Log Analyzer

Motadata Feature

1 Introduction

Motadata log analyser collects, stores and analyses machine log events from multiple sources such as network devices, servers and applications. Motadata acts as a central data store by collecting data across sources to index and search them for review and retention requirements. The built-in correlation engine also provides proactive analytics to detect critical events such as security events, session events, server failover/fallback and VM migration events. Motadata's Data Analytics Platform (DAP) delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility, providing deep operational visibility and faster troubleshooting. It allows It teams to collect, process, and visualize all types of log data generated by heterogeneous sources in a complex IT infra environment.

Log management is the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an information system.

1.1 Configuring Log Receiver

For that open console on motadata server and check motadata-conf.yml file, here you will find the port numbers which are assigned to logs and flow.

#cd /motadata/motadata/config

#cat motadata-conf.yml

Check all ports here.

#log server udp port

log-server-udp-port: 514

#log server tcp port

log-server-tcp-port: 5141

#log secure server tcp port

log-secure-server-tcp-port: 5142

#agent

motadata-agent: yes

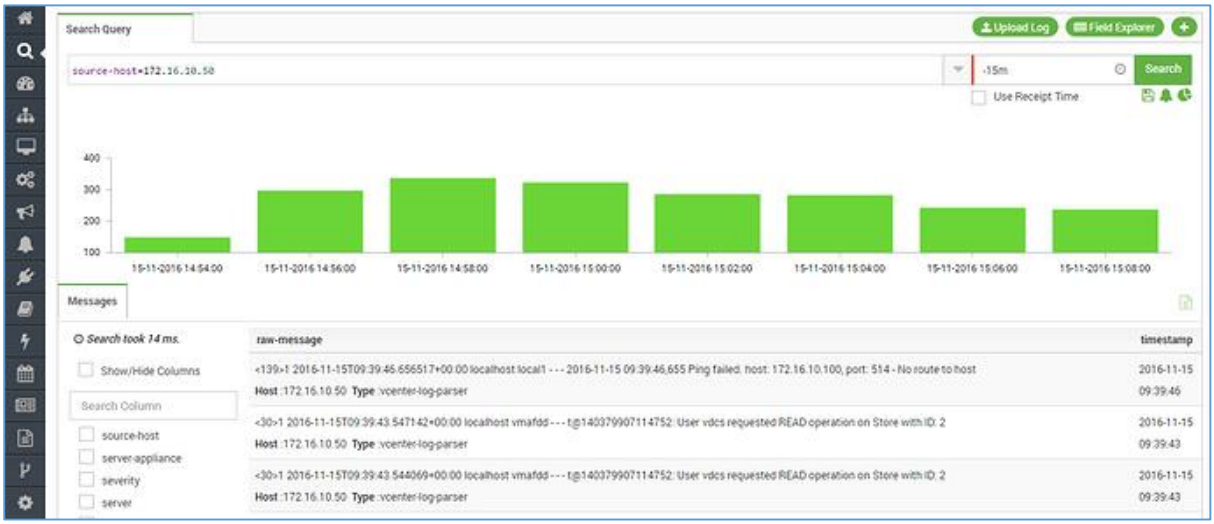
Please forward logs from log host to motadata IP and above mention ports. You may also change ports in YML file and restart motadata service to make them effective.

2 Prerequisites

- You will need license for flow/log monitoring.
- You need to have respected plugin installed for specific patterns of logs.

3 Monitoring Logs

Now check on motadata server.



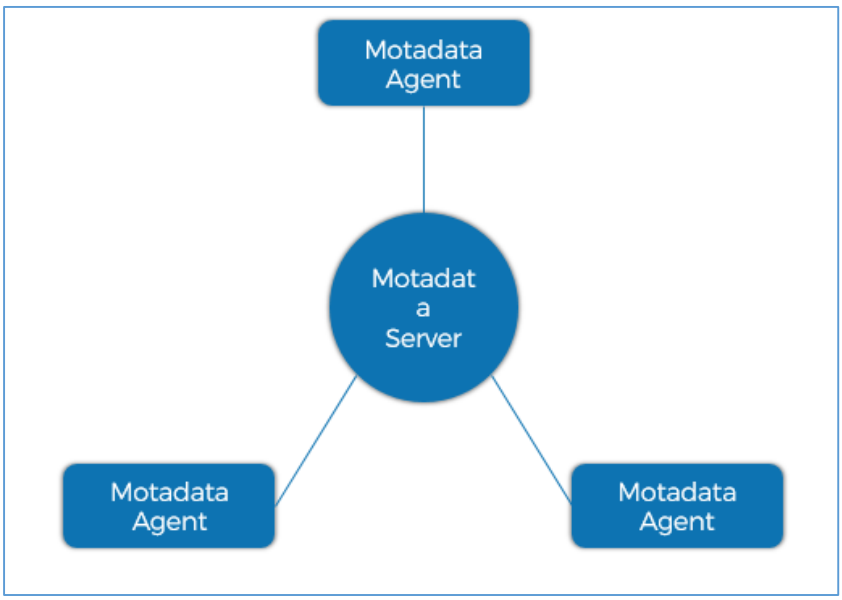
3.1 Motadata Agent Installation Prerequisites

Log management is the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an information system.

3.2 Deployment Strategy

Motadata agents can be installed in targeted servers to collect logs.

3.3 Deployment Overview Diagram



The motadata agent collects events only for the host on which it is installed. You can use this collection method on a Windows host that is busy or has limited resources, for example, domain controller

3.4 System Performance and Deployment Strategies

Communication between Motadata agents and Motadata server must be enabled all the time.

Below open ports are required for data communication between motadata agents and the motadata server

#log server udp port

log-server-udp-port: 514

#log server tcp port

log-server-tcp-port: 5140

#log secure server tcp port

log-secure-server-tcp-port: 5142

Note: these ports are configurable from agent.conf file.

Hardware and software requirements for the motadata host

Ensure that the Windows-based computer that hosts the Motadata agent meets the minimum hardware and software requirements

Motadata agent installations and events per second

Before you install your Motadata agents, it is important to understand the number of events that can be collected by agent.

Keep in touch

www.motadata.com, sales@motadata.com,

India: +91 79-2680-0900, USA: +1 408-418-5229

About Motadata

Mindarray Systems Pvt. Ltd. a global IT product company, offers state of the art affordable yet powerful product suite - Motadata consisting of Network Management & Monitoring, Log & Flow Management, and IT Service Management Platforms. The platform empowers both IT administrators and CXOs to analyze, track & resolve IT operational issues by effectively monitoring various systems and devices from multiple vendors through a unified and centralized dashboard.

Motadata is industry's first IT ops solution that truly correlates the metric, flow and log events and turns them into actionable insights. Our global customers from Telecom, Government and Enterprise domain, rely on Motadata for proactively monitor their network infrastructure.

For more information, visit www.motadata.com.

motadata