TAKING ACTIVE DIRECTORY AUDITING TO THE NEXT LEVEL

How LepideAuditor Suite helps improve IT security

Introduction

The Active Directory is arguably the most important part of any Windows-based IT infrastructure within an organization. For this reason, it is imperative that you take extra steps to protect the Active Directory through regular, pro-active auditing. This process will help to reveal all accesses and changes made to objects so that you can spot anomalies and act faster.

What are the requirements?

By creating a list of requirements before you start auditing your Active Directory you can determine what aspects of the audit are important to your organization. For example, your requirements could be:

- To get real-time information of what all is being changed in the configuration and by whom
- To get before-and-after change values to provide context to any change made. If any change seems suspicious, Administrators can then take steps to revert it
- To stay compliant with regulatory compliances such as HIPAA, GLBA, FISMA, SOX, SAS, PCI DSS and others

Limitations of Native Auditing

The Windows Server operating system does offer inbuilt auditing tools, such as Event Viewer, Windows PowerShell and others. However, there are some limitations which we go through here:

1. Event Viewer generates multiple events for a single action which can result in an unmanageable number of logs. For example, multiple events will be generated when a Directory Service object is created.
2. The event logs are memory-mapped files. If you have configured the maximum size of logs to 2 GB, it means (2 GB x 4 =) 8 GB space will be permanently occupied by the Event Viewer. This size can be increased up to 16 GB provided the maximum size for each type of log has been set to 4 GB. Lower sizes mean fewer events can be monitored simultaneously as the events generated after reaching the threshold limit will either be overwritten or archived.
3. If you have set the logs to be archived for long-term storage, all events will then be archived to "%system32%/winevt/logs" and will continue to consume space on primary drive. There are no automatic processes to move these archived logs to a secondary or external drive.
4. There are no inbuilt pre-defined audit reports. The only option is to create massive Windows PowerShell scripts or use an existing template. This means dealing with multiple, complex scripts if you want to simply find out the health of the server.

5. To view the event logs for all computers on the primary domain controller you have to setup subscriptions on the server and configure each computer in the network. This is a complicated process and Administrators often skip it.

Event logs do contain snippets of relevant information, but more information is needed for IT teams to better understand changes being made. For example, if an Administrator has unlocked an account and reset its password, the auditor may want to know what changes have been made in the access control lists of the primary drive or other folders for that user. Using manual or other scripting methods to check the changes in currently assigned permissions on different folders and drives is a laborious and time-consuming task.

Solution

LepideAuditor Suite is a simple, cost-effective and automated solution designed to overcome the limitations of native auditing. It lets you audit multiple instances of Active Directory, Group Policy Objects, Exchange Server, SQL Server, SharePoint and File Server from a centralized platform. The intuitive dashboard makes it easier for IT Auditors and Administrators to track configuration changes being made to their most critical IT servers.

The solution offers agent-based, agentless or hybrid auditing. There are no major differences between agentless and agent-based auditing, as the agents are very light on the system resources. Agents are only required to audit logon/logoff events, non-owner mailbox accesses and NetApp Filers.

The changes are captured in real-time and displayed in the solution after processing. The logs are stored in a SQL Server or SQL Server Express database and there is no limit the number of audit logs you can store. Administrators also have the option of archiving logs to another SQL database if required.

Real-time alerts on selected critical changes are sent in to the specified recipients by email and they will also be notified through the LepideAuditor App (compatible with any Android or Apple iOS enabled device). Through the Web Console, administrators can create accounts for selected users and determine which reports are to be shared.

In addition to auditing, LepideAuditor Suite also monitors the health of the Active Directory, Exchange Server and SQL Server. The solution creates backup snapshots of the state of Active Directory Objects and Group Policy Objects that can be restored with just a few clicks. Objects can be restored regardless of whether they are in a tombstone state.

The dedicated Radar Tab visually provides information on all aspects of the audited servers, including changes by criticality and by source. With over 270 predefined audit reports and a powerful search function, LepideAuditor Suite enables users to find the root cause of a change or meet regulatory compliance mandates in seconds.

5.