ManageEngine
EventLog Analyzer

Permissions required for SQL server auditing

www.eventloganalyzer.com

Permissions required for SQL server auditing

With many organizations using Microsoft SQL Server, protecting the confidential data within these database servers should be a priority for security professionals. Because organizations tend to have a number of SQL Servers installed, manually configuring each one for log management and auditing is a time-consuming task. Even with successful configuration, tracking SQL Server activity is generally placed on the back burner, as the importance of this task is often overlooked.

EventLog Analyzer is a log management tool that provides a solution for organizations who not only have multiple SQL Servers to configure, but also need to monitor activity on these servers. EventLog Analyzer automatically discovers SQL Servers in your network and displays them in a list; from there, you can decide which ones need to be audited.

It also provides a plethora of predefined reports that select essential information from your SQL Servers' log data to pinpoint events that may need your attention. EventLog Analyzer automatically collects activity logs from SQL Servers and helps you make sense of the information stored there. You can drill down and filter reports, customize alerts, perform log searches, and archive logs for powerful and effective management of SQL Servers, all while sticking to your budget.

Port: 1434
Protocol: UDP

Report Name	Required Minimum Permission for Login			Remarks
	Server Roles	User Mapping	Securables	
DML\DDL Auditing				
-N/A-	1) Public 2) Server admin	1) Public	1) Connect SQL 2) Alter any server audit	- 'Serveradmin' and 'Alter any server audit' permissions are required only for configuration (i.e., enabling/ disabling/ deleting audit), not for the actual auditing process.
COLUMN INTEGRITY MONITORING				
-N/A-	1) Public	1) Public 2) db_ security admin 3) db_ ddladmin	1) Connect SQL 2) Alter Trace	- Map all databases to be audited with Login, else you'll get "java.sql.SQL Exception: Cannot open database" "requested by the login. The login failed." exception - 'db_securityadmin', 'db_ddladmin' and 'Alter Trace' permissions are required ONLY for configuration (i.e., enabling/disabling/ deleting monitoring), not for the actual monitoring process.

DATABASE AUDITING				
Last Login Time Report	1) Public	1) Public	1) Connect SQL 2) View server state	- 'View server state' permission is required to execute 'sys.dm_exec _sessions' - If 'View server state' permission is not provided, only current Login's session information will be retrieved - Reference link
Logins Information Report#	1) Public	1) Public	1) Public 2) Connect SQL 3) View any definition	- 'View any definition' is required to get information of all Logins from 'master.. syslogins' - If 'View any definition' is not provided, only information of current Login and "sa" will be retrieved
Most Used Tables#	1) Public	1) Public	1) Public 2) Connect SQL 3) View any definition	- 'View any definition' is required to get information from 'sys.tables' and 'sys.indexes' - Reference link for sys. tables - Reference link for sys.indexes - Reference link for sys.partitions - Reference link for sys.allocation_units
Table Update Report	1) Public	1) Public	1) Connect SQL 2) View server state	- 'View server state' is required to get information from 'sys.dm_db_index_ usage_stats' - Reference link
Index Information Report#	1) Public	1) Public 2) db_owner	1) Connect SQL	- 'db_owner' permission is required to get information from 'sys.indexes' - If 'db_owner' permission cannot be provided, 'View any definition' permission (under Securables) can be provided instead. But information of some indexes belonging to sys. internal_tables (especially those of type 'CONTAINED_FEATURES') may not be retrieved. - Reference link for sys.indexes - Reference link for sys.internal_tables
Server Information Report	1) Public	1) Public	1) Connect SQL	- Information is retrieved by executing SERVERPROPERTY()

Waits Information Report	1) Public	1) Public	1) Connect SQL 2) View server state	- 'View server state' is required to execute 'sys.dm_os_wait_stats' - Reference link
Blocked Processes Report	1) Public	1) Public	1) Connect SQL 2) View server state	- 'View server state' is required to get information from 'master..sysprocesses' - If 'View server state' is not provided only the current session information will be retrieved - Reference link
Schema Change History	1) Public	1) Public	1) Connect SQL 2) Alter trace	- 'Alter trace' permission is required to get information from 'sys.fn_trace _gettable' - Reference link
Object Change History#	1) Public	1) Public	1) Connect SQL 2) View any definition	- 'View any definition' is required to get information from 'sys.objects' - Reference link
Connected Applications Report	1) Public	1) Public	1) Connect SQL 2) View server state	- 'View server state' is required to get information from 'master..sysprocesses' - Reference link
Security Changes Report#	1) Public	1) Public	1) Connect SQL 2) Alter trace	- 'Alter trace' permission is required to get information from 'sys.fn_trace_ getinfo' and 'sys.fn_trace_gettable' - Reference link for sys.fn_trace_ getinfo - Reference link for sys.fn_trace_ gettable - Reference link for sys.trace_events
Permissions Information Report#	1) Public	1) Public	1) Connect SQL 2) View any definition	- 'View any definition' permission is required to get information from 'sys. database_principals', 'sys.database_ permissions', sys.columns', 'sys.objects' and 'sys.database_role_members' - If 'View any definition' is not provided, then information of only the current user name, the system users, and the fixed database roles will be retrieved - Reference link for sys.database _principals - Reference link for sys. database_ permissions - Reference link for sys.columns - Reference link for sys.objects - Reference link for sys. database_ role_members

Last Backup of Database	1) Public	1) Public	1) Connect SQL	- Information is retrieved from 'msdb.dbo.backupset' and 'msdb.dbo.backupmediafamily'
Last DBCC Activity	1) Sysadmin	1) Sysadmin	1) Connect SQL	- 'sysadmin' permissions required to run "DBCC TRACEON()" command - Reference link for 'DBCC TRACEON'

Our Products

AD360 | Log360 | ADAudit Plus | DataSecurity Plus | Exchange Reporter Plus

SharePoint Manager Plus

ManageEngine
EventLog Analyzer

ventLog Analyzer is complete log management software that provides holistic cybersecurity. It collects, analyzes and manages log data from over 700 log sources. With real-time security auditing capabilities, it’s easier to monitor critical changes in all your end-user devices. EventLog Analyzer offers instant threat detection to uncover security threats using event correlation and threat feed analysis, and instant mitigation using automated workflows. For more information about EventLog Analyzer, visit manageengine.com/products/eventlog/.

$ Get Quote

Download