Conversational

Hybrid Active Directory Security Remediation & Mitigation

A ConversationalGeek Book

Sponsored by Quest

Learn about:

- Why you need to keep AD changes in check
- 5 ways to retain control over changes in your hybrid AD

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.

Quest

Conversational Hybrid AD Security Remediation & Mitigation (Mini Edition)

by Nick Cavalancia

ConversationalGeek®

Conversational Hybrid AD Security Remediation & Mitigation (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:

Author:	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 your Hybrid Active Directory Secure

"There! That should do it!"

You probably already realize the criticality of Active Directory security today. With AD serving as the basis for many on-prem and cloud-based applications, as well as many security platforms, along with the natural extension of on-prem AD into Office 365, the potential security exposure

increases – requiring more vigilant focus on the source of your security – your on-prem AD environment.

Most organizations focus on the periodic assessment of security (to get a sense of the current state of security), and the auditing of changes (to be informed when changes occur).

In the "parent" book to this mini-edition book, *Conversational Hybrid AD Security*, I pointed out that changes made to your hybrid-AD environment can occur daily. And those changes may be inappropriate and, potentially, impact your business. So, neither an assessment of the current state, nor auditing, will ensure security. The assessment is a snapshot of one point in time, so it doesn't help maintain security over time. And auditing alone just tells you something changed, but does nothing to define and rectify any unsanctioned changes.

You can read about how to properly assess the state of your hybrid AD security in my book *Conversational Hybrid AD Security Assessment.* You can also read about the what, when, and how of auditing and detecting changes made to AD in my book *Conversational Hybrid AD Detection & Alerting.*

So, it's necessary to put a focus on being able to both maintain a proper state of AD security, and have a plan to diminish the possibility to further bad changes in the future.

Which brings me to *this* mini-edition book. One of the major tenets in your hybrid AD security strategy needs to include an ability to retain control over some (or all) changes made to AD.

There are two key aspects to keeping a handle on AD changes:

- Remediation – If you've done an assessment, you have a security baseline configuration… and you need to stick to it. *Remediation* is about raising the level of AD security to include defining what parts of the baseline should never change, and rectifying those changes should they ever occur.

- Mitigation – Some environments have many, many hands in the AD soup, making the process of reviewing and remediating changes nearly impossible. For those organizations that wish to take security to a level even higher than that of remediation, the focus shift to a more proactive stance of how to put controls in place that restrict AD changes to only those allowed.

Let's take a look at each and see how you can best keep your hybrid AD as secure as possible.

Remediating Active Directory Security

Since you're reading this book, I'm going to assume you probably have quite a few people who have the authority to manage some or all of AD. These are trusted individuals who have been delegated responsibility to keep all of the AD management off of one person's back.

So, why do you even need to think about remediation?

There are plenty of use cases where remediation would come in handy – accidental deletions, erroneous group membership changes, etc. But, at the end of the day, there are two simple reasons why remediation is needed:

1) Changes are inappropriate

2) Changes take your security outside the desired baseline (see reason #1).

Despite everyone's good efforts, changes may be made that are not sanctioned, and manually "undoing" a change may put you in a worse

situation. These can be something as simple as an email change all the way up to adding a user to Enterprise Admins… and everything in between.

In either case, the goal is to return AD to a *known* secure state. In some cases, that "known" state means the *baseline*, while in other circumstances, it's more about undoing administrative actions that could put the company at risk.

Take the example of a trusted admin who has rights to create user accounts in their assigned OU one day creates 50 users in bulk in a newly created sub OU. Seems a bit odd – and it probably is.

Creating multiple accounts is a tactic used by external attackers once they have access to an account with permissions to manage some part of AD – they do this to establish persistence within AD. If you catch on to one account being a faux user for the attacker and disable it, the attacker still has 49 others lying in wait.

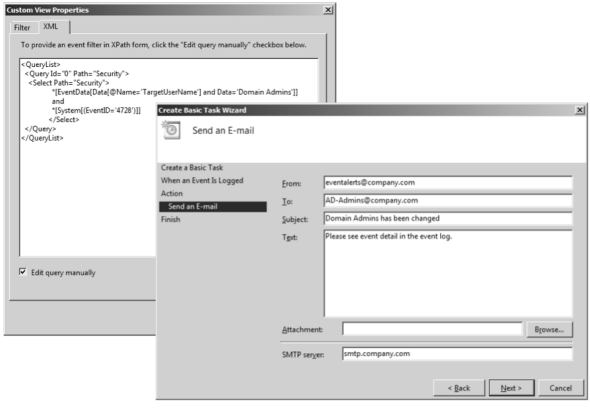
Or perhaps someone adds a user to Domain Admins – a group the organization has deemed off limits to changes.

In cases like this where security has been put at risk – and not just for the 50 users created or the group membership change you know about, but also for any of the other AD actions taken you don't – the best course of action is not to "undo" the changes (as you may not know every change made), but actually to get AD back into a state *before* the changes were made.

So, how do you get started?

Step 1. Establish Auditing & Alerting

You can't remediate what you don't know about. So, you first need an ability to know when changes are happening and be notified with as much specifics as are possible. Microsoft does provide a DIY solution infrastructure via a mixture of Directory Service auditing, Event Viewer, Custom WMI filters (to define what you're watching for), and tasks for email-based alerts (shown below).



Step 2. Define what needs Remediating

You might think "How am I supposed to know *now* what needs remediating? It hasn't happened!" True, but there *are* a few types of actions that you can build into your "Remediation List":

- Prohibited Actions – This can be anything from bulk adds/mods/deletes, to changes made that bypass an established workflow or approval process.

- Protected Accounts – There are some users, groups, and OUs (including contents) that should not be changed pretty much *ever*. If they are, you want the equivalent of that annoying emergency broadcast system test on your TV going off.

Step 3. Define Methods of Remediation

There are two ways of remediating inappropriate changes. Both result in putting AD back the way it was, but differ in their methodologies.

In cases where specific changes have been identified and need to be remediated, reverting of changes can be accomplished using a *Rollback* methodology. This normally involves a third-party solution, as there is no manual way to take frequent AD backups, store them, and select a specific object within AD to roll back.

In cases where changes are made, but IT is uncertain as to exactly what changes have been made (or the scope of the changes in question), a

rollback isn't practical. Instead, a *Recovery* of some or all of AD is necessary to ensure the security and integrity of AD is reestablished.

In either case, the most advantageous place to be is when you have remediation *without human intervention*. That is, with an ability to know when changes are made (*auditing*), and a clear idea of what shouldn't be allowed (*action & account definitions*), it's possible to have automated remediation.

Unfortunately, this isn't something you can really do DIY – I can see it being possible for the *extremely* talented PowerShell guru; but for the IT pro who is too busy to build something from scratch, it's going to need to be third-party.

Mitigation: Kicking Security up a Notch

For some organizations, remediation of certain actions provides enough to maintain an appropriate level of security. But in larger organizations, where delegation of privileges in AD is a way of life, remediation has its limitations.

For example, remediation doesn't scale. Sure, with an automated remediation from a third-party, you can remediate as many changes as is necessary. But, when you consider the number of people that may make inappropriate changes all because they aren't in IT, it becomes necessary to be a bit more restrictive. So, rather than reactively fix inappropriate changes, instead, you should take a more proactive stance using three specific techniques:

Delegation

The key to mitigation is limiting the abilities of delegated users. Employing a least privilege model, look to establish roles and responsibilities – at a minimum, down to the OU and object level, and at a maximum, down to specific

attributes. This should encompass what delegates can see within AD, which parts of AD they can manage, which object types, and what actions they can take.

Process/Policy

Even with delegation properly implemented, there may still be actions taken by delegates that require oversite by peers, superiors, or IT. For example, to maintain security, group names need to conform to a standard or their purpose (and, therefore the privileges granted them) becomes unknown over time. Or membership changes to a group granting access to, say, your customer data may need approvals – or at least notifications.

In general, there should be some kind of policy around the following – and, when appropriate, a process for delegates to follow:

- What changes are appropriate / inappropriate
- Data entry standards

- Whether additional notifications and/or approvals are necessary

In a DIY scenario, this would be relatively easy to create, but extremely difficult to enforce. A third-party solution that proxies AD change requests using a management portal is a better choice for those organizations looking for the highest level of security. A tool like this would handle delegation, establish policy, and enforce processes via workflow, allowing appropriate changes, and stopping unsanctioned actions before they hit AD.

Auditing

I've already talked about this from the standpoint of knowing when changes are made in remediation scenarios, but in a case where mitigation is the goal, auditing is still necessary.

Even if using a third-party management solution, you'd want to keep tabs on changes made, to identify if an action is taken outside the third-party console. Additionally, for the purpose of change control, having that detail is critical to facilitate some form of remediation – should it be necessary.

The Big Takeaways

There are changes made to AD every day in every organization that no one knows about except the person making the change. With the security of AD – both on-prem and in Office 365 – at risk, IT can no longer simple allow administration to run rampant without some levels of security controls in place.

Remediation and mitigation of inappropriate changes are all about having a way to know either actions are being taken or attempted, and having a way to rectify those actions – whether by reverting back to a known good state, or by stopping the action all together.

Having a plan to remediate and/or mitigate AD changes demonstrates an understanding of the criticality of establishing and maintaining AD in a secure state, as well as provides IT with complete visibility into when inappropriate activity occurs – and what was done about it.

Quest: the AD change antidote

Your AD is only secure *if you keep it that way*. So, having a way to be aware, control, and revert changes made to AD that put its security in question is paramount.

Quest offers solutions to put IT in the driver's seat – even when in a heavily delegated administrative model.

Active Roles provides comprehensive delegated account management for both AD and Azure AD environments, enabling complete control by IT. Using a least-privilege model via administrative policies and associated permissions, and a proxy administrative account model, *Active Roles* strictly enforces access, actions, approvals, and oversight, mitigating security errors and accidents common with native approaches to hybrid AD management.

GPOADmin places a layer of control over the management of group policies. With an automated watchful eye over GPO changes, *GPOADmin* protects policies and policy settings

from being inappropriately modified. GPO changes are backed up, allowing for manual and automatic remediation via rollbacks. Using workflows, accountability can be maintained, mitigating unsanctioned changes. Reporting and replication enhance IT's ability to both understand the impact of changes, as well as to ensure consistency throughout the entire AD environment.

With many hands in the AD soup, both malicious and good-intentioned changes can have an adverse impact on your hybrid AD's security – and, therefore, your entire network. Learn how to leverage remediation and mitigation as two strategies to keep AD changes in check.

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.