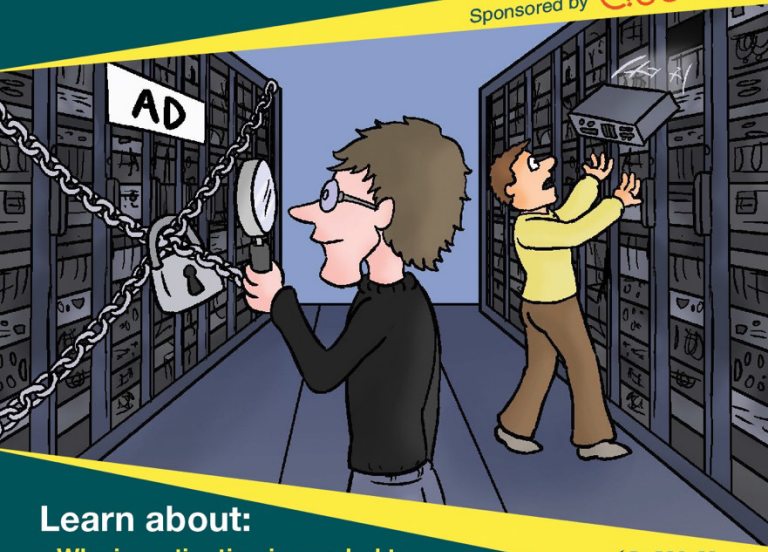
Conversational

Hybrid Active Directory Security Investigation & Recovery

A ConversationalGeek® Book

Sponsored by Quest



Learn about:

- **Why investigation is needed to provide context around suspect activities**
- **The kinds of recovery (and planning) needed to bring AD back into a known state**

MINI Edition

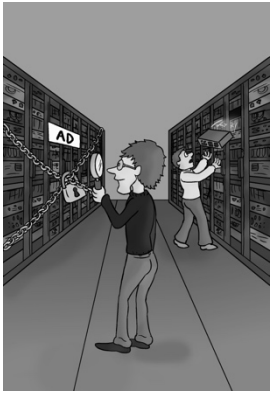
By Nick Cavalancia
(Technical Evangelist and Co-Founder of Conversational Geek)

Sponsored by Quest

Quest helps solve the complex technology and security problems that stand in the way of organizations' ability to always be ready for what's next. With Quest solutions, companies of all sizes can reduce the time and money spent on IT administration and security, so they have more time to focus on and invest in business innovation. Quest has more than 100,000 customers worldwide across its portfolio of software solutions spanning database management, data protection, endpoint systems management, identity and access management, and Microsoft platform management. For more information, visit www.quest.com.

Conversational Hybrid Active Directory Security Investigation & Recovery (Mini Edition)

by Nick Cavalancia



ConversationalGeek®

Conversational Hybrid Active Directory Security Investigation & Recovery (Mini Edition)

Published by Conversational Geek Inc.
www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Authors:	Nick Cavalancia
Project Editor:	J Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer(s):	Jaclyn McGovern

The "Conversational" Method

We have two objectives when we create a "Conversational" book: First, to make sure it's written in a conversational tone so that it's fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

"Geek in the Mirror" Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it's the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read 'em!

Securing AD: One Part Detective, One Part Clean-Up Crew

Because of Active Directory's role as the basis for pretty much all of your on-prem, cloud-based, and Office 365 security, it's critical to maintain a high level of Active Directory security. Should its security become compromised, the impact of that breach no longer ends on-premises; every cloud application – as well as all of Office 365 – becomes susceptible to further compromise.

In *Conversational Hybrid AD Security*, the "parent" book to this mini-edition book, I pointed out that your hybrid-AD environment is in a constant state of flux – with changes being made on a daily basis.

Should those changes turn out to be inappropriate and cause harm to the business or, at a minimum, decrease your organization's security stance, it's necessary to have a sense of what was changed, and how those changes impact the business.

In larger organizations, there are a lot of hands in the AD soup. Many changes made aren't documented. But they should be. Auditing is a solid foundation for establishing security.

If you're wondering how to audit and detect changes made to AD, read my book *Conversational Hybrid AD Detection & Alerting.*

Take the real-world example of an organization where suddenly one of their on-prem Exchange servers stopped functioning properly.

> Once aware of the malfunction, IT did the normal things – check the services, hardware, connectivity, error logs, etc. Everything looked good. Literally zero indicators on the box why it wasn't providing services. No changes to the Exchange environment existed in the audit logs that would cause a problem.
>
> So, they expanded their search, and asked if anyone made any changes at all to anything in the last 10 minutes since the problem started. It turned out an AD admin was modifying the subnets within an AD site, and reconfigured the subnet just so; the result was that the Exchange server was logically isolated on its own subnet, and had no DC to communicate with.

While this is an example that lies outside of the security focus, it does demonstrate the need to be able to identify changes across multiple systems, platforms, and environments.

And, while auditing your hybrid AD is important to help you understand what's changed in the environment, what's also needed is an ability to understand the "why" behind those changes.

A single change that turns up in the audit logs may only be the tip of the iceberg. Let's say a user with permissions to manage the membership of a group that has access to intellectual property abnormally begins to add multiple users to the group within a short period of time. With Directory Service auditing enabled, you can surely see these membership changes. But, what's more critical is understanding what else was done with those permissions.

Suppose it was an external attacker who compromised the account managing the group, and they added multiple users they created within AD (as a means of establishing persistent

access to the intellectual property). You'd need to understand

> a) all the users who were recently created (whether recently added to the group or not), and
>
> b) what actions were taken by those newly added members – did they access/copy/delete the intellectual property?

I'll be using this *External Attacker* example throughout the remainder of the book.

You see, maintaining AD security is as much about what's done with the security, as it is maintaining the security itself. What's required is an ability to do two things:

- Investigate – My previous examples demonstrate the need for a wider scope

of related activity and detail to be accessible in order for IT to have context around actions taken that involve or originate within AD.

- Recover – While I've talked about recovering simple AD changes in my book *Conversational AD security Remediation & Mitigation*, here the process of recovery may extend well beyond just reverting a simple change. In my previous example of the compromised group manager, recovery may take the form of reverting the group's membership, deleting all created users, and changing the password of the initially compromised group manager's account.

In many ways, *IT is like the police* – you're part detective, part clean-up crew. You need to understand what's happened, and then take

action to restore the peace. Thus, the need to both investigate *and* recover.

Let's take a look at how both are necessary as part of your hybrid AD security strategy.

Investigation

The term investigation automatically brings up thoughts of detectives trying to solve a crime. There are some solid parallels here to investigating the details behind changes in AD. The goal of investigation is 2-fold:

Root Cause Analysis

First, you use investigation to determine the root cause of an issue. Work my external attack scenario backwards and assume the indicator of a problem was that an unknown user accessed intellectual property. You'd need to work that backwards to "how did they get access?", and then "who added them to the group?" and even "who created the account?" – all culminating in a root cause – the misuse of an account with privileges.

Context

Next, investigation helps to establish context around the action in question. An action on its own – such as just the adding of a user to the intellectual property group, or the accessing of one of the files containing intellectual property – doesn't give the full picture. It's only in looking at the activity before, during and after the action in question that you get context.

Despite the focus of this book being on securing your hybrid AD, to meet both investigation goals, you need visibility into much more detail than just AD changes (otherwise, this book would simply be the *Detection & Alerting* book I mentioned previously).

So, what sources of data does investigation require?

Activity Data

This being a book on AD security, you obviously start with AD activity. But you should consider including activity data from as many other systems, endpoints, services, and applications as possible – in addition to AD. This should include (when applicable) both change and access data. For example, if you were to include activity from a file server, you'd want to have visibility into when someone, say, opens (accesses) a file, as well as changes the files content or permissions.

In the *External Attacker* example, activities would have included account logons, account creation, group membership changes, and file system access.

State-based Data

When actions are performed, the next logical question often is "how are they being granted permissions to do that?" So, many investigations

require understanding how the environment is configured. This can include the current state of security, or the configuration of a system, application, or service, or even AD itself.

In the *External Attacker* example, state-based data from the file system (e.g. file/folder permissions), and AD (current group membership) would be helpful to better understand the path taken to achieve access to the intellectual property.

Historical Data

In many instances, it's necessary to look at previous versions of both security and configuration settings to understand what the state either *did* or *should* look like. This provides context around whether the current state is sanctioned.

In the *External Attacker* example, seeing the approved configuration of the group's membership would be necessary.

All this data may be used in just about any order – depending on how the unsanctioned action is found out, you may find yourself starting with the current state, followed by historical, and finally activity. There is no right or wrong path to take; the order will follow the investigator's own logic.

Once you understand the scope of what's transpired, there may be the need to put things back the way they were.

Recovery

In many cases, detailed investigations can uncover changes in AD that require recovery. This can involve anything from a single object all the way up to an entire forest.

My *External Attacker* example would require the recovery of the intellectual property group membership, the deletion of any attacker-created user accounts, and any other suspect changes made during that same timeframe.

While my example above is one founded in malicious intent, changes can be unknowingly made, and can even be made by 3rd party AD-integrated applications and systems.

The concept of recovery in the context of an investigation may seem rather simple – just recover whatever was changed. *But it's not that simple.* Recovery can cause even more problems if not properly planned.

So, what kinds of recovery are needed, and what kind of planning does each require?

- Simple, on-prem AD recovery – think one or perhaps a few objects or attributes.

The only planning necessary is in the form of assessing how far back the object needs to be recovered to and are there any foreseen negative consequences of doing so (e.g.: recovering a workstation object may revert its domain password, requiring a removal from and addition to the domain).

- Complex, on-prem AD recovery – Think more along the lines of an entire domain or forest. This would be necessary in cases where external attackers have established persistence in your AD using multiple means (e.g. assigning local permissions to a compromised account, such as *Act as part of the OS* in the DC's GPO, granting Full Control to the *defaultSecurityDescriptor*, or assigning inheritable *Allow Full Control* to the domain root). In situations like this, no object can, in essence, be considered

safe, potentially requiring a recovery of much larger proportions. Organizations planning for such an in-depth recovery often utilize a virtual lab to test and report on a domain or forest-level recovery before doing so in production.

- Cloud-specific recovery – while all your objects originate in your on-prem AD, there are occasions when your recovery involves objects or attributes only used by Office 365 or Azure AD (e.g. Office 365 block sign-in settings, license type, etc.). In these cases, it's much like a simple on-prem recovery, but you will need to understand the Office 365 implications.

The Big Takeaways

Changes to AD sometime only impact AD. But in most cases, a change as simple as giving someone the ability to reset another account's password can have a ripple effect of actions and access that extend well beyond AD and reach into the cloud, Office 365, and other applications and services that rely on AD.

Internal IT organizations need visibility into those potentially affected systems and applications, to investigate and truly understand what actions are taken across the environment, in order to determine how to put AD – and the extended environment – back into a place of security.

Quest: keeping the AD peace

You only can have a true understanding of whether changes to AD and other systems and applications are improper, and come with negative repercussions, if you have visibility across all of AD, and the systems and applications it touches.

Quest offers solutions to empower IT organizations to perform investigations, and any level of recovery deemed necessary to restore AD to a place of security.

Investigations rely on having all three data types mentioned in this book.

Activity Data is made available via *Quest InTrust* and *Quest Change Auditor*. These solutions consolidate and make available privileged user and machine changes across your Windows environment and alert in real-time allowing for speedy investigation and insight.

State-Based Data is accessible via *Quest Enterprise Reporter*, which provides access to the

current state of critical IT assets such as user, computer and group information, direct and nested group memberships, OU and file/folder permissions, ownership and more to empower IT teams to comprehensively understand their state of security.

Historical Data is provided using *Quest Recovery Manager for AD* which lets you view historical configurations of your respective backups for review and comparison.

Rather than digging into data from a number of different systems and devices, Quest has *IT Security Search* – a powerful interactive search engine that pulls together the data found in each solution above, making investigations a fast and simple task.

Once the scope of recovery is determined, *Quest Recovery Manager* – Forest Edition and its *Active Directory virtual lab* which is included, can be used to simulate and recover everything from a single attribute up to the entire forest with the same level of ease.

Because AD is constantly changing, separating approved changes from unsanctioned ones requires context. And context only comes from seeing what other actions have been taken across multiple systems. Learn what it takes to investigate suspect changes and how to recover AD shout it be needed.

About Nick Cavalancia

Nick Cavalancia is Technical Evangelist by trade and is a 20+ year IT veteran who regularly speaks and writes for some of today's more recognizable companies. Follow Nick on Twitter @nickcavalancia and @techvangelism.

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.