ALERTLOGIC
Security. Compliance. Cloud.

WHITEPAPER

# Alert Logic Log Manager

## Configuring Log Sources for Best Practice Reports

CONTENTS



1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.838 | info@alertlogic.com | www.alertlogic.com

# Introduction

A well-defined log management process enables organizations to deal with the large volumes of computer-generated log messages generated each day. By collecting, aggregating, parsing and analyzing these messages, you can better understand what's happening with systems in your IT environment and extract real value from the information for performance, security, compliance and other purposes.

The purpose of this white paper is to outline a set of best practice reports that can be created from a repository of centralized log data and show the configuration steps needed to generate events for these best practice reports.

The report and configuration examples come from Alert Logic Log Manager. Log Manager is a software-as-a-service based log management solution that collects, parses, and normalizes the millions of data points that are embedded in applications and IT infrastructure logs. Reports are presented back to you in an easily understandable, searchable format that can be used for compliance purposes or for further alerting of suspicious log activity.

For more information on Log Manager, visit https://www.alertlogic.com/products-services/log-manager/.

For more detail on configuring Log Manager to collect log data, documentation is available at http://docs.alertlogic.com/.

# Best Practice Reports Available in Alert Logic Log Manager

## Active Directory (AD)

**Active Directory Global Catalog Change** – The Microsoft Active Directory Global Catalog provides searchable information about every object controlled within your AD forest. Additionally, it provides the ability to search across multiple different domains without being required to access the AD for each domain directly. This report details all changes to the AD Global Catalog that are recorded as log messages.

**Active Directory Global Catalog Demotion** – The Microsoft Active Directory Global Catalog provides searchable information about every object controlled within your AD forest. Additionally, it provides the ability to search across multiple different domains without being required to access the AD for each domain directly. This report provides log message details each time a domain controller in your AD forest has been demoted, and can no longer serve the global catalog.

## Databases

**Database Failed Logins** – This report is generated to identify and display database login failure log messages received from all monitored hosts. This report is applicable to Oracle and SQL Server.

## Network Devices

**Network Device Failed Logins** – This report is generated to identify and display network device login failure log messages received from all monitored hosts.

**Network Device Policy Change** – This report is generated when a policy is added/changed/removed on network devices.

## Windows Server (2008 R2, 2008, 2003)

**Excessive Windows Account Lockouts** – This report is generated when a threshold of two log messages has been exceeded. The messages indicate that Windows user accounts have been locked out.

**Excessive Windows Account Lockouts by Administrative User** – This report is generated when a threshold of two log messages has been exceeded. The messages indicate that the Windows Administrator account has been locked out.

**Excessive Windows Failed Logins** – This report is generated to identify and display excessive Windows login failure log messages received from all monitored hosts with a threshold greater than five messages.

**Excessive Windows Failed Logins by Administrative User** – This report is generated when an excessive number of Windows login failure log messages are received from a single host for the Administrator account. The threshold is more than five messages.

**Windows FTP Failed Logins** – This report is generated when log messages indicate that accounts have failed to successfully login to IIS.

**Windows User Account Created** – This report is generated when log messages indicate that user accounts have been successfully created.

**Windows User Account Modified** – This report is generated when log messages indicate that user accounts have been modified (changed, created and deleted).

**Windows User Group Created** – This report is generated when log messages indicate that a user group has been created.

**Windows User Group Modified** – This report is generated when log messages indicate that user groups have been modified (changed, created and deleted).

## UNIX/Linux

**Failed UNIX Switch User Command** – This report provides details of all recorded failed uses of the UNIX switch user (su) command.

**UNIX Account Created** – This report is generated when log messages indicate the creation of UNIX accounts.

**UNIX Failed Logins** – This report is generated when log messages indicate that local and remote accounts have failed to successfully login.

**UNIX Group Created** – This report is generated when log messages indicate that a UNIX user group was added.

UNIX SSH Failed Logins – This report is generated to identify and display SSH login failure log messages received from all monitored hosts.

**UNIX Sudo Access** – This report is generated when a user has executed the UNIX sudo command.

**UNIX Switch User Command Success** – This report is generated when log messages indicate that a user has successfully executed the UNIX switch user (su) command.

# Configure Logging per Platform

## Active Directory

To generate logs messages from Microsoft Active Directory, you need to make changes to the Audit Policy of a Domain Controller with a Domain Administrator login account.

You can configure the Audit policy settings in the following location on the Domain Controller:

Administrative Tools →Domain Controller Security Policy →Security Settings →Local Policies →Audit Policy

There are nine different kinds of events you can audit. To generate meaningful log events that will populate the best practice reports above, here are the settings that should be configured:

| | Success | Failure |
|---|---|---|
| Audit account logon events | • | • |
| Audit account management | • | • |
| Audit directory service access | • | • |
| Audit logon events | • | • |
| Audit object access | | |
| Audit policy change | • | • |
| Audit privilege use | • | • |
| Audit process tracking | | |
| Audit system events | • | • |

## Databases

### MySQL

MySQL logging configuration will vary based on the installed platform. The steps to enable logging for MySQL for Linux and Windows are outlined below.

*Linux*

- Most current versions of MySQL have logging enabled by default. Check /var/log/ directory to ensure logging is enabled.

*Windows*

1. Open the MySQL Administrator and connect to the MySQL server as an administrative user.
2. Click Startup Variables (Windows) or Options (Mac). The first step will be to enable logging, which can be done within this area of the application.
3. Enable login success and failure auditing.

## Microsoft SQL Server

Microsoft SQL Server logging configuration is performed in both SQL Server Management Studio and Windows Audit Policy. The steps are outlined below.

» SQL Server Management Studio

1. Connect to SQL Server in Object Explorer.
2. Right-click SQL Server →Properties.
3. Go to **Security** page.
4. Select **Both failed and successful logins** under **Login auditing** section.
5. Click **OK**.

» Once the above steps are followed to enable auditing within Miscrosoft SQL Server, you will also need to configure some settings at the Windows Server level.

- You can configure the Audit policy settings in the following location on the DB server:
- Administrative Tools →Local Security Policy →Security Settings →Local Policies →User Rights Assignment

1. Double click **Generate security Audits**.
2. Click **Add User or Group**.
3. Click **Object Types** →Check **Computers** and click **OK**.
4. Type the **name of the current database server** into the "Enter the object names to select" field and click **Check Names**.
5. Once the computer name is resolved (it will display an underlined computer name), click **OK**.
6. Click **OK** to close the Generate security audits Properties window.

- Administrative Tools →Local Security Policy →Security Settings →Local Policies →Audit Policy

1. Double click **Audit object access**.
2. Select **Success and Failure**.
3. Close the Local Security Settings window.

- Microsoft SQL Server will start posting logs to the Application log of the server after the next reboot of the server.

## Network Devices

### Cisco ASA and PIX Firewall

By default logging is disabled, and must be enabled.

» Enable message logging:

| Begin sending logging messages to all configured destinations: | |
|---|---|
| FWSM 2.x | Firewall(config)# logging on |
| PIX 6.x | Firewall(config)# logging on |
| PIX 7.x | Firewall(config)# logging enable |

» (Optional) Limit rate in which logging messages are generated:

- FWSM 2.x : Firewall(config)# logging rate-limit {unlimited | number [interval]} {level level | message message_id}
- You can rate-limit messages generated by using level keywords. Alert Logic recommends rate limiting notifications, informational and debugging (5-7):
  - emergencies (0)
  - alerts (1)
  - critical (2)
  - errors (3)
  - warnings (4)
  - notifications (5)
  - informational (6)
  - debugging (7)

### Juniper Firewall

In /var/netscreen/GuiSvr/guiSvr.cfg change the following:

- Find the following:
  - guiSvrManager.auditlog_flag 0
  - guiSvrManager.auditlog_detail_flag 0
- Change to the following:
  - guiSvrManager.auditlog_flag 1
  - guiSvrManager.auditlog_detail_flag 1
- Restart NSM services: /etc/init.d/guiSvr restart
- If firewalls are configured for High Availability:
  - Stop the secondary: /etc/init.d/haSvr stop
  - Restart the primary: /etc/init.d/haSvr restart
  - When the primary is started , Start the services on the secondary: /etc/init.d/haSvr start

## Windows Server (2008 R2, 2008, 2003)

To generate log messages from standalone Windows servers, you need to make changes to the Audit Policy.

You can configure the Audit policy settings in the following location on each server:

Administrative Tools →Local Security Policy →Security Settings →Local Policies →Audit Policy

There are nine different kinds of events you can audit. To generate meaningful log events that will populate the best practice reports above, here are the settings that should be configured:

| | Success | Failure |
|---|---|---|
| Audit account logon events | • | • |
| Audit account management | • | • |
| Audit directory service access | • | • |
| Audit logon events | • | • |
| Audit object access | | |
| Audit policy change | • | • |
| Audit privilege use | • | • |
| Audit process tracking | | |
| Audit system events | • | |

## UNIX/Linux

To generate log messages from UNIX/Linux servers, you need to use syslog. UNIX/Linux servers should already have this configured by default.