Data Sheet

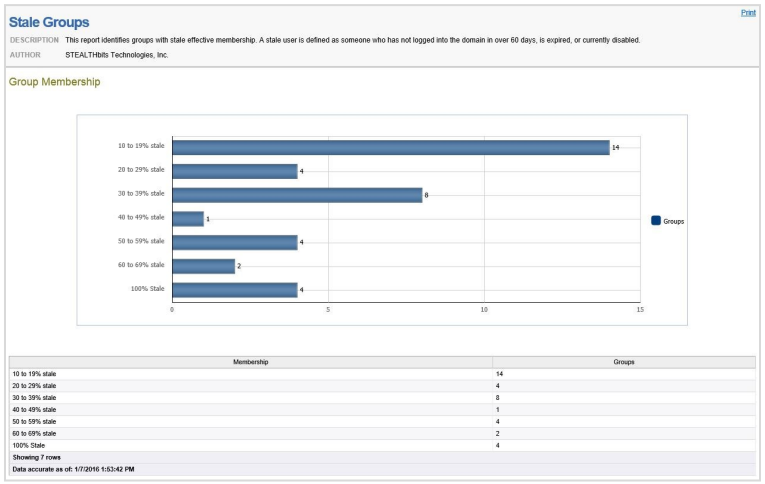
StealthAUDIT® for Active Directory

As the primary authentication and authorization service for the majority of IT systems, the importance of Active Directory (AD) is not to be understated. Over time, AD has grown increasingly complex, less secure, and more difficult to manage, resulting in a growing problem for organizations large and small.

STEALTHbits Technologies' StealthAUDIT ® for Active Directory is an auditing, compliance, and governance framework for AD that provides comprehensive data collection, analysis, remediation, and reporting facilities to combat the complexity, security, and management challenges today's organizations face. Through an agent-less architecture designed to scale in organizations of any size, StealthAUDIT for Active Directory provides the power and tools needed to clean up and manage AD easily, efficiently, and cost-effectively.

StealthAUDIT for Active Directory Features

StealthAUDIT for Active Directory provides a powerful out-of-the-box experience with dozens of preconfigured reports and workflows aligning to security, compliance, and operational management concepts.



StealthAUDIT Stale Groups Report

Active Directory Cleanup – Configure automated or programmatic cleanup of stale objects like users, groups, and computers, as well as enrichment of object attributes through integration with authoritative data sources like HR systems and configuration management databases (CMDBs). Ease administrative burden and strengthen the integrity of Active Directory through supported actions including modifying, moving, deleting, creating, enabling, disabling, resetting, and unlocking user, group, and computer objects.

Group Governance – Examine Active Directory to identify the owners of every group and allow them to perform periodic membership reviews. Ensuring proper ownership and membership increases security while reducing administrative overhead.

Best Practices – Verify key configurations and conditions meet best practice standards, such as the status of user passwords and their associated complexities, service accounts and their levels of privilege, and the usage of historical security identifiers (SIDs). Ensuring your organization follows best practices prevents attackers from exploiting known weaknesses and common vulnerabilities.

Group Membership Analysis – Unravel complex group nesting and other toxic conditions that make determining group memberships difficult—and managing them overly complex. Understanding the effective membership of every group,

and the group conditions that should *not* exist, helps ensure that the right people have the right access to the right information.

Object Permissions – Know who has what permissions to objects in Active Directory, including advanced permissions and organizational units (OUs). Easily conceptualize fine-grained security controls across the enterprise to ensure privileges are in alignment with desired security controls.

Stale and Duplicate Object Remediation – Gather and report on toxic conditions related to stale, orphaned, and duplicate objects within Active Directory. This comprehensive report set assists organizations in highlighting what needs to be cleaned up in Active Directory to reduce complexity and ease management overhead.

Group Policy – Highlight in detail where Group Policy Objects (GPOs) are linked, their order of priority, and the details about all policy settings. Understanding Group Policy's effect on users and computers is essential to foundation-level security.

Access Change Modeling – Model how changes to group memberships affect user access to data resources before committing changes. Having visibility into what the downstream effects of adding or removing group memberships are prior to committing changes reduces the opportunity for overprovisioning access or inadvertently causing resource access loss.

Active Directory Health – Determine the health of Active Directory through a series of metrics focused on optimal directory performance. Assessing Domain Controllers for overall operational efficiency helps promote uptime and proactively identifies issues before they lead to unintended outages.

Customizable Reporting – Easily enhance out-of-the-box reports with the ability to customize and filter report details to precise specifications. Reports are exportable in a variety of formats including HTML, CSV, XLS, XML, and PDF.

Installation Requirements – StealthAUDIT® for Active Directory

StealthAUDIT Console Server

- Windows Server 2008 R2+
  - IIS / .NET Framework 4.5 installed
- 8+ GB RAM & 4+ CPU Cores
- 30 GB Disk Space
- Microsoft Silverlight

StealthAUDIT SQL Database Server

- Microsoft SQL Server 2008+
- 16+ GB RAM / 8 CPU Cores

About STEALTHbits Technologies, Inc.

STEALTHbits Technologies is a data security software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Identify threats. Secure data. Reduce risk.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com