F A Q ' s

Arcserve Cloud Services March Incident

Q1 What occurred?

A1 During planned maintenance, an array of servers containing critical metadata was decommissioned prematurely. As a result, some metadata was compromised, and critical links between the storage environment and our DRaaS cloud (Cloud Services) were disconnected. Engineers could not re-establish the required links between the metadata and a small fraction of the storage system, rendering the data unusable **in those systems.**

Q2 What does it mean?

A2 Impacted partners cannot replicate to or failover machines in some of our Cloud Service legacy data centers. Affected ShadowProtect partners are receiving replication errors in ImageManager, ShadowXafe and Solo partners see replication errors in OneSystem.

Q3 When will the issue be resolved?

A3 We are in the process of re-seeding machines, and efforts are underway to expedite and expand the re-seeding. As soon as we have definitive timeframes for completion, we'll share those with you. **We recommend you create an additional offsite backup as soon as possible while we continue the re-seeding process.**

Q4 What is the status of the data in the impacted clusters?

A4 We are still investigating any possibility of recovery. The most effective way to get back to replicating and being able to do machines failover to the cloud is to re-seed.

Q5 What action is required by you?

A5 We have identified four recovery scenarios. ***PLEASE ENSURE you have your list of affected machines available.*** If you do not have your list, please reach out to your dedicated sales team and they will provide. See below:

ShadowProtect Machines:

Arcserve will initiate re-seeding over the wire.

For affected ShadowProtect machines, Arcserve is remotely initiating a re-seed over the wire operation. This will happen gradually ofollowing heuristics that maximize progress without overwhelming the system. ***No direct action is required by you to facilitate this scenario.***

To check the re-seeding status of your affected ShadowProtect machines:

Log into the MSP Portal, select a specific machine, and check the *"GCP Migration Status"* field for the following values:

- Pending* = migration to GCP has not started
- In Progress/Copying RPS = migration to GCP is in progress
- Complete** = migration to GCP is finished
- Not Applicable = already in GCP

Be advised while the queue of affected machines is processing, the ImageManager replication job may show a status to be in a *"Failed"* state and logs to include *"Uploads have been disabled for this machine" or "The provided credentials were rejected by the cloud."* This is expected status while we work through the machine queue.

***"Pending"* refers to where the data resides in the legacy data center. This means partners may see additional machines in *"pending"* status but have NOT been affected by the issue. Those machines are operating properly.**

****"Complete"* indicates a base image has been created in GCP. It is important to check the specific machine and determine the last recovery point created. This will indicate from what dates that machine is able to recover data.**

ShadowXafe and Solo Machines:

We ask that you re-seed over the wire.

Please refer to this KB article which outlines the steps required to re-seed affected ShadowXafe and Solo machines while making those machines land on GCP.

After re-seeding affected ShadowXafe machines, you may have some ShadowXafe machines in GCP and some in Arcserve's legacy datacenters. We recommend completing the migration of the remaining ShadowXafe machines to GCP. Follow the same KB instructions to accomplish that.

Seed Drives:

ShadowProtect, ShadowXafe, and Solo, we ask that you re-seed via seed drive.

If you have machines over 3TB, you are encouraged to request a seed drive. Partners can follow instructions in the KB article: Seed to Cloud Services to accomplish this task.

Seed drive requests will receive expedited shipping, and partners will not incur any cost associated with the seed drives.

Archived Machines:

ShadowProtect and ShadowXafe machines that haven't replicated since March 4, 2022.

We are still investigating ways to restore this data. We will be sharing additional information on this scenario as it becomes available

Q6 Can Wasabi be utilized to temporarily hold an offsite copy of ShadowProtect backups?

Applicable to impacted machines in the US only.

A6 Yes. Image Manager can be configured to replicate to Wasabi by adding a new replication location and selecting "Amazon S3 Compatible Storage"; See Image Manager User Guide, Chapter 10. Please remember to run Image Manager v7.7.2 if utilizing this option.

Please be aware of the following current limitations with the Wasabi option:

a) ***PLEASE ENSURE you have your list of affected machines available***, if you do not have your list, please reach out to your dedicated sales team and they will provide .
b) Replicating to Wasabi only results in **BaaS capabilities, NOT DRaaS capabilities.**
c) Entire machines are replicated to Wasabi; individual volumes cannot be selected for replication
d) The retention schedule for Wasabi is not customizable. Intra-daily recovery points are not supported; daily recovery points are kept for one week; weekly recovery points are kept for one month; monthly recovery points are kept indefinitely.
e) Only upload impacted machines to Wasabi that are in "Pending" status, to avoid bandwidth contention with Cloud Services uploads. Before initiating replication to Wasabi, replication to Cloud Services in Image Manager should be temporary disabled. After the base image is uploaded to Wasabi, you should re-enable replication to Cloud Services to perform Arcserve-initiated uploads.

Expenses associated with maintaining one machine backup chain in Wasabi for each affected machine for the duration of the Cloud Services service disruption will be credited.

Q7 Will switching to a Solo device or ShadowXafe speed up the ingestion of machines?

A7 Yes. ShadowXafe and Solo write directly to Google Cloud Storage (GCS) without the use of File Store as an intermediate step. For this reason, ingesting data sent by ShadowXafe and Solo will be much faster than from Image Manager. ***If you are already familiar with Solo/ShadowXafe and the differences in central management, deployment, and pricing***, switching affected machines to ShadowXafe or Solo presents a viable option.