Date or text

Exclusive: AD Attacks and Recovery

Stories from the trenches on Real-World Disaster Recovery with Quest.

Brian Hymer – Solutions Architect IV
Bryan Patton – Security Systems Consultant
Joe Tobias – Professional Services Director

Domain Recovery In a Blizzard!

Winter Storm Recovery Fun!

1 Domain attacked in a 5-Domain Forest

COVID – IT staffer working from home

Happened during a ***Blizzard***

The ***Power*** went out!

So, what did he do?

He **WENT OUT TO HIS TRUCK**

Fired up the engine, turned on the heater, used the lighter plug for power, used his cellphone for internet access…

AND CONTINUED the Recovery!

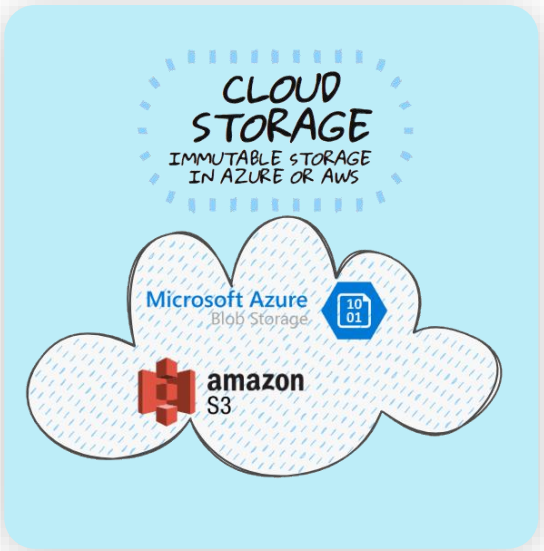
Recovery was **successful!**

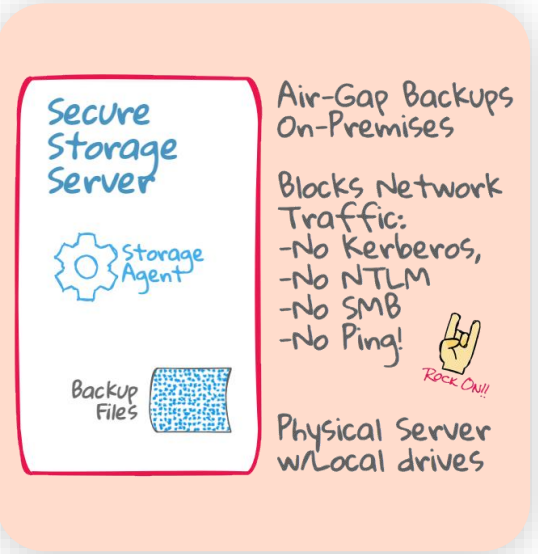
Had to fix some deeper issues with Microsoft afterwards, but the Domain was restored!

The “’figure he can’t fire me” story…

Secondary / Tier 2 Storage Features

Protects backups from being encrypted by Ransomware.





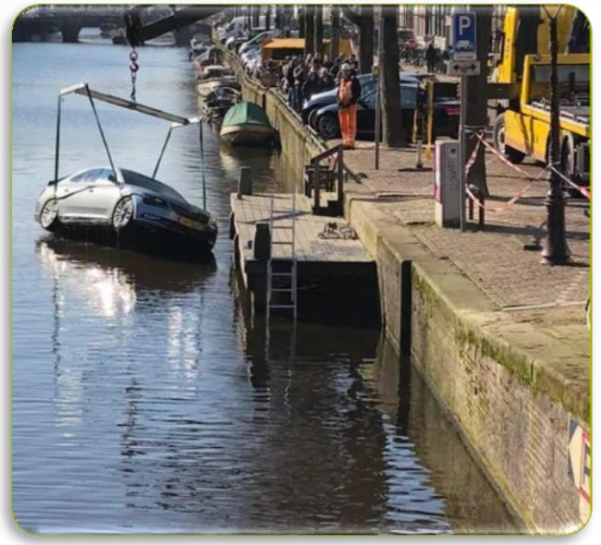
I never thought it would happen to me…!

Client gets hit with **CONTI** ransomware while Secure Storage was running on a VM! 😮

“Brian, I walked right over to the host that had my SS server and I

POWERED IT OFF!

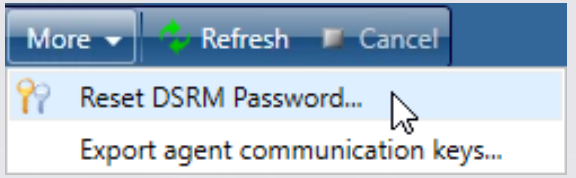
I was NOT going to lose my backups!”



Password Spray Lockout - Resolved

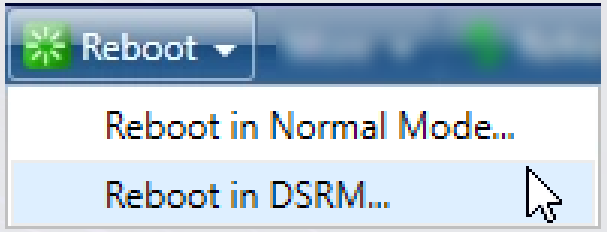
- European Pharmacy hit on Labor day weekend

All Admin Accounts Locked out 🔒



Builtin Administrator Renamed & Disabled! 😮

RMAD DRE tools & DSInternals to the rescue! 😎



✓ Use **DRE** to:
  - reset DSRM Administrator password
  - reboot a DC into DSRM

✓ Use **DSInternals** to find and Enable Administrator, and reset PW

Lessons Learned:

✓ Always deploy FR Agents ahead of time
✓ Always have 1 Forest Recovery Project created
✓ Have at least one Console Config Backup airgapped
✓ Know your RMAD Server SAM Administrator credentials!

DNS is down…

A Managed Service Provider deleted their customer DNS zone by mistake…

Object level recovery isn't just about OU's, Users and Groups.

Quest can recover any type of object, even custom objects from a schema extension!

Don’t Miss What’s Next!

Skills 101 Homepage

https://www.quest.com/skills-101-training/