Centralized Logging

Reading

30 minutes

Status	Incomplete

Introduction

Logs are records in plain text files, where these lines contain information about the date and time of a specific event. Logs make it easier to gain visibility into the health and security of the IT infrastructure. The information contained in these logs can range from system performance, audit data, intrusion alerts, and user transactions and activities.

Log analysis makes it possible to identify and solve problems affecting different business areas. The logs bring a flow of events that contain a vast amount of data related to software, infrastructure, accessibility, and user and access patterns.

Centralized log management monitors what is happening in a given environment, keeping the environment safe against intrusions and improving the performance of applications. It is essential to retain this data centralized so the information can be quickly searched and saved. Efficient monitoring solutions provide real-time alerts for events identified through these logs. These events can be status changes in an environment.

Reading

Steps of Centralized Log Management

1. **Collection**: In this step, it is crucial to collect data and store them centrally to transmit them to the central IT infrastructure.
2. **Ingestion**: In this step, the data is imported and formatted, allowing the inclusion of date and time, in addition to other relevant details. Storage and indexing ensure faster searches.
3. **Research analysis**: This step is carried out in each line of data that is later analyzed to identify what is happening in the device or systems.
4. **Monitoring and alerts**: With log management, it is possible to configure alerts by defining rules that trigger notifications. It is necessary to map which activities are essential to becoming an alert.

5. **Visualization and reporting**: Defining how this generated data is visualized is essential. When creating reports, it is possible to understand specific patterns and think of new solutions.

Log Management Best Practices

Best practices are often spoken of in every industry, but what are they really? In some cases they are established as a result of regulations imposed on industries, and in other cases, they are an organic result of years of trial and error. In both cases, the intent is to create a set of practices that bring about the best results. Implementing best practices can help organizations to improve the quality of their products or services, increase efficiency and productivity, and reduce the risk of errors or problems. You will now take a look at some of the best practices around log management that are recommended.

Use Automated Log Management Tools

Analyzing log data is one of the biggest challenges Cyber Security analysts face. Tracking and analyzing log data by manual methods is impossible because the volume of log data is vast, and the process is prone to human error. Therefore, Cyber Security analysts must rely on automated log management solutions to analyze massive amounts of log data generated by their network infrastructure.

With automated log management tools, Cyber Security analysts can derive real-time security intelligence and be notified when anomalies occur across applications, systems, and devices. This means, within seconds, you can provide powerful insights into user behaviours, network anomalies, system downtime, policy violations, insider threats, and more details and information.

Aggregate Data Records in a Central Location

Aggregating log data from heterogeneous sources, such as Windows, Linux, security devices, and other systems in a central place can be a daunting task for Cyber Security. Using multiple management tools is often found to be ineffective for managing logs across an enterprise.

Cyber Security analysts therefore need to deploy a single log management tool that will allow them to decipher any log format from any source. They should choose a log management tool with a universal log collection feature. This feature enables organizations to collect and analyze any log data format from any source, thus facilitating effective security decisions on time.

Ready for Audits with Safety Reports

Each organization must comply with its internal security policies and the policies of external regulatory bodies, such as **PCI DSS, SOX, FISMA, ISO 27001**, and **HIPAA**.

Regarding external audits, Cyber Security analysts must focus on the requirements and ensure that compliance auditors complete their work with minimal effort. Verbal assurance for compliance auditors is needed, so security reports must be ready, and the reports must be backed up with the necessary log data and management tools.

Perform Forensic Log Investigations

Log data has answers to all network problems. All attackers leave traces, and your log data is the only thing that can help you identify the root cause of a breach and even tell you who started it. Also, the analysis of forensic log reports can be used as evidence in a court of law. With proper forensic logs, tactics, and tools, Cyber Security analysts can get answers to all their

questions. The search capabilities of forensic log analysis tools allow Cyber Security analysts to conduct an investigation that will help them quickly find and fix network issues and strange behaviour.

Proactively Manage Security Threats

To proactively mitigate sophisticated cyberattacks, Cyber Security analysts must correlate log data from their network infrastructure in real time. Log data correlation enhances network security by processing millions of events simultaneously from multiple log sources to proactively detect anomalous network events before an attack or breach occurs. Real-time event correlation proactively handles all threats. To counteract security threats, Cyber Security analysts rely on log correlation tools that accelerate the monitoring and analysis of network events.

With log data correlation in place, Cyber Security analysts can spend less time tracking suspicious behaviour across the network. Log data correlation automatically detects and alerts you about vulnerabilities, user network activities, policy violations, network anomalies, system downtime, and network security threats in real time.

File and Security of Data Records

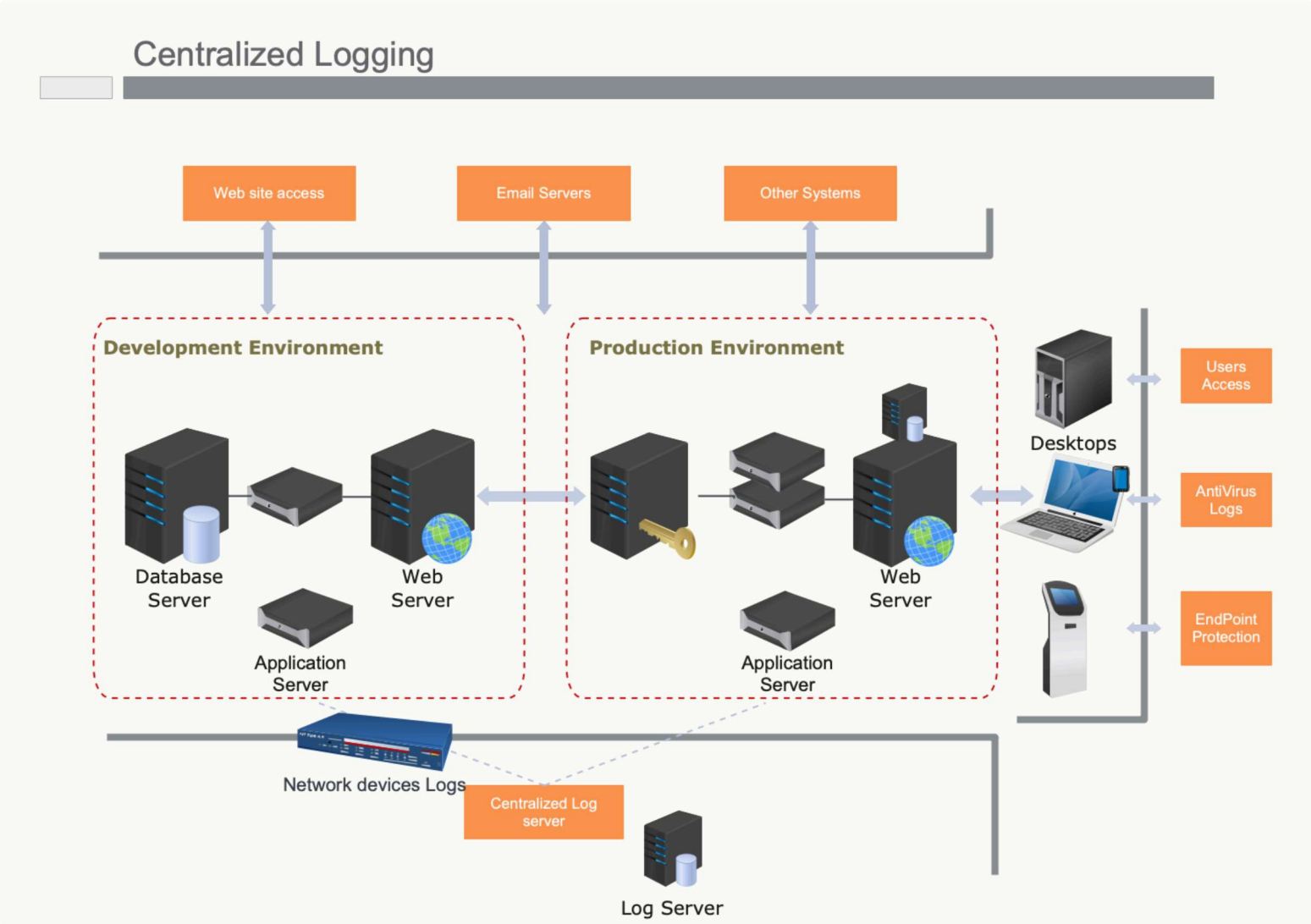
Archiving and backing up data is a mandate for all companies to meet compliance requirements. Log archiving is dependent on company-established policies and resulting regulatory compliance.

The log archiving period varies depending on the compliance audit. For example, PCI DSS requires one year, HIPAA requires seven years, and FISMA requires three years. Another good reason for archiving logs is forensic investigations. The log backup must be protected from changes to ensure authenticity. Cyber Security analysts must encrypt the log data and make it tamper-evident by hashing and time-stamping it for future forensic analysis and compliance or internal audits.

Continue Monitoring and Reviewing Data Records

Cyber Security analysts must track and analyze log data regularly. All best practices mentioned above work together towards fulfilling the complete log environment. Log management is not a one-time-only process that will protect your network. The process must be ongoing to mitigate cybercrime, where log data must be collected, monitored, and analyzed in real time.

The image below illustrates a simple centralized logging system.



The Syslog protocol allows log data to be sent from a variety of systems and applications to a central Syslog server for storage and analysis. The Syslog protocol includes a severity level, which is a numerical value that is used to indicate the importance or severity of a log message. The most common severity levels are:

- 0 (Emergency): System is unusable.
- 1 (Alert): Immediate action is required.
- 2 (Critical): Critical conditions.
- 3 (Error): Error conditions.
- 4 (Warning): Warning conditions.
- 5 (Notice): Normal but significant conditions.
- 6 (Informational): Informational messages.
- 7 (Debug): Debug-level messages.

The Syslog daemon can be configured to set "trap levels" which is the threshold for log message severity. Log messages with a severity level equal to or greater than the trap level will be logged, while messages with a lower severity level will be ignored.

For example, if the trap level is set to 4 (Warning), the Syslog daemon will log all messages with a severity level of Warning, Error, Critical, Alert, and Emergency. However, messages with a severity level of Notice, Informational, and Debug will be ignored.

The trap level can be set in the configuration file of the Syslog daemon, such as /etc/rsyslog.conf or /etc/syslog-ng.conf, depending on the Syslog daemon you are using.

It's important to note that setting the trap level too high can cause important information to be ignored, and setting it too low can cause the log files to become too large and difficult to manage. The appropriate trap level will depend on the specific requirements of the organization and the type of information that needs to be logged.

References

Centralized Logging on AWS

Previous
Linux Logging: Syslog and Log Collection

Next
Logs

W01D4

Thu Jun 27

Lectures (1)

Work (7)

4 hrs

- Common Network Conversations & Their Protocols
- Network Administration Quiz ✓
- Windows Logging
- Linux Logging: Syslog and Log Collection
- Centralized Logging
- Logs
- Troubleshooting Approaches

W01D4 Schedule »