Recovering the Keys to the Digital Kingdom:

How Active Directory Recovery Strengthens Cyber Resilience

For organizations that rely on Microsoft to manage their data and communications, Active Directory (AD) serves as a doorway to their digital functions and services. It's the primary mechanism for authenticating users and enabling access to databases, files, applications, computers and other endpoints.

When a crisis strikes — whether a cyberattack or a natural disaster — nothing can be recovered until AD is up and running again. Constituents can't conduct transactions, access websites or contact call centers. Employees, whether they're remote or in office, can't access the tools and information they need to perform their jobs.

While native AD recovery tools exist, they lack the features needed to ensure the quickest return to business as usual. To recover instantly from disasters and minimize their impact, organizations need a robust AD recovery plan and a comprehensive, automated tool that recovers directory data whether it's in their on-premises, Azure AD or hybrid AD environment.

Every minute counts when it comes to bringing AD back online. Following are some of the common challenges organizations face with their AD environments:

Significant cost of downtime. In a recent survey of 1,000 enterprises, 40 percent of respondents said their cost of downtime exceeds $1 million per hour.[1] Besides lost productivity, delayed or lost revenue, fines and reputation damage, organizations spend thousands (and sometimes millions) of dollars on the recovery operation itself.

Ever-expanding attack surface. Mobile devices, the internet of things (IoT), cloud computing and the massive shift to work from home all create new attack targets. IoT attacks alone increased about 35 percent in the first half of 2020.[2]

External threats. With the vast majority of organizations using AD or Azure AD to authenticate endpoints and other objects, AD is in the cross-hairs of bad actors. Many ransomware strains like SaveTheQueen and DopplePaymer compromise AD and leverage it to spread throughout the target organization's systems. Microsoft reported that ransomware was the most common reason for its incident response engagements from October 2019 through July 2020.[3]

Insider threats. According to Ponemon, insider threats increased 37 percent between 2018 and 2020. What's more, 62 percent of insider incidents were due to negligence, not malice.[4] One principal engineer at an energy company provided insight in a recent survey: "The problem began — as so many AD recovery situations do — with a simple typo. ... Within 15 minutes, every one of the 36 domain controllers in the domain was nonresponsive," he said.[5]

False sense of security. An organization's existing data protection solutions, point-in-time snapshots of their AD environment, geographic distribution of their data centers and other measures are not a substitute for a fully effective AD recovery, especially in a forest-level cyberattack disaster recovery scenario.

USING AUTOMATION TO ACCELERATE RECOVERY AND IMPROVE RESILIENCE

AD recovery is a laborious undertaking. Even recovery of a single domain controller requires meticulous coordination of many

DOMAIN — A logical (non-physical) grouping of users, groups, devices or other objects within an AD network; organized within a single authentication database

DOMAIN CONTROLLER — Responsible for all AD object permissions, authentications and modifications within a domain

FOREST — The top container in an AD hierarchy; contains domains, users, group policies and other important objects processes and numerous redundant steps — from preparing for and actually performing the restore, to syncing the domain controller with its replication partners and making it available again. Bulk restores multiply the number of steps and make recovery even more complex.

When performed manually, these steps are time consuming and error prone. If the recovery process includes Azure AD recovery, the organization may run into synchronization and data consistency issues. For example, hybrid cloud users may have missing attributes like Office 365 licenses, mailboxes, application role assignments and more. Most of these attributes don't go to the Azure AD recycle bin.

Automated recovery management eliminates manual tasks so organizations can move through the recovery process quickly, with fewer IT staff, in the correct order and without errors — whether in an on-premises or hybrid environment. By simplifying recovery operations, automation reduces downtime and accelerates the return to normal operations.

The following features differentiate automated AD recovery solutions from native tools and manual solutions.

Comprehensive recovery. Automated recovery quickly restores the entire directory, including users, attributes, computers, sites and configurations. Restoring with native tools requires more time and resources to think through every process. Microsoft outlines a myriad of unconventional steps in AD forest recovery that are tedious, time consuming and only made worse in a high-pressure, high-stakes "system down" disaster. Having an automated recovery tool relieves that stress.

Hybrid AD and Azure AD recovery. Having a single recovery dashboard and toolset that spans both AD and Azure AD environments is critical to avoid synchronization issues and ensure the availability and integrity of both on-premises AD and Azure AD. With a single recovery dashboard, the IT team can differentiate hybrid and cloud-only objects, compare between production and real-time backups, and easily restore all changes.

Granular recovery. This capability enables recovery teams to restore only the required objects and/or attributes without going through the time-consuming process of restarting the domain controller.

CREATING AN AIRTIGHT AD RECOVERY PLAN

Full, rapid AD recovery depends on a solid AD recovery plan. The following practices help ensure an organization's plan is comprehensive:

- **Have separate emergency communications mechanisms** that don't rely on AD. This will ensure that business, IT and recovery functions can communicate with one another.
- **Identify the escalation path** and key decision-makers at every level of the path — before disaster strikes. Know how to contact them anywhere, anytime.
- **Test the plan** with people who didn't develop the plan. Assumptions about what people understand can stall recovery or send it in the wrong direction.
- **Practice the plan** at least twice a year, more frequently if your plan isn't solid. Those who perform triage in any job know that seconds count, and the best way to shave off seconds is to practice processes until they become automatic.
- **Update the plan** regularly to account for changes in systems, compliance requirements, the recovery team and more.

RECOVERY TIME SHRINKS FROM WEEKS TO MINUTES

When one large financial organization performed AD recovery testing for assessment purposes, two staff members spent more than six hours manually recovering a three-domain forest — just three DCs. Using that metric, the organization determined it would take about two weeks to propagate full recovery to all of its 65 domain controllers — which was untenable. Working with Quest, they discovered that using an automated solution in the same scenario would have them fully up and running in less than 30 minutes.[6]

Active Directory plays a central role in practically every aspect of an organization's digital operations and services. Although most organizations take extensive measures to defend AD in depth, an attack that slips through the cracks or a simple mistake can bring AD down.

Given the exacting and laborious process of recovering AD, an automated AD recovery solution — along with a robust recovery plan — is the smartest and most prudent approach.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Quest Software

1. Information Technology Intelligence Consulting. Forty Percent of Enterprises Say Hourly Downtime Costs Top 1 Million. June 2020. https://itic-corp.com/blog/2020/06/forty-percent-of-enterprises-say-hourly-downtime-costs-top-1million/
2. Microsoft. Digital Defense Report. September 2020. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/
3. Ibid.
4. Ponemon. 2020 Cost of Insider Threats – Global Report.
5. Quest Case Study. Energy Company Is Back to Work within an Hour. 2017
6. Government Technology Webinar. Cyber Resilience and the Important Role of Active Directory Recovery. January 2021.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: Quest

Quest helps migrate, manage, and secure Microsoft environments whether on prem, online or a hybrid of the two, including Active Directory, Exchange, OneDrive for Business, SharePoint and Teams. Quest delivers the most comprehensive set of Office 365 and hybrid management solutions, including solutions from recently acquired Quadrotech and Binary Tree. **www.quest.com.**

IMAGE PROVIDED BY SHUTTERSTOCK.COM