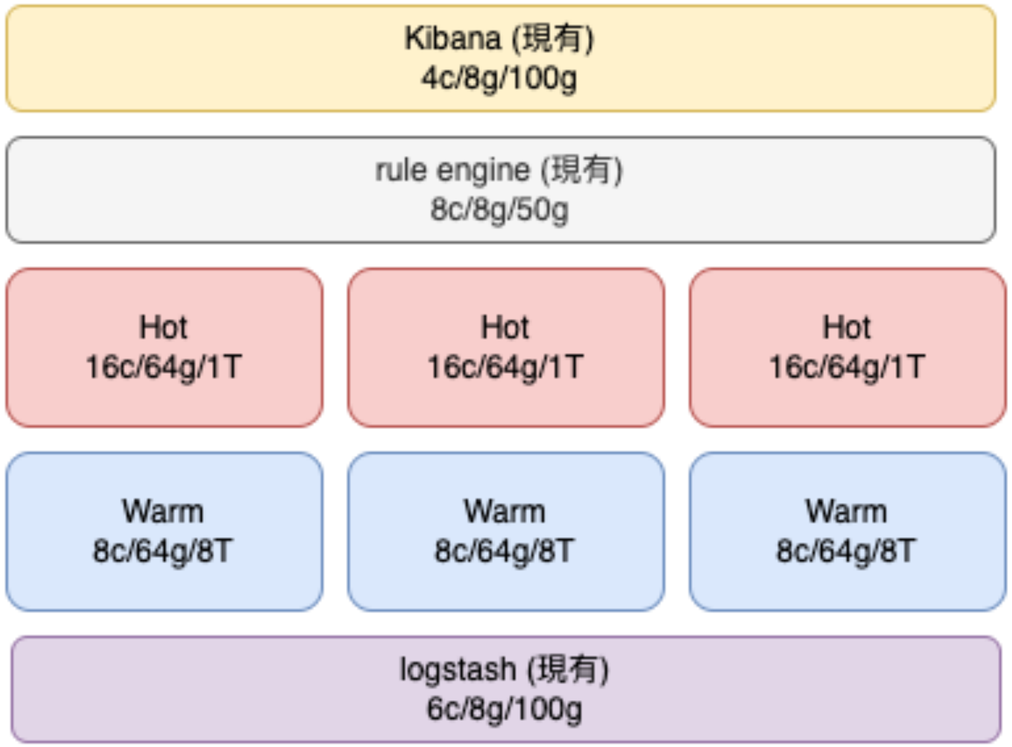
華新 2023 ELK 工作說明

BiMAP Winston

ES 參考架構

log 種類	日流量	月流量
fortigate	100GB	3000GB
ad_server	20GB	600GB
asa	15GB	45GB
asa_equipment	0.7GB	21GB
windows-test		20GB
one-identity		4GB
citrix		1GB
virus		0.4GB
waf		0.3GB
nac		0.2GB
月總量	4096.9GB(4.1T)	



ES 工作計劃

項目	說明
Rule Engine 升級完成	
ES 節點壓力測試&效能分析	1. 針對硬體做效能評估，如 cluster 要擴充，可當成未來硬體的參考。 2. 定期收集 ES runtime 的效能數據。
ES Rolling Upgrade 8.5.3	1. 建置 3 nodes cluster 8.5.3 2. 將 raw data 轉移至新 cluster 3. 拆除舊 ES 4. 重新加入新的 ES cluster 節點
Data Index Review	根據目前資料量，重新調整 replica/shard (有需要的話)