Slashing Active Directory disaster recovery time from days to hours

AtkinsRéalis strengthens cyber resilience across its hybrid IT ecosystem with backup and recovery solutions from Quest.

AtkinsRéalis

Country: **Canada**

Employees: **38,000**

Industry: **Professional services**

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

Active Directory is the foundation of authentication and authorization services.

AtkinsRéalis is a world-class engineering services organization that connects people, data and technology to transform the world's infrastructure and energy systems. The company has played a pivotal role in a wide range of projects, from the Dubai Opera to the world's first carbon-neutral waste treatment plant to numerous bridges, highways and hospitals.

With roots dating back to 1911, AtkinsRéalis now has 38,000 employees at 400 offices around the globe. Its large hybrid IT infrastructure comprises two large Active Directory forests and two smaller ones, each with one domain, along with three Entra ID tenants.

.

Challenges

AtkinsRéalis had a solid Active Directory (AD) disaster recovery plan that even included custom PowerShell scripts to automate some steps in Microsoft's complex manual procedure. However, testing found that recovering a forest still took several days — and getting the business fully back online took one to two weeks.

Solution

With Quest recovery solutions in place, AtkinsRéalis now has peace of mind knowing the IT team could restore the AD forest in just two hours. Plus, the tools even automatically restore Entra ID properties like conditional access policies and prevent reinfection after ransomware attacks.

Benefits

- Mitigates the risk of costly business downtime by slashing AD forest recovery time from 2–3 days to just 2 hours
- Eliminates the risk of ransomware reinfection with recovery to a clean operating system
- Enables easy recovery of Entra ID objects and attributes
- Provides quick time to value by meshing easily with the existing IT ecosystem

The beating heart of this complex IT ecosystem is Active Directory, which performs more than 90 percent of the authentications necessary for the company's operations. AtkinsRéalis was acutely aware that any cyberattack, natural disaster, hardware failure or other adversity that took down AD would jeopardize essential business processes. Accordingly, fast and effective Active Directory disaster recovery was a top priority not just for the IT department but for the top leadership team as well.

With only native tools at hand, an AD disaster can quickly become a business disaster.

To mitigate the risk of AD downtime, AtkinsRéalis had established a solid Active Directory backup strategy, complete with regular backup testing powered by custom scripts. This was coupled with a robust AD disaster recovery plan, which was thoroughly documented and exercised annually.

However, the approach was based on Microsoft's manual forest recovery process, which is highly complex and prone to human error. It requires meticulous coordination of numerous steps: preparation, performing the restore, syncing each DC with its replication partners and making it available again, and more. Indeed, the Microsoft documentation outlines 12 configuration procedures spanning 40+ steps that must be completed accurately on each domain controller.

Not surprisingly, AtkinsRéalis found in testing that the forest recovery process was unacceptably slow. "Even though we had automated some steps with PowerShell scripts, recovering Active Directory still took two or three days — and that was under ideal conditions," says Vikky Hudson, identity technical lead manager at AtkinsRéalis. "In the event of an actual disaster, you have to double or quadruple the recovery time seen in testing because the stress makes mistakes more likely, in which case you have to start over."

Moreover, recovering Active Directory is not the same as restoring business operations — which was projected to require up to two weeks. "It's not just Active Directory that needs to be recovered," Hudson adds. "With our old strategy, a full disaster recovery would take not just days of our time but days of time from other teams as well. We were looking at a week or even two weeks before the business would be fully back online, which of course was unacceptable."

Finally, the company's Active Directory recovery process did not cover the entire hybrid environment. Entra ID has objects and properties that simply do not exist in on-premises AD, including the roles, cloud service licenses, multifactor authentication (MFA) settings, conditional access policies, dynamic group definitions, and service principals for cloud applications. Accordingly, after the initial AD recovery, users would remain unable to access vital cloud resources like Microsoft 365 workloads and the risk of security breaches would be elevated until additional steps were taken to fully restore the account objects.

Even smaller issues can disrupt critical business processes.

AtkinsRéalis was well aware that it doesn't take a full forest disaster to disrupt important business operations. "Many years ago, we had an errant script that deleted practically every user in one of our non-production forests," recalls Hudson. "Instead of a forest recovery, I had to perform an authoritative restore. Although it was a small forest that we no longer have, the process still took me half a day because of all the steps involved and affected timescales of product testing."

In addition, the company knew it needed a better solution for granular recovery of Entra ID objects and attributes. While the Recycle Bin provides a convenient option for restoring certain types of recently deleted objects, it was never designed to be an enterprise recovery solution. For one thing, some critical objects like security groups and service principals are never put into the Entra ID Recycle Bin when they are deleted and therefore cannot be recovered from it. Similarly, if an object is changed rather than deleted, the Recycle Bin cannot help you restore it to its previous state. And even objects that do go into the Entra ID Recycle Bin stay there only 30 days before being permanently deleted. AtkinsRéalis recognized that these limitations of Microsoft tools increased their risk of downtime and business disruption.

> **We now test our backup and recovery strategies far more often because the Quest solutions make it so much easier. Since we have four forests to look after, if we had to do the job manually, we would have to spend weeks testing just the forest recovery. With Recovery Manager, everything is much quicker.**
>
> *Vikky Hudson, Identity Technical Lead Manager, AtkinsRéalis*

In addition, the company knew it needed a better solution for granular recovery of Entra ID objects and attributes. While the Recycle Bin provides a convenient option for restoring certain types of recently deleted objects, it was never designed to be an enterprise recovery solution. For one thing, some critical objects like security groups and service principals are never put into the Entra ID Recycle Bin when they are deleted and therefore cannot be recovered from it. Similarly, if an object is changed rather than deleted, the Recycle Bin cannot help you restore it to its previous state. And even objects that do go into the Entra ID Recycle Bin stay there only 30 days before being permanently deleted. AtkinsRéalis recognized that these limitations of Microsoft tools increased their risk of downtime and business disruption.

For comprehensive disaster recovery, trust the hybrid Active Directory experts

As AtkinsRéalis reviewed the Active Directory disaster recovery solutions on the market, Quest quickly emerged as the vendor of choice. "We looked at several products, and the Quest portfolio provided the most functionality," says Hudson. "We selected Recovery Manager for Active Directory Disaster Recovery Edition and On Demand Recovery."

Together, these solutions enable reliable and secure backups and quick, robust recovery — including both disaster recovery and granular recovery of objects and attributes — across the hybrid IT ecosystem. Moreover, Quest tools provide flexibility to choose the best recovery method in a given scenario, including phased recovery, bare metal recovery (BMR), and recovery to a clean operating system on a physical machine or an on-prem or cloud-hosted VM.

"One important factor in our purchase decision was the secure storage capability in Recovery Manager," notes Himangshu Kalita, Active Directory designer at AtkinsRéalis. "Using air-gapped storage for our AD backups helps ensure they remain uncorrupted and inaccessible to ransomware." To further reduce risk, Recovery Manager can also scan servers for malware before they are used in recovery.

AtkinsRéalis further understood the value of choosing a vendor who would be a true partner. Quest offers not just market-leading solutions but award-winning services and support. In particular, AtkinsRéalis saw that Quest would help their internal teams gain a deep understanding of the granular and disaster recovery processes so they could reliably achieve the company's recovery time objectives and other cyber resilience goals.

AtkinsRéalis slashes AD disaster recovery time from several days to just 2 hours.

With the Quest solutions, AtkinsRéalis was able to slash Active Directory disaster recovery time from days to mere hours, ensuring cyber resilience in the event of a ransomware attack, hardware failure or other catastrophe. "Using Microsoft's AD disaster recovery method requires a lot of downtime — even with our documented strategy and PowerShell scripts, it took us at least two days," explains Hudson. "With the Quest solutions, we can now restore an entire forest with four domain controllers in just two hours."

Moreover, the Quest solutions fully restore hybrid objects, eliminating the need for additional manual steps that extend business downtime. "Previously, when we restored Active Directory, we had to

manually re-add cloud-only attributes like conditional access policies, which lengthened recovery time," says Kalita. "Now, we don't need to perform those tasks; everything is handled automatically by On Demand Recovery."

Quest solutions make granular recovery fast and easy.

The Quest solutions also deliver the granular recovery capabilities that AtkinsRéalis needed across its hybrid IT ecosystem. "The Microsoft Recycle Bin gives you only 30 days to restore a deleted cloud object, and it covers only certain types of objects," Kalita adds. "With On Demand Recovery, we get far more flexibility in granular recovery. Plus, now we know that if a runaway script or malicious actor were to delete 20,000 users across 10 different OUs, we could restore those objects in a few clicks, instead of having to develop and test custom PowerShell scripts to help us with the recovery.

Easy recovery enables more frequent testing and therefore better peace of mind.

With the Quest solutions, AtkinsRéalis has been able to implement an even more rigorous schedule for testing its backup and recovery plans, increasing the company's confidence in its cyber resilience. "We now test our backup and recovery strategies far more often because the Quest solutions make it so much easier," notes Hudson. "Since we have four forests to look after, if we had to do the job manually, we would have to spend weeks testing just the forest recovery. With Recovery Manager, everything is much quicker. For instance, we now exercise the object recovery process once every two weeks."

AtkinsRéalis recommends the "fantastic" suite of Quest tools.

The team at AtkinsRéalis would heartily recommend the Quest solutions to other organizations. "We're very pleased with both On Demand Recovery and Recovery Manager," says Hudson. "All those tools are fantastic; they have really good functionality. I would suggest also investing in Change Auditor for its additional reporting and change prevention capabilities."

> **"Using Microsoft's AD disaster recovery method requires a lot of downtime — even with our documented strategy and PowerShell scripts, it took us at least two days. With the Quest solutions, we can now restore an entire forest with four domain controllers in just two hours."**
>
> *Vikky Hudson, Identity Technical Lead Manager, AtkinsRéalis*

PRODUCTS AND SERVICES

Products

- On Demand Recovery
- Recovery Manager for Active Directory Disaster Recovery Edition

Solutions

- Microsoft Platform Management
- Enterprise Backup and Recovery

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.