Quest Platform Management Virtual Summit 2020

How good is your AD recovery solution?

Alistair Holmes

Principal Solutions Architect

Quest

Where Next Meets Now.

Do I fully understand the challenge?

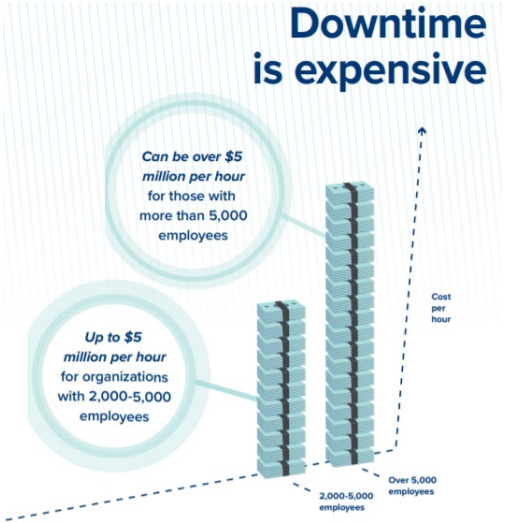
Recovery challenges organizations face today

Need to recover quickly	Objects get modified or deleted, attributes get overwritten by faulty scripts – mistakes, corruption and disasters happen. Need to recover quickly
AD is a target for internal and external actors	There is a growing threat for opportunistic bad actors and your AD environment is very vulnerable
Compliance requires recovery plans are tested regularly	Compliance regulations require proof of disaster recovery and backup plans and testing your plan is resource intensive
Gaps in native tools	Native tools have some gaps, are manual and time intensive (in the case of AD often require that DC'a are taken offline)

Recovery challenges organizations face today

- WFH increases vulnerability from phishing attacks
- A growing remote workforce increases chances for AD mistakes and the possibility of phishing incidents
- Scope of issues can be difficult to assess
- Not knowing which object or attributes have been changed or deleted
- Recovery typically requires Admin permissions
- Can’t delegate restore functions to non-administrators to lighten the load of my more experienced admins
- Documentation of recovery is daunting given the dynamic nature of AD
- Need to document details of how the disaster recovery plan/process will work including timeframes

What is your cost of downtime?



Qualifying questions:

- How long will it take us to investigate and recover from a security incident, manually?
  - What RTO (Return to operations) is acceptable after a disaster?
- What business critical applications (Oracle, SAP, production environments etc) and cloud applications are affected if AD or Azure AD goes down?
- What is your cost of downtime per day/hour?
- How can I test my business continuity plan without going offline?

One mans disaster is another mans inconvenience.

* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

The cost of NotPetya - $10 billion*

$870,000,000	Pharmaceutical company
$400,000,000	Delivery company
$384,000,000	Construction company
$300,000,000	Shipping company
$188,000,000	Food manufacturer
$129,000,000	Consumer goods manufacturer

Some end customer quotes

Describe a major incident where Quest Recovery Manager for AD was used and how it helped?

> The integration with our HR system had a malfunction where it replaced the Swedish letters å,ä, and ö with a question mark (?) and renamed every user with names containing any of these letters. Consequently, the e-mail addresses were changed and users could not log into Office 365. RMAD helped us to quickly identify and restore names and addresses.
>
> — IT Specialist, Large Enterprise Retail Company

Source: IT Specialist, Large Enterprise Retail Company
Validated Published: Aug. 2, 2017 TVID: 2DB-DB7-423

Describe a major incident where Quest Recovery Manager for AD was used and how it helped?

> We've used Recovery Manager for AD (RMAD) twice in production. The first involved an automated process that pushed out bad attributes to many objects. We were able to quickly get the correct attributes restored on all impacted objects. The second involved an administrator that was instructed to delete a large number of User IDs and the list included some that were still needed. The critical items (and access) were restored using RMAD less than 30 minutes after the mistake was recognized.
>
> — IT Manager, Large Enterprise Pharmaceuticals Company

Source: IT Manager, Large Enterprise Pharmaceuticals Company
Validated Published: Aug. 14, 2017 TVID: 934-641-501

Describe a major incident where Quest Recovery Manager for AD was used and how it helped?

> We had an automated update from our HR system that updated several hundred AD accounts incorrectly. This was undone by using Recovery Manager to restore the particular AD attribute for the affected user accounts.
>
> — IT Professional, Medium Enterprise Insurance Company

Source: IT Professional, Medium Enterprise Insurance Company
Validated Published: Aug. 14, 2017 TVID: 2B0-B1E-335

Recovery Manager restores user objects after 'clean up' script inadvertently removes them

> We had a 'clean up' script remove 2500 users from 1 or more of a few hundred security groups. We used Recovery Manager to restore the 2500 user objects back to the state they were prior to being removed from the groups.
>
> — System Administrator, Global 500 Retail Company

Source: System Administrator, Global 500 Retail Company
Validated Published: Mar. 7, 2014 TVID: A02-AAA-6AD

Describe the most beneficial features of Quest Recovery Manager for AD

> Password recovery. Ability to recovery individual accounts. Granular attribute-level recovery. Ability to compare current state to backups.
>
> — Engineer, Large Enterprise Pharmaceuticals Company

Source: Engineer, Large Enterprise Pharmaceuticals Company
Validated Published: Aug. 14, 2017 TVID: 955-508-E71

Business Justification – Object restore

Native Approach:

Internally, our testing has found that it can take upwards of 5 hours to realistically restore objects which may have been deleted or altered. This time can be cataloged as follows:

- Determine Scope of Problem: 45 min
- Acquire and Mount Backup : 30 min
- Boot DC in Restore Mode: 30 min
- Restore Objects: 60 minutes
- Restore Object Links: 60 min
- Perform Authoritative Restore: 90 min

With Quest Tools in Place:

It has been internally validated that by utilizing a 3rd party tool, Quest can perform the same scenario, in a total of **10 minutes**. The tool automates nearly all of the required steps to restore objects. This will allow customer to greatly limit the cost and financial impact of a disaster.

It has been found that the accuracy of such an operation is greatly enhanced by utilizing a tool. This is primarily due to integrated reporting, allowing for quick comparisons of the current state of an object, with how it appeared within a backup. At that point, it can either restore the object in its entirety, or only recover certain attributes (i.e. group membership, username, email address). With this reporting, documentation can be created particularizing the before and after state of any changes initiated by the recovery attempt. This level of auditing is critical to ensure that users don't accidentally increase the level of damage.

Build a list

- Business continuity.
  - Prioritise applications – Phone systems, e-mail, Physical access.
- Talk to stakeholders - Internal user priorities, External users priorities.
- AD Integrated applications.

How efficient is my day-to-day AD recovery process?

Do I ?.....

- Need to restart DC's to recover AD objects.
- Put back snapshots from a point in time.
- Know what was deleted & will it still be in the AD recycle bin.
- Know what has been changed.
- Know exactly what needs to be recovered or am I just guessing.
- Have to recreate objects because I've no other way of recovering them.

Can I get everything back?

Can I recover ?……

- All types of AD objects and attributes at a granular level.
- User and workstation passwords.
- Groups & group memberships.
- OU’s.
- Printers.
- DNS records and zones.
- Group Policy settings.
- Sites & Subnets.

3

If I have a partial AD failure, can I get the domain back without effecting the other domains in the forest?

Quest

Where Next Meets Now.

How do I handle a ?....

- SYSVOL failure.
- DC failure.
- Complete Domain failure.

If I have a complete disaster, how prepared am I?

Lining up the ducks.

- Where's the instructions?
- Has anybody done this before?
- Don’t ignore experience.
- Does everybody understand what needs to happen, when, where and in what order?
- What can and can’t wait?
- Who you gonna’ call?

OK, I wasn't expecting that!, now what do I do?

My DR plan didn’t take account of……

- Loss of hardware.
- Loss of a datacentre.
- Or any other of a myriad of situations you hadn’t planned for.
- So, What options do I have now?

Ask yourself “Can I use this disaster and an opportunity?”

Practice makes perfect.

Can you….

- Keep your plan up to date given the inevitable changes that occur in AD & connected systems?
- Practice your fire drills in a safe environment?
- Test changes to AD without putting your production AD at risk?

Beyond AD.

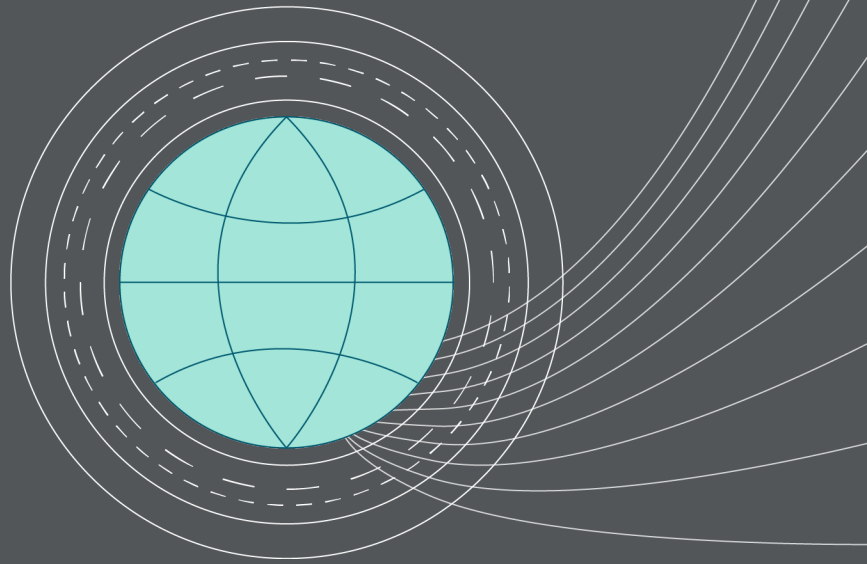
Quest

Where Next Meets Now.

What about…..

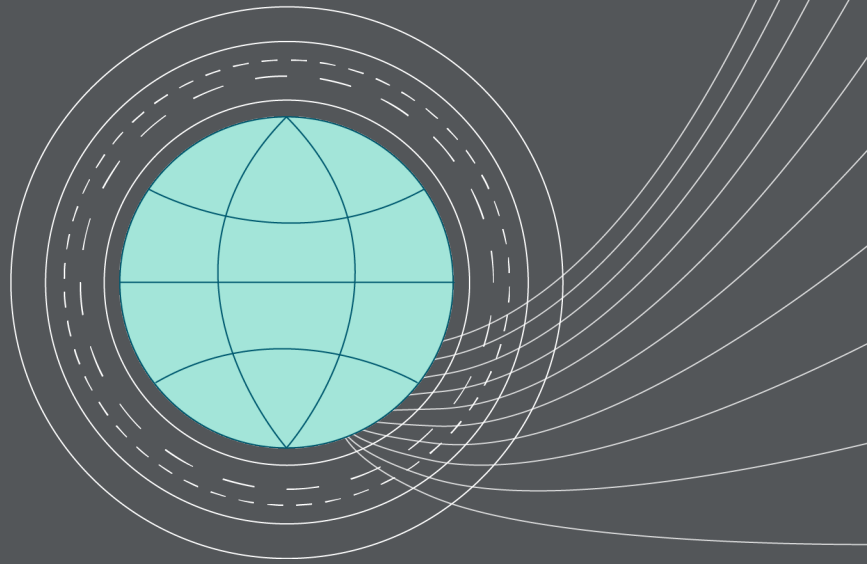
- Azure AD
  - Azure AD Connect is not a recovery solution for Azure AD
    - Cloud only objects
    - Cloud only attributes
    - Hard deleted objects
- AD LDS (ADAM)

Questions



Thank you

Alistair.holmes@quest.com



Quest
Where Next Meets Now.