Disaster Recovery for NetBackup™ Cloud Catalyst

Release: 8.1

VERITAS™

Veritas NetBackup™ Cloud Catalyst Disaster Recovery

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Disaster recovery when Cloud Catalyst is enabled

This document includes the following topics:

About NetBackup Cloud Catalyst

NetBackup 8.1 introduces Cloud Catalyst, which uses MSDP deduplication technology to upload deduplicated data to the cloud. The data is uploaded by a Cloud Catalyst storage server, which first stores data in a local cache before uploading it to cloud storage. This cloud storage server is a dedicated host that can be either a NetBackup appliance or a media server configured for NetBackup Cloud Catalyst.

Cloud Catalyst configuration information is included in the *NetBackup Deduplication Guide*:

http://www.veritas.com/docs/DOC5332

About disaster recovery for NetBackup Cloud Catalyst

The following topics describe disaster recovery procedures in environments where NetBackup Cloud Catalyst is used. NetBackup Cloud Catalyst uses a media server that is configured as a Cloud Catalyst storage server for deduplication to the cloud.

Both procedures assume that an MSDP catalog backup exists.

Both procedures recover the MSDP cloud storage server, whether it was an appliance or a non-appliance host.

- See "Recovering only the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled" on page 5.
  This procedure recovers the host that was configured as the MSDP cloud storage server. This procedure does not include recovery of the master server.
- See "Recovering the master server (partial) and the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled" on page 9.
  This procedure recovers the MSDP cloud storage server without fully recovering the master server.
  If KMS encryption was configured, a master server NetBackup catalog recovery is required to recover the KMS encryption keys. After performing the NetBackup catalog recovery, recover the MSDP cloud storage server as described in the following procedure:
  See "Recovering only the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled" on page 5.

Note: The `drcontrol` command is used in several recovery steps. The command creates logs in the following directory:

`/var/log/puredisk/drcontrol/`

Recovering only the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled

Use this procedure to recover the host that was configured as the MSDP cloud storage server in a NetBackup Cloud Catalyst scenario. This procedure recovers the MSDP cloud storage server, whether it is an appliance or a non-appliance host.

This procedure assumes the following:

- That the master server is still operational.

- That an MSDP catalog backup exists.
- If swapping in a new host, the host name is the same as the name of the previous host.

1. Install NetBackup on the MSDP cloud storage server.
2. Deploy a host name-based security certificate for the MSDP cloud storage server:
   - Run the following command on the master server:
     `bpnbaz -ProvisionCert media_server_name`
     Restart the services on the MSDP cloud storage server after generating a certificate.
   - Run the following on the MSDP cloud storage server:
     `nbcertcmd -getCACertificate`
3. On the MSDP cloud storage server, edit the `esfs_init.sh` file, located in the following directory:

   `/usr/openv/esfs/scripts/esfs_init.sh`

   Add the `readonly` option to the MKESFS call. This assures that the data can be read for restores, but that no new backups are written to the media server. The option also assures that no existing backup images are expired or deleted.

   For example:

   ```
   $MKESFS -o readonly,cache_dir="$CACHEDIR",storage_server=$CLDSRV,
   fs_name=$FSNAME,media_server=$MEDIA,master_server=$MASTER,
   fs_version=$FSVERSION | tee -a "$LOGFILE")
   ```

   Notes on the readonly option:

   - If future duplication or backup jobs try to write to this media server, the job fails with status code 84 (media write error), because the storage is set to `readonly`.
   - The `readonly` option can be removed at a later date to allow the MSDP cloud storage server to once again be used for duplication or backup jobs. However, the best approach is to create a new MSDP cloud storage server for this purpose and to keep this recovered MSDP cloud storage server in a `readonly` mode until the data is no longer needed and it can be retired.
     The `readonly` option is configured in the `esfs.json` file.
     After changing the `readonly` option, you must restart `vxesfsd`.
4. On the MSDP cloud storage server, call `esfs_init.sh` manually, using the following options:

```
/usr/openv/esfs/scripts/esfs_init.sh
--cacheDir=/cache_directory/cache
--mountPath=/cache_directory/storage --fsName=ESFS1
--cloudServer=cloud_server --masterServer=master_name
--mediaServer= media_name
```

Where *cloud_server* is in the format *cloud_type:storage_server_name*. For example:

- *cloud_type* is `amazon_cryptd` (Amazon S3 encryption enabled) or `amazon_rawd` (Amazon S3 with no encryption).
- *storage_server_name* is the name given by the user.

You need to identify the following values before `esfs_init.sh` is executed and they must have the correct values to reinitialize ESFS as it was before:

- *cache_directory*: The absolute path where CloudCatalyst was originally configured. The folder name is `cache`.
- `mountPath`: The absolute path where CloudCatalyst was originally configured. The folder name is `storage`.
- `fsName=ESFS1 --cloudServer=`*`cloud_server`*: The name of the storage server that is created when Cloud Catalyst was originally configured.
- `masterServer=`*`master_name`* `--mediaServer= `*`media_name`*: The Cloud Catalyst media server name.

There may be a file on the Cloud Catalyst Server that contains these values. You can reference the file to confirm the values you use when `esfs_init.sh` is executed. The file is located in `/usr/openv/esfs/log/ops/` and is called `esfs-config-log`.

Note: This procedure assumes that the `--cacheDir` and `--mountPath` options use the same root path. For example, `$ROOTPATH/cache` and `$ROOTPATH/storage`.

---

5. On the MSDP cloud storage server, call `PDDE_initConfig.sh` manually, using the following options:

```
/usr/openv/pdde/pdconfigure/scripts/installers/PDDE_initConfig.sh
--storagepath=/cache_directory/storage --spalogin=cloud_username
--spapasswd=cloud_password --spalogretention=90
--verboselevel=3 --dbpath=/cache_directory/storage --dedupetocloud=true
--spalogpath=/cache_directory/storage/log --storagepoolid=any_value
--installpath=/usr/openv/pdde
```

For Amazon, the `spalogin=cloud_username` is the **Access key ID** that is entered into the cloud storage server wizard. The `spapasswd=cloud_password` is the **Secret access key**.

The `--storagepoolid=any_value` option is overwritten by the recovery process. Any number can be used at this point.

For example:

```
/usr/openv/pdde/pdconfigure/scripts/installers/PDDE_initConfig.sh
--storagepath=/msdpc/storage --spalogin=SEI3O2VOOJS8EJIVIJNG
--spapasswd=EIJFOBROPOPJPO3KPO5MBGL7IJNLLM
--spalogretention=90 --verboselevel=3 --dbpath=/msdpc/storage
--dedupetocloud=true
--spalogpath=/msdpc/storage/log --storagepoolid=1193
--installpath=/usr/openv/pdde
```

Note: This procedure assumes that the `--storagepath` option uses the same root path as `--cacheDir` and `--mountPath`.

As a result of this step, you may see error messages in the output. However, these errors do not affect the disaster recovery process. For example:

```
Fri Jul 21 00:38:38 CDT 2017    * Linked to
/MSDP/d2c_cache/storage/etc/pdregistry.cfg *
Fri Jul 21 00:38:38 CDT 2017 **** Done creating pdregistry.cfg ****
Failed to open input file:
/MSDP/CCat_cache/storage/etc/puredisk/agent.cfg
Failed to load file, error is -4, Since this is writing,
continue to write
the config file: /MSDP/CCat_cache/storage/etc/puredisk/agent.cfg
Fri Jul 21 00:38:39 CDT 2017 **** Init Database Path ***
Fri Jul 21 00:38:39 CDT 2017 **** Done Init Database Path ***
```

6. On the MSDP cloud storage server, run the `setlsu_ioctl` command to set the bucket name.

Note: The `cloud.lsu` file does not need to exist to run this command.

```
/usr/openv/esfs/bin/setlsu_ioctl
/cache_directory/storage/proc/cloud.lsu <name_of bucket>
```

7. On the MSDP cloud storage server, run the `drcontrol` command with the following options to recover the MSDP catalog from the most recent backup image:

   ```
   /usr/openv/pdde/pdcr/bin/drcontrol --auto_recover_DR --policy
   MSDP_policy_name --disk_pool disk_pool_name
   ```

8. In the **NetBackup Administration Console**, navigate to the **Catalog** utility. Run a Verify operation on an existing backup image.

   The Verify operation should verify the following:

   - That the data has been downloaded from the cloud.
   - That the image is available for restore.

9. Some time after verifying that the recovery operation is successful, you can reclaim some disk space by removing saved MDSP catalog directories that were created during the recovery process. To do so, run the following command:

   ```
   /usr/openv/pdde/pdcr/bin/drcontrol --cleanup
   ```

Recovering the master server (partial) and the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled

Use this procedure to recover the host that was configured as the MSDP cloud storage server when the master server has been lost and then reinstalled from scratch without a NetBackup catalog recovery being performed.

If possible, a NetBackup catalog recovery should be performed for the master server, after which the following procedure is performed:

See "Recovering only the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled" on page 5.

Note: This procedure recovers the MSDP cloud storage server without fully recovering the master server. Therefore, if KMS encryption was configured, a master server NetBackup catalog recovery is required to recover the KMS encryption keys.

After performing the NetBackup catalog recovery, recover the MSDP cloud storage server as described in the following topic:

See "Recovering only the MSDP cloud storage server when NetBackup Cloud Catalyst is enabled" on page 5.

This procedure assumes the following:

- That an MSDP catalog backup exists.
- If swapping in a new host, the host name is the same as the name of the previous host.

1. Install NetBackup on the master server.
2. Install NetBackup on the MSDP cloud storage server.
3. Deploy a host name-based security certificate for the MSDP cloud storage server:
   - Run the following command on the master server:
     `bpnbaz -ProvisionCert` *`media_server_name`*
     Restart the services on the MSDP cloud storage server after generating a certificate.
   - Run the following on the MSDP cloud storage server:
     `nbcertcmd -getCACertificate`
4. On the MSDP cloud storage server, edit the `esfs_init.sh` file, located in the following directory:

   `/usr/openv/esfs/scripts/esfs_init.sh`

   Add the `readonly` option to the MKESFS call. This assures that the data can be read for restores, but that no new backups are written to the media server. The option also assures that no existing backup images are expired or deleted.

   For example:

   ```
   $MKESFS -o readonly,cache_dir="$CACHEDIR",storage_server=$CLDSRV,
   fs_name=$FSNAME,media_server=$MEDIA,master_server=$MASTER,
   fs_version=$FSVERSION | tee -a "$LOGFILE")
   ```

   Notes on the readonly option:

   - If future duplication or backup jobs try to write to this media server, the job fails with status code 84 (media write error), because the storage is set to `readonly`.
   - The `readonly` option can be removed at a later date to allow the MSDP cloud storage server to once again be used for duplication or backup jobs. However, the best approach is to create a new MSDP cloud storage server for this purpose and to keep this recovered server in a `readonly` mode until the data is no longer needed and it can be retired.
     The `readonly` option is configured in the `esfs.json` file.
     After changing the `readonly` option, you must restart `vxesfsd`.

5. In the **NetBackup Administration Console** on the master server, navigate to the **Catalog** utility. Import the images that were created by the MSDP catalog policy from the storage unit where they were saved. (That is, the MSDP catalog backup policy that was originally created using the `drcontrol --new_policy` command.)
6. Configure the MSDP cloud storage server.
   - If the MSDP cloud storage server is a non-appliance media server:
     - In the **NetBackup Administration Console**, click **Configure Cloud Storage Servers** to launch the Cloud Storage Server Configuration Wizard.
     - Be sure to enable the option **Enable NetBackup Cloud Catalyst**.
   - If the MSDP cloud storage server is a Cloud Catalyst Appliance:
     - Perform the initial configuration on the appliance.
     - From the main shell menu, launch the Appliance Cloud Storage Server Configuration Wizard.
7. On the MSDP cloud storage server, use the `drcontrol` command to create an MSDP catalog policy if such a policy does not already exist.

   Run the following command. For *catalog_policy_name*, use the same name as the original catalog policy:

   `drcontrol --new_policy` *`catalog_policy_name`*
8. On the MSDP cloud storage server, run the following command:

   `drcontrol --initialize_DR --policy` *`MSDP_policy_name`*
9. Recover the MSDP cloud storage server files and the FSDB database. Run the following command:

   `drcontrol --recover_last_cloud_catalyst_image --policy` *`MSDP_policy_name`*
10. Delete the old files that are not relevant for the recovered MSDP cloud storage server. Run the following command:

    `drcontrol --delete_old_files_for_cloud_catalyst --policy` *`MSDP_policy_name`*
11. Use the **Backup, Archive, and Restore** client interface to restore the files and directories protected by the MSDP catalog policy (*`MSDP_policy_name`* in the previous steps), except for the cache directory.

    That is, select `/`*`cache_directory`*`/storage` and `/usr` for restore, but do not select `/`*`cache_directory`*`/cache` for restore.

12. Start `spad` on the MSDP cloud storage server by running the following command:

    ```
    /usr/openv/pdde/pdconfigure/pdde spad start
    ```

13. Recover the MSDP catalog from the catalog shadow files by running the following command on the MSDP cloud storage server:

    ```
    /usr/openv/pdde/pdcr/bin/cacontrol --catalog disaster_recovery
    ```

14. Start `spoold` on the MSDP cloud storage server by running the following command:

    ```
    /usr/openv/pdde/pdconfigure/pdde spoold start
    ```

15. In the **NetBackup Administration Console** on the master server, navigate to the **Catalog** utility. Import the images from the MSDP cloud storage server to make the images available for restore.

16. Use the **Catalog** utility to run a Verify operation on an existing backup image.

    The Verify operation should verify the following:

    - That the data has been downloaded from the cloud.
    - That the image is available for restore.

17. Some time after verifying that the recovery operation is successful, you can reclaim some disk space by removing saved MDSP catalog directories that were created during the recovery process. To do so, run the following command:

    ```
    /usr/openv/pdde/pdcr/bin/drcontrol --cleanup
    ```