

# Building Centralized Logging Infrastructure For DHIS2

Michael Markevich  
DHIS2 Security Lead

# Introduction

Logging is an essential software component that helps to investigate security incidents and keep audit trails.

Having a properly configured logging setup is often a mandatory compliance requirement.

Poor logging configurations can create a significant overhead and decrease overall performance.

# Available Log Sources

- DHIS2 audit logs
- DHIS2 application logs (Tomcat)
- Database (Postgres) logs
- Reverse proxy (Apache, Nginx) logs
- OS system logs (journald on recent Linux systems)

# Logging in DHIS2

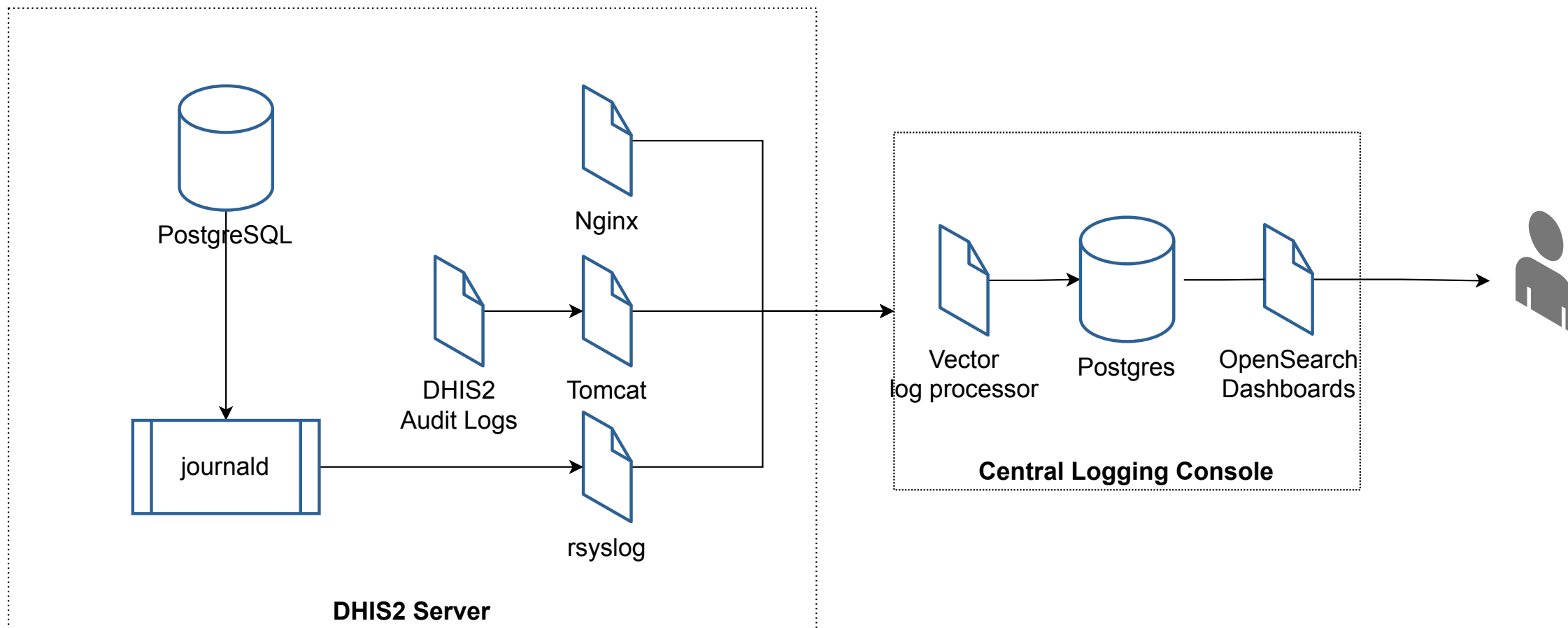
- By default, DHIS2 regular logs are written to a plain text file
- Logging configuration is flexible and can be done either through dhis.conf file or dedicated log4j2.xml.
- Log4j framework supports various destinations, including local files, remote syslog servers, Apache Cassandra or Kafka, ZeroMQ, and many more.

**What architecture should we choose?**

# Challenges

- Various formats (unstructured plain text, structured key-value pairs, JSON)
- We need to combine logs from different sources to get comprehensive information

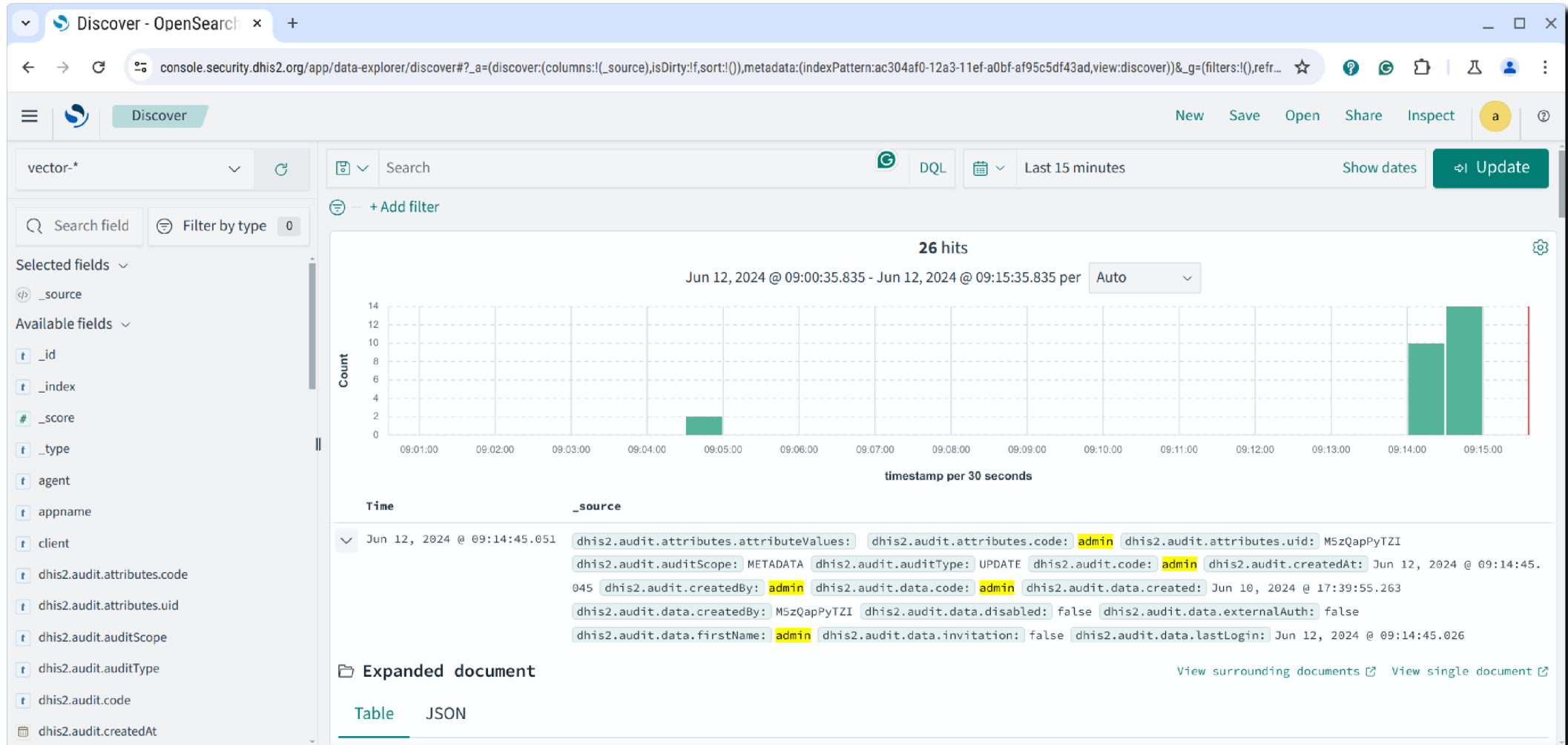
# Logging Architecture



# Technology Stack

- **OpenSearch** - a database and a dashboard (an open-source replacement of ElasticSearch and Kibana)
- **Vector** - a lightweight, ultra-fast tool for building observability pipelines (also open-source, developed by Datadog)

# User Interface



The screenshot displays the Dhis2 Discover - OpenSearch user interface. The browser address bar shows the URL: `console.security.dhis2.org/app/data-explorer/discover#a=(discover:(columns:(!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:ac304af0-12a3-11ef-a0bf-af95c5df43ad,view:discover))&_g=(filters:!(),refr...`

The interface includes a search bar with the query `vector-*` and a search button. The search results are displayed as a bar chart showing the count of hits over time. The chart title is **26 hits** and the time range is `Jun 12, 2024 @ 09:00:35.835 - Jun 12, 2024 @ 09:15:35.835 per`. The chart shows a small bar at 09:05:00 and a larger bar at 09:14:00.

Below the chart, an expanded document is shown for the time `Jun 12, 2024 @ 09:14:45.051`. The document content is as follows:

```

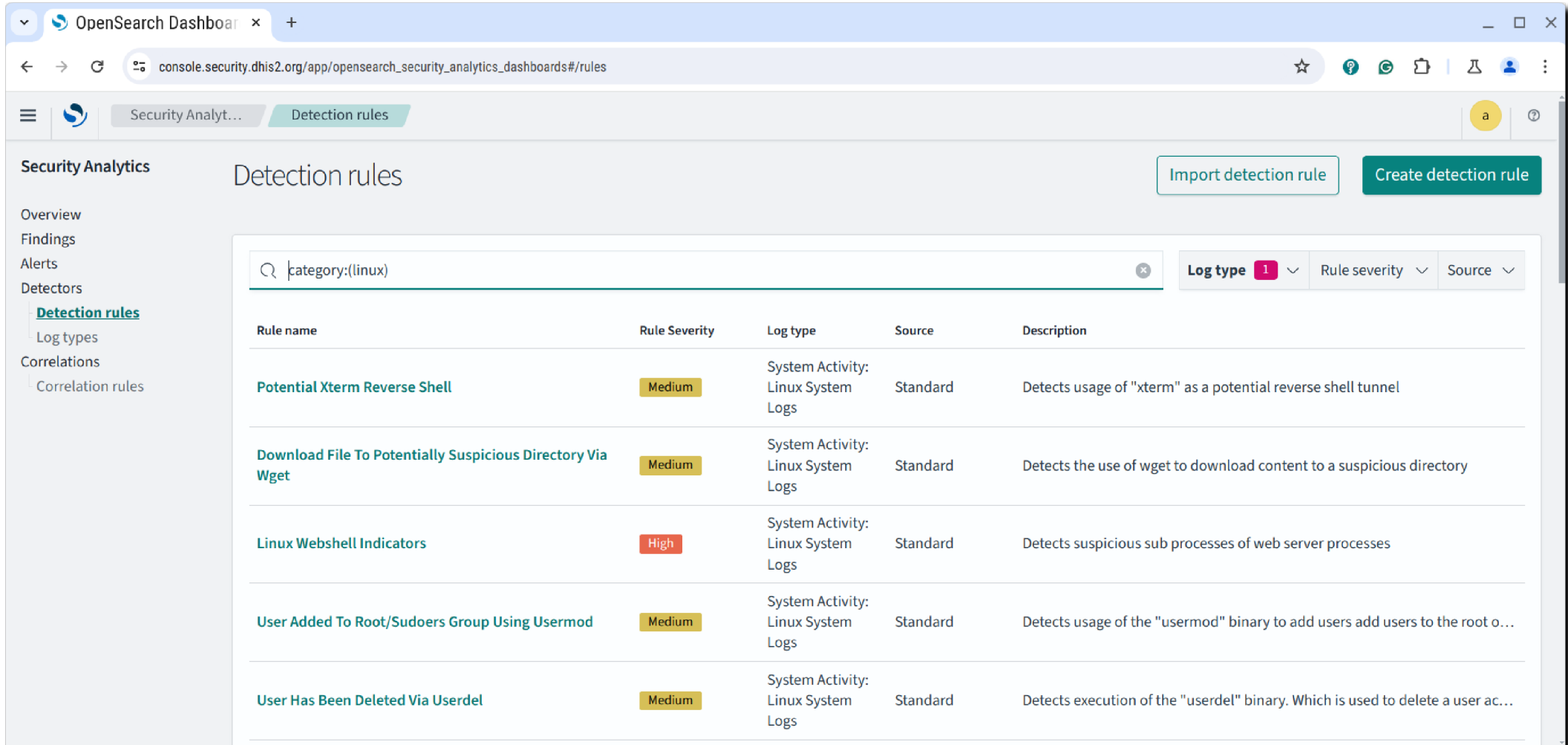
dhis2.audit.attributes.attributeValues: dhis2.audit.attributes.code: admin dhis2.audit.attributes.uid: M5zQapPyTZI
dhis2.audit.auditScope: METADATA dhis2.audit.auditType: UPDATE dhis2.audit.code: admin dhis2.audit.createdAt: Jun 12, 2024 @ 09:14:45.045
dhis2.audit.createdBy: admin dhis2.audit.data.code: admin dhis2.audit.data.created: Jun 10, 2024 @ 17:39:55.263
dhis2.audit.data.createdBy: M5zQapPyTZI dhis2.audit.data.disabled: false dhis2.audit.data.externalAuth: false
dhis2.audit.data.firstName: admin dhis2.audit.data.invitation: false dhis2.audit.data.lastLogin: Jun 12, 2024 @ 09:14:45.026
  
```

The interface also includes a sidebar with a search field and filter by type options. The sidebar lists selected fields (`_source`) and available fields (`_id`, `_index`, `_score`, `_type`, `agent`, `appname`, `client`, `dhis2.audit.attributes.code`, `dhis2.audit.attributes.uid`, `dhis2.audit.auditScope`, `dhis2.audit.auditType`, `dhis2.audit.code`, `dhis2.audit.createdAt`).

At the bottom, there are options to view the expanded document as a **Table** or **JSON**.



# Security Alerts



The screenshot shows the OpenSearch Dashboard interface for security analytics. The main view is titled "Detection rules" and displays a list of rules filtered by the query "category:(linux)". The interface includes a search bar, filter controls for "Log type", "Rule severity", and "Source", and two buttons: "Import detection rule" and "Create detection rule".

Rule name	Rule Severity	Log type	Source	Description
<a href="#">Potential Xterm Reverse Shell</a>	Medium	System Activity: Linux System Logs	Standard	Detects usage of "xterm" as a potential reverse shell tunnel
<a href="#">Download File To Potentially Suspicious Directory Via Wget</a>	Medium	System Activity: Linux System Logs	Standard	Detects the use of wget to download content to a suspicious directory
<a href="#">Linux Webshell Indicators</a>	High	System Activity: Linux System Logs	Standard	Detects suspicious sub processes of web server processes
<a href="#">User Added To Root/Sudoers Group Using Usermod</a>	Medium	System Activity: Linux System Logs	Standard	Detects usage of the "usermod" binary to add users add users to the root o...
<a href="#">User Has Been Deleted Via Userdel</a>	Medium	System Activity: Linux System Logs	Standard	Detects execution of the "userdel" binary. Which is used to delete a user ac...

# Deliverables

Reference DHIS2 setup with custom logging configuration:

<https://github.com/dhis2-sre/dhis2-specimen>

Reference Central Logging Console setup with dashboards:

<https://github.com/dhis2-sre/dhis2-console>

# Thank You

Q&A / Feedback