WHITE PAPER

beyondtrust®

Beyond Traditional Security

Take Back Control of Your Active Directory Auditing

Table of Contents

An Intro to Active Directory 3
Needs for Auditing and Reporting in Today's Active Directory Environment 3
- Up Time 3
- Speed to Recover and Rollback 3
- Granularity of Object(s) Rolled Back 4
- Tracking of changes 4
- Integration of Auditing and Rollback 4

What Microsoft Provides 4
- Auditing Via Event Viewer Logs 4
- Recovery via system state 5
- Recovery via Recycle Bin 5

What PowerBroker Auditor for AD Provides 5
- Integration of Auditing and Rollback 5
- Rollback of Objects Down to Attribute Level 6
- Real Time Change Management 6
- Reports For Changes Over Time 6

Conclusion 6
About BeyondTrust 7

 © 2013. BeyondTrust Software, Inc.

An Intro to Active Directory

Active Directory is a well-known, highly used, highly reliable, and powerful network operating system. Since the introduction of Active Directory by Microsoft in 2000, organizations around the world have implemented Active Directory to be the standard for corporate, government, and military centralized management of the Windows infrastructure. We have seen revolutionary changes to Active Directory which have made the management of all aspects of the environment easier and more reliable. We have seen the introduction of new tools and features that have expanded our minds into areas that we never thought were possible. However, there are still areas that are lacking within our Active Directory installations and suite of tools which seem to be some of the most important aspects that we need. I am referring to the concepts of tracking changes, the ability to audit Active Directory, and the ability to seamlessly rollback objects that are deleted from the Active Directory infrastructure.

Needs for Auditing and Reporting in Today's Active Directory Environment

Whether we like it or not, our organizations are being required to produce more information regarding the activities that are going on than ever before. We must provide information about nearly every aspect of everyday network administration such as management of users, groups, desktops, servers, files, folders, applications, and much more. These requirements are being driven by internal and external mandates and compliance regulations, as well as, the overall security umbrella that is now blanketing our corporations.

From a management standpoint, it's important to have the ability to monitor and know what is going on inside Active Directory. Doing this through the use of reports and auditing is imperative because it reduces resources and in turn allows us to do more with less. We need to have "help" to aide us with insights into complex areas that we can't see with the naked eye and must have knowledge about in order to maintain a stable and standardized system. Every minute that we are tracking down a problem and trying to solve that problem is a minute that we are taking away from being productive and making a profit.

UP TIME

Everyone in the IT business knows that uptime is essential. We are geared and trained to solve problems quickly and even take measures to avoid these problems. We need uptime and in many cases have to meet very high standards of five 9's (99.999%) to assure that we have high availability for our Windows Active Directory and server environment.

This level of high availability puts the Active Directory environment into a very good state for providing services to the corporation. At this level of availability, the domain controllers and Active Directory will only be down for 5.26 minutes every year, which is equivalent to only 25.9 seconds every month. This is the type of uptime that all IT staffs are looking for from their Active Directory infrastructure.

SPEED TO RECOVER AND ROLLBACK

The need to move quickly and precisely when working with Active Directory is essential for the network administrator. When disaster strikes and the Active Directory administrator has a need to fix an issue where an object or objects were 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 by an excellent audit log and reporting tool. The report must have the ability to quickly and 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 used, and try to unravel syntax that is rarely if ever

 © 2013. BeyondTrust Software, Inc.

used except for in these situations.

GRANULARITY OF OBJECT(S) ROLLED BACK

Active Directory objects can be quite complex due to the nature of the attributes that are associated with the object. If even one attribute is omitted, then other network applications and systems could fail which rely on the attribute that is not rolled back when the object is recovered. Administrators need to have the full knowledge and confidence that all possible attributes and key functionality is restored, which the 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 a global and granular issue all in one. If an organizational unit containing hundreds of user accounts were deleted, the administrator needs to know every user account that was included in the organizational unit. If a group was modified by removing 2 other groups and 3 user accounts, the administrator needs to know exactly which groups and users were removed. Even if a user account property such as office number is changed, this must be known and restored if the attribute is altered incorrectly or the user account is deleted.

TRACKING OF CHANGES

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

Often when a change occurs to Active Directory the consequences are not noticed immediately. Therefore, there must be a continuous log generated of all changes that occur to every aspect of Active Directory. Without this type of auditing, there is little hope that the change can be discovered, the errant change recovered, and production set back to the correct state in an expedited manner.

INTEGRATION OF AUDITING AND ROLLBACK

The need to know everything that changes in the Active Directory is essential. 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 causes delays, inaccuracies, and loss of productivity. A well-managed Active Directory environment must integrate these two concepts into one interface to expedite and solidify the correctness of the change and recovery of the object(s) back into the production Active Directory environment.

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 that needs to manage Active Directory. The issues have always relied in the ease and completeness of the solutions. The latest versions of these technologies are better than ever, but still provide some limitations and drawbacks compared to what administrators need in order to manage Active Directory efficiently and precisely.

AUDITING VIA EVENT VIEWER LOGS

Microsoft has always provided a solution for administrators to track events that occur to the file system and to the 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:

 © 2013. BeyondTrust Software, Inc.

- 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

From the initial versions of Active Directory Microsoft has provided administrators with the ability to backup the entire Active Directory database and all of the essential aspects linked to the Active Directory 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 Active Directory directory service and the SYSVOL directory. To backup the System State the built-in Microsoft backup software or a third party software tool can be used. It can backed-up manually at any time or scheduled to be backed up.

Regardless, 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 Active Directory objects that have not changed. For large organizations this backup can take a very long time, not to mention taking up TB 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 simply 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 a new feature, Recycle Bin, to recover from deleted objects from the Active Directory database. Windows Server 2012 Active Directory domains take this feature and add 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, and 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.

What PowerBroker Auditor for Active Directory Provides

INTEGRATION OF AUDITING AND ROLLBACK

It is obvious at this point that both auditing and rollback of all Active Directory behavior is essential for the administrator

 © 2013. BeyondTrust Software, Inc.

to effectively manage the Active Directory 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 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 views into the changes that occur to any object within Active Directory and 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 Active Directory 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 and only a few user accounts were deleted in error, there is no need to restore all of them, just those that were deleted in error. 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.

REPORTS FOR CHANGES OVER TIME

PowerBroker Auditor for Active Directory provides reports to allow administrators, security professionals, and auditors to see the history of an object. These reports can show 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 allow for easier change management controls over Active Directory.

Conclusion

Every organization needs to have management tools that allow them seamless control over all aspects of their Active Directory environment. Uptime is extremely important for every organization and every minute that Active Directory is not functioning properly could cause a financial loss. Administrators need tools that can provide them with insight into when Active Directory is changed, objects modified or deleted, so they can take quick and efficient action if the change is in error. Therefore an audit log and the ability to granularly rollback objects and their attributes is vital. Ideally, these two functions need to be integrated into a single tool, so that the administrator is 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 Auditor for Active Directory provides this integration of realtime auditing of changes to all Active Directory objects, along with the ability to rollback any changed or deleted object efficiently and with great precision. Without PowerBroker Auditor for Active Directory, there is no guarantee that all modified Active Directory objects can be tracked, discovered, or

 © 2013. BeyondTrust Software, Inc.

corrected in a timely manner.

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit **beyondtrust.com**.

CONTACT INFO

NORTH AMERICAN SALES
1.800.234.9072
sales@beyondtrust.com

EMEA SALES
Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS
550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US
Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

 © 2013. BeyondTrust Software, Inc.