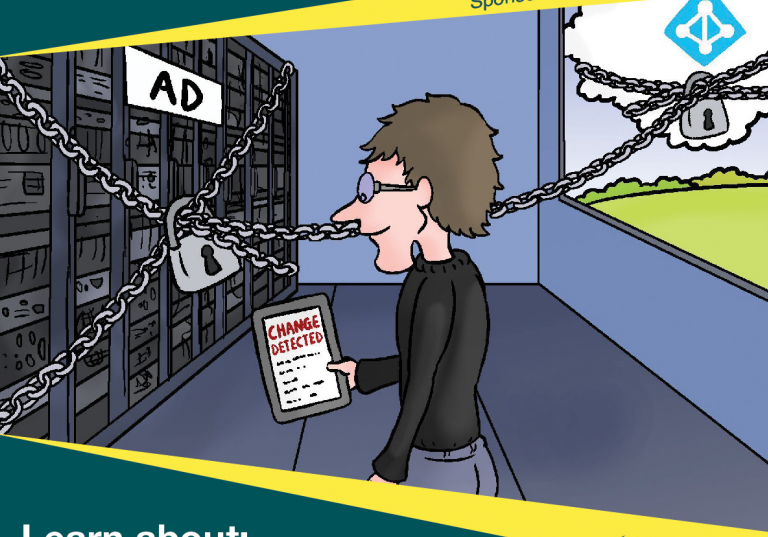
Conversational
Hybrid Active Directory Security Detection & Alerting

A ConversationalGeek® Book

Sponsored by Quest



Learn about:

MINI Edition

- Why detection & alerting is more than just about watching for simple AD changes
- The 4 areas of AD to monitor where changes can have an adverse impact

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 AD Security Detection & Alerting (Mini Edition)

by Nick Cavalancia

© 2017 Conversational Geek

ConversationalGeek®

Conversational Hybrid AD Security Detection & Alerting (Mini Edition)

Published by Conversational Geek Inc.
www.conversationalgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek™. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

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 guide:

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!

Keeping Watch on Hybrid AD Security

"Hey – don't you want to know what's going on??!?"

If you're like most organizations, your AD environment either is, or soon will be, a hybrid AD environment. That is, you utilize the Azure AD connector and sync AD up into Azure AD for use either by applications hosted in Azure, or by Office 365.

As pointed out in *Conversational Hybrid Active Directory Security*, the "parent" to this mini-edition book, by extending your AD out beyond the logical "walls" of the organization, and into the cloud, you also increase the risk of misuse of AD accounts and both the on-prem and cloud-based resources they can access.

The security of such a hybrid AD environment requires constant watch over inappropriate access, misuse of accounts, and any kinds of changes made to your on-premises AD that may assist an attacker (whether external or an insider) in finding and exfiltrating sensitive or critical data.

Which brings me to the title of this book – particularly the part about detection & alerting. If you don't have any kind of proactive detection of improper actions taken in AD or Azure AD, nor a means of alerting you to when they occur, you're managing your AD/AAD environment with blinders on. Think about it – not only are you unaware when potentially bad things are happening, but, even worse, you're not even making an effort to be vigilant!

Now, for some of you, it simply may be too overwhelming - there are countless actions to monitor that each correspond to multiple events, making it difficult at best to even start. So, like the cartoon above, you simply stick your head in the proverbial sand and hope everything's ok.

But, in reality, your AD is not ok.

Unrecorded changes are being made daily that potentially impact the security of your AD environment: Changes to group memberships, delegated AD permissions, passwords, and more – all without you being any the wiser.

So, what's needed is a two-fold strategy where you first define the kinds of actions you deem inappropriate, actions that may indicate a change to the current state of security (and, therefore, need to be detected), and then strategically set up alerting of the proper staff of said detection.

But with so much data that can be generated from changes made in AD, it's reasonable to ask what should you be watching for and be alerted to?

In an effort to do away with the activity noise and focus on ensuring the security of your AD, let's organize the activity you should be monitoring into four categories:

1. Changes to critical objects
2. Changes to access
3. Changes to policy
4. Changes that may indicate an active threat

I'll walk you through each just a bit to provide some insight into the kinds of specific actions you need to be detecting.

1. Changes to Critical Objects

Let's start by breaking this one down into two questions – *What's considered a critical object?* and *Which changes should you detect?*

What defines a critical object varies among organizations. Sure, there's the administrator account and the various "Admins" groups in AD

you definitely need to keep an eye on. But beyond that, what's "critical"?

Here's a short list of the objects you should be detecting changes to:

- Administrator
- Domain / Enterprise / Schema Admins groups (and nested group members)
- Groups given permissions to financial data, intellectual property, personnel information, and any other data of external value (e.g. customer lists, credit cards) – and don't forget nested groups!
- High-profile user accounts of users with influence in the company

While not comprehensive, the list above does cover a lot of ground. As to the issue of what kinds of changes should be detected, the answer depends on the type of object:

- User Objects – Focus detection efforts on changes to passwords, password settings, enabled/disabled values, group memberships, SIDHistory, and attributes related to any kind of SSO/IAM/MFA solution.
- Group Objects – Detection should revolve around changes to group members and members of *Managed By* and *Manager can update membership* values, and nesting of groups.

Most data breaches involve the use of stolen or misused credentials, making the identification of accounts with elevated permissions a key threat action by attackers.

2. Changes to Access

Cyber attackers don't just take the quick and easy route, hoping to luck out and gain access to a domain admin account. They believe in the slow and steady game, where they will gain entry through even a low-level account and work their way up to as much elevated access as possible. Part of this process can include delegating access to objects in AD as a means to potentially elevate another compromised account or to compromise another endpoint.

One method includes adding an inheritable Allow Full Control security permission in the domain root object's ACL to instantly gain domain-wide administrative access to all objects in the domain whose ACL isn't marked *protected*.

So, what access changes should you be detecting?

Focus your detection efforts on permission changes to the following objects:

- Any of the *critical objects* previously mentioned
- Domain Controllers OU
- Organizational Units, in general
- Group Objects (both Security and Distribution)
- Mailboxes (whether on-prem or in Office 365)

While these changes on their own aren't necessarily threatening to the organization, each change has the potential to facilitate further actions (such as changing a user's password, or adding a user to a group with access to intellectual property) that definitely are a threat.

3. Changes to Policies

Changes to policies can be an effective stepping stone for attackers to gain control over yet another account or endpoint on the network.

Take the following two-step method an attacker could use to gain local access to a DC. It involves both changes in access and to policies: by modifying the ACL on the Domain Controller's OU (assuming an attacker gains access to do so), permissions can be granted to link an attacker-created GPO that allows a compromised user to log on locally to a DC.

These are sneaky little buggers!

This is why you need to be detecting changes to any kind of policy that may impact security, no matter how benign it may appear to be. You should be detecting changes to:

- GPOs – particularly the Default Domain Policy, the Default Domain Controllers Policy, and any policy that impacts a material portion of the organization
- Event auditing settings within GPOs
- Password policies
- Account lockout policies
- User Rights Assignment settings (both logon rights and privileges)

Like changes to access, these types of changes are necessary steps in the quest to gain access to needed applications, systems, and data.

4. Changes That (May) Indicate an Active Threat

Nearly all of the previously mentioned changes to be detected are leading indicators of a potential threat.

That reset of the CEO's password may just be the CEO asking IT to reset it. But there are actions that are far more suspicious that require you to err on the side of "it just might be a threat". These include:

- Creation of multiple consecutive new accounts (whether in AD, AAD, or in Office 365) especially after hours
- Changes made directly to AAD (when you're doing a one-way Dirsync from your on-prem AD)
- Logons outside of normal working hours
- Correlated suspicious actions (such as the same account logging onto multiple servers within a short timeframe)

Each of these can, like the CEO password, just be someone in IT doing their job. But, given that we're talking about actions that are out of band, these require immediate attention.

Those last two in the list may require a third-party solution that provides some level of analysis to identify when an action should be considered suspicious.

What About Alerting?

So, most of this book has been focused squarely on what changes need to be monitored for and detected when they occur. But if no one is ever notified, does it even matter?

Alerting is a necessary part of the detection process. And it's much more than just sending an email.

Firstly, alerting is about being able to notify in "real-time" (I put it in quotes because we all realize nothing is truly in real-time; it's going to take a few seconds at least just to have the change show up in a log, have the system detect

it, generate the email, put it in the outbound queue, and finally, send it off).

But secondly – and more importantly, I think – the alerting should be intelligent enough to provide the notified parties with some level of context, insight and guidance as to what the issue is – and what to do about it.

Your alerts should be sent to a distribution list, so that multiple people are (not can be… *are*) notified, giving you the best chance of a quick response.

The Big Takeaway

With AD (and, therefore, AAD) constantly changing, without keeping a watchful eye on each and every change, it's impossible to know when inappropriate activity occurs. That's why you need to, pretty much, be watching *everything*.

And since we all know *that's* impossible as well, I've attempted to outline at least some of the changes in your hybrid AD environment to watch out for.

By putting some of this in place – whether using native tools, or a more powerful third-party solution – you'll at least be in a place where you know when potentially bad things may be happening… and can do something about it.

Quest Software: Masters of Detection

Knowing how to spot just the right change is no easy feat; a deep understanding of events generated and how to interpret them makes all the difference.

Quest Change Auditor enables you to audit, alert, and report on all changes made to Active Directory, Azure AD, Exchange, Office 365, Windows Server, SQL Servers, as well as LDAP queries against AD, and more – all in real time and without enabling native auditing.

Unlike native auditing, understanding what happened is easy, because each event and all related events are displayed in simple terms, giving you the six Ws – *who*, *what*, *when*, *where, workstation* and *why*, plus the previous and current settings.

With visibility into changes made on-premises or in the cloud, Change Auditor provides correlated detection and alerting across all of your hybrid AD and Windows environment. And having the ability to correlate disparate IT data from

numerous systems and devices into an interactive search engine means faster incident response time and easier forensic analysis, if and when something should occur.

Join the Innovation.

Welcome to the new Quest

Technology never stops changing. And you need to be ready to drive what's next. It's time to work together. We'll help you modernize and automate. Get to the cloud quicker. Grow your mobile and data-driven business while keeping it secure and accessible.

It's time for more business innovation and less IT administration.

Quest™

quest.com/join

Your AD security is constantly in a state of change, making it difficult to understand your risks from static reports alone. What's needed is active monitoring of all changes made in AD, with an ability to detect suspicious activity, alerting IT to take further action.

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.