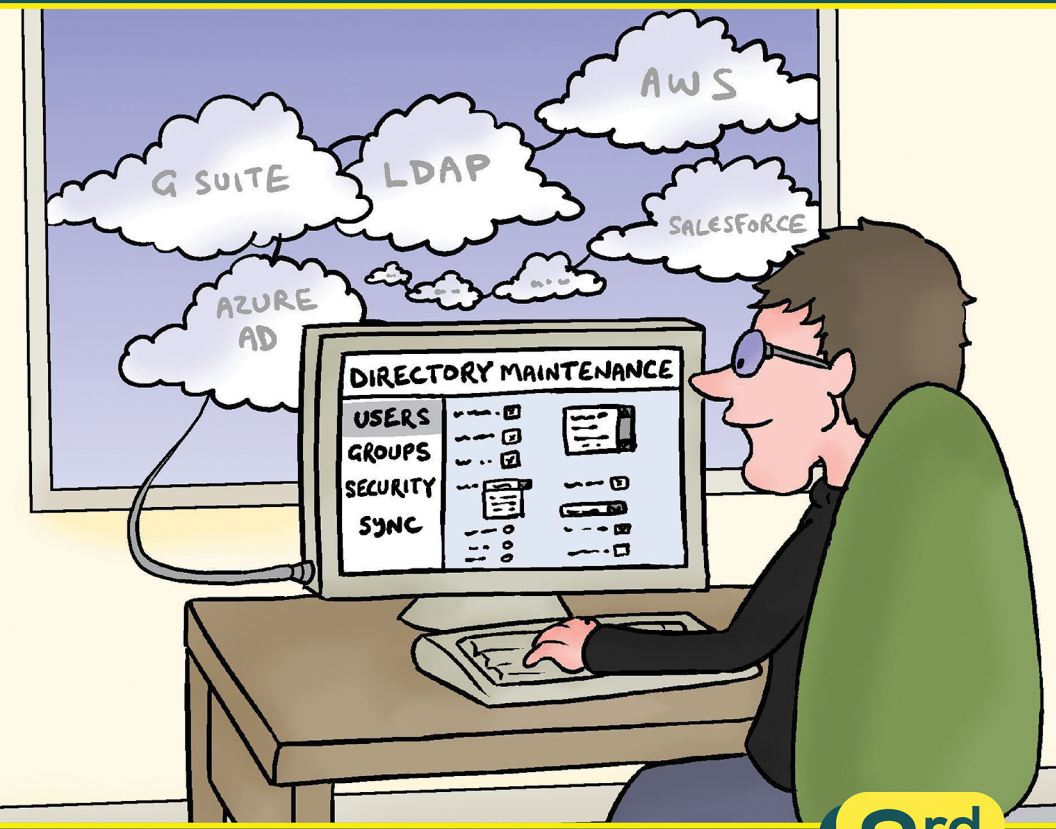
ConversationalGeek®

Conversational Directory Management in the Cloud

By Nick Cavalancia (Microsoft MVP & Co-founder of Conversational Geek)



In this book, you will learn:

- How to manage the risk of syncing AD with multiple cloud-based directories
- How to implement ALM to ensure every directory is correct, current, and secure
- The six steps to understand the current state of all your directories

3rd Edition

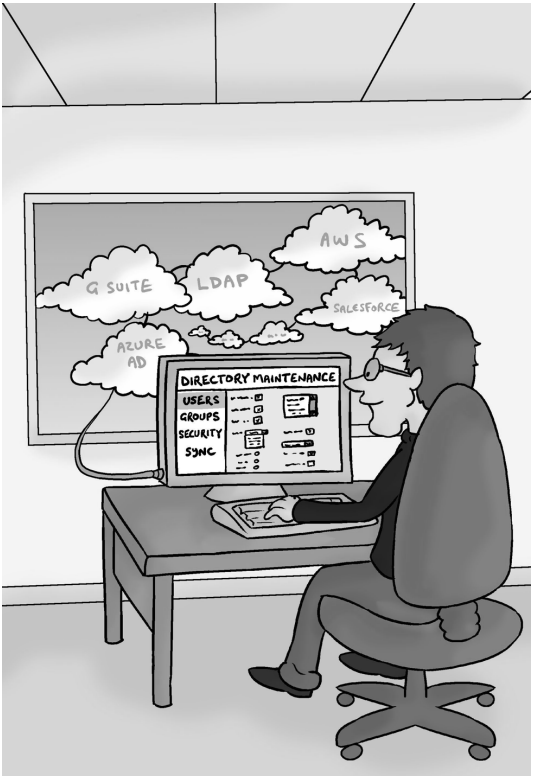
Sponsored by One Identity

One Identity by Quest lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud, or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration, and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems, and data.

Learn more at
OneIdentity.com

Conversational Directory Management in the Cloud

By Nick Cavalancia



ConversationalGeek®

Conversational Directory Management in the Cloud

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 and Copy Editor:	Pete Roythorne
Content Reviewers:	Megan Pennie
	Michele Teniere
	Cristina Pereira

Note from the Author

So many organizations are taking a “cloud first” approach to business, resulting in the adoption of many, many disparate directory services to manage and keep current. But, despite the directory being the very foundation of resource access and, therefore, security, keeping the directory updated falls to the wayside.

Maybe it’s because it’s not interesting, challenging, or even remotely fun to do. I don’t know.

In writing this book, I wanted to present the problems having multiple directories introduces and discuss an organized way to ensure every directory – whether on-premises or in the cloud – is up-to-date.

And to boot, I want to elevate IT’s thinking about how to approach the actual work that needs to be done. The goal is to get the highest levels of accuracy, while involving the least amount of work.

I think it’s possible. Read on and see if you agree.

Nick Cavalancia

Microsoft MVP

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.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor 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 or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

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

The Directory Challenge in the Cloud

The cloud has significantly evolved over the past decade from a technology you *should* be using, to the established solution set for everything from commodity virtual resources and flexible infrastructure, to entire platforms and applications.

Because of this, organizations like yours have shifted operational models to take advantage of any and all that the cloud has to offer. Strategies include using mega-public cloud providers like Azure, AWS, and Google Cloud to host critical workloads, as well as leveraging specific cloud-based applications. The traditional on-premises environment as we've

historically known it is no longer a reality; 83% of organizations are running a hybrid environment that leverages resources and services both on-premises and the cloud[1].

This has created a challenge for many organizations; the *directory*. What was once just Active Directory acting as *the* directory for the entire organization, has slowly added cloud directories – first Office 365, then Salesforce, then Amazon S3, etc. With each newly added application and platform, the potential for distraction and shifting priorities grows significantly. This could lead you down a dangerous path of not just *one directory* that, someday, is so disorganized that you're unsure where to start the cleanup process, but *many*.

More Directories, More Problems

Many of you still see Active Directory (AD) as the directory authority and have ventured into the cloud looking for ways to sync with AD. Others see AD as just one of many directory services being utilized. In either case, with the reality of your environment to consist of a large number of disparate directories, it's now more important than ever to have all of your directories correctly configured, properly managed, and in sync with one another. Without ensuring this, the flaws in accuracy of your system of record are now amplified by synchronizing those same inaccuracies. For each cloud application you incorporate into production, there's one more directory that can be mismanaged with old user accounts, outdated group memberships, and antiquated security settings – all adding up to a nightmare from a few perspectives:

Management

Directory sprawl exists even within your hybrid environment today; within each there are accounts that aren't de-

1. IDG, *Cloud Computing Study* (2020)

provisioned, users that remain members of groups they shouldn't, account details that are antiquated, and security assignments that haven't been updated – let alone evaluated – *in years*. Now multiply the management headache of remediating that by the number of directories you leverage today to create your production environment…

It seems a shame to take on the sheer amount of work necessary to clean it up once, only to allow it to fall back into a state of entropy. And so, like most organizations, you choose to ignore the problem and focus on what seems to be more pressing initiatives.

Security

Credentials are the lifeblood of cyberattacks; without them, an attacker is rendered harmless. Use of stolen credentials is the second biggest threat action in data breaches (just behind phishing) and is involved in over one-third (37%) of all data breaches[2]. And placing credentials in the cloud is already giving IT angst, as 89% of organizations are concerned about storing credentials in the cloud[3].

Organizations are already experiencing the reality of the challenge of keeping a disparate set of cloud environments and resources secure; "securing/protecting cloud resources" is the third biggest challenge felt by organizations using the public cloud today[1].

The point here is that, if you add more cloud directories and continue to manage them as poorly as your on-premises directory (likely Active Directory) may be managed, they *all* grow into a state of configuration entropy, elevating the

---

2. Verizon, *Data Breach Investigations Report* (2020)

3. Dimensional Research, *Barriers to Adoption of Zero Trust* (2020)

organization's risk if a credential becomes compromised during an attack.

Governance

When we're talking about individual changes that have the potential to create a ripple effect across many cloud environments that can impact the organization's security, compliance, and productivity, the concept of governance becomes critically important. It becomes necessary to have a means to control who can manage the directory, what actions can be taken, and whether the actions performed meet organizational policy around standardization, security, and compliance.

Productivity

The inaccuracy of group and user account details can lower user and IT productivity. From incorrect phone numbers to misconfigured security and distribution groups, these simple inaccuracies can disrupt a user's flow and require the assistance of IT to identify and address the underlying problems.

There's a true story of a user who had shares of company stock that wasn't placed in the distribution group to receive related emails. He missed out on a deadline to sell shares that materially impacted the value of his shares. So, he lost real money simply because IT didn't put him in the right group.

Delegation in the Cloud

Thinking more along the lines of "sanctioned Shadow IT", cloud applications make it *really* easy for users to be delegated

control to create application-specific groups (e.g., Microsoft Teams) that don't necessarily make their way back to your other cloud environments or on-premises AD. Since no one wants to stop productivity or perceived advancement, these actions are allowed and users can go wild creating environments for themselves, despite the fact that this proliferates the problem of getting your enterprise's directory under control.

Tangible Costs

It's important to recognize that the previous three perspectives on the "more directories" problem come with real-world costs the organization must incur. Controlling cloud costs is the number one challenge for organizations using the public cloud[1] due to the lack of visibility and control that only multiply the following tangible costs:

- License costs – The cloud thrives on a consumption model; for every user added to any cloud directory, there's almost always an associated license cost.

- Management Costs – If not properly addressed, the work of daily managing the cloud can multiply out of control and require significant cleanup over time.

- Security Costs – Misconfigurations can and do have security repercussions. The average cost/record in a data breach is $146[4] – this includes detection and escalation, post-data breach response, notification costs, and lost business costs. With the average data breach costing just shy of $5.52M[4], the costs

4. Ponemon, *Cost of a Data Breach* (2020)

associated with getting licensing and management right pale in comparison.

How Do You Address the "More Directories" Problem?

Some of you may think Identity Management or Single Sign-On solutions can solve this issue. But it's not a "make everything appear like it's one environment" problem. It's deeper than that; the *directories themselves* aren't being managed properly. And with you likely syncing your on-premises directory out to the cloud, you're only multiplying the problem.

Take the example of John, who no longer works in Accounts Receivable, but *is still a member of the AR group*. He unknowingly has access to the AR SharePoint site in Office 365, the AR group folder on your on-premises file server, and occasionally still gets emails sent to the AR distribution group – all because of the original mismanagement of his user account in AD. Sync that account out to a cloud directory that further gives members of AR rights to applications, data, and services, and John's account only becomes more of a nightmare, and a greater potential asset to a cybercriminal.

The answer lies with implementing *Account Lifecycle Management* (ALM). As your organization expands to include more cloud-based directories as part of the environment, you need to build in lifecycle management processes to ensure each of the identities and accounts within your primary directory are 100% correct and secure, and synced with every other directory.

Account Lifecycle Management and the Cloud

The traditional method of "managing" a directory is completely reactive; every request comes from an outside source, and IT only involves themselves with changes to user and group accounts when requests come in. The very idea of adding in

more directories that leverage your on-premises directory as the source of accurate information, in a world where IT *isn't* focused on keeping the directory correct, is just plain scary.

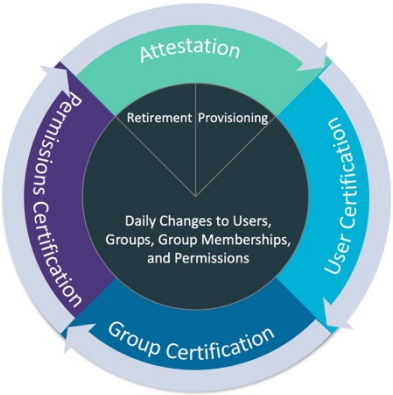
What's needed is a proactive method of managing accounts that ensures the entirety of your directory is constantly in a state of configuration that underpins organizational security and productivity, as well as IT's desire for flexibility, efficiency, and performance.

To accomplish this, your method of managing accounts needs to include a few characteristics:

- Integration – Your environment is made of up tens or possibly hundreds of cloud platforms, applications, etc. each with its own directory. Having a means to manage them all centrally under the umbrella of a single management console that presumably syncs changes out to all directories impacted via integration points is going to be critical.
- Delegation – I'm a big believer that IT shouldn't be the ones performing day-to-day account management. Employees closer to the user being managed and the corporate resources being given access to have much better context around what accounts need to be created/modified/deleted and whether resource access is appropriate. Department heads, business and application owners, etc. can be far better choices to ensure a more secure and correctly configured directory. Your ALM strategy should include some form of delegation.
- Policy-Based Management – Because you are likely going to delegate, it becomes necessary to establish specifics around which accounts can be managed,

what access can be provided, and even details like the format for how a phone number should be inputted – it all matters when this all will be synchronized out to however many directories you have in use. The method of ALM used should include an ability to establish policies and process to ensure a consistent result on the other end of the management task.

It's important that the focus be on both users *and* groups. After all, any abilities granted to an employee are done through either groups the employee's user account is a member of, or through the user account itself. ALM can be summed-up using the following image:



The Directory Management Lifecycle

The idea behind the lifecycle is that during the time a user or group object exists, it should be periodically reviewed to ensure its configurations (think attributes, memberships, permissions, etc.) are all correct. Anything from a wrongly positioned title to a no-longer-needed membership in a group can have repercussions.

The remainder of this section is applicable to every directory you are responsible for. The challenge is going to be how do you do this once and see it reflected everywhere?

The following six parts of the lifecycle outline the tasks that must be accomplished to keep every one of your directories current and secure.

Creation / Provisioning

I'm definitely not going to cover how to create a user or group; that's not the purpose of this book (and I assume you already know how to do both pretty well by now). But in ALM, when creating a user or group, there are a few aspects of doing so that need to be addressed:

- Assigning Ownership – User and group accounts in AD have always had fields in each that denote who's responsible for the created object – groups have the *Managed By* field, users have the *Manager* field. We've never given much thought to these fields, as they were never really used as part of any management process. But, in ALM, the concept behind these fields – holding individuals accountable for the state of a given account – plays a much greater role than just documenting who someone reports to. So, having an ability to assign ownership and delegate management capabilities (more on this later) is going to be critical.
- Attestation – While I'm going to cover this topic in more detail later on, in an ALM-centric environment, users and groups aren't simply created as desired. The

assigned owner (which, initially, may just be HR for new users) must attest to the need for the new account and its singular purpose. Most organizations ignore this process for regular users. But it's probably a good idea to have attestation in play when it comes to creating users or groups that will be granted elevated permissions (e.g. perhaps there's already an account or a group with the permissions you require?).

User Certification

Every user account's purpose has a beginning, a middle, and an end. Employee's get hired, work, change roles, and eventually leave the organization. So, it's important to certify throughout their employment that a user account is still needed and correct within your directories. There are a few points in time throughout the lifecycle of a user account that should be associated with user certification.

- At Provisioning – It's not enough to have IT create a user account. The assigned owner (usually the employee's manager) needs to review the account to ensure the specifics are correct. This should include all account details and group memberships. The scope of who is responsible for review should fit your normal business practices, but it can include IT human resources in addition to manager.
- When Roles Change – When a user takes on a new position, a lot needs to change in their user account: account details, assigned groups to provide proper access, and a newly assigned account owner. My previous example of a user that is no longer in AP exhibits this case.

- When Changes Are Requested – IT needs to build out a change workflow that puts the owner squarely in the approval seat to ensure that no changes made to an account they own are made without their expressed permission. This keeps their accounts in a known state and makes certification easier.

Group Certification

Unlike user accounts, groups tend to live indefinitely in most organizations. Mostly because nobody really owns a group, and so there isn't an individual that knows if the memberships are right, if nested groups should be there, etc. Because of this, groups tend to just evolve over time, growing further and further away from their originally intended purpose.

Group certification starts the moment a group is created. A good practice at time of creation is to compel the creator to state the purpose of the group. In IT, we often forget why we do things ourselves and quite often, someone else created the object and we need context of what it was to be used for.

And because groups are the primary way most organizations grant access to valuable resources that are prime targets for data breaches, these are probably the most critical accounts to manage. The assigned owner should be going through the following tasks:

- Certifying Group Account Details – The owner should make sure all the fields used to define a group are correct. Even something as basic as the name needs to be reviewed. *Why?* Because so many organizations use

cryptic names and over time, without a group owner, groups tend to be repurposed – given additional permissions and added members – which tends to give many members unnecessary rights.

- Certifying Group Permissions – This is a tougher task, as there are a few players involved, as well as a few steps. The goal is to make sure the permissions assigned to the group are correct and still necessary. This means the owner will first need to validate what permissions are necessary for a group member to accomplish their job. Then, the owner will need to verify with IT what permissions were actually assigned.
- Approving Permission Changes – Like users, a workflow needs to be put in place that empowers the owner to approve all permissions assignments. This is critical, as (we all know) permissions aren't documented in the group object, but in the application or environment in question. The workflow is necessary, so the group owner is always up-to-date on what permissions have been assigned to their group object.

If you have a solid change management process for the tasks listed in this part of the book, the periodic certification and attestation processes take a lot less time, as the owner is keenly aware of the state of their user(s) or group(s).

Membership Certification

Managing group memberships is probably the lowest thing on your task list, right? And yet, the addition of a user to a group

has the single largest ability to grant massive amounts of power over everything up to the entire environment. So, memberships need to be scrutinized in the following ways:

- User Accounts as Members – Permissions assigned to a group grant access to everything, from part of your directories to valuable/critical/protected data. As such, only those users that absolutely must be a group member should be. The owner should be validating users as group members by checking with both the appropriate business owner (e.g. a department supervisor) and/or HR. Anyone not appropriate should be removed.
- Nested Groups – Nesting can create some hairy situations. The idea that someone gets permissions to access sensitive data by being in a group that's in a group that's in a group… (you get the point) makes it difficult for an owner to a) see the net result of who's actually a member, and b) be in charge of removing members (as they don't necessarily have the ability to remove someone's membership in a *nested* group). Owners should limit nesting and, if it's necessary, have a process in place to work with nested group owners to validate the need for each nested group member to have the access the owner's group affords.
- Membership Changes – Just as owners need to be privy to changes made to users and groups, any changes to membership should flow through the group owner so they are aware of who is being added by IT and why.

Attestation

The process of attestation is necessary to ensure that a user or group account that currently exists *needs to continue to do so*. Too often, organizations create user and group accounts and either forget they exist or repurpose them without first reviewing the account's configuration thoroughly to ensure the only access provided is that which is necessary for the current need.

At this point in the ALM, attestation is about verifying the following:

- User Account Existence – It's a simple question, really. *Does this account still have a purpose?* If it's still being used by an employee or an automated process, then it should remain. If not, steps need to be taken to remove that account (see the next section for more on this).
- Group Account Existence – Same as above. *Does the group (and the access it affords) still have a purpose?* A group created for a short-term project may have no use. But a group with 20 users as members may still need to be in use, but only 2 of the 20 need to remain as members.

In both cases above, the account's owner needs to attest to the need for the object to IT.

There's always the valid question of "how often should you be certifying/attesting?" There's no one right answer. Groups have the greater potential for long-term mismanagement. So, group certification and attestation should be done quarterly. User certification and attestation for regular user accounts should be done anytime a user's role changes. Elevated accounts should be certified at least twice annually.

Retirement

If attestation results in realizing the need to retire a user or group account, a process should be established to address those unnecessary accounts. There are two basic actions that can be done when an account needs to be retired:

- Disable – Assuming the directory service in question supports it, accounts can be disabled. This action does concern me from a security perspective, as leaving an account in place that has the potential of being re-enabled to be used once and then forgotten creates a security risk for the organization. But, it's an option.
- Reconfiguration – This should only be used in very specific circumstances, such as the short-term project group example above. The danger with reconfiguration is that, if you do not have a complete handle on permissions, the risk of unknowingly granting access to resources is high. I'd suggest deleting and recreating users and/or groups if this is the option you're leaning toward.

- Deletion – Ahhh… now we're getting somewhere. Once an account no longer has a purpose, get rid of it. It's a move most IT folks wince at just a bit – mostly because you're not 100% certain that user or group *isn't* being used any more. But in an ALM scenario, the owner has attested to the fact that it's no longer needed. Take a deep breath… and press delete.

Applying ALM to Every Directory

The last part of the discussion here is to figure out the best and easiest way to get every cloud-based directory current and correct. There are a few ways this is accomplished:

1) Syncing – In some cases, simply syncing with your source directory does the trick (as in the case of a user's phone number). But in some cases, where a cloud application has its own directory-specific attributes, syncing can't address the issue. Additionally, it can get a bit tricky if you don't have a single system (read: directory) of record that *every* other directory syncs with; if you need to do some kind of daisy chain sync (e.g., directory A syncs with B and then B syncs with C, etc.), you're probably going to lose something in translation.
2) Build a Per-Directory Process – Because none of us really wants to work for a living, this should be a last resort and only apply to the exceptions that syncing doesn't address.
3) Use a Third-party Solution – There are solutions that connect to, manage, and sync a wide range of existing directories. Depending on your needs, this is probably going to be the most accurate, productive, and cost-effective option.

The Big Takeaways

The shift to syncing your on-premises AD with multiple cloud-based directories extends the risk of misconfiguration, inaccuracies, and inappropriate access to data and applications. On top of that, this is occurring within an environment we all know exists in a reduced state of IT visibility and control.

The good news is implementing Account Lifecycle Management empowers you to put a process in place by which to ensure *every* directory is correct, current, and secure.

By putting Account Lifecycle Management in place around each of your directories, leveraging delegated responsibility, you create a known-good directory environment. Account details are correct, so users can be more productive, and permissions and memberships are correct, upholding the desired state of security and compliance. The six parts of ALM covered in this book provide you with a foundation of steps necessary to retain a grasp of the current state of all your directories, what's changing, and how changes impact your organization.

It should be noted that native AD tools aren't sufficient for accurate and thorough Account Lifecycle Management in a hybrid environment, so it's going to be necessary to use additional solutions to unify, secure and manage ALM.

Notes

Notes

Notes

Managing and securing AD and AAD isn't one... with One Identity Active Roles.

- Unify, manage and secure AD/AAD
- Improve AD efficiency and enable Zero Trust security
- Deploy in the cloud without compromise
- Estimate your savings with our **ROI Calculator**

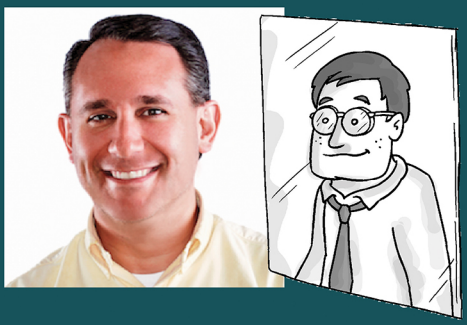
Learn more at **oneidentity.com/products/active-roles/**

Security Starts Here

ONE IDENTITY by Quest

Quickly become conversational about directory management in the cloud with these six steps

Use of the cloud has significantly evolved over the past decade – the traditional on-premises environment is no longer a reality. Where once the on-premises Active Directory was the directory for the entire organization, slowly more and more cloud directories have been added. This book will help you ensure that you maintain clean directories across multiple environments.



About Nick Cavalancia

Nick Cavalancia is Microsoft MVP, a Technical Evangelist by trade, and is a 25+ year IT veteran who regularly speaks and writes for some of today's most recognizable companies.