Logging and Monitoring

Linux Systems Security

Monitoring

- Monitoring can take many forms, from passive periodic inspection to realtime intrusion detection
- For this lesson, we will consider it in the form where we analyze logs produced by various systems and services to identify concerns and possible solutions
- Much more detail on comprehensive logging and monitoring will be covered in the second semester

Logging

- One of three alternatives are typically included by distro vendors for Linux message logging:
  syslog
  syslog-ng
  rsyslog
- The default configurations for all of them log messages as plain text to files in /var/log
- Programs send messages to the logging service by sending them to the /dev/log socket file, syslog daemons read messages from this socket in real time
- Configuration files allow messages to be directed a number of places, including to other log servers
- Only one of these will be present on a system, and there are alternatives to these as well

```
Numerical            Facility
   Code

     0            kernel messages
     1            user-level messages
     2            mail system
     3            system daemons
     4            security/authorization messages
     5            messages generated internally by syslogd
     6            line printer subsystem
     7            network news subsystem
     8            UUCP subsystem
     9            clock daemon
    10            security/authorization messages
    11            FTP daemon
    12            NTP subsystem
    13            log audit
    14            log alert
    15            clock daemon (note 2)
    16            local use 0  (local0)
    17            local use 1  (local1)
    18            local use 2  (local2)
    19            local use 3  (local3)
    20            local use 4  (local4)
    21            local use 5  (local5)
    22            local use 6  (local6)
    23            local use 7  (local7)
```

https://opentodo.wordpress.com/2012/09/17/syslog-centralized-logging/

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

https://unofficialaciguide.com/2018/08/11/configuring-syslog-for-aci/

syslog

- The syslog project started in 1980 to provide a unified method for daemons to save messages for later examination
- syslog uses the concept of labelling messages with a source and priority (i.e. facility.level) and then writing them to text files in /var/log
- syslog runs over UDP for speed and simplicity
- syslogd is still around and uses port 514, included in Apple products and other UNIX variants and derivatives
- Configured in /etc/syslog.conf, it supports the logger command to manually send messages

syslog-ng

- A project started in 1998 to offer an enhanced system logging service
- Supports basic logging like syslog, but adds a number of new capabilities including reliable message delivery, transport security using TLS, database support for message stores, message parsing/filtering/rewriting/classification
- A number of the most interesting features of syslog-ng are only available in the paid version (see balabit.com)

rsyslog

- Created in 2004 to address the shortcomings of the original syslog and to create an alternative to syslog-ng because the most interesting tech in syslog-ng is not available in the OSS version and were unlikely to be folded back into the main branch even when mods were submitted to balabit
- rsyslog can use standard syslog configuration files for backwards compatibility
- Enhancements to syslog found in rsyslog include improved timestamping, reliable transport using TCP and TLS, database message store support, RELP/BEEP support, message buffering, and systemd logging

rsyslog Configuration

- /etc/rsyslog.conf is the main config file and sets global parameters
- /etc/rsyslog.d/*.conf are additional service specific configuration files (e.g. ufw, postfix)
- There are man pages and rsyslog.com has many sample configs
- The config file language is not friendly to humans

Systemd Log Viewing

- The journalctl command is intended to make logs written by systemd-initiated programs easier to find and understand
- Typically run with the -x option, it not only display log entries but tries to look up descriptive text for messages it recognizes to make the entries more useful
- The -e option tells it to jump to the end of the logs so that the most recent log entries are shown by default as entries are displayed in ascending time order
- It has many other options to filter or format the logs entries
- It is only useful for viewing logs on the local machine written by things that are started by systemd

Manual Log Viewing

- Logs are by default kept in plain text file in the /var/log directory
- You can use typical text manipulation tools to view them and find things in them
- It is common to use grep to find specific error message text, process id numbers, port numbers, service names, process names, and user names
- If you use grep for this, it is often helpful to include context (-A, -B, -C) for the log entries found (the lines right before and after)
- It is also often helpful to use specific word searches instead of just pattern matches (-w)
- Remember there can be multiple log files written into for any particular event
- You may wish to search archived log files as well as the current log file

Log Management

- Logs by their nature are data repositories that continuously grow
- Without bounds, they would grow to consume the entire storage space they reside in
- Some programs can use a circular log buffer, such as the kernel message buffer (view with dmesg)
- For standard system log files, the logrotate program is designed to move older messages along a virtual conveyor belt on their way to the great bit bucket in the sky
- logrotate use a configuration file to specify log files to be automatically aged, /etc/logrotate.conf
  - it runs from cron, periodically doing its work, but can be run interactively on the command line
  - can use additional config files to split out configs for different logs, and compresses older logs
  - can handle many logs types, schedules, and has lots of other parameters to control how aging is done

Logwatch

- Logwatch parses log files and extracts summary reports, based on config files in /etc/logwatch/conf/ and /usr/share/logwatch
- The default is text format and output on the terminal
- Commonly implemented as automated daily reports sending email summaries
- Shows software changes, hardware changes, user changes, sudo usage, services access, kernel errors, storage usage, and whatever else you add config files for
- Lots of default config files are in /usr/share/logwatch/default.conf

LogAnalyzer

- GPL'd realtime webserver-based log analysis tools
- Download the package from http://loganalyzer.adiscon.com/downloads/ and extract it
- Install instructions are in the file named INSTALL, mostly just needs to have the files copied to a web server document store

Sending Windows Event Logs to Rsyslog

- rsyslog support UNIX-style messages delivered either locally or over the network
- Windows does not do UNIX-style logging, it has its own logging approach
- There are programs which watch Windows logs and send new messages that are interesting to a syslog service on the network
- Most are paid software, an example of a free program to do this is nxlog which is available in both free (community) and paid (enterprise) versions - see https://nxlog.co/

Web-based Admin Tools

- There are many web-based applications that can run on a Linux system that include log viewing and management capabilities
- cockpit is a Redhat webapp that listens on port 9090 and provides a way to manage a Linux systems derived from Redhat or Debian
- It allows log viewing with simple filtering and date selection, but is not suitable for anything other than taking a look for something fairly specific
- webmin is an OSS webapp that listens on port 10000 and runs on most Linux distros
- It allows full and highly granular control over logging as well as the ability to view, filter, sort, and search logs