AssuredSAN 3000 Series

Using Data Protection Software

P/N 83-00006527-10-01
Revision A
March 2011

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, changes in the product design can be made without reservation and without notification to its users.

Adobe PostScript

Contents

About this guide

The Data Protection Software described in this document includes several tools you can use to protect data, ensure business continuity, and provide disaster recovery:

- AssuredSnap™ provides point-in-time "snapshot" copies or backups of disk volumes and instant restoration of data from any snapshot, maximizing business continuity.
- AssuredCopy™ enables you to create full volume copies or backups of disk volumes which protect against disk failures and enable you to quickly restore whole volumes, folders, or individual files.
- AssuredRemote™ replication performs asynchronous (batch) replication of block-level data from a volume on a local storage system to a local or remote system.

Used together, the Data Protection Software suite is a complete solution for business continuance, disaster recovery and regulatory compliance.

This document describes the use of functionality in software release TS230 and beyond. Upgrade earlier software releases before using this document.

Intended audience

This guide is intended for:

- Storage system administrators
- Configuration managers

Related documentation

In addition to this guide, please refer to other documents for this product:

- AssuredSAN 3000 Series RAIDar User Guide
- 3000 Series CLI Reference Guide
- 3000 Series Getting Started Guide
- 3000 Series Setup Guide

See Dot Hill's Customer Resource Center web site for additional information: http://crc.dothill.com.

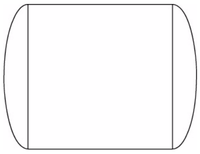
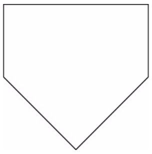
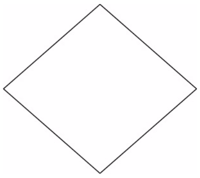
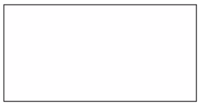
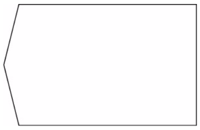
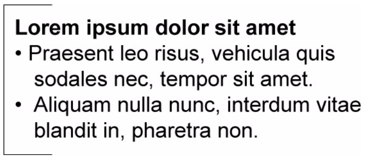
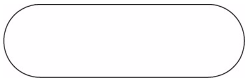
Assumptions

Within this document, basic assumptions are made about the system you are setting up:

- Overall system setup maximizes fault tolerance
- Virtual disks are mapped to volumes
- Volumes are mapped to hosts

Flowchart legend

This is a guide to the commonly used shapes in the flowcharts in the following chapter.

	Process starting point. No action takes place here, but inputs for the process should be ready.
	Subprocess. Links to another process then returns to the same point in the flowchart with outputs from that process
	Decision. The user discerns a decision or action. Represents a branch in the process flow or logic.
	User input is required. Usually where user action takes place.
	Output to user. A message from the application performing the task.
 **Lorem ipsum dolor sit amet** • Praesent leo risus, vehicula quis sodales nec, tempor sit amet. • Aliquam nulla nunc, interdum vitae blandit in, pharetra non.	Textual explanation. Additional guidance provided to the user. This information may refer to a decision or action, but falls outside the normal flow of the process.
	Process end point. The process ends here. All predicted outputs for the process should be apparent at this point.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text	Cross-reference links and e-mail addresses
Blue, underlined text	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

1 Getting started

Volume types and equipment

- Vdisk - A “virtual” disk comprising the capacity of one or more disks. A vdisk can contain different models of disks, and disks with different capacities.
- Volume - A portion of the capacity of a vdisk that can be presented as a storage device to a host. A system presents only volumes, not disks or vdisks, to the host.
- Snap pool - An internal volume, which cannot be mapped, used to store snapshot data.
- Snapshot - A point-in-time image of the data in a volume. Data tracked in a sparse format. A snapshot is a virtual volume, with a set of pointers to data that is located on a different volume (a master volume and/or a snap pool). A snapshot behaves like a regular volume in that a LUN can be assigned to it and it can be mapped to hosts. The snapshot can be mapped as read-only or read/write, depending on the intended purpose of the snapshot.
- Replication snapshot - A special snapshot taken explicitly for the purpose of transferring data from one volume to another, and where the second volume typically resides on a second, independent, controller. The second controller need not be geographically distant. A replication snapshot volume cannot be mapped to a host.
- Replication set - Primary and secondary volumes that are enabled for replication and that typically reside in two physically separate storage systems.
- Volume copy - An independent copy of the data on a volume.
- Master volume - Snapshot-enabled volume with an associated snap pool. A master volume is required for snapshots, volume copy or replication operations.
- Controller - A module in the storage system that configures, monitors and manages the overall storage system.

Unmounting a volume

Some tasks require that you unmount a volume or editable snapshot from a host. This is because ongoing host I/O to a volume or editable snapshot may:

- Corrupt data, either on the source or target of a task
- Fail to include data in the task, thereby creating inconsistencies between task expectations and actual performance

Because unmounting and remounting a volume is specific to the host, best practices are beyond the scope of this document.

Cabling and configuring practices

How you connect the various components of your system is highly specific to the system’s intended usage; the resources available to you (such as space for components, air-handling requirements or restrictions, and access to cable routing needs such as walls, ceilings, raised floors and switches); and various business, security, or regulatory requirements.

The sheer number of components that can be attached and used within a system makes any kind of recommendation impractical. As such, cabling practices are beyond the scope of this document.

However, as you consider the physical connections of your system, specifically connections for replication, there are several important points to keep in mind.

- Ensure that controllers must have connectivity between systems, local or remote.
- Assign specific ports for replication whenever possible. By specifically assigning ports that are available for Replication, you free the controller from scanning ports at the time Replication is performed.
- Ensure that all ports that are assigned for replication are able to communicate appropriately with the replication remote system. See `verify remote-link` in CLI Reference Guide for more information.

- Allow two ports on the same controller to conduct replication. This permits the system to balance the load across those ports as I/O demands rise and fall.
- Utilize at least one port on each controller. This ensures fault tolerance between the two controllers.
- Do not expose the management port to an external network connection.

2 Limiting and scheduling

Balancing limits and business needs

While discussing system limits, refer to Volume types and equipment on page 9 for clarification on terminology used in this section.

Counting volumes on the system

As you begin to calculate how you will utilize these various volumes, keep in mind these rules for counting volumes:

- A master volume counts as two volumes (the master volume and the snap pool volume). An excess of master volumes (and snap pools) can unnecessarily increase the number of volumes used and reduce your snapshot capacity.
- Snapshots within the snap pool each count as one volume
- Replication snapshots do not count against the total number of snapshots with regard to AssuredSnap licensing limits, but do count against the 1,024 total volume limit on the system.
- Initiating a volume copy may create up to three new volumes. See Performing a volume copy, step 1 on page 34 for more information on how volumes are created during this task.

System limits

In addition to volume counts, there are other limits placed on a system, both minimum and maximum.

Table 2 System limits

Vdisks	• 16 vdisks per controller. • 32 vdisks total in a dual controller environment • 64TB maximum size • 16 disks per vdisk on any RAID other than RAID 50 • 32 disks per vdisk on RAID 50
Volumes	• 1,024 volumes per system. This includes standard, master, snapshot, snap pool, and replication volumes. There is no limit on standard volumes except what is stated here. All volumes must be balanced against this number. • 128 master volumes per system • 128 volumes per vdisk • 1MB minimum size, except snap pools. • 64TB maximum size
Snap pools	• 128 per system • 1 master volume mapped to a single snap pool is best practice; however, 128 master volumes may be mapped to a single snap pool. • 6GB minimum size
Snapshots	• **First limited by AssuredSnap licensing, then** • 1,000 per system • 127 per master volume
Replications	• **When AssuredRemote licensing is active, then** • 16 replication sets per system • 2 replication volumes per set; the primary counting as one, the secondary counting as one. Either or both volumes may be on the same system. • 128 kbits per second network bandwidth is required for replication to function correctly. Functionality degrades as bandwidth decreases with I/O.

Balancing volumes on a system

While the total volumes available in a system remains consistent, how you use or balance those volumes on a system can impact the effectiveness of the data protection software.

Table 3 Example cases of balancing maximum volumes on a system

Example case	1	2	3	4	5	6
Total volumes available	1,024	1,024	1,024	1,024	1,024	1,024
Standard volumes	0	15	20	25	20	10
Master volumes	8	10	15	25	100	128
Snap pools	8	10	15	25	100	128
Snapshots per snap pool	126	98	64	37	8	5
Unused volumes	0	9	14	24	4	118

The example cases in Table 3 assume that all snap pools have an equal number of snapshots retained. Note that, in example case one, maximizing the number snapshots retained has the affect of minimizing the number of master and standard volumes that may be created while, in example six, maximizing the number of master volumes minimizes the number of snapshots per snap pool that can be retained. This, also, leaves a high number of volumes unused.

However, there may be no need to retain an equal number of snapshots in all snap pools. By limiting the number of snapshots in one snap pool, you can increase the number in another, add standard volumes, or add additional master volumes as your needs dictate. Unused volumes, also, provide capacity for replications, volume copies, as well as additional master or standard volumes.

In example case one, all volumes are accounted for and there is no remaining capacity for replications. If a replication was started, a standard snapshot would be deleted. See Understanding policy impacts on page 23 for more information. In example six, despite reaching the limit on master volumes in the system, a large number of unused volumes remain. These volumes may be used throughout the various snap pools, for replication, or to create additional standard volumes. However, best practice would avoid maximizing the number of volumes used on a system and allow capacity for volumes to be created for other tasks.

This document does not establish a best practice for balancing volumes within your system. This is based on your business needs.

Licensing limits

The examples in Table 3 do not account for licensing limitations.

AssuredSnap, AssuredRemote and AssuredCopy are features that are individually licensed. While AssuredRemote and AssuredCopy depend on snapshot *functionality* to perform their respective tasks, neither requires an AssuredSnap *license*.

AssuredRemote licensing does not depend on AssuredSnap licensing, though without AssuredSnap licensing the replication functionality is limited (for example, without an AssuredSnap license, a replication snapshot cannot be exported and mounted). AssuredCopy licensing, also, does not depend on AssuredSnap licensing. And AssuredSnap licensing does not automatically enable replication and volume copy functionality present.

AssuredSnap licensing permits multiple point-in-time snapshots, each of which may be replicated or volume copied. Without AssuredSnap licensing, replication and volume copy may occur only on an immediate point-in-time basis. That is, the tasks may occur on the data state as it exists at this moment in time, but snapshots may not be retained for later tasking.

Goals of a well-moderated schedule

A well-moderated schedule has as its primary goal ensuring data continuity. Continuity requirements may vary from business to business, and even volume to volume within the same business.

Prior to beginning the process of scheduling snapshots and replications, you should establish, based on specific business and regulatory needs, how often data should be recorded. These needs are driven by considerations such as frequency of data change via host I/O; disaster recovery requirements; access to data for testing, auditing, or development needs; and licensing limits (see AssuredSAN CLI Reference Guide for information about feature licensing).

Second, the schedule should account for overlapping tasks such as snapshots, replications (which may create a snapshot), snapshot rollbacks or resets (which require the master volume to be unmounted), and volume copies (which require the master volume to be unmounted and may create a snapshot).

Finally, a well-moderated schedule provides windows for tasks such as basic hardware maintenance, installing or updating firmware, and tasks specific to this process such as volume copy and snapshot rollback.

This document does not establish or provide guidance for your business needs.

Example of a well-moderated schedule

This example represents a schedule for a single controller with sixteen master volumes. This example does not take into account business requirements in your or any environment and is presented for illustration purposes only.

In this example, the top rank is snapshots, the middle is replications, and the lowest rank represents maintenance windows. See Table 4 below for a guide to the colors used.

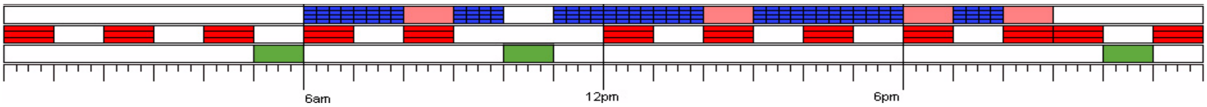


Figure 1 An example of a well-moderated schedule.

Using Figure 1 as an example, note that the twenty-four hour schedule:

- Begins snapshots on no more than four master volumes in a fifteen-minute period, and does not take a snapshot of the same master volume more frequently than once an hour.
- Replicates no more than three master volumes in a one hour period, and allows a minimum of one hour between replication tasks.
- Avoids overlap in snapshot and replication tasks. Because replication may begin by creating a new snapshot, that replication task creates a “shadow” in the snapshot schedule where other snapshot tasks should be avoided. The replications scheduled at 8:00am create a snapshot prior to replicating. See Avoiding collisions between replications and snapshots on page 14 for more information.
- Provides maintenance windows throughout the day.
- Decreases snapshot and replication frequency during non-business hours when I/O and data change are low.
- Performs a snapshot or replication prior to and after maintenance windows.

Table 4 Detailed explanation of business day activities in Figure 1

Time frame	Tasks	Color code
8:00am	Replicate volumes 13–15	🟥
9:00am	Snapshot volumes 1–16	🟦
10:00am	Maintenance window	🟩
11:00am	Snapshot volumes 1–16	🟦

Table 4 Detailed explanation of business day activities in Figure 1 (continued)

Time frame	Tasks	Color code
12:00pm	Replicate volumes 1–3	🟥
1:00pm	Snapshot volumes 1–16	🟦
2:00pm	Replicate volumes 4–6	🟥
3:00pm	Snapshot volumes 1–16	🟦
4:00pm	Replicate volumes 7–9	🟥
5:00pm	Snapshot volumes 17–32	🟦

Considerations in scheduling

Business requirements

When scheduling AssuredSnap and AssuredRemote tasks, you should consider the business requirements being placed on the system. Some examples are:

- Does the business place a higher value on the "currentness" of the snapshot data, or on replication of that data to remote volumes?
- Is successful replication to a remote system in preparation of disaster recovery a high priority?
- Do government or other regulatory requirements demand more frequent replication of data for backup or recovery purposes?
- Are there peaks or nulls in host I/O that require an inconsistent schedule?

Avoiding collisions between replications and snapshots

Depending on the mode under which replication is running, the system may take a new snapshot or may use the most current existing snapshot.

Replicate volume mode takes a new snapshot outside of the normal snapshot service prior to performing the replication. Using this mode provides more up-to-date information to the remote volume, but might interfere with the established snapshot schedule for the volume.

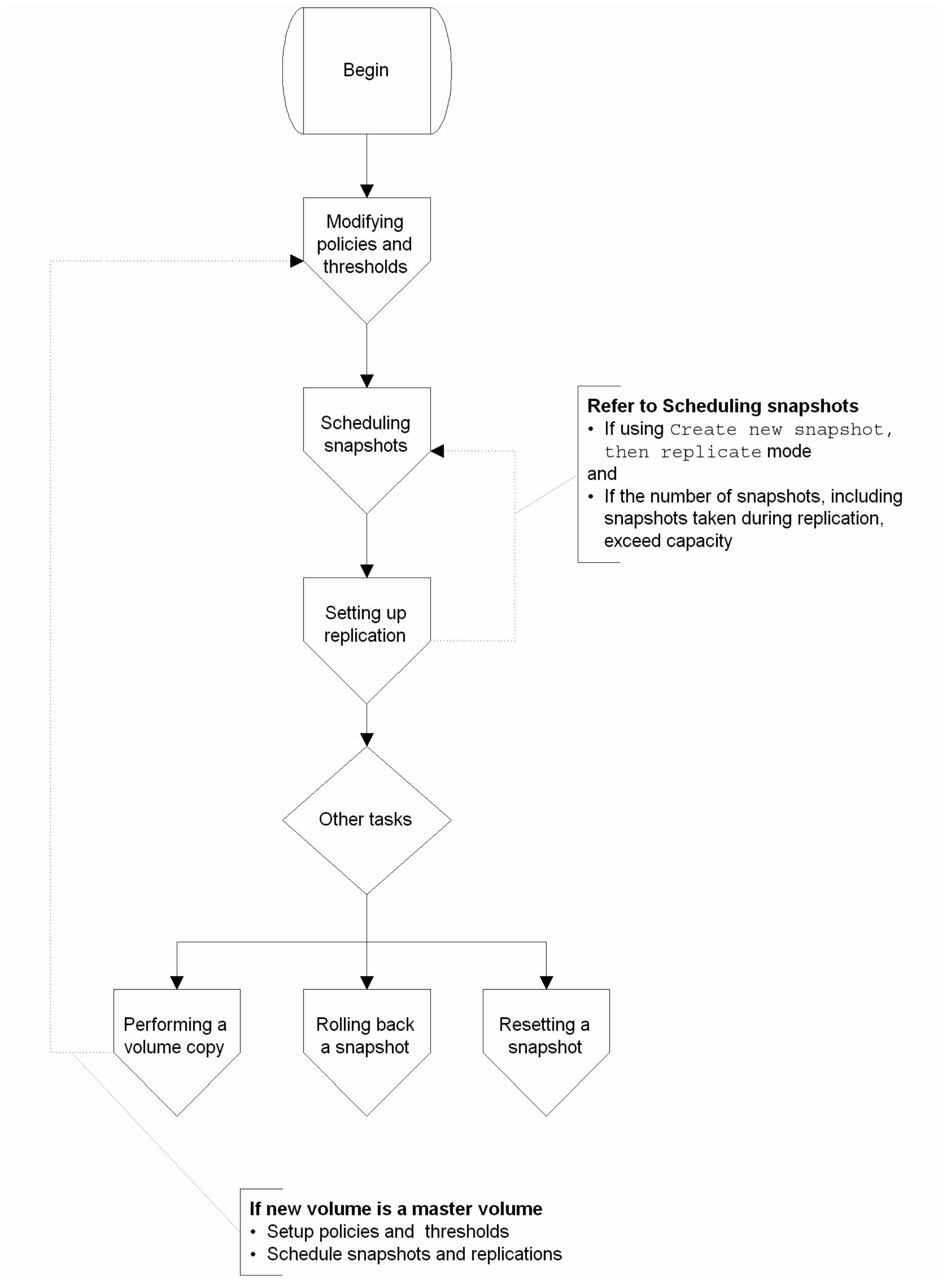
Replicate snapshot mode does not create a snapshot of the volume prior to replication and, therefore, does not interfere with the already established snapshot schedule. Using this mode may provide less up-to-date information by replicating the most recently created snapshot regardless of age, but does not interfere with the established snapshot schedule for the volume.

IMPORTANT: **Replicate snapshot** mode is age-ambivalent. That is, it uses the snapshot having the most recent timestamp, regardless of age. In environments where data frequently changes, this mode may result in replication of "stale" data.

When scheduling snapshots and replications, you should consider snapshots taken in the course of replication tasks in the count of snapshots taken at a specific time. A system performing two snapshots while concurrently performing three replications (under **Replicate Volume** mode) exceeds the four snapshot per 15-minute capacity of the system.

System capacities suggest that for best results, snapshots and replications should not be scheduled concurrently.

3 Overview


Begin
Modifying policies and thresholds
Scheduling snapshots
Setting up replication
Other tasks
Performing a volume copy
Rolling back a snapshot
Resetting a snapshot
Refer to Scheduling snapshots
• If using Create new snapshot, then replicate mode
and
• If the number of snapshots, including snapshots taken during replication, exceed capacity
If new volume is a master volume
• Setup policies and thresholds
• Schedule snapshots and replications

Purpose	• General guide to setting up a system for Snapshot, Replication, Volume Copy, Rollback and Reset
Inputs	• Master volumes
Outputs	• As determined by each referred to process

Modifying policies and thresholds

Snap pools are created when a volume is established as a “master volume.” The snap pool is the allocated destination for snapshots as created by the AssuredSnap feature, or by other features utilizing snapshots to perform their tasks.

Policies and thresholds are the controls by which snap pool content is regulated and maintained.

Thresholds are set as a percentage of space used in the snap pool. Policies determine what action to take as those thresholds are reached.

Policies and thresholds apply to snap pools regardless if Snapshots are licensed or not. In situations where AssuredSnap has not been licensed, snap pools are created for the purpose of performing the other tasks described above. Here, these snapshots cannot be modified or mapped, and are deleted when their use is completed.

Scheduling snapshots

The snapshot functionality is the primary tool by which other features such as AssuredRemote, AssuredCopy, rollback and reset perform their tasks. Both AssuredRemote and AssuredCopy features are licensed separately from AssuredSnap and do not require AssuredSnap licensing to function, but the versatility of all these features working together is enhanced with AssuredSnap licensing. For best results, consider adding AssuredSnap licensing.

Snapshot rollback and reset are functions associated with the AssuredSnap license.

Snapshots preserve a volume's data-state at the point-in-time at which the snapshot is created. The technology is fast, efficient using the copy-on-write function to capture only data that has changed. Only master volumes may create snapshots.

Replication and volume copy begin by creating a snapshot of the master volume, and while this snapshot does not count against the overall AssuredSnap licensing count, it does count against the overall volume limitation (see Balancing limits and business needs on page 11). These licensing limits are separate considerations from best practices.

Setting up replication

AssuredRemote utilizes snapshot functionality to either transfer the most recent snapshot or create a new snapshot of the primary volume and transfer it to a secondary volume. While AssuredRemote uses snapshot functionality, it is not dependant on an AssuredSnap license and snapshots taken with this feature do not count against an AssuredSnap licence count. See Licensing limits on page 12 for more information.

Because AssuredRemote depends on snapshots, you should consider business requirements placed on both features and their interdependency when scheduling either.

Performing a volume copy

AssuredCopy creates a point-in-time copy of data via snapshot functionality from a source volume and places it on a specified destination volume (the copied volume). The source may be a master or standard volume (in the case of a standard volume, it is first converted to a master volume), or a snapshot. The copied volume may be created on the same vdisk as the source or on another vdisk owned by the same controller. Because of the high I/O requirements of a volume copy and the requirement to unmount the source, you should consider both the snapshot and replication schedules for the source volume prior to performing this task.

Though AssuredCopy utilizes snapshot functionality, it is a separate feature from and does not require an AssuredSnap license. The temporary snapshot created when copying a volume is not preserved or accessible after the volume copy task completes.

The copied volume is independent of the source, and immediately diverges from the source as I/O to either begins. Unlike a snapshot which may be deleted over time, the copied volume is volatile only to the extent that I/O is explicitly directed to it making AssuredCopy an excellent tool for re-creating a development, testing, or permanent back-up (though space inefficient) volume. See Creating a recurring development or test environment on page 35 for more information.

The copied volume is independent of the source's snapshot and replications schedules. You should consider setting up snapshot and replication services for the new volume, as needed.

Licensing may affect your use of AssuredCopy and these limits are separate considerations from best practices.

IMPORTANT: Use AssuredCopy to create a persistent representation of a volume's data. Snapshots and replications are volatile and may be deleted by policy or user over time.

Rolling back a snapshot

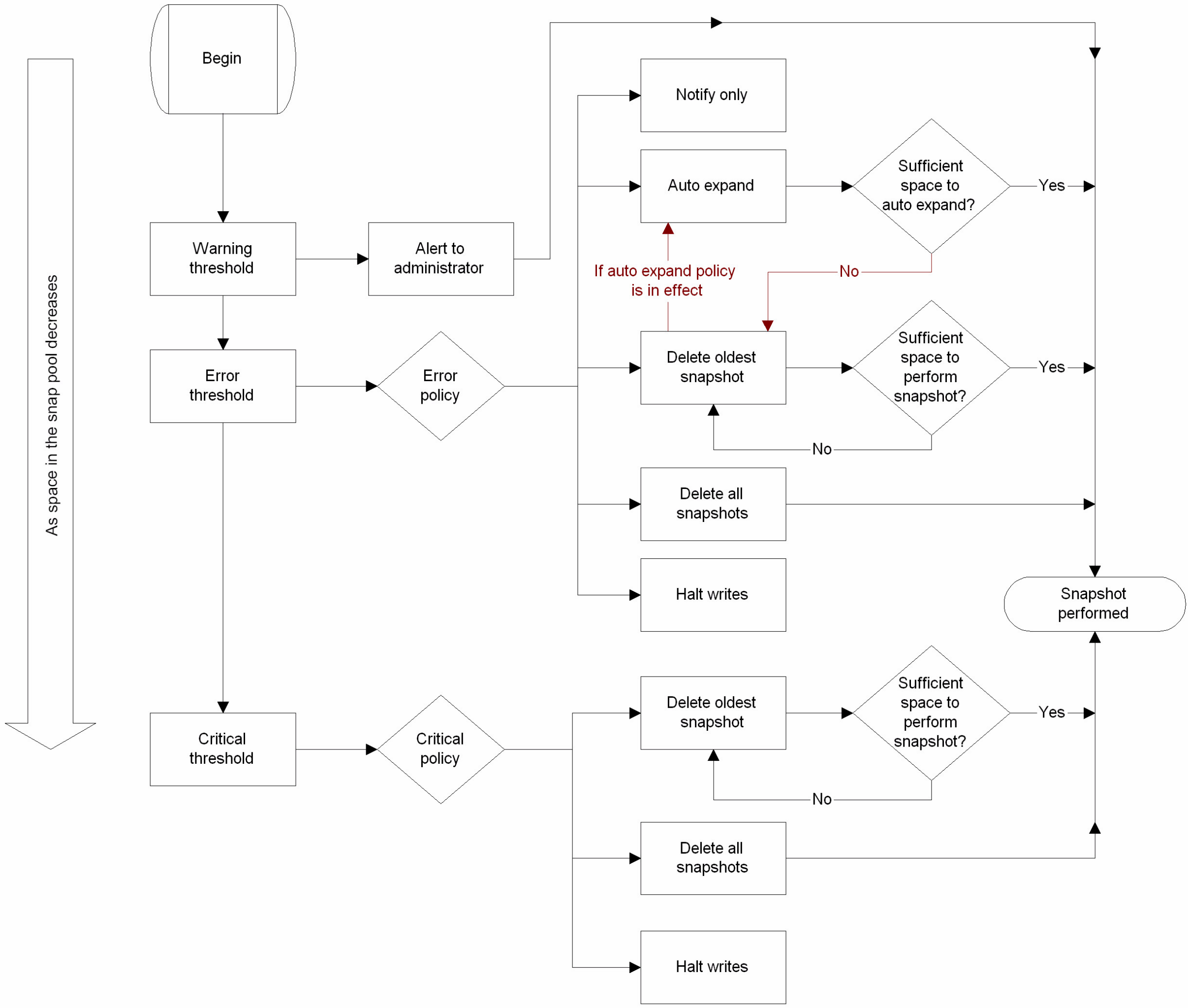
Rollback changes the data on a master volume to the state of the data in a specified snapshot. The snapshot may be either modified or unmodified. While the process is called a rollback, a master volume may be rolled back (to a prior snapshot state), or rolled forward (to a snapshot state later than the current volume state). The new state becomes "current."

Rollback differs from volume copy in that data in the volume is modified to the state of the data in a snapshot. Volume copy fully replaces all data on a volume with data from a snapshot or other source volume.

Resetting a snapshot

Reset is the antithesis of rollback. Where rollback replaces a volume with snapshot data, reset replaces an existing snapshot with volume information. Snapshot reset replaces the data in a snapshot with the current data in the associated master volume.

4 Modifying policies and thresholds



Purpose	• Set snap-pool usage thresholds that determine when associated policies will be enacted • Set policies for actions that the system should take when each threshold is reached.
Inputs	• Snap pool size • Percent of space used in the snap pool at which error policy is enacted • Percent of space used in the snap pool at which critical policy is enacted • Intentions for error policy • Intentions for critical policy
Outputs	• Established snap pool thresholds and policies

See the R/Evolution 3000 Series CLI Reference Guide for specific information about setting thresholds and policies.

1. Set the Warning threshold lower than the Error threshold. The Warning threshold default is 75%, but may be reset. Once this threshold is reached the administrator is notified. This policy is preset and cannot be changed. Continue with step 7.
2. Set Error threshold higher than the Warning threshold and lower than the Critical threshold. The Error threshold default value is 90%, but may be reset. At this threshold, the administrator is notified and the Error policy is enacted.
3. Set Error policy to one of the five following actions:
   - Notify only. As with the Warning threshold, no additional action is taken.
   - Auto expand. The snap pool is expanded by the pre-determined amount as set by the `set snap-pool-policy autoexpansionsize` command. Default expansion is 10GB.
     If sufficient space to expand the snap pool is available, the snap pool is expanded. Continue with step 7.
     If insufficient space to expand the snap pool is available, the `Delete Oldest` snapshot policy is repeated until sufficient space is available.
   - Delete oldest snapshot. The oldest snapshot is deleted.
     If sufficient space to perform the snapshot is available, Continue with step 7.
     If insufficient space to perform the snapshot is available, the `Delete Oldest` snapshot policy is repeated until sufficient space is available. Then continue with step 7
   - Delete all snapshots. All snapshots in the snap pool are deleted.
   - Halt writes. All writes to the snap pool cease until the administrator takes manual action to free space in the snap pool. This policy should be set only when an administrator familiar with policies is available to immediately address the issue.

   △ **CAUTION:** Understand your business needs prior to implementing any policy other than `Notify only`. Data loss may occur with any of these policies. See Understanding policy impacts below for more information

4. Critical threshold is preset to 98% of the snap pool size and cannot be changed.
5. Set Critical policy. Critical policy is set to one of three action.
   - Delete oldest snapshot. The oldest snapshot is deleted.
     If sufficient space to perform the snapshot is available, continue with step 7.
     If insufficient space to perform the snapshot is available, the `Delete Oldest` snapshot policy is repeated until sufficient space is available. Then continue with step 7
   - Delete all snapshots. All snapshots in the snap pool are delete.
   - Halt writes, as in step 3.

6. Halt writes, as in step 3.
7. Snapshot is performed.

Understanding policy impacts

The policies set in this process determine the automated way in which snapshots are retained and deleted; however, it is always preferable for you to make the decision on how snapshots are managed.

Policies such as **Delete oldest snapshot** and **Delete all snapshots** do not apply business logic to the delete decision and may delete snapshots that have been mounted or modified. You may set retention priorities for a snap pool as a way of suggesting that some snapshots are more important than others, but these priorities do not ensure that any specific snapshot is protected.

△ **CAUTION:** Understand your business needs prior to implementing these policies. Even an exported snapshot may be deleted under either of these policies.

Similarly, the **Halt writes** policy can be just as detrimental to data continuity. When the snap pool reaches a threshold at which data is no longer written to disk, the impact is that snapshots no longer represent the most current data state. While snapshots are protected, new data is not.

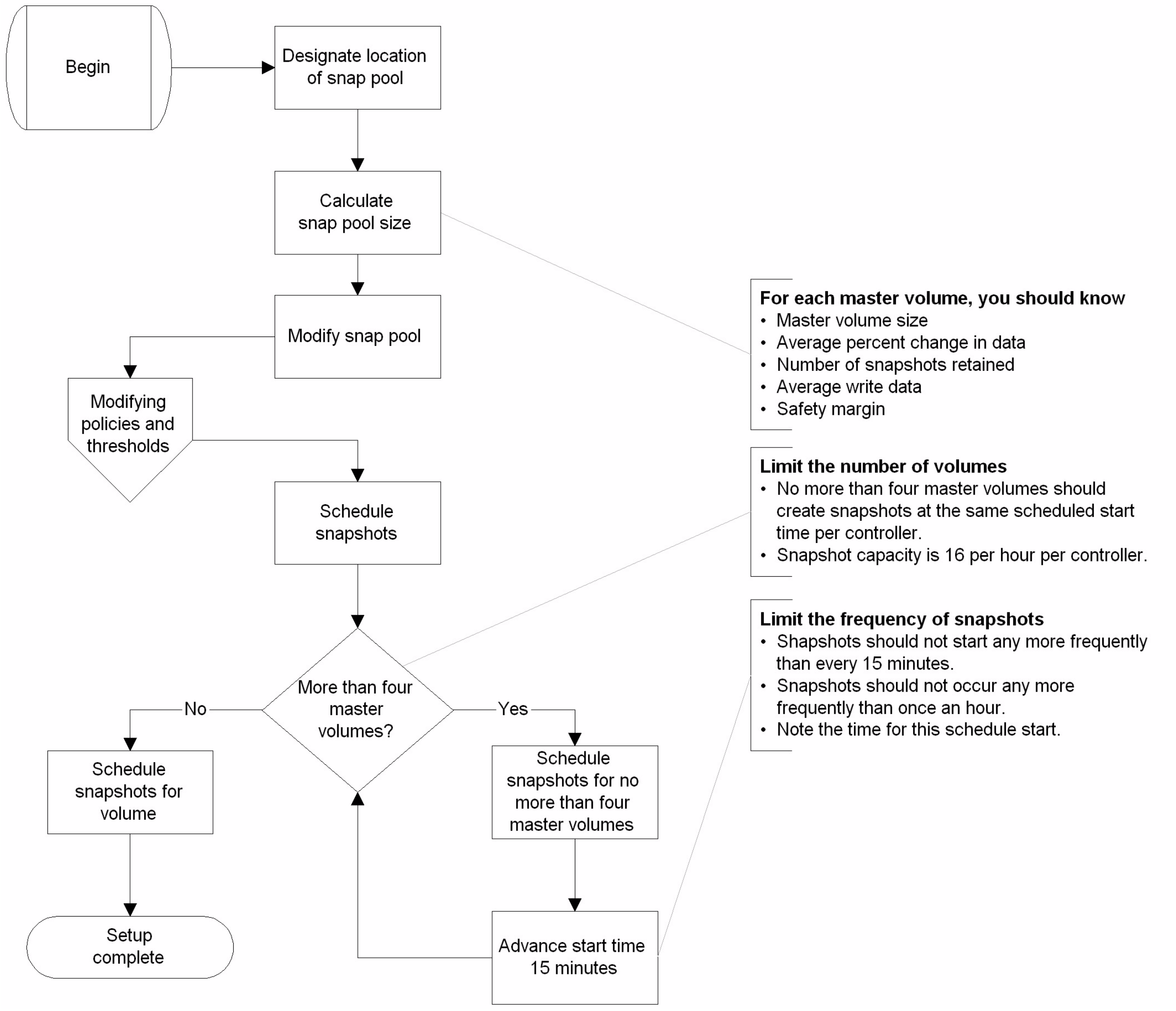
Auto expand allows writes to continue to the snap pool, but consumes volumes. Refer to Balancing limits and business needs on page 11 for information about volume limits. Once a volume limit is reached, no other snapshots or replications are created until a volume is deleted.

Snap pool maintenance is very important. Inadvertent deletes or write cessation can be avoided with some common sense maintenance approaches.

- Designate a person or persons whose responsibility is maintaining adequate space in snap pools for additional snapshots.
- Monitor the total number of volumes on the controller to avoid unintentional deletions when volume limits are reached.
- Restrict undesignated persons from deleting snapshots.
- Determine ahead of time which snapshots may be deleted and do so as part of a regular maintenance plan. Application logic does not differentiate between snapshots that are mounted or in some other way important, and may unintentionally delete snapshots you would otherwise retain. Your business logic should preclude deleting mounted or modified snapshots.
- Frequently re-evaluate the snap pool size and adjust as necessary. Refer to Scheduling snapshots on page 25 for more information regarding snap pool sizing.

IMPORTANT: When the system volume or vdisk limit is reached, the **Delete oldest snapshot** policy is immediately enforced. This delete policy is separate from snap pool space limits and is not configurable.

5 Scheduling snapshots


Begin
Designate location of snap pool
Calculate snap pool size
Modify snap pool
Modifying policies and thresholds
Schedule snapshots
More than four master volumes?
No
Yes
Schedule snapshots for volume
Setup complete
Schedule snapshots for no more than four master volumes
Advance start time 15 minutes

For each master volume, you should know

- Master volume size
- Average percent change in data
- Number of snapshots retained
- Average write data
- Safety margin

Limit the number of volumes

- No more than four master volumes should create snapshots at the same scheduled start time per controller.
- Snapshot capacity is 16 per hour per controller.

Limit the frequency of snapshots

- Shapshots should not start any more frequently than every 15 minutes.
- Snapshots should not occur any more frequently than once an hour.
- Note the time for this schedule start.

Purpose	• Calculate required size of snap pool for a set of master volumes on a single controller • Schedule snapshots to reduce possibility of errors
Inputs	• Volume used for snap pool • Number of master volumes to snapshot • Master volume sizes • Amount of data change per master volume • Number of snapshots that will be modified
Outputs	• Calculated snap pool size • Completed snapshot schedule • Number of snapshots per fifteen-minute period

Scheduling includes determining how much information will change, when it will change and how often. Collect this information prior to setting up the schedule. Each controller has the processing capacity to create a maximum of 16 snapshots per hour.

Snapshot schedules may be set up through the CLI or WBI.

1. Designate location for snap pool. Snapshots are I/O intensive, and when considering the location of the snap pool, consider drive size and speed of the owning vdisk. For best snapshot and replication performance, master volumes and snap pools should not use the same vdisk.
2. Calculate snap pool size. Use this formula for each master volume on the controller:

			Example	
For each master volume to be snapped		Master volume size	20	GB
	x	Average percent of change in data	10	%
	x	Number of snapshots retained	6	
	+			
		Master volume size	20	GB
	x	Number of snapshots modified	5	
	x	Average write data	7	%
	=	Subtotal for this master volume	19	GB
		Sum for all master volumes	19	GB
	+	Reserved for snap pool usage	5	GB
	x	Safety margin	25	%
		Total snap pool space required	30	GB

IMPORTANT: The snap pool minimum size is either 6 GB or 20% of the volume size, whichever is smaller. If the "Total snap pool space required" calculated in the formula above is less than 6 GB, set 6 GB as the snap pool size.

3. Modify the snap pool using the resulting calculations from step 2.
4. Determine and implement the Policies and Thresholds for this snap pool. See Modifying policies and thresholds on page 21.
5. Schedule snap shots. Your snapshot schedule should:
   - Schedule no more than four master volumes to take snapshots in any fifteen-minute period.

- Schedule master volumes to take snapshots no more frequently than once an hour. This gives AssuredSnap adequate time to complete the snapshot before beginning again.
- Provide maintenance windows by allowing exclusion time in the snapshot schedule,
- Attempt to schedule that time during low host I/O periods.

6. Are there more than four master volumes that require AssuredSnap service? Up to four master volumes may begin snapshots within the same fifteen-minute period.

IMPORTANT: Consider AssuredRemote in this count of snapshots. See Considerations in scheduling on page 14. One replication mode creates a new snapshot prior to running. This snapshot should be counted in the total number snapshots taken in a given time period.

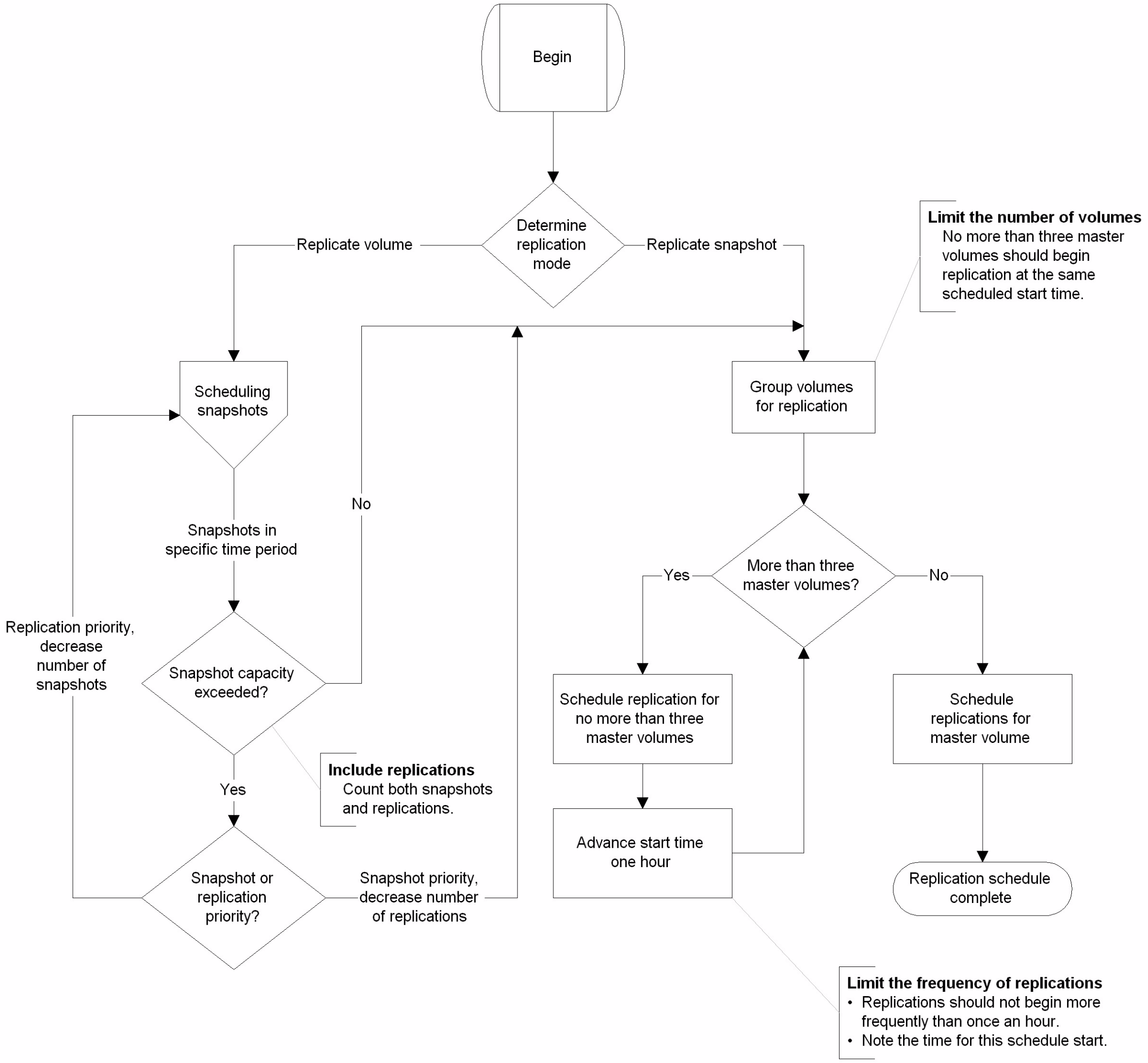
- If more than four, you may continue to schedule master volumes to create snapshots at the same start time. However, once you reach the fifth master volume, continue with step 7.
- If less than four, you may continue to schedule master volumes to create snapshots at the same start time. Continue with step 5.

7. Advance the snapshot start time by a minimum of fifteen minutes. Advancing the start time allows the previous snapshot schedule to complete prior to starting the next scheduled service.

IMPORTANT: Advancing the start time by 15 minutes maximizes the groups of master volumes that may be scheduled in a single hour. Advancing the start time more than 15 minutes does not fall outside acceptable parameters. However, if there are master volumes that snapshot every hour, advancing several groups by more than 15 minutes eventually causes overlap in the schedule and potentially impacts data reliability.

IMPORTANT: The `Halt writes` snap pool policy, Modifying policies and thresholds on page 18, does not allow the snapshot service to continue without direct intervention by a system administrator. In environments where data continuity is highly important, this policy should be enacted cautiously. As the snapshot schedule gets out of synchronization while waiting for intervention, data becomes progressively stale.

6 Setting up replication


Begin
Determine replication mode
Replicate volume
Replicate snapshot
Limit the number of volumes
No more than three master volumes should begin replication at the same scheduled start time.
Scheduling snapshots
Group volumes for replication
No
Snapshots in specific time period
Yes
More than three master volumes?
No
Replication priority, decrease number of snapshots
Snapshot capacity exceeded?
Schedule replication for no more than three master volumes
Schedule replications for master volume
Include replications
Count both snapshots and replications.
Yes
Advance start time one hour
Snapshot or replication priority?
Snapshot priority, decrease number of replications
Replication schedule complete
Limit the frequency of replications
• Replications should not begin more frequently than once an hour.
• Note the time for this schedule start.

Purpose	• Schedule replications • Eliminate conflicts between replication and snapshot schedules
Inputs	• Number of volumes for replication • Intended start time of replications • Snapshot schedule for volumes being replicated • Determination of snapshot or replication priority for system resources
Outputs	• Completed replication schedule • Under certain modes, updated snapshot schedule that does not conflict with replication

Scheduling AssuredRemote service is similar to setting up AssuredSnap schedules. Because replications may begin with a snapshot, take snap pool sizing and snapshot scheduling into account as well.

Replication schedules may be set up through the CLI or WBI.

1. Determine which mode the replication service is running. See Considerations in scheduling on page 14 for more information about differing replication modes.

   `Replicate snapshot` mode uses an existing snapshot as the data source. The advantage of this mode is that replication can occur independent of the snapshot schedule. The disadvantage is that the service may replicate data that is older than desired.

   `Replicate volume` creates a new snapshot then replicates immediately. The advantage of this mode is that the data is more consistent with the current point-in-time representation because the snapshot has just been taken. However, this precludes replication and snapshot schedules from running concurrently.

   If running in `Replicate volume` mode, continue with step 2.

   If running in `Replicate snapshot` mode, continue with step 4.

2. Review Scheduling snapshots on page 25 prior to scheduling replications. Include the replication schedule when totalling the number of master volumes taking snapshots within a fifteen minute time block.

   If the number of snapshots in a given time block exceeds the snapshot capacity for that period, determine if snapshots or replication take priority.

   If snapshots take priority, continue with step 4

   If replication take priority, return to Scheduling snapshots on page 25 and reschedule or constrain snapshots to accommodate the replication schedule.

   NOTE: Avoid scheduling snapshots and replications within the same block of time to prevent these scheduling collisions. See Avoiding collisions between replications and snapshots on page 14 for more information.

3. Limit replications to three in the time period to avoid collisions with snapshot.
4. Group master volumes for replication.

   IMPORTANT: Maximum replication capacity is three per hour, with each replication occurring no closer than one hour apart.

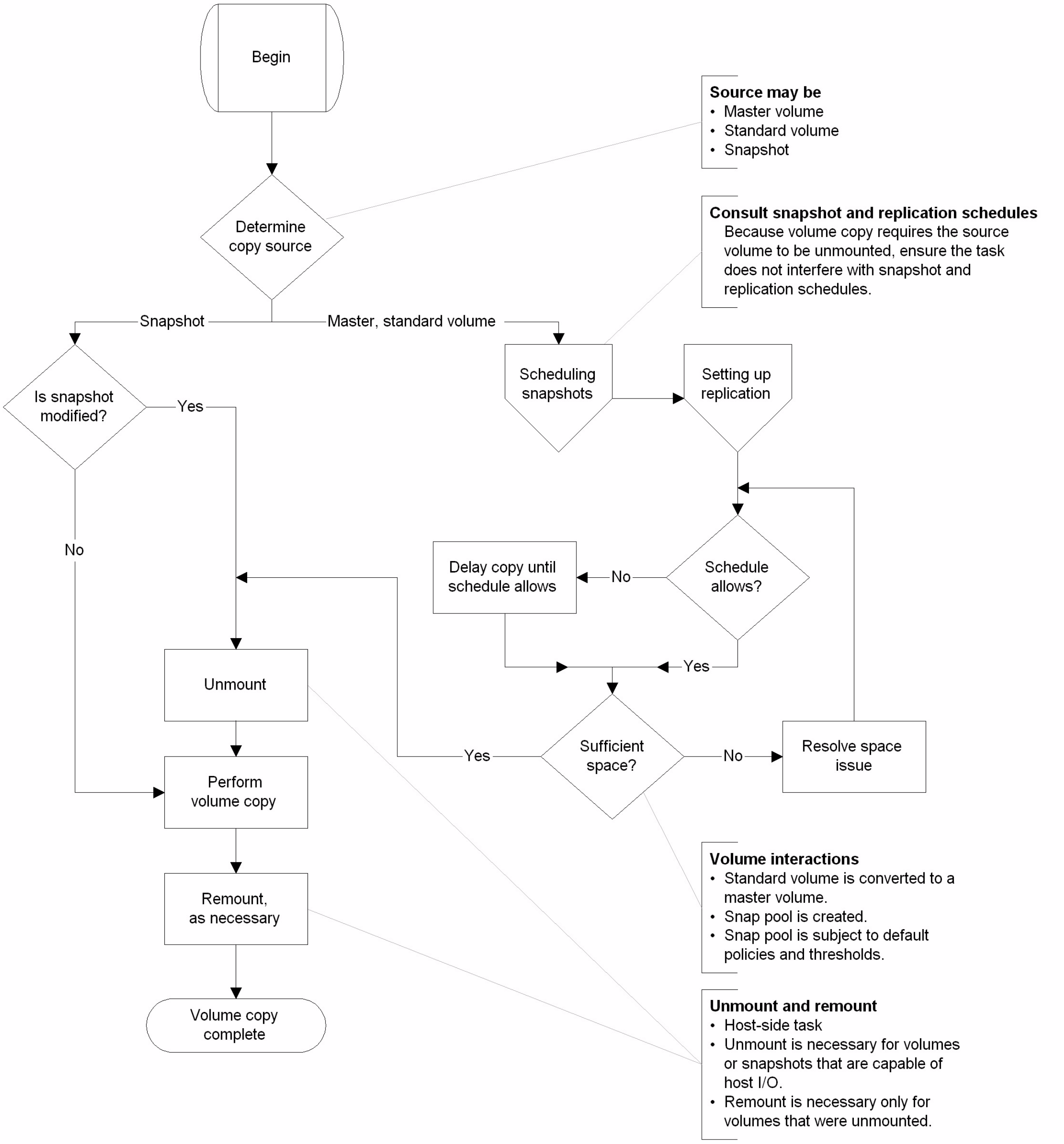
   If more than three, or as prescribed by step 3, reduce the number of volumes to be replicated.

   If less than three, or as prescribed by step 3, continue with step 7.
5. Reduce the number of replications.
6. How much time between replications?

If less than one hour, increase the amount of time between replication recurrence.

7. Replication setup is complete

7 Performing a volume copy



Source may be

- Master volume
- Standard volume
- Snapshot

Consult snapshot and replication schedules

Because volume copy requires the source volume to be unmounted, ensure the task does not interfere with snapshot and replication schedules.

Volume interactions

- Standard volume is converted to a master volume.
- Snap pool is created.
- Snap pool is subject to default policies and thresholds.

Unmount and remount

- Host-side task
- Unmount is necessary for volumes or snapshots that are capable of host I/O.
- Remount is necessary only for volumes that were unmounted.

Purpose	• Create an independent copy of a volume • Avoid conflicts with snapshot and replication schedules that might interfere with data integrity
Inputs	• Source volume to be copied • Location of destination volume • Snapshot schedule for destination volume • Replication schedule for destination volume • Modified or unmodified data if copying a modified snapshot
Outputs	• Completed volume copy

Volume copy may be set up through the CLI or WBI.

To create a volume copy:

1. Determine source for the copy.
   - From an existing snapshot. Any snapshot, modified or unmodified, in a snap pool may be the source of a volume copy. Further, a volume copy of a modified snapshot may or may not include the modified data. Prior to copying a snapshot, you should determine if you want modified or unmodified data from that snapshot. Continue with step 2.
   - From a master volume, continue with step 3.
   - From a standard volume. A volume copy performed on a standard volume first converts that volume to a master volume. A snap pool is automatically created with a size that is the greater of either 20% of the volume size or the minimum snap pool size. Default policies and thresholds are enacted as well. A snapshot is, then, taken of the volume and this is the source of the volume copy. See Modifying policies and thresholds on page 21 for more information about policy and threshold defaults. Continue with step 3.
2. Is the snapshot modified or a snapshot that may be modified?

   If yes, the snapshot must first be unmounted. Continue with step 9

   If no, continue with step 10
3. Consult snapshot schedule for the controller on which the source volume resides.
4. Consult replication schedule for the controller on which the source volume resides.
5. Do the snapshot and replication schedules allow time to perform the volume copy? A volume copy of a master or standard volume begins with a snapshot. Reviewing the snapshot and replication schedules allow you to determine if this snapshot exceeds the snapshot capacity of the controller.

   If yes, continue with step 7.

   If no, continue with step 6.
6. Delay the volume copy until a period in the schedule allows the volume copy to begin.
7. Does sufficient space exist in the snap pool to take a snapshot?

   If yes, continue with step 9.

   If no, continue with step 8.
8. Resolve snap pool space issues.
   - Expand the snap pool
   - Delete snap shots

   Because these tasks may require significant time, return to step 5.
9. Unmount the source volume or snapshot. See Unmounting a volume on page 9 for more information.
10. Perform the volume copy.
11. Once the volume copy begins, remount the source volume. If host I/O resumes prior to the completion of the volume copy, that data will not be present in the volume copy. Only data written prior to the unmount is copied. A remounted volume is immediately available for host I/O, regardless of volume

copy completion. A remounted modified snapshot is not available for host I/O until the volume copy completes.

12. Once the volume copy completes, the new volume is independent from the original volume or snapshot. Some follow up tasks you may consider performing are:
    - Convert the new volume to a master volume to permit AssuredSnap and AssuredRemote services.
    - Setup AssuredSnap services if you have converted the new volume to a master volume.
    - Setup snap pool policies and thresholds if you have converted the new volume to a master volume.
    - Setup AssuredRemote services if you have converted the new volume to a master volume.
    - Convert the source volume back to standard if the volume copy was performed on a standard volume. This is not required; but eliminates the overhead of maintaining separate snapshot and replication schedules, and the additional space requirements of this volume's snap pool.

Creating a recurring development or test environment

AssuredRemote is a more reliable way to "reset" an environment than snapshot, snapshot rollback, or snapshot reset. As time passes, snap pool policies might force the deletion of a needed snapshot.

A copied volume is a good interim archive as it preserves data at a specific point in time. Using AssuredCopy to create a recurring environment is not without disadvantages; chiefly, the increased space requirements to store one pristine volume while testing or development occur on the other make this a less desirable option than a well-maintained snap pool. See Understanding policy impacts on page 23 for more information about snap pool maintenance.

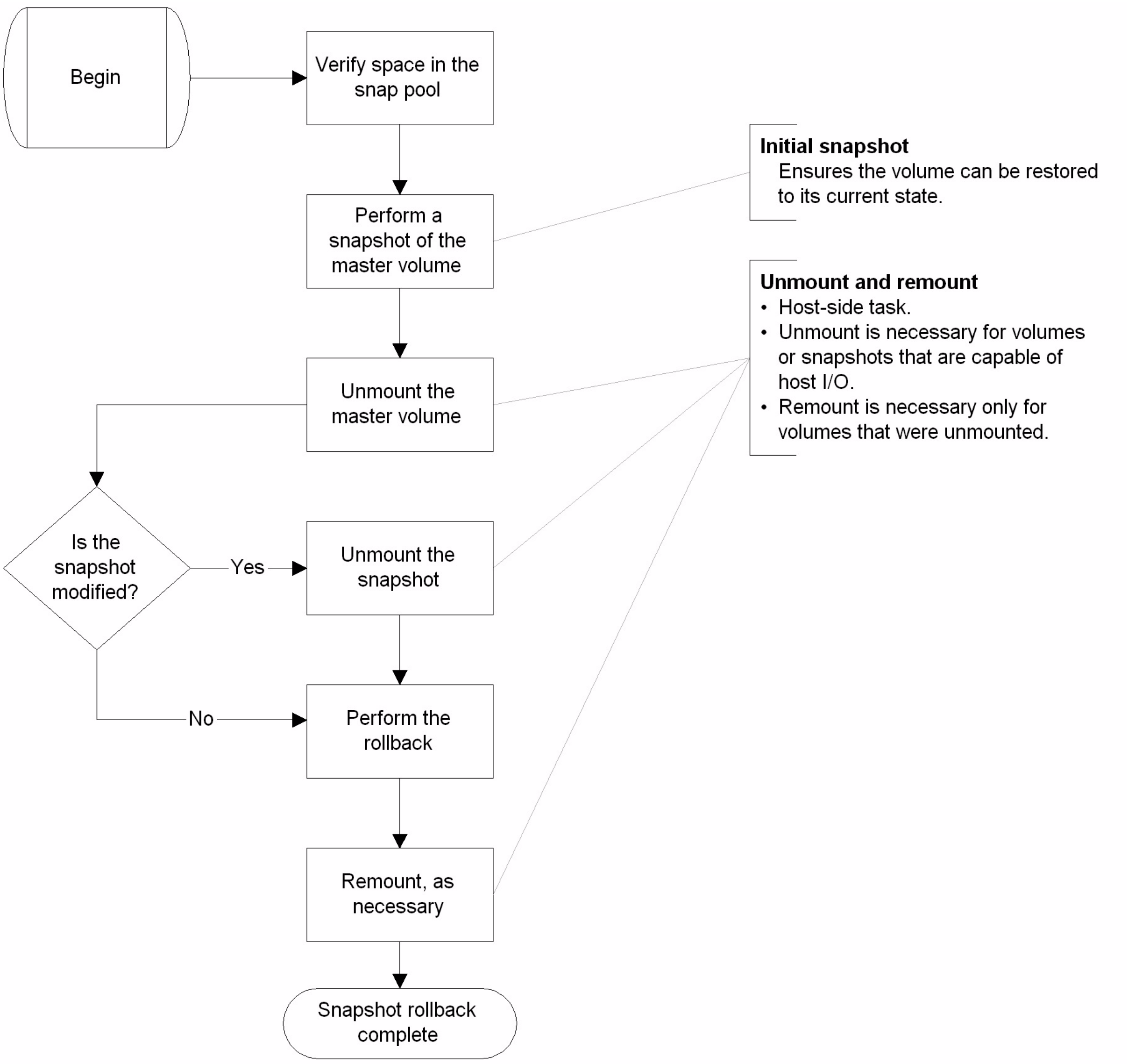
To create a recurring development or test environment:

1. Configure a volume that is used for testing or development with the information needed for those efforts.
2. Perform a volume copy to a new volume. Because this new copy is not intended for host I/O, volume speed and accessibility are less important.
3. Perform testing or development against the source volume as needed.

To "reset" the environment:

1. Unmount the development or test volume.
2. Perform a volume copy from the copied volume back to the original.
3. Remount the volume.

8 Rolling back a snapshot


Begin
Verify space in the snap pool
Perform a snapshot of the master volume
Unmount the master volume
Is the snapshot modified?
Yes
No
Unmount the snapshot
Perform the rollback
Remount, as necessary
Snapshot rollback complete
Initial snapshot
Ensures the volume can be restored to its current state.
Unmount and remount
• Host-side task.
• Unmount is necessary for volumes or snapshots that are capable of host I/O.
• Remount is necessary only for volumes that were unmounted.

Purpose	• Replace volume data with data from a snapshot
Inputs	• Specific volume which data is to be replaced • Specific snapshot which data is used
Outputs	• Replaced volume data

△ **CAUTION:** Performing a snapshot prior to rollback provides a point-in-time to which you can return. All data on the master volume that differs from the snapshot is lost with this task.

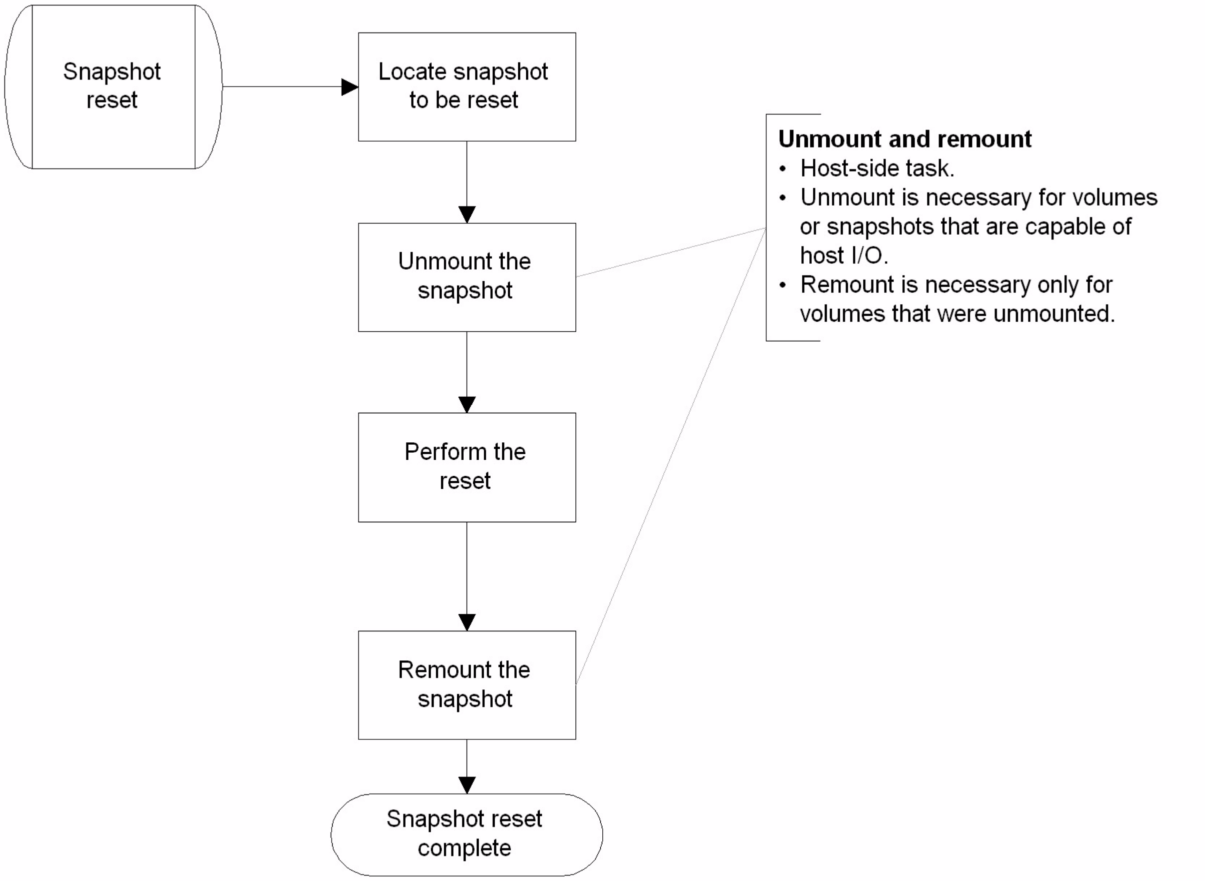
1. Consult the snap pool to determine if sufficient space exists to create a snapshot.

   IMPORTANT: Be aware of thresholds and policies. A snapshot that enacts a “delete” policy could remove the snapshot to which you intend to roll the master volume.

2. Create a snapshot of the master volume.
3. Unmount the master volume. See Unmounting a volume on page 9 for more information.
4. Unmount the snapshot, if the snapshot has data that is or has been modified.
5. Perform the rollback. Host I/O to the master volume may resume after the rollback has been initiated. Access to the master volume and Snapshot is restricted until the rollback is complete.

   IMPORTANT: A rollback cannot be aborted once started.

9 Resetting a snapshot



Unmount and remount

- Host-side task.
- Unmount is necessary for volumes or snapshots that are capable of host I/O.
- Remount is necessary only for volumes that were unmounted.

Purpose	• Deletes the data in a snapshot and resets it to the current data in the master volume
Inputs	• Specific snapshot which data is to be replaced • Specific volume which data is used
Outputs	• Snapshot reset with current data from volume

△ **CAUTION:** Performing a snapshot prior to reset provides a point-in-time to which you can return. All data in the snapshot is lost and replaced with the data current to the master volume during a snapshot reset.

1. Locate the snapshot to be reset.
2. Unmount the snapshot to be reset. See Unmounting a volume on page 9 for more information.
3. Perform the reset.
4. Remount the snapshot.

Index