How to Clean Up Your Active Directory

blog.netwrix.com/2023/05/05/cleanup-active-directory

Joe Dibley

Despite the popularity of the cloud, Microsoft Active Directory (AD) remains a crucial component of the IT infrastructure for many organizations. Indeed, Active Directory often serves as the central identity repository and provides vital authentication and authorization services — so keeping it clean and well organized is vital.

Discover exactly why regular AD cleanup is critical — and the key signs of a poorly maintained AD environment. Then get valuable tips for cleaning up your Active Directory and learn about a solution that can help.

Handpicked related content:

Active Directory Security Best Practices

Benefits of a Clean Active Directory

Active Directory is the central repository for user accounts, computer accounts, server objects, Group Policy objects and other important information. But the AD database can become cluttered and fragmented over time as users join and leave the organization, computer hardware is refreshed, Windows Server is updated on domain controllers, and other changes are made. By cleaning up your AD, you can improve all of the following:

- **Performance** — Changes to the Active Directory database are constantly being replicated among your multiple domain controllers, and a bloated AD creates unnecessary replication traffic. It can take longer to authenticate users, search for AD objects and download Group Policy objects. Cleaning up your AD regularly helps these processes perform optimally.
- **Security** — Threat actors often seek to gain access to networks by taking over Active Directory user accounts of former employees that were never deleted. Regularly removing unused accounts shuts off this attack path.
- **Compliance** — Many regulatory mandates require organizations to implement strong controls over user identities. Regular Active Directory cleanup can help your organization achieve and prove compliance with these provisions.
- **IT operations** — A cluttered AD makes management much harder for administrators. By cleaning it, you can reduce the time they have to spend supporting it, giving them more time for strategic initiatives.
- **Business agility** — Mergers and acquisitions often involve consolidating Active Directory environments, often on a tight schedule. Meeting those deadlines is much easier when AD is clean and organized. More broadly, AD cleanup simplifies the job of adding new applications, updating workflows and making other changes to drive the business forward.

Signs of a Poorly Maintained Active Directory

Signs of a poorly maintained AD environment include the following:

- Stale, duplicate or orphaned user accounts
- Empty or duplicate security and distribution groups
- Little insight into security group access permissions
- Lack of an established process for provisioning and de-provisioning accounts
- Inability to determine ownership of objects and groups
- Inaccurate or incomplete object attribute details

How to Clean Up Active Directory

The following best practices can help you clean up your Active Directory:

- **Regularly identify stale, disabled, inactive and orphaned user accounts** — Adversaries look for unused Active Directory user accounts they can compromise in order to gain access to sensitive data. Some AD management products not only identify risky AD user accounts but provide customizable workflows that can automatically move them to a staging OU so you can review the impact of deleting them individually or in bulk.
- **Identify duplicate user accounts** — Users can end up with multiple accounts after changing roles within the organization, especially if you have multiple AD domains. Cleaning up these duplicate accounts can reduce complexity and confusion that can lead to security risks associated with overprovisioning.
- **Ensure user account attributes are complete and accurate** — Active Directory cleanup is about more than just deleting objects. It's also about ensuring that your AD objects are properly populated with all the information required for proper account management. Be sure to perform metadata cleanup as well.
- **Leverage historical SIDS** — Eliminate token bloat and broken access control by identifying and cleaning up historical SIDS to improve performance.
- **Identify expired passwords** — Identify Active Directory accounts with expired passwords, since they can indicate that the account is infrequently used or inactive. Settings
- **Find empty, duplicate and circularly nested groups** — Identify and remove empty or duplicate AD groups that serve no purpose. Solutions like Netwrix Active Directory Security Solution can also identify and help you remediate circularly nested groups that hinder AD performance.
- **Review security groups with large membership** — While some security groups, such as Everyone, are meant to be large, most security groups should be much smaller. Make sure each group includes only the users who need the resource access that the group provides.
- **Clean up mail-enabled groups** — Distribution lists and mail-enabled security groups often become bloated over time because their owners fail to keep them up to date. Make sure your solution can identify these groups and help you clean them up.

- **Ensure each group has an owner and require regular attestation** — Each group should have an owner who is required to regularly attest that the group is still needed and that it has the correct permissions and membership.

How Netwrix Can Help

Using native tools like PowerShell to clean up your AD is time-consuming, and writing and maintaining scripts requires expertise. But the Netwrix Active Directory Security Solution enables you to easily query, analyze, report on and remediate unwanted objects in your Active Directory and file systems so you can finally bring Active Directory under control. As a result, you can strengthen security, achieve and prove compliance, make your IT teams more efficient, and improve business agility.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.