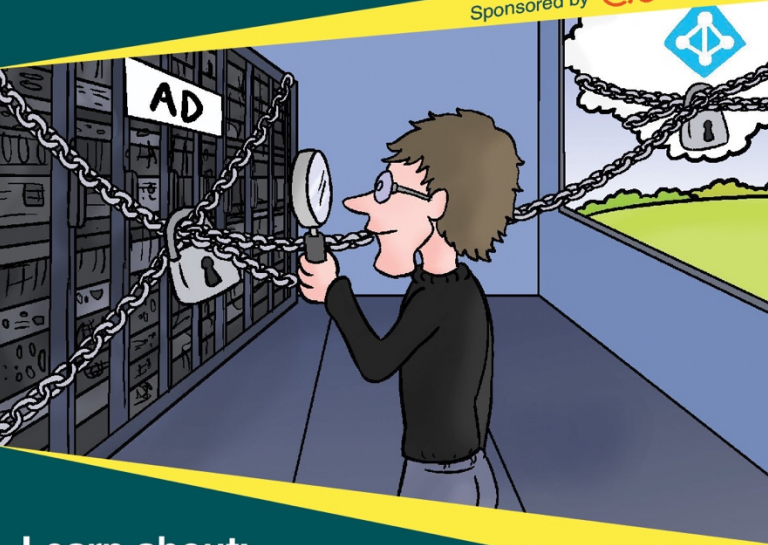
Conversational
Hybrid Active Directory Security Assessment

A ConversationalGeek® Book

Sponsored by Quest



Learn about:

MINI Edition

- Why and how often you should assess the state of your organization's security
- 4 areas of security you should be continually assessing

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 Assessment (Mini Edition)

by Nick Cavalancia

ConversationalGeek®

Conversational Hybrid Active Directory Security Assessment (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 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!

Assessing the State of Hybrid Active Directory Security

Every organization today wants to be secure; it's just a given at this point. With so much potential for cyber-attacks, and the focus on credentials, the need for AD security is critically important. And given the expansion from on-premises AD to one sync'd with Azure AD either for use with

Office 365 or Azure AD-compatible applications, today's organizations are even more at risk.

In *Conversational Hybrid AD Security*, the "parent" to this mini-edition book, I pointed out the fact that because your hybrid-AD's security is based on the security configuration of your on-premises AD, it's necessary to put even more focus on the state of on-prem AD security to ensure a protected stance overall.

And that's what this mini-edition book is all about: Assessing the current state of your hybrid AD environment and how secure it is.

Performing a regular assessment of your hybrid AD security posture provides a few benefits to the organization:

- Defines your security stance – Assessments give you context around the security your current configuration provides.

- Provides visibility into security gaps – Assessments can be helpful in exposing

parts of your configuration that could, potentially, put the organization at risk. For example, if a Finance Exec group was nested within the Domain Admins group because the CFO at one point managed the AD accounts, it could easily be an issue later on when someone adds the new Comptroller into the finance group to facilitate giving them rights to some department folders. See? *Visibility*.

- Establishes a Baseline – Before you can truly know you're secure – or even make changes to improve your security stance – you need to understand the current state of your security. There's an old saying, "you can't know where you're going, until you know where you are" – and it rings true with Hybrid-AD security. Want to figure out if a security change is inappropriate? You first need to know what it was changed from to gain the

context to understand whether it's appropriate or not.

To give you some sense of what you should be assessing, the rest of this book will cover four distinct assessment areas of your Hybrid AD environment that need to be scrutinized:

1) The state of your domain

2) The domain's security configuration

3) The state of your security principles

4) The state of resource privileges

Assess the State of your Domain

The overarching goal here is to look at your domain from a high level, and ensure the domain and its services are intact, that there are no signs of compromise, and that there are no unauthorized changes to the overall configuration.

Start with a simple overview of the domain and the objects it contains. During a cyber-attack, bad guys will misuse accounts with access to create objects in AD; they will create additional users they can leverage to obfuscate their dastardly activities. So, build a report that helps you understand the number of OUs, users, groups, computers, etc.

Without third-party tools, this is likely going to fall to PowerShell commands like the following as part of your reporting:

```
(get-aduser -filter *).count
```

Now, you already have a handle on the growth of new computers and users, so you should have

some idea of whether the counts look right with each assessment.

Another part of your AD to review is the configuration of your domain controllers – because these boxes are the lifeblood of AD, this is more critical to service availability than it is security, but since you're already doing an assessment, it's a good time to check your FSMO roles, AD sites, etc.

Assess Your Domain's Security Configuration

This takes the premise of assessing the state of the domain into the realm of security. Here, you are wanting to review every part of the domain where a simple misconfiguration can create a gap in security.

So, what configuration detail needs assessing?

The list below provides some guidance on areas you should be assessing – some are obvious, while others may surprise you:

- Permissions within AD – Review who has either explicit or inherited delegated access within AD, as well as instances of indirect access through nested groups.
- Domain Trusts – Because trusts provide access to multiple domains from a single account, and are the basis for security dependencies, you need to be reviewing each trust for its type, transitivity, and

direction, making sure each is appropriate.

- Password Policies – Attackers often try to crack password keys, so the more secure the password, the better. Check each set of password policies established within your domain, looking at the settings for password history, age, length, and complexity. Cross-reference these settings with the users they impact, looking for elevated account password insecurities.

- Remote Control Settings – The use of RDP is a common attacker method for traversing servers. Review which servers allow RDP access and consider whether to only allow Log On Locally access.

- Unused User Accounts – Attackers take the long route to gain access to just the right data. This includes doing diligence on many, many accounts just to find the

one with the needed access. Reviewing users not logged in the last "X" number of days can provide visibility into potential security gaps. Consider deleting accounts that are not in use.

- Azure AD Settings – Understand the sync filters used to define which users should exist within AAD (the filters used may be too broad, putting privileged or service accounts in AAD that have no business being there).

Attackers typically gain access through an endpoint, and work to both compromise accounts with elevated privileges and gain access to systems via SMB, RDP, and other access methods. Assessing your domain's security configuration is one way to look for gaps in security that an attacker could take advantage of.

Much of this section involves manual work, using a number of disparate tools and consoles, or an equally disparate number of PowerShell cmdlets. But, beyond the rather large amount of work (or scripting, as the case may be) needed to complete this kind of assessment, one option for doing these in the first place is to ascertain changes by comparing assessment reports. This is going to be difficult at best, and will increase your chances of being compromised, making third-party solutions a viable choice to simplify this process.

Assess the State of Security Principles

This part of your assessment digs MUCH deeper, looking at just about *every single account in your domain* that has rights to anything of value to an attacker. It should be noted that this assessment *isn't* about the rights your security principles have – that's in the next section. Here, I'm more concerned about whether your security

principles themselves are secure and are configured properly.

So, what security principle detail should you assess?

In general, you are looking for any kind of foothold (in the form of an insecure configuration) an attacker can exploit, as well as any indication that an attacker may have already exploited a security principle. This includes:

- Domain Users – There are quite a few attributes you should review for users with privileged, elevated, or critical resource access that could be utilized by an attacker. These include defined logon hours, whether an account is disabled, and password values including *password last changed*, *password never expires*, and *user cannot change password*. Indicators of misuse can be found in values such as last logon, number of logons, and whether the user account is locked.

- Domain Groups with Members – Group membership is of great interest to attackers; they will do impressive amounts of diligence – including following a nested group trail – to identify accounts with the access they need. Assess the membership, including nested groups, looking for inappropriate members.

- Domain Groups Without Members – While this poses no immediate threat, if a group has access to critical resources, it becomes an asset to the attacker, and can potentially be used to give them access. So identifying and eliminating empty groups helps to reduce your risk potential.

- Group Owners – Every group has a *Managed By* field. Looking to see who is assigned as an owner (especially by another *group*) along with whether the *Manager can update membership list* attribute is checked will help identify

potential avenues of attack that may need to be modified.

Once again, turning to PowerShell with cmdlets like *Get-ADUser* and *Get-ADGroup* is the obvious choice to speed up the process of collecting the needed information. For example, the following command would provide the password last changed date and time for a given set of users:

```
get-aduser -filter * -properties passwordlastset
```

However, if you are looking for a consolidated or formatted report (or both), you're either going to need to work some real powerful PowerShell voodoo, or turn to third-party solutions to centrally capture this detail.

Assess the State of Resource Privileges

In lieu of auditing and detecting changes made to AD, performing periodic assessments to report on who has access to what is critical. And even with some form of monitoring of changes made in place, you still need to have visibility into the overall state of access presented in a way that provides stakeholders with intelligence and insight to make good decisions on what needs changing.

So, what privileges should you be assessing?

- User-Centric Privileges – Start with a given user or users and determine where they have access to resources outside of AD (think along the lines of both the "usual" resources like files, application data, etc., but also mailboxes in Office 365, Azure-based applications and data sets, etc.)

- Resource-Centric Privileges – Start with a given resource and work backwards to

see who has privileges to access that resource. Initially, this may seem a bit redundant, but it's not. By taking this second approach, you guarantee you don't miss any privileges granted.

When you take the resource-centric route, you may find some success with PowerShell or even application-specific consoles to provide you with needed privilege details. However, going user-centric is just about impossible to do manually because none of the detail resides in AD. This means you need to somehow query each and every system, application, and data set, inquiring as to whether a given user has permissions anywhere in each system – a task even the best PowerShell guru will find challenging.

The Big Takeaway

Assessing the state of your hybrid AD's security is critical to understanding where your risks are, and what needs to change to improve your security stance. While it's possible to compile just about every piece of information highlighted in this book using PowerShell, it isn't necessarily the right way to do it. You can dig a 6' x 6' x 6' hole in the ground with a teaspoon, but that doesn't make it the right tool for the job.

The goal of an assessment is not the gathering of all the data; it's about making sense of the information gathered and making good business decisions based on it. And as the assessment data set grows, so will the complexity necessary to make sense of it.

No matter your methods – whether DIY or using a third-party solution, assessments need to be done on a regular basis, making automation key to their success. Find a way to properly put a complete view of the state of your AD in view quickly and efficiently, and you're well on your way to a more secure hybrid AD.

Quest Software: Aces of Assessment

The success of an assessment is solely based on the value of the detail gathered. If the act of reviewing the assessment data takes days to correlate and cross-reference data points, it's likely there's no real insight provided, keeping your organization from making good decisions to improve security.

Quest Enterprise Reporter provides visibility into the configuration, settings, and security of your hybrid AD and Windows environments. It's a scalable solution for auditing, analyzing and reporting on your most critical systems and resources, including, but not limited to:

- Active Directory
- Azure Active Directory
- Exchange
- Exchange Online
- File Storage
- SQL Server
- Windows Servers

With its complete visibility and turnkey in-depth reporting, the process of gathering needed information becomes fully automated and

scheduled – making assessments a fast, simple, and repeatable task.

If you have a domain migration or consolidation, *Enterprise Reporter* can help ensure a smooth migration by inventorying what needs to be migrated and cleaning up what doesn't need to migrate.

And if you haven't made the leap to Office 365 just yet, *Quest UC Analytics*, a solution similar in strengths to *Enterprise Reporter*, focuses on not only Exchange on-premise and Exchange Online, but also your Skype for Business, and Cisco environments. It has the ability to identify who has access to mailboxes, who is sending off emails, who is a member of a distribution group, how active are those groups, inactive mailboxes, the size of the mailboxes, and much more.

UC Analytics also goes beyond pre-migration analysis, giving organizations insight into their UC investments by looking at adoption rates of the technologies that Office 365 provides.

With *Quest Enterprise Reporter and UC Analytics* it's easy to perform compliance and security assessments, and pre- and post-migration analyses - enabling your Hybrid AD, Exchange and Windows environment to be more secure and efficiently managed.

AD security is a target that's constantly moving. With AD acting as the foundation for resources access both on-prem and in the cloud, it's critical to assess what state your AD's security is in, understanding where to look, and what to look for.

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.