

Introduction

Introduction

Message Capture

Log Analysis

SNMP

Netflow

SNMP Traps

Proxy Services

Unified Threat Management

Authentication

Network Discovery

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

✉ DEPARTURES				
TIME	DESTINATION	FLIGHT	GATE	REMARKS
12:39	LONDON	CL 903	31	CANCELLED
12:57	SYDNEY	UQ5723	27	CANCELLED
13:08	TORONTO	IC5984	22	CANCELLED
13:21	TOKYO	AM 608	41	DELAYED
13:37	HONG KONG	IC5471	29	CANCELLED
13:48	MADRID	EK3941	30	DELAYED
14:19	BERLIN	AM5021	28	CANCELLED
14:35	NEW YORK	ON 997	11	CANCELLED
14:54	PARIS	MG5870	23	DELAYED
15:10	ROME	RI5324	43	CANCELLED

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

Monitoring Resources

```
dennis — dennis@zubu: ~ — ssh zubu — 87x17
top - 10:41:22 up 14 days, 23:36, 1 user, load average: 0.05, 0.03, 0.00
Tasks: 249 total, 1 running, 160 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.2 sy, 0.1 ni, 99.6 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3950104 total, 193828 free, 1308384 used, 2447892 buff/cache
KiB Swap: 1003516 total, 618236 free, 385280 used. 2349084 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2082	boinc	30	10	301112	11816	5960	S	0.3	0.3	55:33.45	boinc
2774	plex	35	15	1816220	91352	4436	S	0.3	2.3	17:41.12	Plex Script Hos
6173	dennis	20	0	42948	4028	3272	R	0.3	0.1	0:00.38	top
26671	td-agent	20	0	158940	13324	3080	S	0.3	0.3	2:43.78	fluentd
1	root	20	0	226236	6796	4052	S	0.0	0.2	0:16.59	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.17	kthreadd
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
7	root	20	0	0	0	0	S	0.0	0.0	0:12.79	ksoftirqd/0
8	root	20	0	0	0	0	I	0.0	0.0	3:12.24	rcu_sched

- 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

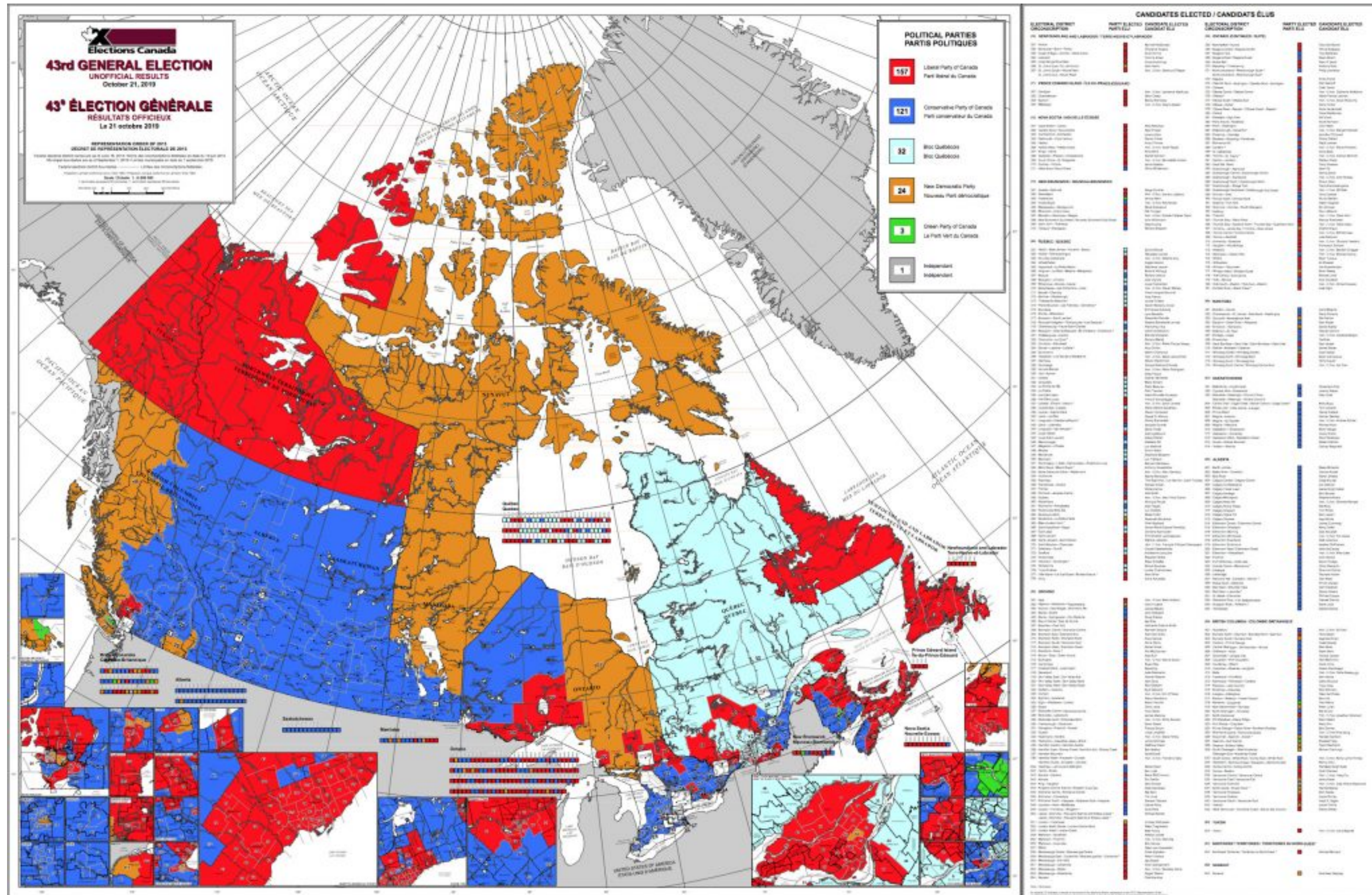
- In order to review historical events, information regarding those events must be available to review
- Logging is the mechanism normally used to capture information regarding events of interest for later summary and analysis
- Logging is traditionally used to provide system activity tracking, error 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

- 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



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

Information Storage

```
dennis@zubu:~$ ls /var/log
aide
alternatives.log
alternatives.log.1
alternatives.log.10.gz
alternatives.log.11.gz
alternatives.log.12.gz
alternatives.log.2.gz
alternatives.log.3.gz
alternatives.log.4.gz
alternatives.log.5.gz
alternatives.log.6.gz
alternatives.log.7.gz
alternatives.log.8.gz
alternatives.log.9.gz
apache2
apparmor
apport.log
apport.log.1
apport.log.2.gz
apport.log.3.gz
apport.log.4.gz
apport.log.5.gz
apport.log.6.gz
apport.log.7.gz
apt
auth.log
auth.log.1
auth.log.2.gz
auth.log.3.gz
auth.log.4.gz
bootstrap.log
btmptmp
btmptmp.1
chkrootkit
cups
dist-upgrade
dpkg.log
dpkg.log.1
dpkg.log.10.gz
dpkg.log.11.gz
dpkg.log.12.gz
dpkg.log.2.gz
dpkg.log.3.gz
dpkg.log.4.gz
dpkg.log.5.gz
dpkg.log.6.gz
dpkg.log.7.gz
dpkg.log.8.gz
dpkg.log.9.gz
fail2ban.log
fail2ban.log.1
fail2ban.log.2.gz
fail2ban.log.3.gz
fail2ban.log.4.gz
faillog
fontconfig.log
fwanalog
installer
journal
kern.log
kern.log.1
kern.log.2.gz
kern.log.3.gz
kern.log.4.gz
landscape
lastlog
letsencrypt
lxd
mail.err
mail.err.1
mail.err.2.gz
mail.log
mail.log.1
mail.log.2.gz
mail.log.3.gz
mail.log.4.gz
metricbeat
mongodb
mysql
nginx
samba
syslog
syslog.1
syslog.2.gz
syslog.3.gz
syslog.4.gz
syslog.5.gz
syslog.6.gz
syslog.7.gz
sysstat
tallylog
td-agent
tiger
ufw.log
ufw.log.1
ufw.log.2.gz
ufw.log.3.gz
ufw.log.4.gz
unattended-upgrades
upgrade
wtmptmp
wtmptmp.1
```

- 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

Software can be chaotic, but we make it work



Expert

Trying Stuff
Until it Works

ORLY?

The Practical Developer
@ThePracticalDev