ADVANCED TECHNOLOGY GROUP (ATG)

Accelerate with ATG Webinar: FlashSystem Safeguarded Copy

Matt Key
Principal Storage Technical Specialist
IBM Advanced Technology Group – FlashSystem
IBM Technology
mkey@us.ibm.com

Byron Grossnickle
IBM Storage Virtualize/FlashSystem SME
byrongro@us.ibm.com

Meet the Speakers – Matt Key

Matt Key is a 20-year veteran of solid state storage and came into IBM through the 2012 acquisition of Texas Memory Systems, the Houston-based engineering group behind the FlashCore Modules in IBM's distributed storage portfolio. Currently, he is the technical lead for Flash in the Advanced Technology Group (ATG), the client-facing group of subject matter experts across the portfolios of storage, servers, and software. Matt graduated Texas A&M (WHOOP!) in 2006 with an engineering degree in telecommunications.

Meet the Speakers

Byron Grossnickle is an IBM Storage Technical Specialist concentrating on Storage Virtualize software. This includes FlashSystem, SVC, and Storage Virtualize for Public Cloud. Byron has been with IBM 21 years exclusively in storage. Prior to working for IBM, Byron spent 6 years engineering storage in the Telcom Industry. Prior to that he worked 8 years in healthcare IT. Byron lives in the Kansas City area and is available to travel to customer engagements.

What is a Safeguarded Copy (SGC)

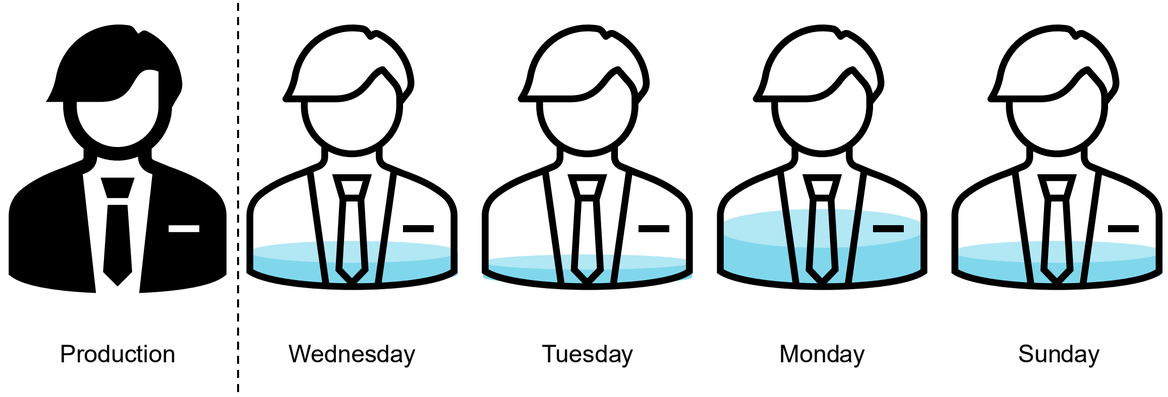
Cyber-resilient copies of volumes that are:

- Immutable by design (Application vector)
- Logically air-gapped (Control-plane vector)
- Separation of duties (Personnel vector)

“Snapshots with extra protections”

Each copy is a space-efficient bucket of changes since the most recent version

- Tracked by linked-lists instead of costly, dedupe tables



Volume Group Snapshots vs Safeguarded Copy

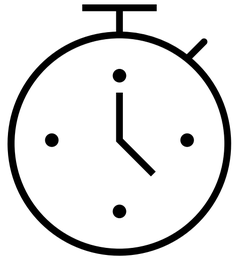
Volume Group Snapshots (VGS) are naturally immutable and logically air gapped

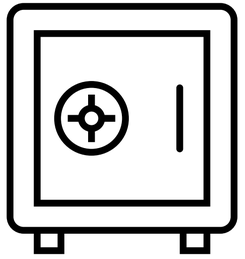
Hidden, inaccessible volume-like objects retain the changed data

Safeguarded Copy protects capacity on the personnel vector whereas a lone, storage admin cannot expire the data

Two-Person Integrity separates authority and privilege so protection can still reside within the team

Because of the linked-list nature, SGC will retain data inheritance when deleting in-between snapshots





Volume Group Snapshots		Safeguarded Copy
✓	Immutable Contents	✓
✓	Hidden objects	✓
✓	Restore over source	✓
✓	Recover to new volumes	✓
✓	Space-efficient	✓
✗	Requires elevated privileges to delete	✓
Optional	Expiration date	Required

The Value It Brings

Always consistent

Each copy is a crash-consistent version of the host. Syncing (“Quiescing”) data from the application will get you “application consistent” when orchestrating a SGC

Quick to execute

Data does not have to wait for array cache to flush. Starting in Virtualize 8.7, host writes track immediately

Quick to restore

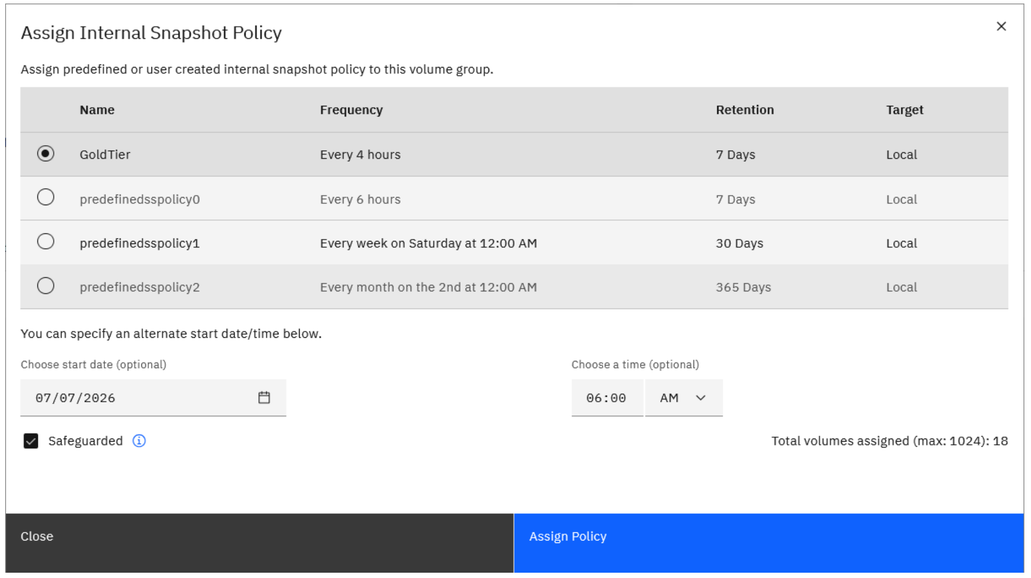
Reverse mapping the relationship between any SGC and the production volumes is a sub-second operation. Size of the data or volumes have no influence on this performance

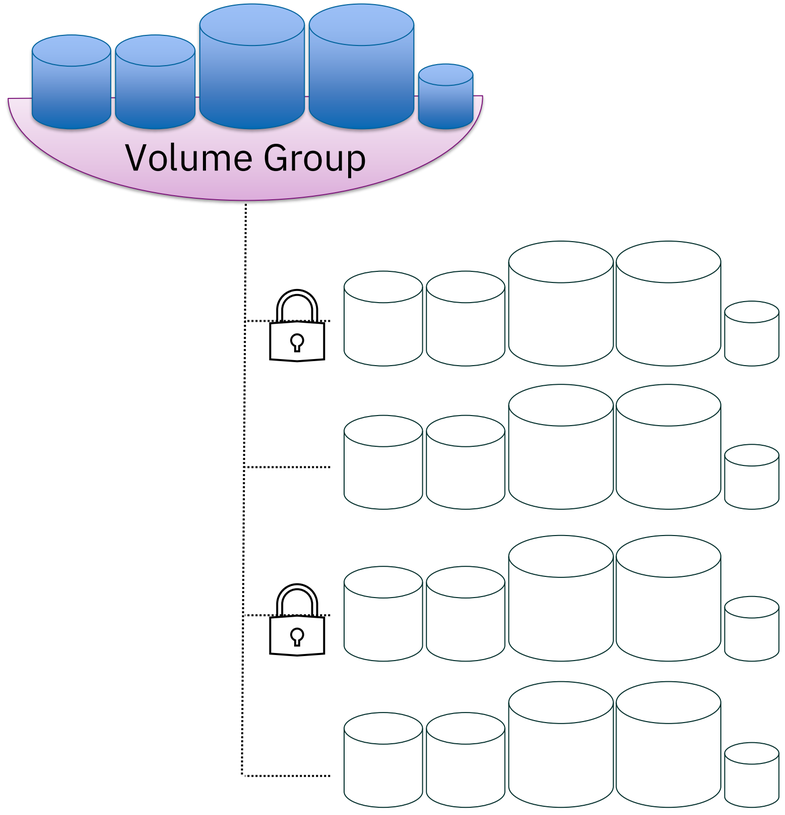
Quick to recover

Spinning up a new set of volumes sourced by linked-list from SGC is just a few seconds

Implementing Safeguarded Copy

1. Assign volumes into a Volume Group
2. Apply policy to Volume Group





Snapshots automatically generated or triggered by an external scheduler (IBM Defender Copy Data Management or Copy Services Manager)

Intermixes safely, securely with standard Volume Group Snapshots

Two Person Integrity: Time based user promotion

Under TPI, superuser is locked down

To work with elevated privileges, a second RestrictedSecurityAdmin can approve time-based requests

Privilege can be immediately revoked, even by SEIM (auditlog across syslog)

IBM Service Reps use token-based authentication

“Keep storage within storage” mentality or push authorization through CISO office

Elevated privilege is only way to proactively remove protected capacity or influence settings such as NTP

Due to application changes, Tom needs to reconfigure his Safeguarded Copy policy

RestrictedSecurityAdmin

Scott

Tom requests elevated access in GUI or CLI.

Request

30-min

Tom needs to request that another Security Admin approves his request

RestrictedSecurityAdmin

Abby

SecurityAdmin

Abby is aware of the application changes and approves the elevated access

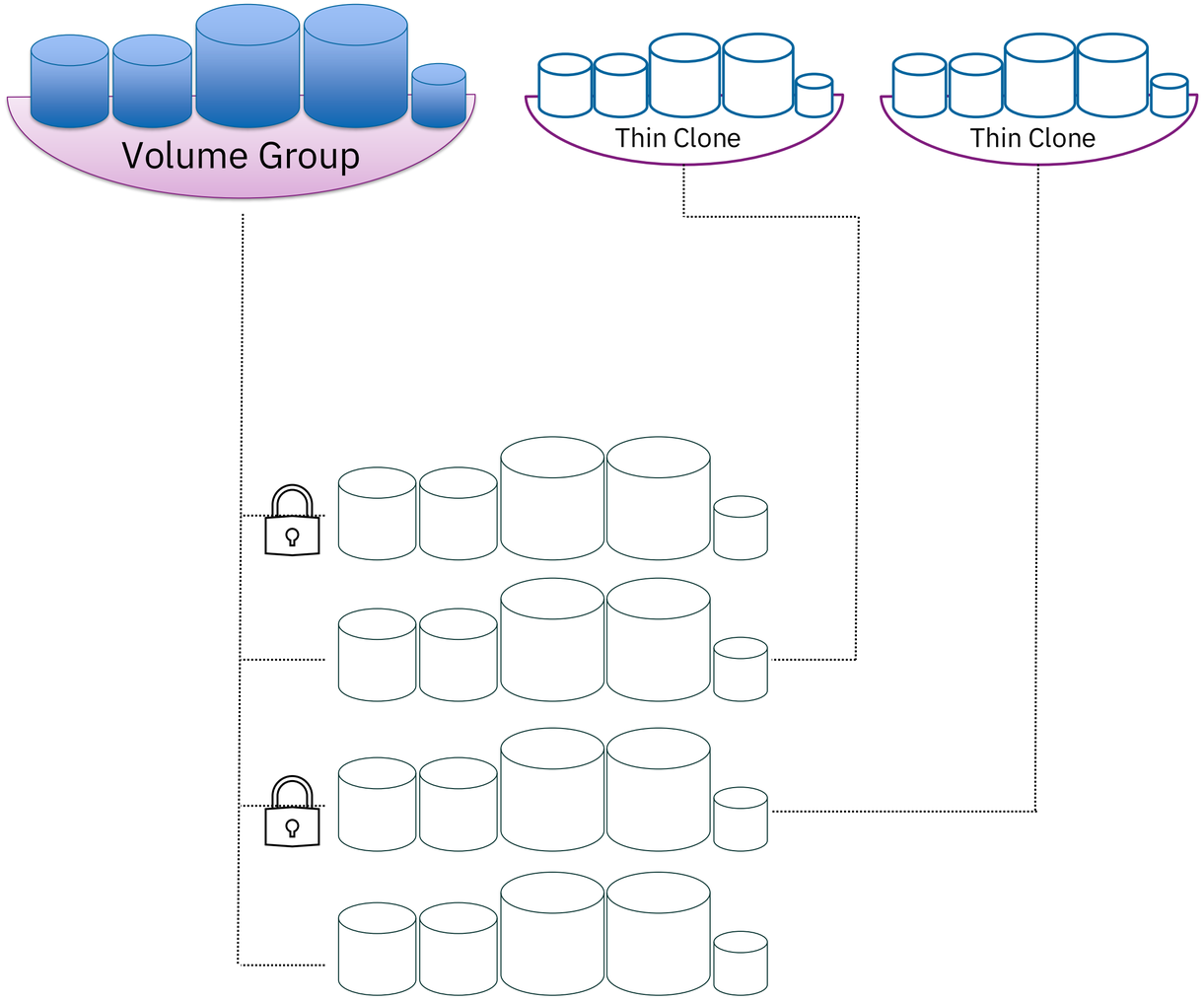
Tom has 30-min of elevated access to perform the changes on Safeguarded Policy before the system terminates his access.

RestrictedSecurityAdmin

Scott

Abby monitors the audit log to ensure Tom is performing the desired actions. If necessary, Abby can cancel his elevated access with a click of a button.

Using Safeguarded Copies for Reporting/Backup Apps



Thin Clones are host-mountable volumes that reference the snapshot (or next newest grain in linked-list) for the data

Writes to the Thin Clones are owned by the Thin Clone and dereference just those blocks from the linked-list

- Contents of snapshots are read, but never written

Thin Clones can be refreshed or even converted to Thick Clones to be independent copies

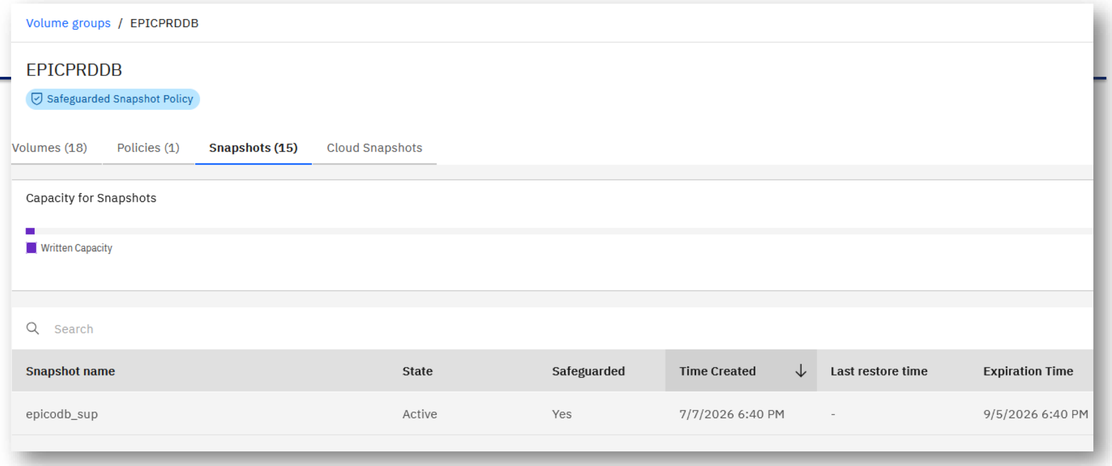
Never have to wait for a data copy to complete, thin/thick clone contents are all immediately available

Scheduler, Ad-hoc, and Orchestration

Internal scheduler allows for simple, crash-consistent copies

IBM Defender CDM and CSM provide portals for app tie-in

Large 3rd party ecosystem of backup software



FlashSystem.ai: “Assign the Gold snapshot policy to EPICPRDDB volume group and flag it as safeguarded”

CLI or RBASH: `>addsnapshot -volumegroup EPICPRDDB -name epicodb_sup -safeguarded -retentiondays 60`

```
Snapshot, id [7], successfully created or triggered
```

REST:

```
curl -L -X POST '<system_ip>:7443/rest/v1/addsnapshot' -H 'X-Auth-Token: <token>'
     -H 'Content-Type: application/json' --data-raw '{…}'
```

```
{
  "volumegroup": "string",
  "volumes": "string",
  "parentuid": 0,
  "pool": "string",
  "prepare": true,
  "ignorelegacy": true,
  "trigger": "string",
  "name": "string",
  "safeguarded": true,
  "triggerid": 0,
  "retentiondays": 0,
  "retentionminutes": 0,
  "commitgenerationsnapshotid": 0
}
```

Autosnapshot

IBM FlashSystem includes always-on Ransomware Threat Detection (RTD) rooted in IBM FlashCore Modules

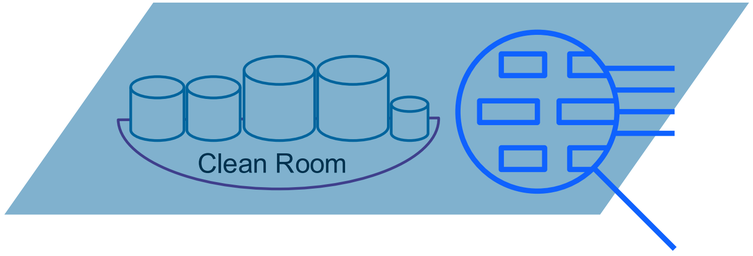
- Looks for I/O mannerisms of attackware (exfiltration, full drive encryption, partial encrypt & overwrite, etc)
- Quickest detection available for block storage
- No performance overhead…seriously

In IBM Storage Virtualize 9.1.1, lsanomalydetetion/chanomalydetection options to allow for automatic snapshot in RTD detection

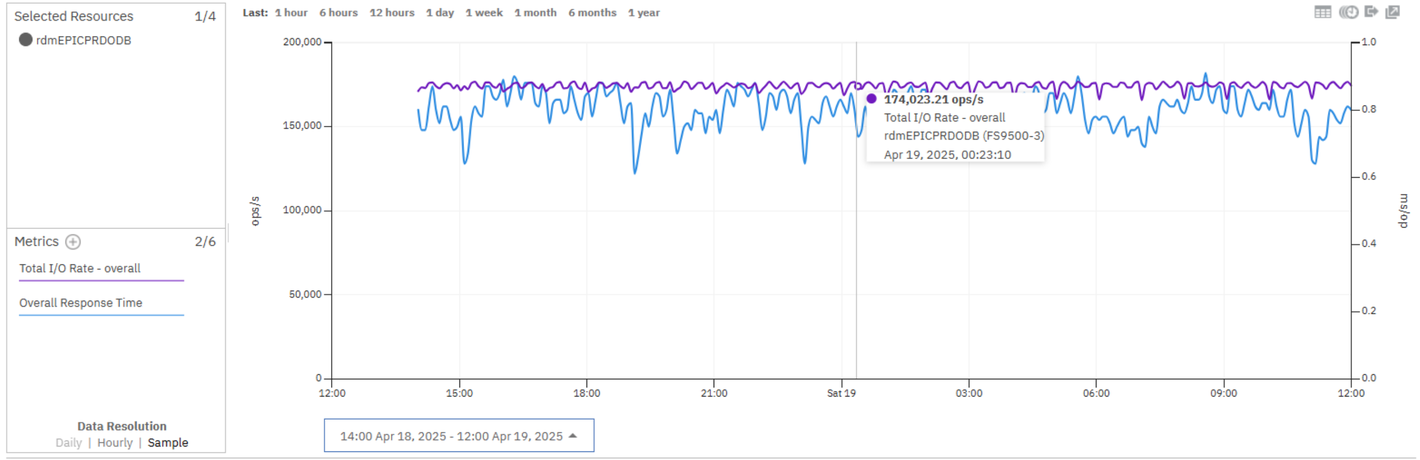
```
IBM_FlashSystem:FS9500-2:superuser>lsanomalydetection
inferencer_version 0.1.8.6
model_version 0.3.35.0
volume_group_support yes
active_array_count 1
anomaly_snapshot on
anomaly_snapshot_retention_days 7
latest_snapshot_extension_days 7
```

Cyber Vault architecture still encouraged:

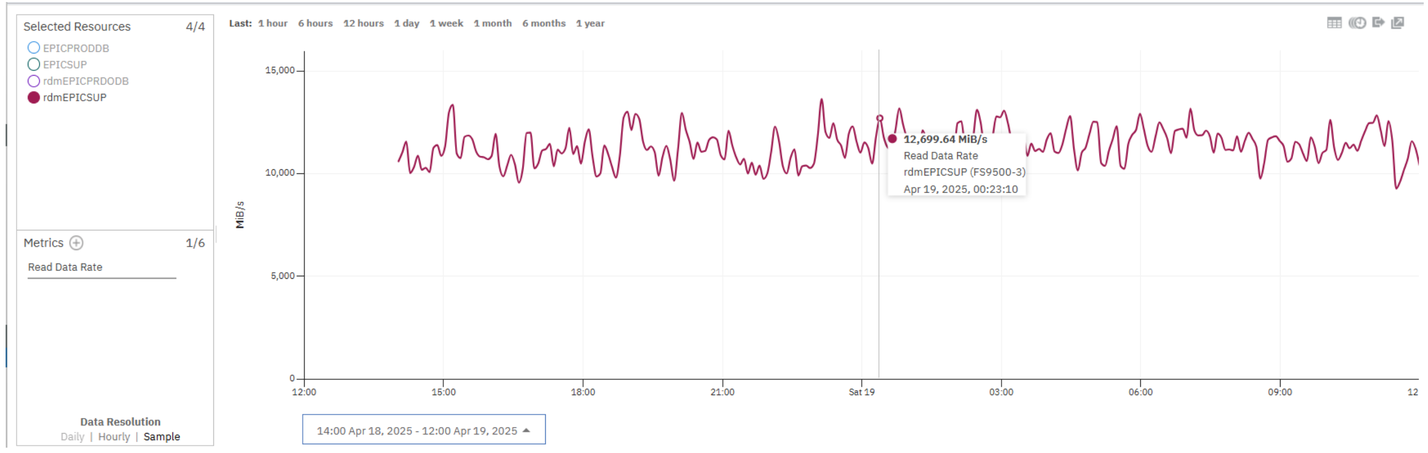
1. Orchestrate SGC snapshot on all sites
2. Orchestrate SGC snapshot scan for integrity AND consistency before claiming “sky is falling”



Performance



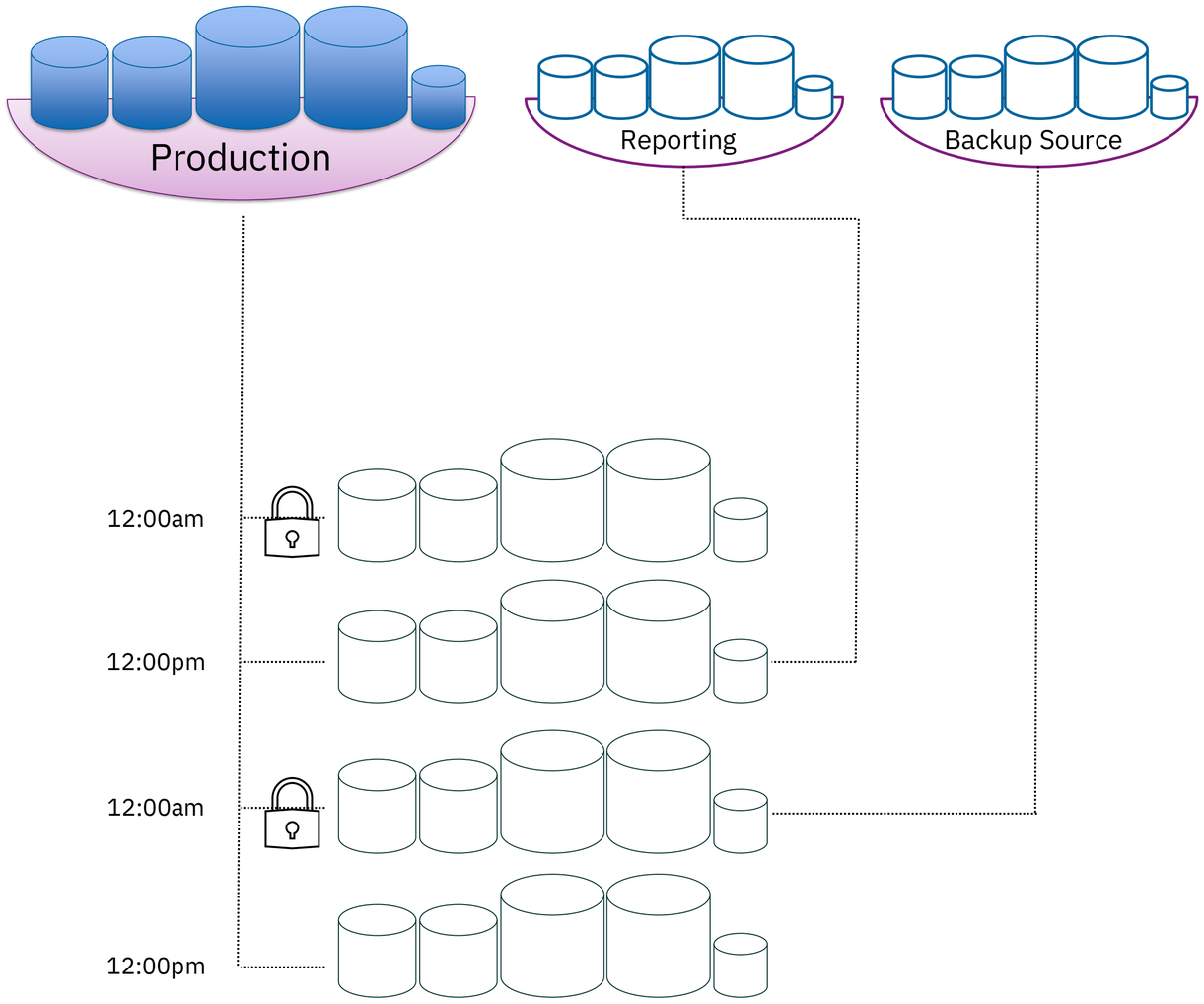
Abrasive, transactional workloads running with SGC and serviing 100K’s of IOPS and sub-1ms



Concurrently reading snapshots of the same source volumes (99% shared blocks)

Conclusion: SGC implemented with confidence and used to build confidence in backups

Recovery and Reuse

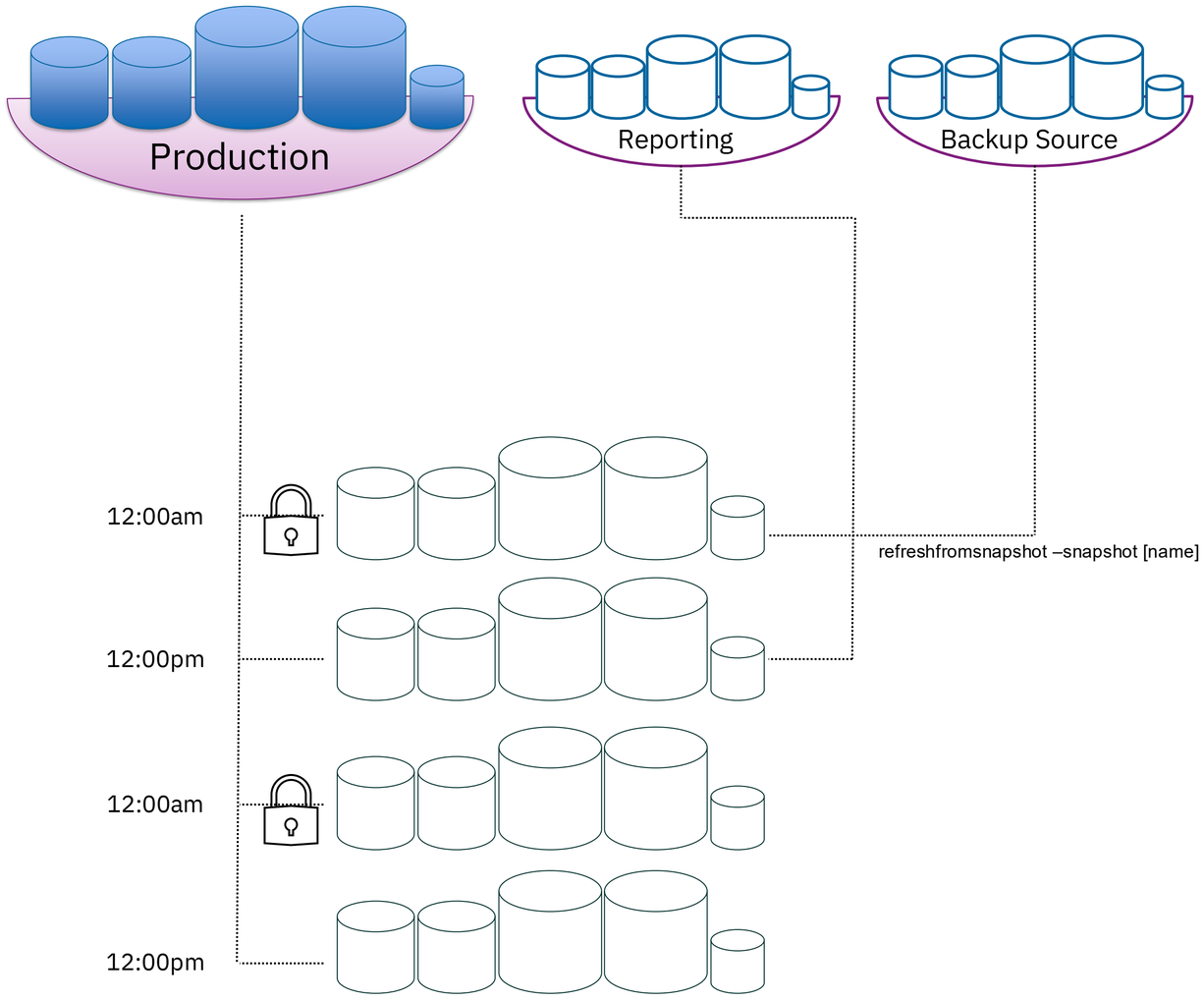


Spinning up thin clones presents new volumes

Easier to stand up environment and refresh the contents WITHOUT remapping new volumes

Example: Backup volumes are referencing the prior day’s midnight copy

Recovery and Reuse



Spinning up thin clones presents new volumes

Easier to stand up environment and refresh the contents WITHOUT remapping new volumes

Example: Backup volumes are referencing the prior day’s midnight copy

So we reboot the Backup Host and ‘refresh from snapshot’ the Backup Source Volume Group to point to the newest midnight copy

Contents of Backup Source are immediately pointed to selected snapshot

- No background copy
- No remapping

Limits and Restrictions

Object Counts

Snapshot objects pull from System Limits

	FS5045	FS5600	FS7600	FS9600	SV3
Volumes	8,192	8,192	16,050	32,500	15,864
Snapshots	8,191	15,863	32,099	64,999	15,863

Capacity

Capacity is the Virtual Capacity (size of presented volumes, not size of data as whitespace is part of linked-lists)
Virtualize v9.1.1 introduced paging bitmaps that extends snapshot capacity to stage production mappings only

	FS5045	FS5600	FS7600	FS9600	SV3
Max Snapshot Virtual Capacity	(9.1.0) 4 PiB	200 PiB	400 PiB	800 PiB	800 PiB

Using `#chsystem -defaultflashcopygrainsize 64`, the snapshot capacity is 25% of presented numbers, but drive-limited configurations scale much higher in performance. Recommended for IBMi and Epic workloads.

IBM openly publishes the System and Configuration Limits for all supported systems here:
https://www.ibm.com/support/pages/v912x-configuration-limits-ibm-flashsystem-and-san-volume-controller

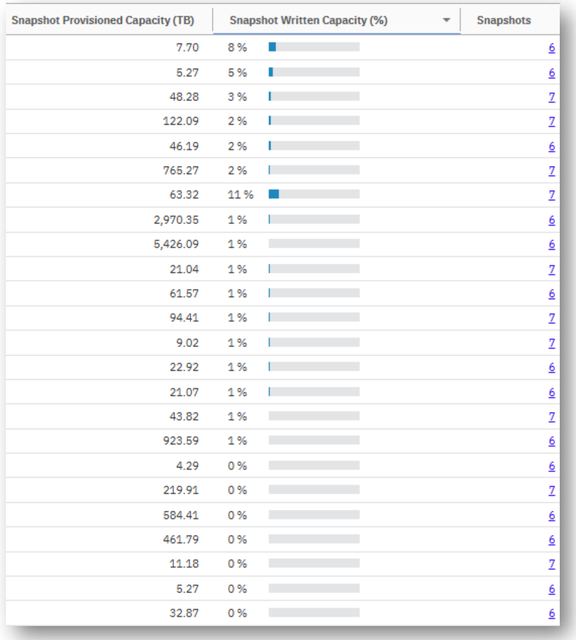
Maintenance and Monitoring

Most applications have <2% Daily Change Rate

- 7 Days of protection ~ 14% capacity

Thin Clones are not threatened by expired snapshots

- Snapshots enter “dependent_deleting” where it keep available while sourcing a thin clone



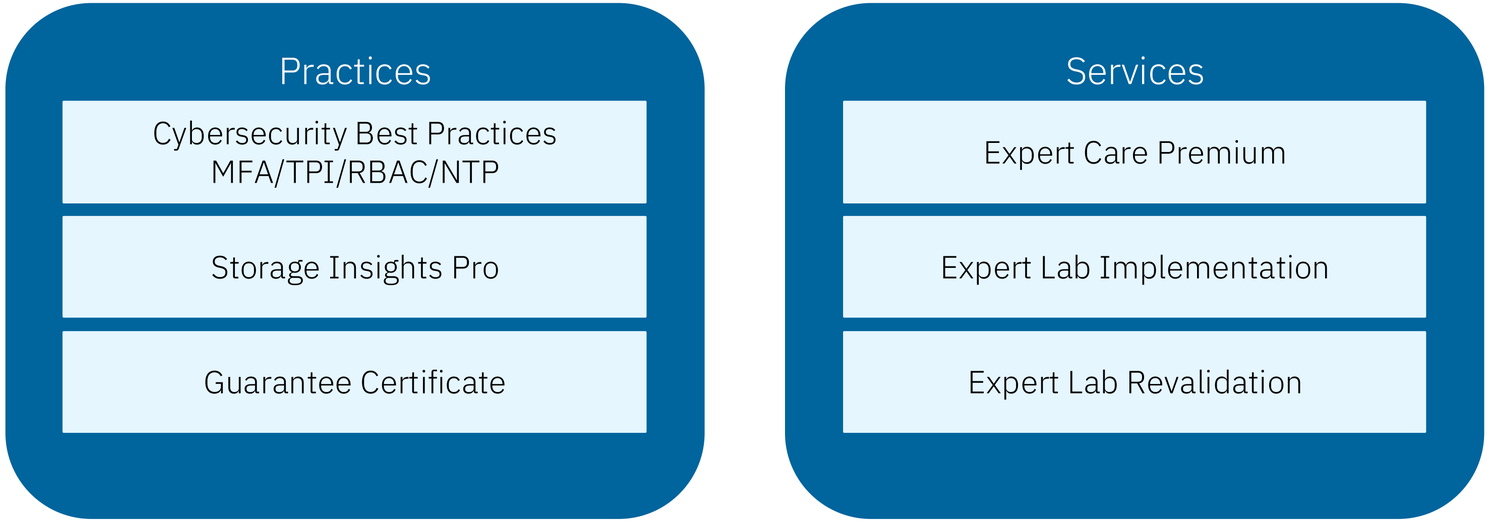
Snapshot Provisioned Capacity (TB)	Snapshot Written Capacity (%)	Snapshots
7.70	8 %	6
5.27	5 %	6
48.28	3 %	7
122.09	2 %	7
46.19	2 %	6
765.27	2 %	7
63.32	11 %	7
2,970.35	1 %	6
5,426.09	1 %	6
21.04	1 %	7
61.57	1 %	6
94.41	1 %	7
9.02	1 %	7
22.92	1 %	6
21.07	1 %	6
43.82	1 %	7
923.59	1 %	6
4.29	0 %	6
219.91	0 %	7
584.41	0 %	6
461.79	0 %	6
11.18	0 %	7
5.27	0 %	6
32.87	0 %	6

Snip from Storage Insights

IBM FlashSystem Cyber Recovery Guarantee

60 seconds

guarantee recovery of Safeguarded Copy immutable snapshot



Reach out to IBM Business Partner or IBM Representative for requirements and details