Introduction

Monitoring and Log Management

Overview

- Logging and monitoring are activities related to having awareness of the manner in which systems are functioning
- Logging is typically part of the ongoing systems management and often used for after-the-act review
- Monitoring is typically part quality assurance for computing services and normally used for live review
- Together they allow an organization to take steps to competently provide needed digital resources to anyone authorized to use them
- All modern computer equipment may participate in logging, servers, desktops, network infrastructure equipment, IOT devices, etc.

Recording vs. Evaluating Information

- Both activities use runtime information from processes
- Logging records data provided by a process usually without user intervention
- The data may be success or failure notifications with varying levels of detail, or may simply be metrics reporting
- Monitoring evaluates the runtime information and reports the evaluation result, often in realtime and normally only when initiated by a user
- In both cases these may be the only way for administrative staff to know whether infrastructure, systems, and software are working properly and identify sources of problems when they do arise

Logging vs. Monitoring

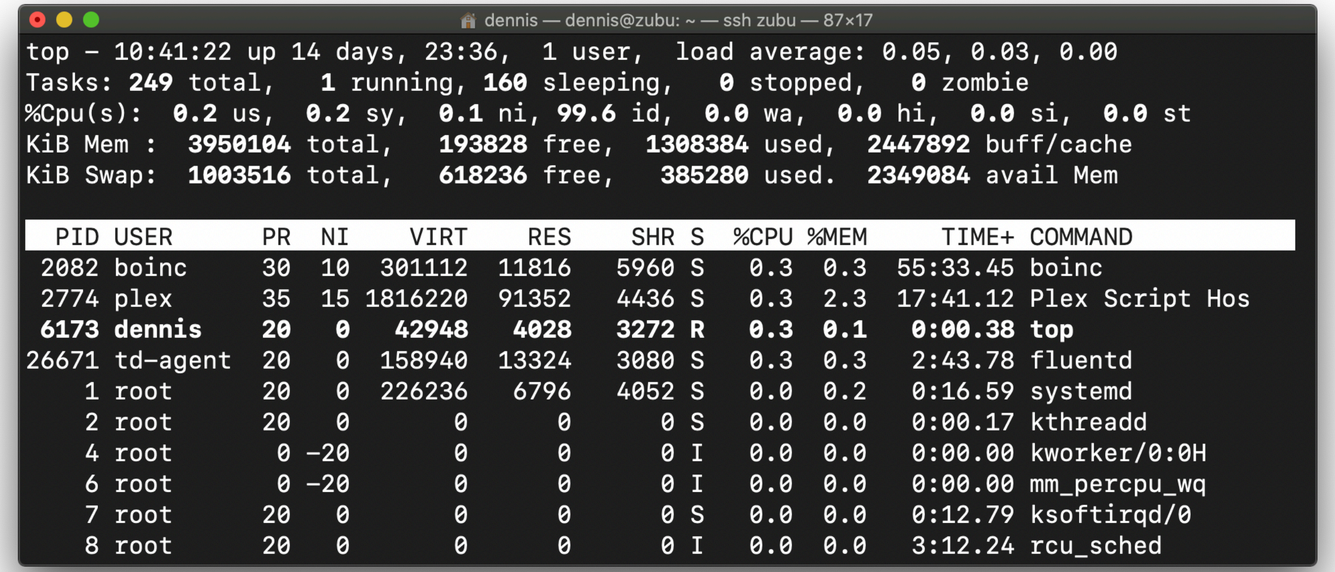
- Logging is the method used to record information from running programs, in order to have visibility into normal system operation and identify abnormal situations
  - e.g. user alice logged in at 10AM, and out at 4PM, consuming a total of 85 seconds of cpu time
  - e.g. the apache2 web service received an unusual URL which it responded to by dumping out the customer database to the requestor

https://www.legalmediaexperts.com/blog/who-owns-a-court-reporter-s-notes

- Monitoring is the act of observing how something is working in order to determine if the resources being used are producing the expected results with regards to usability
  - e.g. user alice is experiencing slow response times for file access to the network share
  - e.g. the security camera system periodically goes offline for up to 30 seconds then comes back online

https://renespoints.boardingarea.com/2019/10/29/trip-delay-coverage-with-the-delta-reserve-cards/

Monitoring Resources



- Monitoring digital resources provides information to assist in the management of those assets throughout their lifecycle
- It can be used to determine hardware and software resource requirements and evaluate how well current resources meet current demands
- It can assist in identifying changes needed to maximize the use of resources
- It can also expose security-related events
- Synchronous and asynchronous (review of historical events) monitoring are both employed to properly manage digital resources
- Monitoring data being displayed live may be retrieved directly by a monitoring program, or extracted from logs already recorded

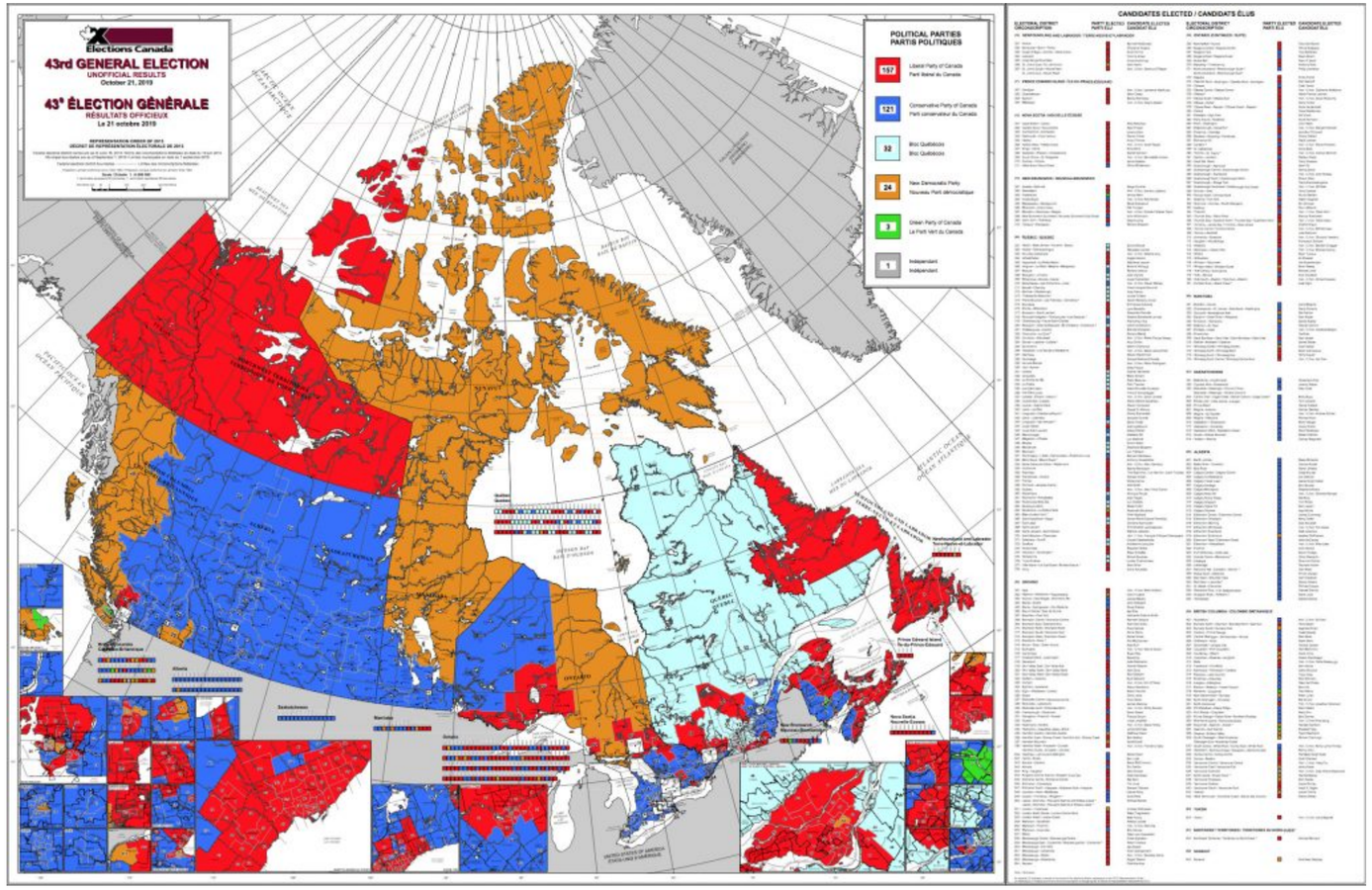
Logging Events

- In order to review historical events, information regarding those events must be available to review
- Logging is the mechanism normally used to capture information regarding events of interest for later summary and analysis
- Logging is traditionally used to provide system activity tracking, error history, and the data used for system loading and performance analysis
- It is becoming increasingly recognized as important from a security perspective
- Because of the wide variety of uses for log data, the type of data captured and the organization of that data and its metadata are important

Information Capture

- Operating systems include basic logging tools for programs in order to capture runtime information, which is then called log data
- Applications and service programs may define their own logging strategies which may or may not include the operating system logging tools
- Different operating systems implement different logging tools and data formats and there are competing 3rd party solutions for all aspects of log data handling, some of which are cross-platform (e.g. logstash)
- Transfer of log data can be done between systems, using multiple protocols, in real time
- Most operating systems, and in particular network infrastructure devices, record logs locally on their own internal storage
- Programs that send copies of log data from the system that generated the messages to remote logging services are sometimes called log shippers

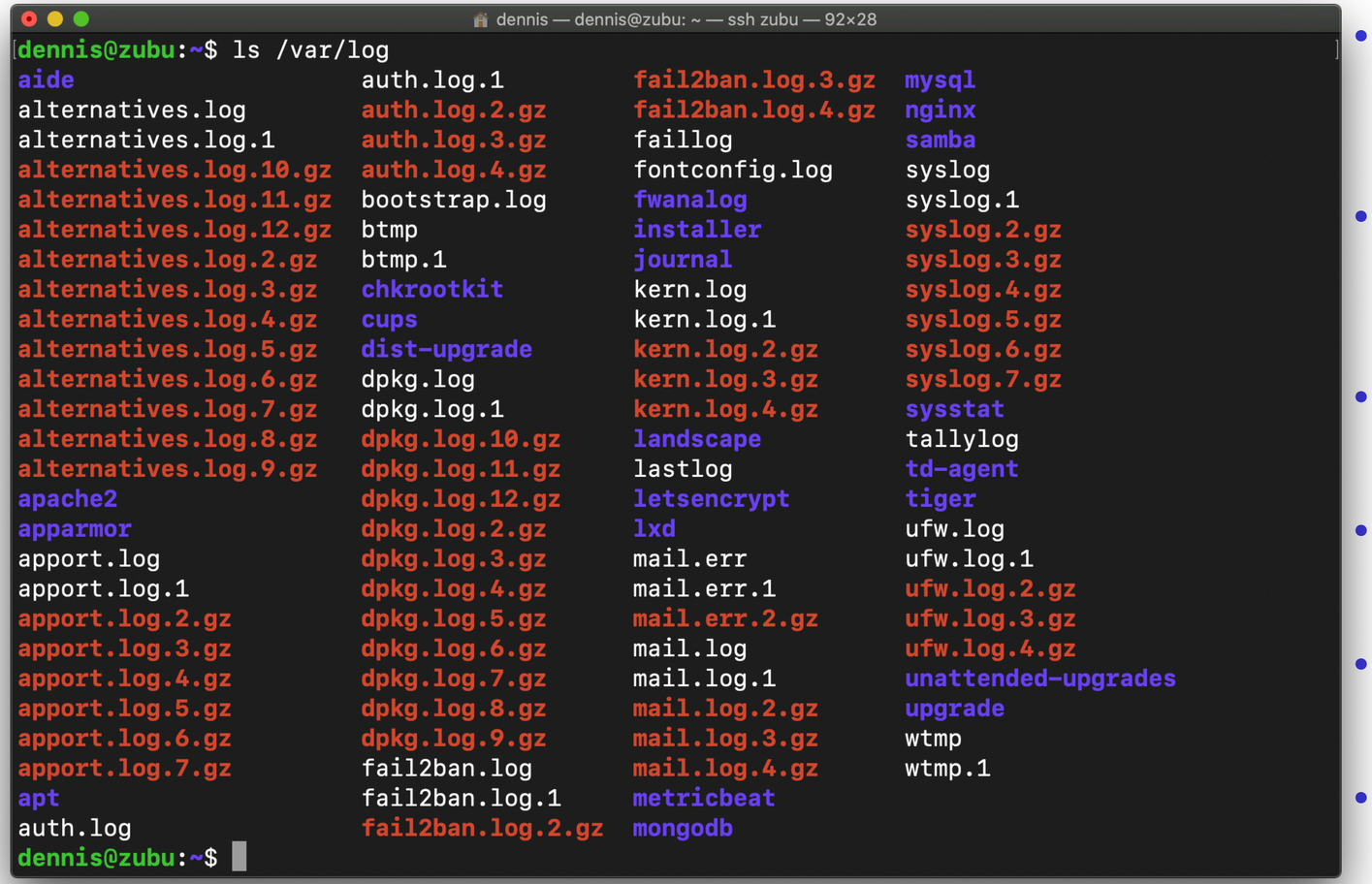
Managing Runtime Information



https://rsfcanada.org/canada-election-results-map-2019.html

- When capturing live events, the data captured may be large, but it is finite, and typically used for a single analysis activity, then archived or discarded
- Ongoing logging of events for later analysis can lead to enormous amounts of raw data, with no specific limit to the amount of data to be collected
- A plan must be in place to capture, store, reduce and analyze this raw data for it to be useful
- Strategies for data reduction may include filtering, summarizing, splitting, and reformatting
- Securing log data also needs to be considered

Information Storage



- The most common default storage method for log data is in plain files, either as plain text or structured data
- These files can be managed using programs that archive old entries and compress old data, eliminating the oldest data periodically
- Log data may be stored on centralized logging servers
- Log data may be stored in logfiles or database systems or multiple containers
- There are log shippers that read log files, and ship selected data to a receiver
- Standard file security methods are typically used to secure log data

Log Analysis

- Many applications are available for analyzing log data
- Some generically summarize logs in simple ways (e.g. Logwatch), others can do sophisticated presentation of data relationships within logs (e.g. Splunk)
- Some analyze logs to produce performance metrics for monitoring purposes
- Some produce security alerts and/or reports
- There are also multi-purpose analysis programs that allow for analyzing the data in any way that makes sense to the user of the program (e.g. ELK stack)
- Applications are responsible for providing log message content and can format that content whatever way the application developer chooses

Data Reduction and Retention

- Analysis tools may only produce reports, or they may store summarized data after generating it
- The original source data may no longer be required depending on what the data is used for, e.g. performance summaries often obviate the need for the raw data
- Saving only summarized information is a form of data reduction
- When there are requirements for saving either the summarized data or the source data in very large quantities, a data retention policy and plan must be developed

Lab - Virtual Network Creation