



Diagnose & secure your network

YATEM LogCollector®

Active Directory Monitor™

What it does?



It allows fast, cost effective and durable change tracking on Microsoft Active Directory system.



Who?
When?
Where?
What happened?

System Load?



No overhead on CPU and network.

Reports & Queries



GUI and reports allows you to easily retrieve the data you seek.

Quick, Simple, Easy



Installation takes several minutes. Settings does not bother you. Easy to learn and use.

Comprehensive and Robust



No matter how big and complex your network, it just works.

Regulatory Compliance



Supports legitimate data logging.

LogCollector® Active Directory Monitor

Sorgu Ağacı		
AKTIF DİZİN OLAYLARI		
Nesne Oluşturma		
Nesne Değiştirme		
Nesne Taşıma		
Nesne Silme		
Nesne Silmeden Kurlama		
Logon		
Logoff		

Tarih (oluş)	Sunucu Adı	Olay
12.4.2014 13:05:12	R2DC	Nesne Oluşturma
12.4.2014 13:03:52	R2DC	Nesne Değiştirme
12.4.2014 13:00:19	R2DC	Nesne Taşıma
12.4.2014 12:59:59	R2DC	Nesne Silme
11.4.2014 13:00:05	R2DC	Logon
17.3.2014 14:33:51	R2DC	Logoff

“

"LogCollector Active Directory Monitor", is a software solution that enables you to determine, analyze and record the changes made by users on Microsoft Windows Active Directory objects in near real time. Thus, you can create a secure environment by controlling the changes on Active Directory Servers.

”

Top Benefits

- **Provides awareness.** You would be the first, who notices about the activities on your network.
- **Protects your investment costs.** Supports you to protect your valuable investment and corporate data with minimum effort and cost.
- **Easy and flexible reporting.** Allows to prepare even complex reports in seconds for all your requests.
- **Supports sustainable security infrastructure.** Ensures sustainable security infrastructure on protection and development of the effectiveness of security policies by offering real-time information.
- **Built-in and scheduled reporting.** Provides built-in reports out-of-the-box for your needs. You can also create scheduled and/or alerting reports to be notified in time.
- **Scalable.** Provides enhanced features for scalability. It suits your deployment needs on your network whatever its size, architecture and complexity.
- **Saves time.** It provides the system administrator to save time during daily activities.

What can you do with LogCollector Active Directory Monitor?

- Who is making changes on "Domain Controller" "D"?
- Who is trying to proceed on "Active Directory" without authorization?
- I want to be informed by email when the member of critical groups like "Domain Admins", "Administrators" has changed .
- Which users have been created on all DC's for last 7 days?
- Which modifications have been made on Active Directory objects by user "U" for last 30 days?
- Who has deleted user "U", when and from which terminal?
- I want to see the graphical representation of user activities on DC's by time.
- Which accounts have been locked?
- I want to be informed about the changes which have been made on groups, everyday at 5 pm, by email in PDF format.



Properties

General

- **Licensing:** Per server and per user.
- **Database:** Collected logs are kept in Microsoft SQL Server or PostgreSQL database.

Event Collection

- **Architecture:** Agent based.
- **Events:** Collects all the change attempts on Active Directory objects which are create, rename, move, delete, undelete etc. Additionally, user logon/logoff events and group policy change attempts are reported.
- **Event Details:** For every event the activity information of user name (who), computer Name (where), timestamp (when), object name (what) are detected and logged. The old and new value of the changed object are kept together.
- **Real Time Collection:** Events are detected recorded by the agents as soon as occurred.
- **Off Line Activity:** Agents continue to detect and collect logs of events when the computer lost the network connection. Agents protect themselves and also the data which are waiting to send. When the computer become online, the data transfer process starts automatically.
- **Agent Protection:** LogCollector prevents any user access to agents and collected event records.
- **Agent Performance:** LogCollector agents have a powerful science of art monitoring engine, it just works.
- **Agent Footprint:** LogCollector agent needs very small system resource to work. It never loads the CPU, memory and bandwidth.
- **Data Reliability :** Every event record is tagged with a MD5 hash as the event happens in order to guarantee that data is not changed. The console application marks the data which has a wrong hash.

Event querying, Analyze and Reports

- **Real Time Event Monitoring:** LogCollector has a powerful user interface in order to query, analyze and get screen and printed reports on collected data in real time.
- **Dynamic Queries:** LogCollector user interface provides simple and powerful queries to retrieve the required data.

- **Query Performance:** LogCollector provides astonishing data retrieving performance on its data store.
- **Build-in Query and Reports:** LogCollector user interface provides a large number of built-in query and reports for data investigation.
- **Interactive Graphical Analyze:** Every text data shown on GUI can easily converted to drill-down chart style.
- **Data Export:** User interface provides data exporting to well known formats like PDF, CSV/Excel, HTML and XML.
- **Scheduling Reporting:** Reports can be scheduled to save in to desired folder as various formats like pdf, excel or text files and/or sent to any email address.
- **Notifications (alarms):** Automated email notifications can be set for desired conditions.

Management

- LogCollector has a central management console tool for installing/uninstalling and tracking status of agents.

Archiving

- LogCollector includes an archiving tool to transfer old records from database to offline xml based store.
- Archiving can be achieved manually or automatically.
- Archived data can be viewed and analyzed with the archiving utility offline.

System Requirements

LogCollector Server:

- CPU: 2 GHz Pentium or above
- OS: Microsoft Windows 7 or above
- RAM: 1 GB+
- DBMS: Microsoft SQL Server 2008+ or PostgreSQL 9+
- Storage: 100 MB+ for initial installation and enough space for data storage.

Agents:

- OS: Windows 7 or above
- Storage: 100 MB+ including offline logging needs.



YATEM Information and Technology Systems Inc.
E-mail: yatem@yatem.com.tr
Phone : +90 (312) 479 4088 Fax: +90 (312) 479 4088
<http://www.yatem.com.tr>

AUTHORIZED DISTRIBUTOR