HOW TO CLEAN UP YOUR AD, AZURE AD AND OFFICE 365 GROUPS

Enhance security and drive productivity by getting group sprawl and authorization creep under control.

Written by Matthew Vinton, strategic systems consultant at Quest, and Bryan Patton, principal strategic systems consultant at Quest

Quest®

Group sprawl: what it is and why it matters

GROUP SPRAWL IN ON-PREM AD

Just how old is your Active Directory (AD)? Many of them date back years or decades. Even if you have an identity management solution (IDS), your AD has almost certainly accumulated some clutter over that time, including user accounts that no one is using and computer accounts for long-gone equipment.

Even more important, you've probably also lost track of many of the security groups tucked away in there. While some of them might be under proper governance and have clear owners, others have likely never made it into your IDS. Some of them may have even come along for the ride way back when you migrated to AD from a legacy platform like Windows NT, Novell NetWare or even Banyan VINES, and no one might remember what they were for — if they even realize they're still hanging around. Plus, AD groups can be nested inside one another, which makes it even more difficult to determine exactly what purpose each one was created to serve.

In addition, of course, you almost certainly have distribution groups, which are used for sending notifications to a group of people, and shared mailboxes, which are used when multiple people need access to the same mailbox, such as a customer support mailbox.

Can you say for certain that all your groups, distribution lists and shared mailboxes are accurate and up to date? Or it is actually quite likely that people — possibly many people — have access to sensitive information and powerful applications that they don't actually need to do their jobs?

GROUP SPRAWL IN THE MICROSOFT CLOUD

Group sprawl can get much worse when you migrate to the cloud. Most organizations synchronize their on-prem AD to Azure AD, so unless you clean house before the migration, your AD group chaos will come with you. Then, you will likely be creating additional security groups in Azure AD, because you'll have cloud-only accounts you need to manage, such as B2B (business-to-business) and B2C (business-to-consumer) accounts that enable partners, customers and other external users to access particular resources in your environment. On top of that are Azure AD's mail-enabled security groups, which are used for granting users access to SharePoint resources and emailing notifications to those users.

The problem doesn't end with AD and Azure AD security groups; you'll have to deal with Office 365 groups as well. An Office 365 group itself is nothing more than an Azure AD object that contains members. But when a group is created, the Office 365 service spins up resources in the associated Office 365 workloads, and members of the group automatically have permissions to access those resources. In particular, each Office 365 group has a shared mailbox and calendar, an associated SharePoint site collection, a OneNote notebook, and shared group resources in applications like Microsoft Teams, Yammer, Planner and PowerBI.

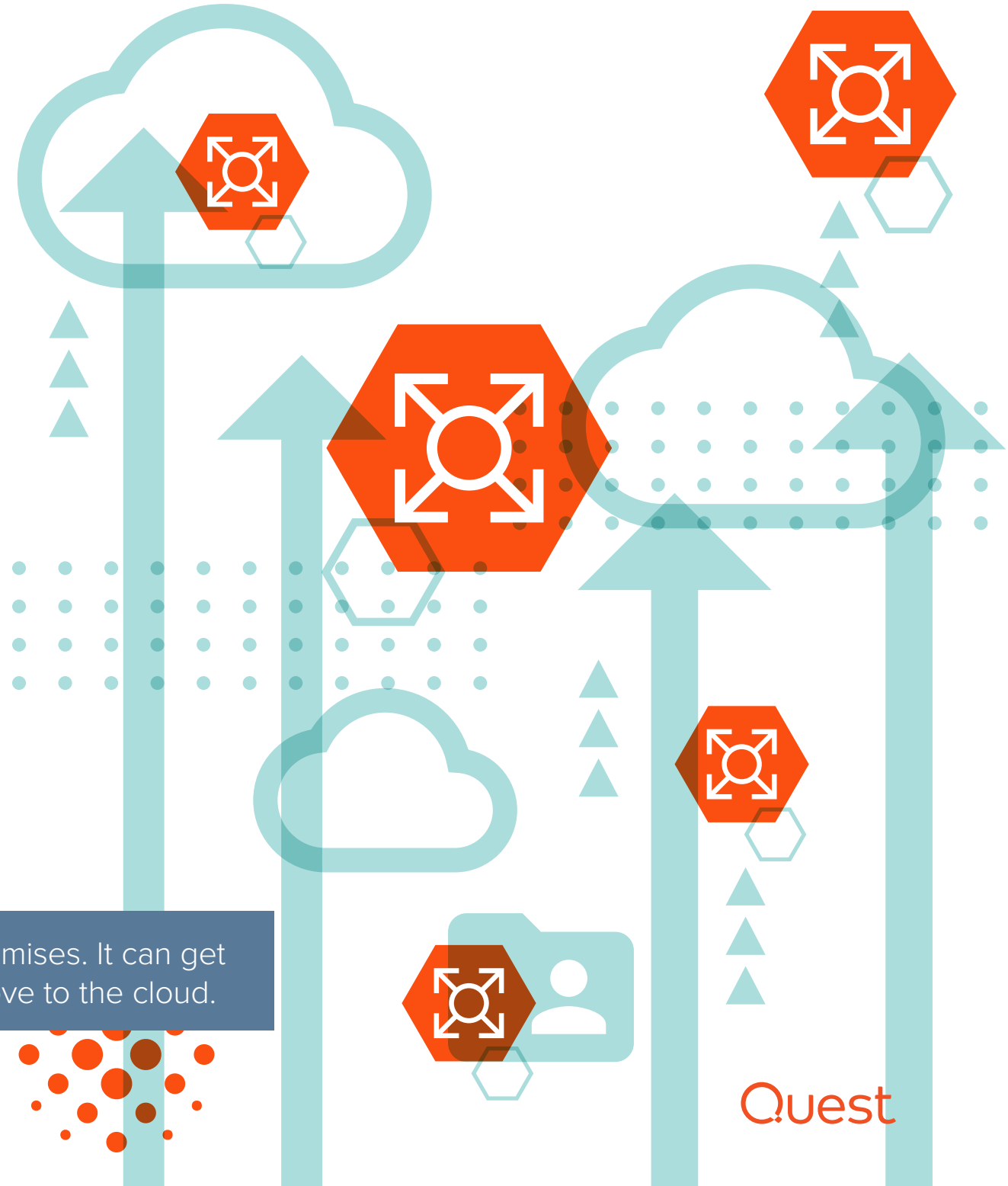
Quest

Members can access all of the resources and participate in all the Office 365 workloads attached to the group. And, importantly, Office 365 groups can include guests — users from outside the organization who have access to the group's resources.

Office 365 groups can spiral out of control exceedingly quickly. By default, users can create Office 365 groups as they please, and Office 365 groups are also created automatically by various applications, such as Microsoft Teams and SharePoint Online. While admins can deny users the ability to create Office 365 groups, that would defeat many of the benefits of your investment in the Microsoft cloud in the first place, since Office 365 groups are designed for the express purpose of facilitating collaboration and communication.

Finally, on top of all those Azure AD security groups and Office 365 groups, you'll probably also have cloud-only distribution groups and shared mailboxes to manage. That's an awful lot of opportunity for sprawl.

Group sprawl is often bad on premises. It can get much, much worse when you move to the cloud.



Why worry about group sprawl?

Does any of that matter? Actually, it does — quite a lot. Group sprawl can be quite costly in terms of both security and productivity.

SECURITY

AD groups and Office 365 groups are a cornerstone of security because they control access to your data, applications and other critical resources. If you don't have clear insight into and control over those groups, you simply cannot implement a least-privilege security model, as required by both security best practices and many regulatory mandates. As a result, users can easily have far more access rights than they need to do their jobs — authorization creep.

For example, suppose a security group is created for a particular project to enable its members to access particular documents and applications. The project comes to an end, but the group isn't deleted (sound familiar?), so everyone in that group retains access to all those resources — which they might accidentally damage or delete, or deliberately steal or sabotage. In addition, any attacker or piece of malware that gains control of a user's credentials has far wider reach than they would have if the group had been cleaned up. In other words, your attack surface area is larger than it needs to be. That matters a great deal, especially given that 95 million AD accounts are the target of cyberattack each day and there is a new ransomware attack every 12 seconds.

Office 365 groups are particularly concerning. One reason is that they can be owned and managed by end users with little oversight from admins. In fact, each Office 365 group can have as many as 100 owners, each with the power to rename the group, change its settings, add and delete members and guests, and so on. Over time, it's almost inevitable that groups will include members who no longer have a legitimate need to be in the group — and Verizon's research shows that 34 percent of data breaches are caused by insiders. In addition, group owners will inevitably leave the organization, and then there will be no one who is accountable for the membership of the orphaned groups. These risks are especially high when a group contains guests, since data is exposed externally.

Quest

In short, group sprawl and the associated authorization creep puts your organization at increased risk of security breaches and compliance failures. And the costs of a breach can mount quickly when you factor in expenses related to breach detection and containment, reporting to authorities, communication and reparations for affected parties, down-time, and lost business. In fact, Ponemon now pegs the average cost of a data breach at $3.92 million.

Your AD, Azure AD and Office 365 groups control access to your critical data and resources — so you have to have control over them.

PRODUCTIVITY

Group sprawl can also hurt productivity. Administrators will face an uphill battle when faced with even basic questions about who has access to a given resource or, conversely, which resources a given user has access to. As a result, both security investigations and compliance audits are a nightmare, and provisioning tasks are far more complicated than they need to be.

Users productivity is affected as well. For one thing, the person who creates an Office 365 group can name it anything they please, and the name of each of group will appear in your global address list (GAL), a tool people use all the time. As the GAL grows by hundreds or thousands of entries, users will find it harder and harder to locate the individuals and groups they need. From there, the problem can snowball: Since it's hard for users to determine whether there's already a group that would serve their needs, they create a new one — making the GAL even longer and perpetuating the cycle.

Best practices for managing groups

Exactly how can you go about cleaning up your groups and keeping your AD and Azure AD in shape moving forward? These best practices will help.

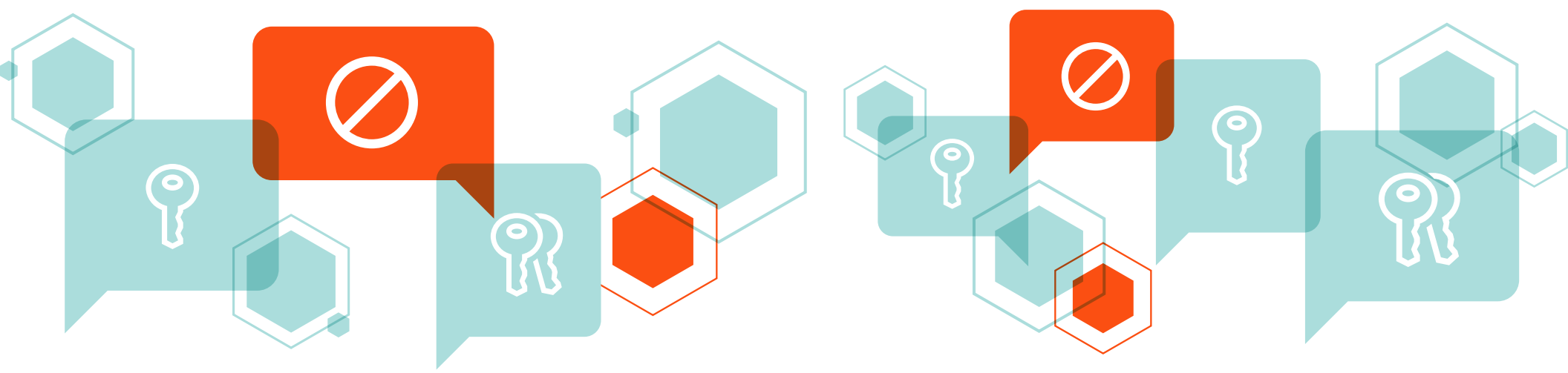
ASSESS YOUR GROUPS CAREFULLY

The first step is to determine the purpose and owner of each group, and then work with the owner to review the group's membership with the least-privilege principle firmly in mind. Be sure to take into account any nested groups in your environment. Audit records can be very helpful here, since you'll be able to see who has actually been using which resources and who might not need to be a member of a particular group. Note that this can be a long and tedious task with native tools; for example, you can't tell when or how a group is being used in your on-prem environment because you can't see its use during access.

Moreover, don't limit yourself to simply reviewing the groups you have. Instead, think carefully about what an ideal group structure would look like. For example, if everyone in a given department is a member of five different security groups, consider whether those groups could be combined into one group, which would simplify administration, streamline authentication and reduce the risk of overprovisioning.

UPDATE YOUR INFORMATION SECURITY POLICY TO ADDRESS LEAST PRIVILEGE

There are great policy templates available to help you create your information security policies, such as those from the SANS Institute. Using them as a guide, you can create a least-privilege access policy that details how and when access should be granted — and revoked — in



your organization. Be sure to cover all types of users, from technical people doing administrative activities in Active Directory to group owners to business users.

> Create a least-privilege access policy that details how and when access should be granted — and revoked — in your organization.

For example, if you have an AD security group that grants access to resources in Accounts Payable, you might want to ensure that someone from the finance department is responsible for regularly validating the membership of that group. Similarly, for any change that can affect many people, such as a change to Group Policy, I recommend requiring a workflow approval so that no one person can make a change that could damage the entire organization.

You might also want to disallow groups that have less than a specified number of members (such as five), or at least require an extra approval step for them. This can reduce the number of groups that have to be managed and keep the user authentication process from bogging down.

Once you're drafted your least-privilege access policy, don't forget to get executive buy-in for it — you need it to have teeth.

MAKE CHANGES, BUT DO SO WITH CARE

Organizations are in the business of providing services or generating revenue, so they are often reluctant to make changes to AD lest someone lose access to resources they need to do their job, disrupting a critical workflow. This fear is legitimate, but you should not let it keep you from doing the cleanup you need.

Instead, simply proceed cautiously. First, back up your current Active Directory and be sure you can granularly undo any changes you make so you can quickly restore any access rights that are improperly lost. Consider setting up a pilot project so you can get insight and feedback from a small set of users, and gain trust in the broader project. Then continue the cleanup based on the information gained from the assessment process and your information security policy.

IMPLEMENT PROPER GROUP GOVERNANCE

After the initial cleanup, be sure to implement a regular attestation process to keep each group's membership in line with your least-privilege access policy. It's smart to automate as much as possible. For instance, if an employee moves from one office to another, you don't want to have to be at the mercy of manual processes, such as someone from HR having to remember to inform IT or the user having to create a helpdesk ticket to get the access they need — that's a guaranteed recipe for authorization creep.

> A regular attestation process is critical to keeping group membership in line with your least-privilege access policy.

In addition, it's wise to set up groups to expire. For example, require group owners to renew their groups every six months if they're still being used. If a group isn't renewed, let it expire. Once you have determined that it is truly not needed anymore, delete it.

Choosing the right tools to help

THE LIMITATIONS OF NATIVE TOOLS

Unfortunately, native tools give you limited ability to know exactly what groups you have, how they are changing and whether they have the correct membership. Running PowerShell scripts and manually reviewing reports is simply not a scalable approach.

Other controls are lacking as well. For instance, as we saw, an Office 365 group can have literally dozens of owners — and native tools provide no way to granularly remove or delegate specific group management functions, such as disabling a group owner's ability to change the group's name. In fact, you have very limited control over the naming of Office 365 groups at all. There is a group naming policy feature in public preview that gives you a bit of control, but it comes at a price: You'll

Native tools give you very limited ability to know what groups you have, how they are changing and whether they have the correct membership.

Quest

need Azure AD Premium P1 licenses for all users who are members of Office 365 groups in the tenant.

Native tools also offer little help during the cleanup process itself or for ongoing management. As we saw, you need to be able to efficiently back up and granularly restore groups and group membership quickly if important access rights are lost by mistake. The AD and Azure AD recycle bins are no substitute for an enterprise backup and recovery solution, especially when critical workflows are at risk. Attestation about group membership is a difficult process that makes it difficult for even the most conscientious group owners to keep membership in line with the company's least-privilege access policy. And remember how Office 365 groups can quickly spiral out of control because users can create them at will? Well, there are no native tools in the base Office 365 licenses that provide an approval workload for group creation. Instead, organizations have to create their own workflows, such as requiring users to download a form from a SharePoint site and submit it manually.

Furthermore, you have to manage your on-premises AD groups separately from your cloud groups, which means constantly juggling different tools. In fact, even within the cloud environment, you need multiple tools, since Office 365 groups are managed in Azure AD while distribution groups are managed in Exchange Online. This fractured approach to group management drives up training and management costs, and fails to deliver the comprehensive understanding of access rights that is required for security and compliance.

HOW QUEST CAN HELP

Quest is your go-to vendor for everything Active Directory: management, migration, compliance, auditing and security. For example, you can:

- Get clear insight into all the groups you have across your on-premises, cloud or hybrid IT environment from a single console.
- Identify the probable owner of each group.
- Audit activity to determine who is using which resources and inform your AD cleanup strategy, all without the overhead of native AD auditing.
- See the last time an email was sent to each Exchange distribution group.
- Automate day-to-day AD management, including account provisioning and deprovisioning.
- Securely delegate AD administration using a least-privilege model.
- Back up and granularly restore AD groups.
- Implement robust group creation policies that control group naming, expiration and more.
- Implement automated workflows, including group membership requests from users and attestation by owners.
- Audit changes to AD, and even prevent changes to critical AD objects such as powerful administrative groups and important GPOs.

Conclusion

Decluttering years of legacy junk from your Active Directory can be time consuming and painful, and keeping it clean is an ongoing challenge. But the effort can really pay off — for example, one large Quest customer was able to eliminate over 14,000 groups from its Active Directory. Just imagine how much that cleanup enhanced security, improved productivity and reduced costs.

> One Quest customer was able to eliminate over 14,000 groups from its Active Directory.

With more than 149 million accounts managed, 101 million accounts audited and 86 million accounts migrated, Quest is the clear leader when it comes to Active Directory. I invite you to learn more at quest.com/solutions/active-directory/.

Quest

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

Ebook-CleaningUpAD-US-GM-40381

Quest