Quantum

DXi Secure Snapshots Best Practices Guide

6-68953-01, Rev. A

Contents

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)** including **SMB/CIFS**, **NFS** and **Application Specific**, and/or **VTL Partition(s)** and/or **OST LSU(s)**.
- **protocol layer(s)**, **protocol(s)**: Unless the specific protocol is explicitly mentioned, the term **protocol layer(s)** shall be taken to mean **SMB/CIFS** and/or **NFS** and/or **Application Specific** and/or **VTL** and/or **OST**.
- **snapshot(s)**: Unless explicitly stated otherwise (e.g. **replication snapshots**), **snapshot(s)** shall be taken to mean **secure snapshot(s)**.
- **destruction of data**: Unless explicitly stated otherwise, **destruction of data** shall be **inadvertent or malicious damage, deletion, or destruction of data**.

Introduction

The DXi Secure Snapshots feature allows the customer to periodically take snapshots of NAS shares, VTLs or OST LSUs. Snapshots may be taken automatically on a scheduled basis, or manually at the CLI.

The DXi attempts to protect the snapshots from modification or deletion.

The customer is free to restore the content of one or more snapshots at any time, for any reason, subject to a few limitations. The restored data can be presented to the client in the same way the original data was.

This is like DXi replication in a way, except it works locally on a single DXi. The Scheduler allows configuration of the snapshot schedule, while the retention period is configurable per share being protected.

Best Practices Summary

The advice in this section serves a summary of the best recommended practices for using DXi Secure Snapshots. It does not intend to replace the detailed discussion in the remainder of the document.

- Set the clock correctly and enable NTP (required). The protection provided by the DXi Secure Snapshots feature is highly dependent on the clock remaining accurate.
- Secure and firewall the DXi. Physical and remote access security is important. Use additional restrictions on the management interface. An attacker with the ability to reach the DXi may be able to gain enough access to destroy data.
- Consider space usage:
    - Enabling DXi Secure Snapshots on a backup share has a similar effect to setting the backup retention period. The snapshot retention period should be added to the configured backup retention to give the total retention period for calculating space usage for the share.
    - Each snapshot also requires a small overhead for its metadata. This should usually be below 200 kiB of raw capacity per GiB of user data in the share for backup application data, which is mostly composed of large archive files. The overhead can grow much larger for general purpose NAS Shares containing many small files.
- The snapshot retention period is the maximum time between ransomware attacking the backup infrastructure and acting after detection. If systems are unattended over weekends or holidays, ensure the period is long enough to account for that.
- Consider the implication of scheduling many snapshot operations concurrently. There is a small but non-zero impact on system performance to take a snapshot.
- Estimate the total number of snapshots which might be retained on the DXi in the steady state for all

shares. This impacts space usage and has some minor performance impacts to consider.

The recommended best practice for scheduling and retaining DXi Secure Snapshots is:

- Schedule snapshots after backup operation(s) are complete. There is usually no benefit to snapshot a share more frequently as the data will either not be changing, or the snapshots will contain partially completed backups.
- Set the snapshot retention period on each share to at least 1 week.
- Take manual snapshots of shares when there becomes a need to retain data for unusual reasons (legal requests, etc.).

Statement of Intentions and Limitations

The DXi Secure Snapshots feature is intended to protect data on the DXi from influences external to the DXi which might cause destruction of data. The feature is intended to:

- Take periodic snapshots of configured dedupe share(s) on a DXi.
- Retain those snapshots for at least the retention period configured on each individual share at the time the snapshot was taken.
- Allow different retention periods on each configured share, as determined by the customer's needs.
- Allow recovering one or more snapshots into shares, should the original share be deleted, or destruction of data be detected.
- Protect its own configuration and snapshots against inadvertent attempts to modify or destroy them.
- Protect its own configuration and snapshots against attempts to modify or destroy them using only the system GUI and/or standard CLI commands.

The feature is not intended or able to:

- Protect non-dedupe shares.
- Serve as a backup of the data on the DXi or replace offsite replication.
- Protect comprehensively against clock changes made by any user with access to set the clock, although NTP is required to be used.
- Protect against a motivated attacker who gains non-protocol access to the DXi and/or finds exploits which cause destruction of data not made available by the protocol layers.
- Protect against any user with the ability to get root access.

Current Limitations:

- Snapshots should be taken when there is no activity, however if there is activity certain files or tapes may not be included correctly.
- Tapes being exported may cause snapshot failures.
- Recovered namespace replications from a source that did not have the secure snapshot feature when the replication was performed may cause errors if they are restored locally.

Restoring snapshots:

- It is not possible to restore a VTL snapshot while cartridges from its original source VTL still exist on the DXi. This is due to a low-level DXi restriction that prevents two cartridges with the same barcode from existing on the DXi at the same time. To restore a VTL snapshot, all cartridges from the original source VTL must be removed from the DXi. The User Interface will present a list of duplicates and fail the operation if restore is attempted while duplicates exist. Non duplicate cartridges will be recovered.

Non-Limitations

The customer has freedom to choose the configuration of the DXi Secure Snapshots feature which best suits their workflow.

There are no arbitrary limits on the following parameters:

- **Enabled Shares**: The customer may snapshot as many or as few shares as required.
- **Snapshot Retention**: The customer is free to set any retention period with the granularity of one day. Retentions periods into thousands of years are possible - albeit impractical.
- **Snapshot Frequency**: The customer is free to schedule snapshots at whatever frequency is permissible by the DXi scheduler in whatever combination of modes they desire. The customer is also free to take manual snapshots from the CLI at any time, as necessary.
- **Total Snapshots**: The upper limit on the number of snapshots is essentially infinite for all practical purposes (it is possible to retain billions of snapshots, should disk space be available to hold them).

Disk space, performance and other practical considerations dictate that the customer should select a reasonable subset of data, retention and frequency to take snapshots in order to balance the protection they require against the disk usage and performance costs of using the feature.

Considerations

There are several considerations that the customer must make before enabling the DXi Secure Snapshots feature. These are outlined within this document.

DXi System Clock

The protection of the DXi Secure Snapshots feature is dependent on the system clock remaining accurate. A clock which is skewing or can be set arbitrarily backwards, and forwards may cause the feature to work improperly or provide an avenue for a malicious attacker to circumvent the protections afforded. Side effects of an inaccurate clock may include preventing snapshots from being taken, preventing snapshots from being deleted (space exhaustion DoS) or causing premature deletion of snapshots (data destruction).

The clock can be adjusted from the console at boot time, remotely through SSH as *root*, *cliadmin*, etc., or from the GUI as any user with administrative rights. The customer should take steps to limit physical and remote access to the DXi.

The customer *must* ensure that DXi is configured to keep its time in sync using NTP. This alleviates many of the concerns about clock skew. The customer should configure NTP to query trusted upstream NTP servers, preferably ones which are under the customer's direct control.

Vulnerabilities

The DXi is subject to disclosed and undisclosed vulnerabilities which may allow a dedicated adversary to attack data on the DXi in several ways.

Quantum continues to work on improving the security of our offering, but it is never possible to be completely certain of the security of any network connected system.

Security/Access Control

The DXi Secure Snapshots feature is designed to protect against the destruction of data on DXi through the protocol layers and through actions taken by a logged-on GUI user or CLI user that is not running as *root*.

A malicious attacker logged onto the DXi may be able to circumvent the protections afforded and cause the destruction of data.

The customer should ensure their DXi is protected as strongly as possible against a malicious attacker gaining access to the console, SSH or GUI. The advice in this section follows the general best practice for limiting access to a machine and using strong authentication mechanisms. The list below is not exhaustive:

- Physical Security
- Limit Console Access (iDRAC should not be connected unless needed, and if needed should be well protected, similarly for third party networked console access).
- Limit Accounts with GUI, SSH Access.
- Use Strong Passwords for Console, GUI and SSH access.
- Replace the default TLS keys with secure customer-generated ones.
- Prefer SSH Keys for SSH authentication.
- Firewall Access to The DXi. If possible, only allow TCP/1062, TCP/80, TCP/443 and TCP/22 to hosts that require it.

Space Usage

Each DXi Secure Snapshot looks similar to a replication snapshot and is a preservation of the complete state of its source share at the time the snapshot was taken.

The data required to recover a DXi Secure Snapshot is stored deduplicated in the Blockpool alongside data ingested to shares. This allows each snapshot to store the full state of the share but consume minimal space.

Each snapshot requires bulk data space to store its associated metadata. The space required for the metadata files is highly dependent on the nature and content of the share which the snapshot is protecting.

The following are reasonable approximations to use when sizing snapshot metadata usage. Be aware that real-world consumption may vary considerably:

Mostly Large Files (backup application archives, VTL, OST, etc.)

Snapshot metadata for shares of this nature should generally consume less than 200 kiB per GiB of data (~0.05% overhead).

General Purpose File Storage

It is difficult to estimate snapshot metadata consumption when the share is used as a general file server without knowing the type of data. Based on tests with many small files, we can expect anywhere between 200 kiB and 2 MiB per GiB of data stored in the share (up to ~0.2% overhead). It may be possible to exceed 2 MiB per GiB if the share primarily contains very tiny (smaller than 1MiB) files.

Performance

System performance may be impacted while snapshot(s) are being taken. The scale of the impact is primarily dependent on the number of concurrent snapshots being taken at the time.

Scheduled snapshots of all shares or all shares of a type examine each share sequentially. Snapshots will only run concurrently if the user schedules more than one concurrent snapshot operation, or manually starts them concurrently.

System performance may be periodically impacted when an excessive number of DXi Secure Snapshots exist. Some DXi tasks must unavoidably traverse all snapshots. This is a primarily IO-bound operation.

Under normal operation the following tasks must traverse all snapshots:

Space Reclamation

The Space Reclamation process scans all in use data, including every snapshot that is being protected. This process will take some time for every snapshot on the system, and more time for larger snapshots.

Health Check

Must examine every snapshot to determine whether all dedupe data required by all snapshots is still available.

Other user-initiated operations must also traverse all snapshots:

Listing Snapshots via CLI or GUI

The GUI and CLI must currently traverse all snapshots to list even a filtered subset of snapshots. This only occurs at the customer's request by accessing the snapshot list functionality.

The customer should be not be concerned about retaining up to about twenty thousand snapshots. The performance impact will be almost negligible up to that point. There is no issue exceeding that number, however the customer may notice that space reclamation and health check take increasingly long as more snapshots are added.

If the customer does find that their total number of snapshots is causing an unwanted performance issue, then they may reduce the snapshot retention of each share or decrease the frequency at which snapshots are taken. The DXi will eventually expire snapshots down to a more manageable number and normal performance will resume over time.

Using DXi Secure Snapshots

Enabling and Disabling

The DXi Secure Snapshots feature ships ready to use but disabled. The user interface will prevent configuring the feature until it is enabled.

DXi Secure Snapshots will not take any snapshots while it is disabled. The customer will receive an error message if a snapshot operation is attempted.

Once enabled, the DXi Secure Snapshots feature cannot be disabled while there are snapshots still retained by the DXi.

Configuring Shares

It is possible to configure DXi Secure Snapshots on any deduped NAS Share, VTL or OST LSU. It can be configured at the time the share is created with the **--add** command, or after the fact with the **--edit** command.

The **--add** and **--edit** commands both provide a new --**snapshotretention** parameter. If the parameter is omitted from the **--add** command, then the share will default to no snapshot retention. If it is omitted from the **--edit** command, then the snapshot retention will not be modified.

Shares which existed on the DXi at the time it was upgraded to support DXi Secure Snapshots will default to snapshot retention disabled. After the upgrade, pre-existing shares are not treated any differently and it is possible to enable snapshot retention on them with the **--edit** command.

The same options are presented via the GUI, which defaults to disabling snapshot retention unless the customer explicitly selects the option.

Schedule

It is possible to schedule snapshots to be taken of one or more of the following at various times in the DXi scheduler:

- All configured NAS Shares.
- All configured VTLs.
- All configured OST LSUs.

Scheduling snapshots very frequently may result in an excessive number of snapshots on the DXi.

Scheduling regular snapshots of important data will ensure that it is always well protected against destruction of data.

The recommended frequency for taking snapshots of backup target shares is once per backup operation shortly after completion of the backup.

DXi is not recommended for use as a general purpose NAS, and snapshots are not intended to work on shares used as such.

Manual Snapshots

It is possible to manually take snapshots using the CLI. This may be useful to preserve the state of a share at a particular time for any number of reasons. Reasons might include:

- Preserve the state of a share before a major update to the customer's backup applications or configuration. If a failure causes the backup to become corrupted, the customer can simply delete the share and restore from the manual snapshot to recover it.
- Preserve evidence of malware attack or other malfeasance before removing the share and re-creating it from a known-good periodic snapshot.
- Complying with unexpected data retention requests (e.g. litigation holds, lawful requests retain data, etc.).

The retention period of a manual snapshot defaults to whatever retention was in effect on the share at the time the manual snapshot was initiated. Once a manual snapshot has been taken its retention period can be manually increased to ensure the data is retained for as long as is necessary.

If regularly scheduled snapshots are being taken of a share, then a manual snapshot of the share should not cause a marked increase in space consumption on the DXi unless its retention period is manually increased beyond the share's usual snapshot retention period.

Retention Period

Snapshots are retained for at least the retention period configured on their source share at the time the snapshot was taken.

It is possible to configure the retention period for each share on the DXi independently of the other shares as any integral multiple of days. e.g. 1 day, 30 days, 61 days, etc. It is possible to alter the retention period, or even disable retention on a share, even after snapshots have been taken. Altering the retention configuration

for a share will not impact the retention period of snapshots which already exist for that share.

It is not possible to reduce the retention period on any snapshot. This security feature may help to protect against inadvertently or maliciously setting all snapshot's retention periods very short and causing them to be expired from the system prematurely.

It is possible to increase the retention period of a single snapshot or a group of snapshots. This feature is useful if the customer has detected destruction of data and wishes to ensure that snapshots are not prematurely expunged before they have a chance to restore the data and understand how, why and when the destruction of data occurred.

A snapshot's lifetime is independent of the source share's lifetime, i.e. snapshots for a share are retained for the correct number of days, even if the share is deleted. Re-creating the share will not modify existing snapshots for the previously deleted share. This is a security feature which may help recover data for a share after it is maliciously or inadvertently deleted.

The customer is advised to select a snapshot retention period which makes sense for their application and their expected time to detect and recover from malware activity.

Snapshot Deletion

It is not possible for the customer to manually delete snapshots from the system. This security feature may help protect snapshots in the event a malicious attacker gains access to the DXi CLI or GUI. Unless the attacker can become *root* on the DXi they should be unable to damage snapshots.

During each space reclamation run, snapshots which have exceeded their retention period are purged from the system and their space recovered for reuse. The customer should ensure that space reclamation is scheduled to run at least weekly.

Snapshots may live on the system until sometime after their retention date if space reclamation is only run infrequently. This is normal and is nothing to be concerned about. Normal low space behavior will cause space reclamation to run and purge expired snapshots if the DXi runs low on space.

Preventing Snapshot Deletion

There may come a time when it is required to prevent snapshot deletion. There are many reasons for this. It is possible to extend the retention period of one or more snapshots to cause DXi Secure Snapshots to retain them for longer. This may be appropriate where the customer only needs to secure access to the data from a small number of snapshots.

There may be cases where the customer needs to pause snapshot deletion for many snapshots or across the entire system. In these cases, it is possible to pause snapshot deletion globally for a specified number of days. It is also possible to extend the number of pause days, should data recovery take longer than expected.

Pausing snapshot deletion does not prevent creating new snapshots. The customer is free to manually take further snapshots or leave scheduled snapshots active. The customer is warned that continuing to ingest data into the DXi while snapshot deletion is paused, and scheduled snapshots are active may lead to exhausting all the free space on the DXi.

Once engaged, the deletion pause feature cannot be disengaged or have its period reduced by the customer. The only way to resume snapshot deletion is to wait until the requested number of days has passed. This is a security feature which may help prevent a malicious attacker undoing the deletion pause in the middle of the

data recovery process.

Quantum®

ABOUT QUANTUM

Quantum technology and services help customers capture, create, and share digital content—and preserve and protect it for decades. With solutions built for every stage of the data lifecycle, Quantum's platforms provide the fastest performance for high-resolution video, images, and industrial IoT. That's why the world's leading entertainment companies, sports franchises, researchers, government agencies, enterprises, and cloud providers are making the world happier, safer, and smarter on Quantum. See how at **www.quantum.com**.

www.quantum.com • 800-677-6268