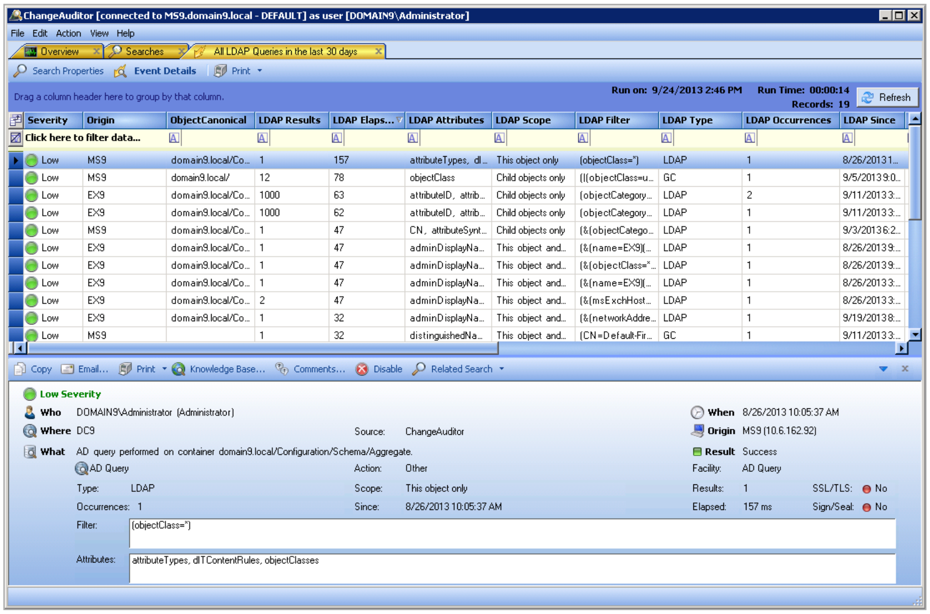
# Change Auditor for Active Directory Queries

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.

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.


ChangeAuditor [connected to MS9.domain9.local - DEFAULT] as user [DOMAIN9\Administrator]
File
Edit
Action
View
Help
Overview
Searches
All LDAP Queries in the last 30 days
Search Properties
Event Details
Print
Drag a column header here to group by that column.
Refresh
Click here to filter data...
Copy
Email...
Print
Knowledge Base...
Comments...
Disable
Related Search

Run on: 9/24/2013 2:46 PM Run Time: 00:00:14
Records: 19

| Severity | Origin | ObjectCanonical | LDAP Results | LDAP Elaps... | LDAP Attributes | LDAP Scope | LDAP Filter | LDAP Type | LDAP Occurrences | LDAP Since |
|---|---|---|---|---|---|---|---|---|---|---|
| Low | MS9 | domain9.local/Co... | 1 | 157 | attributeTypes, dl... | This object only | (objectClass=*) | LDAP | 1 | 8/26/2013 1... |
| Low | MS9 | domain9.local/ | 12 | 78 | objectClass | Child objects only | (I(objectClass=u... | GC | 1 | 9/5/2013 9:0... |
| Low | EX9 | domain9.local/Co... | 1000 | 63 | attributeID, attrib... | Child objects only | (objectCategory... | LDAP | 2 | 9/11/2013 3:... |
| Low | EX9 | domain9.local/Co... | 1000 | 62 | attributeID, attrib... | Child objects only | (objectCategory... | LDAP | 1 | 9/11/2013 3:... |
| Low | MS9 | domain9.local/Co... | 1 | 47 | CN, attributeSynt... | Child objects only | (&(objectCatego... | LDAP | 1 | 9/3/2013 6:2... |
| Low | EX9 | domain9.local/Co... | 1 | 47 | adminDisplayNa... | This object and... | (&(name=EX9)(... | LDAP | 1 | 8/26/2013 9:... |
| Low | EX9 | domain9.local/Co... | 1 | 47 | adminDisplayNa... | This object and... | (&(objectClass=*... | LDAP | 1 | 8/26/2013 9:... |
| Low | EX9 | domain9.local/Co... | 1 | 47 | adminDisplayNa... | This object and... | (&(name=EX9)(... | LDAP | 1 | 8/26/2013 3:... |
| Low | EX9 | domain9.local/Co... | 2 | 47 | adminDisplayNa... | This object and... | (&(msExchHost... | LDAP | 1 | 8/26/2013 3:... |
| Low | EX9 | domain9.local/Co... | 1 | 32 | adminDisplayNa... | This object and... | (&(networkAddre... | LDAP | 1 | 9/19/2013 8:... |
| Low | MS9 | | 1 | 32 | distinguishedNa... | This object and... | (CN=Default-Fir... | GC | 1 | 9/11/2013 3:... |

Low Severity

Who DOMAIN9\Administrator (Administrator)

When 8/26/2013 10:05:37 AM

Where DC9

Source: ChangeAuditor

Origin MS9 (10.6.162.92)

What AD query performed on container domain9.local/Configuration/Schema/Aggregate.

Result Success

AD Query

Action: Other

Facility: AD Query

Type: LDAP

Scope: This object only

Results: 1

SSL/TLS: ● No

Occurrences: 1

Since: 8/26/2013 10:05:37 AM

Elapsed: 157 ms

Sign/Seal: ● No

Filter: (objectClass=*)

Attributes: attributeTypes, dITContentRules, objectClasses

*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.*

## 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 SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more
- Turns information into intelligent, in-depth forensics for auditors and management

## 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

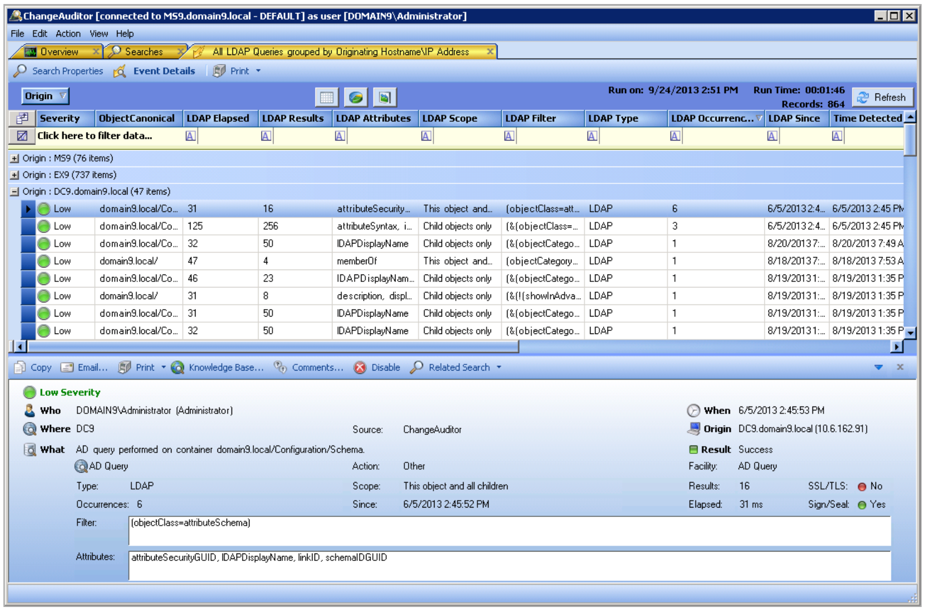
Change Auditor for Active Directory Queries tracks queries to your Active Directory environment, and then translates raw data into meaningful intelligent data to keep your infrastructure efficient and provide detailed analysis. And without the need for native audit logs, you'll see faster results and 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

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.



ChangeAuditor [connected to MS9.domain9.local - DEFAULT] as user [DOMAIN9\Administrator]

All LDAP Queries grouped by Originating Hostname\IP Address

Run on: 9/24/2013 2:51 PM Run Time: 00:01:46 Records: 864

Origin : MS9 (76 items)
Origin : EX9 (737 items)
Origin : DC9.domain9.local (47 items)

| Severity | ObjectCanonical | LDAP Elapsed | LDAP Results | LDAP Attributes | LDAP Scope | LDAP Filter | LDAP Type | LDAP Occurrenc... | LDAP Since | Time Detected |
|---|---|---|---|---|---|---|---|---|---|---|
| Low | domain9.local/Co... | 31 | 16 | attributeSecurity... | This object and... | (objectClass=att... | LDAP | 6 | 6/5/2013 2:4... | 6/5/2013 2:45 PM |
| Low | domain9.local/Co... | 125 | 256 | attributeSyntax, i... | Child objects only | (&(objectClass=... | LDAP | 3 | 6/5/2013 2:4... | 6/5/2013 2:45 PM |
| Low | domain9.local/Co... | 32 | 50 | lDAPDisplayName | Child objects only | (&(objectCatego... | LDAP | 1 | 8/20/2013 7:... | 8/20/2013 7:49 A |
| Low | domain9.local/ | 47 | 4 | memberOf | This object and... | (objectCategory... | LDAP | 1 | 8/18/2013 7:... | 8/18/2013 7:53 A |
| Low | domain9.local/Co... | 46 | 23 | lDAPDisplayNam... | Child objects only | (&(objectCatego... | LDAP | 1 | 8/19/2013 1:... | 8/19/2013 1:35 P |
| Low | domain9.local/ | 31 | 8 | description, displ... | Child objects only | (&(!(showInAdva... | LDAP | 1 | 8/19/2013 1:... | 8/19/2013 1:35 P |
| Low | domain9.local/Co... | 31 | 50 | lDAPDisplayName | Child objects only | (&(objectCatego... | LDAP | 1 | 8/19/2013 1:... | 8/19/2013 1:35 P |
| Low | domain9.local/Co... | 32 | 50 | lDAPDisplayName | Child objects only | (&(objectCatego... | LDAP | 1 | 8/19/2013 1:... | 8/19/2013 1:35 P |

Low Severity

Who DOMAIN9\Administrator (Administrator)
When 6/5/2013 2:45:53 PM
Where DC9
Source: ChangeAuditor
Origin DC9.domain9.local (10.6.162.91)
What AD query performed on container domain9.local/Configuration/Schema.
Result Success
AD Query
Action: Other
Facility: AD Query
Type: LDAP
Scope: This object and all children
Results: 16
SSL/TLS: ● No
Occurrences: 6
Since: 6/5/2013 2:45:52 PM
Elapsed: 31 ms
Sign/Seal: ● Yes
Filter: (objectClass=attributeSchema)
Attributes: attributeSecurityGUID, lDAPDisplayName, linkID, schemaIDGUID

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