NetBackup™ 10.0.0.1 Application Guide

For Flex Appliance 2.1

VERITAS™

NetBackup™ Application Guide

Last updated: 2022-09-23

Legal Notice

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

This chapter includes the following topics:

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 10.0.0.1:

- 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 16.0.1
  The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 16.0.1 requires a version 10.0.0.1 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 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 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.

Chapter 2

Release notes

This chapter includes the following topics:

NetBackup 10.0.0.1 application new features, enhancements, and changes

The following list describes the new features, enhancements, and changes that are specific to the NetBackup 10.0.0.1 application. The application also includes the new features from NetBackup unless they are called out as exceptions in this guide. See the *NetBackup Release Notes* for more information.

- NetBackup WORM storage server instances now include an air gap solution. You can configure an isolated recovery environment to restrict network access to the protected data except during the timeframe when data replication occurs. This air gap helps to protect against ransomware and malware.
  See "Configuring an isolated recovery environment on a Flex Appliance WORM storage server instance" on page 72.
- The commands in the WORM storage server shell have been updated to use the new "primary server" terminology. The parameters in the following commands have changed from `master_server` to `primary_server`:
  - `setting get-CA-certificate`
  - `setting get-certificate`

Supported upgrade paths to this release

You can upgrade directly from any previous NetBackup application version to version 10.0.0.1.

Operational notes

This topic explains important aspects of the NetBackup 10.0.0.1 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/openv/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.
- When you create an instance, if you enter the IP address before you select a network interface, the **IP address** field displays the following error message:

"IP address does not belong to the selected network's subnet."

This message still displays after you select the network interface that corresponds to the IP address. To clear the message, click inside the **IP address** field and then click or tab outside of it.

- The username **maintenance** is no longer supported on application instances. If an existing user has the username **maintenance** when you upgrade to this release, that user becomes disabled.

Chapter 3

Geting started

This chapter includes the following topics:

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 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.

Chapter 4

Creating NetBackup application instances

This chapter includes the following topics:

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 10.0.0.1:

- 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 16.0.1
  The WORM storage server application is included with the NetBackup release but follows a different version scheme. WORM storage server version 16.0.1 requires a version 10.0.0.1 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 15.

See "Creating a NetBackup media server instance" on page 17.

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

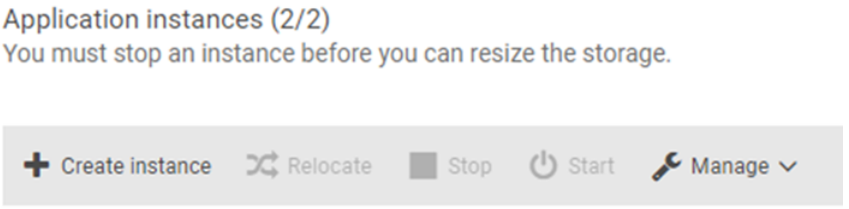
A Veritas Usage Insights customer registration key is required to create this instance. To obtain a key, log in to the Veritas NetInsights Console site with your VEMS credentials. Go to the **Registration Keys** page to download the key

- (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.



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

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

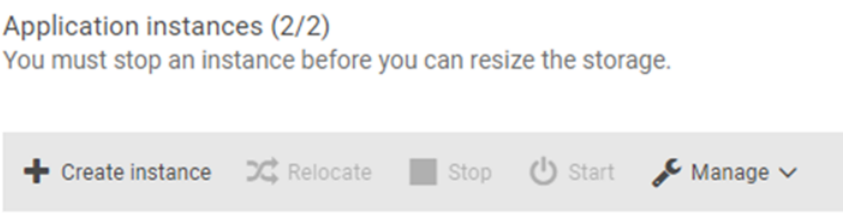
4 Add the hostname for the new instance to the **Media Servers** list or the **Additional Servers** list on the primary server, as follows:

- Log on to the NetBackup Administration Console as the administrator.
- In the main console window, in the left pane, click **NetBackup Management** > **Host Properties** > **Primary Servers**.
- In the right pane, double click on the primary server hostname.
- In the **Primary Server Properties** window, click one of the following:
  - If you want MSDP storage on the instance, click **Servers** > **Additional Servers**.
  - If you want AdvancedDisk storage on the instance, click **Servers** > **Media Servers**.
- Click **Add** and enter the hostname for the new instance. The hostname should appear in the list.
- Click **OK**.

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

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

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



7. Click **Create instance**.
8. Select the appropriate media server application from the repository list that appears, making sure to verify the version number. Click **Next**.
9. Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

   Note: If you 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:
    - Log on to the NetBackup Administration Console and select either **NetBackup Management** or **Media and Device Management**.
    - Click **Configure Disk Storage Servers** 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 or Cloud Catalyst storage, Veritas recommends that you tune the `MaxCacheSize` according to the following guidelines:

- On each instance, allocate .75 GB to 1 GB of RAM for each TiB of storage that is allocated to deduplication or Cloud Catalyst. For example, if the storage pool has 80 TiB allocated, the `MaxCacheSize` should be 60 GB to 80 GB of RAM.
- The sum of the `MaxCacheSize` for all instances with deduplication or Cloud Catalyst storage should not exceed 70% of the physical RAM on the appliance.

To tune the MSDP `MaxCacheSize` on this instance:

- Run the following command on the instance:

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

  Where *<percent%>* is the percentage of the appliance RAM to use for the cache on the instance.
- Restart the `pdde-storage` process with the following commands:

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

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

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

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

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

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

To tune the parameters on a Veritas 5250 Appliance:

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

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

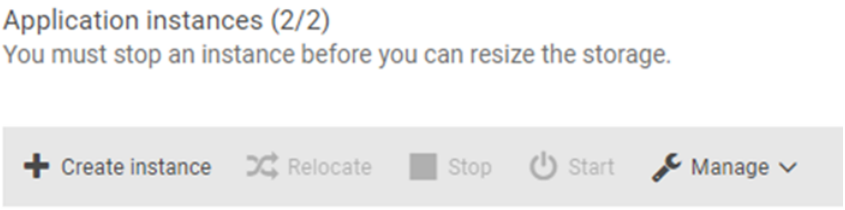
`MSDP_SERVER=<MSDP hostname>`

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.



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 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 or Cloud Catalyst storage, Veritas recommends that you tune the `MaxCacheSize` according to the following guidelines:

- On each instance, allocate .75 GB to 1 GB of RAM for each TiB of storage that is allocated to deduplication on the instance. For example, if the storage pool has 80 TiB allocated, the `MaxCacheSize` should be 60 GB to 80 GB of RAM.
- The sum of the `MaxCacheSize` for all instances with deduplication or Cloud Catalyst storage should not exceed 70% of the physical RAM on the appliance.

To tune the deduplication `MaxCacheSize` on this instance:

- From the SSH session, run the following command on the instance:

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

  Where *<percent%>* is the percentage of the appliance RAM to use for the cache on the instance.
- Restart the `dedupe` process with the following commands:

  ```
  dedupe MSDP stop
  dedupe MSDP start
  ```

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

- From the NetBackup Administration Console, select either **NetBackup Management** or **Media and Device Management**, then click **Configure Disk Pool** in the right pane. Follow the prompts to configure the disk pool.
- 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 Do one of the following to create a deduplication storage unit for your instance:

- From the NetBackup Administration Console, expand **NetBackup Management** > **Storage** > **Storage Units**, then click **New** > **Storage Unit**. Complete the fields and select the **Use WORM** check box.
- 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.

Chapter 5

Managing NetBackup application instances

This chapter includes the following topics:

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.

Note that the following NetBackup features are not supported on application instances:

- Bare Metal Restore boot servers
- IPv6

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@ssw0rd**

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 media server application instance" on page 34.

Managing users on a primary or 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 media server instance" on page 30.
  See "Changing a user password on a primary or media server instance" on page 34.
- Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users
  See "Connecting an Active Directory user domain to a primary or a media server instance" on page 31.

Adding and removing local users on a primary or 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/sssd/sssd.conf` on the instance and locate the following section:

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

- Add the following directive to this section:

```
enumerate = True
```

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

---

7 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. See the *NetBackup Web UI Security Administrator's Guide* for details.

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

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

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

To connect an LDAP user domain

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

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

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

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

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

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

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

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

- `ldap_uri =`
  Enter the LDAP server name and port. If you want to enable SSL for the connection, use port 636. If you do not want to enable SSL, use port 389.
  For example: `ldap_uri = ldaps://example.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 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. See the *NetBackup Web UI Security Administrator's Guide* for details.

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

Changing a user password on a primary or 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.

Running NetBackup commands on a primary or 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 media server application instance" on page 36.
- `/opt/veritas/vxapp-manage/cp-nbu-notify`
  See "Installing NetBackup notify scripts on a primary or media server application instance" on page 37.
- `/usr/openv/netbackup/bin`*
- `/usr/openv/netbackup/bin/admincmd`*
- `/usr/openv/netbackup/bin/goodies`*
- `/usr/openv/netbackup/bin/support`*
- `/usr/openv/volmgr/bin`*
- `/usr/openv/volmgr/bin/goodies`*

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

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

For example:

```
sudo -i bpps
```

Commands on media servers only

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

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

- /usr/sbin/umount.nfs
- /usr/sbin/umount.nfs4

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

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

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

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

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

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

To create or edit a touch configuration file

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

   For example:

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

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

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

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

   For example:

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

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

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

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

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

To install or edit a NetBackup notify script

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

   For example:

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

3 Make changes to the file in the home directory.

4 Run the following command to install the modified file in its original location:

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

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

For example:

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

Monitoring NetBackup services on a 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 Administration Console, use the **Backup Policy Configuration Wizard** 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 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.

   For example, if you need to store SSH `authorized_key` files on the instance, you can make the following directory:

   ```
   sudo mkdir /mnt/nblogs/authorized_keys
   ```

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.

   In the `authorized_keys` example, you can create the following subdirectory to store a specific user's `authorized_key` file:

   ```
   sudo mkdir /mnt/nblogs/authorized_keys/example_user
   ```

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/openv/var/global/nbdeployutilconfig.txt`

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

Disabling SMB server signing on a media server instance

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

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

To disable SMB server signing

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

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

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

   ```
   server signing = mandatory
   ```

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

   ```
   sudo systemctl restart smb
   ```

Establishing trust with a NetBackup 7.7.3 primary server instance

To establish a trust relationship between a later version primary server instance and a NetBackup 7.7.3 primary server instance, you must perform the following steps.

To establish trust with a NetBackup 7.7.3 primary server instance

1. Log in to the instance as the **appadmin** user and use the following command to enable the **root** account and set the password:

   ```
   sudo passwd
   ```

   Warning: The **root** account is a restricted user account that can put the system at risk. It should only be enabled during configuration procedures or under the direct supervision of Veritas Technical Support.

2. Establish trust between the source and the target domains. Use the **root** account to add the 7.7.3 instance as a trusted primary server. Refer to the NetBackup documentation for specific instructions.
3. Run the following command on the instance to disable the **root** account:

   ```
   sudo passwd -l root
   ```

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 WORM storage server 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 WORM storage shell, you can run commands to manage the instance and your WORM storage. See "About the NetBackup WORM storage server shell" on page 43.

About the NetBackup WORM storage server shell

Use the NetBackup WORM storage server shell to configure the immutable and indelible data from your Veritas Appliance. The interface provides tab-completed command options.

These are the main categories of commands:

- `dedupe`

This command lets you manage the deduplication service.
See "About the dedupe command" on page 44.

- `retention`
  This command lets you manage image retention.
  See "About the retention command" on page 46.
- `setting`
  This command lets you manage the deduplication and the system configuration settings.
  See "About the setting command" on page 47.
- `support`
  This command lets you access and upload the relevant logs and configuration files for troubleshooting.
  See "About the support command" on page 60.

About the dedupe command

The `dedupe` commands lets you manage the deduplication services.

The following table describes the options and arguments for the `dedupe` command.

Table 5-1 The options and arguments for the `dedupe` command.

Option and its description	Argument	Description
`CRC` Check and manage the deduplication CRC service.	`state`	Display the state of the CRC checking services.
	`enable`	Enable the CRC checking services.
	`enable-fixmode`	Enable the CRC checking services with a fix mode.
	`disable-fixmode`	Disable the fix mode of the CRC checking services.
	`disable`	Disable the CRC checking services.
	`fast`	Restart the CRC checking services in a mode.
	`fixmode-state`	Display the state of the fix mode of the CRC checking services.

Table 5-1 The options and arguments for the `dedupe` command. *(continued)*

Option and its description	Argument	Description
`CRQP` Manage the transaction log (`Tlog`) process service.	`status`	Display the status of the CRQP services.
	`start`	Start the CRQP services.
	`info`	Show the CRQP services information.
`online-check` Manage online checking services.	`enable`	Enable the online checking services.
	`status`	Display the status of the online checking services.
	`disable`	Disable the online checking services.
`compaction` Manage the MSDP compaction service.	`start`	Start the deduplication compaction services.
	`state`	Display the status of the deduplication compaction services.
	`disable`	Disable the deduplication compaction services.
	`enable`	Enable the deduplication compaction services.
`MSDP` Manage the MSDP services.	`start`	Start the deduplication (MSDP) services.
	`status`	Display the status of the deduplication (MSDP) services.
	`stop`	Stop the deduplication (MSDP) services.
`spws` Manage the Storage Platform Web Service (SPWS).	`start`	Start the SPWS.
	`status`	Display the status of the SPWS.
	`stop`	Stop the SPWS.
`vpfs` Manage the Veritas provisioning file system (VPFS) mounts.	`start`	Start the VPFS mounts.
	`status`	Display the status of the VPFS mounts.
	`stop`	Stop the VPFS mounts.

Stopping and starting the MSDP services

To stop the MSDP services:

1. Check the health monitor status using the following command:

   ```
   setting health status
   ```

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

   ```
   setting health disable
   ```

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

   ```
   dedupe MSDP stop
   ```

To start the MSDP services:

1. Start the MSDP services using the following command:

   ```
   dedupe MSDP start
   ```

2. Start the health monitor using the following command:

   ```
   setting health enable
   ```

About the retention command

The `retention` command lets you manage image retention.

The following table describes the options and arguments for the `retention` command.

Table 5-2 The options and arguments for the `retention` command.

Option and its description	Argument	Description
`policy` The backup policy to use for the image retention with a retention lock.	`list`	List the images that have a retention lock.
	`audit`	Display the audit information for the images with a retention lock.
	`disable`	Disable the image retention using the backup ID of the image. For example: `retention policy disable backup_ID=<test_123> copynumber=<number>` You can find the backup ID and the copy number in the output of the `retention policy list` command.

About the setting command

Thie `setting` command lets you manage the deduplication and system configuration settings.

The following table describes the options and arguments for the `setting` command.

Table 5-3 The options and arguments for the `setting` command.

Option and its description	Argument	Description
`certificate` Configure settings for CA certificates.	`remove-enrollment`	Remove the external certificate details with respect to the specified primary server from the local certificate store.
	`get-external-certificates`	Download and replace the external certificates. This command requires the following parameters: ■ `private_key` Enter the RSA private key of the host certificate. ■ `cert` Enter the X.509 certificate of the host in PEM format. ■ `scp_host` Specify the host that stores the external certificates. ■ `scp_port` Specify the port to connect to on the remote host. ■ `passphrase` Enter the passphrase of the RSA private key if the key is encrypted.
	`set-CRL-check-level`	Set the revocation check level for the external certificates. Use the `check_level` parameter to enter the value for the revocation check level.
	`show-CA-cert-detail`	Display the NetBackup CA certificate details of the specified primary server.
	`get-CA-certificate`	

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
		Obtain the NetBackup CA certificate from the primary server. By default, the command uses the first primary server entry in the NetBackup configuration file. You can specify an alternate primary server using the `primary_server` parameter. For example: `setting certificate get-CA-certificate primary_server` *`alternate primary server`*
	`external-CA-health-check`	Verify the entered certificates, RSA keys, and the trust store.
	`disable-CA`	Disable the NetBackup CA support from this NetBackup host. Use the host ID and the CA fingerprint of the NetBackup host whose CA you want to disable. For example: `setting certificate disable-CA host_ID` *`specify hostID`* `cafp` *`host CA fingerprint`*
	`install-external-certificates`	

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
		Download and install the external CA certificates. This command requires the following parameters: ■ `private_key` Enter the RSA private key of the host certificate. ■ `cert` Enter the X.509 certificate of the host in PEM format. ■ `scp_host` Specify the host that stores the external certificates. ■ `scp_port` Specify the port to connect to on the remote host. ■ `cacert` Enter the external CA trust store in PEM format. ■ `passphrase` Enter the passphrase of the RSA private key if the key is encrypted.
	`list-certificates`	List details of all the security certificates that are available on the NetBackup host.
	`list-CA-cert-details`	List the CA details from the local NetBackup trust store.
	`show-CRL-check-level`	Retrieve the revocation check level for the external certificates.
	`get-external-CA-certificate`	

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
		Download and install the external CA certificate. This command requires the following parameters: ■ `scp_host` Specify the host that stores the external certificates. ■ `scp_port` Specify the port to connect to on the remote host. ■ `cacert` Enter the external CA trust store in PEM format.
	`get-certificate`	Request a NetBackup certificate for the host from the primary server. This command requires the following parameters: ■ `primary_server` Specify an alternate primary server. By default, this command uses the first primary server entry in the NetBackup configuration file. ■ `force=true` Overwrite the certificate if it already exists. ■ `token` Securely enter an authorization token if the command prompts that a token is required for the request.
	`list-enrollment-status`	Retrieve the enrollment status of the associated primary servers from the local certificate store.
	`host-self-check`	Verify whether the host certificate is in the certificate revocation list.
	`show-external-CA-cert-detail`	Display the External CA certificate details of the specified primary server.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`FIPS` Manage FIPS settings.	`disable`	Disable FIPS in MSDP.
	`enable`	Enable FIPS in MSDP.
	`status`	Display the status of FIPS in MSDP.
`MSDP-VLAN` Configure the settings for MSDP VLAN.	`add`	Add a VLAN for the NetBackup WORM storage server. Use the `interface` parameter to enter the IP address for the VLAN that you want to add.
	`remove`	Remove a VLAN for the NetBackup WORM storage server. Use the `interface` parameter to enter the IP address for the VLAN that you want to remove.
	`list`	List all the VLANs for the NetBackup WORM storage server.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`user` Configure the settings for the SSH user.	`show-password-exp-date`	Display the password expiration date of the user. Use the `username` parameter to display the password expiration date of the user.
	`change-password`	Change the password for a user. This command requires the following parameters: ■ `username` Enter the username to change its password. ■ `password` Enter the password for the user. The password must have characters between 15 but not greater than 32. The password requires at least one uppercase character, one lowercase character, one number, and one special character (`_, ., /, @, *, !, %, #, &`).
	`random-password`	Generate a random password.
	`show-user`	Display the user information. Use the `username` parameter to display the information of that user.
	`set-password-exp-date`	Set the expiration date for the user password. This command requires the following parameters: ■ `username` Enter the username to set the user's password expiration date. ■ `password_exp_date` Set a password expiration date in the **YYYY-MM-DD** format.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
	`delete-user`	Disable an SSH user. Use the `username` parameter to disable the user.
	`list-users`	List all the SSH users.
	`add-user`	Create an SSH user. This command requires the following parameters: ■ `username` Enter the username of the new user. ■ `password` Enter the password for the newuser that you want to create. The password must have characters between 4 but not greater than 30. The characters can be uppercase (A-Z), lowercase letters (a-z), numbers (0-9), and special characters (`_, ., /, @, *, !, %, #, &`).
`network` Configure the network settings.	`ping`	Ping the network for a connection status. Use the `ip` parameter to enter the IP address of the network to check the connection status.
	`ifconfig`	Display the IP address of the network.
	`route`	Display the network route information.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`WORM` Configure the settings for immutable and indelible storage.	`status`	Display the status of WORM storage.
	`set-max`	Specify the maximum duration to keep the storage immutable and indelible. Use the `worm_max` parameter to specify the maximum duration in seconds to keep the storage immutable and indelible (WORM).
	`set-min`	Specify the minimum duration to keep the storage immutable and indelible. Use the `worm_min` parameter to specify the minimum duration in seconds to keep the storage immutable and indelible (WORM).
	`show-mode`	Display the WORM mode.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`set-MSDP-param` Set the parameters in the MSDP configuration files.	`write-thread-num`	Get and set the <`WriteThreadNum`> parameter. Use the `value` parameter to enter the value that is used by the MSDP parameters.
	`spoold-logging`	Get and set the <`SpooldLogging`> parameter.
	`allocation-unit-size`	Get and set the <`AllocationUnitSize`> parameter.
	`data-check-days`	Get and set the <`DataCheckDays`> parameter.
	`max-fp-cache-size`	Get and set the <`MaxFPCacheSize`> parameter.
	`max-retry-count`	Get and set the <`MaxRetryCount`> parameter.
	`spad-logging`	Get and set the <`SpadLogging`> parameter.
	`log-retention`	Get and set the <`LogRetention`> parameter.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`get-MSDP-param` Get the parameters from the MSDP configuration files.	`write-thread-num`	Get and set the <`WriteThreadNum`> parameter.
	`spoold-logging`	Get and set the <`SpooldLogging`> parameter.
	`allocation-unit-size`	Get and set the <`AllocationUnitSize`> parameter.
	`data-check-days`	Get and set the <`DataCheckDays`> parameter.
	`max-fp-cache-size`	Get and set the <`MaxFPCacheSize`> parameter.
	`max-retry-count`	Get and set the <`MaxRetryCount`> parameter.
	`spad-logging`	Get and set the <`SpadLogging`> parameter.
	`log-retention`	Get and set the <`LogRetention`> parameter.
`MSDP-user` Configure the settings for the MSDP user.	`random-password`	Generate a random password.
	`list`	List all the MSDP users.
	`verify-user`	Verify user password and user role.
	`add-MSDP-user`	Create an MSDP user.
	`reset-password`	Reset the password for the MSDP user.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`encryption` Configure the settings for MSDP encryption.	`enable-kms`	Enable KMS for MSDP. This command requires the following parameters: ■ `kms_server` Enter the hostname of the KMS server. ■ `key_group` Enter the KMS key group name..
	`status`	Display the current encryption status.
	`enable`	Enable encryption for MSDP.
	`kms-status`	Display the current KMS status.
`kernel` Get the information about the kernel.	`search-param`	Search for a keyword in the kernel parameters. Use the `keyword` to specify a keyword to search in the keyword parameters.
`nginx` Manage the NGINX service.	`start`	Start the NGINX service.
	`config-self-signed-cert`	Create and configure a self-signed certificate.
	`show-cert`	Show details of the SSL certificate that is configured with NGINX.
	`status`	Check the status of the NGINX service.
	`stop`	Stop the NGINX service.

Table 5-3 The options and arguments for the `setting` command. *(continued)*

Option and its description	Argument	Description
`samba` Manage the Samba service.	`start`	Start the Samba service.
	`add-user`	Add a local Samba user or change the password of an existing local Samba user.
	`remove-user`	Remove a local Samba user.
	`list-users`	Display all local Samba users.
	`status`	Check the status of the Samba service.
	`stop`	Stop the Samba service.
`ActiveDirectory` Connect or disconnect from an Active Directory (AD) user domain.	`configure`	Configure AD user authentication and connect to an AD domain. This command requires the following parameters: ■ `ad_server` Specify the AD server name. ■ `domain_admin` Specify the username of the AD administrator. ■ `domain` Specify the AD domain name.
	`unconfigure`	Unconfigure AD user authentication and disconnect from an AD domain. This command requires the following parameters: ■ `ad_server` Specify the AD server name. ■ `domain_admin` Specify the username of the AD administrator. ■ `domain` Specify the AD domain name.

About the support command

The `support` command lets you access and upload the relevant logs and configuration files for troubleshooting.

The following table describes the options and arguments for the `support` command.

Table 5-4 The options and arguments for the `support` command.

Option and its description	Argument	Description
`MSDP-history` Access the MSDP history files.	`tail`	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
	`collect`	Collect files for transferring to the target host. This command requires the following parameters: ■ `mmin` Find files that are modified `n` minutes ago. Same as `mmin` option in find command. For example, 15, +15, -15. ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. ■ `mtime` Finds files that are modified `n*24` hours ago. Same as `mtime` option in find command. For example, 2, +2, -2.
	`ls`	List information about the FILEs. Use the `dir` parameter to enter the directory name.
	`scp`	

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ `scp_port` Specifies the port to connect to on the remote host. ■ `scp_target` Specifies the target host and path for transferring files. Use the `user@host:/directory path/` format. This is a required parameter.
	`cat`	Concatenate files and print on the standard output. Use the `file` parameter to enter the file name.
	`grep`	Print lines that match patterns. This command requires the following parameters: ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. This is a required parameter. ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`process` Displays information about the MSDP processes.	`MSDP-process`	Display the MSDP processes.
	`htop`	Display the CPU and memory information.
	`atop`	Display information about the operating system.
	`pidstat`	Display the PID statistics.
	`memory-usage`	Displays the free and used memory.
`software` Displays information about the software.	`show-MSDP-version`	Display the MSDP version.
	`show-OS-version`	Display the operating system information.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`MSDP-log` Access the MSDP log files.	`tail`	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
	`collect`	Collect files for transferring to the target host. This command requires the following parameters: ■ `mmin` Find files that are modified `n` minutes ago. Same as `mmin` option in find command. For example, 15, +15, -15. ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. ■ `mtime` Finds files that are modified `n*24` hours ago. Same as `mtime` option in find command. For example, 2, +2, -2.
	`ls`	List information about the files. Use the `dir` parameter to enter the directory name.
	`scp`	

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ `scp_port` Specifies the port to connect to on the remote host. ■ `scp_target` Specifies the target host and path for transferring files. Use the `user@host:/directory path/` format. This is a required parameter.
	`cat`	Concatenate files and print on the standard output. Use the `file` parameter to enter the file name.
	`grep`	Print lines that match patterns. This command requires the following parameters: ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. This is a required parameter. ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
`hardware` Displays information about the hardware.	`cpumem`	Display the CPU and memory information.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`MSDP-config` Access the MSDP configuration files.	`tail`	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
	`collect`	Collect files for transferring to the target host. This command requires the following parameters: ■ `mmin` Find files that are modified `n` minutes ago. Same as `mmin` option in find command. For example, 15, +15, -15. ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. ■ `mtime` Finds files that are modified `n*24` hours ago. Same as `mtime` option in find command. For example, 2, +2, -2.
	`ls`	List information about the FILEs. Use the `dir` parameter to enter the directory name.
	`scp`	

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ `scp_port` Specifies the port to connect to on the remote host. ■ `scp_target` Specifies the target host and path for transferring files. Use the `user@host:/directory path/` format. This is a required parameter.
	`cat`	Concatenate files and print on the standard output. Use the `file` parameter to enter the file name.
	`grep`	Print lines that match patterns. This command requires the following parameters: ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. This is a required parameter. ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`diskio` Displays information about the disk I/O.	`iostat`	Displays the information about the disk I/O.
	`vmstat`	Displays the information on the wait on the disk I/O.
	`nmon`	Display the information about the monitor system.
	`disk-volume`	Display information about the disk volume.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`syslogs` Access the system logs.	`tail`	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
	`collect`	Collect files for transferring to the target host. This command requires the following parameters: ■ `mmin` Find files that are modified `n` minutes ago. Same as `mmin` option in find command. For example, 15, +15, -15. ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. ■ `mtime` Finds files that are modified `n*24` hours ago. Same as `mtime` option in find command. For example, 2, +2, -2.
	`ls`	List information about the FILEs. Use the `dir` parameter to enter the directory name.
	`scp`	

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ `scp_port` Specifies the port to connect to on the remote host. ■ `scp_target` Specifies the target host and path for transferring files. Use the `user@host:/directory path/` format. This is a required parameter.
	`cat`	Concatenate files and print on the standard output. Use the `file` parameter to enter the file name.
	`grep`	Print lines that match patterns. This command requires the following parameters: ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. This is a required parameter. ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.

Table 5-4 The options and arguments for the `support` command. *(continued)*

Option and its description	Argument	Description
`proc` Access process information about the pseudo-filesystem.	`tail`	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.
	`ls`	List information about the FILEs. Use the `dir` parameter to enter the directory name.
	`cat`	Concatenate files and print on the standard output. Use the `file` parameter to enter the file name.
	`grep`	Print lines that match patterns. This command requires the following parameters: ■ `pattern` Specify the naming pattern to find and select matching files and folders. For example, `spoold`, or `spad*`. This is a required parameter. ■ `file` Enter the filename. This is a required parameter. ■ `options` Enter the supported options for `grep: -i, -w, -E`, or `tail: -f, -n`.

Here are some examples of the support command usage:

```
support MSDP-log ls dir=spoold
support MSDP-log ls dir=spad/sof1vm08.tec.com/spoold/spad/072320.log
support MSDP-log cat file=pdde-config.log
support MSDP-log cat file=spad/sof1vm08.tec.com/spoold/spad/072320.log
support MSDP-log tail file=pdde-config.log
support MSDP-log tail file=pdde-config.log options="-f"
support MSDP-log tail file=pdde-config.log options="-n 5"
support MSDP-log tail file=spad/sofia11vm08/spoold/spad/072320.log
options="-f -n 5"
support MSDP-log grep file=spad* pattern=sessionStartAgent
options="-r"
support MSDP-log grep file=pdde-setup.log pattern="pid  455"
support MSDP-log grep file=pdde-setup.log pattern="Pid" options="-w
 -i"
support MSDP-log grep file=spoold* pattern="Pid" options="-w -i -r"
support MSDP-log grep file=pdde-setup.log pattern="MSDP-X|PureDisk"
 options="-w -i -r -E"
```

Uploading logs is a two-step process:

- Run the `collect` command for the desired category to collect files of interest. For example:

  ```
  support MSDP-log collect pattern=spoold* mmin="+2"
  support MSDP-history collect
  support MSDP-config collect
  support syslogs collect pattern=crash mmin="-2"
  ```

- Transfer files using `scp` command

  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.

  ```
  support MSDP-config scp scp_target=user@example.com:/tmp
  ```

Configuring an isolated recovery environment on a Flex Appliance WORM storage server instance

You can configure an isolated recovery environment (IRE) on a WORM storage server instance 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 a WORM storage server instance.

Note: This procedure only applies to Flex Appliance version 2.1.1 and later. Veritas recommends that you use version 2.1.1 or later if you want to use this feature. However, a hotfix is also available for version 2.1. To configure an IRE on Flex Appliance 2.1, see the Flex Appliance Isolated Recovery Environment (IRE) Air Gap Solution Deployment Guide.

To configure an IRE

1. Configure Auto Image Replication from the production domain to the IRE domain. Choose the WORM storage server instance as the target storage unit.

   For instructions, see the chapter "Configuring replication" in the *NetBackup Administrator's Guide, Volume 1*.

2. Log in to the WORM storage server shell. Run the following command to show the SLP windows from the primary server to the WORM instance:

   ```
   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.
   - *<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 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.

Note: If an SLP window is greater than 24 hours, `show-slp-windows` may display the duration incorrectly. Environments that have SLP windows greater than 24 hours are not candidates for IRE, as the network would always be open.

---

3 Based on the output for your environment, determine a daily schedule that accommodates the SLP windows and take note of it.

In the previous example, a daily schedule from 10:00 A.M. to 1:00 P.M. accommodates both SLP windows.

Note: The start times in the output of this command are in the production primary server's time zone. If the production environment and the IRE are in different time zones, make sure that you adjust the start times accordingly before you set the air gap schedule.

---

4 Run the following command to configure which subnets and IP addresses are allowed to access the WORM storage server instance:

```
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.

---

5 Run the following command to set the daily air gap schedule:

For example:

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

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

Managing an isolated recovery environment on a Flex Appliance WORM storage server instance

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

- To view the SLP windows from the primary server to the WORM instance:
  `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.
  - *<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 the SLPs and storage units in the IRE.

  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 start times in the output of this command are in the production primary server's time zone. If the production environment and the IRE are in different time zones, make sure that you adjust the start times accordingly if you change the air gap schedule.

- To view the allowed IP addresses and subnets:
  `setting ire-network-control show-allows`
- 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.

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

- 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
  ```