



Oracle ZFS Storage Appliance

Best Practices for Implementing Snapshot Retention

November, 2021 | Version [1.00]
Copyright © 2021, Oracle and/or its affiliates
Public

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

TABLE OF CONTENTS

DISCLAIMER	2
INTRODUCTION.....	4
RECOMMENDATIONS FOR SNAPSHOT RETENTION	4
OVERVIEW OF SNAPSHOT RETENTION	5
OVERVIEW OF MANUAL SNAPSHOT RETENTION	7
OVERVIEW OF SCHEDULED (AUTOMATIC) SNAPSHOT RETENTION	8
SEND RETAINED SNAPSHOT TO OCI (CLOUD) OBJECT STORAGE	11
MANAGING SNAPSHOT RETENTION USING THE CLI.....	12
ADVANCED SNAPSHOT RETENTION TOPICS.....	12
RETENTION VAULT CONFIGURATION	13

INTRODUCTION

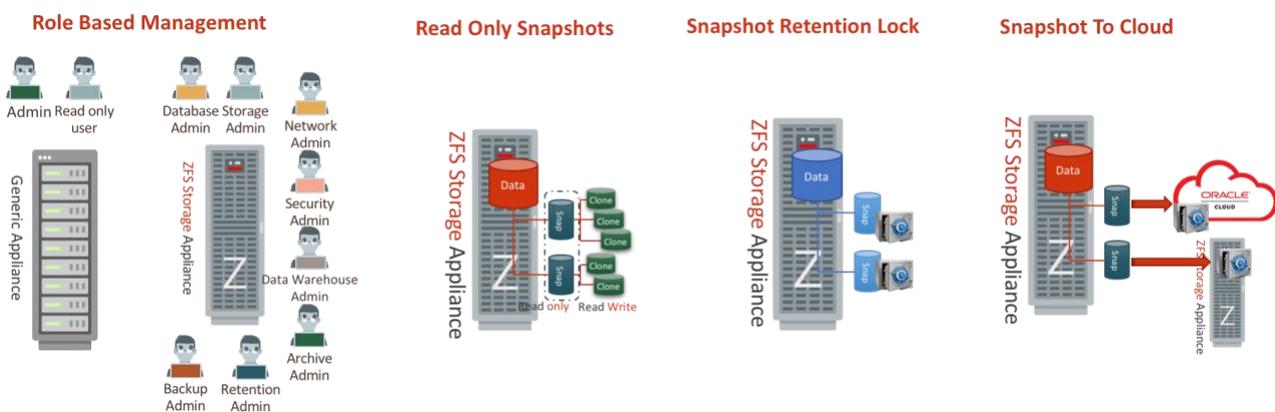
Oracle ZFS Storage Appliance systems provide a high-performance unified storage that combine NAS, SAN, and object storage capabilities with the extreme performance and superior efficiency required by demanding enterprise applications and unpredictable cloud workloads.

Data protection in today's world requires layers of defensive protections as well as recovery procedures. The ZFS Storage Appliance has always included integrated snapshots that can be scheduled and replicated to other locations. As another layer of protection, ZFS snapshots are immune to ransomware-like encryption attempts. And critically important is that ZFS snapshots can be rolled back to recover from a ransomware attack.

In this solution brief, we describe the snapshot retention features that can be used to meet data governance, legal hold, and regulatory requirements. They also add another layer of protection to prevent malicious or accidental deletion.

Overall ZFS Snapshot Retention Policy Strategy

The ZFS Storage data protection foundation includes role-based access control (RBAC) for separation of powers for all management or operational tasks including snapshot retention management. Integrated snapshots are another foundational component that provides a layer of protection, as read-only versions of file system data and also provide a recovery mechanism.



1. Separation of powers is provided with very granular rights in role based management and allows delegation of roles with the right level of access.
2. Snapshots are immune to ransomware encryption attempts are preserved as read only for R/W thin clones, adding extra security.
3. Snapshot retention provides another protection layer that makes malicious or accidental removal even harder.
4. Snapshot to the cloud and/or to another on-premises ZFS Storage Appliance acting as cloud object storage. At both locations 'retention lock' / 'immutability' can be set.

RECOMMENDATIONS FOR SNAPSHOT RETENTION

ZFS Storage snapshot retention can be used to support data governance, regulatory compliance, or legal hold use cases. Snapshot retention also provides another layer of protection to prevent malicious or accidental removal.

- Consider an overall strategy for meeting compliance requirements that might include snapshot retention.
- Snapshots are space efficient in that they share blocks with the file system itself and only consume additional space when the file system is modified.
- Confirm disk capacity requirements to meet your retention requirements. Carefully review this section for more information: [Verifying Disk Capacity Requirements for Retained Snapshots](#).
 - Set LZ4 compression to optimize space consumption on projects or shares for snapshot data that is retained.
- Consider that setting a snapshot schedule with retained snapshots means that after the schedule starts, the snapshots are retained until they roll off the schedule. Otherwise, they cannot be removed.

OVERVIEW OF SNAPSHOT RETENTION

ZFS Storage snapshot retention allows you to retain a snapshot for a retention period that is locked using scheduled snapshots. Or, a snapshot can be retained for an indefinite period that is unlocked using manual snapshots. Note the following behavior:

- Only users with the adequate authorization can add or remove retention from a snapshot.
- Retained snapshots cannot be removed. Projects and shares containing retained snapshots cannot be removed.
- After a retention policy is added to a snapshot, the snapshot as well as the share and project containing this snapshot cannot be deleted.
- Retained snapshots that are part of a replication action are also retained when replicated.
- Snapshots with retention policies disabled that are generated or included with replication packages are not impacted.

Snapshot Retention Authorization Summary

Only a user with the proper authorization can add or remove retention from a snapshot and schedule a snapshot with retention.

AUTHORIZATION	FUNCTION
releaseSnapRetention	Release a snapshot retention policy
retainSnap	Retain a snapshot
scheduleLockedSnap	Configure retention on schedule of snapshots

Snapshot Retention Use Case Summary

SNAPSHOT TYPE	DESCRIPTION	COMPLIANCE TYPE
Manual Snapshots	<ul style="list-style-type: none"> • Perfect for legal hold use cases • New or existing snapshots can be retained • No specified time limit • Can be retained and then released 	Legal Hold
Scheduled (Automatic) Snapshots	<ul style="list-style-type: none"> • Supports both data governance and regulatory compliance for routinely retaining snapshot data for defined or extended periods. • Includes both KEEP-AT-MOST and RETENTION settings so that you can keep a number of scheduled snapshots and then also retain/lock an equivalent number or subset of those scheduled snapshots. • If scheduled snapshots include a RETENTION value and schedule has started, you cannot remove or reduce the schedule, you can only extend it. • After the retention threshold is reached, the retention policy of a snapshot will change from locked/unlocked to off. • For example, scheduled snapshot KEEP-AT-MOST value is 7, RETENTION value is 4. The 7 most recent snapshots are kept and the newest 4 snapshots are retained /locked. 	Data Governance, Regulatory

Two Levels of Retention: Unlocked and Locked

- Manual snapshots include unlocked retention. Settings are: Off or Unlocked
 - Cannot lock a manual snapshot retention because the retention is unlocked, meaning that it is open-end and can be removed.
- Scheduled (automatic) snapshots include a retention lock. Settings are: Off or Locked
 - Schedule snapshots provide the ability to retain a number of snapshots based on a snapshot schedule.
 - A locked snapshot cannot be deleted by a user after the snapshot schedule is initiated.
 - A scheduled snapshot that is retained can only be removed when the schedule expires and the snapshot is discarded.

Company Ares Snapshot Retention Scenario

The following section describes a customer scenario with different types of data that needs to be retained for a period of time that will be covered in this paper.

SCENARIO	RETENTION TYPE	COMPLIANCE TYPE	PROJECT/SHARE NAME
Legal dept notifies of legal hold requirement on existing data - previous fiscal year	Manual snapshot - unlocked	Legal hold	<ul style="list-style-type: none"> • Project: CompanyA-Ret • Share: finance-legal-share
Auditors require financial data is retained for 3-6 years	Scheduled snapshot - locked	Regulatory	<ul style="list-style-type: none"> • Project: CompanyA-Ret • Share: finance-data-share
Auditors require RMAN backups are retained for 3-6 years	Scheduled snapshot - locked	Regulatory	<ul style="list-style-type: none"> • Project: CompanyA-Backup • Share: backup-1
Company requires that critical IP data is retained	Scheduled snapshot - unlocked	Data governance	<ul style="list-style-type: none"> • Project: CompanyA-Ret • Share: app-data-share

Verifying Disk Capacity Requirements for Retained Snapshots

Balancing data retention policies with disk storage capacity require that you identify the storage capacity that will be consumed by scheduled snapshot retention. After a scheduled snapshot is locked, you can only extend the schedule. The locked schedule snapshots can roll off if the schedule expires them, but consider estimating the amount of snapshot data to be retained before the snapshot scheduled is locked.

Formula: existing project/shares size + scheduled snapshot size = estimated size of retained scheduled snapshots

- Consider creating manual snapshots with unlocked retention as a way to test the amount of disk space that will be required to retain snapshots.
- If the test identifies that you have adequate disk space to retain your snapshots over a period of time and you have estimated disk capacity for future snapshots, create a scheduled snapshot with retention for your retention requirements.

OVERVIEW OF MANUAL SNAPSHOT RETENTION

Retention can be set on a manual snapshot for some immediate requirement for either data governance including security, legal hold, or regulatory purposes. For long-term regulatory purposes, the scheduled snapshot retention is more convenient.

- Retention can be added while creating a snapshot
- Retention can be added to an existing snapshot
- In either case, the retention lock on a manual snapshot can be enabled and then disabled

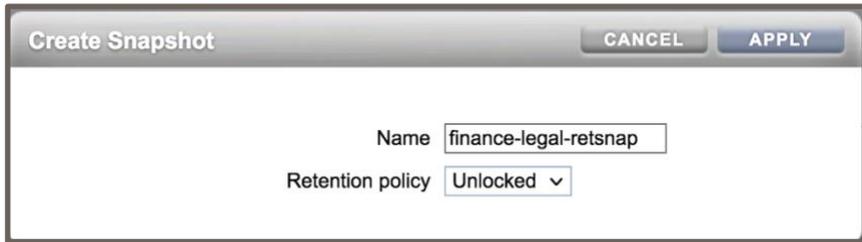
Retaining Manual Snapshots

In this example, Company Ares need to create an out-of-cycle manual snapshot of data to be retained for legal hold. The goal is to retain the snapshots indefinitely.

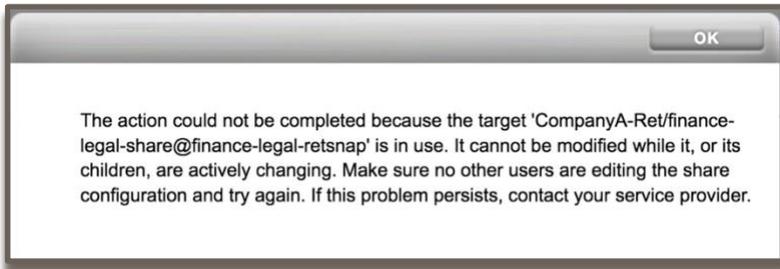
How to Retain Manual Snapshots

The following example shows how to create a snapshot that is retained for a legal hold.

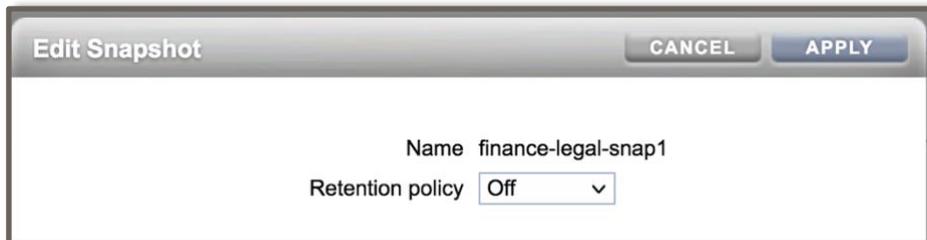
1. Create a manual snapshot. For example, the finance-legal data must be retained immediately.



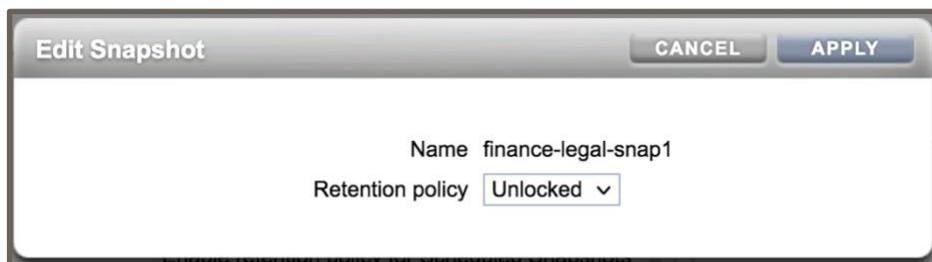
2. Verify the manual snapshot is retained. For example, attempt to remove the manual snapshot.



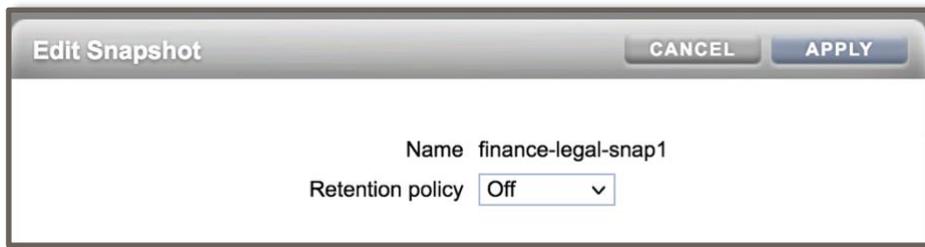
3. You can also retain an existing snapshot.
 - a) Select snapshot to retain.



- b) Change Off to Unlocked.



4. Set the snapshot retention policy to Off to remove the snapshot retention when the legal hold is released.



OVERVIEW OF SCHEDULED (AUTOMATIC) SNAPSHOT RETENTION

Scheduled snapshots allow you to retain a number of snapshots, for example, keep 5 weekly snapshots but specify that the 2 of the most recent ones are retained. Previous behavior of scheduled snapshots is that you could keep a number of copies, for example, 5, but they could be removed with the proper authorization.

In the OS8.8.39 release, the number of retained snapshots, for example, 2, cannot be removed until the schedule allows them to be discarded.

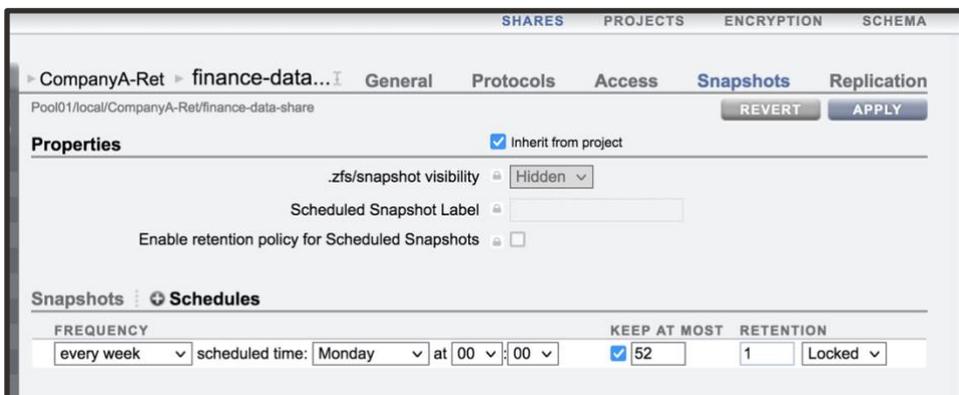
Notes on behavior:

- “KEEP AT MOST” and “RETENTION” values can be increased but not decreased. For example, you can change the “KEEP AT MOST” value from 5 to 6, in which case a snapshot will have a retention period for 6 weeks (so cannot be removed by any means for 6 weeks).
- A schedule can be deleted or modified (decreased) as long as no snapshots from this schedule have been generated yet.

Project-Level Snapshot Retention

Review the following behavior for project-level snapshot retention:

- Enable the Enable retention policy for Scheduled Snapshots option when you want to create a scheduled snapshot retention policy. Otherwise, if you select a snapshot schedule with locked retention and this option is not enabled, the generated snapshot will not have retention set.
- If you want the scheduled retained snapshots to expire before the snapshot schedule expires, then disable the Enable retention policy for Scheduled Snapshots option.
 - For example, to delete the corresponding share when there is a daily schedule of keep=7 and retain=5, disable the option and then wait 5 days until the snapshot with a retention expire. Then after 5 days, you can delete the share.
- When scheduled snapshot retention is set at the project level, shares will inherit the scheduled snapshot retention policy unless specified otherwise.

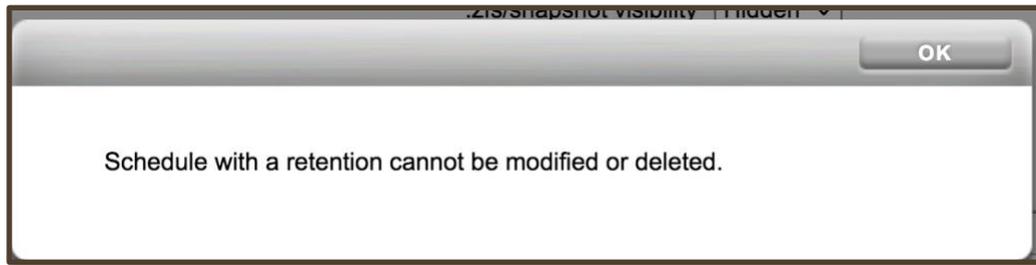


How to Retain Scheduled (Automatic) Snapshots

Review the following before you begin:

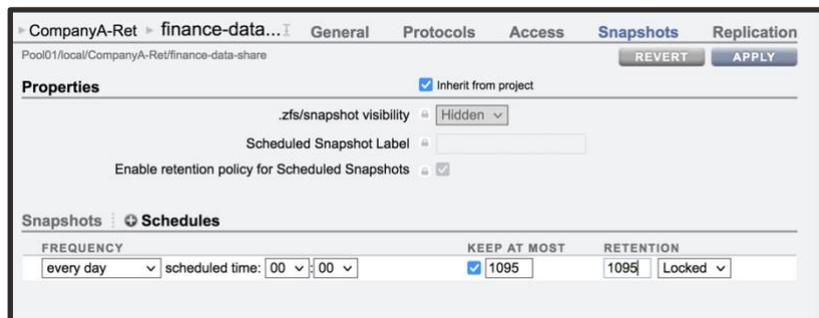
- Scheduled snapshots retention can be locked or OFF.

- If scheduled snapshot retention is locked, the number of snapshots retained cannot be reduced but the number can be increased.
- If scheduled snapshot retention is locked, the schedule cannot be changed nor can the retention be unlocked, but the schedule can be extended.



In this example, Company Ares must retain scheduled snapshots of daily financial data for 3 years for regulatory compliance.

1. **Caution:** See [Verifying Disk Capacity Requirements for Retained Snapshots](#) for considerations on estimating the storage capacity of keeping snapshot for 3-6 years. After the schedule has started and the snapshots are generated, you cannot remove the schedule or decrease the retention period.
2. Select a share for retained scheduled snapshots. In this example, finance-data-share.
3. Select the Snapshots tab.
4. Click Schedules and select the snapshot schedule. For example, select daily, keep 1095 snapshots, and retain 1095.
5. Switch Retention to Locked.

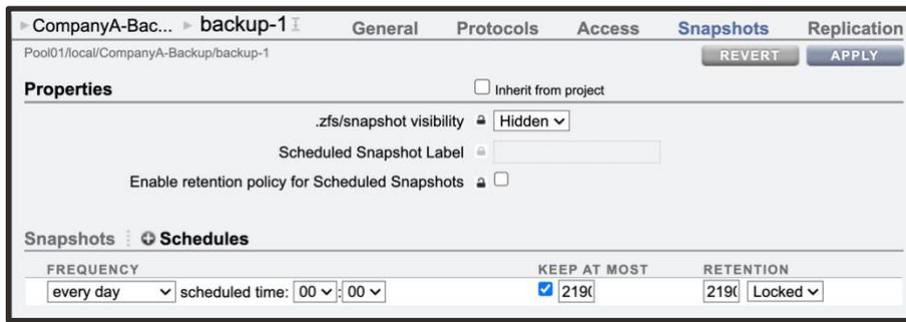


6. Click Apply.

How to Retain Snapshots of RMAN Backups

The following steps show how to retain scheduled snapshots of RMAN backups for regulatory compliance. Daily snapshots of a backup share are retained for 6 years.

1. **Caution:** See [Verifying Disk Capacity Requirements for Retained Snapshots](#) for considerations on estimating the storage capacity of keeping snapshot for 3-6 years. After the schedule has started and the snapshots are generating, you cannot remove the schedule or decrease the retention period.
2. Select the CompanyA-Backup project and then select the Snapshots tab.
3. Click Enable retention policy for Scheduled Snapshots.
4. Select the backup-1 share.
5. Select the Snapshots tab.
6. Select Schedules and then click Locked Retention.
7. Set the Frequency to daily and Keep at Most to 2,190 and set Retention to 2,190.



8. Click Apply.

Scheduled Snapshot Retention Policy Behavior for Project or Shares

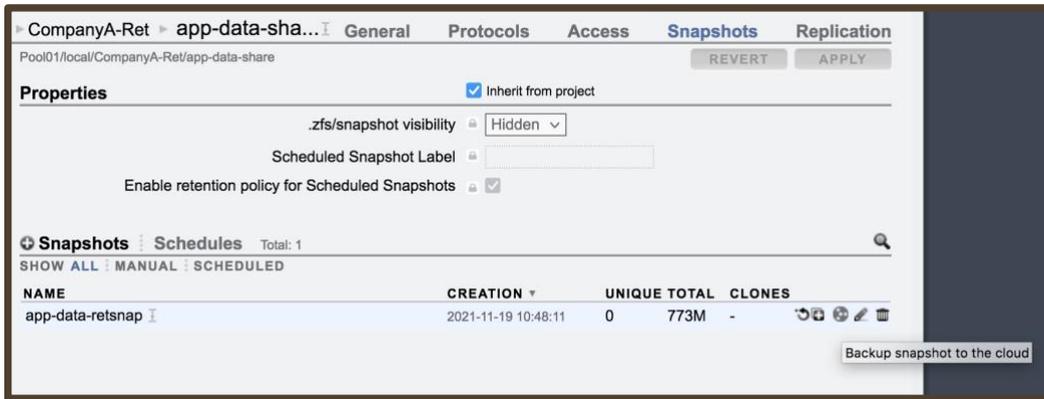
1. If this project-level property is enabled and a scheduled snapshot retention policy is set, you cannot implement a separate scheduled snapshot retention policy on individual shares.
2. If this project-level property is disabled and there is a project-level scheduled snapshot retention policy, then you cannot have a separate scheduled snapshot retention on individual shares.
3. If you disable the "inherit from project" property for scheduled snapshots at the individual share level, you still cannot implement a different scheduled snapshot retention policy.
4. If this project-level property is disabled and there is no project-level scheduled snapshot retention policy, then you can have a separate scheduled snapshot retention on individual shares.
5. After the retention threshold is reached, the retention policy of a snapshot will change from locked/unlocked to off.

A snapshot schedule is currently in effect for the project.
Scheduled snapshots can only be active for a project or a share, but not both.

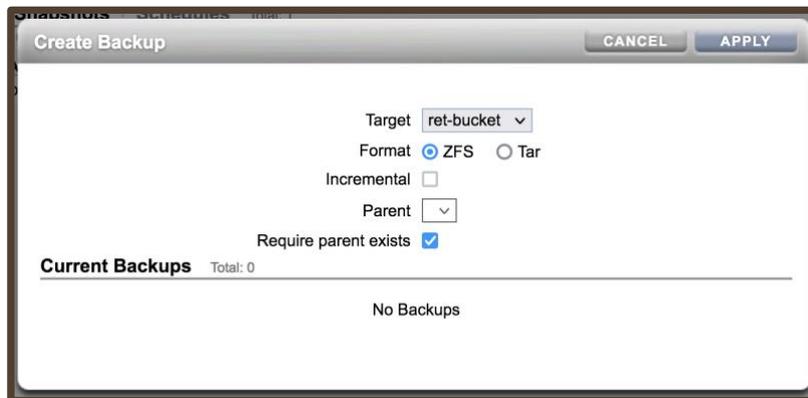
SEND RETAINED SNAPSHOT TO OCI (CLOUD) OBJECT STORAGE

You can send a retained snapshot to an OCI (cloud) object storage bucket for longer term storage and the OCI cloud object storage bucket can also have a retention policy set. For information on setting retention on an OCI (cloud) object storage bucket when using cloud snapshot backups, see [Configuring ZFS Storage for Cloud Snapshot Backups to OCI Object Store](#).

1. Select the retained snapshot to be sent to OCI object storage.



2. Select the Backup snapshot to the cloud option.
3. Identify the target cloud backup and the snapshot backup format.
4. Click Apply.



MANAGING SNAPSHOT RETENTION USING THE CLI

Snapshot retention can be managed from the CLI.

In the following example, a manual snapshot is created and retained for data governance.

```
ares-1:shares CompanyA-Ret/app-data-share snapshots> snapshot app-data-retsnap
ares-1:shares CompanyA-Ret/app-data-share snapshots> select app-data-retsnap
ares-1:shares CompanyA-Ret/app-data-share@app-data-retsnap> set retentionpolicy=unlocked
retentionpolicy = unlocked (uncommitted)
```

The snapshot retention in the following example is removed when the retention period has expired.

```
ares-1:shares CompanyA-Ret/app-data-share@app-data-retsnap> set retentionpolicy=off
retentionpolicy = off (uncommitted)
```

The following example shows how to display snapshot retention rules from the CLI.

```
ares-1:shares CompanyA-Ret/finance-data-share> get snapret_enabled
snapret_enabled = true (inherited)
ares-1:shares CompanyA-Ret/finance-data-share> snapshots
ares-1:shares CompanyA-Ret/finance-data-share snapshots> automatic
ares-1:shares CompanyA-Ret/finance-data-share snapshots automatic> select automatic-000
ares-1:shares CompanyA-Ret/finance-data-share snapshots automatic-000> ls
Properties:
    frequency = week
    day = Monday
    hour = 06
    minute = 00
    keep = 52
    retentionhold = 52
    retentionpolicy = locked
```

ADVANCED SNAPSHOT RETENTION TOPICS

Applying Legal Hold to a Different Snapshot or to a Subset of a Scheduled Snapshot

If you need to apply a legal hold to snapshot data that has a different retention period than the current retention period or is within the current retention period, consider the following options:

Convert existing schedule snapshot/cloning method:

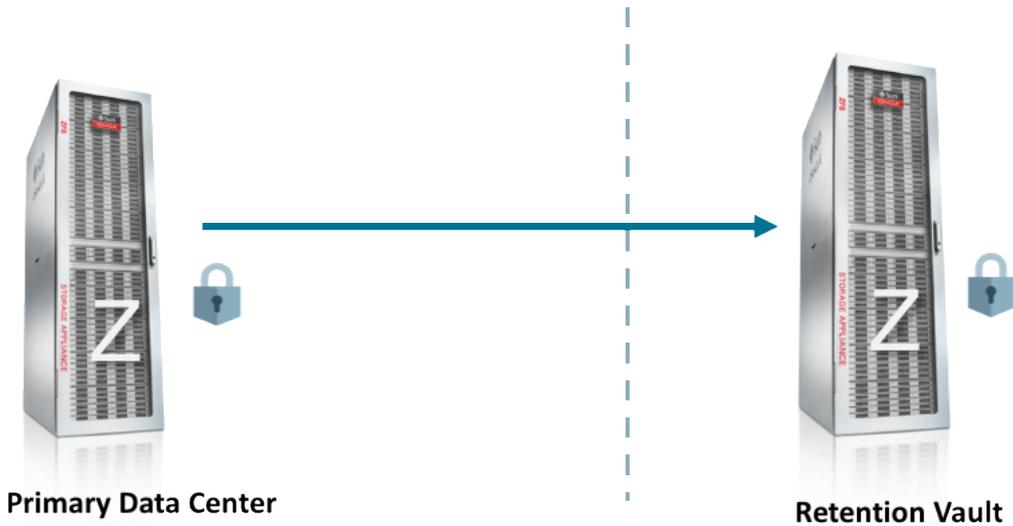
- Single snapshot: create a filesystem, generate a scheduled snapshot of this filesystem, clone this snapshot to a new filesystem, take a manual snapshot of the new filesystem (before writing any data to this filesystem)
- Range of snapshots: Search scheduled snapshots for the required time frame and create clones of these snapshots. Then, create a manual snapshot with UNLOCKED retention.
 - For example: Assume an existing daily snapshot schedule for 5 years (1825 snaps) and set the values of KEEP-AT-MOST and RETENTION to: 1825.
 - This approach ensures that a snapshot is retained and cannot be deleted for 5 years. If you want to recover snapshots from the day 60 to day 65 window, which includes modifications from this period, you will have to clone snap-60 and clone snap-65 to 2 new filesystems, calculate the difference of these two filesystems and generate a new file system.

Existing share/create manual snapshot method:

If the filesystem share of the older data still exists, create a manual snapshot with UNLOCKED retention.

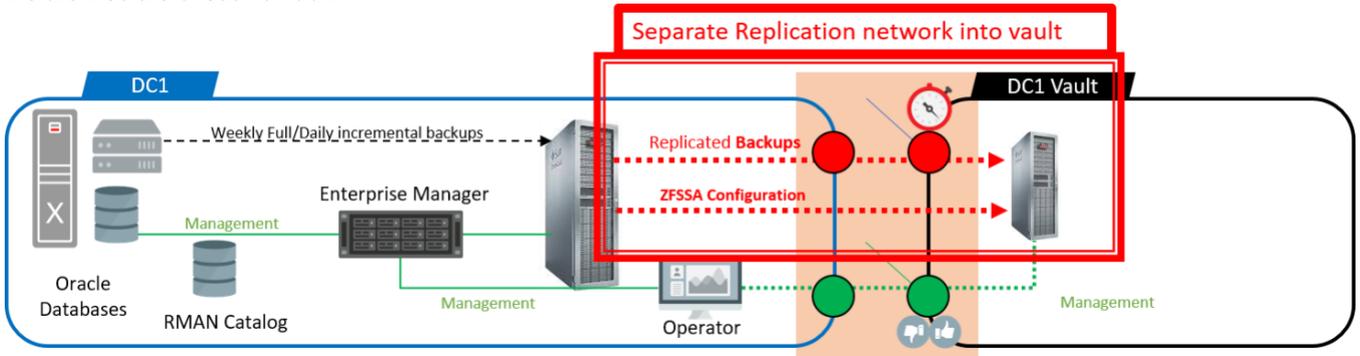
RETENTION VAULT CONFIGURATION

Replicate encrypted, read-only snapshots with retention lock



Improving security against a cyberattack is a common concern and although ZFS Storage systems have snapshots that are immune to a ransomware encryption attack, you can further protect critical data by implementing retention policies and replicating read-only snapshots to an Oracle ZFS Storage Appliance designated as a retention vault.

A retention vault appliance should be on an isolated network. Access to such networks is often available for a limited time through switch ports that are turned on and off by management software inside the vault. The following diagram illustrates the architecture of such a vault.



A ZFS Storage Appliance located in such a vault should have extra measures taken to restrict access.

- **Disable Data Services** – All data services that could pass the data to clients should be disabled. SMB and NFS are the most obvious, but don't forget about others such as HTTP and FTP.
- **Limit root access** – Create a role with system access and replication privileges and disable root/ssh access.
- **Limit management port access** – This can be done by allowing access only through the ILOM and/or a serial connection, or by requiring the administrator to use a computer with a web browser that can only access systems within the vault.

It is common in such vault installations to want to retain snapshots in the vault for a longer period of time than they are kept on the primary Oracle ZFS Storage Appliance. To achieve this, the snapshot schedule on the target appliance in the vault can be edited with a longer retention period than on the source, as shown in the example below.

Example:

The DBAs at Ares Corp. run a full backup every Sunday, and the company has mandated that these backups be kept in the vault for 5 years (1825 weeks). The DBAs want to keep a month's worth of full backups in snapshots on the ZFS appliance they back up to, but sometimes have space issues and will delete older snapshots. The snapshot schedule defined below on the source appliance will keep 5 snapshots but allow the two oldest snaps to be deleted if necessary:

Snapshots :: **Schedules**

FREQUENCY		KEEP AT MOST	RETENTION
every week	scheduled time: Monday at 04:30	<input checked="" type="checkbox"/> 5	3 Locked

The replication schedule is then set to automatically send a snapshot to the target appliance in the vault whenever one is taken:

Schedule :: **Cascading Schedule** :: **Snapshots**

Update frequency Scheduled Continuous

Replication Schedules

FREQUENCY

auto-snapshots

Finally, snapshot retention policies are set to be independent on the target, allowing them to be changed there. The target is also set to keep five years of backups:

Schedule :: **Cascading Schedule** :: **Snapshots**

Auto snapshot retention policies synchronized independent

Configure auto snapshot retention on the target

FREQUENCY	KEEP AT MOST
every hour scheduled time: 26 minutes past the hour	<input checked="" type="checkbox"/> 1825

On the target appliance in the vault, the retention is changed from three weeks, which had been set when the first replication occurred, to five years. This ensures that none of the snapshots that have been replicated to the vault can be deleted for that time period.

Snapshots :: **Schedules**

FREQUENCY	KEEP AT MOST	RETENTION
every week scheduled time: Monday at 04:30	1825	1825 Locked

Backup and Retention Considerations

As noted earlier in this brief, the space required on the ZFS Storage Appliance to store snapshots for a long period of time can be considerable. Extensive testing of scheduled replications without a retention policy should be done for a period of time to help determine the amount of disk space required. Care should be taken when adding a retention policy, as scheduled snapshots and replications may not be removed until the last locked snapshot has had its retention period expire.

Enabling data deduplication (which uses specialized SSDs in the appliance) may help save a considerable amount of space, but not all data lends itself to deduplication. Again, extensive testing is recommended. Consider the use of the ZFS Storage Appliance Simulator to test this functionality.

Monitoring Replication from Inside the Vault

It is common in many retention vault architectures to limit network access to the vault by disabling ports on a switch when a time limit is reached or the replication jobs have completed, whichever happens first. This functionality is usually controlled from a system inside the vault that can monitor the systems within the vault.

On the source appliance the replication actions can be monitored, but these actions cannot be viewed from the target appliance. Instead, the replication packages will give the information needed by the monitoring system.

Monitoring Replication Packages with CLI

The status of all replication packages on a target can be seen from the CLI with the command "shares replication packages show", as seen here:

```
zfs2:shares replication packages> show
Packages:

ID           STATE  DATA_TIMESTAMP      SOURCE   DATASET
package-008  recv   unknown              zfssa   DB-backup
package-007  idle   2021-10-07 13:02:38  zfssa   default
```

This shows that package-007 is associated with the "default" project on the source appliance named "zfssa" and is not receiving data at this time.

It also shows that package-008 is associated with the "DB-backup" project on the source appliance, and that it is currently receiving data. The network ports should not be closed as this indicates an active replication.

Monitoring Replication Packages with RESTful API

This information can also be obtained via the RESTful API command `"/api/storage/v2/replication/packages"`:

```
{
  "packages": [
    {
      "href": "/api/storage/v2/replication/packages/29a7dfc1-92b2-4134-835d-c9fada874afb",
      "id": "29a7dfc1-92b2-4134-835d-c9fada874afb",
      "source_name": "zfssa",
      "source_asn": "df0c6049-dfae-4022-8320-edc1b00b8d8c",
      "source_ip": "192.168.3.10:216",
      "source_pool": "dedup",
      "target_pool": "p1",
      "replica_of": "default",
      "enabled": true,
      "conflict_detected": false,
      "state": "idle",
      "state_description": "Idle (no update in progress)",
      "offline": false,
      "import_path": "",
      "data_timestamp": "2021-10-07T13:02:38Z",
      "last_sync": "2021-10-07T13:02:39Z",
      "last_try": "2021-10-07T13:02:39Z",
      "last_result": "success",
      "encryption": "",
      "keystore": "",
      "keyname": "",
      "compression": ""
    },
    {
      "href": "/api/storage/v2/replication/packages/7217fe4b-289f-4a1e-b02c-de5fc5888d35",
      "id": "7217fe4b-289f-4a1e-b02c-de5fc5888d35",
      "source_name": "zfssa",
      "source_asn": "df0c6049-dfae-4022-8320-edc1b00b8d8c",
      "source_ip": "192.168.3.10:216",
      "source_pool": "dedup",
      "target_pool": "p1",
      "replica_of": "JH",
      "enabled": true,
      "conflict_detected": false,
      "state": "idle",
      "state_description": "Idle (no update in progress)",
      "offline": false,
      "import_path": "",
      "data_timestamp": "2021-10-07T13:02:47Z",
      "last_sync": "2021-10-07T13:04:13Z",
      "last_try": "2021-10-07T13:04:13Z",
      "last_result": "success",
      "encryption": "",
      "keystore": "",
      "keyname": "",
      "compression": ""
    }
  ]
}
```

For more information on monitoring and controlling the Oracle ZFS Storage Appliance through its RESTful API, please refer to the solution brief ["Working with the RESTful API for the Oracle ZFS Storage Appliance."](#)

CONNECT WITH US

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com).

Outside North America, find your local office at [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Oracle ZFS Storage Appliance: Best Practices for Implementing Snapshot Retention
November 2021

Author: Cindy Swearingen, Joseph Hartley, and Olivia Wang

