CIA cloud 重啟說明

為了當負責人不在時,代理人能順利處理CIA遇到緊急狀態需要重開(ex:斷電,電力設備維修…etc),留下這篇說明以利處理

1. 目前CIA相關server共有12台,其ip分別為192.168.50.100~192.168.50.111

用途如下:

50.100: Utest (for CIA cloud)

50.111: AV\_scanner (static analysis)

50.101: Center [101~105 1 group]

50.102~105: Analyzer

50.106: Center [106~110 1 group]

50.107~110: Analyzer

2. 目前根據設定檔,樣本流程如下:

Utest -> Center -> AV\_scanner [-> Analyzer] -> parsing -> rule\_generate -> End

3. Utest, Center, Analyzer均在rc.local中有設定好開機腳本會自動執行對應的程式,但是AV\_scanner雖然docker部份會自動開啟,但Restful server的部份無法自動執行,需手動設定啟動,因此在這段時間所有送到AV\_scanner的task均會失敗,因為沒有服務接下來執行並回傳,因此CIA無法根據回傳結果繼續執行,因此在手動關Utest機器前(若有時間),需上web介面將CIA的服務改成暫停中,這樣只要Utest仍在運作,task會被停在Utest這邊不會後送到CIA,也不會進到AV\_scanner了; 若是不幸來不及將Utest的CIA服務手動中止,那開機之後到我們手動停止服務為止所有的task將失敗

4. AV\_scanner restful server重啟方法: 在rc.local設定下,AV的111在重開時會將docker還有vncserver都開好,這時要利用vncviewer進入到5901port, 然後在開啟的終端機,將路徑移到/root/jee-latest-released/eclipse/ 執行./eclipse然後在底下的視窗選擇綠色的restart server鈕開始執行,當console跳出init csf, init cloud字串就開好了,將視窗從server分頁移到console分頁以監看後續跳出的提示字串

5. 在step4做完時理論上整個系統就能正常運作,但是為了方便監看狀況,需要從111當跳板連到101及106,開2個putty視窗各自連到101和106,並且在101和106上面用screen –a 開好6個分頁,前5個依序連上對應的ip(101~105, 106~110), 前5分頁各自以ps –ef | grep center(analyzer) 取得id再以kill 將程式終止,手動以java –jar cia\_XXX(center or analyzer) [NTU 2.5].jar啟動,要先啟動center再啟動analyzer

6. 在監看視窗也都開完後,若一開始就暫停Utest服務就可以打開恢復運作,若是後來才手動停止的,要先去CIA的 web介面h2 console將執行中的所有task手動將其status改成1後再開啟Utest的CIA服務