SolutionScope™

Active Directory Change Auditing

concentrated technology
maximum knowledge • minimum time

Executive Overview

Change auditing has become an important activity in business networks using Microsoft Active Directory. In general, Active Directory's native auditing features are insufficient to adequately support business needs such as troubleshooting, compliance enforcement, security auditing, and change management. These inadequacies in Windows' native auditing are evidenced by the robust third-party market that has grown to fill this functional gap. The products and services of that third-party market offer customers a variety of choices and approaches.

For this analysis, Concentrated Technology surveyed 1,214 Active Directory administrators and front-line IT managers. We interviewed 18 survey respondents for follow-up questions. We also interviewed four Independent Software Vendors (ISVs) who currently offer products in this space, comparing their products' feature sets to the capabilities required by our survey respondents and interviewees. Finally, a small focus group was introduced to each of the products and asked for their feedback.

We reviewed shipping versions of all products as of January 2011. All data and statements in this analysis are believed to be accurate as of January 2011.

Contents

The Auditing Features Companies Need

Respondents to our survey identified an almost uniform set of features they felt were missing in the native Windows and Active Directory auditing architecture. Many of these features have been driven, in recent years, by the need for organizations to comply with external industry and legislative requirements. In the US, for example, legislation such as HIPAA, Sarbanes-Oxley, GLB, and so on were commonly cited, along with industry requirements such as PCI DSS. The commonly-requested features are as follows.

Centralized, Secure Audit Trail

Windows' native auditing is neither centralized nor particularly secure, since administrators can clear the log at any time. Recent versions of Windows Server now include the ability to forward events to a centralized event log; however, the event forwarding system works on a less-than-realtime basis, and does not adequately fulfill the requirement of a tamperproof or tamper-evident event repository. The native forwarding forwards events to a standard event log, rather than a true database, which means the consolidated log still has many of the other weaknesses of the native log system, which we discuss next.

Searching, Filtering, and Reporting

Windows has no built-in reporting mechanism in its event logs, and provides fairly basic filtering and searching capabilities. Because the native event logs aren't stored in a relational database, extensive searching can also be time-consuming. Reporting was particularly cited as a weakness, since constructing the reports needed by security auditors is a time-consuming, almost entirely-manual task. Robust reporting is an absolute necessity, including the ability to automatically generate and deliver reports on a subscription basis.

Event Translation

Windows' native events tend to include detailed technical data which is not always meaningful to an auditor or IT administrator. Many of our respondents indicated a need for more meaningful, "plain-English" events. Events that include "before and after" information about changes was also a request; while this has been partially provided in Windows Server 2008 and later for many Active Directory events, more complete coverage of this feature is desired.

Alerting

Windows includes features for automatically generating alerts and notifications for specified events, such as changes to critical groups or sensitive directory objects. This kind of alerting was identified as a requirement by most respondents. A weakness in Windows' native alerting capabilities, however, is the dependence on specific event characteristics. For example, defining an alert for changes to a specific Active Directory group is fairly complicated given the alert criteria that must be specified. Alerts are also not centralized (since the logs themselves aren't), which is a significant weakness: In order to effective monitor changes to a group (for example), that alert must be configured on *every domain controller* in the environment.

Backup, Recovery, and Rollback

While not specifically tied to change auditing, the ability to undo or roll back unwanted changes was cited as a highly-desirable feature by respondents. Rollback features imply backup and recovery capabilities. Windows includes basic native backup and recovery features, and Windows Server 2008 R2 introduces an optional *Active Directory Recycle Bin* feature. However, these features are primarily designed at restoring single objects or groups of objects. They are not intended for use in undoing attribute-level object changes.

Archival

Windows provides poor native capabilities for long-term archival of event logs, although many organizations are now required (or desire) to maintain logs for up to 7 years. Windows simply permits you to manually save the log files; scripting is required to automate this process, but it doesn't provide a true archiving solution.

Separation of Duties

Most security and compliance policies mandate that auditing systems offer separation of duties functionality. Auditors must be able to access the system in a read-only fashion, and administrators who manage the auditing system must be prevented from tampering with the audit trail. Windows does not provide this separation in its native event logging capabilities.

Additional Systems to be Audited

Active Directory is not the only system that needs to be audited within organizations. While not within the scope of this analysis, respondents also indicated a need to audit other Microsoft-based systems, including Exchange Server, SharePoint Server, and SQL Server. Non-Microsoft file storage systems from EMC and NetApp were commonly cited as needing auditing. Where appropriate, we have noted vendors and solutions who offer auditing solutions that include, or that can be extended to include, auditing for these other products and technologies.

Architectural Notes for Third-Party Solutions

Third-party change auditing solutions must typically make two key architectural decisions. Each of these decisions has both upsides and downsides.

First, solutions must gather data from Active Directory. This can be done through an agentless system, or by using locally-installed agents on domain controllers. Agents provide better information-gathering, performance, and often enable more robust features, but require deployment and ongoing maintenance. Agentless systems can create less overall impact on the environment (although they do not necessarily offer better performance), but typically offer less functionality. The solutions we evaluated for this analysis all offer an agent-based approach, although some also offer an agentless deployment option that includes reduced functionality.

Second, solutions must decide where they will gather data. The main choices are to either rely on the native event logs, to connect directly to Active Directory Application Programming Interfaces (APIs), or a combination of the two. The API approach often offers better performance and an increased amount of information. If well-implemented, it can also offer the option to disable native logging capabilities (which are not renowned for their high performance and low impact).

Business Concerns Around ISVs

While many organizations are willing to consider third-party software tools to fill the gap left by Windows' native features, organizations are increasingly concerned about the stability and robustness of the ISVs they choose to deal with. Our respondents indicated a desire to work with ISVs that have a robust and responsive support organization. Managerial-level respondents indicated an additional desire to work with vendors who show signs of financial and organizational stability, suggesting that they will be able to weather economic downturns and remain in business to continue supporting their products in the long-term.

Product licensing is also a concern. In most cases, auditing solutions are licensed either *per enabled directory account* or *per heartbeat;* the latter model requires one license per human being in the environment, without regard to the number of user accounts in the directory, meaning service accounts and other accounts not tied to a human being are not required to be licensed.

Blackbird Group
Blackbird Management Suite

Blackbird Group has been in business since 2002, and has offered an Active Directory auditing solution since 2009. Approximately 500 customers have deployed the solution to date, with an average customer size of 3,000-5,000 users with the largest customer having more than 5 million users. Blackbird Group employs approximately 30 people worldwide, and claims to have a strong financial position with no significant debt. The company is privately held.

Blackbird Management Suite is an internally-developed suite of applications, including Blackbird Auditor for Active Directory, Blackbird Recovery for Active Directory, Blackbird Protector, and Blackbird Privilege Explorer. The products are licensed per heartbeat.

Blackbird Management Suite relies on locally-installed agents connecting to native Windows APIs instead of the event logs, which is a common approach in this product category. The product's management console provides a means of centrally deploying or updating the agent, which helps to reduce the maintenance overhead often associated with the agent-based approach.

Events are forwarded to a secured SQL Server database in near-realtime (also common in this product category), providing a tamper-evident audit trail and the opportunity for separation of duties. Blackbird also supports database encryption.

Archiving is accomplished through SQL Server database archiving. Because the product is fairly new, no customers are currently retaining more than a couple of years' worth of data, so the efficacy of Blackbird's archival approach remains to be seen over the long term. While SQL Server can absolutely be relied upon to manage enormous databases in the multi-terabyte range, conducting backup and restore operations of very large databases are operationally challenging.

Real-time alerts are provided through e-mail.

The product provides full change rollback capability, and does so in a way that is better-integrated and more intuitive than most products in this category. When viewing the change log, a "rollback" button is available for each change listed. Overall, we feel that the product's relative newness to the market gives it a "second comer advantage," meaning the company has had the opportunity to look at existing products and design improvements to things like the user interface. The rollback functionality is an excellent example of this, as it feels more integrated and accessible than is often seen elsewhere.

Blackbird currently uses a proprietary reporting mechanism, but states that reporting will be moved to SQL Server Reporting Services (SSRS) in the future, an increasingly-common approach and one we recommend. SSRS provides automated report generation and subscription delivery, as well as Web-based report delivery. Blackbird currently bundles 74 predefined reports and supports ad-hoc report creation. Reporting is integrated into the main console, enabling report generation through right-click context menus on directory objects. Blackbird also currently supports scheduled report generation and delivery in PDF or XML formats. Note: The Privilege Explorer component already utilizes SSRS for reporting; this component is focused on permissions management and was not reviewed for this analysis.

Blackbird provides an MMC snap-in for management, but also integrates functionality into native Microsoft snap-ins, including Active Directory Users and Computers, GPMC, ADSIEdit, and so forth.

Blackbird Management Suite has had one major release and two minor releases in the past eighteen months, with five patch releases that also included new functionality. This frequency suggests a product that is fairly stable and mature.

Blackbird does not currently support direct integration with standard monitoring frameworks such as System Center Operations Manager, OpenView, Tivoli, etc. The company notes that its email alerts can be used to funnel information into those systems, and they are planning both SNMP support and Operations Manager management packs for future releases.

The company offers similar auditing support for the Windows file system, and is in the process of developing components to cover SharePoint and Exchange.

Analysis

We believe the Blackbird Management Suite reflects a strong, clear vision for the market segment. Because of its relative newness in the market, the company has been able to create a product that has a modern user interface, which integrates tightly with native Windows consoles, and which offers deeply-integrated functionality across the product's feature set.

The Blackbird Management Suite product is competitive from an Active Directory perspective. It also has a good roadmap. The Management Suite's various components look and feel like a single, integrated product, rather than separate products that have specific integration points. Cross-market analysis, however, suggests that its feature set lags behind the competition in other areas, such as support for SQL Server, Exchange, SharePoint, and so on.

NetWrix
Active Directory Change Reporter

NetWrix has been in business since 2006, offering their first Active Directory change auditing solution in 2007. The product is in use by approximately 600 customers. An average-sized deployment is 1,000 to 2,000 directory users across 5-10 domain controllers in 2-3 sites; the largest deployment is 60,000 users, 300 domain controllers, and 30 sites.

NetWrix employs approximately 70 people and is privately-held. No financial information is available, but the company appears to be stable and well-funded. Existing customers state that they receive a good level of technical support when needed.

Active Directory Change Reporter can be installed separately, but is also available as an integrated part of a larger Change Reporter Suite. The complete Suite includes a Change Reporter module for Exchange Server, Group Policy, Fie servers, SQL Server, VMware, System Center Virtual Machine Manager, SharePoint Server, Server Configuration, and Network Infrastructure. The products are all developed in-house, and are licensed per enabled Active Directory account.

NetWrix offers both an agent-based and agentless infrastructure. Agents are recommended for distributed deployments of more than one AD site due to the agent's ability to compress network traffic. The product uses a combination of techniques to collect data, including native event logs as well as native APIs. This is an unusual approach in the market segment, which generally relies solely on native APIs and requires an agent-based deployment.

The company states that the product scales up to 100,000 directory accounts and 500 domain controllers. Information is forwarded in near-real-time to the SQL Server database. The product does not currently include functionality required to make the audit trail tamperproof or tamper-evident; however, the company does include that functionality in its product roadmap. Separation of duties is provided, and individual reports can have customized permissions governing who can view the information contained in each.

The company has a detailed strategy for ensuring that administrators cannot "fool" the audit trail. We feel this strategy can make the existing database capable of being tamper-evident, but only when proper SQL Server permissions are applied to the storage database and the long-term archival files. That strategy includes capturing all changes via DirSync monitoring, automatic restarting of their monitoring agent, among other techniques.

NetWrix offers one of the most well thought-out long-term data archival strategies, using a two-tiered system that utilizes SQL Server for online reporting, and file-based compressed storage for long-term storage. The company states that the product can accommodate "years' worth" of data.

Real-time alerting is provided both via e-mail and SMS text messages.

The product supports rollback of changes, down to individual attribute-level changes.

Reporting is based on SQL Server Reporting Services (SSRS) with approximately 50 built-in reports and support for ad-hoc reporting. Scheduled report generation and delivery via e-mail are included for any pre-defined or custom report.

NetWrix utilizes a proprietary MMC snap-in to manage the product, and utilizes the SSRS Web interface for reporting.

In the past 18 months, NetWrix has issued one major release and seven minor updates to the product. We feel that this falls within the realm of an operationally-stable product, and indicates active development and improvement of the product.

NetWrix provides direct integration with System Center Operations Manager, but not with other non-Microsoft enterprise management frameworks.

We feel that the NetWrix product provides a solid foundation of functionality. Through the other Change Reporter modules available in their Change Reporter Suite, NetWrix offers what is perhaps the broadest reach among those in the comparison, including network infrastructure, server configuration, and VMware vSphere, among other technologies.

The ability to purchase only needed modules will be appreciated by companies, as they're not required to pay for functionality they won't use.

Change Reporter's functionality is straightforward, and the user interface is intuitive and easy to operate. However, we feel some features could be better integrated. One example of this relates to the product's change rollback functionality, which feels somewhat more difficult to use with other products in this category. We don't feel this difference is a major product drawback, primarily because the UI still works well enough that administrators will quickly become familiar and comfortable with it.

Quest Software ChangeAuditor for Active Directory and ChangeAuditor for LDAP

Quest Software was formed in 1987, and originally released ChangeAuditor in 2004. ChangeAuditor was originally released by NetPro Computing, which Quest acquired *in toto* in 2008. ChangeAuditor is used by approximately 2,000 customers, with an average environment of 2,000 to 10,000 Active Directory users. The largest deployment is in a one million user environment. The product is license per enabled user.

Quest employs approximately 3,400 people worldwide, and is a publicly-traded company (NASDAQ: QSFT). As such, more information is available about the company's size, revenue, and financial stability than for privately-held companies: Quest has $493 million in cash investments, an R&D budget that is approximately 18.5% of revenue, and more than 100,000 customers worldwide – including 87% of the Fortune 500. The company maintains more than 60 offices in 23 countries, with 2010 revenue of $767 million.

ChangeAuditor relies on an agent-based architecture to connect directly to native Windows APIs, and does not rely on native event logs. This is by far the more common approach in the market segment. A complementary Quest product, InTrust, provides log aggregation of native event logs. InTrust also offers a twist to Quest's long-term archival strategy: Natively, ChangeAuditor can be configured to purge noise events and archive data to another SQL Server database. The company states that most customers maintain an annual archive database. With InTrust, ChangeAuditor events can be archived using InTrust's more-robust archival system.

The company states that ChangeAuditor will scale to any size environment, because any number of servers can be used to load balance the volume of events in the environment. Events are forwarded in near-realtime to a SQL Server database that can be independently secured to provide tamper-evident or tamperproof storage. The product supports separation of duties.

Realtime alerts are provided through e-mail. The collection agent also sends an alert when it is stopped, helping to prevent administrators from maliciously stopping the agent to cover their activity. Proper permission assignment on the agent service can further prevent administrative tampering.

ChangeAuditor does not provide rollback capabilities for unwanted changes. We regard this as a potentially-significant omission. Products in this market segment are increasingly using the audit trail as a form of backup, and offering rollback capabilities at the directory object attribute level. Other Quest products provide this kind of backup and recovery but do not integrate it with the ChangeAuditor log, disallowing the ability to click a button to roll a change back.

ChangeAuditor offers one of the largest built-in report libraries, featuring more than 700 built-in reports. Ad-hoc or custom reports are also provided, and reporting is based on SQL Server Reporting Services (SSRS), providing automated report generation and delivery. Reports can be delivered via e-mail, to a network share, or to a SharePoint site.

ChangeAuditor is managed through a proprietary console, which can also be used to manage the broad array of ChangeAuditor modules. Those modules include auditing for Windows file servers, Exchange Server, SQL Server, SharePoint Server, and both NetApp and EMC file servers. The console provides central control for deploying and updating agents installed on domain controllers.

Quest has issued four patches or updates to ChangeAuditor for Active Directory in the past eighteen months, indicating a stable product that is under active development.

ChangeAuditor is one of the oldest products in this market segment, and shows an expected level of maturity. NetPro (and now Quest) have been slow to expand ChangeAuditor's breadth, only recently adding EMC and NetApp file servers to the list of auditable technologies.

Analysis

We regard the lack of rollback capabilities as significant, and encourage evaluators to consider their need for such a feature. Even if organizations have an existing backup and recovery solution that supports granular, attribute-level recovery, having that ability integrated with the change log can streamline numerous processes and provide the opportunity for automated remediation.

ScriptLogic
Active Administrator

ScriptLogic is a wholly-owned subsidiary of Quest Software; we refer readers to this analysis' section on Quest ChangeAuditor for Active Directory for details regarding the company. ScriptLogic itself has been in business since 2001, and acquired Small Wonders software in 2003. Small Wonders originally produced Active Administrator, and ScriptLogic marketed the product well prior to its own acquisition by Quest. ScriptLogic has approximately 200 full-time employees.

Active Administrator is in use by approximately 2,000 customers, with an average-sized deployment at around 1,500 users. The largest deployment is 300,000 users with several hundred domain controllers.

Active Administrator is unique in this product category in that it is not solely a change auditing product, but rather a centralized Active Directory administration product intended to replace Microsoft's native management tools. The product is not modularized. It is a single, integrated product sold for a single price. Thus, acquiring its auditing capabilities means acquiring its management capabilities as well. This fact makes difficult an equivalent comparison based solely on price.

The product is licensed per enabled user account, and can be restricted to manage specific organizational units (OUs). When restricted in that fashion, it is only licensed per enabled user account in the managed OU. This approach allows larger companies to delegate permission over specific OUs to departments or subdivisions, and to have those departments or subdivisions use Active Administrator only for their part of the directory.

Active Administrator gathers information from the native Windows event logs using an agent-based architecture. Because it is not accessing Windows APIs, the agent does not need to reside on the domain controller. It can instead reside on another machine that has connectivity to the DC. This approach means that Active Administrator will have somewhat less-detailed auditing information than a product which connects directly to the native APIs. Events are forwarded from the log in near-real-time,. As with other products in this category, agent services can be permissioned to prevent administrative tampering. Active Administrator's agent can be configured to send an alert, run a batch file to re-start the service, and so on as further protective measures.

Separation of duties can be provided via a separate set of security configurations to the product's SQL Server database. Active Administrator does not provide any additional layer of separation atop this functionality.

Events are aggregated to a SQL Server database, which customers can secure to provide tamperproof storage. The product does not have an integrated archival system, and only permits customers to purge older data on demand.

The product provides real-time alerts, but does not provide an integrated means of rolling back changes.

Active Administrator uses a proprietary reporting engine, with numerous built-in reports. Reports can be scheduled for generation and delivery in a variety of formats, including PDF, TXT, HTML, RTF, XLS, CSV, or even as images.

The product uses its own console, as its primary goal is to replace the various native consoles provided by Microsoft. A separate console is provided to manage the deployment and updating of agents.

ScriptLogic released one major version, one minor update, and two hotfixes in the past eighteen months. This is within the scope of a product that is mature, operationally stable, yet still under active support and development.

No integration is provided for enterprise management frameworks such as OpenView or Tivoli.

Analysis

Unlike the other products reviewed, Active Administrator is intended to fulfill a wide range of Active Directory management tasks. It is marketed to small- and medium-sized businesses, whereas the other products also scale to enterprise levels. Active Administrator can be deployed as a departmental solution within a larger company, where the other auditing products would typically be deployed organization-wide.

According to our focus group, many companies in Active Administrator's target audience are less concerned about regulatory compliance than they are having a breadth of administrative features, making certain auditing features less of a priority for those environments. In all, our research suggests that Active Administrator offers a good mix of functionality for its intended audience, for those organizations who don't require more-robust auditing features, and also want a more integrated, all-in-one Active Directory management solution.

Conclusion

Of the three auditing-only products, we feel Blackbird Management Suite exhibits the most-developed long-term vision. The structure of the product and the tight integration of its features could eventually make the company a market leader.

As yet, however, that vision is only partially realized. Our focus group responded enthusiastically to the product's user interface and operational patterns. That said, rare is the company who requires only Active Directory and file system auditing, without the broader needs of SQL Server, Exchange, SharePoint, and so forth. As Blackbird extends its reach, we feel Blackbird Management Suite can become a strong contender in any auditing solution evaluation.

NetWrix' product vision for Change Reporter is also strong and well-developed., NetWrix has developed a product suite that offers the broadest product and technology coverage. Our focus group felt that NetWrix' user interface and integration could use some fine-tuning, particularly in improving its rollback functionality integration with the actual change log. The option to deploy the product without agents is compelling, although we think most organizations will benefit more from the agent-based approach.

Quest has a market share leader in ChangeAuditor. The company has built good coverage beyond Active Directory, although not as broad as NetWrix. The maturity and stability of ChangeAuditor is a significant positive factor, as is Quest's size and financial stability.

We believe ChangeAuditor currently reflects the least-developed product vision for the three auditing-only products, as it lacks in key functional areas available with the other products reviewed. Within the product's vision, however, ChangeAuditor is arguably one of the best-realized implementations, with strong reporting capabilities, a solid user interface, and deep functionality. Our focus group had numerous positive comments about the user interface and breadth of available reports. Functional weaknesses in ChangeAuditor – such as its lack of distinct archival capabilities or inability to roll back changes – can be supplemented with other Quest products, although without an integrated experience.

We should point out, however, that members of our focus group representing enterprise-class organizations preferred ChangeAuditor's single focus. They stated that their needs include a separation of duties that made ChangeAuditor's auditing-only focus – with no functionality for things like rolling back changes – more desirable.

We feel that all three of these products deserve a place in an auditing solution evaluation. All take a unique approach to the problem, meaning some will appeal more strongly to some organizations than others. All three companies compete strongly, meaning price will also become a strong factor in any final decision. We did not review pricing with any of the companies included in this analysis.

The fourth product, ScriptLogic Active Administrator, is unique among the others. It attempts to close the gap on numerous native Windows shortcomings and doesn't limit itself to auditing alone. It, however, does not provide best-of-market auditing functionality. It does provide a level of functionality that is well-suited to its intended audience, along with a wealth of other capabilities that its intended audience will find compelling. We recommend including Active Administrator in evaluations within organizations who are looking for an all-in-one administrative solution of which auditing is one requirement amongst many, and where higher-level, more-robust auditing is less critical. Small- to medium-sized businesses, the product's target, should pay special attention to the other challenges Active Administrator addresses to see if the product would be a good fit for their needs.

About Concentrated Technology

Concentrated Technology, LLC is a technology education and analysis consulting firm founded by industry luminaries Don Jones and Greg Shields. The company provides strategic consulting services to companies around the world, and performs market research and analysis for technology vendors and customers. The company distinguishes itself through its motto, “Maximum Knowledge - Minimum Time,” focusing on producing concise, accurate materials that help modern businesses accomplish more, with less effort.