

Government agency accelerates AD disaster recovery amid growing cyberthreats

Quest®

A public sector organization prevents service disruptions with Quest® Recovery Manager for Active Directory Disaster Recovery Edition

Government Agency

Country: **United Kingdom**

Industry: **Public Sector**

Cybercrime poses a significant threat to critical public services

Cyberattacks continue to increase at an alarming rate, making fast and secure Active Directory recovery more important than ever. That's especially true for the public sector, where downtime affecting critical services can be catastrophic. So, when a large government agency in the UK that's part of the CNI needed a fast and reliable way to ensure they could recover from any disaster, they knew they needed to look beyond complicated manual recovery processes.

A high-risk approach to Active Directory disaster recovery

As the organization's Active Directory environment grew, so did its technical challenges. With about 10 different domains within eight or so forests that support 12,000 users, relying solely on native vendor guidance for AD recovery testing and implementation had become wholly impractical.

Challenges

An important public services agency that's part of the Critical National Infrastructure (CNI) needed a fast and reliable way to recover Active Directory identities and forests, preventing disruption to critical services.

Solution

Quest® Recovery Manager for Active Directory Disaster Recovery Edition empowers the organization to easily recover identities and entire forests with unprecedented speed, reducing risk and providing peace of mind.

Benefits

- Gained complete AD disaster recovery
- Automated and accelerated identity recovery
- Reduced risk by eliminating the need for complicated manual processes
- Sped issue-resolution time by gaining full visibility into changes

"I distinctly remember going through the recommendations for AD recovery that Microsoft provides," recalled the agency's infrastructure and cloud team lead. "It's something like 40 to 60 steps. Each step is incredibly daunting. It's horrendous," he explained, adding that it's nearly impossible to anticipate the hurdles

you'll face along the way. "The risks involved in doing any kind of test recovery of Active Directory are enormous," he said. "If you've missed a step, you'll end up overwriting your live environment with your test backup by mistake. And it's so common."

Of course, the stakes are even higher in an actual disaster recovery scenario. "You hear horror stories of organizations going through that and then finding out there's one small problem that's cropped up six months ago that's basically invalidated any recovery attempt. And that's something our organization just cannot afford because of the impact that will have. It's something that has literally kept me up at night."

AD recovery: a moral imperative for public sector organizations

Active Directory downtime is extremely costly for any organization, but the stakes are even higher in the public sector where downtime can have a direct impact on people's lives.

"It's just not something that's tolerable," the agency's team lead stated. "As a public sector organization or government body, you have an obligation to the communities you serve. Public-facing services are there for people when they need you the most. The idea that you'd be unable to help because of a technical problem, that doesn't give any kind of reassurance."

He added, "For me, it's a moral and an ethical obligation we have to our communities. And that means when things happen, we're able to identify problems and recover from those problems as quickly as humanly possible. A failure to do that is ultimately a failure on our part."

Overcoming obstacles with honesty

The agency's infrastructure and cloud team lead knew their Active Directory recovery plans weren't strong enough to prevent significant disruption in the face of a disaster. So, he worked hard to communicate the risks to upper management. "Senior leadership and senior management teams have an idea as to what will happen that is not accurate. We need to be

really honest and transparent when what we have in place is not suitable or effective."

He explained that while everyone understands the importance of identity and Active Directory, most non-technical people take it for granted. "You think, 'Well, I just log onto my PC at home, it's fine. That's what will happen.' But actually, when you work for a large enterprise organization, it doesn't work that way. You've got a lot of interdependencies and interoperability between various systems. The pro is you don't have to remember a dozen passwords for all the different applications because it's all done through single sign-on. But the downside of that is if there's a problem, you can't access anything," he said.

"You can't log onto a workstation without your identity. You can't send an email. You can't look at your calendar. You can't really do anything. And for many organizations, that's just the worst-case scenario. If we lose access to those core services, we grind to a halt. So, it really increases the priority you need to assign to those identity services."

But with only complicated manual recovery processes in place, the team lead had serious concerns, noting there was no assurance the 60-step vendor guidance would even work. By continuing to honestly and clearly communicate the risks his organization faced, he eventually gained support to implement a faster and safer approach to Active Directory disaster recovery.

A long-awaited AD recovery solution

Thanks to the perseverance of their dedicated infrastructure and cloud team lead, the agency turned to Quest® for a powerful AD recovery solution. With Quest® Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE) in place, the public sector organization can now automate and accelerate Active Directory disaster recovery.

"Quest Recovery Manager gives you that assurance that if there is a problem, you can have things sorted quickly. And that's a massive weight off our senior management team's mind. They know they can provide that assurance to the rest of the business to

say, 'We understand there's some concern, but we've also got a really good contingency to make sure we can continue to operate normally.'

Quest Recovery Manager gives you that assurance that if there is a problem, you can have things sorted quickly.

Infrastructure and cloud team lead at a government agency

Slashing AD forest recovery time from days or weeks to just hours

By providing extensive automation, RMAD DRE reduces the risk of human error that would force the agency to restart its recovery processes. Before implementing the Quest AD recovery solution, the organization's team lead knew their chances of a successful recovery were low. "It goes through your mind, recovery could immediately go from days or weeks to months if not years, if you ever can."

Now, he has peace of mind that his organization could recover quickly from a disaster. "With RMAD DRE, I immediately have a lot more information to work on to know what's happened. Having that additional protection and making it easier for you to undo those changes and to see what's done it, that's absolutely game changing."

RMAD DRE just takes all the aggravation out of the disaster recovery process.

Infrastructure and cloud team lead at a government agency

He added, "Another thing that really impressed me about RMAD DRE, is that you're not just recovering your forest, you're also recovering all of the domain controllers within that forest at the same time. If you are managing an environment across multiple sites, that's incredible. The tool also pauses at the

appropriate moments to let things catch up. It does quality checks. It makes sure that everything's at the appropriate stage before it then moves on to the next bit. And that really just blew me away, that you're able to condense that process down to that point is just awesome."

What was once inconvenient, stressful and time-consuming is now fast and easy. "RMAD DRE just takes all the aggravation out of the disaster recovery process."

Powerful backup protection

RMAD DRE also protects their AD backups from compromise and eliminates the risk of malware reinfection. It's like an insurance policy for AD – only better. "You're far better off investing that money in protecting yourself and making sure that you've got a clear recovery path than you are putting that money into the insurance companies' pockets, because they're not going to give it back to you," he said. "There's just no guarantees. What you can have a guarantee of is your own plans, your own processes and your own technologies. That's within our control and gives us far more confidence."

Building a solid foundation for Active Directory recovery

"At the end of the day, data is money regardless of how people view it," the agency's infrastructure and cloud team lead said. "So, we know that is something we need to be really careful and cognizant of. We must keep ourselves secure and make sure that if the worst does happen, that we're able to recover from that and also then be able to investigate what's happened." With the Quest AD recovery solution, he knows he can, and that's a huge relief, given the growing threats to cybersecurity in the public sector.

"To assume it's not going to happen to you is incredibly naïve. The risk is phenomenal. Any organization is at risk," he said. "The common misconception is that, are we too small that no one's going to bother with us? Well, actually that just makes you an easy target. If you're a bigger organization, you just have to be aware that people will have a go.

Opportunists are everywhere. We see that all the time, and data leaks genuinely impact people's lives. It's just not something that we can tolerate." And they don't have to because Recovery Manager for Active Directory is empowering government agencies to take control and prevent cybercriminals from disrupting critical public services.

"The reality is that if you don't have good foundations, the house is coming down. If you don't keep Active Directory safe and protected and recoverable, you're going to have a bad time. Looking at Recovery Manager for Active Directory and seeing what it can do, the amount of time that it saves us, the assurance that it gives us, it really does speak for itself."

PRODUCTS AND SERVICES

Products

- [Quest® Recovery Manager for Active Directory Disaster Recovery Edition](#)

Solutions

- [Microsoft Platform Management](#)

“Looking at Recovery Manager for Active Directory and seeing what it can do, the amount of time that it saves us, the assurance that it gives us, it really does speak for itself.”

*Infrastructure and cloud team lead
at a government agency*

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.