Best Practices for Auditing Changes in Active Directory
Executive Summary

Active Directory (AD) is a well-known, highly used, very reliable and powerful network operating system. Since the introduction of Active Directory by Microsoft in 2000, organizations around the world have implemented AD to be the standard for centralized management of the Windows infrastructure.

Since its introduction, we have seen revolutionary changes to Active Directory, which have made the management of all aspects of the environment easier and more reliable. However, there are still areas that are lacking within AD – specifically in the areas of tracking changes, privileged user auditing, and the ability to seamlessly rollback objects that are deleted from the AD infrastructure. These shortcomings can lead to damaging security breaches, business downtime, and loss of employee productivity if not properly addressed.

This white paper explores the most significant privileged user auditing and recovery gaps in AD, and provides best practices guidance on addressing those gaps.

- **Administrators** will benefit from reading this paper by learning how to use solutions to quickly and simply gather and correlate change data while leveraging familiar, native tools.
- **Security and Compliance Officers** will benefit from reading this paper by learning strategies for simplifying identity management and entitlement challenges for the enterprise.
- **Business leaders** will benefit from reading this paper by learning strategies to keep corporate data safe, assess and prioritize risk levels, and quickly report on non-compliance to auditors and the board.
Needs for Auditing and Recovery in Active Directory

Organizations are required to produce ever-growing amounts of information regarding the activities of users and administrators. Driven by compliance or security requirements, this information often covers nearly every aspect of everyday network administration, such as the management of users, groups, desktops, servers, files, folders, applications, and more.

From a management standpoint, it’s important to have the ability to monitor and know what is going on within Active Directory. However, help is needed to provide insights into complex changes that can’t be seen with the naked eye. Every minute spent tracking down a problem is a minute taken away from being productive and making a profit.

Let’s take a look at the core requirements necessary in a comprehensive AD auditing and recovery solution.

Tracking of Changes

Organizations need to know on an event-by-event basis what changes occur within Active Directory. Without this knowledge, it could take hours – or worse, days – to track down what was changed, not to mention trying to recover from the changes or deletions. Every AD administrator needs to have the ability to check manually, as well as be notified immediately, when a change occurs to any aspect of AD.

Often, the consequences of a change to Active Directory are not immediately recognized. Therefore, it’s important to have a continuous log generated of all changes that occur to every aspect of AD. Without this type of auditing, there is scant hope that the change can be discovered and reversed, and production set back to the correct state, in a timely manner.

Entitlement Reporting

Knowing who has access to which resources (so IT can identify potential exposures of sensitive information and intellectual property) is a requirement of AD auditing solutions. Without this capability, IT and security teams can’t be sure that users have access to the resources they need to do their jobs – and only to those resources.

Speed to Recovery

The need to move quickly and precisely when working with Active Directory is essential. When disaster strikes and the AD administrator has a need to fix an issue where an object(s) was modified or deleted, time is of the essence.

The administrator might only have a limited amount of time to discover what was modified or deleted – not to mention the time to recover from the issue. Discovering what was modified or deleted can be expedited with the help of a powerful audit log and reporting tool. Reporting must accurately display the most recent changes so that the administrator can quickly analyze what was altered to fix the problem.

After discovering what was modified or deleted, the administrator must have the tools
and ability to quickly restore the object(s) to the exact configuration before the modification or deletion. The administrator does not have time to reboot a domain controller into a special mode, launch tools that are rarely utilized, and try to unravel syntax that is rarely if ever used except for in these situations.

Uptime (Or, Minimizing the Cost of Downtime)

As far as the Windows AD server environment is concerned, five 9’s (99.999%) high availability is the default requirement. At this level of availability, domain controllers and Active Directory will be down for 5.26 minutes every year, or 25.9 seconds every month. Consider the cost to the business if downtime is extended further.

Granularity of Objects Rolled Back

Active Directory objects can be extraordinarily complex due to the nature of the attributes that are associated with each object. Administrators need to have the full knowledge and confidence that all possible attributes and key functionality is restored, which auditing and reporting aspects should help prove.

The administrator must know exactly what was modified or deleted in order to recover from the issue. This is both a global and granular issue. If an organizational unit containing hundreds of user accounts was deleted, the administrator needs to know every user account that was included in the organizational unit. If a group was modified by removing two other groups and three user accounts, the administrator needs to know exactly which groups and users were removed. Even if a user account property, such as an office number, is changed, this must be known and restored if the attribute is altered incorrectly or the user account is deleted.

Integration of Auditing and Rollback

The need to know everything that changes in Active Directory is essential. At the same time, the need to be able to take a modified or deleted object and restore it quickly is also essential. To have these two systems separated results in delays, inaccuracies, and loss of productivity. A well-managed Active Directory environment will integrate these two concepts into one streamlined interface to deliver fast and accurate rollback and recovery.

What Microsoft Provides

Microsoft has made headway in providing auditing for Active Directory changes and the ability to bring an object back once it has been deleted. Although Microsoft provides both of these features, neither one is a complete solution for the administrator who needs to manage AD. The latest versions of these technologies, while improved, still present limitations and drawbacks with regards to what administrators actually need in order to efficaciously manage Active Directory.
Auditing via Event Viewer Logs

Microsoft has always provided a solution for administrators to track events that occur to the file system and to Active Directory objects. This level of tracking is referred to as “auditing” within the Windows system, and the technology has been available since Active Directory was first released.

The technology is configured in Group Policy and the results are reported in the security log within Event Viewer. There are multiple auditing configurations that can be made to a domain controller in order for the tracking to be initialized. The key auditing configurations that can be set to track changes made within Active Directory include:

- Auditing account management
- Auditing directory service access
- Auditing object access

All of these auditing controls will create entries in the security log within Event Viewer when a change triggers one of the settings that fall under one of the categories. For example, when a user is created, that will be tracked for account management, and when a group membership is listed that will track an entry for object access.

A few limiting factors for this type of auditing include:

- Decentralized storage of the security logs from multiple domain controllers
- Lacking of information within the log entry regarding the old setting
- Inability to recover the object/configuration from the audit log

Recovery via System State

Starting with the initial versions of Active Directory, Microsoft has provided administrators with the ability to back up the entire AD database and all of the essential aspects linked to the AD database using the System State. The System State consists of many aspects of a Windows computer, but when the computer is a domain controller, it also includes the AD directory service and the SYSVOL directory. To back up the System State, the built-in Microsoft backup software, or a third party software tool can be used. System State can be backed-up manually at any time, or via scheduled back up.

When the System State is backed up, it must backup the entire System State, including all of the other aspects (Registry, COM+, etc.), including all of the AD objects that have not changed. For large organizations, this wholesale backup can take an inordinately long time, not to mention filling up terabytes of space. The recovery of the objects that are located in the System State are accessed using the built-in tool of ntdsutil by Microsoft, or third party products. With such a large and cumbersome backup to work with, the efficiency to find what you are looking for and the ability to restore just what you need can be a complicated task, especially if you are relying squarely on the auditing to indicate what was changed and when it was changed.
Recovery via Recycle Bin

Windows Server 2008 R2 Active Directory domains have Recycle Bin to recover deleted objects from the AD database. Windows Server 2012 Active Directory domains took this feature and added a GUI around the Recycle Bin to allow for recovery of deleted objects. The technology does provide the administrator the ability to restore one or more deleted objects, along with all of their properties.

Unfortunately, there are severe limitations with the Active Directory Recycle Bin, which include:

- Time limitations for restore
- No auditing of behavior
- No recovery from changed properties

The Active Directory Recycle Bin also requires that all domain controllers be at least Windows Server 2008 R2, and the forest functional level must be Windows Server 2008 R2 or higher. Finally, the Active Directory Recycle Bin is not enabled by default, and when enabled, can’t be disabled.

Overcoming Native AD Auditing & Recovery Tool Limitations

There are several reasons why using a commercial solution, such as the PowerBroker Auditing & Security Suite, is preferable over the free native tools available from Microsoft.

BeyondTrust PowerBroker Auditing & Security Suite centralizes real-time change auditing for Active Directory, File Systems, Exchange, SQL, and NetApp, restores Active Directory objects or attributes, and helps to establish and enforce entitlements across AD and file systems. Through simpler administration, IT organizations can mitigate the risks of unwanted changes and better understand user activity to meet compliance requirements.

Integration of Auditing and Rollback

Auditing and rollback capabilities of all Active Directory activity are absolutely essential for the administrator to effectively manage the AD enterprise. PowerBroker Auditor for Active Directory is the only solution that provides this tight integration to enable administrators the ability to see the audit log and rollback an object in the same interface.

This functionality is paramount for daily Active Directory administration as there is little time to sift through an audit log to find where one or more objects were deleted, only to try and match the same entry in some form of recovery tool. PowerBroker Auditor for Active Directory provides real-time visibility into the changes that occur to any object within Active Directory and allows immediate rollback of these objects and/or properties from the same console.
Rollback of Objects Down to Attribute Level

PowerBroker Auditor for Active Directory provides ultimate control over objects, whether the object was deleted or modified. The continuous tracking of all activities in the AD database provides a clear and concise look at what exactly was changed and who made the changes. The database also provides information regarding what the old attribute level setting was and what the new setting currently is.

This provides the administrator with precision control over which object and/or attribute will be rolled back. If a set of user accounts were deleted, but only a few of the user accounts were deleted in error, there is no need to restore all of them, just those that were deleted in
error. Likewise, if multiple attributes were changed and just one or two were set in error, there is no need to rollback attributes that are set correctly, only those attributes that were changed in error.

Real-time Change Management

PowerBroker Auditor for Active Directory is a unique solution providing real-time change management. This means that no matter when an object is deleted or modified, PowerBroker Auditor for Active Directory has logged that change to the object. PowerBroker Auditor for Active Directory tracks all changes to Active Directory objects, including organizational units, user accounts, group accounts, Group Policy Objects, and more.

With real-time management, an administrator now has the ability to quickly find a deleted or modified object in the audit log and, from the same entry, rollback all or part of the object to fix the errant modification. This real-time management capability reduces the time required to find the entry in two different logs (audit and recovery) and allows for granular control over what is to be restored.

Reporting for Changes Over Time

PowerBroker Auditor for Active Directory reporting provides administrators, security professionals, and auditors with full visibility into an object’s history. These reports can display all aspects of the object, including modifications, deletions, and rollbacks. The reports can also be customized to show specific object deletions and/or modifications over a set period of time, to support easier change management controls over Active Directory.
Reporting for Privileged Access Changes Over Time

**PowerBroker Privilege Explorer** for AD and File Systems offers a centralized view of enterprise access, ensuring that the right people have access to the right resources, minimizing the risk of data theft, security breaches or system attacks. Reporting capabilities deliver the documentation and data needed to identify violations, and prove compliance to auditors and managers. Advanced filtering allows you to quickly target access reports to specific resources, users, groups, permissions and dates.

Integration with the PowerBroker Auditing & Security Suite enables administrators to instantly drill down on any privilege to find out how access to a resource was granted — and then click to roll back the change to return to the previous state with the appropriate access privileges set.
# Checklist of Required Functionality

When evaluating AD auditing and recovery solutions, consider the following capabilities:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Function</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-Time, Centralized Auditing and Alerting</td>
<td>Audit, alert, &amp; report on all changes made in Active Directory, File Systems (including NetApp), Exchange, &amp; SQL in real-time – including before and after values – without relying on native event logs.</td>
<td>Helps to quickly identify changes that can impact the security and compliance of the environment, speeding time to resolution.</td>
</tr>
<tr>
<td>Compliance Reporting</td>
<td>Capture all change activity in a centralized auditing database.</td>
<td>Accelerates compliance with regulations such as HIPAA, SOX, PCI, GLBA, and more by providing greater insight into audit data in plain language.</td>
</tr>
<tr>
<td>Continuous Backup</td>
<td>Store every object change in a continuous change log.</td>
<td>Provides complete object backup and recovery to ensure uninterrupted business operations.</td>
</tr>
<tr>
<td>Integration of Audit and Recovery</td>
<td>Recover deleted or changed Group Policy and directory objects, a full tree, a portion of the directory, or individual attributes with a single click.</td>
<td>Helps to maintain business continuity and avoid productivity and revenue losses caused by disasters or accidental deletions.</td>
</tr>
<tr>
<td>No Requirement for Native Auditing</td>
<td>Does not require any GPO changes or native System Access Control Lists to be managed or defined. IT can leverage native auditing using Microsoft ACS along with PowerBroker to narrow the search for which audit log contains the needed information.</td>
<td>Makes the process to find and remediate a change much quicker than using native auditing alone.</td>
</tr>
<tr>
<td>Integration with Native Management Tools</td>
<td>Single-click access to item and user histories via integration with native management tools, such as Active Directory Users and Computers, Sites, and Services, ADSI Edit, and others.</td>
<td>Reduces cost of ownership and simplify administration by enabling IT teams to leverage existing solutions.</td>
</tr>
<tr>
<td>Agentless and Single-Agent Options</td>
<td>All modules that require an agent use a common footprint.</td>
<td>Mitigates performance impacts on domain controllers or other servers.</td>
</tr>
<tr>
<td>Interactive Analysis Reports</td>
<td>Provide insight to help make better decisions on share and drive access.</td>
<td>Reduces the administration of shares and drives by getting the intelligence on data access into the hands of data owners.</td>
</tr>
<tr>
<td>NetApp Auditing</td>
<td>Audit, report, and alert on all changes including file create, delete, update, and modify.</td>
<td>Ensure the security, compliance and control of NetApp files and folders.</td>
</tr>
<tr>
<td>Non-Owner Mailbox Access Reporting</td>
<td>Audit and report on non-owner mailbox activity.</td>
<td>Prevents inappropriate access to sensitive information and mitigates the risk of possible data loss or security breaches.</td>
</tr>
<tr>
<td>SQL Server Auditing</td>
<td>Monitor and review privileged changes to SQL server configuration, security, and database structure.</td>
<td>Helps to achieve tighter security and audit procedures over access to business-critical data.</td>
</tr>
<tr>
<td>Access and Permission Reporting</td>
<td>Reveal rights history for users, and examines access changes to resources through centralized view of enterprise access.</td>
<td>Ensures that the right people have access to the right resources, minimizing the risk of data theft, security breaches or system attacks.</td>
</tr>
</tbody>
</table>
Conclusion

Every organization needs management tools that enable seamless control over all aspects of their Active Directory environment. Uptime is critical for every organization, and every minute that AD is not functioning properly could mean disruption to business operations and financial loss. Administrators need reliable tools that can provide them with insight into when and where Active Directory was changed, what objects were modified or deleted, and who made the change so that they can take quick and efficient action if the change is in error. Consequently, an audit log and the ability to granularly rollback objects and their attributes, are vital capabilities. Ideally, these two functions will be seamlessly integrated within a single solution so administrators are not spending cycles trying to match an entry from one tool with an entry in another tool in hopes to find the correct matching entry.

PowerBroker Auditing & Security Suite provides this integration of real-time auditing of changes to all Active Directory objects, along with the ability to rollback any changed or deleted object efficiently and with tremendous precision. Without PowerBroker Auditor, there is no guarantee that all modified Active Directory objects can be tracked, discovered, or corrected in a timely manner.

Appendix: The PowerBroker Auditing & Security Suite

BeyondTrust PowerBroker Auditor for Active Directory is part of the BeyondTrust PowerBroker Auditing & Security Suite which centralizes real-time change auditing for Active Directory, File Systems, Exchange, SQL, and NetApp; restores Active Directory objects or attributes, and helps to establish and enforce entitlements across AD and file systems. Through simpler administration, IT organizations can mitigate the risks of unwanted changes and better understand user activity to meet compliance requirements.

Audit and Alert

BeyondTrust PowerBroker Auditor & Security Suite helps to achieve requirements for PCI, SOX, HIPAA, and regulations by auditing and alerting to Active Directory configuration and GPO changes, and changes to File Systems, Exchange, NetApp, and SQL configurations. Pinpoint changes that introduce security risks, jeopardize compliance, or reduce operational efficiency by understanding who performed each change, what changed (including pre/post values), when the change occurred and where the change was made – all in plain language.

Recover and Roll Back

PowerBroker stores every object change in a continuous change log, enabling IT to instantly roll back unwanted changes or just what’s needed to any previous state, right up to the point of the error. Recover the full tree, a portion of the directory, selected objects, or individual attributes, avoiding end user disruption or affecting other parts of the Active Directory system. Restoring from the recycle bin without having to extract the backup provides continuous data protection and makes recovery faster and easier. The solution's centralized database enables both auditing and recovery, delivering a broader set of capabilities than native AD auditing – and without the operational impacts.

Discover and Enforce

PowerBroker offers a centralized view of access and privileges so administrators know who has access to which resources and can see the exposure of sensitive information and intellectual property. With PowerBroker, IT can ensure that users have access to the resources they need to do their jobs, and only those resources.

Extend and Enhance

PowerBroker Auditing & Security Suite audits, alerts, and reports on all changes made in Active Directory, Exchange, File Systems, SQL, and NetApp environments via a centralized real-time web console, without the need for native audit logs. This centralized dashboard in distributed enterprise environments simplifies administration and reduces the number of tools administrators have to manage.
BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.