Highlights from a recent webcast on Active Directory

ACTIVE DIRECTORY GROUPS: OUT OF SIGHT, OUT OF MIND, OUT OF CONTROL

Managing Active Directory Groups is a hassle, but it's critical. Here's how to get groups under control.

There aren't many of us who are afraid to admit it: the last task on your list of favorite things to do is manage your Active Directory groups. It's one of those things we try to get done as quickly — and as pain-free — as possible. Once you've created a group, added some members, and assigned it permissions, you've probably never looked back.

And while group management seems simple enough, it's that simplicity that causes IT to focus on more important tasks. We all know the adage "the squeaky wheel gets the oil." Because groups never really complain — they don't set off alerts, never produce errors, nothing — they're naturally going to fall off of IT's radar.

However, if you were to stop and take an inventory of the current state of your AD groups — and dig deep, just a little — you'd likely find problems like incorrect memberships caused by the duplicative use of a single group, now with disparate and unaligned sets of permissions, granting too much access to applications and data to the already bloated membership.

And that's just one group!

As you begin to wonder how your groups even got into the shape they're in, the good news is that you can do something to fix it. But it does involve understanding the leading indicators of group mismanagement, recognizing the true state of insecurity this puts the organization in, and taking steps to rectify the issue.

Out of Sight, Out of Mind

There are some common AD group "red flags" that help you identify when AD group management is clearly not part of IT's focus:

- No Group Membership (no members in the group)
- No Ownership
- No Recent Changes
- No Attestation
- Duplicate Groups
- Repurposing Groups

In each of these cases, if left alone over time, the state of AD groups simply gets worse. Take the lack of ownership as an example. While we're talking about a group with no Managed By value, the real issue is what that implies — there's no management or accountability. Like most groups in AD, the group was simply created, some users were added, and permissions were assigned. And, over time, that means IT loses touch with why the group exists and how it should be kept up-to-date.

"The last thing the person who is responsible for the directory really knows is how a group is being used," says Jonathan Blackwell, product manager at Imanami. "They don't understand the content that that group is governing, nor the employees that make up the group membership. No one's providing any kind of maintenance."

So, even if someone does review a group's membership, there is little context around whether it's correct or not. And as time passes — like the chaos experiment with a deck of cards where you repeatedly pick them up and drop them — it simply grows to be in a continually worse condition.

Out of Control

One of the reasons for this chaotic group growth is that IT feels the need to be the only ones in charge of groups. Choosing who should be a member? IT's job. Deciding what permissions should be applied? That's IT, too. The challenge with that line of thinking is that the IT pro isn't necessarily the

> "The best thing to do is to realize that this is a problem in your organization, even if you don't visibly see it." —Jonathan Blackwell, Imanami product manager

expert in, say, who's in the sales department, or where within the CRM application salespeople should have permissions. "The IT worker is usually several degrees removed from what the group is intended for," says Blackwell.

And it gets worse. IT probably hasn't delegated responsibility to line of business owners, department heads, and others within the organization who are far closer to the groups themselves. This lack of ownership then mixes with IT's inability to ever get back to these groups and ensure proper permissions, membership, and usage. The resulting situation is one where you're left with groups under no one's control at all, granting more access than assumed, to more people than intended, for far longer than ever desired.

Getting Groups Back Under Control

The first step, like any good multi-step recovery program, is to admit that you have a problem. "The best thing to do is to realize that this is a problem in your organization, even if you don't visibly see it," says Blackwell, "You don't want to wait until an accident happens." After that, it's a matter of following a process that matures you from the aforementioned "set it and forget it" group management of yesteryear, towards an actual group management lifecycle. The steps include:

- **Assessment —** Take a look at the current state of your groups, using the red flags to identify those groups that are in worse shape, to get a handle on what you have.
- **Assignment —** Owners need to be assigned. And don't just set the Managed By value. An actual person needs to own the group and the access it represents. In some cases, there should be one owner for the group, another for the membership, and another for the permissions. And they may not all be the same person, or even someone in IT.
- **Accountability —** All requestors for membership changes, or assignment of permissions need to be held accountable to ensure that the changes requested align with the purpose, access, and security of a group. In some cases, a new group needs to be created, or in others a request for a new group can be appropriately accommodated in an existing one.

All of this culminates in maturing to a group management lifecycle, where each part of traditional group management — group creation, membership, and assigning of permissions — is certified and attested to by an owner. This creates a secure AD environment where permissions are no longer out of hand, users only have appropriate access for their job, and the overall organization is more secure.

The Imanami GroupID Approach

Imanami enables continual ownership and management of Active Directory groups through the use of automation, empowering organizations to maintain a complete group management lifecycle that includes the creation, use, expiration, and deletion of Active Directory groups.

Imanami's GroupID solution automates the creation and management of Microsoft's Exchange and Active Directory distribution lists and security groups, utilizing dynamic memberships. For groups requiring personal attention, the group management workload during a group's use is offloaded from IT by allowing users to manage their own groups, but giving IT the control to keep it from getting out of hand. Automated group expiration forces an owner to actively renew a group to continue to use it: group owners are notified before expiration, giving them time to renew it or let it expire. And automated deletion of a non-renewed group keeps Active Directory clean and more secure.

Through this comprehensive approach to group management, Imanami puts the control of AD groups actively back into the hands of IT, while placing the burden of day-to-day management of groups on business owners who are aligned with their use.