Department for Levelling Up,
Housing & Communities

Guidance for logging

Version1.0

LOCAL DIGITAL Cyber

Objective

- To help you devise an approach to logging that will help answer some of the following questions:

    - What has happened?
    - What is the impact?
    - What should we do next?
    - Has any post-incident remediation been effective?
    - Are our security controls working?

- Overview of using centralised logging systems and the benefits they bring.

- Understand the NCSC's expectations regarding basic good practice for logging.

LOCAL DIGITAL Cyber

What are log files ?

- Log files are essentially a history of actions collected by a device, and usually stored on the same device.
- They vary in detail between devices, and devices such as Servers log in multiple different areas, usually grouped by function or service.
- Log files are the usually the first place to be checked when troubleshooting.

LOCAL DIGITAL Cyber

Centralised vs decentralised logging

- A centralised solution can be used to provide a standalone logging service.
- The more sources that feed into a centralised store, the more useful it will be, and the better the return on your investment.
- Centralising logging will mean you don’t have to physically go to each machine when investigating an incident.
- A decentralised setup involves leaving the logs in-situ.
- In most cases, a centralised store is used in combination with other vendor dashboards/APIs.

LOCAL DIGITAL Cyber

Implement a Logging Solution

- Logging data can be used to investigate performance issues, provide administrative alerts (such as a storage disk being near capacity) and help verify that the Council's IT policy is working as intended.
- You will be better prepared for the most pressing questions put to you by incident investigators should you suffer a cyber attack.
- Giving you the best chance of recovering swiftly, and learning how to defend your systems better against future incursions.

LOCAL DIGITAL Cyber

Centralised Logging Components

During setting up a centralised logging solution you will need to consider how to implement the following components:

- Logging source
- Log transport
- Processing and storage
- Querying and analytics
- Configuring log sources

LOCAL DIGITAL Cyber

Centralised Logging Components (cont…)

Logging source

- Log sources may generate large volumes of traffic, so you will need to refine what events (and context) is collected.
- Start with the default settings, then remove the information that is least likely to answer the incident questions until you achieve your desired cost/benefit balance.
- It is important to configure log sources properly, including synchronisation to an accurate time source and a level of verbosity which captures the fields needed to answer the incident questions.

LOCAL DIGITAL Cyber

Centralised Logging Components (cont…)

Log transport

- Dictated by the logging source and the service that ingests logs.
- The NCSC recommends using transport encryption where possible.
- Common protocols include Syslog, SNMP traps, and Windows Event Forwarding.
- Logs should use a one-way flow control (e.g. UDP or a data diode) when sent across trust boundaries, to make it harder for an attacker to modify stored logs.

LOCAL DIGITAL Cyber

Centralised Logging Components (cont…)

Processing and storage

- Accepts logs pushed (or pulled) from device sources, cleans them up (formatting), normalises and then loads them into a data store.
- Plan for storage to roll-over, avoiding disks filling and the service failing.

Querying and analytics

- Authenticates users and allows searches to be performed on the data set.

LOCAL DIGITAL Cyber

Centralised Logging Components (cont…)

Configuring log sources

Some logs at their default settings may not provide all the information required. Consider some of the following points that the NCSC has found useful in real world scenarios.

- Log everything with UTC timestamps.
- Firewall and proxy logs identify the originating IPs, and not just the IP of the proxy or gateway.
- Detail on process execution or crashes provides context as fully as possible (Parent process, user, machine, failure codes, etc).

LOCAL DIGITAL Cyber

Centralised Logging Components (cont…)

Configuring log sources (cont…)

You should ensure that:

- Your local operating system log cache is large enough to account for any network interruption between uploads to a central service.
- The fields you are expecting are actually logged, including:
  - Source and destination IP address/host name to identify the machine
  - Account names are available to identify the user

LOCAL DIGITAL Cyber

Centralised logging considerations

A centralised solution can be used to provide convenient, enhanced data access and alerting over and above multiple standalone logging services.
The more sources that feed into a centralised store, the more useful it will be, and the better the return on any investment made (in both terms of time and CapEx).

Centralising logging will also mean you don't have to physically go to each machine when investigating an incident. This will create a more responsive system, requiring minimal resources to operate it.

SIEM (Security Information and Event Management) is the general classification of products which handle centralised logging.

There are both free (open source) products, and commercial (paid for) versions of SIEM products.

LOCAL DIGITAL Cyber

Open Source SIEM Products

Free open source options include the following products for log ingestion, processing, dashboard and analysis (*These are provided as examples and are not endorsements*):

- **Logging Made Easy**: https://www.ncsc.gov.uk/blog-post/logging-made-easy
- **ELK**: https://www.elastic.co/elk-stack
- **Graylog**: https://github.com/Graylog2
- **HELK**: https://github.com/Cyb3rWard0g/HELK
- **Nagios**: https://www.nagios.com
- **Security Onion**: https://securityonion.net
- **STROOM**: https://github.com/gchq/stroom

LOCAL DIGITAL Cyber

Logging Made Easy (LME)

National Cyber Security Centre

LOCAL DIGITAL Cyber

What does LME actually do?

- LME* will guide you through the process of installing a set of open-source and free software.
- Working together, these components will provide you with a basic end-to-end Windows logging capability and a set of tools for viewing and analysing the data you gather.
- Show software patch levels on enrolled devices.
- Show where administrative commands are being run.
- See which users are using which machine.
- In conjunction with threat reports, LME allows you to search for the presence of an attacker in the form of Tools, Techniques and Procedures (TTPs).
- All the logs LME generates remain entirely within your control. This means you can turn the log events over to an incident investigation team, should you ever need to.

LOCAL DIGITAL Cyber

Who is LME for?

LME is mainly for organisations that:

- Don’t have a SOC, SIEM, or any monitoring in place at the moment.
- Lack the budget, time or understanding to set up their own logging system, or buy a professional solution.
- Recognise the need to begin gathering logs and monitoring their IT.

LOCAL DIGITAL Cyber

Premium SIEM products

The following list contains examples of premium SIEM products, and is not a fully exhaustive list. *These are provided as examples and are not endorsements*:

- **Splunk Enterprise:** https://www.splunk.com/en_us/software/splunk-enterprise.html
- **LogRhythm NextGen:** https://logrhythm.com/products/nextgen-siem-platform/
- **SolarWinds:** https://www.solarwinds.com/security-event-manager
- **FortiSIEM:** https://www.fortinet.com/products/siem/fortisiem
- **Azure Sentinel:** https://azure.microsoft.com/en-gb/services/microsoft-sentinel/
- **LogPoint :** https://www.logpoint.com/en

LOCAL DIGITAL Cyber

What data should be captured

The data captured should be driven by what threat you are mitigating against or which outcomes you need to monitor (performance, capacity etc.).

This in turn drives what systems you will enable logging on and what type of logs should be captured.

Primarily logging data should be captured on the following types of device:

- Windows Domain Controllers & Windows Application Servers
  - Event Viewer Logs (Security, System, Support, Application, Directory Services etc.)
  - Performance logging
- Linux Servers and appliances
  - /var/log | application, event, service and system log files

LOCAL DIGITAL Cyber

What data should be captured (cont…)

Primarily logging data should be captured on the following types of device:

- Database Logging
  - SQL Log files from your databases may be generated too frequently, but those on the servers themselves should be considered for inclusion in the centralised logging
- Email Servers
  - Traffic logs | database logs | system logs
- Firewalls
  - Traffic logs | audit logs | VPN logs
- Remote Access Devices
  - VPN / RAS logging | Load balancing
- Network Switches & Routers
  - General log files | Port access

LOCAL DIGITAL Cyber

What data should be captured (cont…)

Application logging should always be included for security events, as they are an invaluable source of data for Identifying security incidents.

- Monitoring policy violations.
- Establishing baselines.
- Business process monitoring.
- Audit trails e.g. data addition, modification and deletion, data exports.
- Performance monitoring e.g. data load time, page timeouts.
- Data for subsequent requests for information e.g. freedom of information.

LOCAL DIGITAL Cyber

Frequency of capture

The frequency of log data capture will be driven by the following factors

- System type.
- System criticality.
- Transaction generation rate of system.
- Storage capacity locally to the generating device.
- Storage capacity of the centralised logging system.

It is important not to overload your logging system or else you will not be able to locate the important piece of information that the central system was put in place to identify.

LOCAL DIGITAL Cyber

Refining your logging

After the initial setup has been completed and you are now sending your initial logging data to the SIEM product, you may be suffering from data overload. This needs to be corrected to make your logging useful.

This is why you will need to ensure the relevant team is monitoring the correct data e.g.

- Infrastructure - performance monitor, syslog and other capacity logs.
- DBAs - DB server log files.
- Security - security, application logs.
- Networking - firewalls, switches, router logs.

LOCAL DIGITAL Cyber

Log file retention

The key question to ask when deciding on log file data retention is ‘how important is the history of this information’. You may have a legal requirement to keep a long history of information from certain systems.

Secondary questions on data retention would be based around:

- How much space does this logging take up?
- Am I required to keep a backup of this information?
- How easy will it be to search the log files?
- Are the log files being stored in a secure location that is safe from tampering and unauthorised access?
- Are the log files being held for long enough period of time for incident histories?

Alerting

When you collect log files, they provide the most use when critical/high alerts at the very least are acted upon immediately. As a result of this requirement **alerting** on key systems and any critical/high alerts should be configured.

- Alerts flag up issues without staff having to spend time looking for them.
- This will allow you to investigate and remediate issues as they arise.
- If you don’t regularly check your log files, without alerting you may not discover issues until it is too late and an incident has occurred.
- This area is now so prone to data overload that Artificial Intelligence (AI) is being used to help make alerting manageable and cut down on ‘false positives’.

LOCAL DIGITAL Cyber

Triaging

Whether you have been alerted to a log event, or if you are performing a regular review of log files, you should implement a system of triaging the alerts to address the issues found.

- Concentrate on Critical/High log items first.
- Medium level log items should then be tackled.
- Low level log items should be reviewed and either addressed or accepted as a low priority.
- After the primary triage is carried out the issue located can be assigned to the specific team to which it pertains. Then the team in question can prioritise each issue accordingly.

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book using this link: https://calendly.com/andrea-baron/ad-hoc-call-with-council .
These are longer 1:1 sessions between DLUHC cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber support drop in sessions These regular 1:1 sessions are available for you to book anytime using the Calendly link: https://calendly.com/andrea-baron/drop-in-support-session.

Cyber clinics usually occur on the 3rd Thursday of the month between 11.30am - 12.30pm where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber