WHITEPAPER

motadata

Log Management Delivers Intelligence with Speed

Contents

Log Management Delivers Intelligence with Speed....1
Introduction - Log Data Matters....3
Log Management is an Integral Part of IT and Security Operations....4
Intelligence that can be received from Log Management....5
Traditional Approach or New Approach....5
Architected with Openness....8
Be Proactive than Reactive....8
Summary....9
Try Before You Buy....9
What’s Next?....9

Introduction - Log Data Matters

Logs such as audit records, intrusion alerts, transaction logs, connection logs, system performance records, event-logs, user activity logs, etc. are generated by nearly every computing device, applications, and databases. With the growing complexity (cloud, virtualization, BYOD, compliances, multiple databases etc.), and in many cases “organically grown architecture”, logs have become an integral part of IT infrastructure monitoring and compliance process.

Network devices, servers, databases, and applications generate log data on a variety of events and processes, from simply stating “all okay” or “there is an issue”. The key is to derive intelligence out of it i.e. knowing what needs to be monitored and managed. Having the right kind of tool or software makes it easier to monitor, report and take corrective actions from bulk log data.

IT departments should view Log data management as an opportunity to turn data into an insights but not as a challenge of large amount of structured and unstructured data.

Volume: Log data is capable of occupying nearly terabytes of data per day in case of a large organization. Just collecting, centralizing and storing data at this volume may turn out to be difficult.

Normalization: Every computing device produces a log in a different format, a common output format is derived using normalization.

Examples:

Apache HTTP Server Error Log:

Log body:

```
[Wed Oct 11 14:32:52 2000] [error] [client
127.0.0.1] client denied by server
configuration:
/export/home/live/ap/htdocs/test
```

Fortinet Firewall Log:

Log header:

```
2011-01-08 12:55:06 log_id=24577 type=dlp
subtype=dlp pri=notice vd=root
```

Log body:

```
policyid=1 identidx=0 serial=73855
src=“10.10.10.1” sport=1190 src_port=1190
srcint=internal dst=“192.168.1.122” dport=80
dst_port=80 dst_int=“wan1” service=“https”
status=“detected” hostname=“example.com”
url=“/image/trees_pine_forest/” msg=“data
leak detected(Data Leak Prevention Rule
matched)” rulename=“AllHTTP” action=“log-
only” severity=1
```

Velocity: The speed at which logs are produced from systems can make collection and aggregation difficult. The speed unit that is being used is called EPS - Event Per second.

Veracity: Log events may not be accurate. This is particularly problematic for systems that carry out the activity of detection, such as intrusion detection systems.

As the saying goes *“Devil is in the details”* so deriving intelligence and correlating log data from the network (servers, routers, switches), applications, databases are very valuable to both NOC (Network Operations Center) and SOC (Security Operations Center) teams. Here are few examples -

How quickly can you find root-cause of performance degradation of an application server?

How quickly can you identify an unauthorized file access or attack?

Log Management is an Integral Part of IT and Security Operations

Log management comprises of the complete collection of log, aggregation, original (unhampered) log retention; log text analysis; presentation (mostly in the form of search and reporting); related workflow (notifications, alerts, corrective action) and content. With log management, the use cases are broad and cover every possible use for log data across IT infrastructure and even beyond.

There are quite a few differences between SIEM and Log Management. But the primary difference being SIEM focusing on security—the first word in "Security Information and Event Management"—and utilization of various IT information for security purposes. Meanwhile, log management is all about logs and across the board use of log data, both within as well as outside the security domain with several use cases of log data, it is important for both operations teams (NOC) and for security teams (SOC).

Monitoring and Availability – Production

Fast analysis of issues - debug or diagnosis of systems and apps when they crash, slow down or any kind of malfunction

Troubleshooting and debugging – during production and development

Debugging or analyzing exceptions, errors, and events

Business Analytics

Every detail starting from the number of transactions per hour to details on the value of individual transactions

Security & Compliance

Log data is necessary for forensic analysis of security events and for detection & countering of attacks before damage is done.

An intelligent log management tool exposes the events that were buried in those logs and brings them to the surface, especially if you want to set up connections between events recorded in different logs for related systems.

From the security perspective, the importance is that attackers often exploit multiple vulnerabilities on separate but connected systems. With current distributed applications, the challenge of troubleshooting more routine failures or slowdowns is not very different—normally the breakdown is the connection between two systems, in spite of just one or the other. The investigation may be initiated by looking at the web server. Checking the logs can help to show that the problem is actually with the database server or vice versa.

Assuming wrong will lead to loss of valuable time which is not only impacting productivity but also a business.

That's why it's important to root-cause the problem as fast as possible.

Intelligence that can be received from Log Management

A system administrator would utilize Log Management software in along with other specialized software, like those used for monitoring networks, applications, and databases. The unique benefit of Motadata is breadth and its unified approach (Integrated Monitoring & Log Management) — it can track activity from most type of systems (includes applications, devices, database etc.) and discover patterns that span over multiple systems

Here are few examples of real-life use cases of Log Management that we are confident you can relate to

Operations

Software installs, updates or configuration changes made just before a server or application failure. Cause and effect?

Top 10 error messages reported on the server over the past hour, day, or week.

Performance

Web application response time, broken out on a per-page or per web service basis

Virtual machines created, started, stopped, or moved, along with log data on the performance of the hypervisor regulating this activity.

Security/Access/Change Management

List of users who logged into the server most recently, either overall or at a specific access level, such as admin.

Audit trail of files accessed, added, or modified.

Inappropriate file or database access, such as someone from marketing attempting to access HR records.

File or database record permission changes.

Devices added to or removed from the network.

Active Directory® changes, including users or groups added, deleted, or modified.

Network traffic patterns and activity directed at specific server ports.

Connections permitted or denied by firewall rules.

Compliance

Events tracked in specific submission reports for regulatory/compliance needs, like PCI, HIPAA, SOX, and many others.

Traditional Approach or New Approach

When the problem occurs, the usual practice is to look into logs for any available insights but the challenge is there are so many logs and all are dispersed unless they have been centralized.

Almost all information is recorded in some log. The challenge is how to find that information, usually scripts are written to extract that information. Motadata's capability provides an easy way to find information out of logs and correlating that information.

In lieu of working with raw logs, Motadata presents a merged database of events pulled into logs, compressed into a tamperproof database, normalized and optimized for search and intelligent enough to help you identify meaningful correlations. For instance, you can see the relationships of web application server and database events documented in separate logs and the sequence in which they occurred.

Motadata helps you sort through the noise embedded in log data and identify the events which are most significant. Motadata lets you see what other events occurred immediately before or after and then put those series of events related to the problem together. Similarly, you can start your search with the IP address of the web server front end of a malfunctioning application.

Motadata also presents the log data from the associated systems such as the database back end. So even if you were certain at the outset, that the problem was on the web server, you would instantly check to see in case the database server was generating any sort of error messages, suggesting where you should continue your search for clues.

Here are two examples:

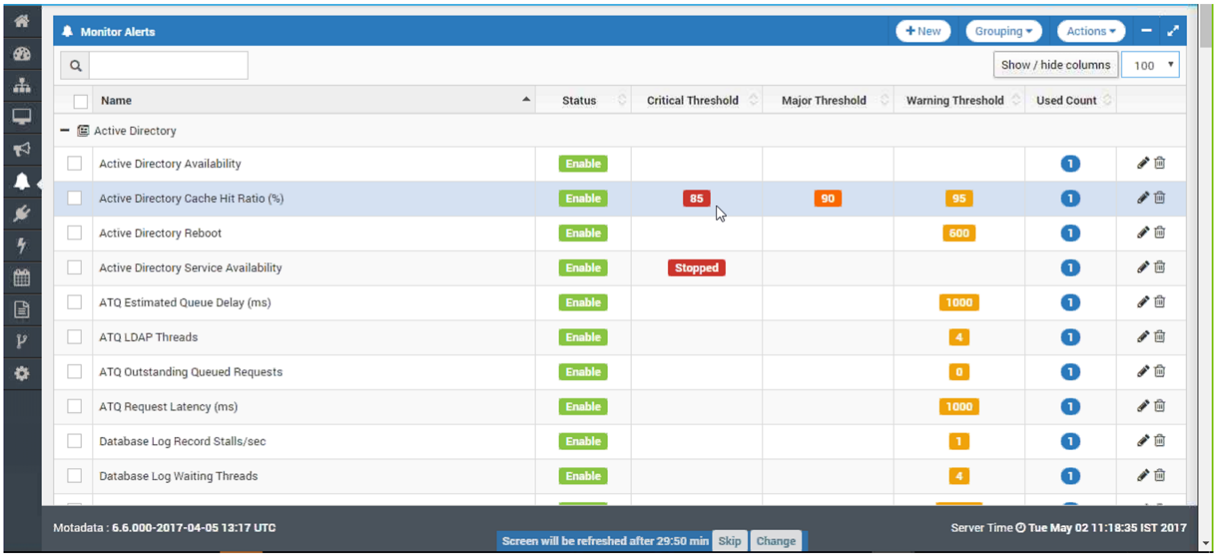
Example # 1 - You would like to find out why your intranet went down during your CEO's live-cast to all employees. Here is what you could find out by using Motadata's Log Management and Network Monitoring software

Log Management – Change was made in firewall rule and that port was exposed to a new service

Networking Monitoring: A surge in web server's CPU utilization, peaking at 99% and rebooting itself

Example # 2 -

From the security perspective, it is very important to get alerted on key events such as



□	Name	Status	Critical Threshold	Major Threshold	Warning Threshold	Used Count
−	Active Directory					
□	Active Directory Availability	Enable				1
□	Active Directory Cache Hit Ratio (%)	Enable	85	90	95	1
□	Active Directory Reboot	Enable			600	1
□	Active Directory Service Availability	Enable	Stopped			1
□	ATQ Estimated Queue Delay (ms)	Enable			1000	1
□	ATQ LDAP Threads	Enable			4	1
□	ATQ Outstanding Queued Requests	Enable			0	1
□	ATQ Request Latency (ms)	Enable			1000	1
□	Database Log Record Stalls/sec	Enable			1	1
□	Database Log Waiting Threads	Enable			4	1

Motadata : 6.6.000-2017-04-05 13:17 UTC

Screen will be refreshed after 29:50 min Skip Change

Server Time Tue May 02 11:18:35 IST 2017

Figure 1 OOB Alerts

Alert me when AD is not available

Alert me when AD (Active Directory) user is deleted

Alert me when AD user is created/modified

Alert me on DDoS attack on AD i.e. log-in failed for a specific user more than 5 times in last 10 seconds

Alert me when unauthorized access attempted

A notification can be received when someone is abusing his or her access rights since AD log will capture access event with username and file names.

Architected with Openness

Motadata's server receives all logs which are being forwarded and it analyses logs to derive intelligence and correlation of data.

Motadata's Log Management has the ability to compress original log data, indexing, and normalizing data. This makes it easy to see correlations between or among events recorded by different systems. The original log data is stored so that you can always refer back to it after discovering a significant event.

Motadata is implemented in the form of a virtual appliance, a ready-made virtual machine image you can execute on VMware® ESX® or Microsoft® Windows® Hyper-V® or Bare Metal hardware. A Motadata instance includes a hardened operating system and a combination of column-based database and the elastic search engine for data storage and retrieval. Once recorded, data becomes read-only, making it a trustworthy source for audits and compliance review.

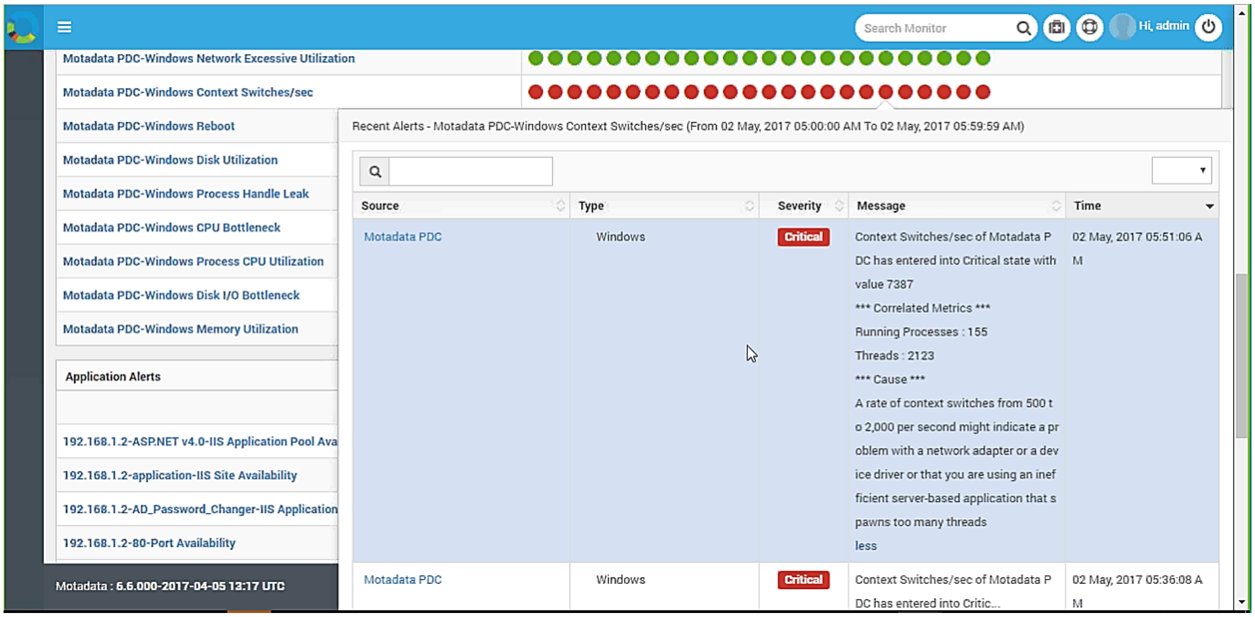
Be Proactive than Reactive

Prevention is better than cure. It is important to detect the real issue at the right time but it is more important to get hold of the issue ahead of the time.

Motadata can be configured to detect important events, such as the shutdown of a critical system, and alert you immediately.

With our integrated "Remedy Actions", you can also define rules that dictate actions to be performed automatically.

For instance, Windows agents can be modified to restart applications that crash or freeze automatically. Other possible actions involve blocking of an access from a specified IP, shutting down a service, or deactivating a user account.



Motadata PDC-Windows Network Excessive Utilization
Motadata PDC-Windows Context Switches/sec
Motadata PDC-Windows Reboot
Motadata PDC-Windows Disk Utilization
Motadata PDC-Windows Process Handle Leak
Motadata PDC-Windows CPU Bottleneck
Motadata PDC-Windows Process CPU Utilization
Motadata PDC-Windows Disk I/O Bottleneck
Motadata PDC-Windows Memory Utilization

Application Alerts

192.168.1.2-ASP.NET v4.0-IIS Application Pool Ava
192.168.1.2-application-IIS Site Availability
192.168.1.2-AD_Password_Changer-IIS Application
192.168.1.2-80-Port Availability

Motadata : 6.6.000-2017-04-05 13:17 UTC

Recent Alerts - Motadata PDC-Windows Context Switches/sec (From 02 May, 2017 05:00:00 AM To 02 May, 2017 05:59:59 AM)

Source	Type	Severity	Message	Time
Motadata PDC	Windows	Critical	Context Switches/sec of Motadata PDC has entered into Critical state with value 7387 *** Correlated Metrics *** Running Processes : 155 Threads : 2123 *** Cause *** A rate of context switches from 500 to 2,000 per second might indicate a problem with a network adapter or a device driver or that you are using an inefficient server-based application that spawns too many threads less	02 May, 2017 05:51:06 AM
Motadata PDC	Windows	Critical	Context Switches/sec of Motadata PDC has entered into Critic...	02 May, 2017 05:36:08 AM

Figure 2 RCA with correlated metrics

Motadata also comes with Root Cause Analysis (RCA) along with correlated metrics -

Problem Statement/ Issue: Context Switches/sec of 192.168.2.135 has entered into Major state with value 1679

Correlated Metrics:

Running Processes: 72

Threads: 895

Cause: A rate of context switches from 500 to 2,000 per second might indicate a problem with a network adapter or a device driver or that you are using an inefficient server-based application that spawns too many threads Using correlation rules, one can go beyond detecting a single event to watching for patterns of related events associated with common problems, like a router rule configuration change that causes slow database connection. You could specify that the configuration file be automatically restored from a backup before restarting the database. Or a correlation rule might detect three failed attempts to logon to the server that manages payroll within a 30 second window and deactivate that user's account, either across a domain or on that local machine. Motadata comes with built-in event correlation rules.

Summary

Log management will help IT department many ways - to react faster, become more proactive, improve security efficiency and compliance automation and most importantly it will reduce operations support and cost.

Try Before You Buy

It is best to try out before making a purchase decision. We provide 30-day free trial which will help you evaluate Motadata in your environment for your business and technical needs. Motadata comes with more than 100 parsers/plug-ins for collecting and analyzing that data, and extensive libraries of reports and filters, as well as intelligent Correlation Rules.

What's Next?

Learn more about it by visiting log management section on our website www.motadata.com/features/log-management/

Try it for yourself. Download a free 30-day trial from here www.motadata.com/download/