

NetBackup™ 10.2.0.1 Application Guide

For Flex Appliance 3.1, 3.2, and 3.3

NetBackup™ Application Guide

Last updated: 2023-10-25

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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. VERITAS TECHNOLOGIES LLC 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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Product overview	6
	Introduction to NetBackup applications for Flex Appliance	6
	About the Flex Appliance documentation	7
Chapter 2	Release notes	9
	NetBackup 10.2.0.1 application new features, enhancements, and changes	9
	Supported upgrade paths to this release	9
	Operational notes	9
Chapter 3	Getting started	11
	Prerequisites before you can create NetBackup application instances	11
	Installing the NetBackup Administration Console and client packages	12
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	22
Chapter 5	Managing NetBackup application instances	28
	Managing application instances from Flex Appliance and NetBackup	28
	Accessing NetBackup primary and media server instances for management tasks	29
	Managing users on a primary or a media server instance	29
	Running NetBackup commands on a primary or a media server application instance	37
	Monitoring NetBackup services on a NetBackup primary server instance	41

Mounting an NFS share on a NetBackup primary server instance	42
Setting environment variables on primary and media server instances	43
Storing custom data on a primary or a media server instance	44
Modifying or disabling the nbdeployutil utility on a primary server instance	44
Disabling SMB server signing on a media server instance	45
Enabling extra OS STIG hardening on a primary or a media server instance	45
Using a login banner on a primary or a media server instance	46
Using a primary server instance for disaster recovery	47
Accessing NetBackup WORM storage server instances for management tasks	49
Managing users from the deduplication shell	49
Managing VLAN interfaces from the deduplication shell	54
Viewing the lockdown mode on a WORM storage server	55
Managing the retention policy on a WORM storage server	55
Managing images with a retention lock on a WORM storage server	56
Auditing WORM retention changes	57
Protecting the NetBackup catalog on a WORM storage server	58
Managing certificates from the deduplication shell	58
Managing FIPS mode from the deduplication shell	62
Encrypting backups from the deduplication shell	63
Configuring an isolated recovery environment from the deduplication shell	64
Managing an isolated recovery environment from the deduplication shell	70
Tuning the MSDP configuration from the deduplication shell	73
Setting the MSDP log level from the deduplication shell	76
Managing NetBackup services from the deduplication shell	77
Monitoring and troubleshooting NetBackup services from the deduplication shell	85
Managing S3 service from the deduplication shell	90

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

Veritas Flex Appliance is a customizable data management solution that lets you consolidate multiple applications on a single hardware platform. An application is a Veritas 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 10.2.0.1:

- 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 18.0.1
 - The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 18.0.1 requires a version 10.2.0.1 or later 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 Veritas 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 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 Veritas 5360 Appliance Hardware Installation Guide*
- *The Veritas 5360 Appliance Product Description*
- *The Veritas 5350 Appliance Hardware Installation Guide*
- *The Veritas 5350 Appliance Product Description*
- *The Veritas 5340 Appliance Hardware Installation Guide*
- *The Veritas 5340 Appliance Product Description*
- *The Veritas 5260 Appliance Hardware Installation Guide*
- *The Veritas 5260 Appliance Product Description*
- *The Veritas 5250 Appliance Hardware Installation Guide*
- *The Veritas 5250 Appliance Product Description*
- *The Veritas 5150 Appliance Hardware Installation Guide*
- *The Veritas 5150 Appliance Product Description*
- *The Veritas Appliance Safety and Maintenance Guide*

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

You can find the latest documentation on the [Documentation page](#) of the Veritas Support website. Navigate to the **Documentation** tab, then select **Flex Appliance OS** on the left-hand side.

API documentation is also available from the **Knowledge Base** page on [Veritas SORT](#).

Release notes

This chapter includes the following topics:

- [NetBackup 10.2.0.1 application new features, enhancements, and changes](#)
- [Supported upgrade paths to this release](#)
- [Operational notes](#)

NetBackup 10.2.0.1 application new features, enhancements, and changes

This release does not include any new features, enhancements, or changes that are specific to the NetBackup 10.2.0.1 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 10.2.0.1.

Operational notes

This topic explains important aspects of the NetBackup 10.2.0.1 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:

- If a media server instance restarts due to an appliance operation such as a restart or a power cycle, or if the instance is relocated as part of any operation, the following problems may result:

- SAN client backups run over LAN instead of Fibre Transport.
- SAN client backups fail.
- Backups and restores through Fibre Transport fail.
- Remote tape devices become unusable.

To avoid these issues, monitor the **Fibre Channel interfaces** page of the Flex Appliance Console after an appliance restart or instance relocation. You can also check the **Fibre Channel** tab of the instance details page. Wait for the link state of the ports to be up before you run any backups. The ports may take up to 10 minutes to become active.

If the ports are up, but you still encounter problems with your backup jobs, do one of the following:

- Log in to the NetBackup Java console, navigate to **Media and Device Management > Devices > SAN Clients**, then choose each SAN client that is affected and trigger a Fibre Channel (FC) rescan.

- Log in to the media server instance and run the following command:

```
sudo /usr/opensv/netbackup/bin/admincmd/nbftconfig  
-rescanallclients
```

- When you create a new application instance, the **Application instances** section of the **System topology** page may show the instance status as **Partially Deleted** while the creation is in progress. The **Partially Deleted** status displays in error and can be safely ignored. You can track the instance creation progress from the Activity Monitor, and the instance status changes to **Online** when the instance creation has completed successfully.

Getting started

This chapter includes the following topics:

- [Prerequisites before you can create NetBackup application instances](#)
- [Installing the NetBackup Administration Console and 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 *Flex Appliance Getting Started 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, the NetBackup Administration Console or the NetBackup Remote Administration Console, and the NetBackup client software. See [“Installing the NetBackup Administration Console and client packages”](#) on page 12.

Installing the NetBackup Administration Console and client packages

To create and manage NetBackup instances, you need access to the NetBackup Administration Console or the NetBackup Remote Administration Console. Use the NetBackup Remote Administration Console if you want to manage your instances from a computer that does not have NetBackup software installed.

You also need access to the NetBackup client software so that you can install it on the computers that you want to back up.

The NetBackup Administration Console and 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 [Veritas Support website](#).

For more information about the interfaces or installing the client software, refer to the *NetBackup Installation Guide*, which is accessible from the [NetBackup page](#) on the Support website.

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 10.2.0.1:

- 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 18.0.1
The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 18.0.1 requires a version 10.2.0.1 or later 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 Veritas 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 22.

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
- Usage Insights customer registration key

A Veritas Usage Insights customer registration key is required to create this instance. To obtain a key, log in to the [Veritas NetInsights Console](#) site with your VEMS credentials. Go to the **Registration Keys** page to download the key

- (Optional) NetBackup license key
 NetBackup applications come with an evaluation license key. You must add a permanent NetBackup license key before the evaluation key expires. You can add your permanent key when you create the instance to avoid future issues.

Note: If the evaluation key expires before you create the instance, the instance creation fails. Make sure that you have a valid license key before you create an instance.

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

Application instances (2/2)

You must stop an instance before you can resize the storage.



- 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 successfully, you must change the password from the known default password.

Warning: You cannot access the NetBackup web UI to manage the instance until you have changed the password.

To change the password, open an SSH session to the instance and log in with the following credentials:

- Username: **appadmin**
- Password: **P@ssw0rd**

Follow the prompt to enter a new password. When the password change is complete, you are logged out. You can log back in with the new password.

Note: Do not configure AdvancedDisk storage on a NetBackup primary server instance. The NetBackup web UI and the NetBackup Administration Console let 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 28.

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.
- 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.

Application instances (2/2)

You must stop an instance before you can resize the storage.



- 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 successfully, you must change the password from the known default password. To change the password, open an SSH session to the instance and log in with the following credentials:
 - Username: **appadmin**

- Password: **P@ssw0rd**

Follow the prompt to enter a new password. When the password change is complete, you are logged out. You can log back in with the new password.

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

- Sign in to the NetBackup web UI. On the left, click **Storage > Storage configuration** and then click **Add**.
- Select **AdvancedDisk** or **Media Server Deduplication Pool (MSDP)** 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/opensv/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/opensv/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/opensv/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/opensv/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 Veritas 5250 Appliance:

- Log in to the instance as the **appadmin** user and run the following commands:
 - `sudo /usr/opensv/pdde/pdag/bin/pdcfg --write /mnt/msdp/vol0/etc/puredisk/contentrouter.cfg --section CRDataStore --option MaxFileSize --value 256Mib`
 - `sudo /usr/opensv/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 28.

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 *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 *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.

- 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.

Application instances (2/2)

You must stop an instance before you can resize the storage.



- 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 successfully, you must change the password from the known default password. To change the password, open an SSH session to the instance and log in with the following credentials:

- Username: **msdpadm**
- Password: **P@ssw0rd**

Follow the prompt to enter a new password. When the password change is complete, you are logged out. You can log back in with the new password.

- 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 28.

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

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

Instance operations that you can perform from NetBackup

All 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 following default credentials:

- Username: **appadmin**
- Password: **P@s#w0rd**

You are required to change your password the first time you log in.

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 37.

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 30.
 - See [“Changing a user password on a primary or a media server instance”](#) on page 36.

- Active Directory (AD) users
See [“Connecting an Active Directory user domain to a primary or a media server instance”](#) on page 31.
- Lightweight Directory Access Protocol (LDAP) users
See [“Connecting an LDAP user domain to a primary or a media server instance”](#) on page 33.

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
 - 145

- 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/sss/sss.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 Veritas 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/sss/sss.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.

Accessing NetBackup primary and media server instances for management tasks

- 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/sss/sss.conf.
```
- 4 Run the following command to copy the file and create a backup:


```
sudo cp /etc/sss/sss.conf /mnt/Nbdata/sss.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.veritas.com:636`
- `ldap_search_base =`
Enter the LDAP search domain.
For example: `ldap_search_base = dc=example,dc=veritas,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/sss/sss.conf` on the instance and verify that the file includes the following line:

Accessing NetBackup primary and media server instances for management tasks

```
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:

Accessing NetBackup primary and media server instances for management tasks

```
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.

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>
```

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.

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 39.
- `/opt/veritas/vxapp-manage/cp-nbu-notify`
See [“Installing NetBackup notify scripts on a primary or a media server application instance”](#) on page 40.
- `/usr/opensv/netbackup/bin*`
- `/usr/opensv/netbackup/bin/admincmd*`
- `/usr/opensv/netbackup/bin/goodies*`
- `/usr/opensv/netbackup/bin/support*`
- `/usr/opensv/volmgr/bin*`
- `/usr/opensv/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:

Accessing NetBackup primary and media server instances for management tasks

- `/opt/veritas/vxapp-manage/tune`
- `/usr/opensv/pdde/pdag/bin/mtstrmd`
- `/usr/opensv/pdde/pdag/bin/pdcfg`
- `/usr/opensv/pdde/pdag/bin/pdusercfg`
- `/usr/opensv/pdde/pdconfigure/pdde`
- `/usr/opensv/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/opensv/netbackup`
- `/usr/opensv/netbackup/bin`
- `/usr/opensv/java`
- `/usr/opensv/lib/ost-plugins`
- `/usr/opensv/netbackup/bin/snapcfg`
- `/usr/opensv/netbackup/db/cloudSnap/credential`
- `/usr/opensv/netbackup/db/cloudSnap/proxy`
- `/usr/opensv/netbackup/db/config`

Accessing NetBackup primary and media server instances for management tasks

- /usr/opensv/netbackup/db/event
- /usr/opensv/netbackup/db/images
- /usr/opensv/netbackup/db/media
- /usr/opensv/netbackup/ext/db_ext
- /usr/opensv/netbackup/ext/db_ext/db2
- /usr/opensv/var
- /usr/opensv/volmgr
- /usr/opensv/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/opensv/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/opensv/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/opensv/netbackup/bin/goodies`
- `/usr/opensv/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/opensv/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 NetBackup primary server instance

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

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, create a user with the user ID 1000 and the group ID 100. You do not need to do this step if a user with these credentials already exists.

To create the user, run the following command:

```
useradd <username> -u 1000 -g 100
```

Where *<username>* is the username of the new user.

- 2 On the NFS server, navigate to `/etc/exports` and add the following directive:

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

Where *<NFS directory>* is the directory for the NFS share, 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.

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

```
$ sudo bash
```

```
bash-4.2# cat > /mnt/nbdata/vxos/etc/fstab
```

```
<NFS IP address>:<NFS directory> /mnt/nbcatdr nfs v<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 v3,rw,x-mount.mkdir
```

- 5 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:** appadmin
- **Password:** Your **appadmin** user password

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 Veritas 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/opensv/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.

Accessing NetBackup primary and media server instances for management tasks

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


```
sudo /usr/opensv/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/opensv/netbackup/bin/goodies/netbackup stop`
 - `sudo /usr/opensv/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/opensv/netbackup/bin/goodies/netbackup stop`
 - `sudo /usr/opensv/netbackup/bin/goodies/netbackup start`
- 11 From the NetBackup web UI, navigate to **Hosts > Host Properties**. Select each media server and click **Connect**.
 - 12 From the NetBackup Administration Console, navigate to **Devices > Media servers**. Right click on each media server and click **Activate**.
 - 13 Perform a backup and restore test to each media server to verify that everything is working correctly.

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 following default credentials:

- Username: **msdpadm**
- Password: **P@ssw0rd**

You are required to change your password the first time you log in.

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.

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 50.
- MSDP users
See [“Adding MSDP users from the deduplication shell”](#) on page 51.
- 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 52.

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> password=<password>
```

Where *<username>* is the username of the user that you want to add, and *<password>* is a password for that 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>
password=<password>
```

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

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

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
 - 145

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 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 in enterprise lockdown mode and compliance lockdown mode, which have different levels of access restrictions.

For more information about the lockdown modes, see the *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 is in enterprise mode. You cannot disable the lock if the appliance is in compliance mode.

To disable the retention lock

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

```
retention policy disable backup_ID=<ID> 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, you can configure additional copies. Use the following procedures to manage the NetBackup catalog copies from the deduplication shell.

To view the catalog copies

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

```
cacontrol --catalog listshadowcopies
```

To configure an additional copy

- 1 Open an SSH session to the server.
- 2 Run the following command to determine which volumes exist in the `/mnt/msdp` directory:

```
df -h
```

Select one of the volumes other than `vol0`.

Note: To configure an additional catalog copy, at least one volume other than `vol0` must exist in the `/mnt/msdp` directory.

- 3 Run the following command:

```
cacontrol --catalog addshadowcopy /mnt/msdp/<volume name>
```

Where `<volume name>` is the volume that you chose in the previous step.

For example:

```
cacontrol --catalog addshadowcopy /mnt/msdp/vol1
```

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:

Accessing NetBackup WORM storage server instances for management tasks

- `<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
```

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 hostname 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.

Configuring an isolated recovery environment from the deduplication shell

You can configure an isolated recovery environment (IRE) on a WORM storage server to create an air gap between your production environment and a copy of the protected data. The air gap restricts network access to the data except during the timeframe when data replication occurs. This feature helps to protect against ransomware and malware.

To configure an IRE, you need a production NetBackup environment and a target Flex Appliance with a WORM storage server instance.

The production environment does not require any additional steps for this feature. Use the following procedure to configure an IRE on the target WORM storage server from the deduplication shell.

To configure an IRE

- 1 If A.I.R. is not configured on the production domain, continue to the next step. If A.I.R. is already configured on the production domain, log in to the deduplication shell as the **msdpadm** user. Run the following command to show the SLP windows for replication from the primary server to the WORM server.

```
setting ire-network-control show-slp-windows
production_primary_server=<production domain>
production_primary_server_username=<production username>
ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
username>
```

Where:

- *<production domain>* is the fully qualified domain name (FQDN) of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.

Accessing NetBackup WORM storage server instances for management tasks

- *<IRE domain>* is the FQDN of the primary server in the IRE. Use the same hostname that you used for the target primary server when you configured the SLPs in the production environment.
- *<IRE username>* is the username of a NetBackup user with permission to list SLPs and storage units in the IRE. For Windows users, enter the username in the format *<domain name>\<username>*. For other users, enter the username only.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

The following is an example output of the command:

```
EveryDayAtNoon:
SLPs: SLP1
Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59
Tuesday start: 12:00:00 duration: 00:59:59
Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59
Friday start: 12:00:00 duration: 00:59:59
Saturday start: 12:00:00 duration: 00:59:59

WeeklyWindow:
SLPs: SLP2
Sunday start: 10:00:00 duration: 01:59:59
Monday NONE
Tuesday NONE
Wednesday NONE
Thursday NONE
Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

This example shows two SLP windows:

- A daily window for one hour starting at noon.
 - A weekly window for two hours starting at 10:00 A.M.
- 2** Based on the requirements for your environment, determine a schedule and take note of it. For an existing A.I.R. environment, the schedule must accommodate the SLP windows that you viewed in the previous step.

You can set a daily schedule that is open at the same time each day, or you can set a different schedule for each day of the week.

In the previous example, you can accommodate both SLP windows with either of the following:

- A daily schedule from 10:00 A.M. to 1:00 P.M.
- A schedule from 12:00 P.M. to 1:00 P.M. on Monday through Friday and a schedule from 10:00 A.M. to 1:00 P.M. on Saturday and Sunday

Note: If the production environment and the IRE are in different time zones, the schedule must begin only once per day in both time zones. For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times get converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

- 3** Run the following command to configure which subnets and IP addresses are allowed to access the WORM storage server:

```
setting ire-network-control allow-subnets subnets=<CIDR subnets
or IP addresses>
```

Where *<CIDR subnets or IP addresses>* is a comma-separated list of the allowed IP addresses and subnets, in CIDR notation.

For example:

```
setting ire-network-control allow-subnets
subnets=10.80.120.208,10.84.48.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE must be included in the allowed list. If all of these servers are in the same subnet, only the subnet is required to be in the allowed list. If you have a dual stack IPv4-IPv6 network, make sure that you add both the IPv4 and the IPv6 addresses to the allowed list.

- 4 Run the following command to set the daily air gap schedule:

```
setting ire-network-control set-schedule start_time=<time>
duration=<duration> [weekday=<0-6>]
```

Where [weekday=<0-6>] is an optional parameter to indicate the day if you need to set different schedules for different days. 0 is Sunday, 1 is Monday, etc.

For example:

```
setting ire-network-control set-schedule start_time=10:00:00
duration=03:00:00 weekday=0
```

- 5 Before you can send data between the production domain and the IRE storage server, you must add MSDP reverse connections and add the replication operation.

See [“Configuring data transmission between a production environment and an IRE WORM storage server from the deduplication shell”](#) on page 67.

Configuring data transmission between a production environment and an IRE WORM storage server from the deduplication shell

Once the configuration of an isolated recovery environment (IRE) is completed, the production NetBackup hosts are no longer able to access the WORM storage server. You need to add MSDP reverse connections to allow data transmission between the production MSDP storage server and the IRE WORM storage server. Then you can add the replication operation.

To configure data transmission between a production environment and an IRE

- 1 Open an SSH session to the IRE WORM storage server. Run the following command to determine if the external network is open:

```
setting ire-network-control external-network-status
```

If it is not, run the following command:

```
setting ire-network-control external-network-open
```

- 2 Depending on the type of certificate authority that you use for host communication, do one of the following:
 - If you use a NetBackup Certificate Authority, run the following commands to request the certificates from the production domain:

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

Accessing NetBackup WORM storage server instances for management tasks

```
setting certificate get-certificate primary_server=<production
primary server> token=<token>
```

- If you use an external certificate authority, run the following commands to enroll the certificates with the production domain:

```
setting certificate enroll-external-certificates
server=<production primary server>
```

3 Run the following command to add an MSDP reverse connection:

```
setting ire-network-control add-reverse-connection
remote_storage_server=<production MSDP server>
[remote_primary_server=<production primary server>]
[local_storage_server=<IRE network interface>]
```

Where:

- *<production MSDP server>* is the fully qualified domain name (FQDN) of the MSDP server in your production environment.
 - *[remote_primary_server=<production primary server>]* is an optional parameter for the FQDN of the primary server in your production environment. This parameter is required if the IRE domain uses an alternative name to access the production primary server. This scenario usually occurs if the production primary server runs on multiple networks with multiple hostnames.
 - *[local_storage_server=<IRE network interface>]* is an optional parameter for the hostname of the network interface to use for image replication on the IRE storage server. This parameter is required if the network interface for replication is different than the IRE storage server name.
- 4** If necessary, repeat the previous step to add additional MSDP reverse connections.
- 5** If Auto Image Replication (AIR) is not already configured on the production domain, run the following command to copy the IRE schedule to the production domain as a storage lifecycle policy (SLP) window:

```
setting ire-network-control sync-ire-window
production_primary_server=<production primary server>
production_primary_server_username=<production username>
[slp_window_name=<SLP window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.

Accessing NetBackup WORM storage server instances for management tasks

- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.
 - `[slp_window_name=<SLP window name>]` is an optional parameter to give a name for the SLP window. If you do not provide this parameter, the name of the SLP window is `IRE_DEFAULT_WINDOW`.
- 6** If you do not have them already, create a source SLP on the production primary server and a target import SLP on the IRE primary server. See the section "Creating a storage lifecycle policy" in the *NetBackup Deduplication Guide* for details.

Note: You cannot add the replication operation from NetBackup when you create the SLPs. Continue to the next step to add the replication operation.

- 7** Run the following command to add the IRE WORM storage server as a replication target of the production NetBackup domain and to add the replication operation to the SLP:

```
setting ire-network-control add-replication-op
production_primary_server=<production primary server>
production_primary_server_username=<production username>
production_storage_server=<production storage server>
ire_primary_server_username=<IRE username>
source_slp_name=<production SLP name> target_import_slp_name=<IRE
SLP name> target_storage_server=<target storage server>
target_storage_server_username=<target storage server username>
production_storage_unit=<MSDP storage unit> [slp_window_name=<slp
window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.
- *<production storage server>* is the FQDN of the production storage server in your production environment.

- *<IRE username>* is the username for an administrator on the IRE primary server. For Windows users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.
 - *<source SLP name>* is the SLP name from the production primary server to add the replication operation to.
 - *<target SLP name>* is the import SLP name from the IRE primary server.
 - *<target storage server>* is the FQDN of the target WORM storage server in your IRE environment.
 - *<target storage server username>* is the username for an administrator on the target WORM storage server.
 - *<MSDP storage unit>* is the name of the MSDP storage unit that is the replication source in the source SLP.
 - `[slp_window_name=<slp window name>]` is an optional parameter for the name of the SLP window that is synced with the IRE schedule. This parameter must match the SLP window name from the previous step, if applicable. If you do not provide this parameter, the default name is used.
- 8** If you opened the external network at the beginning of this procedure, run the following command to close it and resume the air gap schedule:

```
setting ire-network-control resume-schedule
```

Managing an isolated recovery environment from the deduplication shell

Once you have configured an isolated recovery environment (IRE) on a WORM storage server, you can manage it from the deduplication shell as the **msdpadm** user. Use the following commands.

- To view the SLP windows from the primary server to the WORM server:


```
setting ire-network-control show-slp-windows
production_primary_server=<production domain>
production_primary_server_username=<production username>
ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
username>
```

Where:

- *<production domain>* is the fully qualified domain name (FQDN) of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows

users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.

- **<IRE domain>** is the FQDN of the primary server in the IRE. Use the same hostname that you used for the target primary server when you configured the SLPs in the production environment.
- **<IRE username>** is the username of a NetBackup user with permission to list SLPs and storage units in the IRE. For Windows users, enter the username in the format **<domain name>\<username>**. For other users, enter the username only.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

Note: The SLP replication window on the production domain must be configured to be open at the same time as the IRE schedule.

- To list the MSDP reverse connections:

```
setting ire-network-control list-reverse-connections
```

- To add an MSDP reverse connection:

```
setting ire-network-control add-reverse-connection
remote_storage_server=<production MSDP server>
[remote_primary_server=<production primary server>]
[local_storage_server=<IRE network interface>]
```

Where:

- **<production MSDP server>** is the FQDN of the MSDP server in your production environment.
- **[remote_primary_server=<production primary server>]** is an optional parameter for the FQDN of the primary server in your production environment. This parameter is required if the IRE domain uses an alternative name to access the production primary server. This scenario usually occurs if the production primary server runs on multiple networks with multiple hostnames.
- **[local_storage_server=<IRE network interface>]** is an optional parameter for the hostname of the network interface to use for image replication on the IRE storage server. This parameter is required if the network interface for replication is different than the IRE storage server name.
- To verify that a reverse connection works:

```
setting ire-network-control validate-reverse-connection
remote_storage_server=<production MSDP server>
[remote_primary_server=<production primary server>]
[local_storage_server=<IRE network interface>]
```

- To remove an MSDP reverse connection:

```
setting ire-network-control remove-reverse-connection
remote_storage_server=<production MSDP server>
```

- To view the allowed IP addresses and subnets:

```
setting ire-network-control show-allows
```

Note: You can also view the live firewall settings of the instance from the Flex Appliance Console on version 3.2 and later. Navigate to the **Application instances** section of the **System topology** page and click the instance name, then click **Live firewall settings**. Note that this link can take up to a minute to appear after you configure the allowed subnets and does not appear if you have not done so.

- To add IP addresses and subnets to the allowed list:

```
setting ire-network-control allow-subnets subnets=<CIDR subnets
or IP addresses>
```

Where *<CIDR subnets or IP addresses>* is a comma-separated list of the allowed IP addresses and subnets, in CIDR notation.

For example:

```
setting ire-network-control allow-subnets
subnets=10.80.120.208,10.84.48.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE must be included in the allowed list. If all of these servers are in the same subnet, only the subnet is required to be in the allowed list. If you have a dual stack IPv4-IPv6 network, make sure that you add both the IPv4 and the IPv6 addresses to the allowed list.

- To remove the IP addresses and subnets from the allowed list:

```
setting ire-network-control allow-subnets subnets=,
```

- To view the daily air gap schedule:

```
setting ire-network-control show-schedule
```

- To change the air gap schedule:

```
setting ire-network-control set-schedule start_time=<time>
duration=<duration>
```

For example:

```
setting ire-network-control set-schedule start_time=10:00:00
duration=03:00:00
```

Note: If the production environment and the IRE are in different time zones, the schedule must begin only once per day in both time zones. For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times get converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

- To stop the air gap schedule:


```
setting ire-network-control delete-schedule
```
- To view the current network status and check whether the external network is open or closed:


```
setting ire-network-control external-network-status
```
- To manually open the external network:


```
setting ire-network-control external-network-open
```
- To manually close the external network and resume the air gap schedule:


```
setting ire-network-control resume-schedule
```

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	<p>To set the parameter: <code>setting set-MSDP-param allocation-unit-size value=<number of MiB></code></p> <p>To view the parameter: <code>setting get-MSDP-param allocation-unit-size</code></p>

Parameter	Description	Commands
DataCheckDays	The number of days to check the data for consistency	<p>To set the parameter: <code>setting set-MSDP-param data-check-days value=<number of days></code></p> <p>To view the parameter: <code>setting get-MSDP-param data-check-days</code></p>
LogRetention	The length of time to keep logs	<p>To set the parameter: <code>setting set-MSDP-param log-retention value=<number of days></code></p> <p>To view the parameter: <code>setting get-MSDP-param log-retention</code></p>
MaxCacheSize	The maximum size of the NetBackup Deduplication Engine (spoold) fingerprint cache	<p>To set the parameter: <code>setting set-MSDP-param max-cache-size value=<number of GB></code></p> <p>To view the parameter: <code>setting get-MSDP-param max-cache-size</code></p>
MaxRetryCount	The maximum number of times to retry a failed transmission	<p>To set the parameter: <code>setting set-MSDP-param max-retry-count value=<number of retry times></code></p> <p>To view the parameter: <code>setting get-MSDP-param max-retry-count</code></p>
SpadLogging	The log level for the NetBackup Deduplication Manager (spad)	<p>To set the parameter: <code>setting set-MSDP-param spad-logging log_level=<value></code></p> <p>See “Setting the MSDP log level from the deduplication shell” on page 76.</p> <p>To view the parameter: <code>setting get-MSDP-param spad-logging</code></p>
SpooldLogging	The log level for the NetBackup Deduplication Engine (spoold)	<p>To set the parameter: <code>setting set-MSDP-param spoold-logging log_level=<value></code></p> <p>See “Setting the MSDP log level from the deduplication shell” on page 76.</p> <p>To view the parameter: <code>setting get-MSDP-param spoold-logging</code></p>

Parameter	Description	Commands
WriteThreadNum	The number of threads for writing data to the data container in parallel	<p>To set the parameter: <code>setting set-MSDP-param write-thread-num value=<number of threads></code></p> <p>To view the parameter: <code>setting get-MSDP-param write-thread-num</code></p>
CloudDataCacheSize	The default data cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	<p>To set the parameter: <code>setting set-MSDP-param cloud-data-cache-size value=<number></code></p> <p>To view the parameter: <code>setting get-MSDP-param cloud-data-cache-size</code></p>
CloudMapCacheSize	The default map cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	<p>To set the parameter: <code>setting set-MSDP-param cloud-map-cache-size value=<number></code></p> <p>To view the parameter: <code>setting get-MSDP-param cloud-map-cache-size</code></p>
CloudMetaCacheSize	The default meta cache size when the cloud LSU is added. Decrease this value if sufficient free space is not available.	<p>To set the parameter: <code>setting set-MSDP-param cloud-meta-cache-size value=<number></code></p> <p>To view the parameter: <code>setting get-MSDP-param cloud-meta-cache-size</code></p>
CloudUploadCacheSize	The default upload cache size when the cloud LSU is added. The minimum value is 12 GiB.	<p>To set the parameter: <code>setting set-MSDP-param cloud-upload-cache-size value=<number></code></p> <p>To view the parameter: <code>setting get-MSDP-param cloud-upload-cache-size</code></p>

Parameter	Description	Commands
EnableLocalPredictiveSamplingCache	The parameter to enable or disable the local predictive sampling cache. Both <code>spoold</code> and <code>spad</code> have this parameter, and it should be synced between them.	<p>To set the parameter:</p> <pre>setting set-MSDP-param enable-local-predictive-sampling-cache value=<true/false></pre> <p>To view the parameter:</p> <pre>setting get-MSDP-param enable-local-predictive-sampling-cache</pre>
MaxPredictiveCacheSize	The maximum size of the <code>spoold</code> predictive cache.	<p>To set the parameter:</p> <pre>setting set-MSDP-param max-predictive-cache-size value=<number of bytes/%></pre> <p>To view the parameter:</p> <pre>setting get-MSDP-param max-predictive-cache-size</pre>
MaxSamplingCacheSize	The maximum size of the <code>spoold</code> sampling cache.	<p>To set the parameter:</p> <pre>setting set-MSDP-param max-sampling-cache-size value=<number of bytes/%></pre> <p>To view the parameter:</p> <pre>setting get-MSDP-param max-sampling-cache-size</pre>
UsableMemoryLimit	The maximum usable memory size in <code>spoold</code> .	<p>To set the parameter:</p> <pre>setting set-MSDP-param usable-memory-limit value=<number of bytes/%></pre> <p>To view the parameter:</p> <pre>setting get-MSDP-param usable-memory-limit</pre>

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 78.
- The content router queue processing (CRQP) service
See [“Managing the content router queue processing \(CRQP\) service”](#) on page 79.

- The online checking service
See [“Managing the online checking service”](#) on page 80.
- The compaction service
See [“Managing the compaction service”](#) on page 80.
- The deduplication (MSDP) services
See [“Managing the deduplication \(MSDP\) services”](#) on page 81.
- The Storage Platform Web Service (SPWS)
See [“Managing the Storage Platform Web Service \(SPWS\)”](#) on page 82.
- The Veritas provisioning file system (VPFS) mounts
See [“Managing the Veritas provisioning file system \(VPFS\) mounts”](#) on page 83.
- The NGINX service
See [“Managing the NGINX service”](#) on page 84.
- The SMB service
See [“Managing the SMB service”](#) on page 84.
- 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 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
```

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
```

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 start
```

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

```
setting nginx config-cert
```

```
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
```

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 85.
- The `support` command

This command lets you access logs and configuration files for troubleshooting.
See [“Viewing information about the system”](#) on page 86.
See [“Viewing the deduplication \(MSDP\) history or configuration files”](#) on page 87.
See [“Viewing the log files”](#) on page 88.
See [“Collecting and transferring troubleshooting files”](#) on page 89.
- The `setting kernel` command

This command lets you search for a keyword in the kernel parameters.
See [“Viewing information about the system”](#) on page 86.
- 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*.

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 information about the disk I/O
- `support diskio vmstat`: Displays information about the wait on the disk I/O
- `support diskio nmon`: Displays information about the monitor system, which monitors the disk I/O, the network I/O, and the CPU usage
- `support diskio disk-volume`: Displays 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.

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 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*, *spola*, *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 91.
- Create or reset the root credentials.
See [“Creating or resetting root credentials”](#) on page 91.
- Change S3 service certificates.
See [“Changing the S3 service certificates”](#) on page 92.
- Manage the S3 service status.
See [“Managing the S3 service”](#) on page 92.

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
```