concentrated technology

ProductScope™

NetWrix Change Reporter Suite

January 2012

Contents

Overview

Change auditing and tracking is important for detailed IT governance by legislative and industry requirements and to abbreviate the time to solution when technology problems occur. Most server products and technologies offer their own native logging mechanisms, but they are not always sufficient. Additional auditing information must be obtained by plugging into portions of a product rather than native logs, such as various APIs.

By itself, native logging presents challenges. In many cases, native logs are easily modified by administrators, reducing the reliability of the log as an audit trail. Native logs often produce a great deal of information, making it difficult to search and filter in order to find something specific. Native logging mechanisms rarely include robust reporting tools that would make the raw log data more useful. And native logs are often highly distributed, or stored across multiple servers, making it difficult for organizations to get a consolidated view into the activity within their environment.

The third party tool NetWrix Change Reporter Suite (CRS) offers a different approach from native logging in a number of auditing challenges, including log consolidation, event gathering, log security, reporting, and log archival. NetWrix CRS is the subject of this ProductScope™ paper.

Methodology

For this paper, we conducted a survey of 643 IT professionals, managers, and executives. The survey was designed to reveal the most common organizational requirements, and to determine respondents' preferences for various implementation methods and approaches.

We conducted interviews with 17 of our survey respondents to gather further information and clarification. Our respondents and interviewees were drawn from organizations of all sizes in a variety of fields, and were mostly headquartered in the United States.

We also conducted a focus group study with 18 IT professionals and managers, demonstrating key NetWrix product features and asking for the participants' feedback. Finally, we conducted our own analysis of the product based upon industry trends and common requirements.

Breadth of Visibility

One growing challenge in technology management is the proliferation of tools. It's desirable to move as many functions as possible into as few tools as possible. Change auditing is particularly affected by this challenge, because in many cases auditing information makes the most sense when specific user activity can be correlated across multiple products. For example, tracking user activity as they are added to an Active Directory user group, then as they use the group's permissions in SQL Server, and as they take themselves out of the group, all form a pattern of behavior that would be of interest to the organization.

NetWrix CRS provides change auditing across a wide range of products – the widest, in fact, among competing products in this category. The product supports:

- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft Group Policy
- Microsoft SharePoint Server
- Microsoft SQL Server
- Microsoft System Center Virtual Machine Manager
- Microsoft Windows file servers
- Microsoft Windows server configuration
- NetApp and EMC storage solutions
- Network devices such as Cisco firewalls
- VMware vSphere

NetWrix's roadmap includes adding support across a variety of additional products, such as Oracle database solutions, cloud-based services, and generic Syslog log collection, which are useful for a variety of network infrastructure devices as well as for Unix/Linux servers. There are also plans in the roadmap to expose change auditing data to support change management platforms such as BMC Remedy.

NetWrix's licensing and maintenance model involves updates to their products, including significant functionality changes such as adding Syslog data collection. Change logs for their products indicate a rapid and steady pace of development – sometimes as many as four significant updates in a year – all provided to customers at no additional charge beyond the maintenance agreement. NetWrix also offers all new product modules that are added to their product suites at no additional cost to customers with the maintenance agreement.

Organizations using System Center Operations Manager (SCOM) can also implement a free NetWrix add-on that feeds auditing information to SCOM, further reducing the number of tools administrators must use and increasing the visibility of audit data within the environment. They also offer integration with other third-party SIEM solutions like ArcSight and Tivoli to further extend enterprise auditing and change management.

Collection Approach and Alerting

There's a great deal of back-and-forth in the industry about "agent" versus "agentless" data collection. Our survey and interviews made it clear that the industry generally prefers an agentless approach, in which a central auditing server collects data from servers without any software being installed on that server. Our interviewees primarily cited stability and maintenance concerns as the driver for their agentless preference.

A locally-installed agent offers performance advantages, including reduced network bandwidth due to compression, but also offers disadvantages, such as being an additional piece of software that has to be patched and maintained. Poorly written agents also offer the risk of destabilizing the machine on which they're installed. Agents can potentially cause incompatibilities with first-party patches and service packs, as well, requiring additional testing prior to deploying those updates. Of course, a reputable software vendor who has a close relationship with first-party vendors (such as Microsoft) can usually mitigate these potential risks; our interviewees told us that well-written agents typically perform well and were not a significant source of trouble in their environments.

Obviously, some technologies only work with an agentless model. For example, when auditing changes on an EMC or NetApp storage system, an agentless approach is the only option because there's no way to install an agent on those systems. When auditing information from a product such as Microsoft SQL Server, the technology itself would make either an agent-based or agentless approach feasible.

NetWrix CRS offers both an agentless and an agent-based approach, enabling customers to choose whichever they prefer. Generally speaking, we expect that most customers start with the agentless approach ("bandwidth is cheap" was a common refrain from our participants when we noted that an agentless approach would generally consume more network bandwidth), and then move to an agent-based approach on an as-needed basis.

One area in which an agent-based approach can become necessary is alerting. NetWrix CRS can issue alerts for specified events, bringing attention to potentially harmful activity without someone manually searching through logs or generating reports. CRS defaults to a collection interval of ten minutes or more, depending upon the product being audited.

Our participants indicated that for some products, receiving alerts that had been delayed by up to ten minutes was fine, and that in some cases a delay of a day or more would be acceptable. In other cases, particularly with identity management, ten minutes was too long to delay, and our participants said that they would want the option to have alerts generated much more quickly – the qualitative metric most commonly suggested was "less than a couple of minutes."

NetWrix CRS offers the ability to configure its collection interval, which necessitates the installation of a local agent. The majority of our participants described this as a "valid compromise." NetWrix cautions that frequent collection intervals, especially in a busy environment, can cause additional resource consumption. Our participants acknowledged that risk, and said that in cases where they needed real-time auditing, they would provision the environment accordingly to handle the workload.

This highlights a key management principle regarding auditing: The more you want, the more you'll pay, typically in terms of performance. Auditing – especially high-volume, real-time auditing – is not something you can layer onto an existing environment, no matter what products you are using. Auditing is a form of workload, and that workload must be factored into your overall plan. We urge any customer who is evaluating auditing solutions to conduct a thorough pilot, with an emphasis on studying potential performance impact.

From an analysis perspective, we appreciate that NetWrix offers customers the choice of collection models. In practice, neither the agentless nor agent-based models individually meet every need within every customer environment. Both models require compromises of various kinds, and enabling customers to choose their compromise based on their particular needs is both generous and forward-looking for a vendor.

Collection Source

Another area in which auditing solutions compete vigorously is in *where* they obtain the data they collect. Some vendors eschew the use of native event logs entirely, because in many situations – such as on a busy Windows server – enabling full auditing can severely impact system performance. Instead, those vendors tap either public APIs or, in some cases, use unpublished APIs to collect information. Some vendors rely primarily on native event logs and others rely on a mix of sources.

Our standard guidance to customers is to understand the compromise. A solution that uses public APIs rather than native event logs could also have a negative performance impact, and customers should pilot solutions and test their performance prior to making an acquisition. Solutions relying entirely on the native event logs may miss information that isn't included in the log, and again customers should understand what's available from a particular solution.

Solutions that use non-public APIs (or "hacks," as some refer to them) carry a somewhat higher inherent risk, because those APIs may not be fully supported in future versions of whatever technology is being audited. The use of non-public APIs also carries a somewhat higher risk of system instability, because the first-party vendor may not have tested the use of those APIs on third party software. Customers must understand how each product works to make their decisions. For example, a well-respected, trusted vendor who can deliver timely software updates might also be trusted to work with non-public APIs.

Using public APIs does not necessarily mitigate all risk, as those APIs can be just as buggy as non-public ones and are equally subject to changes or patches from the first-party software vendor.

In some cases, there are no publicly available native ways to collect information. For example, moving a file from one place to another on the same volume does not generate any native log events on a Windows file server (specifically, a file deletion and creation event are logged, but without any cross-references explicitly showing that a file was moved from one location to another). If a customer needed to audit that information, the only means would likely be some low-level "shim" or "filter" in the Windows file system. Such filters are written according to a public and supported Microsoft API. Like any low-level software, these filters carry a risk of failure, performance impact, and incompatibility with future Microsoft patches or service packs. Choosing to use them is a compromise made in order to obtain information.

We caution customers not to get caught up in vendors' marketing positions and statements; instead, understand what their approach is, the potential risks and benefits, and why they chose that approach. Focus on what your business needs to audit and know that data collection will necessarily involve some level of compromise and overhead.

NetWrix uses a hybrid approach. Upon installation, CRS helps administrators configure native event logging to the minimum degree required. Information is also collected through other sources, and NetWrix states that they do not make use of non-public APIs for data collection. NetWrix has stated that they would consider other mechanisms in cases where there was no other way to retrieve the data, but would do so only after informing customers of the potential risk and that such mechanisms would not be enabled by default in their products. We feel that this is a reasonable approach: NetWrix is taking what they believe is the safest path for their customers by default, and then departing from that only when necessary and only after informing their customers of the potential downsides.

Auditing Granularity

Granularity is another area where change auditing vendors compete heavily. In our analysis, NetWrix CRS captured, on average, as much or more information as most other products in this category. We looked at a few key areas that are admittedly Microsoft-heavy, but which represent some of the most common areas of concern.

For Active Directory auditing, CRS captures the standard who, what, when, and where information. In many cases it is also able to capture before and after information, showing what values existed prior to

the change.

For Group Policy Objects (GPOs), CRS captures setting-level changes. For example, clearing an entire GPO results in a change report for each setting that had been in that GPO.

For Exchange Server, we looked at a variety of commonly desired events, including non-owner mailbox access, and CRS did a good job of capturing that information.

We noted that the product is good at filtering out duplicate events in its log. This can significantly reduce the amount of "noise" normally present in native logs, as well as reducing storage requirements and report-generation time. This de-duplication also reduces the number of duplicate alerts sent out for events for which an alert has been configured.

Archiving

One often-overlooked area of auditing is data archiving. Because most auditing solutions use a database as a back-end (NetWrix relies on Microsoft SQL Server), customers tend to assume that they can leave all of their data in the database forever. That's rarely true, and for performance reasons, customers often want to archive old data out of the database.

NetWrix CRS offers native archiving capabilities, and does not charge extra for the feature. The archive feature uses a two-tier approach, where older data is removed from the SQL Server database and placed into secured, compressed storage. NetWrix claims that customers can use this approach to store up to seven years of data, which is the longest period generally required by various laws and industry practices.

We feel that long-term storage is something that every customer will need and use in relation to an auditing solution. If long-term storage is provided as an archive feature or if a solution is architected in such a way that sufficiently long-term data can be stored in the main database, that's great. Customers should understand their own data retention needs and ensure that a solution can meet them. However, we note that not all vendors in this market space provide a well-thought-out long-term storage strategy, and some offer it through add-on products. When considering change auditing solutions, we urge customers to consider products' long-term storage capabilities and to obtain product pricing inclusive of such archival features.

Security and Separation of Duties

A problem with many technologies' native event logs is that they can be easily cleared by administrators. When configured (as it is by default) for periodic data collection, NetWrix CRS audit data is partially vulnerable to log clearing in that any log events created since the last collection could be lost. Because CRS gathers information from a variety of sources, it's possible to know that someone had cleared the log and to know who did it. There is access to information that did not originate in the cleared log, so unless multiple audit sources were successfully cleared or blocked, there might well be more direct evidence of the activity.

In most organizations, that fact is enough to deter administrators from actually clearing logs without authorization, because they know they'd be caught. In reality, any product that collects data in anything less than absolute real time could potentially miss log data. In many cases, the technology or product being audited can also be configured to provide better separation of duties, such as configuring log files so that day-to-day administrators do not have permission to clear them.

Based on our customer interviews, we must identify this as a potential weakness in NetWrix CRS for some customers. Some of our interviewees indicated that the potential for data to be permanently lost when an administrator clears a log would be unacceptable for their environments.

We note that some solutions, including the Microsoft Audit Collection Services included with System Center Operations Manager, offer log collection that is more real-time, and thus significantly reduces the potential for lost data due to log clearing. We also note that CRS *can* be configured for more-frequent collection intervals, which would reduce or eliminate this weakness. Customers need to evaluate the performance impact of such a configuration where real-time collection is a core requirement. Additionally, some customers might not find this situation to be troublesome; fewer than a quarter of our interviewees felt that it would be problematic in their environments, and their concerns related primarily to legally related auditing requirements that would not affect all organizations.

NetWrix CRS stores its audit data in a Microsoft SQL Server instance, and can use the freely available Express edition, avoiding the need for an additional SQL Server license. NetWrix states that a SQL Server Express database (which has hard-coded size limits) should be able to store about two years' worth of data for most organizations. Because the data is stored in a separate database, that database can be secured so that IT administrators cannot modify it.

Change Rollback

Although CRS is not sold as a backup and recovery solution, it offers an Active Directory object restoration wizard and the ability to restore both Group Policy and Windows File Server data. The Active Directory object restoration wizard can restore anything from an entire container of deleted objects to a single changed attribute of an object.

Administrators start by discovering an unwanted change, either in an e-mail report or in the CRS console. They then launch the CRS management console to invoke the rollback wizard. We would like to see tighter integration of the rollback wizard so that it could be launched directly while viewing a change report. Other products in this category offer tighter integration and our study participants indicated that the rollback feature would be much more useful and more likely to be used if it could be initiated from the spot where they first notice the change.

CRS does not take the place of a full Active Directory backup and recovery solution. We did not evaluate its ability to recover an entire domain, and it would not be a suitable tool for a full-forest recovery (which must generally be accomplished by working with Microsoft product support, although specialized tools can be used to speed the process). However, CRS' capabilities do make for a very functional Active Directory Recycle Bin, and definitely provide capabilities superior to those native to Windows.

Reporting

CRS offers robust searching and filtering capabilities, making it straightforward to list all changes made on a certain date, or changes made by a certain person, and so forth.

Because the product's data store is based on SQL Server, it is able to leverage SQL Server Reporting Services (SSRS) for reporting. That means reports can be delivered in a variety of ways, including online and through scheduled e-mail delivery. More than 200 built-in reports are provided as a starting point, and SSRS permits the creation of custom reports. Reports can include information from the second-tier archive as well as from the active data stored in SQL Server. SSRS permits reports to be exported in a variety of formats, including PDF, XML, Excel, CSV, and so on.

Additional Considerations

Our study participants found NetWrix CRS to be easy to install, configure, and use. The product's various components all reside in a single console and have a highly-integrated and consistent appearance.

NetWrix claims over 5,000 customers for the product, spread across 50 countries and in industries such as healthcare, government, financial services, education, energy, and so forth, including several Fortune 500 companies. The company maintains offices in several US states as well as in the United Kingdom and Japan. NetWrix is privately held and claims to be profitable. The company employs approximately 75 people, with about half in product development and another fifth in technical support. More than three-quarters of the company's sales are made directly to customers, with the remainder made through channel partners. NetWrix' largest customer sector consists of mid-sized companies (55%), with a solid showing in the enterprise (30%) category.

Potential Weaknesses

Like any change-auditing product, CRS is useful to customers only if it can capture audit data from as many sources as possible within the organization. NetWrix CRS already has impressive reach in this regard. The company states that Oracle and Syslog support, along with other sources, are on the product's roadmap, which will increase the product's reach considerably. However, it's important for customers to have a complete wish list of things they'd like to audit and to evaluate competing solutions for their ability to audit as many of them as possible.

Conclusion

Both our study participants and our own analysis position NetWrix Change Reporter Suite as a significant contender in the marketplace. The product's breadth, as well as its ability to support both agent-based and agentless collection models, will make it suitable for a very wide range of organizations. NetWrix offers a competitive pricing model, and has thought through several of this product category's bigger challenges, such as long-term archives, reporting, and security.

We recommend that any customer looking for a change-auditing solution include NetWrix in their shortlist of products to evaluate.