

Troubleshooting and Tool Recommendation: SITREP Sample Report

Problem:

Each of the networked 15 servers and 400 hosts are generating logs. Some of these logs are likely due to security issues. We only have 10 network security workers, and they don't have the time to review each log that is generated across the network. This is a problem because the logs can identify security issues, host events, network optimization challenges, and errors. We need an automated method to collect, centrally store, and analyze the logs, only generating an alert when human intervention is needed.

Troubleshooting Steps:

[List the networking troubleshooting methodology]

Tool and Description:

To solve the problem identified, it is proposed that [Logstash] be implemented within the network. Logstash (a fictional tool) is a free and open server-side data processing pipeline that ingests data from varying sources, transforms it, and display the results. This tool allows for the collection of logs from virtually any source to include hosts, network devices, and servers. Most logs are in the format of their creator and therefore are not standardized across a network of systems. Logstash normalizes the logs by converting them into key fields and elements that are most important to network security and optimization. This allows users to program alerts on the Logstash server and automatically be alerted to only the most important log alerts. Logstash provides the ability to save time and human capital resources while ensuring network security and optimization capability.

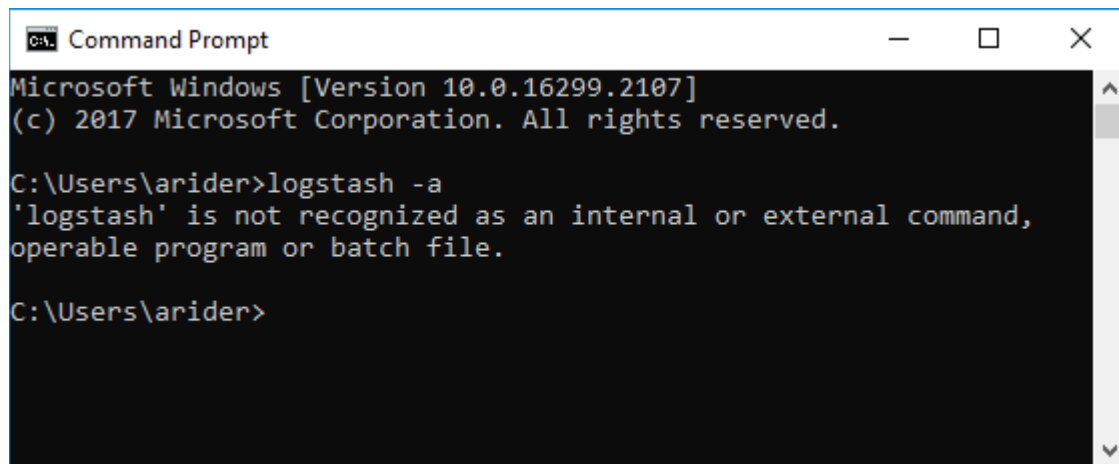
Tool Operational Use Case:

Logstash is being employed in our network to solve the log analysis problem identified above. Once implemented and properly configured, we expect Logstash to allow us to comply with internal security policies and outside regulations and audits, understand and respond to data breaches and other security incidents, troubleshoot systems, computer, and network devices, understand user behaviors, and conduct forensics in the event of an investigation. The deployment of Logstash will also save us valuable time and resources given we only have 10 personnel. The log alerts will enable network support personnel to respond only to the most crucial alerts, while ensuring nothing of critical importance is not known.

Tool Functionality:

Once installed on the server and Linux operating system, the command functionality includes multiple options:

- Logstash start (this command starts the Logstash service)
- Logstash -f (this command identifies the log file location)
- Logstash -in (this command ingests the log files)
- Logstash -c (this command sets the number of files to ingest before stopping)
- Logstash -cs (this command sets the ingest to continuous)
- Logstash -a (this command sets the parameters to analyze and alert)

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt" with standard window controls. The text inside shows the Windows version and copyright information, followed by a command prompt at "C:\Users\arider>". The user has entered "logstash -a", which has resulted in an error message: "'logstash' is not recognized as an internal or external command, operable program or batch file." The prompt is now at "C:\Users\arider>".

```
Microsoft Windows [Version 10.0.16299.2107]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\arider>logstash -a
'logstash' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\arider>
```

Example Screenshot of the Windows Command Prompt