Log Archiving and Analysis Town Hall Announcement

DCSS - April 19, 2016

Philip Kobezak - pdk@vt.edu

What is the LAA project?

The Log Archiving and Analysis (LAA) project will provide a comprehensive, university-wide, service for collecting, analyzing, and archiving log events.

- Security Task Force led to LAA Working Group
  - LAA Working Group report outlined a high-level plan
- Core technology: Elasticsearch, Logstash, Kibana (ELK), and Kafka
- Sponsored by Scott Midkiff with these goals:
  - Improve security posture and reduce risk of data exposure
  - Improve information technology operational processes
  - Develop predictive analytics
- Documentation: https://webapps.es.vt.edu/confluence/display/laa

What will be discussed at the town hall meeting?

- Quick overview of the project
  - Architectural plans and timeline
- Status update
  - Deployment of Elasticsearch, Logstash, Kibana, and Kafka
  - Current logs feeding
  - Metrics: GBs per day, TBs searchable, ingest latency, etc.
- Use cases and demonstration of Kibana
- Open forum for questions

Who should attend?

- Anyone in the Division of IT who didn’t attend previous town hall
- Anyone in distributed IT (anyone involved in IT at Virginia Tech)
- Anyone who has questions or interest in the project

We want to involve you in the development of this service to help meet your needs

When and Where?

Log Archiving and Analysis Town Hall Meeting

Tuesday April 26, 2016 at 9:00 AM

Assembly Hall, Alumni Center

Or via WebEx

Email will be sent with details to techsupport-g, Network Liaisons, and IT Council

We hope to see you there!