Quantum®

DXi Cloud Share

Best Practices Guide

6-69104-01 Rev A

DXi Cloud Share Best Practices Guide

Contents

Overview 2

Terminology 3

Set up 3

Application Vendor Support 3

Veritas NetBackup 4

Veritas BackupExec OST 4

Veeam 4

Cloud Operation 6

Cloud Provider 6

Archive 6

Restore 6

Release 7

Reclaim 7

Deleting Shares 7

SYSCLI Cloud Operation 7

Overview

This document will provide best practices for using the Cloud Share feature released with DXi version 4.9. Cloud Share is supported on most appliances (details in user manual). Cloud Share allows DXi systems to store deduplicated backup data sets to any S3 compliant public or private cloud. Check the user guide for S3 targets that have been verified. Most S3 compliant storage devices will be accessible.

This document will be a living document that changes in the future as new information is learned and new features are added to Cloud Share.

The Cloud Share feature is only supported on NAS Shares, Application Specific Shares, and OST LSUs.

Terminology

For the sake of simplifying this document, the following terms will be defined:

- Share(s): Unless explicitly stated as NAS Share(s), the term share(s) shall be taken to mean NAS share(s) (SMB/CIFS, NFS), Application Specific shares, and/or OST LSU(s).
- Cloud: general term to mean your S3 provider. Could be local or over the internet.

Set up

See the DXi Users Guide for details on configuring Cloud Share. Key points to note:

- HTTP/HTTPS port access needs to be allowed between the DXi and S3 Cloud provider.
- A bucket must be created on your Cloud Provider and the Endpoint (default is Amazon S3 US East), Key Id, and Secret Key known.
- The cloud provider's Endpoint region/locality should be the closest possible to the DXi source with the lowest possible latency.
- QOS should be carefully considered from the corporate WAN link to the cloud provider to ensure best possible connectivity to and from the buckets.
- NTP needs to be enabled.
- Application Environment needs to be configured to enable Cloud Share.
- A Cloud share is NOT compatible with DXi Replication (Shares, OST AIR, OST OpDup.) Replication will work on other shares on the appliance, of course.
- For 4.x systems (4800/9000/9100) Cloud Share is not compatible with Increased Stream Count (ISC) or Dynamic Application Environment (DAE).
- Copies between DXi shares, which can be scheduled within the GUI, are compatible with Cloud Share.

Application Vendor Support

Because different Application Vendors have different requirements and uses of their backup files written to disk, it is possible not all applications will be supported because the application is unaware the entire file is not available on the cloud share. The DXi 4.9 release has been tested with Veritas NetBackup, Veritas BackupExec OST, and Veeam.

Veritas NetBackup

NetBackup OST and NAS have been tested and have no special considerations. Select all the files created for a backup when restoring the files from cloud to do a restore from NetBackup.

Veritas BackupExec OST

BackupExec OST has been tested and has no special considerations. Select all the files created for a backup when restoring the files from cloud to do a restore from BackupExec. BackupExec NAS is not supported with DXi 4.9.

Veeam

Two scenarios have been tested with Cloud Share:

1. Veeam Full Backups
   Create an NFS Share on DXi and enter Cloud Share details. This Share will be used as a **VDMS** repository within Veeam. **You must use a unique bucket for each share.** When creating the deduplication repository in Veeam **do not select "fast clone"**.
   This Share will be used for direct Veeam Backups. **Only Virtual Machine full backups are supported.** Incremental backups nor NAS backups (file share, NFS, CIFS, etc) are supported.
   Prior to restoring Virtual Machine backups from the DXi you must restore the images from cloud to the DXi. Failing to do this will result in a Veeam restore failure. You can append full backups to this share until the DXi runs out of resources. This share will honor the retention policies set forth by Veeam Backup & Replication (as long as the time from backup to archive are reasonably close).

2. Create an NFS Share on DXi and do **NOT** enable Cloud Share on it. Perform Virtual Machine backups of any type. Once the backups are complete, use syscli to perform a "server side copy" operation to a cloud enabled share. (this can also

be accomplished via the GUI scheduler, but without the granularity available via the CLI)

```
syscli --copy path --name <sharename> --source <path>
[--destname <sharename>] --dest <path> [--terse]
```

Example where **veeam1** is the source share and **cloud1** is target share (has cloud archive enabled) and **sdbackups1** is the Veeam backup job name:

```
syscli --copy path --name veeam1 --source sdbackups1 --
destname cloud1 --dest sdbackups1 –terse
```

Once the server side copy command completes (it will only be a few moments) you may perform a Cloud Share archive from the copy destination share on the DXi.

In order to do a restore by Veeam in this scenario, there are two options. 1) After data is retrieved from the Cloud via the restore operation, you can do a server side copy to a 3rd NFS Share that is mapped to Veeam and import the backups for Veeam restore, or 2) you can map the destination share that is configured for Cloud to Veeam. But this share MUST not be used for backups (think of this as a Read-Only share.

This "server side copy scenario" will allow for incremental backups, NAS source backups, and fast clone on the non-cloud enabled share.

Other considerations:

Do NOT enable Health Check nor File Polling on a cloud enabled VDMS share. The health check will fail as the files are in the cloud and not on premises.

Memory Usage and Application Environment

The Application Environment feature reserves memory to be specifically used for the feature selected.

Veeam VDMS and Cloud Share are special in that they can be run at the same time. In this case, the memory generally reserved for a single App Environment feature will be divided into two. This means that less streams will be available for each.

Cloud Operation

See the DXi Users Guide for specific information on how the Cloud operations are performed.

Cloud Provider

When creating buckets on your Cloud provider, **buckets must not be configured for Versioning nor have Life Cycle policies enabled. Also, Cloud tiering, like Amazon Glacier, is not supported.**

Data in buckets is stored in a proprietary format and compression. It will not look like the filesystem on the DXi.

Archive

Data from the Share is sent to the Cloud. DXi sends deduplicated data and uses proprietary technology to minimize data sent to the Cloud. Data is transmitted via either HTTP or HTTPS depending on your endpoint.

Tag reference counts are decremented, and the next time Space Reclamation is run, data can possibly be freed from the DXi. **Once data has been archived and Space Reclamation has freed data from the DXi, that data only exists in the Cloud.**

Archive automatically turns off any currently running Space Reclamation and blocks Space Reclamation from running until all archives are finished. Space Reclamation can be turned back on manually via the GUI or CLI. It will be turned back on automatically by a Space Reclamation Scheduler Event. It is recommended to properly schedule the series of backup, archive, and Space Reclamation to handle this restriction. If Space Reclamation has not run for a while, confirm that Space Reclamation and Cloud Share archives do not overlap.

When an archive job is running on a Share, data **MUST NOT** be changed in that Share. If a change occurs, the archive job will immediately fail. So please schedule archive outside of the backup window.

Restore

Restore brings data back from the Cloud to the DXi. You will need free space on the DXi to successfully retrieve the data, and it is recommended to have 10-20% extra free space than the files will consume. DXi Cloud Share works in 2 GB “bundles” thus a retrieve of a smaller amount of data might require more data than the original deduplicated size depending on how many “bundles” need to be retrieved to rehydrate the local files.

Release

Release allows space reclamation to free disk space on the DXi.

Reclaim

Reclaim will compare data on the DXi (at the file level) and data in the Cloud, and remove data in the Cloud that no longer exists on the DXi. This releases cloud space but requires the cloud data to be accessed (which may incur a charge). Space released is based on the 2GB bundles written to cloud so may not be as much as expected.

Deleting Shares

If a Share is deleted on the DXi, the data in the Cloud will NOT be deleted. It is better to remove the data on the DXi Share (via the Vendor Application or connected filesystem) and run Reclaim. If there is a one Share to one Bucket correlation, and the Share has been deleted, the Cloud data can be removed via the Cloud tools.

SYSCLI Cloud Operation

See the SYSCLI Guide for Cloud Share commands.

If a Cloud Share operation is being run via ssh/syscli and the ssh session is closed, that operation will fail. The operation will need to be rerun.

Quantum®

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit www.quantum.com.

www.quantum.com | 800-677-6268