

Change Auditor for Active Directory Queries

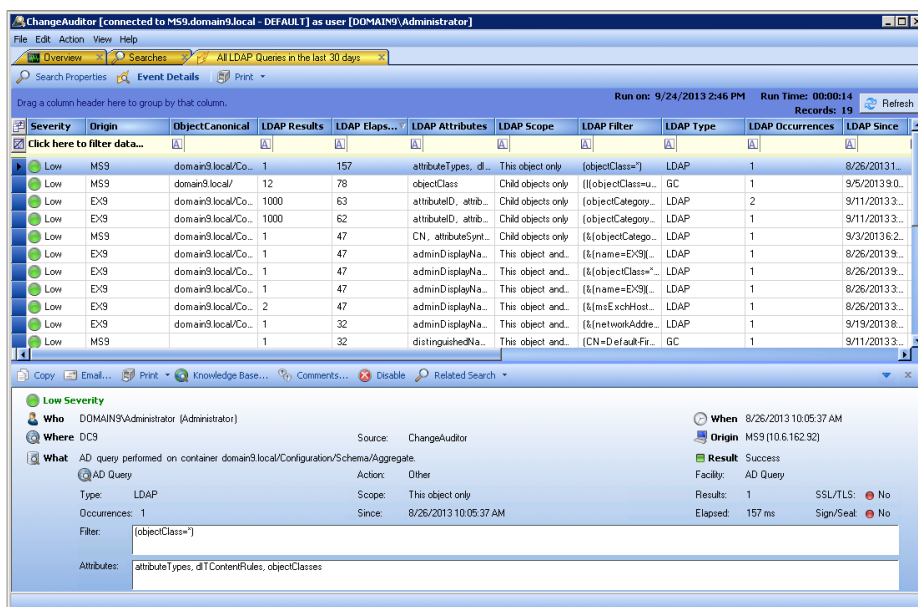
Determining what applications and users are accessing Microsoft Active Directory (AD) is nearly impossible using native tools, fraught with risk and can cripple Active Directory environments to a halt if not monitored correctly. Administrators run the risk of missing poorly written or sluggish queries that affect performance, and not knowing what applications are hard coded and dependent on AD can disrupt migrations and consolidations. Because of this inability to monitor and assess queries, organizations find it difficult to optimize the service they provide to their users, plan for migrations or perform a directory consolidation. To achieve and maintain stability of AD as well as compliance with regulations and policy, an organization must be able to identify and measure the performance of Active Directory queries.

Quest® Change Auditor for Active Directory Queries tracks, analyzes and reports on all Active Directory queries in real time, translating them into simple terms and eliminating the time and complexity required for auditing. You can immediately detect queries and their results in one quick glance, determining whether you need to investigate further.

Best of all, Change Auditor for Active Directory Queries gives you complete visibility into all queries over the course of time with forensics on who, what, when, where and workstation, including any related queries. And with real-time alerts sent to any device, you can immediately address problems and avoid system downtime.

BENEFITS:

- Saves time spent obtaining details for every Active Directory query
- Strengthens internal controls by identifying insecure or unsigned queries against Active Directory that do not conform to internal security policies
- Improves availability by identifying users and applications performing queries that can affect domain controller performance
- Assists in the discovery process for migrations by determining what machines need connectivity
- Reduces security risks with real-time alerts to any device for immediate response
- Eliminates unknown security and performance concerns, ensuring continuous access to queries and related events, such as queries coming from specific applications or users
- Streamlines internal policies and compliance regulations, including GDPR, SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more
- Turns information into intelligent, in-depth forensics for auditors and management



With Change Auditor, you'll see the results of all Active Directory queries in real time and gain instant insight to queries that do not conform to internal security policies.

AUDIT ALL CRITICAL AD QUERIES

Change Auditor provides extensive, customizable auditing and reporting for all queries against Active Directory. In addition, each event will show the scope of the query, the filter used, the attributes and the number of results returned. You'll also be able to identify queries against Active Directory that don't conform to internal security policies as well as poorly written queries that degrade Active Directory performance.

TRACK QUERY ACTIVITY

Change Auditor for Active Directory Queries locates all queries and then filters searches by type, location, user and more. You can easily show which users and applications are performing queries that affect AD performance, and learn what machines need connectivity during and after migrations.

With 24x7 real-time alerts, in-depth analysis and reporting capabilities, you will always know what's going on in your environment.

TURN IRRELEVANT DATA INTO MEANINGFUL INFORMATION FOR OPERATIONAL EFFICIENCY

Change Auditor for Active Directory Queries tracks queries to your Active

Directory environment, and then translates raw data into meaningful intelligent data to keep your infrastructure efficient and provide detailed analysis. And without the need for native audit logs, you'll see faster results and savings of storage resources.

GET X-RAY VISION OF YOUR ACTIVE DIRECTORY ENVIRONMENT

You'll have a detailed view of what's going on behind the scenes in your environment. Change Auditor for Active Directory Queries is ideal for those preparing for a migration, to help prepare for disaster recovery contingency plans or gathering insight into Active Directory.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

The screenshot displays the Change Auditor application window. The top section shows a table of LDAP queries with columns for Severity, Object Canonical, LDAP Elapsed, LDAP Results, LDAP Attributes, LDAP Scope, LDAP Filter, LDAP Type, LDAP Occurrence, LDAP Since, and Time Detected. Below the table, a detailed view of a query is shown, including fields for Who (DOMAIN9\Administrator), Where (DC3), What (AD Query), Type (LDAP), Scope (This object and all children), Filter ([objectClass=attributeSchema]), and Attributes (attributeSecurityGUID, IDAPDisplayName, linkID, schemaIDGUID). The interface also shows a 'Low Severity' alert and various navigation and search options.

Eliminate repetitive queries that slow performance with the ability to group, sort and filter results by origin and number of occurrences.