Quest

Energy company strengthens cyber resilience with robust Active Directory recovery.

National Grid helps ensure uninterrupted delivery of electricity and gas with Recovery Manager for Active Directory Disaster Recovery Edition from Quest®.

nationalgrid

Country: **United States & United Kingdom**

Employees: **30,000+**

Industry: **Energy**

Website: **https://www.nationalgrid.com/**

> Recovery Manager for Active Directory is my safety net. It allows me to sleep at night.

John Davies, Global Active Directory and Infrastructure Architect, National Grid

Active Directory is vital to supplying energy to millions of customers.

If your Active Directory (AD) is down, your business is down. No one knows that better than the IT pros who were on the front lines when the NotPetya malware took down companies around the world; some, including shipping giant Maersk, needed months to restore their operations.

Challenges

National Grid delivers energy to millions of people in both the UK and the US, a responsibility it takes quite seriously. Accordingly, when the IT team realized the company needed a robust disaster recovery strategy to enable prompt restoration of core operations, they quickly worked with Microsoft to develop a detailed recovery plan. However, they quickly discovered that executing a plan with 40+ complex manual steps would take many days — which was unacceptable for its customers, from households to crucial businesses like hospitals and airports.

Solution

National Grid turned to longtime partner Quest for help. A thorough evaluation of Recovery Manager for Active Directory Disaster Recovery Edition demonstrated the enormous value of an enterprise-quality solution. The team tested nearly 100 different scenarios, from deleting a single user object to deleting hundreds of servers to deleting the entire forest — and recovery took mere minutes for some cases and just a couple of hours for the full-on disasters. As a result, National Grid now has confidence that it can promptly restore its vital services promptly if disaster were to strike.

Benefits

- Slashed Active Directory recovery time from many days to a couple of hours
- Minimized the risk of costly errors through automation
- Reduced the risk of malware reinfection with features like backup checks and restore to a clean operating system
- Handles any recovery scenario, from accidental attribute changes to full AD forest disasters

At the time, John Davies was a consultant for Microsoft who helped organizations get back on their feet after malware attacks like NotPetya, as well as improve their identity resilience. So, when he joined National Grid, one of the largest investor-owned utility companies in the world, to help them re-engineer their Active Directory infrastructure after years of mergers and divestitures, he was determined to also ensure the company's cyber resilience. Knowing just how critical the company's services are, the management team at National Grid gave him their full support.

National Grid owns and operates the largest electricity distribution network in the United Kingdom, serving nearly 8 million customers. And in the United States, it owns and operates electricity distribution networks, electricity transmission facilities and gas distribution networks that serve more than 20 million people. The beating heart of National Grid's IT infrastructure is its identity service, Active Directory. AD provides the vital authentication and authorization services that enable users to log on and key business processes to run.

"If Active Directory is down, people can't work — there is no email, no internet, no Teams calls, no access to any applications. That means immediate losses to productivity and revenue," explains John Davies, global Active Directory and infrastructure architect at National Grid. "For example, if a bank loses its AD, that's a serious problem; people can't get money out of their accounts and business transactions can't be completed. But if National Grid can't supply gas and electricity, the ramifications are far more dire: Hospitals, airports, government services and other critical services would be unavailable. It would be horrible. I couldn't even begin to put a figure on the reputational damage, financial penalties and other consequences we would suffer."

Trying to recover Active Directory manually can take days or even weeks.

Like many organizations, National Grid had focused its disaster recovery planning around its core business data and applications, without giving sufficient consideration to the special backup and recovery needs for its core identity system.

> **If Active Directory is down, people can't work — there is no email, no internet, no Teams calls, no access to any applications. That means immediate losses to productivity and revenue.**
>
> *John Davies, Global Active Directory and Infrastructure Architect, National Grid*

"When I joined National Grid, I found that the company had many disaster recovery plans for its various applications and databases, but it did not have a documented AD recovery plan," recalls Davies. "In fact, over the years, the company outsourced a lot of their IT, and in case of disaster, it was up to the current vendor to recover Active Directory in accordance with Microsoft's published procedures. My experience during NotPetya taught me that the person in charge of Active Directory needs to have a detailed recovery plan because they will be one expected to execute it — and the one whose job is on the line if they can't restore operations quickly."

The first order of business was to develop a detailed AD recovery plan. "We engaged Microsoft to write up formal disaster recovery plans, one for the US infrastructure and one for the UK operations," adds Davies. "However, we quickly realized that manually performing the page-by-page recovery would take quite a long time, and the process was highly prone to human errors. The risk to our business and to our customers was simply too high, so we began looking for a solution that would automate the AD recovery process."

Quest Recovery Manager for Active Directory slashes recovery time from days to hours or minutes.

National Grid had long had a strong relationship with Quest. "I don't see Quest as simply a vendor," Davies says. "Our representative has become somebody that I can phone or email or text, whether I need something or simply want to chat. For example, I might tell him I've seen a particular Quest tool and wouldn't mind investigating it, and he'll get me a trial license the very next day. And the technical specialists are equally ready to help when we have questions. They are all incredibly accommodating."

Despite the years of trust, Davies and his team were still careful to put the Quest AD recovery solution through its paces before making their decision to invest. "We installed Recovery Manager for AD and ran some 80 or 90 different tests," recalls Davies. "We didn't simply want to see if we could recover the latest backup; we developed a wide range of specific scenarios that we'd encountered in our careers, from deleting an individual user to deleting hundreds of servers to deleting the whole forest."

The results were impressive. "In our first attempt using the manual plan from Microsoft, recovery took about four or five days. Practice helped, but it still took two days to get the basics back in the full-on disaster test," Davies reports. "With Recovery Manager for AD, we were able to slash disaster recovery time from days to just a couple of hours. In addition, the tool enables us to recover individual objects or attributes in just minutes. It's brilliant."

Indeed, even before the solution was fully deployed in production, it delivered value. "When some 5,000 user accounts were accidentally modified, we were able to recover them in 42 minutes. That is incredible," recalls Davies. "Moreover, we were able to present a full report on the objects from before and after the change. Without the Quest tool, we would not have been able to identify what the difference was. Recovery Manager for Active Directory really did save the day."

> **"With Recovery Manager for AD, we were able to slash disaster recovery time from days to just a couple of hours. In addition, the tool enables us to recover individual objects or attributes in just minutes. It's brilliant."**
>
> *John Davies, Global Active Directory and Infrastructure Architect, National Grid*

Recovery Manager also prevents malware reinfections during recovery.

On top of the automation and speed of Recovery Manager for AD, National Grid appreciates its enterprise-level power and flexibility. "When a company realizes it has suffered a cyberattack, it's likely that the intruders had actually been lurking in the IT infrastructure for weeks or months. Therefore, if you recover to a recent backup, you might well be restoring their malware, backdoors and other unwanted changes to AD," explains Davies. "Thanks to Recovery Manager for AD, we can now store many months' worth of backups so we can restore to a known good state and prevent reinfection."

In addition, the Quest solution enables National Grid to securely store copies of its backups out of the reach of ransomware or other disaster. "We have two different estates, one in the US and one in the UK," Davies says. "Recovery Manager enables us to store copies of backups in both places and synchronizes them automatically. This belt-and-braces approach gives us additional confidence — at the end of the day, if I lose the whole of the UK, I've still got backups in the US to recover from, and vice versa."

Recovery Manager for Active Directory is an invaluable insurance policy.

Davies would heartily recommend Quest and its enterprise-level backup and recovery solution to his peers. "I hope I never have to use the tool apart from the twice-a-year test scenarios that I organize," he says. "But Recovery Manager for Active Directory is my safety net. It allows me to sleep at night."

PRODUCTS AND SERVICES

Products

- Recovery Manager for Active Directory Disaster Recovery Edition

Solutions

- Microsoft Platform Management
- Enterprise Backup and Recovery

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

Quest, 4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com. If you are located outside North America, you can find local office information on our website.