A GATHID LABS SERIES: EPISODE 2

Gathid: Bringing Simplicity to AD Complexity

Conquering Acme's AD Chaos with Visibility

Once upon a time, Acme Inc., a thriving mid-sized enterprise, had a pristine, well-organized Active Directory (AD). Life was good. The IT team was in control, security was tight, and everything just worked.

Then came the growth. Acquisitions, rapid hiring, and a revolving door of IT admins turned Acme's once-simple AD into a tangled mess. Security risks mounted. The IT team lived in constant fear of breaking something. Leadership kept punting AD cleanup to "next quarter."

Sound familiar? This is the story of how Acme's IT team got buried under their AD sprawl—and how Gathid helped them dig their way out.

Phase 1: A Well-Structured Start

In the early 2000s, Acme's IT team built their AD with love and care. It was a single, elegant instance with logical naming conventions and strict security policies.

Jack, the IT manager, took pride in how everything was structured. Offboarding was seamless—when IT was informed of departures, access was revoked immediately. Role changes? No problem. AD was an efficient, well-oiled machine.

Everything worked beautifully... until it didn't.

Phase 2: Expansion – The Domino Effect

Then, Acme grew. Fast.

New offices popped up nationwide, each demanding its own IT infrastructure. Acquisitions brought in three smaller companies, each with their own unique (and some outdated) AD environments.

Suddenly, IT was managing multiple forests, conflicting authentication policies, and ghost accounts from employees long gone. Plans to consolidate were repeatedly stalled by nagging doubts:

Which structure made the most sense?
What accounts need to be reviewed and or disabled?
Which roles and groups can be deprecated?
Is there duplication within and across the instances?

What if we've missed something? – Maybe we should just keep it running in parallel just to be sure. – And do we continue to manage and support mirrored environments, for how long?

The team's solution was to proceed as normal, all the while hoping for a better way to manage the sprawl. What could go wrong? (Spoiler: A lot!)

Phase 3: The Fear of Deprecation

Acme's AD sprawl spiralled out of control. Auditors waved red flags. Security holes multiplied. The IT team now managed:

- Three AD forests and multiple domains with countless complex trust relationships.
- Unknown dependencies between applications and old AD instances.
- Overlapping security policies, creating permission conflicts.
- Orphaned privileged accounts, some from employees who left years ago.
- Outdated authentication protocols, exposing security vulnerabilities.

Lisa, Acme's new IT Director, wanted to clean up the mess. But her team hesitated:

·"Do we even know what's connected to these forests?"
·"What if we break something critical?"
·"Shouldn't we focus on our cloud future state first?"

Next quarter became next year. Nothing changed. They kept growing and moving deeper into the jungle of their AD chaos.

Phase 4: The Breaking Point

Then came the wake-up call. Doing nothing was no longer an option:

- Maintaining multiple AD environments was bleeding money.
- The IT team was stretched too thin, managing too many environments.
- Security auditors flagged major risks, making Acme a prime breach target.
- Vendors dropped support for outdated systems still tied to legacy forests.

Acme was officially stuck—paying for infrastructure they couldn't audit and were too afraid to touch.

Phase 5: Rescued by Gathid

Enter Gathid—the game-changer.

Unlike traditional AD cleanup tools, Gathid didn't require risky, manual changes upfront. Instead, it provided context with other related attributes such as HR, ERP and other applications. Through Gathid's instant no-touch visibility into Acme's gathered AD identities and access without disrupting operations.

With Gathid's patented digital twin and knowledge graph technology, Lisa's team could:

- Map every dependency, duplication, and gap, across their forests and domains.
- Model the relationships from AD to other related applications and data, such as: HR, physical access, operational technology, and other privileges held across the enterprise.
- Simulate decommissioning scenarios, demonstrating completion of migration activities before deprecating instances.
- Identify security gaps, duplicated accounts, empty groups and unowned accounts, prioritizing fixes by risk-level.
- Demonstrate their quick wins, giving the team and their leadership confidence to move forward with clarity, while reducing risk.

For the first time in years, Acme's IT team had confidence in their AD strategy.

Phase 6: Future-Proofing AD

Armed with Gathid's insights, Lisa's team crafted a structured, phased decommissioning plan to:

- Retire legacy forests and domains without disrupting business operations.
- Enforce Zero Trust security principles, balancing security with usability.
- Streamline identity governance, preventing future sprawl.
- Develop a strategic roadmap, aligning IT with business growth.

The transformation wasn't overnight—it took months (not years) of iterative analysis and execution. But this time, Acme was in control. No more fear-based decision-making. Just data-driven, dynamic, confident action.

Most importantly, Acme implemented a dynamic approach to better understand and scale their identity and access goals and demonstrate the wins along the way.

Conclusion

Acme Inc.'s story is all too common. Many companies struggle with AD complexity but fear the risks and strategy to implement scalable change.

Gathid offers a low-risk, high-visibility solution—empowering IT teams to take back control, enhance security, and future-proof their identity infrastructure.

Taking control of your AD strategy shouldn't feel like searching in the dark. With Gathid, you're able to see your identities like never before.

Schedule a Demo | Learn More | Read Online