliance for any tasks that are related to the appliance or the application files. Use NetBackup for any tasks that are related to your backups. Refer to the following information for more details.

Instance operations that you can perform from Flex Appliance

Use Flex Appliance to do the following:

- Resize instance storage
- Edit instance network settings
- Assign or unassign Fibre Channel ports
- View instance performance metrics
- Upgrade application instances

- Manage application add-ons, including NetBackup EEBs
- Delete application instances
- Clear a configuration error status
- Manage remote replication
- Setting resource limits
- Network Access Control settings for the instance
- Configuring IPsec for application instances

Refer to the *Flex Appliance Getting Started and Administration Guide* for these procedures.

Instance operations that you can perform from NetBackup

Other management tasks happen from NetBackup. This guide covers the information that is specific to the NetBackup application. For all other tasks, refer to the regular NetBackup documentation as you would for any other environment.

Accessing NetBackup primary and media server instances for management tasks

To perform some management tasks on a primary or a media server instance, you must open an SSH session to the instance.

When you log in to the instance for the first time, use the `appadmin` account with the administrator password that was set during instance creation in the Create Instance wizard. There is no default password, and no password change is required on first login.

From the SSH session, you can run commands to manage the instance. Some commands are specific to the NetBackup application, but you can also run NetBackup commands. To run NetBackup commands, specify `sudo` and enter the absolute or the relative path. See "Running NetBackup commands on a primary or a media server application instance" on page 40.

Managing users on a primary or a media server instance

After you create a NetBackup primary or media server application instance, you can log in to the instance with the **appadmin** user account to add and manage additional users.

The following types of users are supported:

- Local users

See "Adding and removing local users on a primary or a media server instance" on page 29.
See "Changing a user password on a primary or a media server instance" on page 35.

- Active Directory (AD) users
  See "Connecting an Active Directory user domain to a primary or a media server instance" on page 30.
- Lightweight Directory Access Protocol (LDAP) users
  See "Connecting an LDAP user domain to a primary or a media server instance" on page 32.

Adding and removing local users on a primary or a media server instance

Use the following procedures to add or remove local users on a NetBackup primary or media server instance.

Adding local users

To add a local user

1. Open an SSH session to the instance as the **appadmin** user.
2. Run the following command:

   ```
   sudo useradd <username>
   ```

   Where *<username>* is the username of the user that you want to add.

   Note: The username **maintenance** is not supported on application instances.

3. Run the following command to set a password for the new user:

   ```
   sudo passwd <username>
   ```

   Where *<username>* is the username that you added in the previous step.

Removing local users

To remove a local user

1. Open an SSH session to the instance as the **appadmin** user.
2. Run the following command:

   ```
   sudo userdel <username>
   ```

   Where *<username>* is the username of the user that you want to remove.

Connecting an Active Directory user domain to a primary or a media server instance

Use the following procedure to connect an Active Directory (AD) user domain to a primary or a media server instance.

To connect an AD user domain

1. From the Flex Appliance Console, verify that the instance is on the same network as the AD domain. If it is not, edit the settings so that the instance can reach the domain.
2. Open the following ports between the instance and the remote host if they are not already open:
   - 139
   - 445
3. Open an SSH session to the instance as the **appadmin** user and run the following command:

   ```
   sudo realm join <domain name> -v -U <domain administrator>
   ```

   Where *<domain name>* is the domain that you want to connect, and *<domain administrator>* is the username of an administrator user on that domain.

   Enter the **appadmin** user password when prompted.
4. When the following prompts appear, enter the password for the domain administrator user:

   ```
   Password for Administrator:
   ```

   ```
   Enter Administrator's password:
   ```
5. Wait for the process to complete. The following message should appear:

   ```
   Successfully enrolled machine in realm
   ```

   Run the following command to confirm:

   ```
   sudo realm list
   ```
6. If you need to add user groups from this domain in the NetBackup web UI, you must modify the `sssd.conf` file before you can add the groups. If you do not need to add user groups and plan to add each user individually, do not perform this step.

   To modify the `sssd.conf` file:

   - Navigate to `/etc/sssd/sssd.conf` on the instance and locate the following section:

```
[domain/<domain name>]
```

- Add the following directive to this section:

```
enumerate = True
```

Note: If you have a large AD environment, you may need to perform additional tuning of the `sssd.conf` file. Refer to the Red Hat documentation or contact Technical Support.

---

7 By default, all users on the remote user domain can log in to the instance. If you need to restrict access to specific users or groups, perform the following steps:

- Navigate to `/etc/sssd/sssd.conf` on the instance and verify that the file includes the following line:

  ```
  access_provider = ad
  ```

  If it does not, add it.

- Add the following filter to the file:

  ```
  ad_access_filter = <user list>
  ```

  Where *<user list>* is the list of users that you want to have access, in one of the following formats:

  - To add user groups, replace *<user list>* with the following:

    ```
    (memberOf=cn=<common name>,ou=<organizational
    unit>,dc=<domain component>)
    ```

    Where everything after `memberOf=` specifies the group that you want to provide access to.

    There may be more than one `ou` or `dc`, and you can also add multiple groups to the filter. For example:

    ```
    ad_access_filter =
    (|(memberOf=cn=users1,ou=groups,dc=example,dc=company,dc=com)
    (memberOf=cn=users2,ou=admins,ou=groups,dc=example,dc=company,dc=com))
    ```

  - To add users, replace *<user list>* with the following:

    ```
    (sAMAccountName=<username>)
    ```

    You can also add multiple users. For example:

    ```
    ad_access_filter = (|(sAMAccountName=user1)
    (sAMAccountName=user2))
    ```

  For more information on the AD access filter, refer to the Red Hat documentation.

- Run the following command:

  ```
  systemctl restart sssd
  ```

8. By default, AD users have super administrator privileges and full access to the instance. To remove those privileges and designate the **appadmin** user as the only super administrator, perform the following steps:

   - Navigate to `/etc/ssh/sshd_config` and add the following line to the end of the file:

     ```
     AllowUsers appadmin
     ```

   - Run the following command:

     ```
     systemctl restart sshd
     ```

9. When the connection is complete, sign in to the instance as the **appadmin** user from the NetBackup web UI. Add and configure the remote users that you want to have access to the instance from the web UI. See the *NetBackup Web UI Administrator's Guide* for details.

Note: The username **maintenance** is not supported on application instances.

Connecting an LDAP user domain to a primary or a media server instance

Use the following procedure to connect an LDAP user domain to a primary or a media server instance.

To connect an LDAP user domain

1. From the Flex Appliance Console, verify that the instance is on the same network as the LDAP domain. If it is not, edit the settings so that the instance can reach the domain.

2. Open the following port between the instance and the remote host if it is not already open:

   - If you want to enable SSL for the connection: port 389
   - If you do not want to enable SSL for the connection: port 636

3. Open an SSH session to the instance as the **appadmin** user and run the following command to navigate to the SSSD configuration file:

   ```
   sudo vi /etc/sssd/sssd.conf.
   ```

4. Run the following command to copy the file and create a backup:

   ```
   sudo cp /etc/sssd/sssd.conf /mnt/nbdata/sssd.conf.orig
   ```

5 In the `sssd.conf` file, locate and modify the following entries:

- `ldap_uri =`
  Enter the LDAP server name and port. If you want to enable SSL for the connection, use port 636. If you do not want to enable SSL, use port 389.
  For example: `ldap_uri = ldaps://example.cohesity.com:636`
- `ldap_search_base =`
  Enter the LDAP search domain.
  For example: `ldap_search_base = dc=example,dc=cohesity,dc=com`
- `ldap_tls_reqcert =`
  If you want to enable SSL for the connection, enter `hard`.
  If you do not want to enable SSL for the connection, enter `never`.
  For example: `ldap_tls_reqcert = hard`

Note: Other fields may also need to be modified depending on your LDAP configuration. Check the LDAP vendor documentation and follow those instructions if there are any differences.

---

6 If you did not enable SSL, proceed to the next step.

If you enabled SSL, perform the following additional steps:

- Add the following lines to the `sssd.conf` file:
  - `ldap_tls_cacertdir = /mnt/nbdata/sssd/certs`
  - `ldap_tls_cacert = /mnt/nbdata/sssd/certs/<CA certificate>`
    Where <*CA certificate*> is the file name of the LDAP CA certificate.
- Run the following command to create a directory for the LDAP certificates:
  `sudo mkdir -p /mnt/nbdata/sssd/certs`
- Copy all LDAP certificate files to this directory.
- Run the following command to navigate to the LDAP configuration file:
  `sudo vi /etc/openldap/ldap.conf`
- Add the following entry to this file:
  `TLS_CACERTDIR /mnt/nbdata/sssd/certs`

7 By default, all users on the remote user domain can log in to the instance. If you need to restrict access to specific users or groups, perform the following steps:

- Navigate to `/etc/sssd/sssd.conf` on the instance and verify that the file includes the following line:

```
access_provider = ldap
```

If it does not, add it.

- Add the following filter to the file:

  ```
  ldap_access_filter = <user list>
  ```

  Where *<user list>* is the list of users that you want to have access, in one of the following formats:

  - To add user groups, replace *<user list>* with the following:

    ```
    (memberOf=cn=<common name>,ou=<organizational
    unit>,dc=<domain component>)
    ```

    Where everything after `memberOf=` specifies the group that you want to provide access to.

    There may be more than one `ou` or `dc`, and you can also add multiple groups to the filter. For example:

    ```
    ldap_access_filter =
    (|(memberOf=cn=users1,ou=groups,dc=example,dc=company,dc=com)
    (memberOf=cn=users2,ou=admins,ou=groups,dc=example,dc=company,dc=com))
    ```

  - To add users, replace *<user list>* with the following:

    ```
    (sAMAccountName=<username>)
    ```

    You can also add multiple users. For example:

    ```
    ldap_access_filter = (|(sAMAccountName=user1)
    (sAMAccountName=user2))
    ```

  For more information on the LDAP access filter, refer to the Red Hat documentation.

- Run the following command:

  ```
  systemctl restart sssd
  ```

8 By default, LDAP users have super administrator privileges and full access to the instance. To remove those privileges and designate the **appadmin** user as the only super administrator, perform the following steps:

- Navigate to `/etc/ssh/sshd_config` and add the following line to the end of the file:

  ```
  AllowUsers appadmin
  ```

- Run the following command:

```
systemctl restart sshd
```

9 When the connection is complete, sign in to the instance as the **appadmin** user from the NetBackup web UI. Add and configure the remote users that you want to have access to the instance from the web UI. See the *NetBackup Web UI Administrator's Guide* for details.

Note: The username **maintenance** is not supported on application instances.

Changing a user password on a primary or a media server instance

Follow these steps to change the password of a local user or the default **appadmin** user on a NetBackup primary or media server application instance.

Note: Remote directory user passwords cannot be changed from an instance. They must be changed from the server on which they reside.

To change a user password from that user's account

1 Open an SSH session to the instance as the user that you want to change the password for and run the following command:

```
passwd
```

2 Follow the prompt to change the password.

To change another user's password from the appadmin account

1 Open an SSH session to the instance as the **appadmin** user and run the following command:

```
sudo passwd <username>
```

Where *<username>* is the username of the user whose password you want to change.

2 Follow the prompt to change the password.

Using SSH keys for authentication on a primary or a media server instance

You can configure a primary or a media server application instance to allow users to log in with SSH keys instead of passwords. You must already have a public and private key pair for each user. You can generate the keys with the `ssh-keygen` utility. For FIPS compliance, only RSA and ECDSA keys are supported at this time.

The user who wants to log in with SSH keys must work together with the **appadmin** user to configure authentication.

Steps for the appadmin user

The **appadmin** user must create an `sshkeys` directory for the other user. Use the following steps.

To create an `sshkeys` directory

1. Open an SSH session to the instance as the **appadmin** user.
2. Run the following command to create the new directory:

   ```
   sudo mkdir -p /var/sshkeys/<user>
   ```

   Where *<user>* is the username of the user to provide access to.
3. Run the following command to change the ownership of the directory to the other user:

   ```
   sudo chown <user> /var/sshkeys/<user>
   ```
4. Run the following command and check the output:

   ```
   sudo grep AuthenticationMethods /etc/ssh/sshd_config
   ```

   Then do one of the following:

   - If the output does not have any entries, or if any entries begin with a #, no action is required.
   - If `publickey` is present in the list before `keyboard-interactive`, no action is required.
   - If `publickey` is not present, run the following command to add `publickey` before `keyboard-interactive`:

     ```
     sudo sed -i 's/AuthenticationMethods/AuthenticationMethods
     publickey/' /etc/ssh/sshd_config
     ```

     Then run the following command:

     ```
     sudo systemctl restart sshd
     ```

Steps for the user who wants to log in with SSH keys

The other user must copy their public SSH key to the instance. Use the following steps.

To copy the key to the instance

1. From the host that you want to connect from, run the following command:

   ```
   ssh-copy-id <user>@<instance>
   ```

   Where *<user>* is your username, and *<instance>* is the hostname or the IP address of the instance.

2. Open an SSH session to the instance and log in with your username and password.

3. Run the following command:

   ```
   mv ~/.ssh/authorized_keys /var/sshkeys/<user>
   ```

4. Log out of the instance. You should now be able to log back in without a password.

Managing multifactor authentication on a primary or a media server instance

NetBackup primary and media server application instances support multifactor authentication for local, Active Directory (AD), and LDAP users. Multifactor authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication individually, or the **appadmin** user can enforce multifactor authentication for all users.

See "Configuring or disabling multifactor authentication on a primary server instance" on page 37.

See "Configuring or disabling multifactor authentication on a media server instance" on page 38.

See "Enforcing multifactor authentication on a primary or a media server instance" on page 39.

See "Resetting multifactor authentication on a primary or a media server instance" on page 39.

Configuring or disabling multifactor authentication on a primary server instance

For NetBackup primary server application instances, you can configure or disable multifactor authentication through the NetBackup web UI the same way that you would for any other primary server. Once you configure multifactor authentication, it is required for both the NetBackup web UI and for SSH access to the instance.

See the *NetBackup Web UI Administrator's Guide* for the steps to configure or disable multifactor authentication on a primary server instance.

Configuring or disabling multifactor authentication on a media server instance

Use the following procedures to configure or disable multifactor authentication on a NetBackup media server application instance.

Note: If multifactor authentication is enforced, users cannot disable it after the grace period.

To configure multifactor authentication on a media server instance

1. (Optional) If you have already configured multifactor authentication for another instance and want to use the same authenticator account to log in to this instance, run the following command on the other instance:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -show
   ```

   Take note of the key.

2. On the instance that you need to configure multifactor authentication for, run one of the following commands:

   - To enroll with a random key, run the following command:

     ```
     /usr/openv/netbackup/bin/goodies/nbmfacfg -enroll
     ```

   - To use an existing key, run the following command:

     ```
     /usr/openv/netbackup/bin/goodies/nbmfacfg -enroll -secret
     <existing key>
     ```

3. If you generated a new key, scan the QR code with an authentication app on your mobile phone. For example, Google Authenticator or Microsoft Authenticator.

   Note that the token validation is based on the server time. Ensure that the clock of the Flex Appliance and the mobile phone are correct.

   Note: If the **appadmin** user becomes locked, they cannot reset multifactor authentication for themself. To avoid this situation, Cohesity recommends that two or multiple users scan the same QR code of the **appadmin** user with their mobile phones. If one user loses access to the token, another user can help them to enroll again.

To disable multifactor authentication on a media server instance

1. Log in to the instance as the user that you want to disable multifactor authentication for.
2. Run the following command:

```
/usr/openv/netbackup/bin/goodies/nbmfacfg -reset
```

Enforcing multifactor authentication on a primary or a media server instance

By default, multifactor authentication is optional. However, the **appadmin** user can enforce it for all users on the application instance.

Use the following procedures to enforce or stop enforcing multifactor authentication on a primary or a media server instance.

To enforce multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command:

```
/usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 1
[-grace-period <days>]
```

Where [-grace-period <*days*>] is an optional parameter to specify the number of days before users are forced to configure multifactor authentication before they can log in. If you do not include this parameter, the default of 90 days is used.

For example:

```
/usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 1
-grace-period 30
```

To stop enforcing multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command:

```
/usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 0
```

Resetting multifactor authentication on a primary or a media server instance

If a user with multifactor authentication changes or loses access to their mobile device and cannot sign in, use the following procedure to reset multifactor

authentication for that user. After a reset, the user is forced to reconfigure multifactor authentication the next time that they log in.

To reset multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -reset -user <username>
   ```

   Where *<username>* is the user that you need to reset.

Note: If you have any remote users that were added with the `vssat` command, you must use the `nbseccmd -resetMFA` command to reset them instead. See the *NetBackup Commands Reference Guide* for details.

Running NetBackup commands on a primary or a media server application instance

Flex Appliance provides the capability for the **appadmin** user to run NetBackup commands on all NetBackup primary and media server instances.

Note: Flex Appliance does not support adding local directories or manually editing any of the files on application instances. If you create a local directory or manually edit a file and the instance is relocated or stopped for any reason, the changes are not maintained when the instance restarts.

To run NetBackup commands on an instance, open an SSH session to the instance and log in as the **appadmin** user. For each command that you want to run, specify `sudo` and enter the absolute or the relative path. For example:

```
sudo /opt/veritas/vxapp-manage/tune -s
```

Commands on primary and media servers

You can run commands for the following directories and executables on primary and media server instances:

- `/opt/veritas/vxapp-manage/cp-nbu-config`

  See "Creating a NetBackup touch file on a primary or a media server application instance" on page 42.

- `/opt/veritas/vxapp-manage/cp-nbu-notify`

See "Installing NetBackup notify scripts on a primary or a media server application instance" on page 43.

- `/usr/openv/netbackup/bin`*
- `/usr/openv/netbackup/bin/admincmd`*
- `/usr/openv/netbackup/bin/goodies`*
- `/usr/openv/netbackup/bin/support`*
- `/usr/openv/volmgr/bin`*
- `/usr/openv/volmgr/bin/goodies`*

Note: Commands in the directories that are marked with an asterisk (*) can also be run in the following format without the path:

```
sudo -i <command>
```

For example:

```
sudo -i bpps
```

Commands on media servers only

You can run commands for the following directories and executables on media server instances only:

- `/opt/veritas/vxapp-manage/tune`
- `/usr/openv/pdde/pdag/bin/mtstrmd`
- `/usr/openv/pdde/pdag/bin/pdcfg`
- `/usr/openv/pdde/pdag/bin/pdusercfg`
- `/usr/openv/pdde/pdconfigure/pdde`
- `/usr/openv/pdde/pdcr/bin`
- `/usr/sbin/mount.nfs`
- `/usr/sbin/mount.nfs4`
- `/usr/sbin/umount.nfs`
- `/usr/sbin/umount.nfs4`

Note: The `df` command may show incorrect usage information for application instances. However, the total storage and the available storage are correct. To determine the correct usage information, subtract the available storage from the total storage.

For more information on NetBackup commands, refer to the *NetBackup Commands Reference Guide*.

Creating a NetBackup touch file on a primary or a media server application instance

The `cp-nbu-config` command copies the NetBackup configuration file from the user's home space to the specified NetBackup configuration destination directory. A NetBackup administrator can use the `cp-nbu-config` command to create and edit a NetBackup touch configuration file in any of the following directories:

- `/usr/openv/netbackup`
- `/usr/openv/netbackup/bin`
- `/usr/openv/java`
- `/usr/openv/lib/ost-plugins`
- `/usr/openv/netbackup/bin/snapcfg`
- `/usr/openv/netbackup/db/cloudSnap/credential`
- `/usr/openv/netbackup/db/cloudSnap/proxy`
- `/usr/openv/netbackup/db/config`
- `/usr/openv/netbackup/db/event`
- `/usr/openv/netbackup/db/images`
- `/usr/openv/netbackup/db/media`
- `/usr/openv/netbackup/ext/db_ext`
- `/usr/openv/netbackup/ext/db_ext/db2`
- `/usr/openv/var`
- `/usr/openv/volmgr`
- `/usr/openv/volmgr/database`

You cannot use the `cp-nbu-config` command to delete a touch configuration file.

To create or edit a touch configuration file

1. Log in to the NetBackup application instance.
2. Create a new configuration file in the NetBackup administrator home directory, or use the `cp` command to copy an existing configuration file from its original location to the home directory.

   For example:

   ```
   cp /usr/openv/lib/ost-plugins/pd.conf ~/
   ```

3. Make changes to the file in the home directory.
4. Run the following command to install the modified file in its original directory or a supported destination directory:

   ```
   sudo /opt/veritas/vxapp-manage/cp-nbu-config <configuration-file>
   <destination>
   ```

   Where *<configuration-file>* is the file that you created or edited, and *<destination>* is the directory where it needs to be installed.

   For example:

   ```
   sudo /opt/veritas/vxapp-manage/cp-nbu-config ~/pd.conf
   /usr/openv/lib/ost-plugins
   ```

Installing NetBackup notify scripts on a primary or a media server application instance

The `cp-nbu-notify` command installs NetBackup notify scripts from the user's home space onto the application instance.

If you have not previously installed the notify scripts on the instance, they exist as templates in the following directories:

- `/usr/openv/netbackup/bin/goodies`
- `/usr/openv/volmgr/bin/goodies`

To install or edit a NetBackup notify script

1. Log in to the NetBackup application instance.
2. Copy the NetBackup notify script from its original location to the home directory.

   For example:

   ```
   cp /usr/openv/netbackup/bin/goodies/bpstart_notify ~/
   ```

3. Make changes to the file in the home directory.
4. Run the following command to install the modified file in its original location:

   ```
   sudo /opt/veritas/vxapp-manage/cp-nbu-notify ~/<notify script>
   ```

   Where *<notify script>* is the script that you edited.

   For example:

   ```
   sudo /opt/veritas/vxapp-manage/cp-nbu-notify ~/bpstart_notify
   ```

Monitoring NetBackup services on a primary or a media server instance

The NetBackup services health monitoring feature allows Flex Appliance to monitor critical NetBackup services on primary and media server instances. If any of the services go down, the appliance attempts to restart them.

The application health is monitored every 60 seconds. You can view the detailed logs at `/mnt/nblogs/health-server.log`. Note that they are periodically cleaned up to avoid storage space exhaustion.

Note: Make sure to disable the health monitoring before you start any maintenance activity.

Use the following procedures to enable or disable NetBackup services health monitoring.

Enabling NetBackup services health monitoring

To enable NetBackup services health monitoring

1. Log in to the instance as the **appadmin** user.
2. Enter the following command to run a precheck before you enable health monitoring:

   ```
   sudo /opt/veritas/vxapp-manage/health precheck
   ```

3. Verify that the precheck did not return any errors, then run the following command:

   ```
   sudo /opt/veritas/vxapp-manage/health enable
   ```

4. Verify the health monitoring status with the following command:

   ```
   sudo /opt/veritas/vxapp-manage/health status
   ```

Disabling NetBackup services health monitoring

To disable NetBackup services health monitoring

1. Log in to the instance as the **appadmin** user.
2. Enter the following command:

   ```
   sudo /opt/veritas/vxapp-manage/health disable
   ```

3. Verify the health monitoring status with the following command:

   ```
   sudo /opt/veritas/vxapp-manage/health status
   ```

Mounting an NFS share on a NetBackup primary server instance

You can configure the NetBackup catalog backup policy to send disaster recovery files to a Network File System (NFS) share. Use the following procedure to mount an NFS share on a primary server application instance for disaster recovery.

To mount the NFS share and configure the catalog backup policy:

1. On the NFS server, run the following command to create a directory for the NFS share:

   ```
   mkdir <NFS directory>
   ```

2. Navigate to `/etc/exports` and add the following directive:

   ```
   <NFS directory> <primary IP address>(rw,no_root_squash)
   ```

   Where *<NFS directory>* is the directory that you created, and *<primary IP address>* is the IP address of the primary server instance.

   For example:

   ```
   /nfsdir 11.11.11.111(rw,no_root_squash)
   ```

3. Restart the NFS service or reload the configuration file with the `exportfs` command.

4. Log in to the primary server instance as the **appadmin** user and run the following commands:

   ```
   sudo bash
   ```

   ```
   cat > /mnt/nbdata/vxos/etc/fstab
   ```

   ```
   <NFS IP address>:<NFS directory> /mnt/nbcatdr nfs nfsvers=<NFS
   version>,rw,x-mount.mkdir
   ```

   Where *<NFS IP address>* is the IP address of the NFS server, *<NFS directory>* is the directory for the NFS share, and *<NFS version>* is either 3 or 4.

   For example:

   ```
   22.22.22.222:/nfsdir /mnt/nbcatdr nfs nfsvers=3,rw,x-mount.mkdir
   ```

5. From the Flex Appliance Console, restart the instance.
6. Log back in to the instance and run the following command:

   ```
   chown -R nbsvcusr:users /mnt/nbcatdr
   ```

7. From the NetBackup web UI, select **Protection** > **Policies** and click **Add**. Follow the prompts to configure a backup policy with the type **NBU-Catalog**. Specify the following information for the catalog disaster recovery file:

   - **Path**: `/mnt/nbcatdr/`
   - **Logon** and **Password**: Leave empty

   For more information about the catalog backup policy, see the chapter "Protecting the NetBackup Catalog" in the *NetBackup Administrator's Guide, Volume I*.

Setting environment variables on primary and media server instances

Use the following procedure to set environment variables on primary and media server application instances.

To add an environment variable

1. Log in to the instance as the **appadmin** user.
2. Navigate to one of the following locations:

   - If you want to set a variable for both interactive and non-interactive user sessions, navigate to `/etc/profile.d/custom.sh`.
   - If you want to set a variable for interactive user sessions only, navigate to `/etc/profile.d/sh.local`.

3. Edit the file to add the new variable.

Storing custom data on a primary or a media server instance

Flex Appliance does not generally support adding or editing directories and files on application instances. If you create or edit a directory or file and the instance is relocated or stopped for any reason, the changes are not maintained when the instance restarts.

However, if you have critical data that you must store on a NetBackup primary or media server application instance, use the following procedure to add it to the `/mnt/nblogs` directory.

Warning: The `/mnt/nblogs` directory is used for NetBackup logs and has 250GB of storage space that cannot be resized. The data that you add to this directory must be critical and small in size. If you use too much storage space, the instance may be affected.

To store custom data on a NetBackup primary or media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command to create a directory under `/mnt/nblogs`:

   `sudo mkdir /mnt/nblogs/<directory>`, where <*directory*> is the name of the new directory.
3. If required, run the following command to create a subdirectory:

   `sudo mkdir /mnt/nblogs/<directory>/<subdirectory>`, where <*directory*> is the name of the directory that you created in the previous step and <*subdirectory*> is the name of the subdirectory.
4. Add the required information to the new directory.

Modifying or disabling the nbdeployutil utility on a primary server instance

The `nbdeployutil` utility may adversely affect performance of NetBackup application instances on a 5150 appliance. If you do not need this feature or if you determine that it causes performance issues due to high CPU usage, you can modify the configuration or disable it as follows:

- Log in to the primary server instance and create the following **nbdeployutil** configuration file if it is not present:

  `/usr/openv/var/global/nbdeployutilconfig.txt`

- Refer to the topic "Scheduling capacity licensing reports" in the *NetBackup Administrator's Guide, Volume II* for the procedure to use custom values for the capacity licensing report.

Disabling SMB server signing on a media server instance

The Server Message Block (SMB) configuration on media server application instances enforces SMB server signing by default. This configuration may cause a performance reduction with Universal Shares. If you see a performance reduction, you can use the following procedure to disable server signing.

Warning: Disabling SMB server signing leaves the instance vulnerable to man-in-the-middle attacks. Only disable server signing if your instance is in a fully trusted private network.

To disable SMB server signing

1. Log in to the media server instance as the **appadmin** user and run the following command to navigate to the SMB configuration file:

   ```
   sudo vi /etc/samba/smb.conf
   ```

2. Modify this file to comment out the following entry:

   ```
   server signing = mandatory
   ```

3. Run the following command to restart the SMB service:

   ```
   sudo systemctl restart smb
   ```

Enabling extra OS STIG hardening on a primary or a media server instance

The Security Technical Implementation Guides (STIGs) provide technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. This type of security is also referred to as hardening.

OS STIG hardening rules are automatically enabled on primary and media server instances. These rules are based on the following profile from the Defense Information Systems Agency (DISA):

STIG for Red Hat Enterprise Linux Server

You can enable extra OS STIG hardening for increased security. The additional rules add protection to the `sshd` process and enforce stricter password policies.

Note the following about enabling extra OS STIG hardening:

- This command does not allow individual rule control.
- Once the option is enabled, it cannot be disabled.
- Before the extra rules are enabled on the instance, you can have unlimited concurrent SSH sessions. After OS STIG hardening is enabled, the maximum number of concurrent SSH sessions is limited to 10.

To enable extra OS STIG hardening

1. Open an SSH session to the instance as the **appadmin** user.
2. Run the following command:

```
sudo
/opt/veritas/appliance/pxcc/compliance/bin/pxcc_hardenvxos_on_demand.sh
-s
```

Using a login banner on a primary or a media server instance

You can set a text banner that appears before a user logs in to a primary or a media server instance. Typical uses for the login banner include legal notices, warning messages, and company policy information.

To add a login banner

1. Log in to the instance as the **appadmin** user and run the following command to access and edit the `/etc/issue` file:

```
sudo -i vi /etc/issue
```

2. Add the text that you want to appear in the banner.
3. Run the following command to access and edit the `sshd_config` file:

```
sudo -i vi /etc/ssh/sshd_config
```

4. In the file, locate the following entry:

```
#Banner none
```

Change it to the following:

```
Banner /etc/issue
```

5. Run the following command to restart the `sshd` service:

```
sudo systemctl restart sshd
```

To edit a login banner

1. Log in to the instance as the **appadmin** user and run the following command to access and edit the `/etc/issue` file:

   ```
   sudo -i vi /etc/issue
   ```

2. Edit the text as needed.

To remove a login banner

1. Log in to the instance as the **appadmin** user and run the following command to access and edit the `sshd_config` file:

   ```
   sudo -i vi /etc/ssh/sshd_config
   ```

2. In the file, locate the following entry:

   ```
   Banner /etc/issue
   ```

   Change it to the following:

   ```
   #Banner none
   ```

3. Run the following command to restart the `sshd` service:

   ```
   sudo systemctl restart sshd
   ```

Using a primary server instance for disaster recovery

If a NetBackup primary server application instance is lost in a disaster scenario, you can create a new instance to recover the identity of the instance that was lost. To recover the instance identity, you need the following information:

- The configuration details of the lost instance
- The NetBackup disaster recovery package
  For more information about the disaster recovery package, see the chapter "Disaster recovery" in the *NetBackup Troubleshooting Guide*.

To recover a primary server instance identity

1. Create a primary server instance with the same configuration as the instance that was lost. During instance creation, select the option **Use instance for disaster recovery**.

   See "Creating a NetBackup primary server instance" on page 14.

2. Open an SSH session to the instance. If you have not already, change the default password.

3. Copy the following NetBackup disaster recovery files to a local folder on the instance:
   - `PolicyName_XXXXXXXX_FULL`
   - `PolicyName_XXXXXXXX_FULL.drpkg`
4. Run the following command to import the disaster recovery package:

   ```
   sudo /usr/openv/netbackup/bin/admincmd/nbhostidentity -import
   -infile PolicyName_XXXXXXXX_FULL.drpkg
   ```
5. Run the following command to start all NetBackup services:

   ```
   sudo /usr/openv/netbackup/bin/goodies/netbackup start
   ```
6. From the NetBackup web UI, reissue a token for each associated media server and WORM storage server. Use the following steps:
   - On the left, click **Security > Hosts**.
   - Click **NetBackup certificates**.
   - Select the host and click **Generate reissue token**.
   - Enter a token name and indicate how long the token should be valid for.
   - Click **Create**.
7. Add the media servers to the primary server's host properties. Use the following steps:
   - On the left, click **Hosts > Host properties**.
   - Select the primary server, then click **Edit primary server > Servers**.
   - For a media server with MSDP storage, navigate to the **Additional servers** tab and click **Add**.

     For a media server with AdvancedDisk storage, navigate to the **Media servers** tab and click **Add.**
8. Run the Catalog Recovery Wizard. For instructions, see the section "Recovering the entire NetBackup catalog using the Catalog Recovery Wizard" in the *NetBackup Troubleshooting Guide*.
9. Once the catalog recovery completes successfully, run the following commands on the primary server instance to stop and start all primary server daemons:
   - `sudo /usr/openv/netbackup/bin/goodies/netbackup stop`
   - `sudo /usr/openv/netbackup/bin/goodies/netbackup start`
10. Log in to the media server instances and run the following command to stop and restart all media server daemons:

- `sudo /usr/openv/netbackup/bin/goodies/netbackup stop`
- `sudo /usr/openv/netbackup/bin/goodies/netbackup start`

11 From the NetBackup web UI, navigate to **Hosts > Host Properties**. Select each media server and click **Connect**.

12 On the left, click **Storage > Media servers**. Then click the **Media servers** tab. Select each media server and click **Activate**.

13 Perform a backup and restore test to each media server to verify that everything is working correctly.

Authorizing a primary or a media server instance for deletion

Deleting a NetBackup application instance requires multiperson authorization. Multiperson authorization requires that you unlock the deletion option before the instance can be deleted.

Use the following procedure to authorize a primary or a media server instance for deletion.

To authorize a primary or a media server instance for deletion

1 Open an SSH session to the instance as the **appadmin** user.

2 Run the following command:

```
sudo /opt/veritas/vxapp-manage/delete-ready --set
```

If you need to lock the deletion option again so that the instance can no longer be deleted, run the following command:

```
sudo /opt/veritas/vxapp-manage/delete-ready --unset
```

Accessing NetBackup WORM storage server instances for management tasks

To perform some management tasks on a WORM storage server instance, you must open an SSH session to the instance and log in to the deduplication shell. When you log in to the instance for the first time, use the `msdpadm` credentials with the administrator password that was set during instance creation in the Create Instance wizard. There is no default password, and no password change is required on first login.

From the deduplication shell, you can run commands to manage the instance and your WORM storage.

These are the main categories of commands:

- `dedupe`
  This command lets you manage the deduplication service.
- `retention`
  This command lets you manage image retention.
- `setting`
  This command lets you manage the deduplication and system configuration settings.
- `support`
  This command lets you access and upload the relevant logs and configuration files for troubleshooting.
- `recovery`
  This command lets you run the MSDPCheck tool to check the data integrity and report possible corrupted images.

Managing users from the deduplication shell

After you create a NetBackup WORM storage server application instance, you can use the deduplication shell to add and manage additional users.

The following types of users are supported:

- Local users
  See "Adding and removing local users from the deduplication shell" on page 53.
- MSDP users
  See "Adding MSDP users from the deduplication shell" on page 54.
- Active Directory (AD) users for Universal Shares and Instant Access
  See "Connecting an Active Directory domain to a WORM storage server for Universal Shares and Instant Access" on page 55.

Adding and removing local users from the deduplication shell

Use the following procedures to add or remove local users from the deduplication shell.

Adding local users

To add a local user

1. Open an SSH session to the server as the **msdpadm** user.
2. (Optional) If you want to use a random password for the new user, generate one with the following command:

   ```
   setting user random-password
   ```

3. Run the following command:

   ```
   setting user add-user username=<username>
   ```

   Where *<username>* is the username of the user that you want to add. When the prompt appears, enter the password for the user.

   The password must have between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~@={}?!).

4. Run the following commands to view the new user:

   - `setting user show-user username=<username>`
     This command shows the information about the new user.
   - `setting user list-users`
     This command shows a list of all local users.

Removing local users

To remove a local user

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting user delete-user username=<username>
   ```

   Where *<username>* is the username of the user that you want to remove.

   Note: The **msdpadm** user cannot be removed.

Adding MSDP users from the deduplication shell

NetBackup requires an MSDP user to connect to the deduplication storage. One MSDP user is required when you configure the storage server. If you use multiple NetBackup domains with the WORM instance, you need to add an additional MSDP user for each NetBackup domain after you create the instance.

Use the following procedure to add MSDP users from the deduplication shell.

To add an MSDP user

1. Open an SSH session to the server as the **msdpadm** user.
2. (Optional) If you want to use a random password for the new user, generate one with the following command:

   ```
   setting MSDP-user random-password
   ```

3. Run the following command:

   ```
   setting MSDP-user add-MSDP-user username=<username> role=<role>
   ```

   Where *<username>* is the username of the user that you want to add, and *<role>* is role of that user.

   The username must have between 4 and 30 characters and can include letters and numbers.

   Enter the user password when prompted.

   The password must be between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~={}?!).

4. Run the following commands to view the new user:

   - `setting MSDP-user verify-user username=<username>`
     This command verifies the username and the password for the new user.
   - `setting MSDP-user list`
     This command shows a list of all MSDP users.

Connecting an Active Directory domain to a WORM storage server for Universal Shares and Instant Access

You can connect an Active Directory (AD) user domain to a WORM storage server for Universal Shares and Instant Access.

Note: The AD domain is only used for Universal Shares and Instant Access. AD users are not currently supported on the deduplication shell.

Use the following procedure to connect an AD user domain from the deduplication shell.

To connect an AD user domain

1. Verify that the storage server is on the same network as the AD domain. If it is not, edit the settings so that the server can reach the domain.
2. Open the following ports between the storage server and the remote host if they are not already open:
   - 139
   - 445
3. Open an SSH session to the server as the **msdpadm** user.
4. Run the following command:

   ```
   setting ActiveDirectory configure ad_server=<server name>
   domain=<domain name> domain_admin=<username>
   ```

   Where *<server name>* is the AD server name, *<domain name>* is the domain that you want to connect, and *<username>* is the username of an administrator user on that domain.
5. When the prompt appears, enter the password for the domain administrator user.

Disconnecting an Active Directory domain from the deduplication shell

Use the following procedure to disconnect an Active Directory (AD) user domain from the deduplication shell.

To disconnect an AD user domain

1. Open an SSH session to the storage server as the **msdpadm** user.
2. Run the following command:

   ```
   setting ActiveDirectory unconfigure ad_server=<server name>
   domain=<domain name> domain_admin=<username>
   ```

   Where *<server name>* is the AD server name, *<domain name>* is the domain that you want to disconnect, and *<username>* is the username of an administrator user on that domain.
3. When the prompt appears, enter the password for the domain administrator user.

Changing a user password from the deduplication shell

Use the following procedures to change the password of a local user or an MSDP user from the deduplication shell.

Note: Remote directory user passwords cannot be changed from the shell. They must be changed from the server on which they reside.

Changing a local user password

Use the following procedure to change the password of a local user or the default **msdpadm** user.

To change a local user password

1. Open an SSH session to the server as the **msdpadm** user or the user that you want to change the password for.
2. (Optional) If you want to use a random password, generate one with the following command:

   ```
   setting user random-password
   ```

3. Run the following command:

   ```
   setting user change-password username=<username>
   ```

   Where <*username*> is the username of the user whose password you want to change.

4. Follow the prompt to change the password.

   The password must have between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~@={}?!).

5. (Optional) By default, passwords do not expire. To specify an expiration date for the password, run the following command:

   ```
   setting user set-password-exp-date username=<username>
   password_exp_date=<date>
   ```

   Where <*date*> is the expiration date in YYYY-MM-DD format.

   Once an expiration date has been set, you can view it with the following command:

   ```
   setting user show-password-exp-date username=<username>
   ```

Changing an MSDP user password

Use the following procedure to change the password of an MSDP user.

To change an MSDP user password

1. Open an SSH session to the server as the **msdpadm** user.
2. (Optional) If you want to use a random password, generate one with the following command:

   ```
   setting MSDP-user random-password
   ```

3. Run the following command:

   ```
   setting MSDP-user reset-password
   ```

4. Follow the prompt to enter the new password.

   The password must be between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~={}?!).

Managing multifactor authentication on a WORM storage server

NetBackup WORM storage servers support multifactor authentication for local users. Multifactor authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication individually, or the **msdpadm** user can enforce multifactor authentication for all users.

See "Configuring or disabling multifactor authentication on a WORM storage server" on page 58.

See "Enforcing multifactor authentication on a WORM storage server" on page 59.

See "Resetting multifactor authentication on a WORM storage server" on page 60.

Configuring or disabling multifactor authentication on a WORM storage server

Use the following procedures to configure or disable multifactor authentication on a NetBackup WORM storage server.

Note: If multifactor authentication is enforced, users cannot disable it after the grace period.

To configure multifactor authentication on a WORM storage server

1. (Optional) If you have already configured multifactor authentication for another server and want to use the same authenticator account to log in to this server, run the following command on the other server:

   ```
   setting MFA show
   ```

   Take note of the key.

2. On the server that you need to configure multifactor authentication for, run one of the following commands:

   - To enroll with a random key, run the following command:

     ```
     setting MFA enroll
     ```

   - To use an existing key, run the following command:

     ```
     setting MFA enroll secret=<existing key>
     ```

3. If you generated a new key, scan the QR code with an authentication app on your mobile phone. For example, Google Authenticator or Microsoft Authenticator.

   Note that the token validation is based on the server time. Ensure that the clock of the Flex Appliance and the mobile phone are correct.

Note: If the **msdpadm** user becomes locked, they cannot reset multifactor authentication for themself. To avoid this situation, Cohesity recommends that two or multiple users scan the same QR code of the **msdpadm** user with their mobile phones. If one user loses access to the token, another user can help them to enroll again.

To disable multifactor authentication on a WORM storage server

1. Log in to the server as the user that you want to disable multifactor authentication for.

2. Run the following command:

   ```
   setting MFA reset
   ```

Enforcing multifactor authentication on a WORM storage server

By default, multifactor authentication is optional. However, the **msdpadm** user can enforce it for all users on the server.

Use the following procedures to enforce or stop enforcing multifactor authentication on a WORM storage server.

To enforce multifactor authentication on a WORM storage server

1. Log in to the instance as the **msdpadm** user.
2. Run the following command:

   ```
   setting MFA setenforce enforce=1 [grace_period=<days>]
   ```

   Where [grace_period=<*days*>] is an optional parameter to specify the number of days before users are forced to configure multifactor authentication before they can log in. If you do not include this parameter, the default of 90 days is used.

   For example:

   ```
   setting MFA setenforce enforce=1 grace_period=30
   ```

To stop enforcing multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **msdpadm** user.
2. Run the following command:

   ```
   setting MFA setenforce enforce=0
   ```

Resetting multifactor authentication on a WORM storage server

If a user with multifactor authentication changes or loses access to their mobile device and cannot sign in, use the following procedure to reset multifactor authentication for that user. After a reset, the user is forced to reconfigure multifactor authentication the next time that they log in.

To reset multifactor authentication on a WORM storage server

1. Log in to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting MFA reset user=<username>
   ```

   Where <*username*> is the user that you need to reset.

Managing VLAN interfaces from the deduplication shell

If you use multiple NetBackup domains with a WORM storage server, you can add additional VLAN interfaces for the server to connect with the other domains. Use the following procedures to manage the VLAN interfaces.

Adding a VLAN interface

To add a VLAN interface

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting MSDP-VLAN add interface=<VLAN IP address>
```

Removing a VLAN interface

To remove a VLAN interface

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting MSDP-VLAN remove interface=<VLAN IP address>
```

Viewing the VLAN interfaces

To view the VLAN interfaces

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting MSDP-VLAN list
```

Viewing the lockdown mode on a WORM storage server

The appliance lockdown mode offers additional security levels to protect your data. WORM storage is supported when lockdown mode is enabled.

For more information about the lockdown modes, see the *NetBackup Flex Appliance Getting Started and Administration Guide*.

The lockdown mode is managed from the appliance, but you can also view the current lockdown mode from the deduplication shell.

To view the lockdown mode from a WORM instance

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting WORM show-mode
```

Managing the retention policy on a WORM storage server

The WORM retention policy defines how long the saved data on a WORM storage server is protected with immutability and indelibility. The initial retention policy is

determined when you configure the server. Use the following procedures to view or change the policy from the deduplication shell.

Viewing the retention policy

To view the retention policy

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting WORM status
```

Changing the retention policy

Use the following procedure to change the retention policy. The new retention policy applies for future backups. It does not apply to backups that were taken before you made the change.

To change the retention policy

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command and specify the minimum duration to keep the storage immutable and indelible:

```
setting WORM set-min worm_min=<duration in seconds>
```

3. Run the following command and specify the maximum duration to keep the storage immutable and indelible:

```
setting WORM set-max worm_max=<duration in seconds>
```

Managing images with a retention lock on a WORM storage server

The backup images on a WORM storage server have a retention lock based on the retention policy. The retention lock prevents the images from being modified or deleted. Use the following procedures to manage the backup images with a retention lock from the deduplication shell.

Note: You can also run the `catdbutil` command in the shell to manage the images. This command does not appear in the shell menu, but you can run it directly. However, the arguments for the command cannot include path separators (/).

For more information, see the section "About the NetBackup command line options to configure immutable and indelible data" in the *NetBackup Deduplication Guide*.

Viewing the backup images with a retention lock

To view the backup images with a retention lock

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
retention policy list
```

Disabling the retention lock on a backup image

You can disable the retention lock on a backup image if the appliance instance is in enterprise lockdown mode. You cannot disable the lock if the appliance instance is in compliance lockdown mode.

To disable the retention lock

1. Open an SSH session to the server as the **msdpadm** user.
2. Run one of the following commands:
   - To disable the retention lock on a single backup image:

     ```
     retention policy disable backup_id="<ID>" copynumber=<number>
     ```

   - To disable the retention lock on multiple backup images with the same copy number:

     ```
     retention policy batch-disable
     backupids="<backupid1,backupid2,backupid3,...,backupidn>"
     copynumber=<number>
     ```

   You can find the backup ID and the copy number in the output of the `retention policy list` command.

Auditing WORM retention changes

Use the following procedure to view a full history of the WORM configuration changes, including changes to the retention policy and to backup images.

Note: You can also run the `catdbutil` command in the shell to audit the retention changes. This command does not appear in the shell menu, but you can run it directly. However, the arguments for the command cannot include path separators (/).

For more information, see the section "About the NetBackup command line options to configure immutable and indelible data" in the *NetBackup Deduplication Guide*.

To audit retention changes

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
retention policy audit
```

Protecting the NetBackup catalog on a WORM storage server

By default, WORM storage servers store a copy of the NetBackup catalog in the directory `/mnt/msdp/vol0` in addition to the original copy that is available under the dedicated catalog volume (`/mnt/msdpcat`).

If you want extra protection for the catalog, the following options are available:

- Create additional local copies of the catalog.
  For more information on this option, see the topic "Protecting the NetBackup catalog from the deduplication shell" in the *NetBackup Deduplication Guide*.
- Configure an external backup of the catalog.
  For more information on this option, see the topic "Configuring an external MSDP catalog backup from the deduplication shell" in the *NetBackup Deduplication Guide*.

Managing certificates from the deduplication shell

To authenticate NetBackup hosts, NetBackup uses security certificates that are issued by a Certificate Authority (CA). A NetBackup storage server can use either a NetBackup CA or an external CA. The CA is first configured when you configure the server. After configuration, you can use the deduplication shell to manage the CA certificates.

For more information on how NetBackup uses certificates, see the *NetBackup Security and Encryption Guide*.

Viewing the certificate details from the deduplication shell

To view the certificate details, log in to the deduplication shell as the **msdpadm** user.

Use the following commands to view the details of the current certificate configuration:

- `setting certificate list-certificates`
  Displays the details of all the host certificates that are available on the server
- `setting certificate list-CA-cert-details`
  Displays the details of all the CA certificates that are available on the server

- `setting certificate show-CA-cert-detail`

  Displays the NetBackup CA certificate details of the primary server that is currently in use

- `setting certificate show-external-CA-cert-detail`

  Displays the external CA certificate details of the primary server that is currently in use

- `setting certificate list-enrollment-status`

  Retrieves the enrollment status of the associated primary servers from the local certificate store

- `setting certificate show-CRL-check-level`

  Displays the revocation check level for the external certificates

Use the following commands to verify the status of the certificates:

- `setting certificate host-self-check`

  Verifies whether the host certificate for the server is in the certificate revocation list (CRL)

- `setting certificate external-CA-health-check`

  Verifies the external certificates, the RSA keys, and the trust store

Importing certificates from the deduplication shell

Use the following procedures to import NetBackup or external certificates from the deduplication shell.

Importing a NetBackup certificate

To import a NetBackup certificate

1. Open an SSH session to the server as the **msdpadm** user.
2. Run one of the following commands:

   - To request the NetBackup CA certificate from the primary server:

     `setting certificate get-CA-certificate`

     By default, the command uses the first primary server entry in the NetBackup configuration file. You can specify an alternate primary server with the `primary_server` parameter. For example:

     `setting certificate get-CA-certificate primary_server=<alternate primary server hostname>`

   - To request a host certificate from the primary server:

     `setting certificate get-certificate [force=true]`

     Where [force=true] is an optional parameter that overwrites the existing certificate if it already exists.

By default, the command uses the first primary server entry in the NetBackup configuration file. You can specify an alternate primary server with the `primary_server` parameter. For example:

```
setting certificate get-certificate primary_server=<alternate primary server hostname>
```

Depending on the primary server security level, the host may require an authorization or a reissue token. If the command prompts that a token is required for the request, enter the command again with the token for the host ID-based certificate. For example:

```
setting certificate get-certificate primary_server=<alternate primary server hostname> token=<certificate token> force=true
```

Importing external certificates

To import external certificates

1. Open an SSH session to the server as the **msdpadm** user.
2. Run one of the following commands:
   - To download and install both the external CA certificate and the host certificate:

     ```
     setting certificate install-external-certificates cacert=<trust store> cert=<host certificate> private_key=<key>
     [passphrase=<passphrase>] scp_host=<host> scp_port=<port>
     ```

     Where:
     - *<trust store>* is the trust store in PEM format.
     - *<host certificate>* is the X.509 certificate of the host in PEM format.
     - *<key>* is the RSA private key in PEM format.
     - [passphrase=*<passphrase>*] is an optional parameter for the passphrase of the private key. This parameter is required if the key is encrypted.
     - *<host>* is the hostname of the host that stores the external certificates.
     - *<port>* is the port to connect to on the remote host.
   - To download and install the external CA certificate:

     ```
     setting certificate get-external-CA-certificate cacert=<trust store> scp_host=<host> scp_port=<port>
     ```

     Where:
     - *<trust store>* is the trust store in PEM format.
     - *<host>* is the hostname of the host that stores the external certificates.

- *<port>* is the port to connect to on the remote host.

- To download and install the external host certificate:

  `setting certificate get-external-certificates cert=<host certificate> private_key=<key> [passphrase=<passphrase>] scp_host=<host> scp_port=<port>`

  Where:

  - *<host certificate>* is the X.509 certificate of the host in PEM format.
  - *<key>* is the RSA private key in PEM format.
  - [passphrase=*<passphrase>*] is an optional parameter for the passphrase of the private key. This parameter is required if the key is encrypted.
  - *<host>* is the hostname of the host that stores the external certificates.
  - *<port>* is the port to connect to on the remote host.

  Note: If an external host certificate already exists on the server, it is overwritten.

3 (Optional) Run the following command to specify the revocation check level for the external certificates:

`setting certificate set-CRL-check-level check_level=<DISABLE, LEAF, or CHAIN>`

The check levels are as follows:

- DISABLE: The revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
- LEAF: The revocation status of the leaf certificate is validated against the CRL. LEAF is the default value.
- CHAIN: The revocation status of all certificates from the certificate chain is validated against the CRL.

Removing certificates from the deduplication shell

Use the following procedures to remove NetBackup or external certificates from the deduplication shell.

Warning: If you remove the existing certificates but have not installed new certificates, the WORM server can no longer communicate with the primary server. To switch from one type of certificate authority (CA) to the other, install the new NetBackup or external certificates before you remove the existing certificates.

To remove the NetBackup certificates

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting certificate disable-CA
```

To remove the external certificates

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting certificate remove-enrollment
```

Managing FIPS mode from the deduplication shell

You can use FIPS mode on a WORM storage server to conform to the Federal Information Process Standards (FIPS) 140-2. Use the following procedures to manage FIPS mode.

Viewing the FIPS mode

To check if FIPS mode is enabled or disabled

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting FIPS status
```

Enabling FIPS mode

To enable FIPS mode

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting FIPS enable
```

Disabling FIPS mode

To disable FIPS mode

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

```
setting FIPS disable
```

Managing post-quantum cryptography (PQC) mode from the deduplication shell

You can enable post-quantum cryptography (PQC) mode on a WORM storage server to enable use of the PQC algorithm in TLS 1.3 Hybrid Key Exchange. PQC mode can be enabled only if FIPS mode is disabled.

To learn more about PQC support in NetBackup, refer to the *NetBackup Security and Encryption guide*.

Caution: NetBackup uses the OQS provider to support post-quantum cryptography (PQC) for secure communications. While the OQS provider is a significant step towards preparing for a quantum-safe future, it is currently widely used in experimental and research environments. Cohesity recommends that you thoroughly assess all associated risks and ensure that its usage aligns with your organization's security policies and compliance requirements before enabling PQC mode.

Use the following procedures to manage PQC mode.

Viewing the PQC mode status

To check if PQC mode is enabled or disabled

1. Open an SSH session on the server as the `msdpadm` user.
2. Run the following command:

```
setting PQC status
```

Enabling PQC mode

To enable PQC mode

1. Open an SSH session on the server as the `msdpadm` user.
2. Run the following command:

```
setting PQC enable
```

Disabling PQC mode

To disable PQC mode

1. Open an SSH session on the server as the `msdpadm` user.
2. Run the following command:

   ```
   setting PQC disable
   ```

Encrypting backups from the deduplication shell

To encrypt backups on a WORM storage server, you can configure MSDP encryption with or without the Key Management Service (KMS).

Use the following procedures to configure encryption for your backups from the deduplication shell.

To configure MSDP encryption with KMS

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting encryption enable-kms kms_server=<server> key_group=<key group>
   ```

   Where *<server>* is the host name of the external KMS server and *<key group>* is the KMS server key group name.
3. To verify the KMS encryption status, run the `setting encryption kms-status` command.

To configure MSDP encryption without KMS

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting encryption enable
   ```
3. To verify the MSDP encryption status, run the `setting encryption status` command.

Converting legacy KMS to Key Encryption Key (KEK)

The `convert-legacy-kms` command migrates the legacy index-based KMS to KEK-based KMS. This migration unencrypts the SO records using the legacy KMS key and then re-encrypts the SO record using the active KEK.

To rotate keys for KEK encryption:

- Use the `rotate-kektag` command to create a new KEK and rotate SO records to the new KEK using the new three-tiered KMS system. In this system, KMS keys now encrypt KEKs which in turn encrypt SOs.
- The `rotate-kms-keys` command rotates the KMS keys under the new KMS system. KEKs, which are stored in the KMS proxy database, are unencrypted using the corresponding KMS key and then re-encrypted using the active KMS key.

Configuring an isolated recovery environment using the web UI

Perform the following steps to configure an isolated recovery environment using the NetBackup web UI.

Note: You can also configure and manage an IRE from the deduplication shell. See the *NetBackup Deduplication Guide* for more details.

Table 5-1 IRE configuration using the NetBackup web UI

Step	Task	Description
1.	Configure allowed subnets to allow only the hosts in the subnets to access the storage server.	See "Configuring the allowed subnets" on page 71.
2.	Configure reverse connections to support replicating backup images from storage servers outside the isolated recovery environment.	See "Configuring the reverse connections" on page 72.
3.	(Optional) Configure reverse replication schedule to allow network activities in a specific window.	See "Configuring the reverse replication schedule" on page 73.
4.	Configure SLP for replicating backup images from a production environment.	See "Adding a replication operation to SLP at the production primary server" on page 74.

Configuring the allowed subnets

Allowed subnets are like a firewall. Any hosts that are not in the allowed subnets has no access to the IRE MSDP server. Ensure that the IRE primary server is in the allowed subnets, otherwise you lose the control to the IRE MSDP server from the web UI. The computer you use to configure the IRE also must be in the allowed subnets.

To configure the allowed subnets

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment** > **Allowed subnets**, click **Add subnet**.
5. Select **IPv4** or **IPv6** and type the IP address of the subnet and click **Add to list**.
6. Add all the subnets in the IRE domain that are required to access the MSDP server and click **Save**.

Configuring the reverse connections

Before you add reverse connections from the IRE storage server to production storage server, ensure that NBCA or ECA are configured on the IRE storage server for the production domain.

To configure the reverse connections

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment** > **Reverse connections**, click **Add reverse connection**.
5. On the **Add reverse connection** page, provide the production primary server name.
6. Select the existing login credentials or add new credentials and click **Next**.
   - **Select existing credentials**: Select the existing credentials.
   - **Add a new credential**: Add a new credential for the production primary server. Under **Credential type**, select **Username Password authentication** or **Use API key**.

     Note: The user of the production primary server needs privileges in the **default IRE SLP Administrator** role.
7. Click **Connect**.

8 On the next page, select **Remote MSDP storage server**.

You can select an MSDP storage server from the production domain. If the MSDP storage server has multiple network interfaces configured and you want the reverse connection, use another interface rather than the storage server name. You can type the FQDN of the network interface for the production MSDP storage server.

9 In the **Local interface** field, provide the local storage server interface name for data transmission.

If the IRE MSDP server has multiple interfaces and you want the IRE MSDP server to use a specific interface to connect to the production MSDP storage server, type the FQDN of the network interface for the IRE MSDP storage server.

If nothing is specified in **Local interface** field, IRE MSDP server uses the default network interface to connect to the production storage server.

10 Click **Add**.

A reverse connection is configured from the IRE MSDP server to the production MSDP server.

Configuring the reverse replication schedule

By default, an IRE MSDP storage server allows reverse connections to production storage server in a big window (24x7). For security purpose, administrator may want the reverse connections to be created in a small window.

To configure the allowed subnets

1 On the left, click **Storage > Disk storage**.

2 Click the **Storage servers** tab.

3 Click on the MSDP storage server that you want to configure.

4 Under **Isolated Recovery Environment** > **Reverse replication schedule**, click **Configure schedule**.

5 Configure the window for each weekday to allow reverse connections. Click the **Reset to default 24/7schedule** to restore the window to the default.

6 Click **Save**.

Adding a replication operation to SLP at the production primary server

To configure the reverse connections

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment**, click **Modify SLP on the remote primary server**.
5. On the **Modify SLP on the remote primary server** page, provide the production primary server name.
6. Select the existing login credentials or add new credentials and click **Next**.
   - **Select existing credentials**: Select the existing credentials.
   - A**dd a new credential**: Add a new credential for the production primary server. Under **Credential type**, select **Username Password authentication** or **Use API key**.

     Note: The user of the production primary server needs privileges in the **default IRE SLP Administrator** role.
7. Click **Connect**.
8. Select the SLP that you want to add a replication operation to the IRE MSDP storage server and click **Next**.
9. Select an operation that you want to replicate to IRE MSDP storage server after the operation and click **Next**.
10. Select an SLP of the IRE domain for image import after replication completed.

11 On the **Window** tab, configure SLP window for the replication operation. Create a new SLP window or select an existing SLP window.

When you adjust the SLP window, ensure that the SLP window is covered by IRE schedule. If a replication is triggered outside the IRE schedule, reverse connection does not happen, and the replication job fails.

The **Synchronize with the reverse connection schedule** helps to replace the current SLP window with the IRE Schedule. You can adjust the SLP window based on the IRE Schedule.

The date and time that is shown on the page are based on the time zone of IRE primary server. If the production primary server and the IRE primary server are in different time zones, the time difference is calculated and the SLP window for the production primary server is converted automatically.

Click **Finish**.

12 Click **Save**.

All the configurations including MSDP storage server replication target, SLP window, and replication operation in the SLP are applied to the production primary server.

Tuning the MSDP configuration from the deduplication shell

The default MSDP configuration should work for most installations. However, if you need to make adjustments, use the following commands to set or view the parameters.

Parameter	Description	Commands
`AllocationUnitSize`	The allocation unit size for the data on the server	To set the parameter: `setting set-MSDP-param allocation-unit-size value=<number of MiB>` To view the parameter: `setting get-MSDP-param allocation-unit-size`
`DataCheckDays`	The number of days to check the data for consistency	To set the parameter: `setting set-MSDP-param data-check-days value=<number of days>` To view the parameter: `setting get-MSDP-param data-check-days`

Parameter	Description	Commands
`LogRetention`	The length of time to keep logs	To set the parameter: `setting set-MSDP-param log-retention value=<number of days>` To view the parameter: `setting get-MSDP-param log-retention`
`MaxCacheSize`	The maximum size of the NetBackup Deduplication Engine (`spoold`) fingerprint cache	To set the parameter: `setting set-MSDP-param max-cache-size value=<number of GB>` To view the parameter: `setting get-MSDP-param max-cache-size`
`MaxRetryCount`	The maximum number of times to retry a failed transmission	To set the parameter: `setting set-MSDP-param max-retry-count value=<number of retry times>` To view the parameter: `setting get-MSDP-param max-retry-count`
`SpadLogging`	The log level for the NetBackup Deduplication Manager (`spad`)	To set the parameter: `setting set-MSDP-param spad-logging log_level=<value>` See "Setting the MSDP log level from the deduplication shell" on page 78. To view the parameter: `setting get-MSDP-param spad-logging`
`SpooldLogging`	The log level for the NetBackup Deduplication Engine (`spoold`)	To set the parameter: `setting set-MSDP-param spoold-logging log_level=<value>` See "Setting the MSDP log level from the deduplication shell" on page 78. To view the parameter: `setting get-MSDP-param spoold-logging`
`WriteThreadNum`	The number of threads for writing data to the data container in parallel	To set the parameter: `setting set-MSDP-param write-thread-num value=<number of threads>` To view the parameter: `setting get-MSDP-param write-thread-num`

Parameter	Description	Commands

`CloudDataCacheSize`	The default data cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	To set the parameter:
		`setting set-MSDP-param cloud-data-cache-size value=<number>`
		To view the parameter:
		`setting get-MSDP-param cloud-data-cache-size`

`CloudMapCacheSize`	The default map cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	To set the parameter:
		`setting set-MSDP-param cloud-map-cache-size value=<number>`
		To view the parameter:
		`setting get-MSDP-param cloud-map-cache-size`

`CloudMetaCacheSize`	The default meta cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	To set the parameter:
		`setting set-MSDP-param cloud-meta-cache-size value=<number>`
		To view the parameter:
		`setting get-MSDP-param cloud-meta-cache-size`

`CloudUploadCacheSize`	The default upload cache size when the cloud LSU is added. The minimum value is 12 GiB.	To set the parameter:
		`setting set-MSDP-param cloud-upload-cache-size value=<number>`
		To view the parameter:
		`setting get-MSDP-param cloud-upload-cache-size`

Parameter	Description	Commands

`EnableLocalPredictive SamplingCache`	The parameter to enable or disable the local predictive sampling cache. Both `spoold` and `spad` have this parameter, and it should be synced between them.	To set the parameter:
		`setting set-MSDP-param enable-local-predictive-sampling-cache value=<true/false>`
		To view the parameter:
		`setting get-MSDP-param enable-local-predictive-sampling-cache`

`MaxPredictiveCacheSize`	The maximum size of the `spoold` predictive cache.	To set the parameter:
		`setting set-MSDP-param max-predictive-cache-size value=<number of bytes/%>`
		To view the parameter:
		`setting get-MSDP-param max-predictive-cache-size`

`MaxSamplingCacheSize`	The maximum size of the `spoold` sampling cache.	To set the parameter:
		`setting set-MSDP-param max-sampling-cache-size value=<number of bytes/%>`
		To view the parameter:
		`setting get-MSDP-param max-sampling-cache-size`

`UsableMemoryLimit`	The maximum usable memory size in `spoold`.	To set the parameter:
		`setting set-MSDP-param usable-memory-limit value=<number of bytes/%>`
		To view the parameter:
		`setting get-MSDP-param usable-memory-limit`

Setting the MSDP log level from the deduplication shell

You can set the log level on a WORM storage server for the following MSDP services:

- The NetBackup Deduplication Manager (`spad`)
- The NetBackup Deduplication Engine (`spoold`)

To set the log level

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `setting set-MSDP-param spad-logging log_level=<value>,[thread],[date],[timing],[silent]`
   - `setting set-MSDP-param spoold-logging log_level=<value>,[thread],[date],[timing],[silent]`

   Where:
   - *<value>* is one of the following:
     - minimal: enables the critical, error, authorization, and bug logs
     - short: enables all minimal logs and adds warning logs
     - long: enables all short logs and adds info logs
     - verbose: enables all long logs and adds notice logs
     - full: enables all verbose logs and adds trace messages (all available logs)
     - none: disables logging
   - [thread] is an optional parameter to enable thread ID logging.
   - [date] is an optional parameter to include the date at the beginning of each logged event.
   - [timing] is an optional parameter to enable high-resolution timestamps.
   - [silent] is an optional parameter to stop the logs from printing on the console or the screen.

   For example:

   ```
   setting set-MSDP-param spoold-logging log_level=full,thread
   ```

Managing NetBackup services from the deduplication shell

You can manage the following NetBackup services from the deduplication shell:

- The cyclic redundancy checking (CRC) service
  See "Managing the cyclic redundancy checking (CRC) service" on page 80.
- The content router queue processing (CRQP) service
  See "Managing the content router queue processing (CRQP) service" on page 81.

- The online checking service
  See "Managing the online checking service" on page 82.
- The compaction service
  See "Managing the compaction service" on page 82.
- The deduplication (MSDP) services
  See "Managing the deduplication (MSDP) services" on page 83.
- The Storage Platform Web Service (SPWS)
  See "Managing the Storage Platform Web Service (SPWS)" on page 84.
- The Veritas provisioning file system (VPFS)
  See "Managing the Veritas provisioning file system (VPFS) configuration parameters" on page 85.
  See "Managing the Veritas provisioning file system (VPFS) mounts" on page 87.
- The NGINX service
  See "Managing the NGINX service" on page 87.
- The SMB service
  See "Managing the SMB service" on page 88.
- The following deduplication utilities:
  - The deduplication manager utility (`cacontrol`)
    For more information about this utility, see the section "Oracle stream handler" in the *NetBackup Deduplication Guide*.
  - The deduplication engine utility (`crcontrol`)
    For more information about this utility, see the section "Viewing storage usage within MSDP container files" in the *NetBackup Deduplication Guide*.

Note: These commands do not appear in the shell menu, but you can run them directly. The arguments for these commands cannot include path separators (/).

Managing the cyclic redundancy checking (CRC) service

The cyclic redundancy checking (CRC) service is a data integrity check. Use the following procedures to manage the CRC service from the deduplication shell.

To view the status of the CRC service

1. Open an SSH session to the server.
2. Run one of the following commands:

- To view the general status of the CRC service:

  ```
  dedupe CRC state
  ```

- To view the status of the fix mode on the CRC service:

  ```
  dedupe CRC fixmode-state
  ```

To enable the CRC service or enable a different CRC mode

1. Open an SSH session to the server.
2. Run one of the following commands:
   - To enable the CRC service:

     ```
     dedupe CRC enable
     ```

   - To enable fast checking, which begins the check from container 64 and does not sleep between checking containers:

     ```
     dedupe CRC fast
     ```

     When the fast CRC ends, CRC behavior reverts to the behavior before fast checking was invoked.

   - To enable fix mode, which runs the check and attempts to fix any inconsistent metadata:

     ```
     dedupe CRC enable-fixmode
     ```

To disable the CRC service or fix mode

1. Open an SSH session to the server.
2. Run one of the following commands:
   - To disable the CRC service:

     ```
     dedupe CRC disable
     ```

   - To disable fix mode:

     ```
     dedupe CRC disable-fixmode
     ```

Managing the content router queue processing (CRQP) service

The content router queue processing (CRQP) service ensures that the internal databases are in sync with the storage. Use the following procedures to manage the CRQP service from the deduplication shell.

To view the status of the CRQP service

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `dedupe CRQP status`

This command shows the status from the last time that the CRQP service ran.

- `dedupe CRQP info`
  This command shows information about the current activity of the CRQP service.

To start the CRQP service

1. Open an SSH session to the server.
2. Run the following command:

```
dedupe CRQP start
```

Managing the online checking service

The online checking service is a data integrity check. Use the following procedures to manage the online checking service.

To start the online checking service

1. Open an SSH session to the server
2. Run the following command:

```
dedupe online-check start
```

To view the status of the online checking service

1. Open an SSH session to the server.
2. Run the following command:

```
dedupe online-check status
```

To enable or disable the online checking service

1. Open an SSH session to the server.
2. Run one of the following commands:

```
dedupe online-check enable
```

```
dedupe online-check disable
```

Managing the compaction service

The compaction service removes unnecessary data from the MSDP catalog. Use the following procedures to manage the compaction service.

To view the status of the compaction service

1. Open an SSH session to the server.
2. Run the following command:

```
dedupe compaction state
```

To enable or disable the compaction service

1. Open an SSH session to the server.
2. Run one of the following commands:

```
dedupe compaction enable
```

```
dedupe compaction disable
```

To start the compaction service outside of the system schedule

1. Open an SSH session to the server.
2. Run the following command:

```
dedupe compaction start
```

Managing the deduplication (MSDP) services

The deduplication services operate the Media Server Deduplication Pool (MSDP) storage on the storage server. Use the following procedures to manage the MSDP services.

To view the status of the MSDP services

1. Open an SSH session to the server.
2. Run the following command:

```
dedupe MSDP status
```

To stop the MSDP services

1. Open an SSH session to the server.
2. Check the health monitor status using the following command:

```
setting health status
```

3. If the health monitor is enabled, stop the monitor using the following command:

```
setting health disable
```

4. After disabling the health monitor, use the following command to stop the MSDP services:

```
dedupe MSDP stop
```

To start the MSDP services

1. Open an SSH session to the server.
2. Start the MSDP services using the following command:

   ```
   dedupe MSDP start
   ```

3. Start the health monitor using the following command:

   ```
   setting health enable
   ```

Managing the Storage Platform Web Service (SPWS)

The Storage Platform Web Service (SPWS) is a service for Instant Access and Universal Shares. Use the following procedures to manage the SPWS.

To view the status of the SPWS

1. Open an SSH session to the server.
2. Run the following command:

   ```
   dedupe spws status
   ```

To stop or start the SPWS

1. Open an SSH session to the server.
2. Run one of the following commands:

   ```
   dedupe SPWS stop
   ```

   ```
   dedupe SPWS start
   ```

To view an SPWS configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting spws-config get-spws-param spws_configkey=<parameter>
   ```

   Where `<parameter>` is the parameter that you want to view.

To change an SPWS configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting spws-config set-spws-param spws_configsection=<section>
   spws_configkey=<parameter> spws_configvalue=<value>
   ```

   Where `<section>` is the Samba configuration section, `<parameter>` is the parameter that you want to change, and `<value>` is the value that you want to change it to. For example:

   ```
   setting spws-config set-spws-param spws_configsection=Livemount
   spws_configkey=maxallowedusharebackupjobs spws_configvalue=5
   ```

Troubleshooting connection failures

If you experience persistent connection failures to the SPWS, use the following procedure to push the certificate from the SPWS to the primary NetBackup Web Service.

To push the certificate

1. Open an SSH session to the server.
2. Run the following command:

   ```
   dedupe spws push-spws-certificate
   ```

Managing the Veritas provisioning file system (VPFS) configuration parameters

The Veritas provisioning file system (VPFS) is a service for Instant Access and Universal Shares. The default VPFS configuration works for most environments. However, you can adjust the parameters if needed. Some of the parameters that may affect performance include:

- `numOfInstance`

  This parameter specifies the number of `vpfsd` instances. A universal share uses one `vpfsd` instance by default. In most cases, one instance is adequate. Increasing the number of `vpfsd` instances might improve universal share performance, although it also requires more CPU and memory. You can increase the number of `vpfsd` instances from 1 to up to 16 and distribute the shares cross all the `vpfsd` instances.

- `CloudCacheSize`

  This parameter specifies the local disk cache size. This option applies only to Universal Shares with object store and Instant Access with object store.

Use the following procedures to manage the VPFS configuration parameters.

To view a VPFS configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting vpfs-config get-vpfs-param vpfs_configkey=<parameter>
   ```

   Where *<parameter>* is the parameter that you want to view.

To change a VPFS configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting vpfs-config set-vpfs-param vpfs_configkey=<parameter>
   vpfs_configvalue=<value>
   ```

   Where *<parameter>* is the parameter that you want to change, and *<value>* is the value that you want to change it to. For example:

   ```
   setting vpfs-config set-vpfs-param vpfs_configkey=numOfInstance
   vpfs_configvalue=2
   ```

To temporarily change the log level of a VPFS share

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting vpfs-config set-log-level vpfs_loglevel=<level>
   vpfs_shareid=<share ID>
   ```

   Where *<level>* is `debug`, `information`, or `error`, and *<share ID>* is the ID of the share that you want to change the log level of. For example:

   ```
   setting vpfs-config set-log-level vpfs_loglevel=debug
   vpfs_shareid=my-db-share
   ```

Note: This command is meant for a short debugging session, and the change is not preserved if you restart the instance. To permanently change the log level, use the following command:

```
setting vpfs-config set-vpfs-param vpfs_configkey=logLevel
vpfs_configvalue=<level>
```

The default log level is `information`.

Managing the Veritas provisioning file system (VPFS) mounts

The Veritas provisioning file system (VPFS) is a service for Instant Access and Universal Shares. Use the following procedures to manage the VPFS mounts.

To view the status of the VPFS mounts

1. Open an SSH session to the server.
2. Run the following command:

   ```
   dedupe vpfs status
   ```

To stop or start the VPFS mounts

1. Open an SSH session to the server.
2. Run one of the following commands:

   `dedupe vpfs stop`

   `dedupe vpfs force-stop` (Use this command only if the `dedupe vpfs stop` command does not work or becomes stuck.)

   `dedupe vpfs start`

To view the list of VPFS shares

1. Open an SSH session to the server.
2. Run the following command:

   ```
   dedupe vpfs list-shares
   ```

Managing the NGINX service

The NGINX service is the gateway for the Storage Platform Web Service (SPWS). Use the following procedures to manage the NGINX service.

To view the status of the NGINX service

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting nginx status
   ```

To stop or start the NGINX service

1. Open an SSH session to the server as the **msdpadm** user.
2. Run one of the following commands:

   `setting nginx stop`

   `setting nginx start`

Configuring the NGINX certificate

The NGINX certificate lets NGINX communicate with the NetBackup primary server. Use the following procedure to manage the configuration if there are issues with the certificate.

To configure the NGINX certificate

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting nginx config-cert
   ```

3. You can view the details of the NGINX certificate with the following command:

   ```
   setting nginx show-cert
   ```

Managing the SMB service

The SMB service includes the SMB users for Instant Access and Universal Shares. Use the following procedures to manage the SMB service.

To view the status of the SMB service

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting smb status
   ```

To stop or start the SMB service

1. Open an SSH session to the server as the **msdpadm** user.
2. Run one of the following commands:

   ```
   setting smb stop
   setting smb start
   ```

To view an SMB configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting smb get-smb-param smb_configkey=<parameter>
   ```

   Where `<parameter>` is the parameter you want to view.

To change an SMB configuration parameter

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting smb set-smb-param smb_configsection=<section>
   smb_configkey=<parameter> smb_configvalue=<value>
   ```

   Where `<section>` is the Samba configuration section, `<parameter>` is the parameter that you want to change, and `<value>` is the value that you want to change it to. For example:

   ```
   setting smb set-smb-param smb_configsection="global"
   smb_configkey="server signing" smb_configvalue="mandatory"
   ```

Monitoring and troubleshooting NetBackup services from the deduplication shell

You can use the following commands to monitor and troubleshoot the NetBackup services on a WORM storage server.

- The `setting health` command

  This command manages the health monitor on the server, which monitors the application high availability status.

  See "Managing the health monitor" on page 90.

- The `support` command

  This command lets you access logs and configuration files for troubleshooting.

  See "Viewing information about the system" on page 90.
  See "Viewing the deduplication (MSDP) history or configuration files" on page 91.
  See "Viewing the log files" on page 93.
  See "Collecting and transferring troubleshooting files" on page 95.

- The `setting kernel` command

  This command lets you search for a keyword in the kernel parameters.

  See "Viewing information about the system" on page 90.

- The `crstats` and `dcscan` commands

  Note: These commands do not appear in the shell menu, but you can run them directly. The arguments for these commands cannot include path separators (/).

  For more information about the `crstats` and `dcscan` commands, see the section "About the tool updates for cloud support" in the *NetBackup Deduplication Guide*.

- The `msdpimgutil` command

  This command lets you check deduplication pool encryption status or image encryption status on the storage server.

Managing the health monitor

The health monitor is enabled by default to monitor the application high availability status. Use the following procedures to manage the health monitor from the deduplication shell.

To view the status of the health monitor

1. Open an SSH session to the server.
2. Run the following command:

   ```
   setting health status
   ```

To enable or disable the health monitor

1. Open an SSH session to the server.
2. Run one of the following commands:

   ```
   setting health enable
   setting health disable
   ```

Viewing information about the system

Use the following commands to view information about the system from the deduplication shell.

To view information about the hardware:

- `support hardware cpumem` or `support process htop`: Displays the CPU and memory information

To view information about the software:

- `support software show-MSDP-version`: Displays the Media Server Deduplication Pool (MSDP) version
- `support software show-OS-version`: Displays the Linux operating system version

To view information about the system processes:

- `support process MSDP-process`: Displays the MSDP processes
- `support process pidstat`: Displays the operating system processes (PIDs)

To view information about the system performance:

- `support diskio iostat`: Displays the information about the disk I/O
- `support diskio vmstat`: Displays the information about the wait on the disk I/O
- `support diskio nmon`: Displays the information about the monitor system, which monitors the disk I/O, the network I/O, and the CPU usage.
- `support diskio disk-volume`: Displays the information about the disk volume
- `support process memory-usage`: Displays the free and the used memory
- `support process atop`: Displays detailed information about the operating system and process activity

To search the kernel parameters:

- `setting kernel search-param keyword=<keyword>`
  Where *<keyword>* is the word that you want to search for.

To view network settings:

- `setting network ifconfig`: Displays the internet configuration
- `setting network ping ip=<ip_address>`: Pings the target IP address
- `setting network route route=<route>`: Displays the network routing information
- `setting network netstat`: Displays the network status and the protocol statistics

Viewing the deduplication (MSDP) history or configuration files

The deduplication services operate the Media Server Deduplication Pool (MSDP) storage on the storage server. You can view the following files from the MSDP services:

- The MSDP history files
- The MSDP configuration files

Use the following procedures to view or search these files from the deduplication shell.

To view information about the files

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `support MSDP-history ls [dir=<directory>]`

- `support MSDP-config ls [dir=<directory>]`

  Where [dir=*<directory>*] is an optional parameter to specify the directory that you want to view the files from. For example:

  ```
  support MSDP-config ls dir=config
  ```

To view a file

1. Open an SSH session to the server.
2. Do one of the following:
   - To view an entire file, run one of the following commands:
     - `support MSDP-history cat file=<file>`
     - `support MSDP-config cat file=<file>`

     Where *<file>* is the file name of the file that you want to view.
   - To view the last 10 lines of a file, run one of the following commands:
     - `support MSDP-history tail file=<file>`
     - `support MSDP-config tail file=<file>`

     Where *<file>* is the file name of the file that you want to view.

To search a file

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `support MSDP-history grep file=<file> pattern=<keyword>`
   - `support MSDP-config grep file=<file> pattern=<keyword>`

   Where `<file>` is the file name of the file that you want to search and `<keyword>` is the naming pattern that you want to search for. For example:

   ```
   support MSDP-config grep file=spa.cfg pattern=address
   ```

Viewing process information in the pseudo-file system

Use the following procedures to view or search files from the /proc/ directory.

To view information about the files

1. Open an SSH session to the server.
2. Run the command:

   ```
   support proc ls [dir=<directory>]
   ```

   - Where `[dir=<directory>]` is an optional parameter to specify the directory that you want to view the files from. For example:

```
support proc ls dir=config
```

To view a file

1. Open an SSH session to the server.
2. Do one of the following:
   - To view an entire file, run the command:
     ```
     support proc cat file=<file>
     ```
     Where `<file>` is the file name of the file that you want to view.
   - To view the last 10 lines of a file, run the following command:
     ```
     support proc tail file=<file>
     ```
     Where `<file>` is the file name of the file that you want to view.

To search a file

1. Open an SSH session to the server.
2. Run the following command:
   ```
   support proc grep file=<file> pattern=<keyword>
   ```
   Where `<file>` is the file name of the file that you want to search and `<keyword>` is the naming pattern that you want to search for. For example:
   ```
   support proc grep file=spa.cfg pattern=address
   ```

Viewing the deduplication rate of a Veritas provisioning file service (VPFS) share

Use the following procedure to view the deduplication rate of a Veritas provisioning file service (VPFS) share

To view the deduplication rate

1. Open an SSH session to the server.
2. Run the following command:
   ```
   dedupe vpfs meta-dump vpfs_metakind=dedupe vpfs_shareid=<share
   ID>
   ```
   Where *<share ID>* is the ID of the share that you want to view the deduplication rate of.

Viewing the log files

The following logs are available on a WORM storage server:

- The Media Server Deduplication Pool (MSDP) logs

These files include the logs for the `spad`, `spoold`, `ocsd`, and `vpfsd` services.

- The system logs
  These files include the logs in the `/mnt/nblogs` directory, which includes the logs related to instance management and certificates.

Use the following procedures to view or search the log files from the deduplication shell.

To view information about the files

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `support MSDP-log ls [dir=<directory>]`
   - `support syslogs ls [dir=<directory>]`

   Where [dir=*<directory>*] is an optional parameter to specify the directory that you want to view the files from. For example:

   ```
   support MSDP-log ls dir=spoold
   ```

To view a file

1. Open an SSH session to the server.
2. Do one of the following:
   - To view an entire file, run one of the following commands:
     - `support MSDP-log cat file=<file>`
     - `support syslogs cat file=<file>`

     Where *<file>* is the file name of the file that you want to view.
   - To view the last 10 lines of a file, run one of the following commands:
     - `support MSDP-log tail file=<file>`
     - `support syslogs tail file=<file>`

     Where *<file>* is the file name of the file that you want to view.

To search a file

1. Open an SSH session to the server.
2. Run one of the following commands:
   - `support MSDP-log grep file=<file> pattern=<keyword>`
   - `support syslogs grep file=<file> pattern=<keyword>`

   Where `<file>` is the file name of the file that you want to search and `<keyword>` is the naming pattern that you want to search for. For example:

```
support MSDP-log grep file=spad* pattern=sessionStartAgent
```

Collecting and transferring troubleshooting files

You can collect files from the following categories and transfer them to another host for easier viewing:

- The Media Server Deduplication Pool (MSDP) history files
- The MSDP configuration files
- The MSDP log files
- The system log files

Use the following procedure to collect and transfer these files from the deduplication shell:

To collect and transfer files

1. Open an SSH session to the server as the **msdpadm** user.
2. If you plan to collect and transfer a large log file, you may need to increase the amount of time before the SSH connection times out. The default is 10 minutes. Use the following steps to increase the time:
   - Run the following command:
     `setting ssh set-ssh-timeout ssh_timeout=<number of seconds>`
   - Run the following command to verify the change:
     `setting ssh show-ssh-timeout`
   - Close the current SSH session and open a new one.
3. Run one of the following commands to collect files of interest from the desired category:
   - `support MSDP-history collect`
   - `support MSDP-config collect`
   - `support MSDP-log collect`
   - `support syslogs collect`

   You can also use the following optional parameters:
   - `pattern=<keyword>`
     This parameter searches for a keyword within the files.
   - `mmin="<minutes, +minutes, or -minutes>"`
     This parameter specifies the timeframe to collect files from, in minutes. To collect the files from x minutes ago, enter `mmin="x"`. To collect the files

from less than x minutes ago, enter `mmin="-x"`. To collect the files from more than x minutes ago, enter `mmin="+x"`.

- `mtime="<days, +days, or -days>"`
  This parameter specifies the timeframe to collect files from, in days. To collect the files from x days ago, enter `mtime="x"`. To collect the files from less than x days ago, enter `mtime="-x"`. To collect the files from more than x days ago, enter `mtime="+x"`.

For example:

```
support MSDP-log collect pattern=spoold* mmin="+2"
```

4 Run the `scp` command from any category to create a tarball of all previously collected files (from all categories) and transfer the tarball to the target host using the `scp` protocol. For example:

```
support MSDP-config scp scp_target=user@example.com:/tmp
```

5 If applicable, run the following command to set the SSH time-out back to the default:

```
setting ssh set-ssh-timeout ssh_timeout=600
```

Verify the change with the `setting ssh show-ssh-timeout` command.

Managing S3 service from the deduplication shell

After you configure an MSDP WORM storage server on the Flex appliance, you can use the deduplication shell to configure and manage the S3 service.

- Configure the S3 service.
  See "Configuring the S3 service" on page 96.
- Create or reset the root credentials.
  See "Creating or resetting root credentials" on page 97.
- Change S3 service certificates.
  See "Changing the S3 service certificates" on page 97.
- Manage the S3 service status.
  See "Managing the S3 service " on page 97.

Configuring the S3 service

To use S3 interface for MSDP, you can configure S3 service on an MSDP WORM storage server instance.

To configure the S3 service

1. Open an SSH session to the server.
2. Run the following command:

```
setting s3srv s3srv-config s3srv_ca_type=<ca type>
[s3srv_loglevel=<log level>] [s3srv_port=<s3 port>]
```

   - **s3srv_ca_type**: Certificate authority type. NBCA: 1, ECA: 2.
   - **s3srv_loglevel**: S3 server log level.
     None: 0
     Error: 1
     Warning: 2
     Info: 3 (default)
     Debug: 4
   - **s3srv_port**: S3 server port. Default port is 8443.

Creating or resetting root credentials

After S3 interface for MSDP is configured, you can create root user's credentials to manage S3 credentials.

To create or reset root credentials of the S3 service

1. Open an SSH session to the server.
2. Run the following command:

```
setting s3srv s3srv-reset-iam
```

Changing the S3 service certificates

S3 server HTTPS certificate must be renewed manually when it expires.

To change the S3 service certificates

1. Open an SSH session to the server.
2. Run the following command:

```
setting s3srv s3srv-change-ca s3srv_ca_type=<ca type>
```

   - **s3srv_ca_type**: Certificate authority type. NBCA: 1, ECA: 2

Managing the S3 service

Perform the following steps to manage the S3 service status.

To manage the S3 service

1. Open an SSH session to the server.
2. View the status of the S3 service.

   ```
   setting s3srv status
   ```

3. Stop the S3 service.

   ```
   setting s3srv stop
   ```

4. Start the S3 services.

   ```
   setting s3srv start
   ```

Authorizing a WORM storage server for deletion

Deleting a WORM storage server requires multiperson authorization. Multiperson authorization requires that you unlock the deletion option before the server can be deleted.

Use the following procedure to authorize a WORM storage server for deletion.

To authorize a WORM storage server for deletion

1. Open an SSH session to the server as the **msdpadm** user.
2. Run the following command:

   ```
   setting storage-server unlock-deletion
   ```

3. You can check the status with the following command:

   ```
   setting storage-server get-status
   ```

If you need to lock the deletion option again so that the server can no longer be deleted, run the following command:

```
setting storage-server lock-deletion
```

Chapter 6

Creating and using a NextGen malware scanner instance

This chapter includes the following topics:

- Creating a NextGen malware scanner instance
- Malware scanning workflow for MSDP backup images using Flex application as the scan host
- Authorizing a malware scanner instance for deletion

Creating a NextGen malware scanner instance

Flex Appliance supports the NextGen Malware Scanner (Sophos) with the NFS share type.

Use the following procedure to create a NextGen malware scanner instance on Flex Appliance.

To create a NextGen malware scanner instance

1. Make sure that the NextGen malware scanner application you want to use is located in the repository on the Flex Appliance Console.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
3. Gather the following information for the new instance:

Note: The hostname and IP address must not be in use anywhere else in your domain.

- Tenant that you want to assign it to
- Hostname (maximum of 63 characters including the domain name)
- IP address
- Network interface
- Domain name
- Name servers
- Search domains
- Administrator password for the `appadmin` account (minimum 8 characters, re-entered for confirmation)
- Primary server hostname

  Note: The Flex Appliance Console does not prevent entering the same hostname in both the **Hostname for NextGen Malware Scanner** and the **Primary server hostname** fields, but that configuration is not supported. You must have a preexisting primary server with a different hostname.

- API key for primary server operations
  For more information about API keys, see the chapter "Creating and using API keys" in the *NetBackup Web UI Security Administrator's Guide*.
- Scanner host pool name
  If the scanner host pool doesn't exist, it is created when you create the instance.
- Certificate Authority (CA) information for one of the following:

  For a NetBackup CA:

  - CA SHA-1 or SHA-256 certificate fingerprint
    If the primary server is a Flex instance, you can locate this information from the instance details page of the primary server instance. Click on the instance name under **Application instances** on the **System topology** page.
    If the primary server is not a Flex instance, see the *NetBackup Security and Encryption Guide* for the steps to locate this information from NetBackup.

- (Optional) Token for host ID-based certificate
  Depending on the primary server security level, the host may require an authorization or a reissue token. If you do not specify a token when you create the instance, the wizard attempts to automatically obtain the certificate.

For an external CA:

- Trust store, in PEM format
- Host certificate, in PEM format
- Private key, in PEM format
- (Optional) Passphrase of the private key
  A passphrase is required if the key is encrypted.
- (Optional) Custom CRL files

4. If a firewall exists between the primary server and the new instance, open the following port on the primary server to allow communication:

   `PBX: 1556`

5. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
6. Click **Create instance**.
7. Select the appropriate malware scanner application from the repository list that appears, making sure to verify the version number. Click **Next**.
8. Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the primary server and any other NetBackup hosts that you want to communicate with the instance.

---

9. Once the instance has been created, open an SSH session to the instance and log in as `appadmin` using the password that you set in the **Create Instance** wizard. No default password ships with the image, and no password change is required on first login.

10 (Optional) If you entered the information for an HTTPS proxy server when you created the instance, perform the following additional steps:

- Log in to the instance and upload the CA certificates to `/mnt/nbdata`.
- Run the following command:

  ```
  sudo su -
  vi ~/.bashrc
  ```

- Add the following line to the file:

  ```
  SOPHOS_CA_CERTIFICATE_PATH=/mnt/nbdata/<certificate path>
  ```

  Where *<certificate path>* is the path to the CA certificates.

11 Cohesity recommends that you configure email alerts so that you receive a notification if the staging volume becomes full. To configure email alerts, see the topic "Configuring email alerts" in the *NetBackup Flex Appliance Getting Started and Administration Guide*.

Note: If you receive alerts that the staging volume is close to full, and it is already at the maximum size of 50 GB, you can reduce the number of images that are scanned at the same time. To do so, set the scan host resource limits to a lower value on the primary server from the NetBackup web UI. For more details, see the topic "Configure resource limits for malware detection" in the *NetBackup Security and Encryption Guide*.

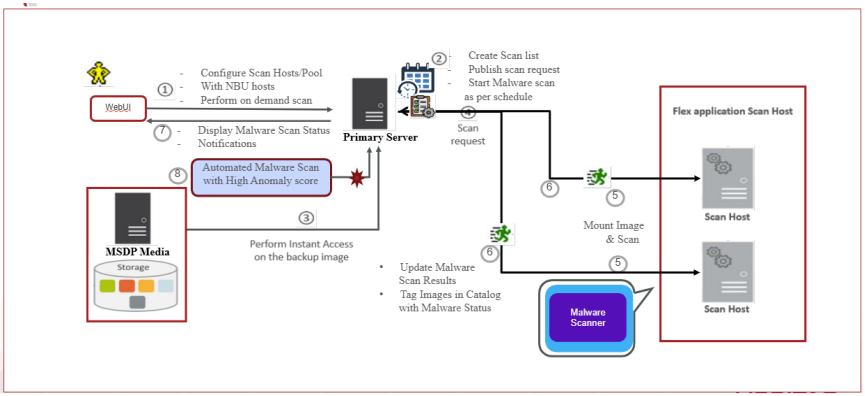
Note: When you start the instance, it is activated on the NetBackup side. When you stop the instance, it is deactivated.

If the scan host is not activated after starting the scanner container, wait until the NetBackup primary server is fully started, then restart the scanner container so the scan host activation can be retried.

Malware scanning workflow for MSDP backup images using Flex application as the scan host

NetBackup version 11.2.0.1 and later provides support for **Flex application** as the scan host to perform the malware scan. The **Flex application** uses the Flex Appliance secure communication and performs the scan on the Flex application.

The following figure displays the workflow of malware scanning for MSDP backup images:



The following steps depict the workflow for malware scanning for MSDP backup images:

1. After you start the **On Demand Scan**, the primary server validates the backup images and creates the scan jobs for each eligible backup image and identifies the available scan host for them. The following are a few of the criteria by which the backup images are validated:
   - Backup image must be supported for malware detection.
   - Backup image must have a valid Instant Access copy.
   - For an on-demand scan, no scans must be running for the same backup image. For DNAS the related streams are also considered.
   - Malware detection does not support a media server that is associated with storage.
   - Catalog must have details of the backup image.
2. After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.

Note: Currently the primary server starts 50 scan threads at a time. After the thread is available it processes the next job in the queue. Until then the queued jobs are in the pending state.

For NetBackup version 10.3 and later, large backups are scanned in batches of 500KB files. Each batch is scanned separately.

For recovery time scan, scan in batches feature is not supported.

---

3. The primary server identifies the available and the supported MSDP media server and instructs the media server to initiate the malware scan.

   If the scan host connectivity type is **Flex application**, then the primary server identifies the available Flex application scan host from the scan host pool. It then instructs the Flex application scan host to initiate the malware scan.

   Note: The **Flex application** scan host is applicable only for NFS share type and Sophos.

   ---

4. **Flex application** as the scan host:
   - The Flex application mounts the instant access mount on the scan host.
   - Scan is initiated using the malware tool that is configured in the scan host pool.
   - The Flex application performs the scan operation and updates the progress of the scan from scan host to the primary server.
5. After the scan is completed, the scan host unmounts the instant access mount from the scan host.

   Flex application as the scan host:
   - Malware scan status is updated to the primary server. The scan logs are copied to the Flex Appliance client scan host log directory (`nbmalwarescanner`).
   - The Flex Appliance client scan host updates the scan status and the infected file list along with the skipped file list (if any infected files) to the primary server.
6. The primary server updates the scan results and deletes instant access.
7. A malware scan status notification is generated.
8. The malware scan times out if there is no update on the scan. Default time out period is 48 hours.

   Malware detection performs an automated cleanup of eligible scan jobs that are older than 30 days.

Authorizing a malware scanner instance for deletion

Deleting a NetBackup application instance requires multiperson authorization. Multiperson authorization requires that you unlock the deletion option before the instance can be deleted.

Use the following procedure to authorize a malware scanner instance for deletion.

To authorize a malware scanner instance for deletion

1. Open an SSH session to the instance as the **appadmin** user.
2. Run the following command:

   ```
   sudo /opt/veritas/vxapp-manage/delete-ready --set
   ```

If you need to lock the deletion option again so that the instance can no longer be deleted, run the following command:

```
sudo /opt/veritas/vxapp-manage/delete-ready --unset
```