

LME Configuration

Full LME Documentation can be found at [CISA LME Documentation](#)

PBR is utilizing LME to centralize the logs from all windows based devices (Servers & Workstations) to a single server where detailed analysis can be undertaken through the use of dashboards and summarized data

- **LME ELK Server - LME-PBR-KL1**

- This server is used for storing and analyzing the collected logs
- O/S - Ubuntu

- **LME Event logging Server - PRTG-PBR-KL1**

- This server collects and forwards the logs from the client computers to the ELK server
- O/S - Windows 10

- **LME Clients**

- All devices that are configured for monitoring
- O/S - Windows devices

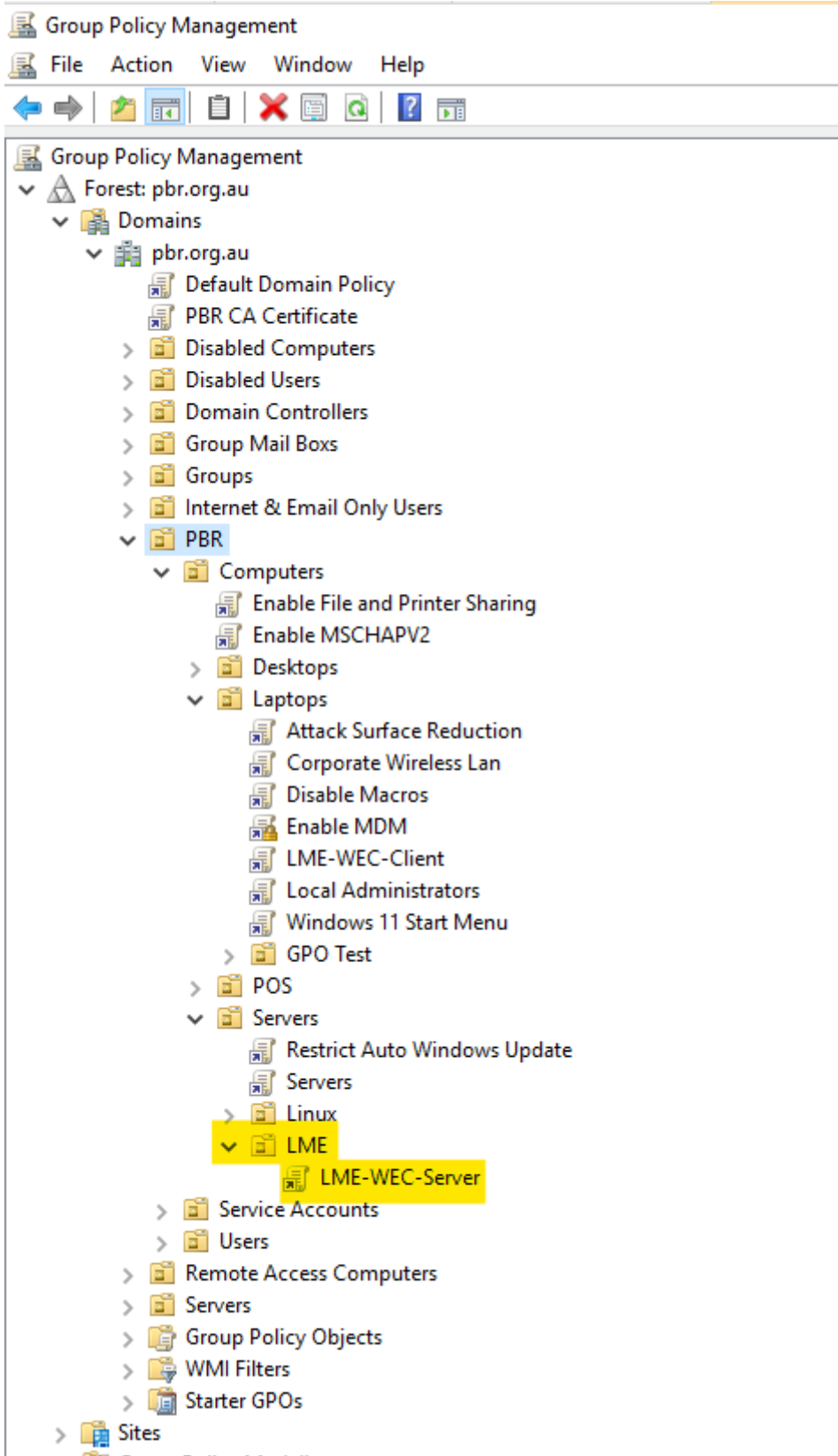
There are 2 Group Policy Objects (GPO's)

LME-WEC-Client - This GPO forwards event logs from the client computer to the Event Logging Server

This GPO is linked to the OU *Laptops & Desktops*. Devices in these OU's will have their events forwarded to the event logging server

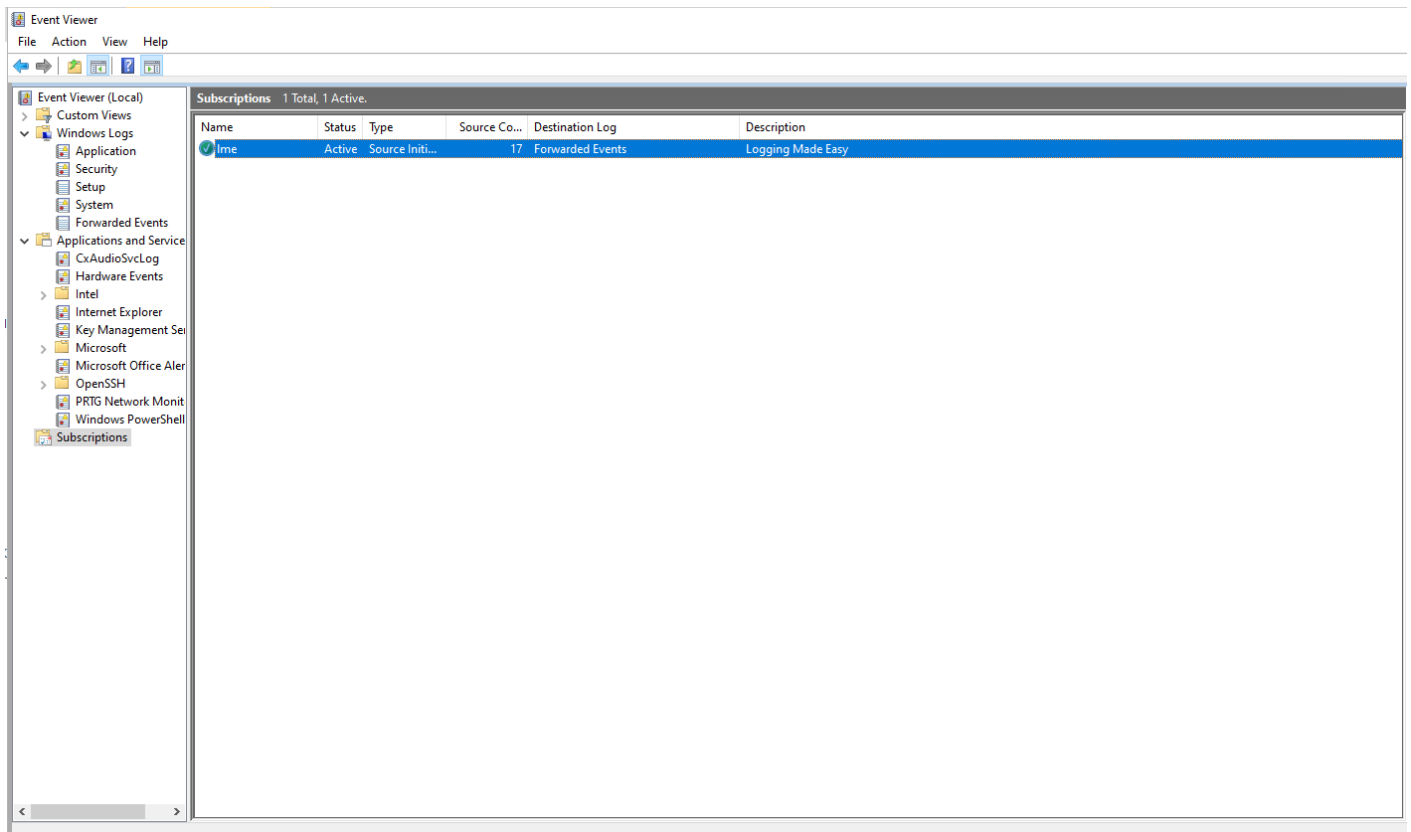
LME-WEC-Server - This GPO enables the Windows Remote Management Service (WinRM) to automatically listen on the network for requests on port 5985 from IP address range 192.168.134.1 - 192.168.134.254

This GPO is linked to the OU *LME*, which is located under PBR\Computers\Servers. The only computer in this OU is the LME Server



On the Event Logging Server (prt-g-pbr-kl1) you can view the number of connect devices (computers that are having events forwarded to the Event Logging Server) by going to Event

Viewer, and selecting subscriptions



All collected logs from the client computers are located in the Forwarded Events section listed under Windows Logs in the event viewer on prt看pbr-kl1

Current log size on prt看pbr-kl1 is 10GB

Log Properties - Forwarded Events (Type: Operational) X

GeneralSubscriptions

Full Name:ForwardedEvents

Log path:%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx

Log size:21.07 MB(22,089,728 bytes)

Created:Tuesday, 23 April 2024 2:33:02 PM

Modified:Thursday, 23 May 2024 4:06:52 PM

Accessed:Thursday, 23 May 2024 4:06:53 PM

☒ Enable logging

Maximum log size (KB):10020480

When maximum event log size is reached:

☒ Overwrite events as needed (oldest events first)

☐ Archive the log when full, do not overwrite events

☐ Do not overwrite events (Clear logs manually)

Clear Log

OK

Cancel

Apply

Full LME Documentation can be found at [CISA LME Documentation](#)

Still to be documented

Are we adding the servers? Can we collect ubuntu logs?

Sysmon purpose & config

Dashboards & reporting

Revision #3

Created 23 May 2024 05:03:41 by David Diamond

Updated 23 May 2024 06:08:43 by David Diamond