ManageEngine
EventLog Analyzer

EventLog Analyzer

Requirements Guide

www.eventloganalyzer.com

Table of contents

1. Log collection

The first step in log management is collecting log data. Log collection can be an arduous task because some systems such as firewalls, intrusion detection systems, and intrusion prevention systems have EPS (events per second) that generate large amounts of log data.

To collect and process log data in real time, regardless of the volume of log data and the number of devices in the network, organizations need a robust log collection mechanism.

EventLog Analyze requires the following ports, permissions, etc., to collect logs seamlessly and generate real-time alerts.

Ports, rights, and permissions Required

Ports	Protocols	UserGroups	User Rights	User Permissions	Environment Permissions
WMI Log Collection					
135,445,139 Dynamic ranges of RPC ports - 1024 to 65,535	TCP	*Event Log Readers *Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token *Manage Auditing and Security Log Properties	*Enable Account *Remote Enable *Read Security	WMI log collection using a non-admin domain user
Syslog Collection					
513,514 514 513	UDP TCP TLS				The ports mentioned should be allowed in firewall
AS400 Log Collection					
446-449, 8470-8476, 9470-9476	TCP TCP TCP				The credentials provided must have an authority level of 50. Otherwise, EventLog Analyzer will not be able to login to fetch History logs from these devices.

Auto Log Forwarding					
22	SSH		Service restart rights for '**rsyslog**' or '**syslog**' service	Enable "**rw**" permission to files (**/etc/ rsyslog.conf** or **/etc/syslog.conf)**	
SNMP Trap Collection					
162	SNMP				
IIS Log Collection					
135,139,445	SMB			*Enable read access to the IIS log folder and *Permissions for the system 32/inetsrv	

2. Agent orchestration

EventLog Analyzer Agent collects event logs generated by Windows devices. Installation and set up of EventLog Analyzer Agent to collect and report on event logs from Windows devices is a simple process. When the agent is installed, the result status 'Success/Failed <with reason>/Retry' will be displayed. In case of failure of automatic installation of agents, manual installation is possible. The agent can be deployed in any server in the network or sub-net. It is installed as a 'Service' in that server.

Agents will be automatically discovered by EventLog Analyzer server and the agents will automatically collect the logs from Windows devices. The agent remotely collects the logs. It pre-processes and transfers the logs to the server in real-time and in an uninterrupted manner.

The agent can collect the logs from up to 25 devices. Devices can be assigned to any agent for log collection as required and also logs can be directly collected by the EventLog Analyzer server with out the agent. Devices can be unassigned from one agent and assigned to another device as per your requirement.

In order to facilitate seamless agent installation, the following ports, permissions, etc., are required.

Ports	Protocols	UserGroups	User Rights	User Permissions	Environment Permissions
Windows Agent Installation					
135, 1024 - 65534	DCOM, WMI, RPC			Enable **read,write** and **modify** permissions to files in (**\\Admin $\\TEMP**) Exact location	WMI and DCOM permissions are needed to set WMI connection, create a process and install MSI.

139,445 [SMB] 135[RPC] 1024-65535[RPC]	Remcom (SMB) RPC			**\Admin$\\TEMP\\EventLogAgent.** Access to remote registry and "Remote Registry" service should be up.	**Remcom** Remote Administration should be enabled i.e, We should be able to execute command in remote machine by connecting through username and password.
Windows Agent Management					
135 1024 - 65535	RPC			*At least **read** control should be granted for winreg registry key *(Computer \HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\Control\ SecurePipe Servers\winreg).* *Access/Read /Write registry keys - **SOFTWARE\\Wow6432Node\\ZOHO Corp\\EventLog Analyzer\\ (or) SOFTWARE\\ZOHO Corp\\EventLog Analyzer\\** There should be access to remote services.msc.	Access to service named "Remote Registry"
Windows Agent Communication					
8400 (webserver port)	HTTP				The web server ports of both agent and server should be open
Linux Agent Installation					
22	SSH			*SFTP "**rw**" permissions to transfer files to **/opt/ManageEngine/EventLogAnalyzer_**	

				Agent and /etc/audisp/ plugins.d *Service start/ stop/restart permission for *auditd.*	
Linux Agent Management					
22 8400	SSH HTTP HTTPS			*SFTP permissions to transfer files to **/opt/ManageEngine/EventLogAnalyzer_Agent and /etc/audisp/plugins.d***Service start /stop/restart permission for *auditd.*	
Linux Agent Communication					
8400 (webserver port)					The web server ports of both agent and server should be open

Note:

These ports and permissions (except communication) are non-mandatory. Manual installation can be done.

3. SQL Server as backend database

While using SQL Server as your back end database, the following ports, permissions, etc., are required.

Stage	Required Minimum Permission for Login			Other Requirement	Remarks
	Server Roles	User Mapping	Securables		
Change DB to SQL Server	1) public 2) dbcreator	-N/A-	1) Connect SQL		- 'dbcreator' is required to create 'eventlog' database. If it is not provided, *"CREATE DATABASE permission denied in database master'"* error will be shown

Cold Start (First Start)	1) public	1) public 2) db_owner	1) Connect SQL		

Warm Start	1) public	1) public
		2) db_datareader
		3) db_datawriter
		4) db_ddladmin
		5) db_backupoperator
			1) Connect SQL	1) Control privilege on the created certificate, execute following queries:-
				GRANT CONTROL ON SYMMETRIC KEY::[##MS_DatabaseMasterKey##] TO [user]; -- if not provided, user will not know if a master key exists in DB
				GRANT CONTROL ON SYMMETRIC KEY::[ZOHO_SYMM_KEY] TO [user];
				GRANT CONTROL ON CERTIFICATE::[ZOHO_CERT] TO [user];
					'db_backupoperator' is required *only* if the user wishes to back-up the 'eventlog' database
					- For the queries, substitute [*user*] with required *Login* name

4. Importing logs

You can import logs in EventLog Analyzer. However in the case of Oracle, Print Server, and IBM iSeries applications logs can be fetched in real-time. The software can import the application logs automatically at regular interval. Alternatively, using FTP you can transfer the application logs to a host machine that is monitored by EventLog Analyzer and then using HTTP the same application log can be imported into EventLog Analyzer from the host machine. EventLog Analyzer will also import the log files with periodical file name change. Optionally, you can associate the imported log file with the existing host.

You can import logs using either Server Message Block (SMB) or File Transfer Protocol (FTP).

Ports	Protocols	UserGroups	User Rights	User Permissions	Environment Permissions
Importing Logs using SMB					
139,445 137,138	SMB TCP, UDP			***Network access: Do not allow anonymous not allow anonymous enumeration of SAM accounts and shares** property in local security policy should be disabled. *Sometimes, connecting to different workgroups need credentials even to view the shared resources.	***File and Printer Sharing (SMB-In)** (local port 445) and **File and Printer Sharing (NB-Session-In)** (local port139) inbound rule should be enabled. ***SMB 1.0/SMB 2.0/CIFS File Sharing Support** in windows features should be enabled. ***Function Discovery Provider Host and Function Discovery Resource Publication** services should be running. ***File and Printer Sharing and Internet Protocol** should be enabled in LAN properties.
Importing logs using FTP					
20,21	FTP			Authentication for the FTP server should be enabled.	ftpsvc service should be running on the server.

5. Discovery

a. Event Source Discovery

Ports	Protocols	UserGroups	User Rights	User Permissions	Environment Permissions
Event Source Discovery					
139,445 135,137,138	SMB,Rem com RPC			*At least **read** control should be granted for winreg registry key*(Computer \HKEY_LOCAL _MACHINE\ SYSTEM*	*Remote registry service should be running. *Should have files in event file location (C:\ Windows\System 32\winevt\Logs).

				CurrentControlSet\Control\SecurePipeServers\winreg) *Full control permission should be granted for credentials in the EventLog registry key (Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog). *In the registry Key (Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System), LocalAccountTokenFilterPolicy should be enabled while using local accounts other than domain accounts.	

b. MySQL Discovery

MYSQL SERVER DISCOVERY - LINUX					
22	SSH,SFTP			*Read permission to the MySQL server configuration file using SFTP	
MYSQL SERVER DISCOVERY-WINDOWS					
135 445	TCP SMB			*WMI permission is needed to find the MySQL server configuration file using SFTP	

				Read Permission to the MySQL server configuration file using SFTP	

c. Windows domain discovery

Windows Domain Discovery					
389	LDAP			*User should have read permission to Active Directory Domain Objects *Permission to run LDAP query in ADS_SECURE_AUTHENTICATION mode should be present.	

d. Windows workgroup discovery

Windows Workgroup Discovery					
135,139,445 1024-65535	SMB RPC			*User should have read permission to Active Directory Domain Objects *Permission to run WinNT query in **ADS_SECURE_AUTHENTICATION** mode.	

e. IIS discovery

Port Numbers	Ports Usage
445 (TCP)	The Server Message Block (SMB) protocol uses this port to read the log files.

f. Network device discovery

Port Numbers	Ports Usage
162 (SNMP ersion v1, v2, v3)	Fetches a list of live SNMP-enabled IP devices that responds to the SNMP ping.

6. 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	
DDL/DML AUDITING (including extended events)				
-N/A-	1) public 2) serveradmin	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 "<DB name>" 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
Delete Operations Report	1) public 2) sysadmin	1) public	1) Connect SQL	'sysadmin' permission is required to run 'fn_dblog'
Logins Information Report#	1) public	1) public	1) public 1) Connect SQL 2) 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 1) Connect SQL 2) 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) public	1) Connect SQL	- 'sysadmin' permission is required to run "DBCC TRACEON()" command - Reference link for 'DBCC TRACEON'

# - Visibility of the metadata in catalog views is limited to securables that a user either owns or on which the user has been granted some permission. Thus, for some reports, 'VIEW ANY DEFINITION' permission was finalized.

7. Incident workflow management

Quickly detecting security threats and mitigating attacks is the fundamental objective of any security operations center. The time it takes to detect and respond to security incidents should be as short as possible in order to limit the time an attacker has to carry out the attack. EventLog Analyzer's real-time alerting system, along with its integrated incident management console, empowers you to instantly identify and handle any security event of interest in your network, including attacks. Configure real-time alerts for threat indicators, so you can quickly manage incidents as soon as they occur.

EventLog Analyzer allows you to automate incident response through the use of incident workflows. An incident workflow describes a series of automated measures to be taken in response to a security incident. You can create multiple incident workflows using the flexible workflow builder and assign each of them to one or more security incidents.

EventLog Analyzer requires the following permissions to handle incident efficiently.

BLOCK	OS Type	Ports	Proto col	User Permission	User Groups	User Rights	Environment Permission
NETWORK ACTIONS							
PING DEVICE	BOTH	No ports	ICMP	-	-		-
TRACE ROUTE	Windows	No ports	ICMP	-	-		-
	Linux	33434 -33534	UDP	-	-		-
PROCESS ACTIONS							
Start Process	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM,	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	-
	Linux	port specified.	SSH				The user whose credentials provided should have permission to execute the command.

Stop Process	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM,	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	*If the user is not administrator, processes started by other users cannot be stopped.
	Linux	port specified.	SSH				If the user used is not a root user, user can't kill system processes or processes that was started by other users
Test Process	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	operating system *Log on as a batch job *Log on as a service *Replace a process level token	
	Linux	port specified.	SSH				
SERVICE ACTIONS							
All Service Block	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users *Administrators	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	
	Linux	port specified.	SSH				Sudoers permission
WINDOWS ACTIONS							
LogOff	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	*The computer should not be EventLog Analyzer Installed server.

Shutdown and Restart	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM,	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Allow force shutdown from remote computer *Act as part of the operating system *Log on as a batch job *Log on as a service	*The computer should not be EventLog Analyzer Installed server.
Execute windows Script	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM, SMB	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	*The user should have read,write and modify access to the shared path in the script.
Disable USB	Windows	135,139, 445 RPC ports - 1024 to 65,535	TCP, DCOM, SMB	For **root\default** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	*Remote Registry Service should be running. *Full Control permission to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR**
LINUX ACTIONS							
Shutdown and Restart	Linux	port specified.	SSH				The user should be root user.
Execute Linux Script	Linux	port specified.	SSH, SFTP	User should have **'rwx'** permission in the mentioned directory			Sudoers permission for user.

NOTIFICATIONS							
Pop Up	Windows	135 RPC ports - 1024 to 65,535	TCP	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	**"AllowRemoteRPC"** should be 1 for **HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\Terminal Server**
	Linux	port specified.	SSH				sudoers permission
Send Email	Both	port mentioned while configuring SMTP server	SMTP				SMTP server should be configured on Eventlog analyzer server
Send SMS	Both						SMS Server should be configured in the product.
Send SNMP Trap	Both	Port specified in workflow block	SNMP				The port mentioned in workflow configuration should be open.
AD ACTIONS							
Delete AD User	Both	389	LDAP	*The user should have "Delete" Right in the AD to delete other Accounts. * The user to delete should not have "Protect Object from accidental deletion" checked.			*User to delete should not be present in the exclude list *Domain should have been added in the product. *The given username should be unique in the domain.
Disable AD User	Both	389	LDAP	The User account provided should have "Read","Write","modify owners" and "modify permissions" permissions enabled.			*User to delete should not be present in the exclude list *Domain should have been added in the product. *The given username should be unique in the domain.

Disable User Computer	Both	389	LDAP	The User account provided should have "Read", "Write" , "modify owners" and "modify permissions" permissions enabled.			*Should not be localhost. *Computer to disable should not be present in the exclude list.
Miscallanous							
Write to File	Windows	135 RPC ports - 1024 to 65,535	TCP	For **root\cimv2** In COM Properties *Execute Methods *Enable Account *Remote Enable *Read Security	*Distributed COM Users	*Act as part of the operating system *Log on as a batch job *Log on as a service *Replace a process level token	*The user should have read,write and modify access to the shared path.
	Linux	port specified.	SSH, SFTP	User should have '**rwx**' permission to specified path			sudoers permisssion Needed
HTTP Webhook	Both			A "connect" SocketPermission to the host/port combination of the destination URL or a "URLPermission" that permits this request.			ReferenceUrl
Forward Logs	Both	Specified Port	Specified Protocol				
CSV Lookup	Both	Specified Port	Read permission to the specified CSV file.				

8. Distributed communication Setup

EventLog Analyzer Distributed Edition is a distributed setup of EventLog Analyzers.
It consists of one Admin server and N number of Managed servers. The Managed servers are installed at different geographical locations (one or more per LAN environment) and are connected to the Admin server. This allows the network administrators to access the details of the hosts at different remote locations in a central place. All the reports, alerts and other host information can be accessed through one single console. The administrator of large enterprises with various branch locations through out the globe stand benefited with this edition. For Managed Security Service Providers (MSSP) it is a boon. They can monitor the Managed server installed at different customer places from one point.

Ports	Protocols	UserGroups	User Rights	User Permissions	Environment Permissions
1. Webserver ports					
8400 (default)	HTTP			The admin and managed server ports should be open. The default port number is 8400. This can be customized.	If customized, the respective port number should be kept open.
2. Centralized Archiving Ports					
8080 (default)	SSH			User can customize the port. The value should be between 1024 and 65535	If enabled, the following firewall changes are required : In Admin Server, the Inbound Rules should be allowed for the Admin Server IP (SSH Port). In the Manage Server, the Outbound Rules should be allowed for Admin Server IP (SSH Port).

9. Miscellaneous

1. Web Server Ports

Port Numbers	Ports Usage
8400 (HTTP)	By default, the ports will be used for commnication between agents and server and also for communication between Admin server and managed server

2. Internal Communication

Port Numbers	Ports Usage
5000,5001,5002 (UDP)	EventLog Analyzer uses these UDP ports internally for agent to server communication. Ensure that the ports are free and not occupied by other local applications running in the machine. Some additional higher range ports (1024-65534) will be opened to connect with these ports for internal communication.

3. Elasticsearch

Port Numbers	Ports Usage
Any port in range 9300-9400 (TCP)	This is the port used by Elasticsearch server in EventLog Analyzer.

4. Database

Port Numbers	Ports Usage
33335 (TCP)	PostgreSQL/MySQL database port. This is the port used for connecting to the PostgreSQL/MySQL database in EventLog Analyzer.

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

For more information about EventLog Analyzer, visit manageengine.com/eventloganalyzer.

$ Get Quote

Download