The importance of a dedicated Active Directory recovery plan for ransomware attacks

Brian Hymer
Solutions Architect
Quest Software
Protecting Active Directory with NIST CSF

- Strong AD cyber resilience requires defense in depth across the NIST framework
- But today we’ll focus on Recover

- **Identify**
  Assets, policies, vulnerabilities & risk

- **Protect**
  Limit the impact of a cybersecurity event

- **Detect**
  Continually monitor for anomalies

- **Respond**
  Take appropriate action

- **Recover**
  Restore impaired services or capabilities
Active Directory is the Keystone

Most organizations use Active Directory to manage identities and provide access to business resources.

- **Active Directory**: Primary authentication and access provider

- **Databases**: Structured data used for business analysis and research

- **Files**: Unstructured data used for communication inside and outside the company

- **Applications**: Tools necessary to promote business endeavors

- **Endpoints**: Computers, tablets, phones – the devices used to consume business resources
Without AD …

… The rest just falls apart

“If we can’t recover our domain controllers,” a Maersk IT staffer remembers thinking, “we can’t recover anything.”
How to Recover From a Ransomware Attack Using Modern Backup Infrastructure

Published 4 June 2021 - ID G00738061 - 40 min read

By Analysts Fintan Quinn

“The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process.”
AD backup, recovery & security considerations

- Airgap your AD backups
- Don’t rely on ONE type of backup
- AD recovery automation is essential
- Malware detection
- Phased recovery
Airgap your AD backups

Anything on the network is at risk

• Off Prem?
  • Offsite tape backups…?
  • Cloud immutable storage

• On Prem? Use firewalled server
  • Disable SMB protocols
  • Isolate via IPSec rules
  • “Pull” backups in

• No budget?: USB Drive

No Backup? 😞
Don’t rely on **ONE** type of backup

e.g.: System State backups carry too much bloat and too much risk – **Kaseya** attack hid in WinSxS!

Read on: [The Varied History of System State Backups](#)
AD recovery automation is essential

AD Forest Recovery Guide | Microsoft Docs
Outlines 40+ manual steps that must be performed on each DC & coordinated across entire forest

- Configuring the DNS Server service
- Removing the global catalog
- Raising the value of available RID pools
- Invalidating the current RID pool
- Seizing an operations master role
- Cleaning up after a restore
- Cleaning metadata of removed writable domain controllers
- Resetting the computer account password of the domain controller
- Resetting the krbtgt password
- Resetting a trust password on one side of the trust
- Adding the global catalog
- Resources to verify replication is working
Malware detection

Scan your backups for malware before recovery

This reduces the likelihood of reintroducing infection into the environment.
**Phased recovery shortens RTO**

Phase 1:
- Restore Key DCs from backup

Phase 2:
- Promote Remaining DCs

All AD sites compromised
Thank You!

Visit www.Quest.com to learn more about

Quest Recovery Manager for AD
Disaster Recovery Edition