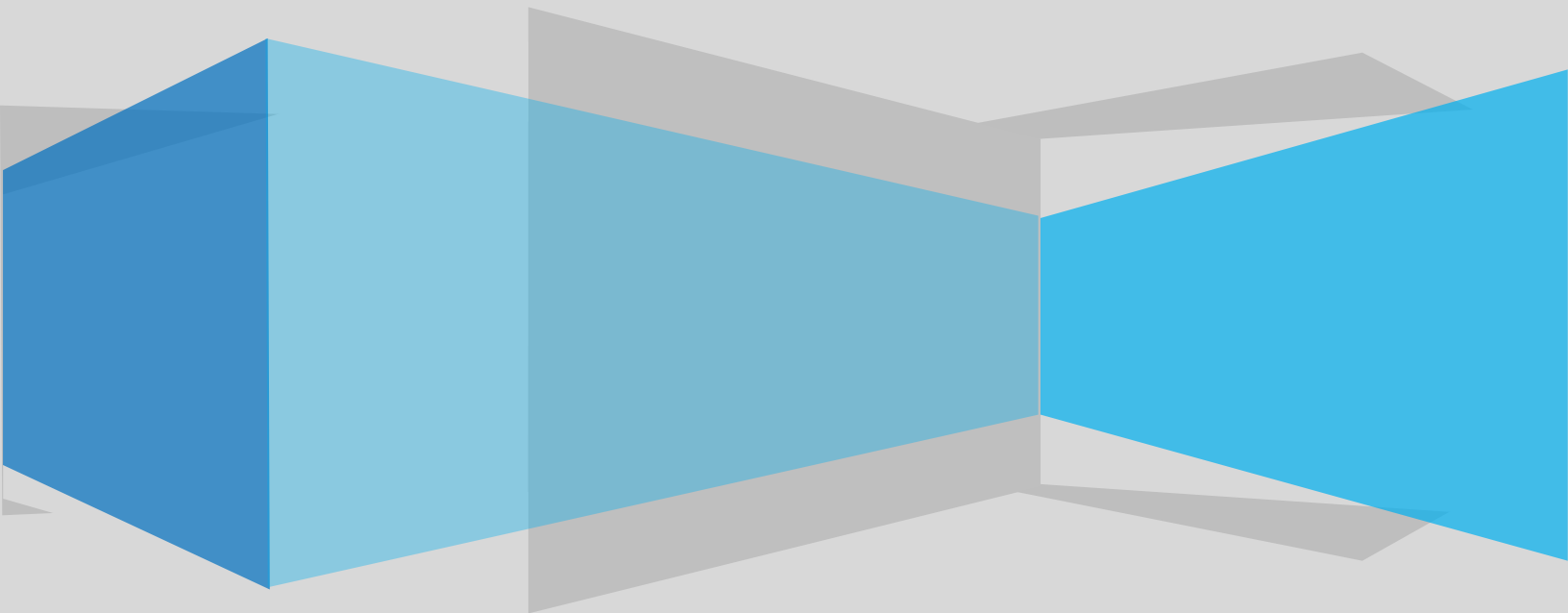


BEST PRACTICES TIPSHEET

ACTIVE DIRECTORY

MAINTENANCE & CLEANUP



The Problem

At the heart of your Active Directory forest is the user, group, and computer base. Systems administrators, managers, end users and even new employees will hound access and administration groups whenever new user accounts, group memberships, and computer accounts are needed. *Business processes can't happen without access to the infrastructure.* As a result, certain groups are empowered to add these objects directly into AD without oversight or formal process for tracking new objects. Directories grow over time from normal business processes, mergers, acquisitions, domain consolidations, and even certain configuration or upgrade paths.

The process and follow-through drops off tremendously when these resources are no longer needed. Users retire or leave organizations, certain security and distribution groups are temporary for projects and collaborative needs, and servers and workstations are rebuilt with new names, or decommissioned all together. *Business processes will still continue to operate when objects that are no longer needed remain in your directory.*

The task of identifying stale or unused resources falls to many different groups, and most times, the central Directory Services Groups do not want to bear the burden of the data held within AD. However, it is in the best interest of all parties involved—including the organization itself—to regularly look for and clean out these stale and unneeded resources.

Our Solution

The StealthAUDIT Management Platform helps to build a streamlined process to identify, review, and ultimately retire thousands of stale objects from your directory. SMP for AD lets you quickly take inventory of these directory objects to summarize key information and correlate data between them based on the relationships they have to one another. Moreover, clean-up campaigns will be largely unsuccessful without applications like SMP, which allow for facilitated workflow methodologies that let you interact with the thousands of systems administrators, managers, and custodians in your environment to solicit their participation and approval to make the changes on the resources that they know best.

Clean-Up and Maintenance Tips

Now, let's take a deeper dive and examine some key business issues that arise when there are stale or needed items left behind for each of the key object types.

Users

User objects are often tied directly to different application and service licensing agreements. Many organizations get around this issue by negotiating to an official employee count. Beyond licensing, user objects left in AD create overhead for the directory backup, restore, and other application synchronization tasks. They make finding the right user more difficult, which leads to wrong users being added to resources, security groups, and distribution groups. The impact to your messaging environment includes a growing Global Address List, longer download times for mobile users, misdirected email messages, and extra disk space that's required for abandoned mailboxes and system processing when email is returned from mailboxes that are at capacity. Cleaning up stale and unneeded user objects reduces the operational impact, end user experience, unintentional actions, and also reduces security exposure where older accounts are prime targets for hackers.

TIP 1: Combat these risks by using each user object's Last Logon to Domain timestamp as an indicator to find stale and unneeded employee, contractor, and service accounts.

TIP 2: Survey managers at least on an annual basis to re-certify these accounts and/or request permission to disable and/or delete them.

Computers

Computer objects are continually added for servers, workstations, and mobile devices. Much like user objects, these are usually tied directly to different application and service licensing agreements. Inaccurate system counts can lead to gross overpayments for applications and services. Active Directory is supposed to be the authoritative source for understanding and securing what's in your infrastructure, but when these stale objects are not maintained, the information becomes unreliable. Any application that relies on the systems stored within AD will begin to have issues with finding and interacting with systems, which may cause failures or delays due to processing times. Cleaning up stale and unneeded computer objects reduces operational impact, administrative time, and unintentional actions. It also reduces security risks, as older accounts are prime targets for hackers.

TIP 3: Combat risk by using each computer object's Last Logon to Domain timestamp as an indicator to find stale and unneeded servers, workstations, and mobile devices.

Tip 4: Survey managers at least on an annual basis to re-certify these accounts and/or request permission to disable and delete them.

Tip 5: Track and trend system administrators/custodians while systems are in production for reference when systems are offline, having issues, missing, or being retired.

Distribution Groups

Having an excessive amount of stale or unneeded Distribution Groups causes situations where mail can be misdirected, and increases the potential for security leaks, where sensitive information gets sent to inappropriate individuals, groups, or even outside parties.

Tip 6: Track and trend message logs for a review of *who is sending to what distribution groups*, as well as, *what distribution groups are no longer being sent to at all*.

Tip 7: Review distribution groups that are nested inside other distribution groups to identify exceptions of direct mailing statistics.

Tip 8: Survey managers at least on an annual basis to re-certify groups and their direct and effective membership, and/or request permission to delete any that are no longer needed.

Security Groups

Security Groups, in addition to their user accounts, define what individuals have access to within the infrastructure—including computers, applications, and data. Stale or unneeded Security Groups in the environment present confusion, and often there's no oversight to ensure that direct and effective group memberships are accurate.

Tip 9: Review the last Direct or Effective Member Change Date as an indicator of security groups that have gotten stale or are no longer needed.

Tip 10: Survey managers at least on an annual basis to re-certify groups, their direct and effective membership, and/or request permission to delete any that are no longer needed.

Token Bloat

A user's token grows in size as a result of normal business activity when he or she is added to additional security groups, has been migrated from another domain, or when any security group they are a part of has been moved from another domain. Key business scenarios where tokens grow as a result of migrating objects from other domains include mergers, acquisitions, or certain upgrade paths. The more groups an individual is a part of, the bigger the token size. Large tokens cause latency in login times and can even cause the inability to log into Exchange, File Servers, Active Directory, and other Applications. This in turn increases help desk calls and reduces productivity from all tiers of response personnel.

Some key indicators of token-related issues are when a single user cannot log on to the Domain or a resource, multiple users cannot log on to the Domain or a resource, or when there is significant degradation of Exchange server performance.

Tip 11: Identify and reduce users with excessive direct and/or effective group memberships.

Tip 12: Review and educate administrators on token bloat issues that *can* and *are* managing groups and respective group memberships.

Tip 13: Remove SID history from user and group objects after careful impact assessment to see where those historical SIDs are tied to systems, applications, and data within your infrastructure.

About STEALTHbits

STEALTHbits Technologies, Inc. provides a rich set of solutions to help manage your Microsoft infrastructure and beyond. As an industry leader in Auditing, Reporting, and Compliance software, solutions from STEALTHbits increase efficiencies, reduce downtime, and optimize the performance of your systems and applications to provide instant value and the quickest return on investment.

About StealthAUDIT

Using over 30 comprehensive Data Collectors, the StealthAUDIT Management Platform (SMP) gathers information about Windows servers, workstations, Active Directory, Exchange, BlackBerry, Share Point and more, all from a single product.

Once the data is returned, administrators can view the results in customizable reports, use the platform's Analysis Modules to interact with the data, and even make changes using integrated Action Modules—all from within SMP!

System Requirements

Operating Systems

Workstation: Windows 2000 and up
Server: Server 2000 and up

Application Versions*

MS Exchange Server v.5.5 - 2010
BlackBerry Enterprise Server v4.x - v5.x
Active Directory NT4 - 2008

Platform

Pentium 4 class or greater
Memory and Disk Space
1Gb RAM minimum (2 GB rec.)
1Gb Available Disk minimum
100Mb Network Connection

Additional Software

Microsoft SQL 2000 or greater (including SQL Express)
Exchange System Manager
Adobe Flash

*Requirements vary based on product

Contact Us

STEALTHbits Technologies, Inc.
55 Harristown Road, Suite 106
Glen Rock, NJ 07452
USA

P. +1.201.447.9300

F. 201.447.1818

W. www.STEALTHbits.com

Like:

www.facebook.com/stealthbits

Follow:

www.twitter.com/stealthbits

Watch & Learn:

www.youtube.com/stealthbits

Read:

www.stealthbits.com/blog