Active Directory Change Tracker

Reporting tool for changes made in Microsoft Active Directory

Product Overview

Vyapin's Active Directory Change Tracker tracks, analyzes and reports all changes made to the Active Directory configuration. The tool audits all changes made to the Active Directory by periodically collecting only the changed data, reporting what exactly changed, along with the new and old values, when the change was made, where the change happened in your Active Directory. The tool also determines who made the change by looking up the Security Event logs of the audit-enabled Active Directory.

Active Directory Change Tracker records and maintains the entire history of changes, along with the relevant Event log data, in a SQL server database for future reference and analysis. This powerful search tool helps you analyze all past changes on any predefined search criteria. Changes can be selectively tracked on OUs and other containers with several different delivery options in the form of reports, which can then be exported or emailed to the required address.

Active Directory Change Tracker may be configured to work with or without the native Auditing capabilities of the Active Directory. You can use the tool to track and audit AD configuration changes on what exactly changed, even without using the native auditing of AD. You can additionally combine the tool with the default native auditing of AD to capture Security Event Log audit records of changes from all domain controllers in your domain (since Event Log data is not replicated). Thus, the tool gives you the choice to have complete control on how you would like to track and manage changes to the Active Directory.

Change Management is a critical component in Enterprise Systems Management and is also required to meet your organization's compliance and regulatory needs such as SOX and HIPAA. Vyapin's Active Directory Change Tracker serves the demanding needs of tracking and maintaining records of critical changes to the Active Directory and is a must-have tool for Active Directory administration.

System Requirements

For the computer running ADChangeTracker

Processor: Intel Pentium III or higher processor

Disk space & Memory: 512 MB RAM and minimum of 20 MB of free disk space

Operating System: Windows 8.1 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2003 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 with .NET Framework 4.0 or higher with the latest service packs.

Database: Microsoft SQL Server 2012 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2008 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2005 (Enterprise / Standard / Developer / Express edition) running in local / remote computer with latest Service Pack.

Software: MDAC v2.5/2.6/2.8.

For the computer reported by the ADChangeTracker

Windows Server 2012 R2 /
Windows Server 2012 /
Windows Server 2008 R2 /
Windows Server 2008 /
Windows Server 2003 (SP2)
running Active Directory.

Benefits

- No Agent installation. Works as a desktop application connecting to your domain controllers. Installing and configuring the tool takes just a few minutes.

- Track and audit all changes made to the Active Directory, in your Windows enterprise. Selectively track changes on specific OUs or containers.

- Selectively track what changed (the old and the new values) on objects and their properties without using Active Directory's native auditing capabilities. Helps you track changes with almost no additional load on the domain controllers. Only incremental Change data is collected.

- Capture Audit records from Event logs by using native Active Directory auditing and combine them with the tool to produce reports on who made the change and when the change occurred. Provides a comprehensive solution for auditing changes to your Active Directory without investing in additional tools.

- Create and maintain a Change History of all changes in a SQL database and optionally, store them along with Security Event log Audit records. Helps you store several years of Change data for compliance and regulation purposes.

- Track different types of changes such as newly Created data, Modified data and Deleted data. Track Old and New values for both single and multi-valued attributes.

- Notify different Users of changes. Helps you to become aware of critical changes straight from your mail box.

- Search your entire Change History for Created, Deleted and Modified data on specific OUs or containers. Search for specific attributes that changed within a time period.

- Schedule your incremental change data collection to any desired frequency (for example, once every day or once every 8 hours). Schedule your reports for immediate email notification as soon as changes are detected.

- Security Event log data collection for the configured Event IDs.\

- Search your entire Events History using powerful Search criteria - search for Event IDs, Date range and Domains.

- Create and maintain an Events History of all the Event ID(s) for AD object changes, User logon/logoff activities, Password changes and Terminal Services activities with Security Event log data in a SQL data base. Helps you to store several years' worth of Events data for compliance and regulation purposes.
- Generate your Events Reports for the specified Date range, Domains, change type, category and filter criteria.

Key Features

Configuration Wizard: Configure your Domain Controller connections, SQL server settings, Data collection settings and Email notification settings using a Wizard.

Reports: Reports display the list of available timestamps of Change history starting from the most recent timestamp. Timestamps are neatly organized in a Day, Month, and Year categories. Generate reports on the most recent changes or changes that happened between two time periods (for example, all changes that happened last month).

Search: The powerful search tool lets you select the time period range, the change type (Created, Deleted, and Modified), OUs or containers. A powerful Free-text search filter allows you to extract changes based on keywords. For example, extract all changes made to a particular User in the month of January.

Search Events: The powerful search tool lets you select the Event IDs for the selected Date range and Domains. For example, extract all the '4662' Event ID's in the Events history database that occurred in the month of March.

Events Reports: Events Reports is a powerful feature that enables the user to report Events data for AD object changes (created, modified and deleted objects), User logon/logoff activities, Password changes and Terminal Services activities (User disconnected and re-connected to the session). This feature is driven by ADCT Listener Service application.

A Free-text search filter allows you to generate the Events reports based on keywords. For example, report the User logon/logoff activities of a particular user in the last 30 days.

Real time alerts: Real time alerts through email - powered by the multi-tasking background listener (ADCT Listener Service). Enables notification of a Change Event in Domain controller's Security Event log in real time.

Fast data collection and storage of Change Events using asynchronous, multi-threaded data collection from multiple domain controllers.

Advanced Filter: Advanced Filter tool in Events Reports allows you to filter the report based on complex filter conditions. Advanced Filter allows the user to perform advanced query based filtering using Field names and their values and save the filter configuration for future use. Selecting and applying a saved filter will apply the filter and directly produce the desired subset of data.

For example, all rows of changes in User information pertaining to certain properties can be filtered by compound filter (([Property Name]='Telephone number') or ([Property Name]='city')).

Quick Filter: Quickly filter data based on search strings and dates. Wildcard characters may be applied. For example, all rows of change data pertaining to "Administrators" may be filtered by a simple string filter "*admin*" across all fields or a single field. A simple string filter using "Full Control" as the search string will display all objects that had some change related to the "Full Control" permission.

Find: A simple string-based Find operation highlights all cells containing the string. Especially useful in determining string occurrences and their frequencies in a large set of displayed data. For example, find all occurrences of a particular OU.

Export: Flexible Export feature to export the Change reports to HTML/ CSV /XLSX file formats instantly or in a scheduled manner.

Instant Email notification: Instantly notify changes to different groups of Users as soon as changes are detected.

Vyapin Software Systems Private Limited
Website: http://www.vyapin.com/
Sales Contact: sales@vyapin.com
Technical Support: support@vyapin.com