Logging Made Easy - Installation Guide

October 2019

What is Logging Made Easy (LME)?

Logging Made Easy is a self-install tutorial for organisations to gain a basic level of centralised security logging for Windows clients and provide functionality to detect attacks.

Logging Made Easy can:

- Tell you about software patch levels on enrolled devices
- Show where administrative commands are being run on enrolled devices
- See who is using which machine(s)
- In conjunction with threat reports, it is possible to query for the presence of an attacker in the form of Tools, Techniques and Procedures (TTPs)

Summary of LME Installation

- Install Microsoft Sysmon across some test machines (using a deployment method of your choosing)
- Enable built-in Windows Event Forwarding (WEF), to send to a central Windows Server
- Install Winlogbeat on the WEF Server and sync to an Elasticsearch-Logstash-Kibana (ELK) stack.
- Install the Elasticsearch Logstash and Kibana (ELK) stack, likely though Docker either on-prem or in the cloud. Customers choice.

Hosting for the Windows server needs to be somewhere where clients can easily access. The ELK stack needs to be accessible to the Windows server.

The end result will be Windows and Sysmon logs (from Windows machines you choose), transported across Windows networking and being synchronised to an Opensource database with simple dashboard front end.

Skill level required to install LME

We are pitching this at the skill level of a systems administrator or enthusiast. If you have ever…

- Installed a Windows server and connected it to an active directory domain
- Ideally deployed a Group Policy Object (GPO)
- Changed firewall rules
- Installed a Linux operating system, and logged in over SSH.

… then you are likely to have the skills to install LME!

We estimate that you should allow a couple of days to run through the entire installation process, though you can break up the process to fit your schedule. Whilst we have automated steps where we can, and made the instructions as detailed as possible, this is not going to be as easy as using an installation wizard.

Required infrastructure

To begin your Logging Made Easy installation, you will need access to (or creation of) the following servers:

- A Windows Active Directory. This is for deploying Group Policy Objects (GPO)
- A server with 2 processor cores and 8GB RAM. We will install the Windows Event Collector Service on this machine, and set it up as a Windows Event Collector (WEC) and join it to the domain.
    - If budget allows, we recommend having a dedicated server for WEC. If this is not possible, WEC can be setup on an existing server but consider the performance impacts.
    - The WEC server could be Windows Server 2016 (or later) or Windows 8.1 client (or later)
- A Linux server with 2 processor cores and a minimum of 16GB RAM. We will install our database (Elasticsearch) and dashboard software on this machine. This is all taken care of through Docker containers. **DO NOT install Docker from Ubuntu installation wizard ('Snaps'); we install the Docker community edition later.**
    - The deploy script has been tested only on Ubuntu 18.04 Long Term Support (LTS).

Servers can be either on premise, in a public cloud or private cloud. It is your choice, but you'll need to consider how to network between the clients and servers.

Before you install LME

1) Change Control. Ensure that any internal process affecting governance and change control is in place and understood.
   It is recommended to start off on a small number of machines, before rolling out further. This could aid your change control case.
2) A Windows server, joined to the active directory for Windows Event Forwarding.
    a. It could be an existing server, or new build.
    b. It doesn't have to be particularly powerful, minimum of 8GB RAM. Hard disk space can be small, as this server will temporarily hold logs (and Windows allows no more than 4GB anyway).
    c. It needs to be network accessible to your Windows end-user-devices, and other servers. This would probably require access from your corporate LAN, as the service runs over the Windows Networking protocols (WinRM). We would not recommend exposing this server directly to the internet.
3) An OU with test machines, ready to roll out the first deployment.

Installation steps

1) Create Elasticsearch infrastructure, recommended through Docker
    a. This could be in a cloud or on-prem.
    b. Requires access to someone who can create new infrastructure (on-prem, or in a cloud account) AND someone who can change network firewall rules to allow access
2) Configure on premise log collection
    a. Create GPO for client log forwarding
    b. Create GPO for server log collector
    c. Create security policy for security log forwarding
    d. Create windows firewall policy if windows firewall is deployed
    e. Requires a staff member who has access to Microsoft AD (most likely Domain Admin)
3) Create GPO for Sysmon deployment / Create SCCM package for Sysmon deployment

4) Solution checking
    a. Confirm Windows logs are reaching the collector
    b. Confirm Sysmon logs are reaching the collector
    c. Confirm logs are reaching Elasticsearch and viewable in Kibana

Follow the links below for a detailed guide to the installation process:

Stage 1: Set up Windows event forwarding

https://github.com/ukncsc/lme/blob/master/docs/chapter1.md

Stage 2: Sysmon Install

https://github.com/ukncsc/lme/blob/master/docs/chapter2.md

Stage 3: Database Easy Install

https://github.com/ukncsc/lme/blob/master/docs/chapter3-easy.md

Stage 4: Post-Install Actions

https://github.com/ukncsc/lme/blob/master/docs/chapter4.md