PVE ??syslog??????

????

- **PVE 8.2**

??rsyslog

由於 **PVE**已改成 `systemd-journald` 簡化日誌架構，需啟用轉發到 **Syslog**並安裝 **rsyslog**傳送 **log**到遠端

編輯 `/etc/systemd/journald.conf`

```
ForwardToSyslog=yes
```

安裝 **rsyslog**

```
apt install rsyslog
```

新增 `/etc/rsyslog.d/remotelog.conf`

傳送所有 **log**

```
*.* @remoteip:516
```

篩選 **log**，範例為篩選 **sshd**程式訊息包含 **pam_unix**則傳送

```
if ($programname == "sshd" and $msg contains "pam_unix") then {
    action(type="omfwd" target="remoteip" port="516")
    stop
}
```

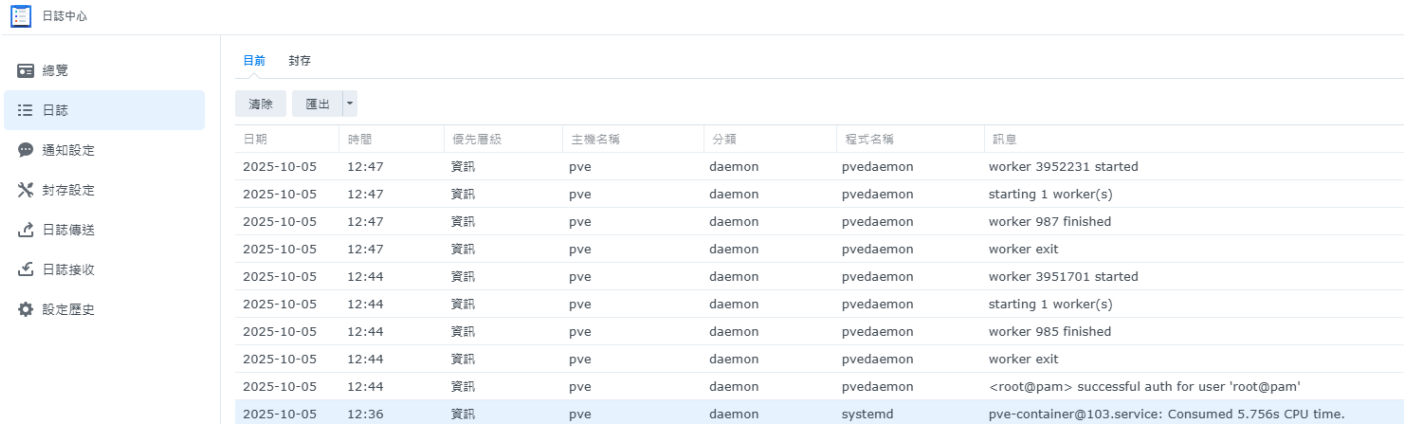
重啟系統服務

```
systemctl enable rsyslog
systemctl restart rsyslog

systemctl restart systemd-journald
```

??

□□ Synology□□□□□□□□ PVE□ log



Revision #2
Created 5 October 2025 04:41:06 by Jason
Updated 8 October 2025 03:06:19 by Jason