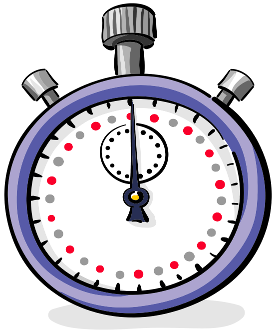
Taifon Your Solution Partner

IBM Guardium 教育訓練
Guardium 操作介紹

泰鋒電腦 洪禮育

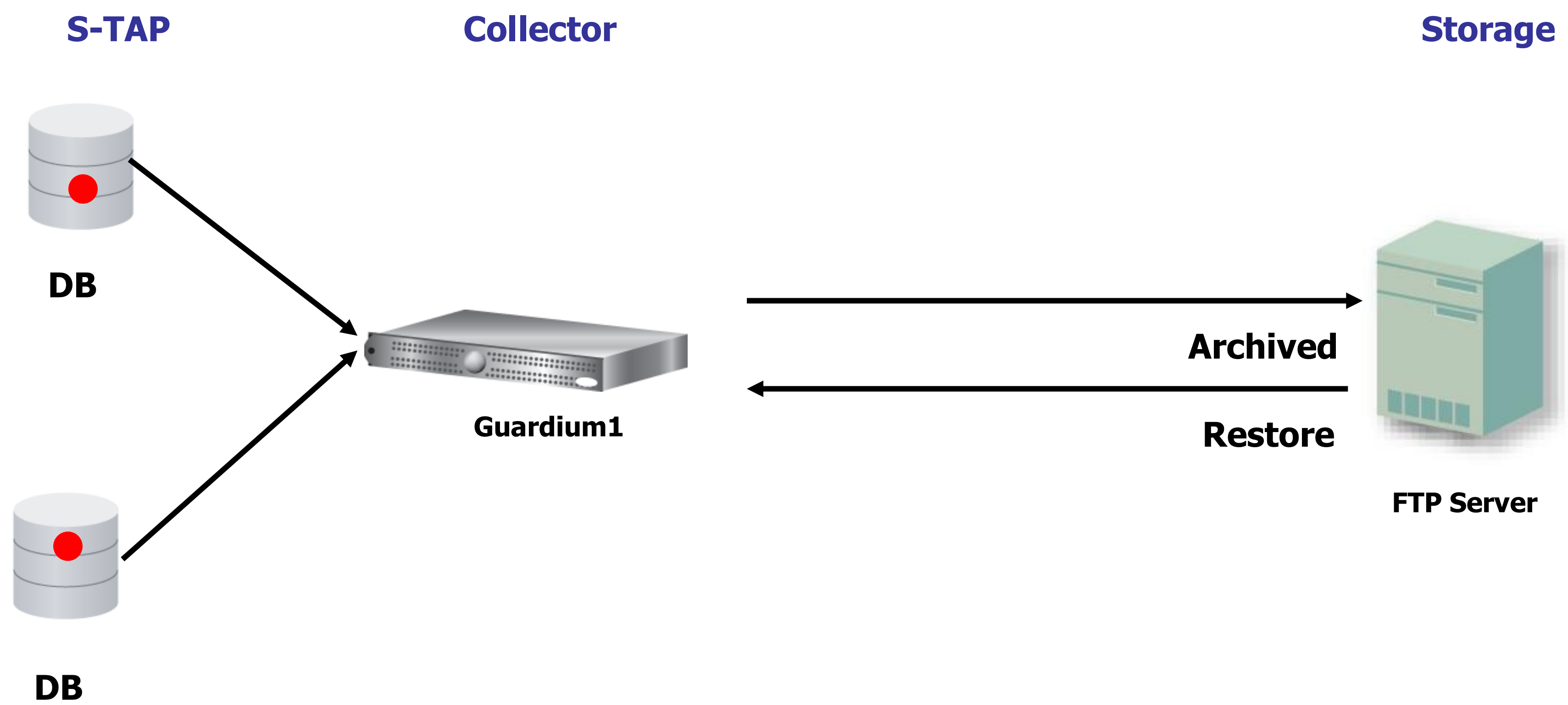
簡報綱要

- 系統基本管理
- 資料管理
- Policy管理
- 中央控管機制
- 資料還原
- 帳號管理
- 稽核使用者-報表操作
- 稽核使用者-報表製作
- 稽核使用者-每日稽核報表
- 稽核使用者-群組功能操作
- 問題與討論



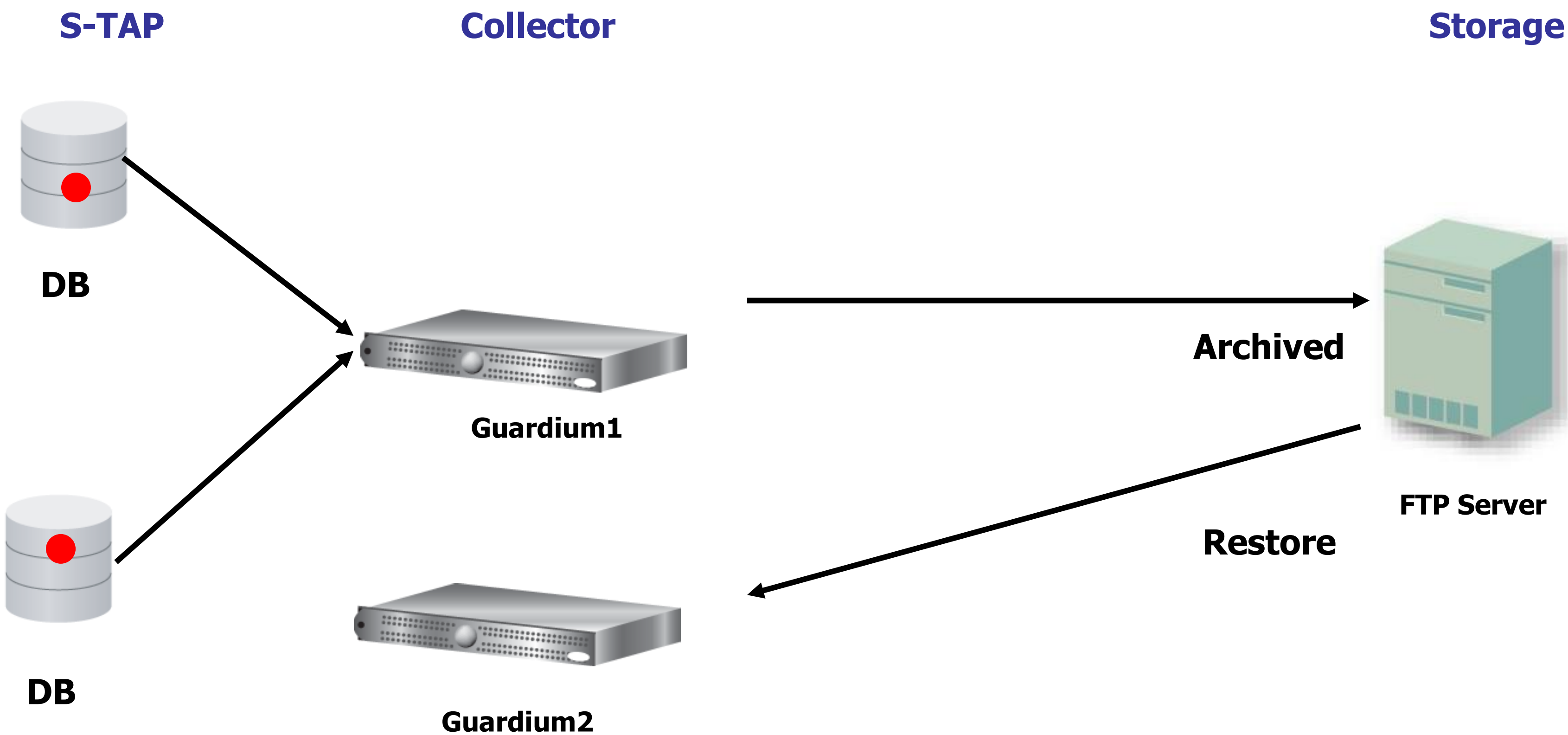
系統基本管理

基本Guardium 建置環境



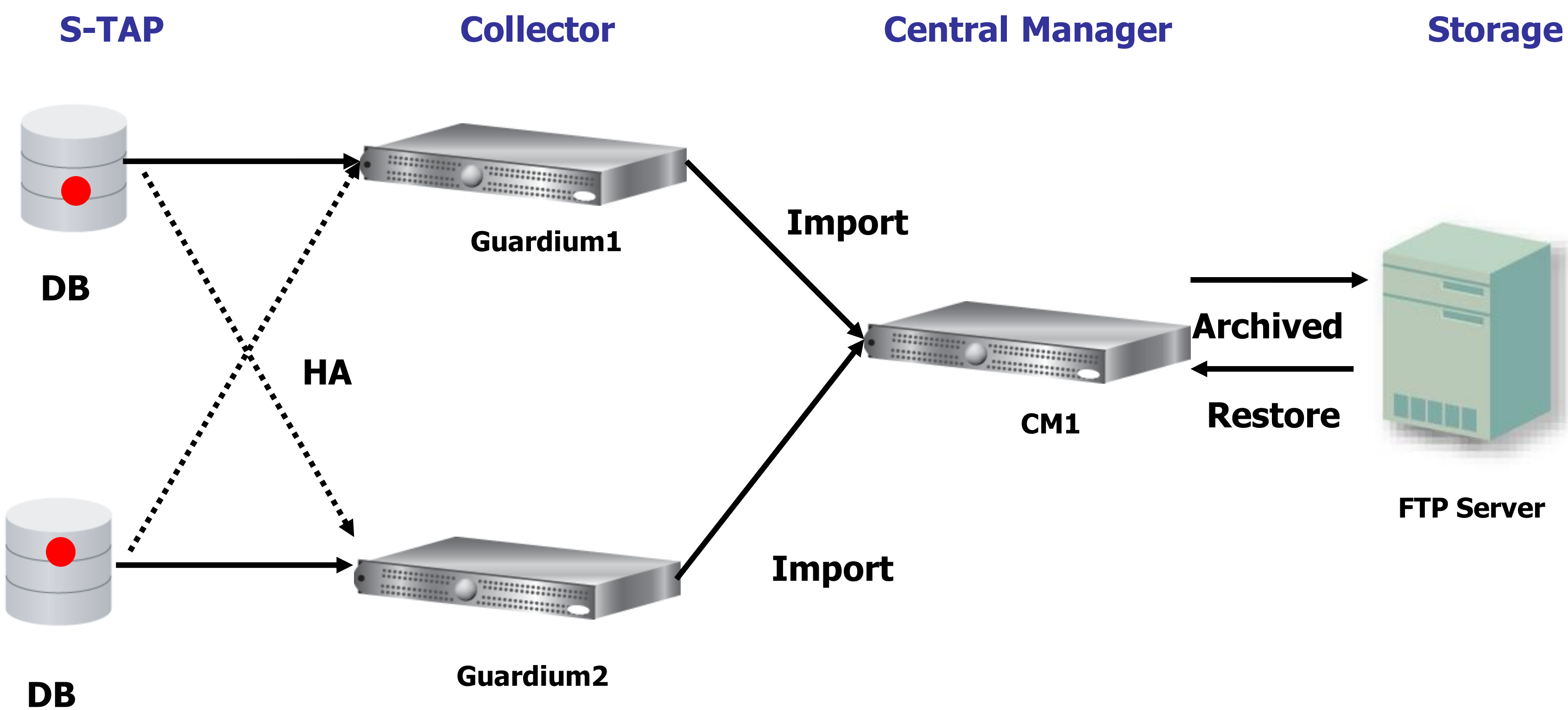
IBM x3650M4
300G SAS x8
Raid 0+1

較佳Guardium 建置環境



IBM x3650M4
300G SAS x8
Raid 0+1

建議Guardium 建置環境



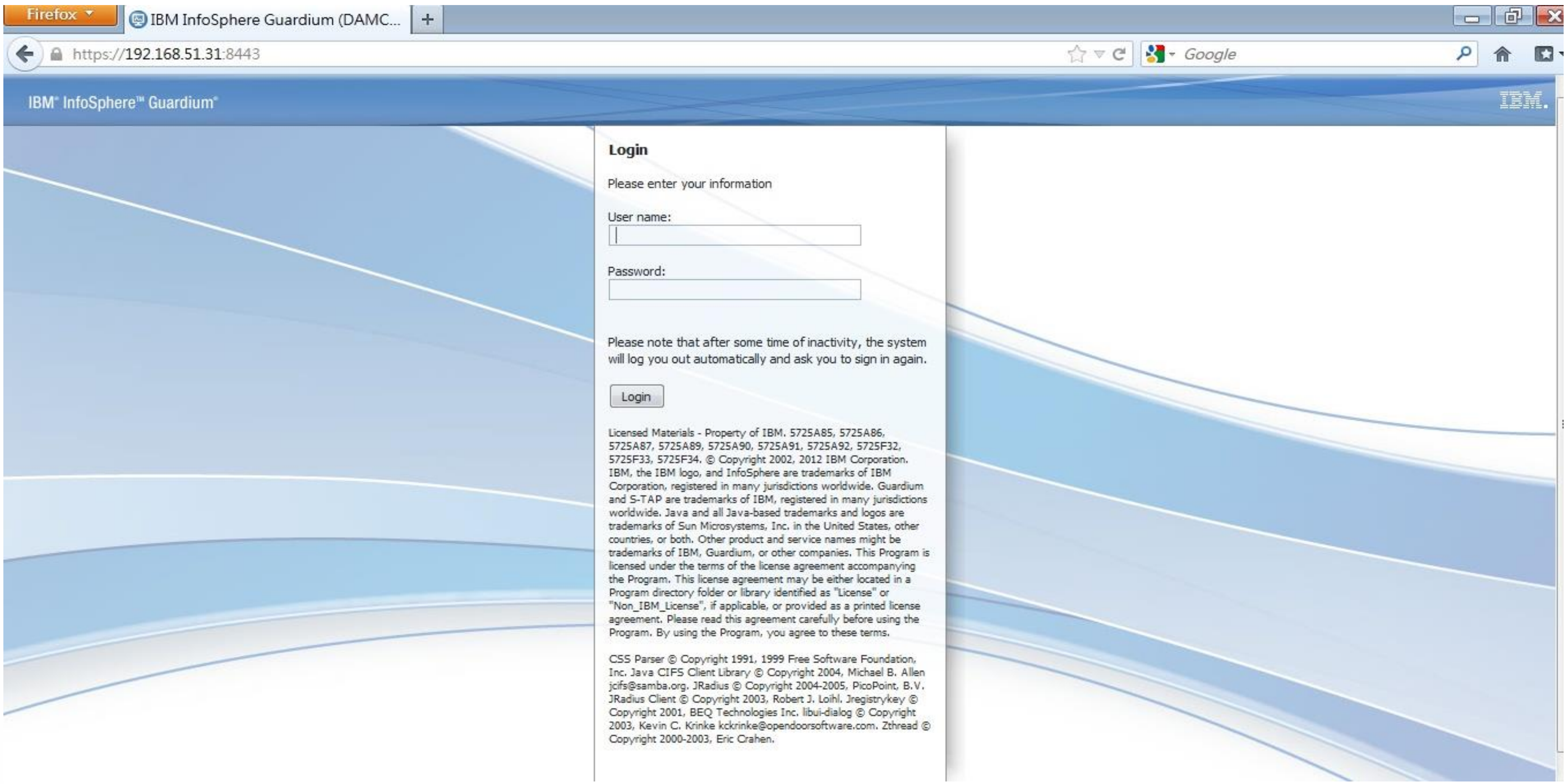
IBM x3650M4 300G SAS x8 Raid 0+1	IBM x3650M4 300G SAS x8 Raid 0+1

連線方式

透過Firefox或IE(另需安裝SVG Viewer)瀏覽器

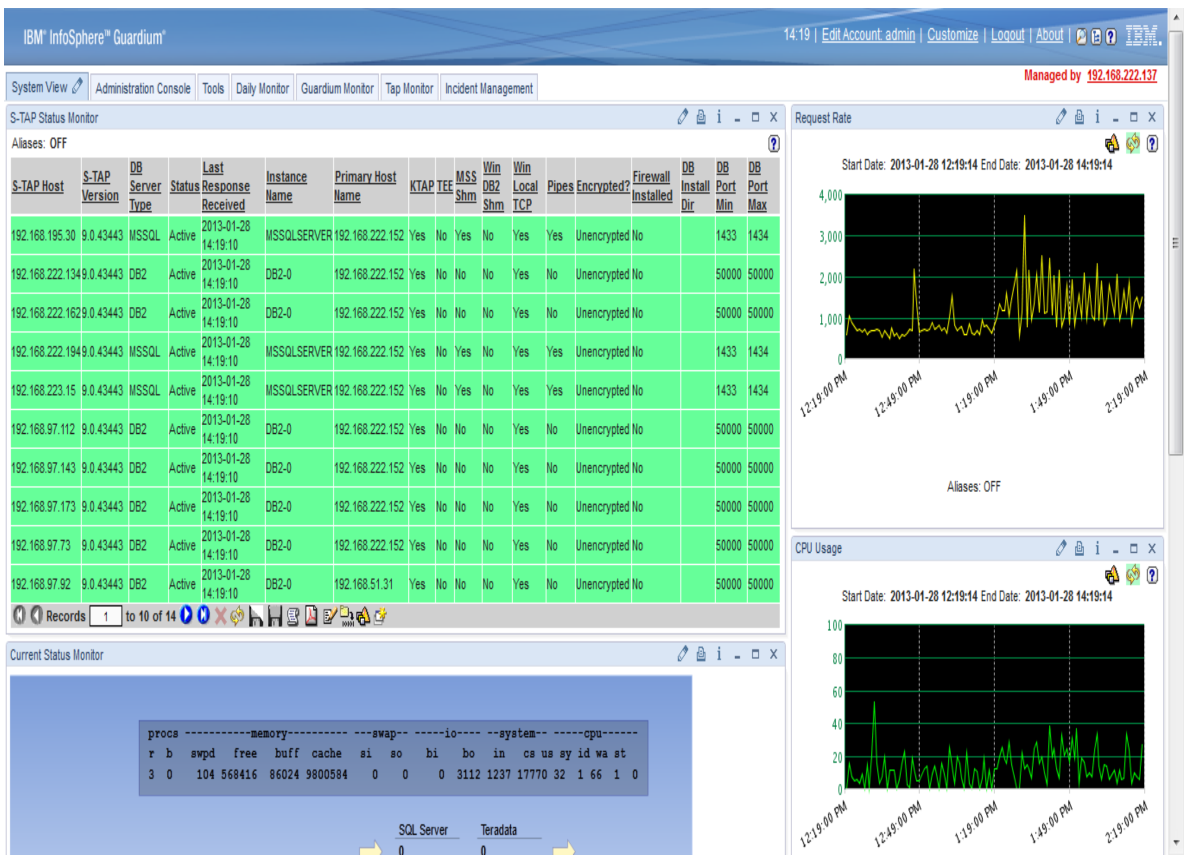
輸入https://<guardium-server>:8443 輸入登入帳號（CM主機 Collector）

例如：https://192.168.51.31:8443



主管理者畫面(Collector)

功能名稱	功能簡介
STAP Status Monitor	Agent運作狀態
Current Status Monitor	SQL Guard硬碟使用狀況與資料收集量分佈圖
Request Rate	Request的比例分析圖
CPU Usage	CPU使用狀況分析圖
Logins to Guardium	登入SQL Guard的使用者名單
Scheduled Job Exceptions	已排定Schedule的任務執行狀況

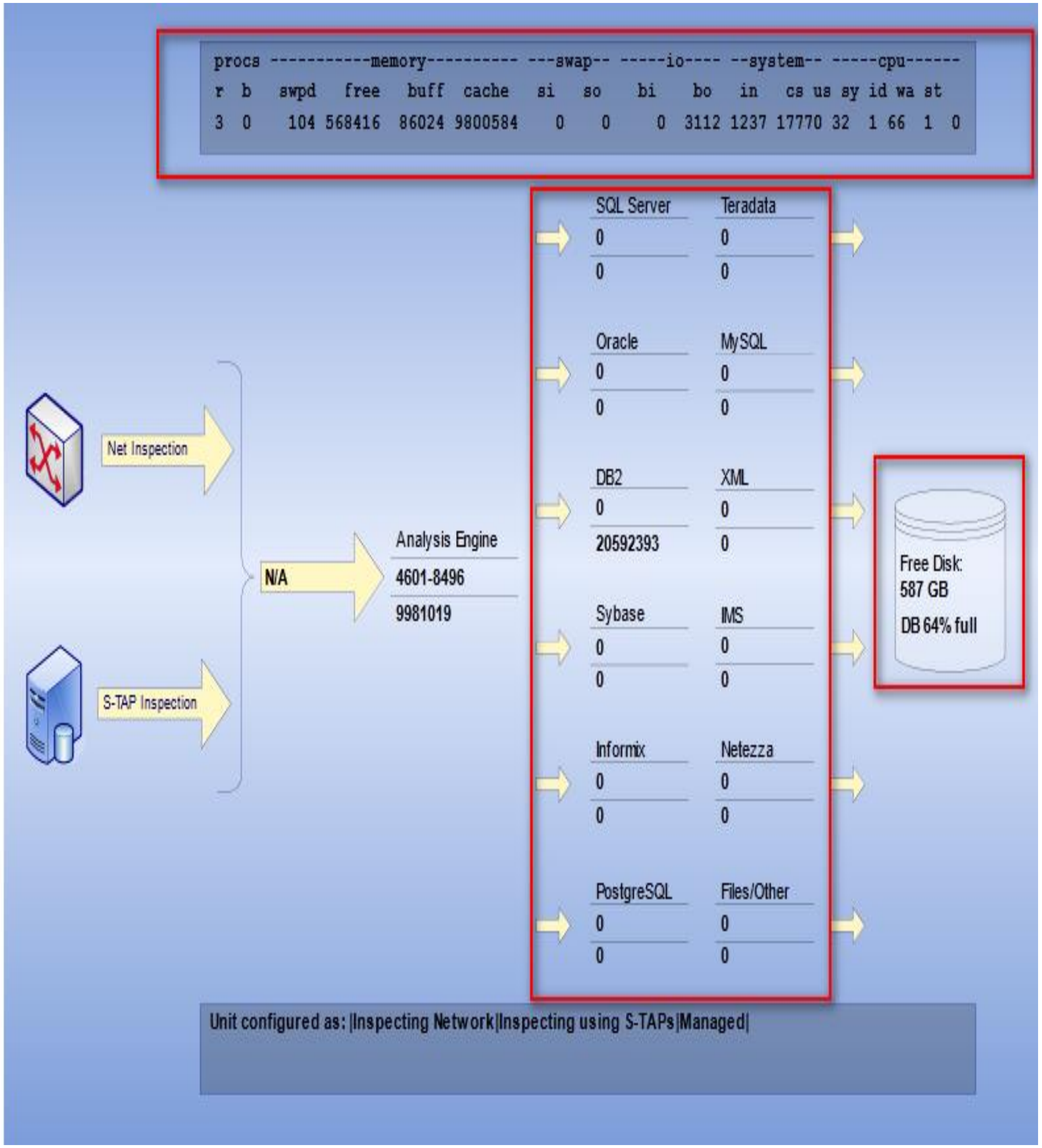


用admin user登入畫面

若S-TAP運作正常則為綠色，若為紅色則監控端STAP服務可能異常

HA機制運作中，若Collector異常會自動切換至備援機，恢復後會切回原機運作

主管理者畫面(Collector) -續

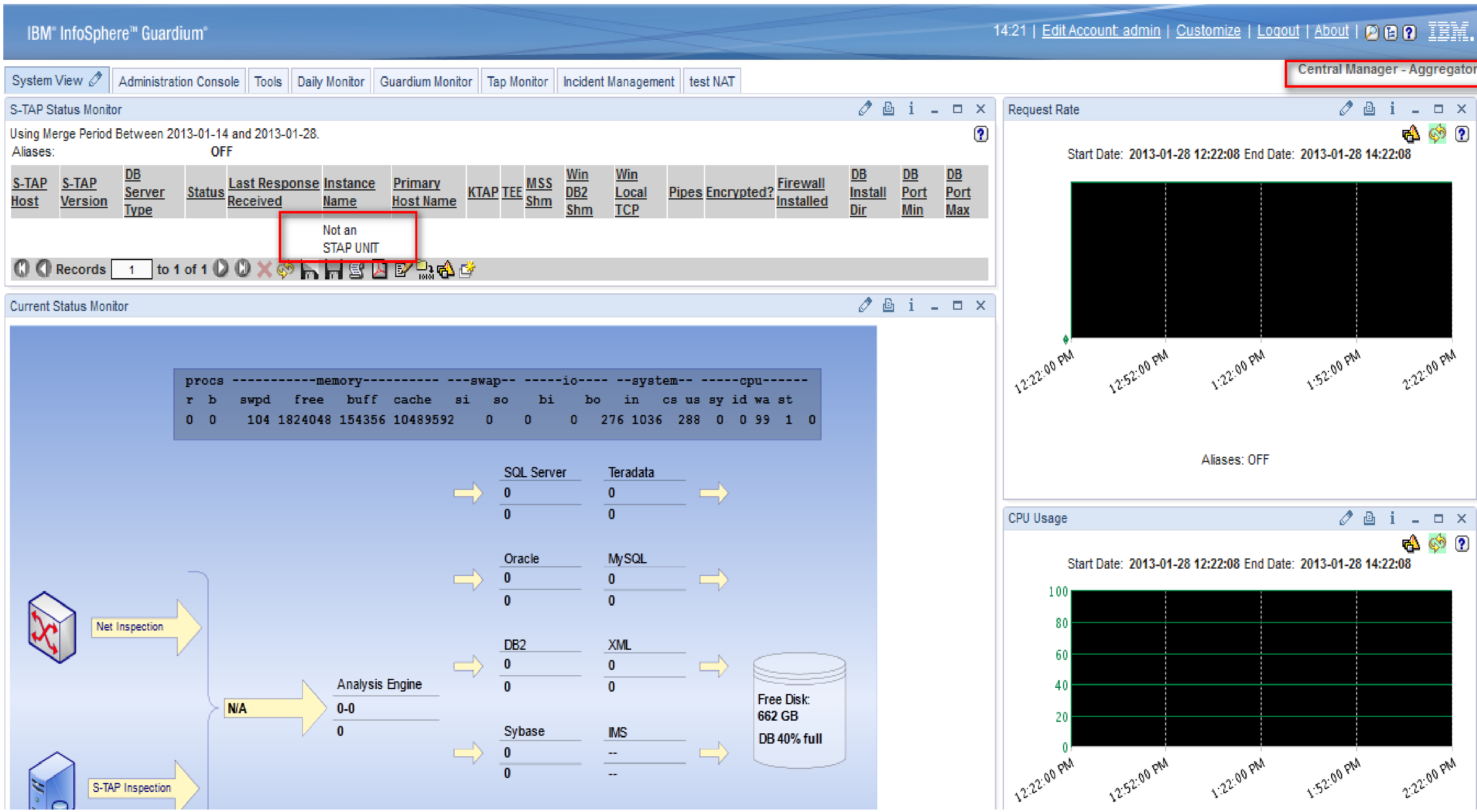


下方圖示可查詢到:
1. Guardium主機負載
2. 各DB主機流量狀況
3. Free Disk空間,
需注意之後DB Full其值不要超過90%,超過其服務會停止,將收不到流量

主管理者畫面(Central Management /CM)

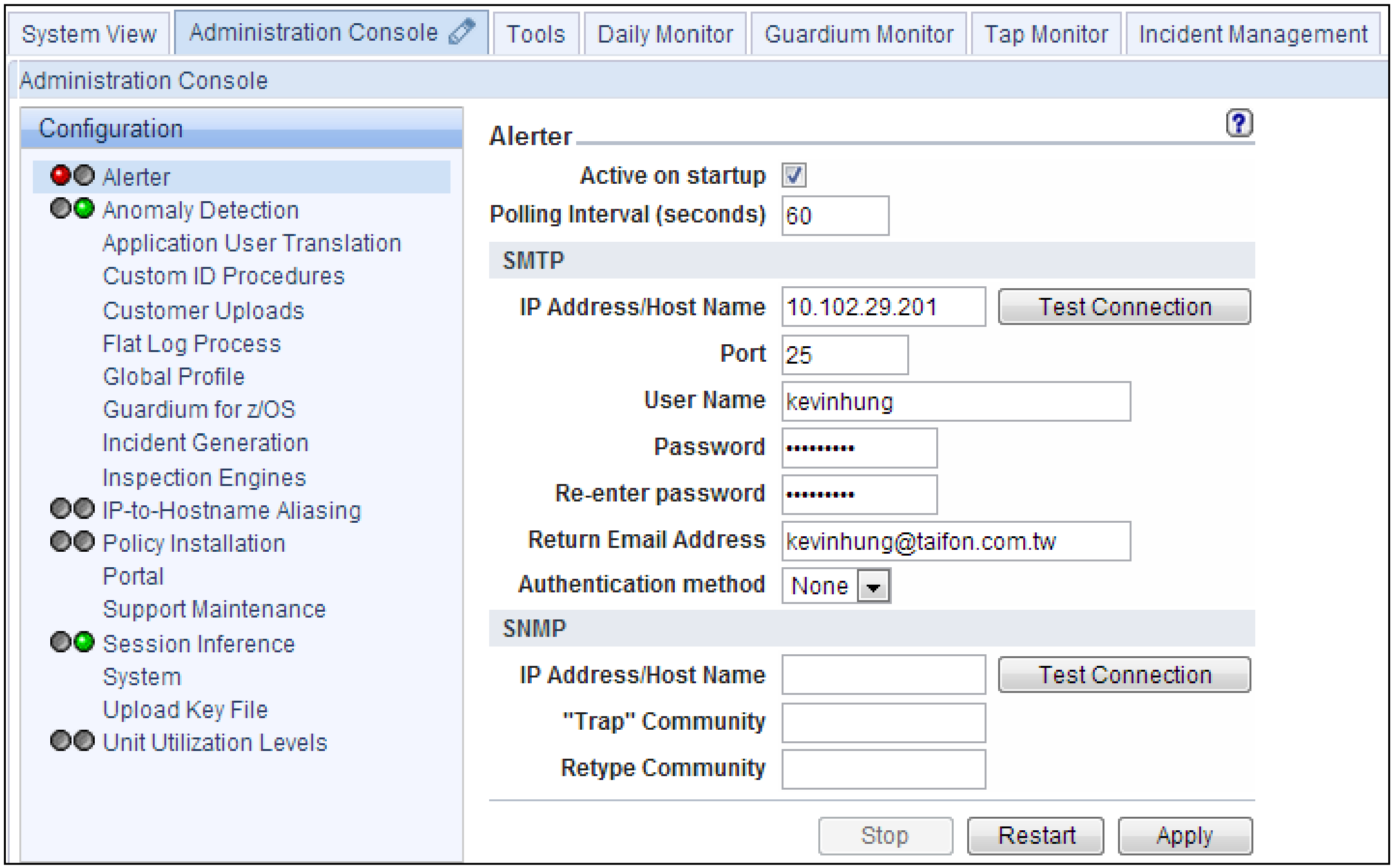
用admin user登入畫面

CM 做為中央控管主機,本身並無收集流量,於S-TAP Monitor為空白



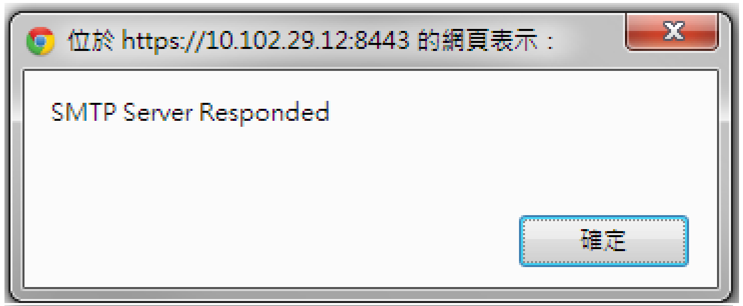
Administration Console設定-Alerter

系統發出Alerter
的Mail相關設定

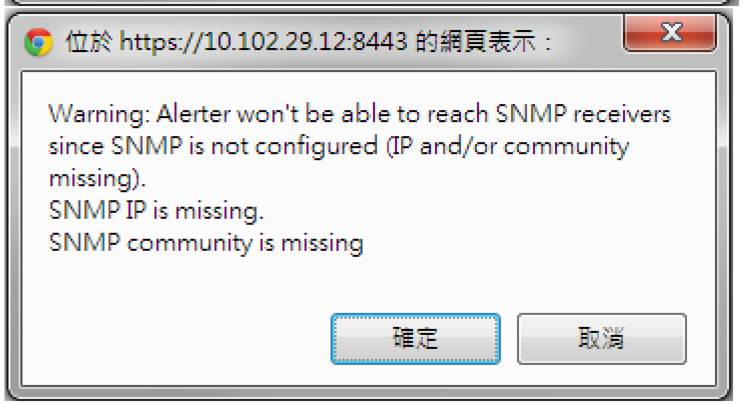


IP Address/Host Name	SMTP IP位置
Port	SMTP Port號
User Name	信箱寄信者名稱
Password	輸入密碼
Re-enter Passeord	重複輸入密碼
Return Email Address	發送訊息信箱帳號

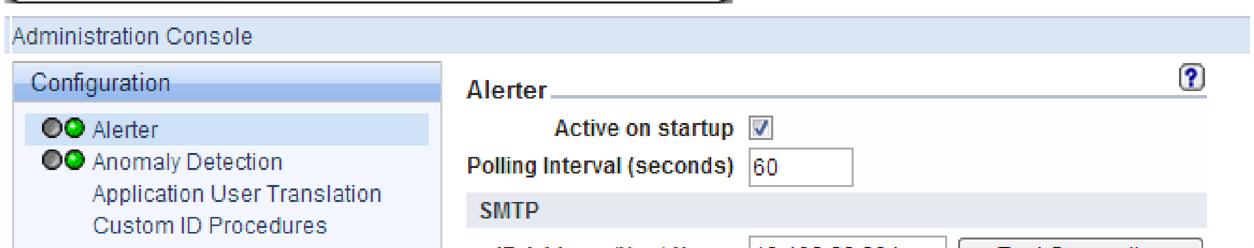
Test Connect
For SMTP



Apply
SNMP 錯誤, 可忽略



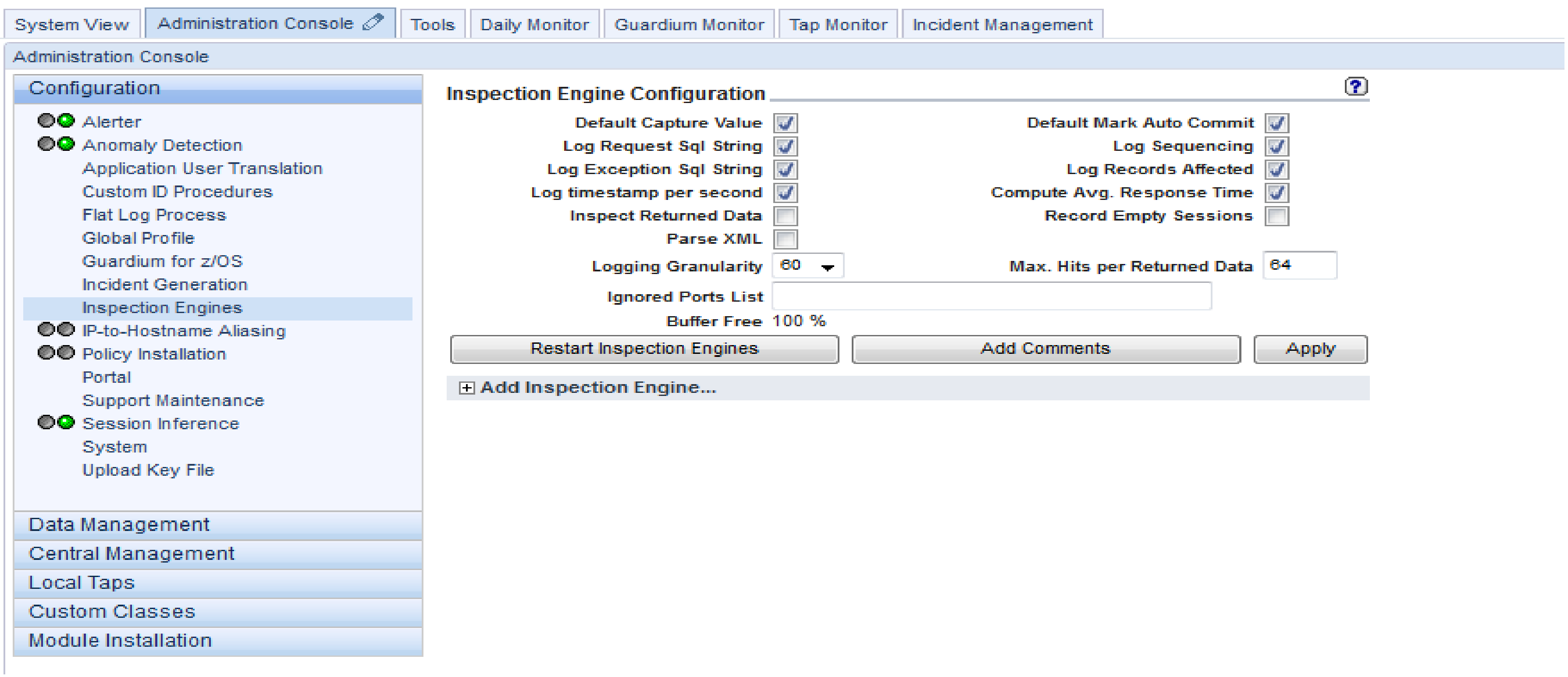
Restart
需出現綠燈



Administration Console設定- Inspection Engines (Collector)

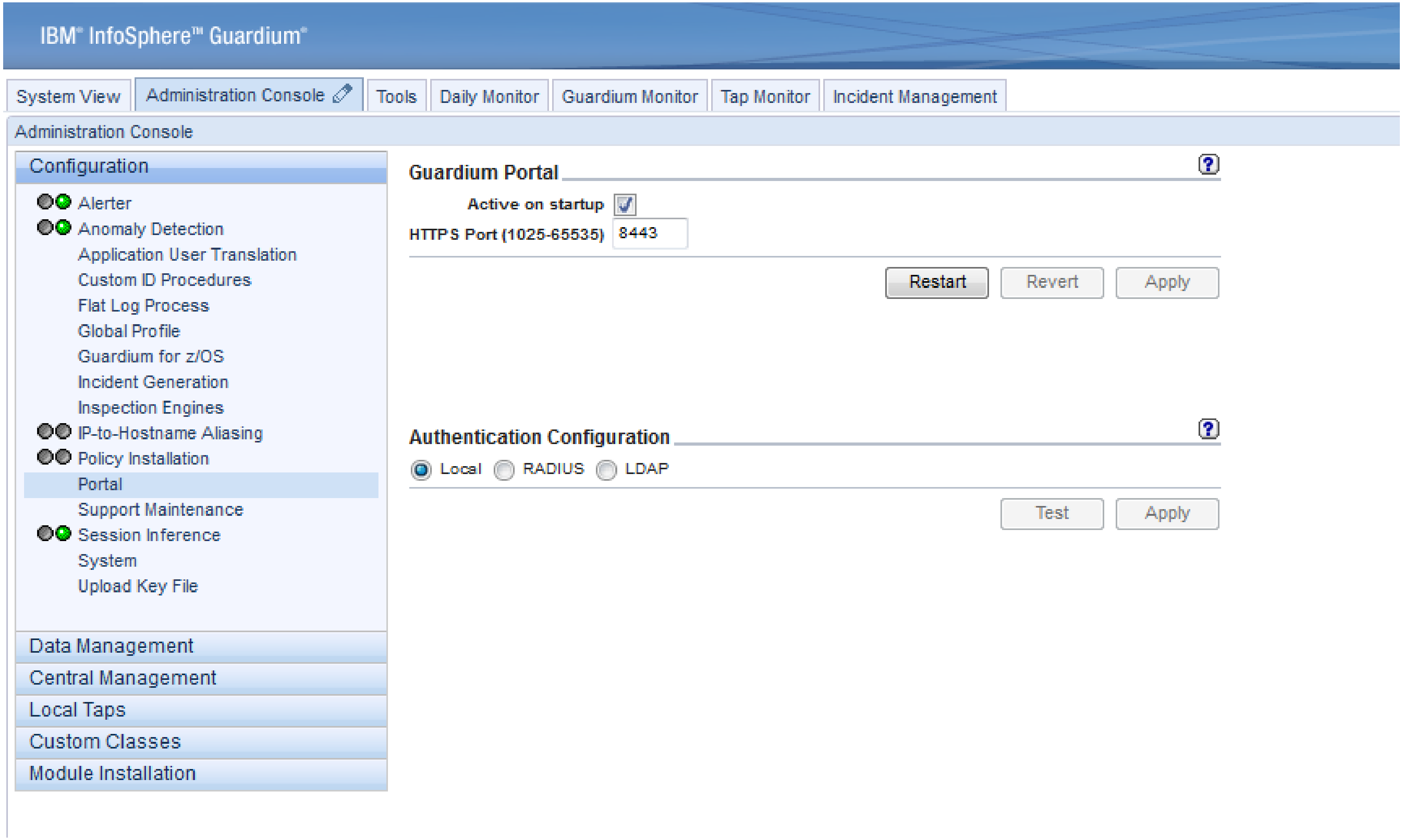
"Inspection Engine Configuration" 決定要收集資料的內容,有修改過需Restart

或若採用Port Mirror方式來監控主機,也是於此設定Add Inspection Engines



Administration Console設定- Portal

設定視窗登入SQL Guard時https所使用的Portal,預設為8443

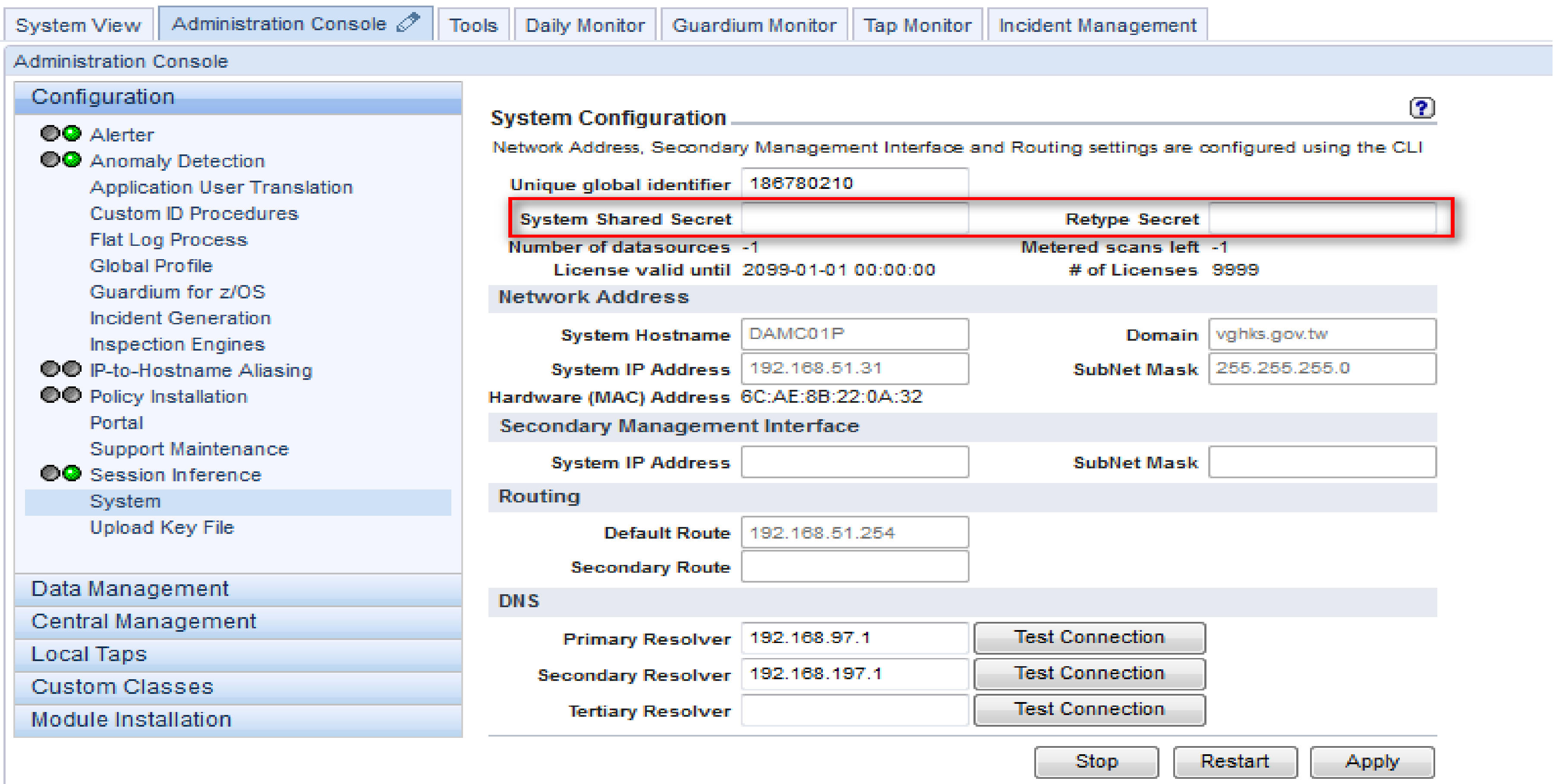


Administration Console設定- SYSTEM

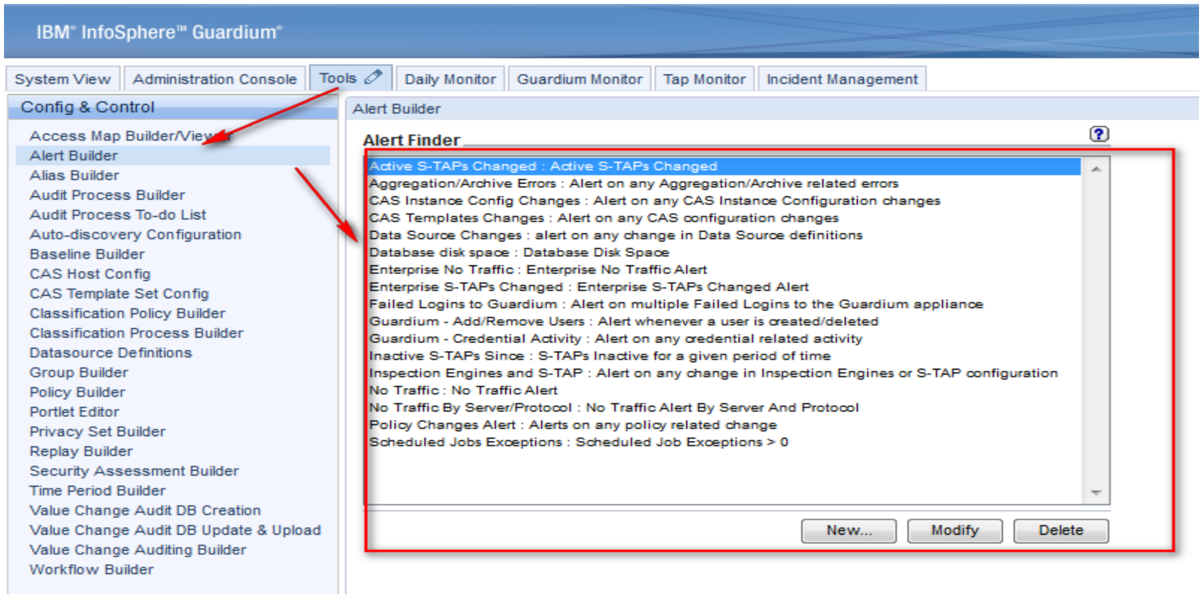
Guardium System設定，包括：

主機名稱、網路設定、DNS設定與Routing設定等

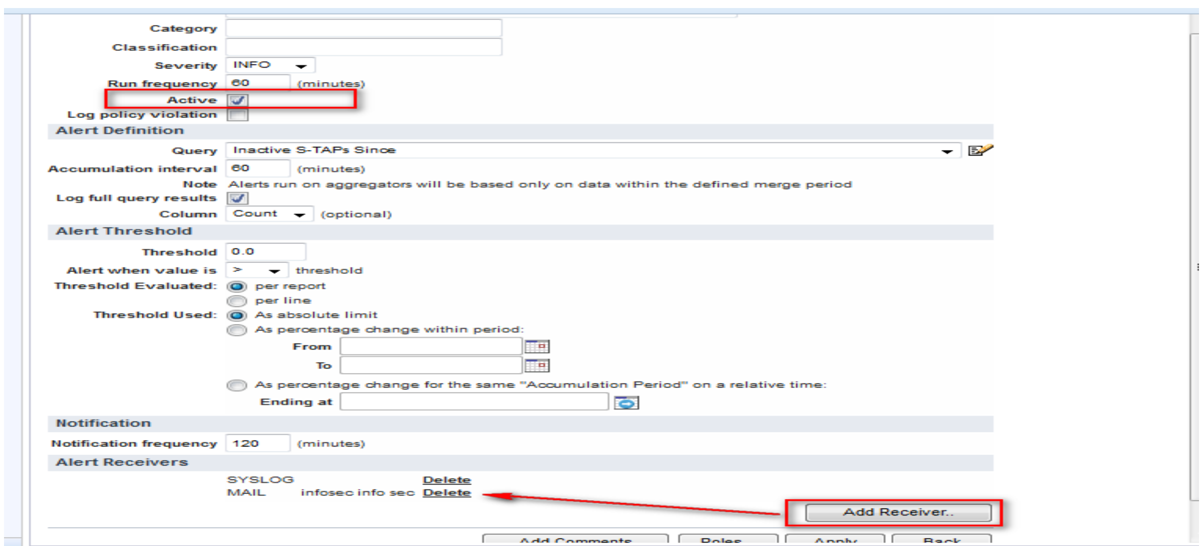
System Shared Secret:各主機需設定相同,CM,資料還原,Export, Import會用到,若不相同將影響該功能



Guardium 系統警示

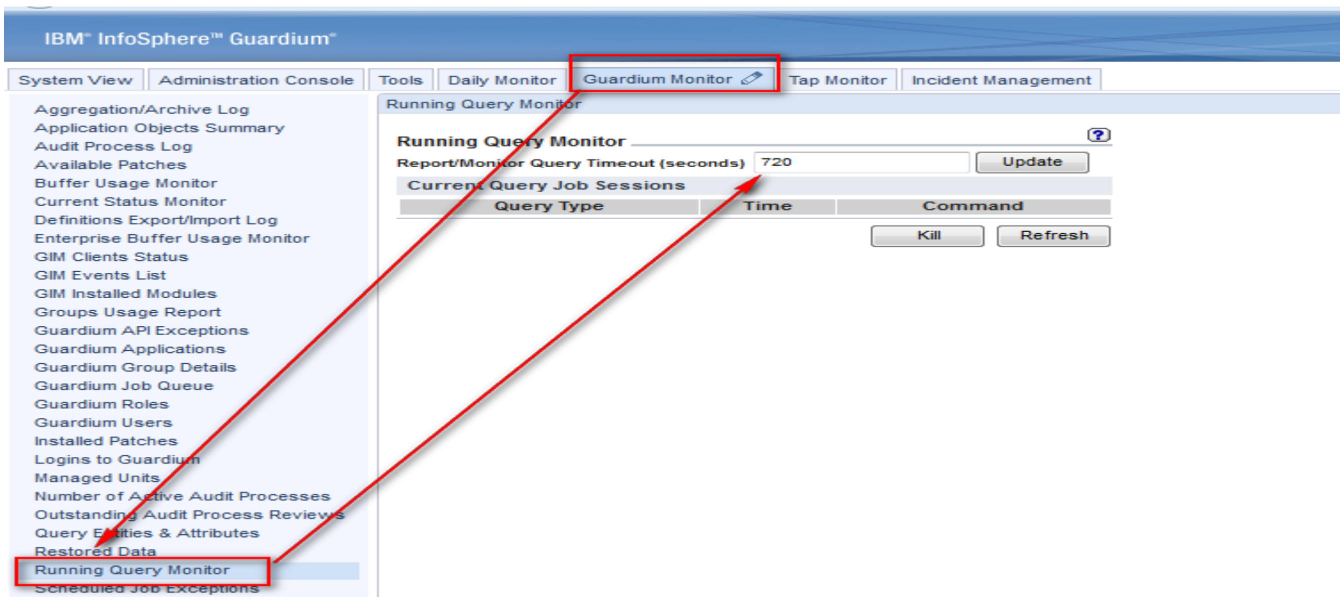


Guardium已內建17種
系統異常警示,
建議啟動
備份異常,
STAP異常,
Guardium DB空間
3個Alert

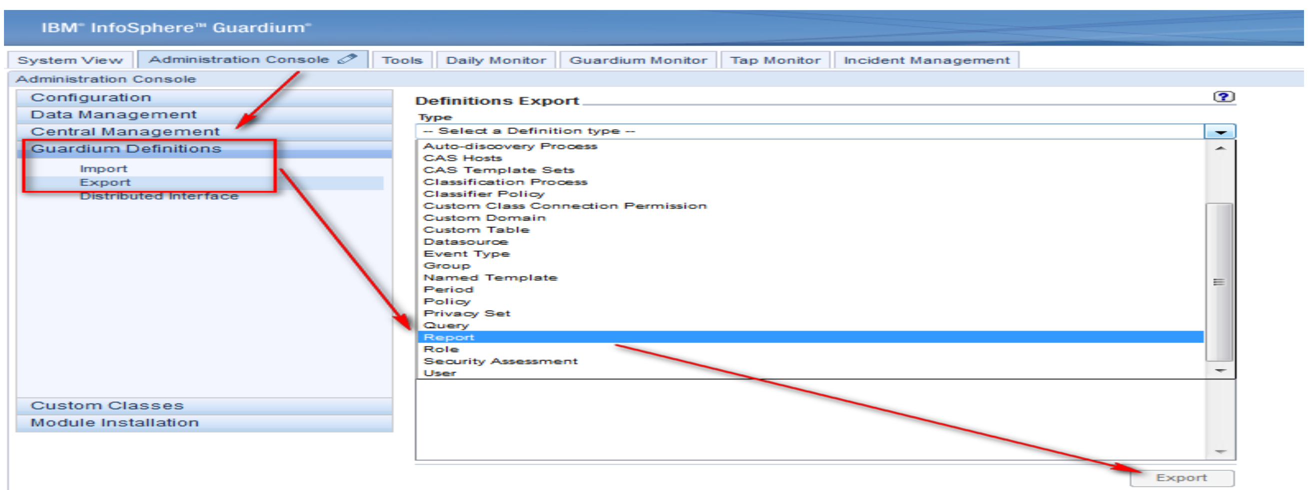


點選進入後,僅要點
選Active,與加上Add
Receiver ,選擇mail,
再選收件使用者
其它用預設值即可

其它常用功能



預設報表查詢時間為300秒,若時間超過則會Time Out,可自行將時間設定拉長

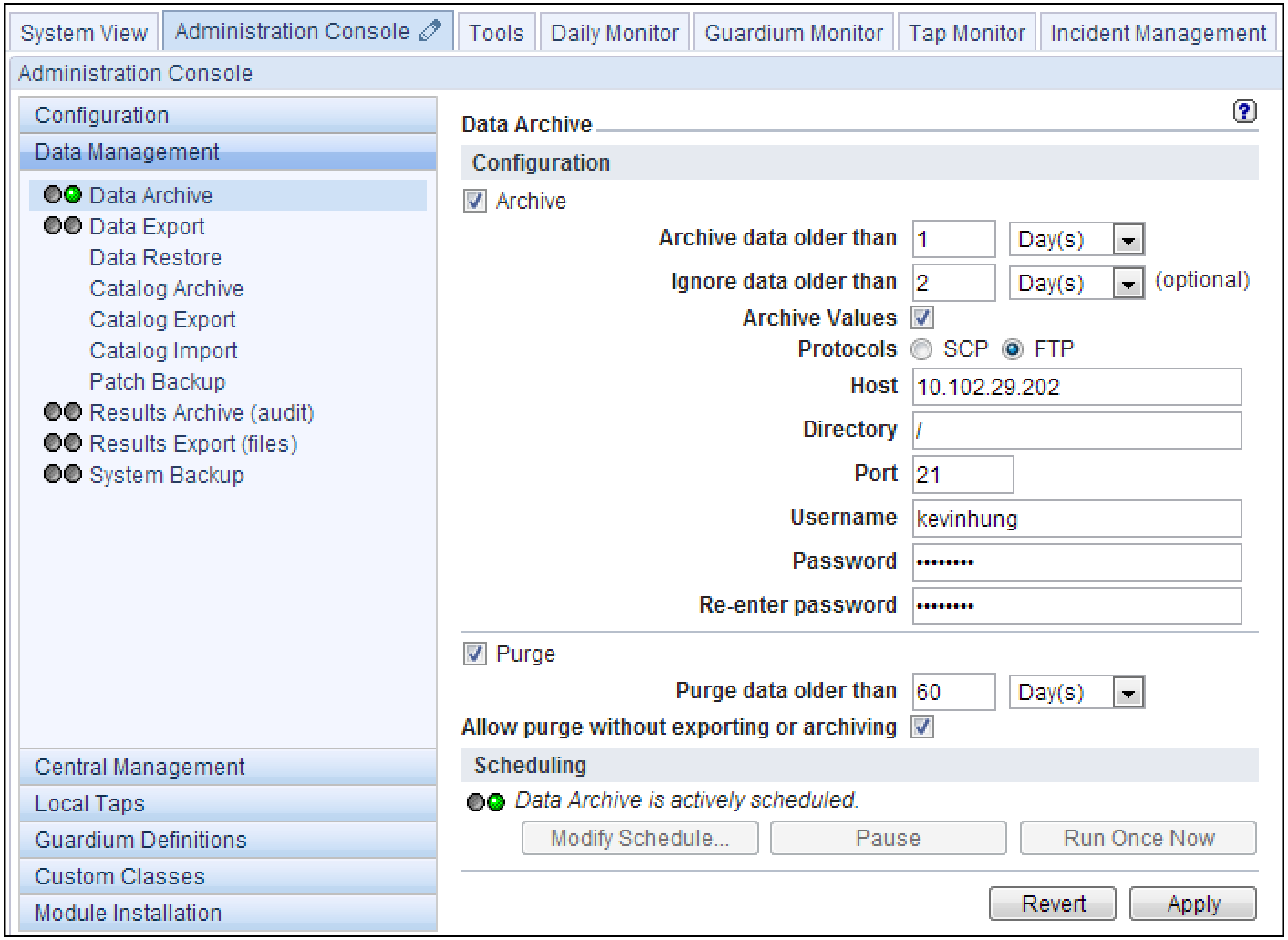


系統相關Policy,報表等設定,可將其Export出來後,Import至另一台主機上,減少設定時間

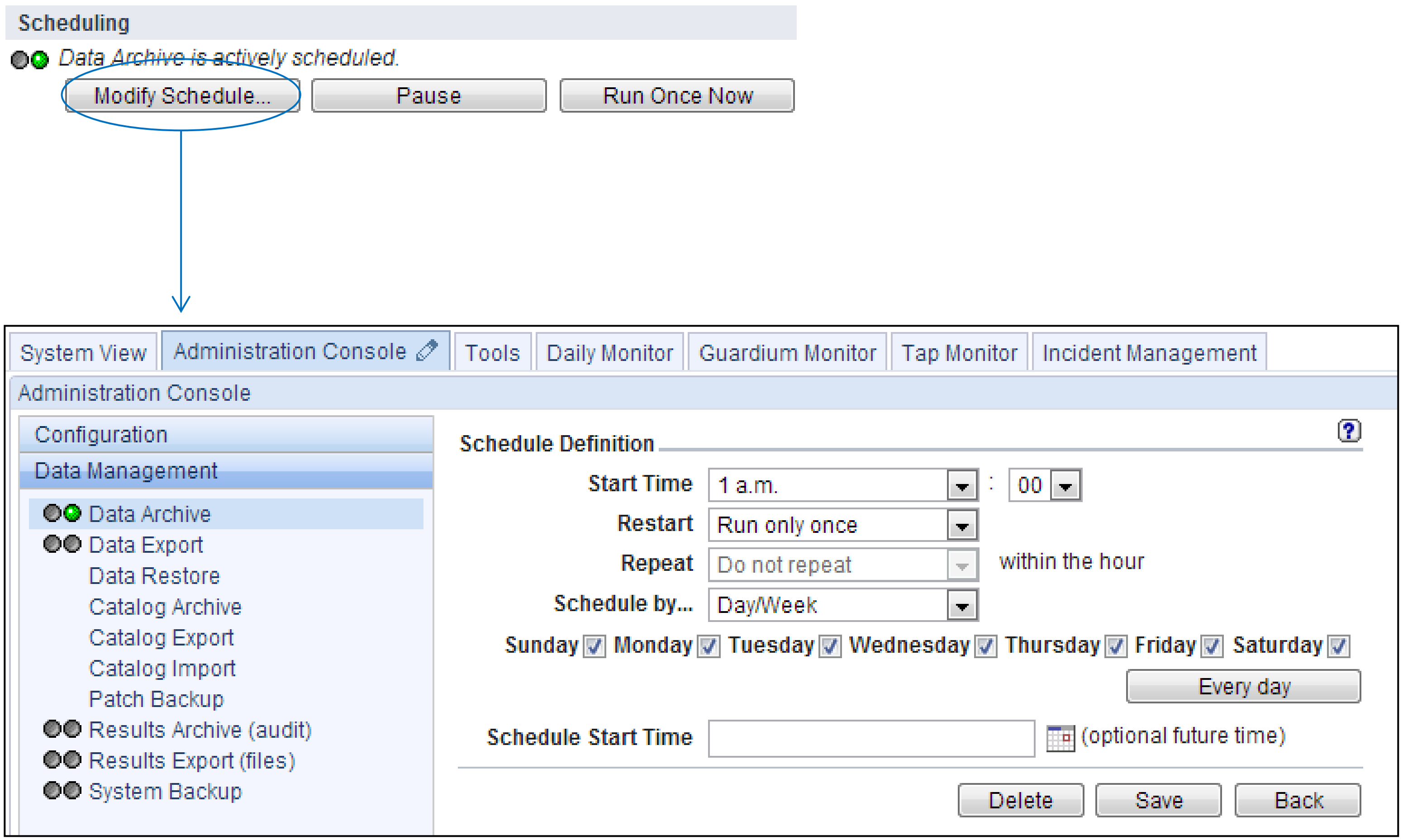
資料管理

Administration Console \ Data Management

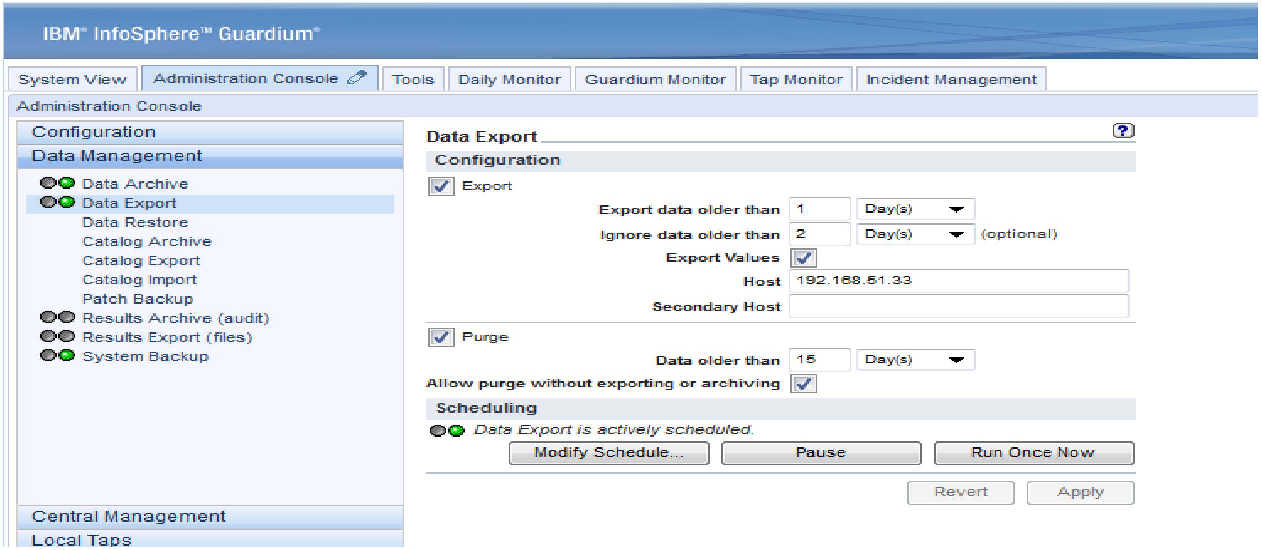
Data Archive



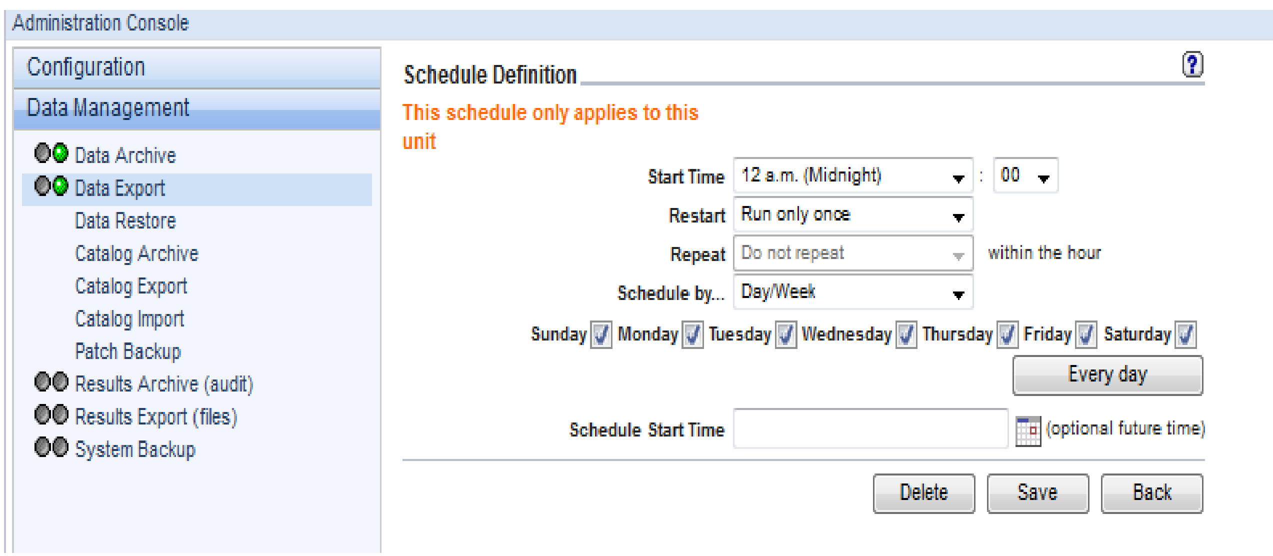
Data Archive : Schedule



Export (Collector -> CM)

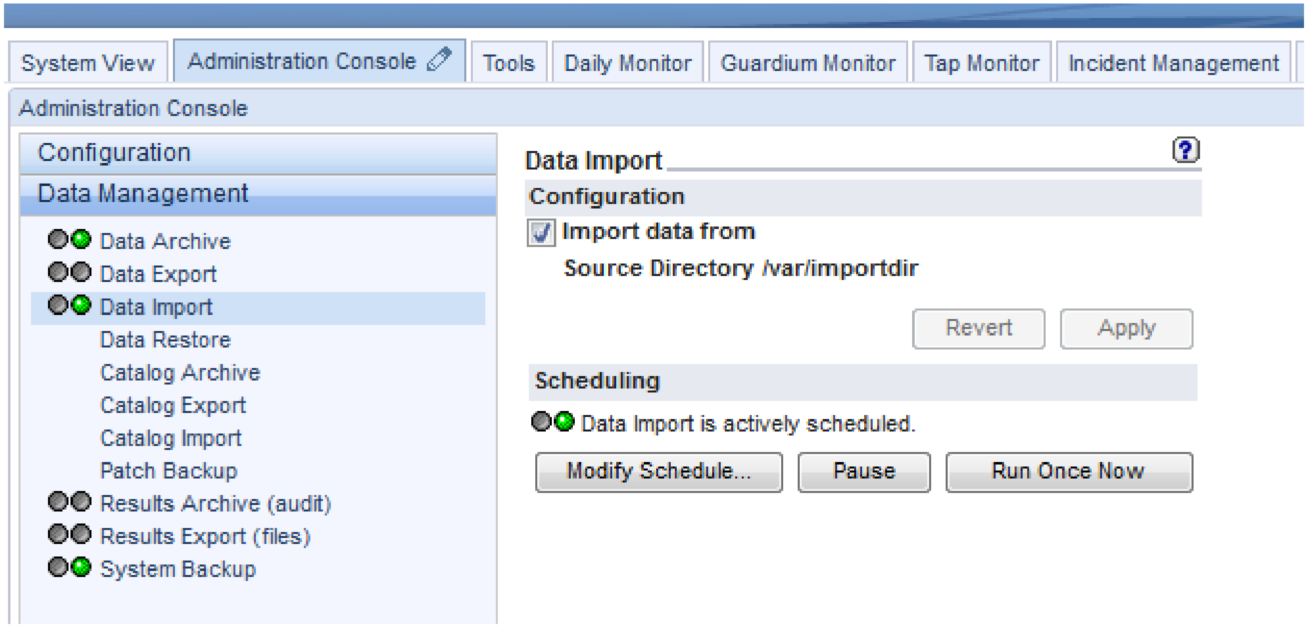


每天匯出資料至CM主機上,並刪除15天(31主機)與20天(32主機)前資料

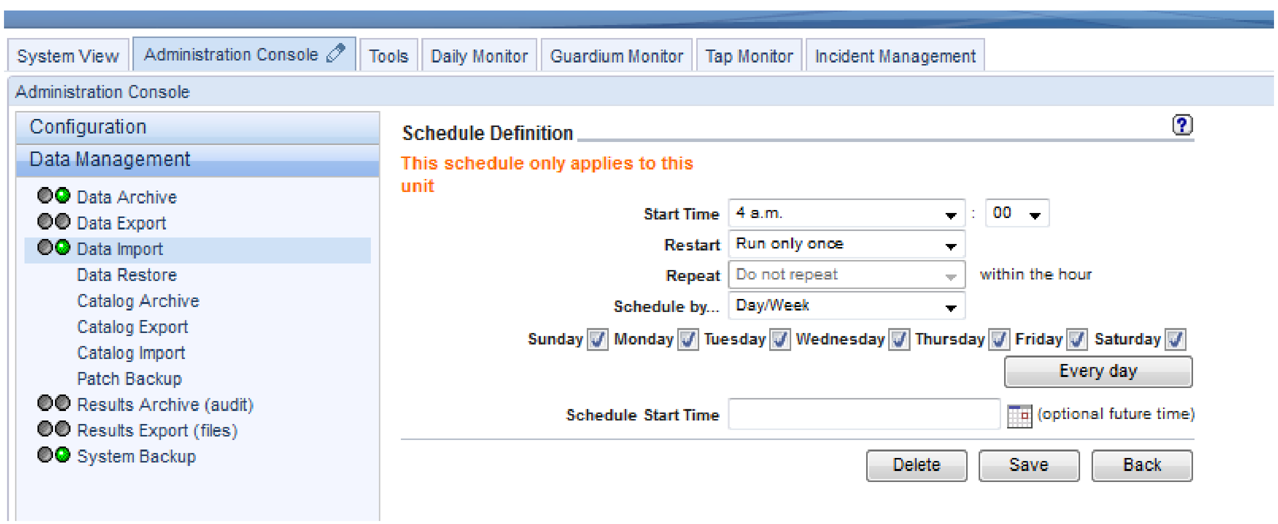


每天清晨12:00執行

Import (CM : Dumpfile -> DB)

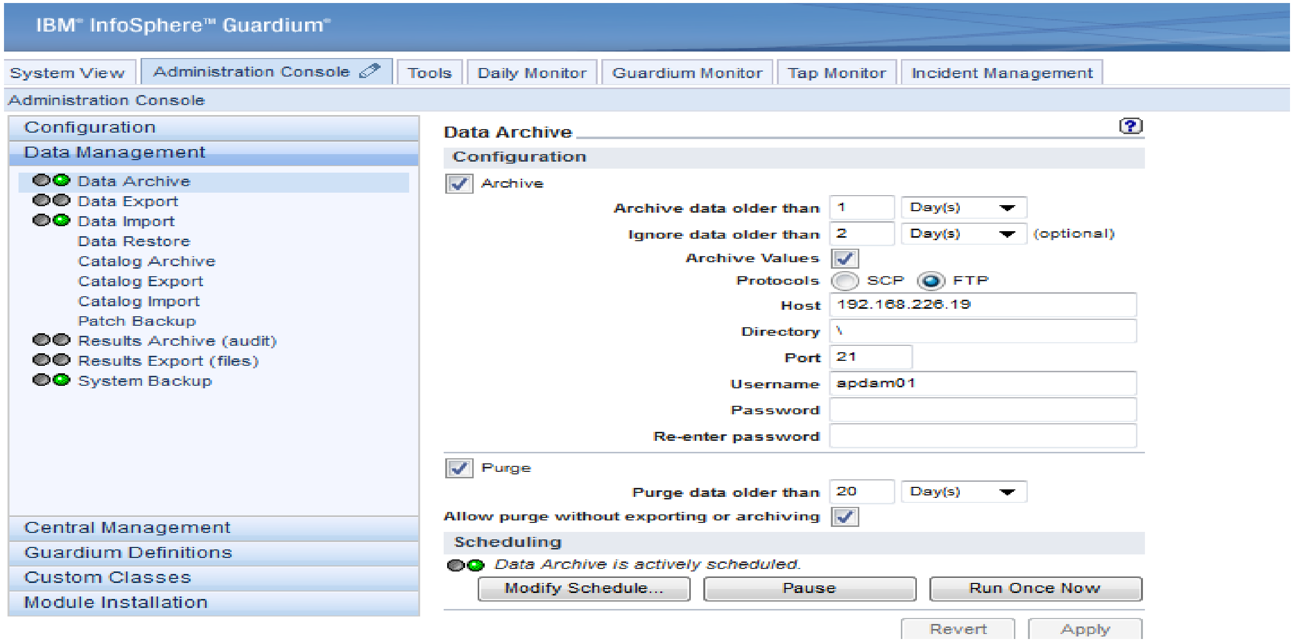


CM主機每天將Collector Export出的資料, Import到本機

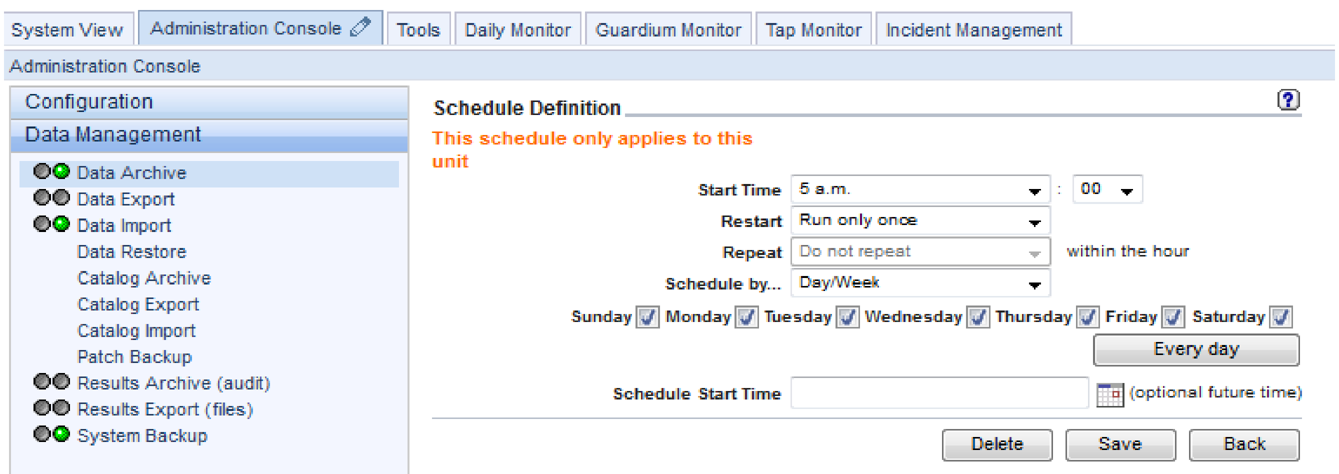


每天清晨4:00執行

Administration Console設定-Data Management (CM主機備份)

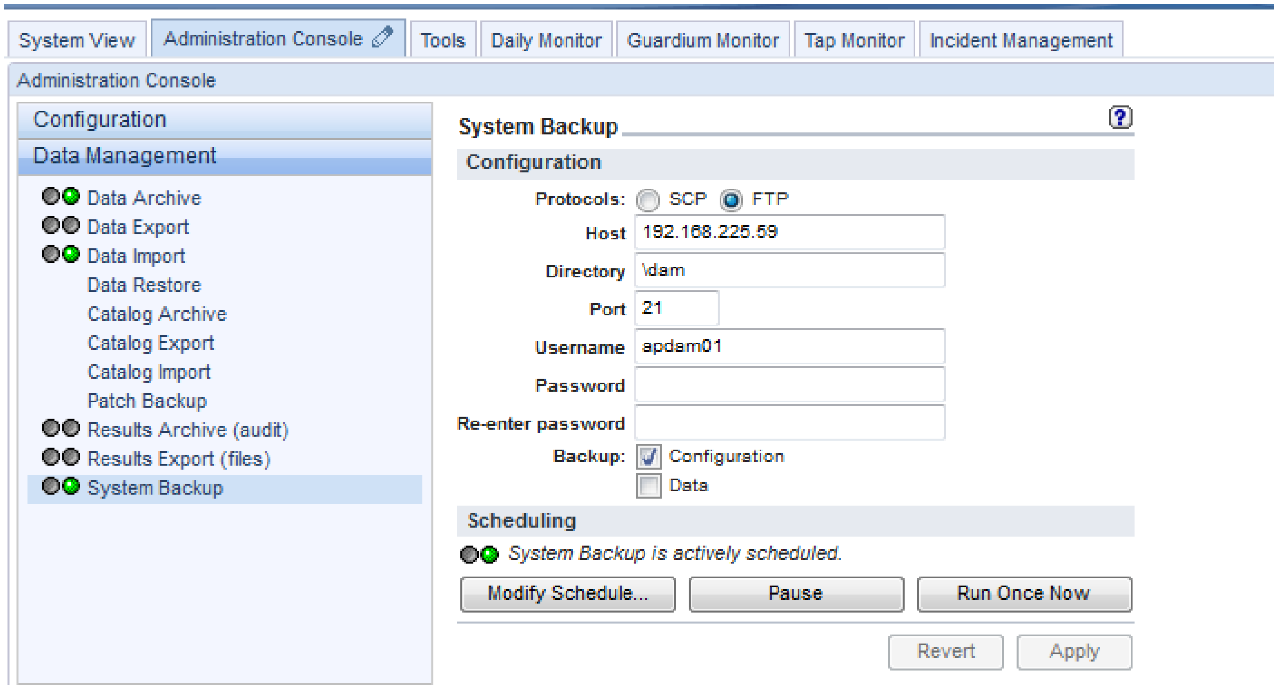


CM主機每天將資料備份到FTP Server上,並刪除20天前資料

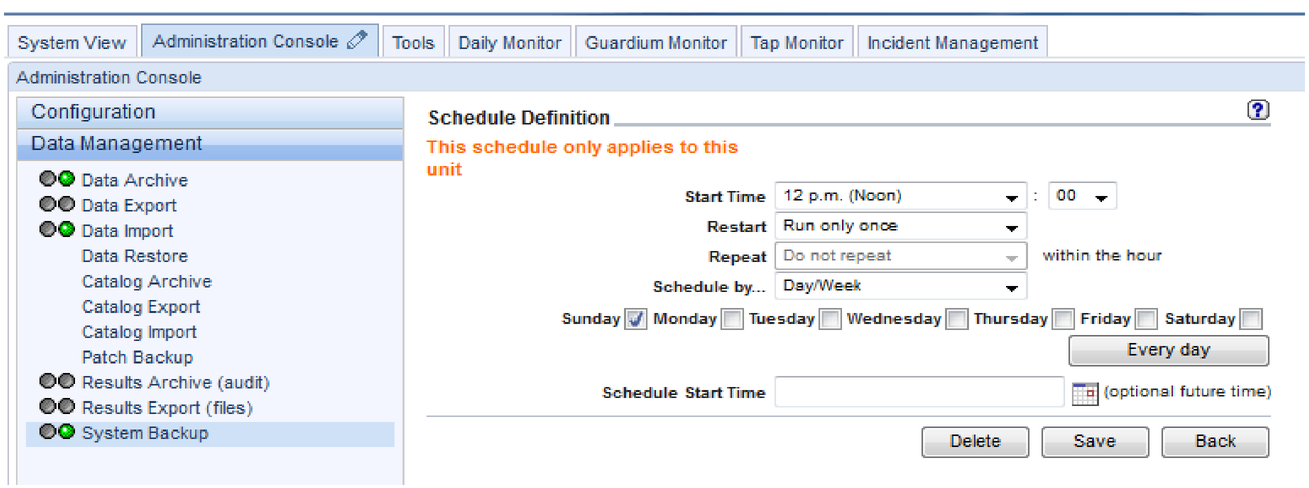


每天清晨5:00執行

System Backup（系統設定備份）



Collector與CM主機每週也將主機系統設定檔備份至FTP Server 上



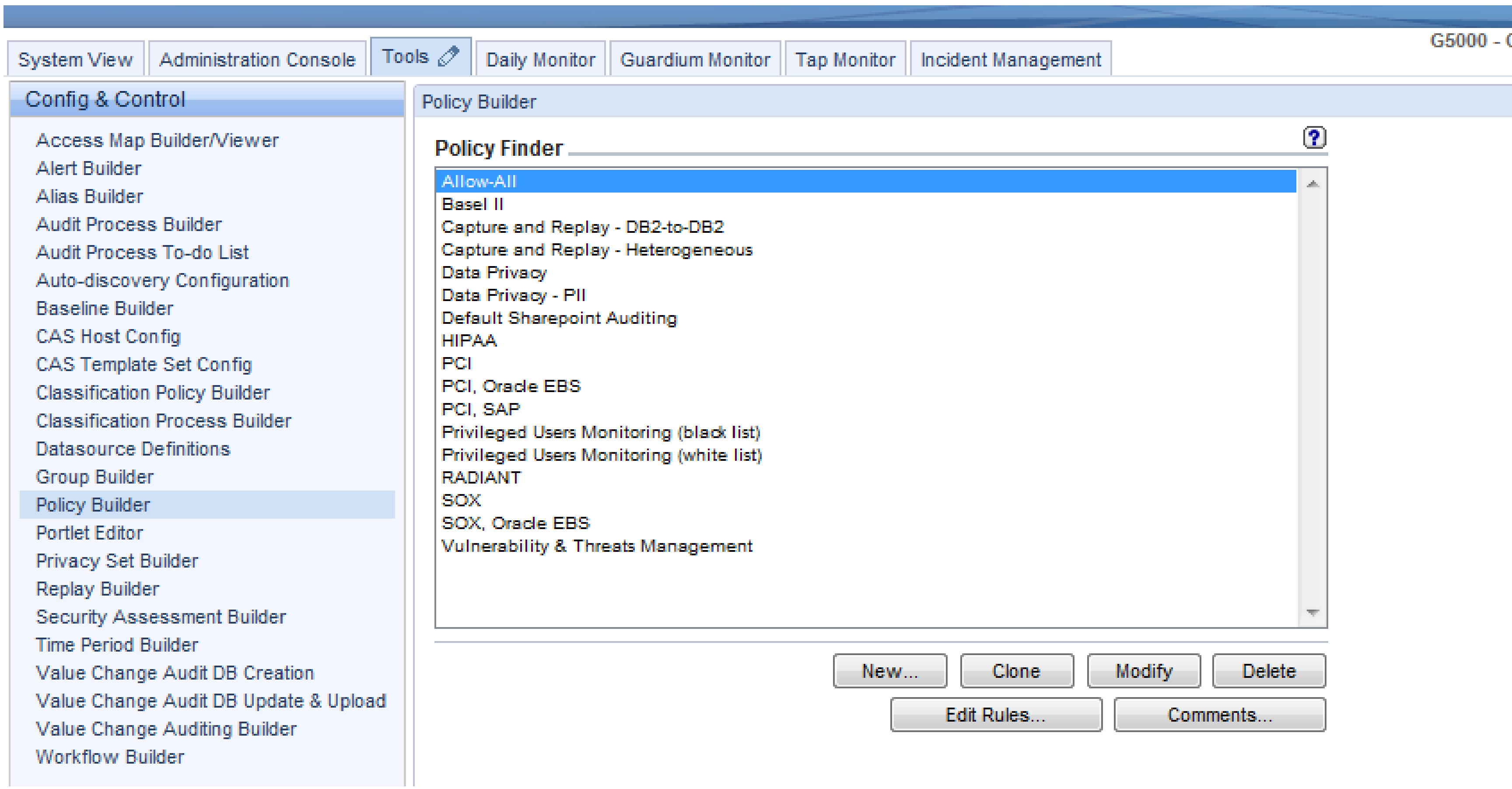
每週日中午12:00執行

Policy管理

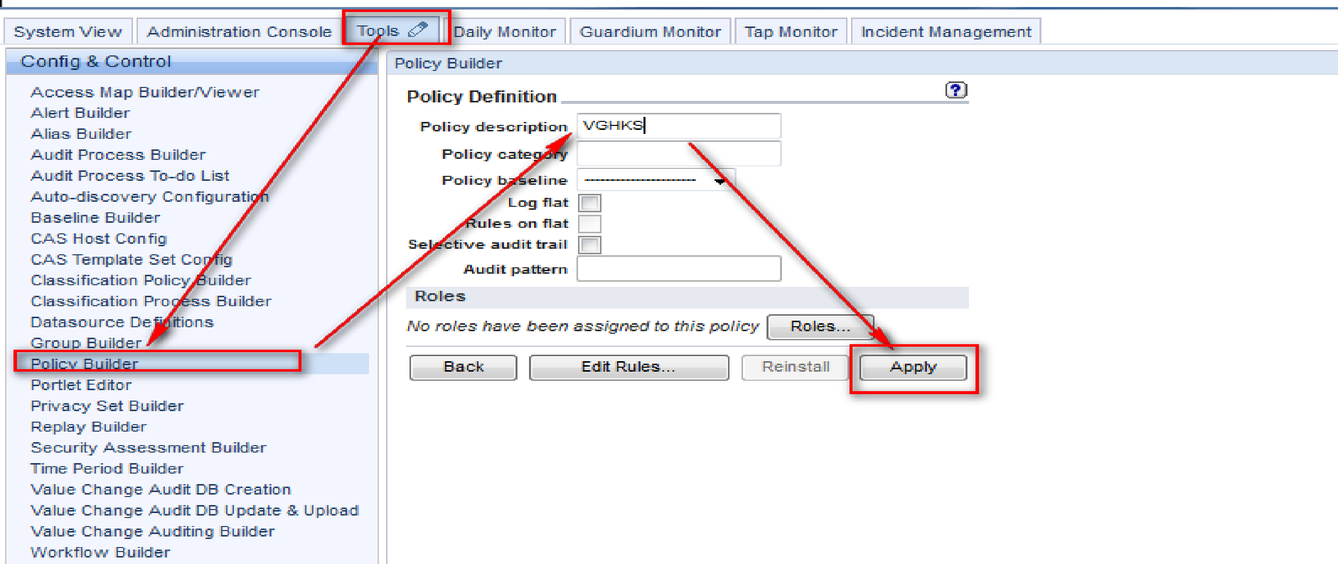
Guardium Policy制定

透過Policy制定,可過濾欲收集的資料類型,或當符合自訂Policy政策時進行警示等動作.

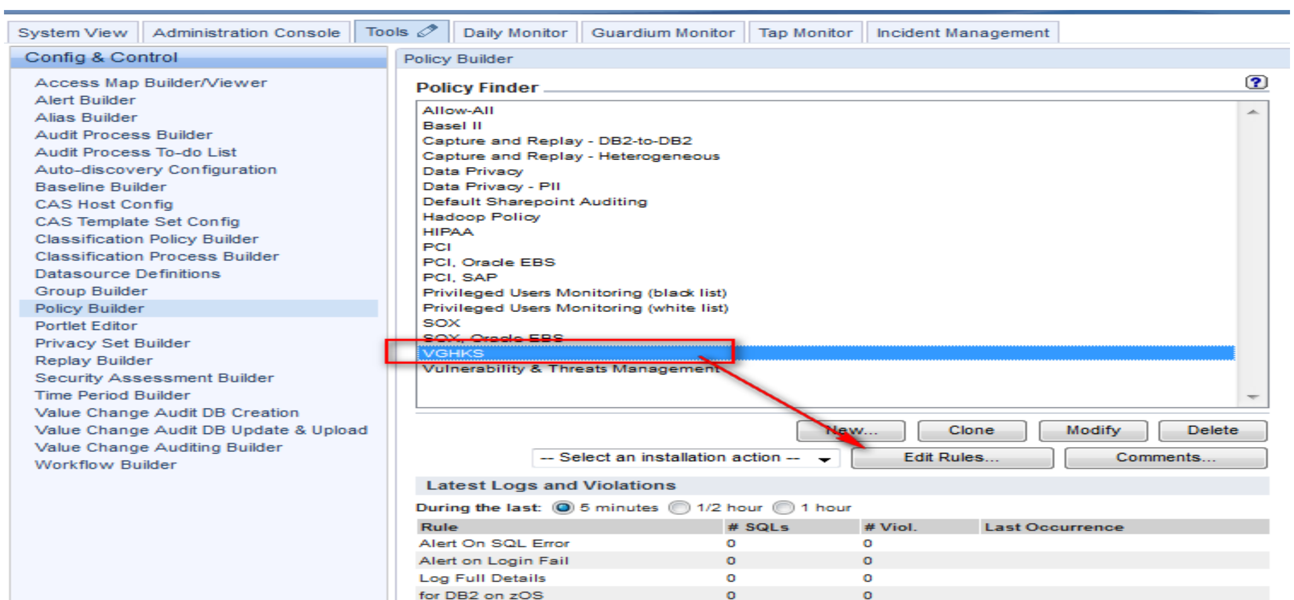
若有CM主機,相關Policy建議於CM主機上制定再派送至Collector



Guardium Policy 名稱

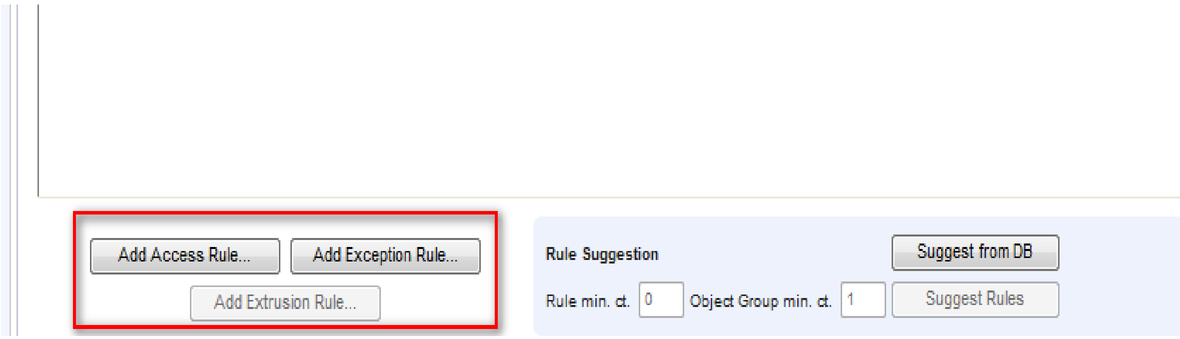


由Tools -> Policy Builder -> New進入 Policy Definition 新增VGHKS名稱之 Policy

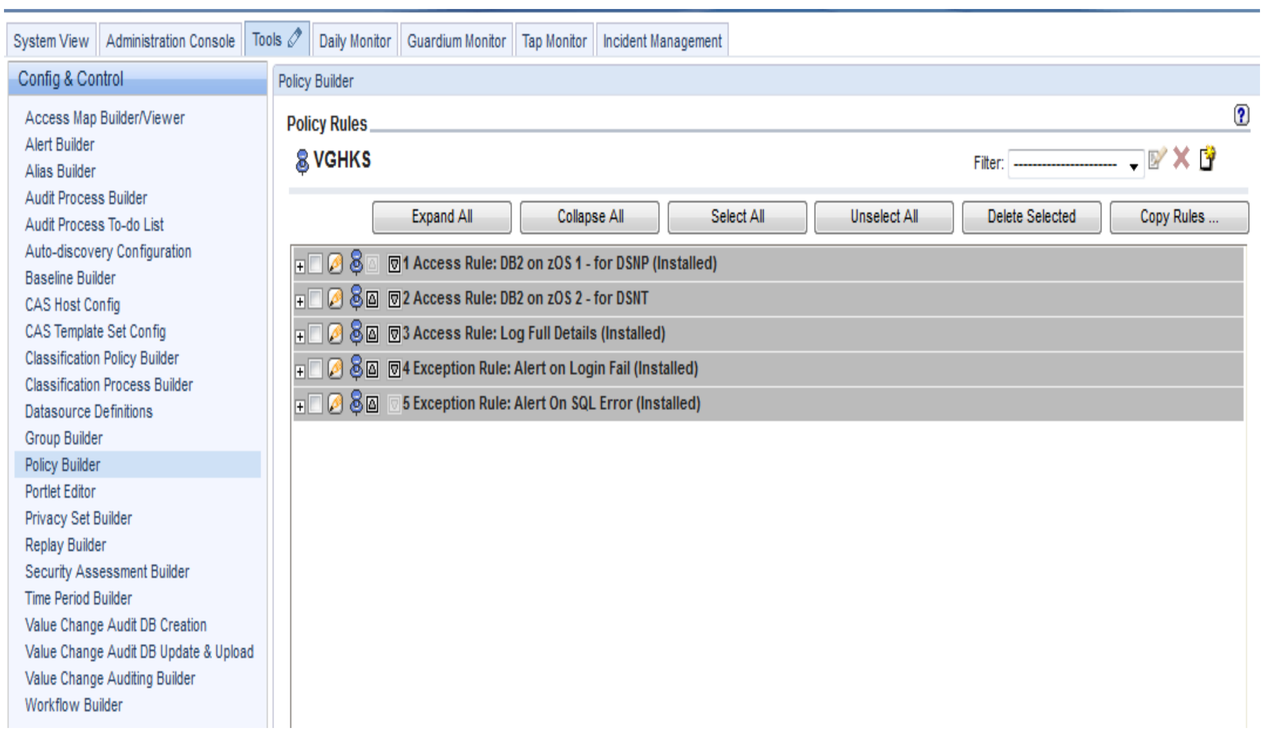


選取VGHKS後,點選 “Edit Rules” ，進入 “Policy Rule” 設定

Guardium Policy Rule制定（續）

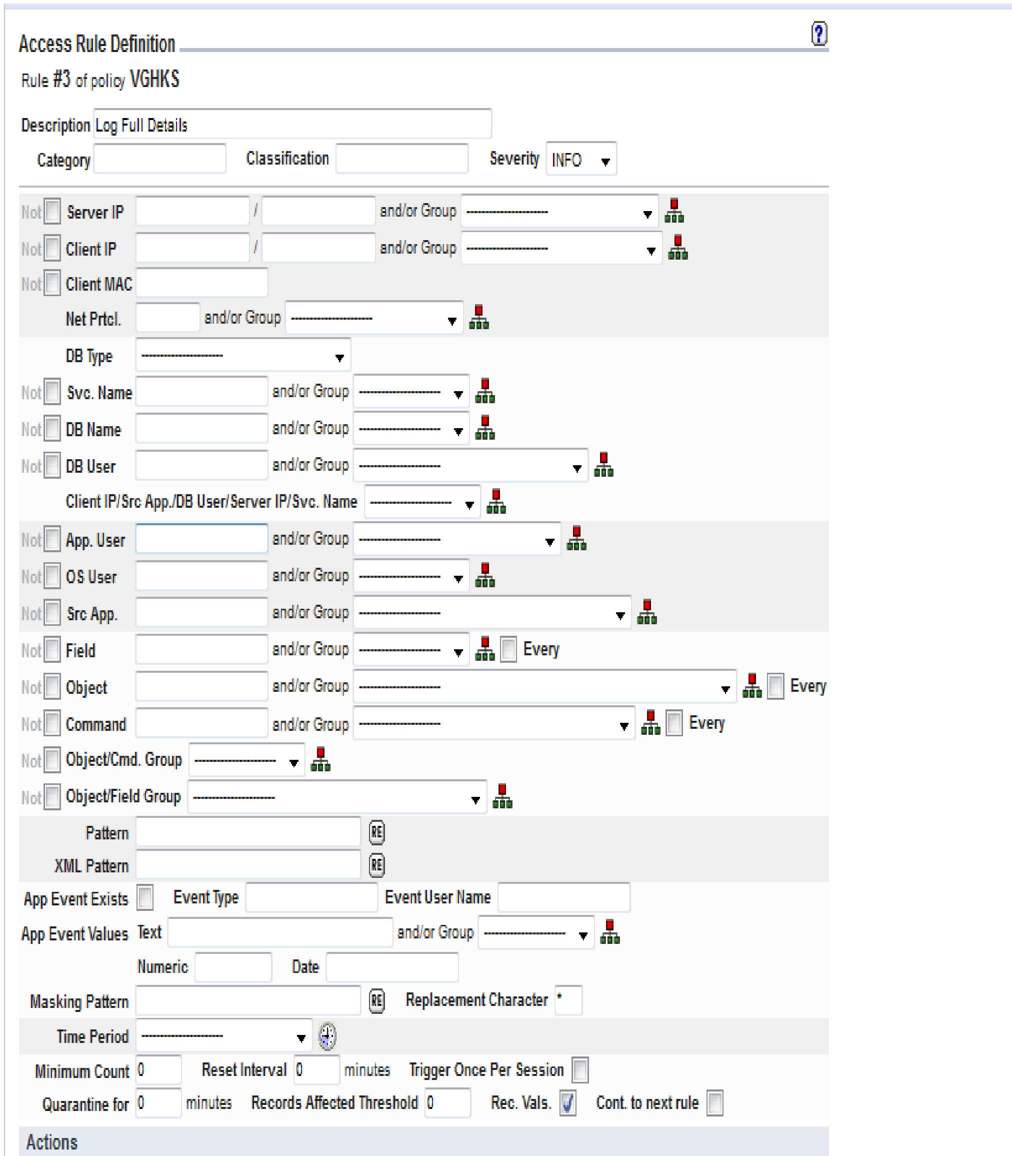


依類別有Access, Exception, Extrusion Rule可制定

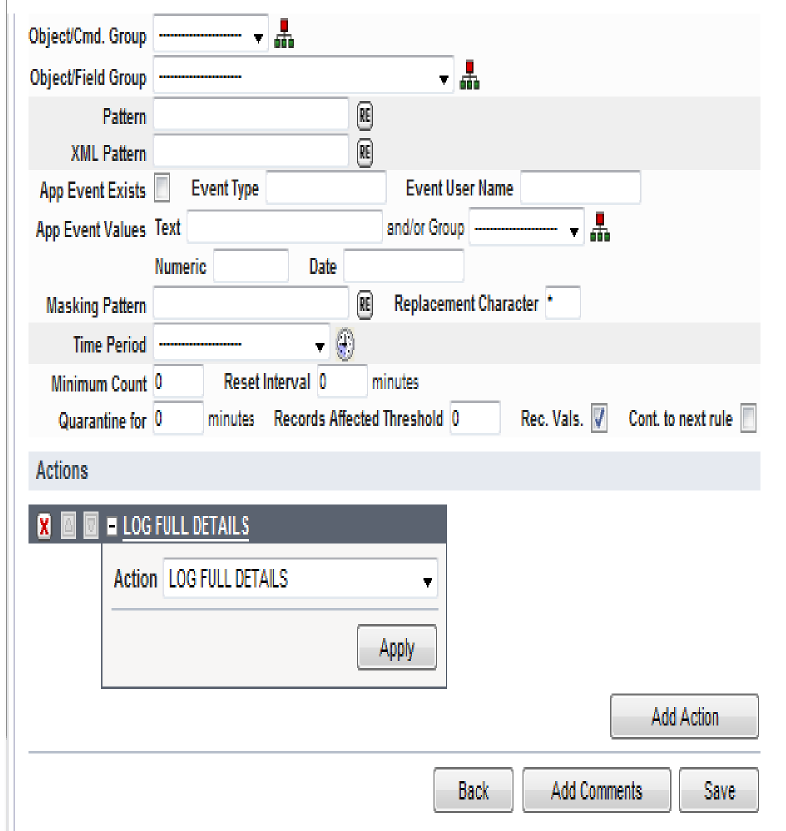


目前訂定Log Full Details &Alert on Login Fail & SQL Error ,zOS使用共5條Rule

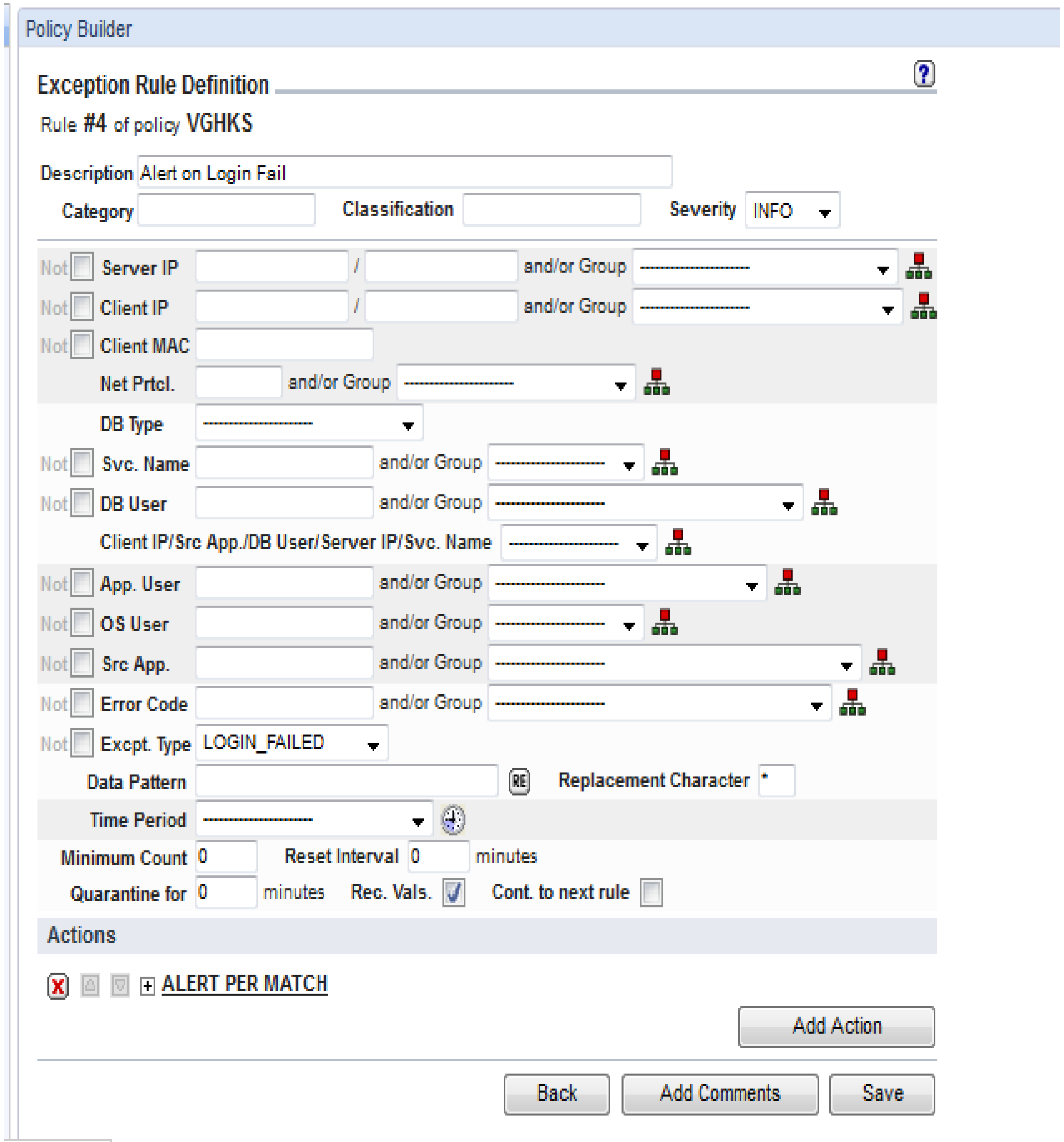
Guardium Policy Rule制定（續）



Log Full Details 不設任何條件，全都錄至主機

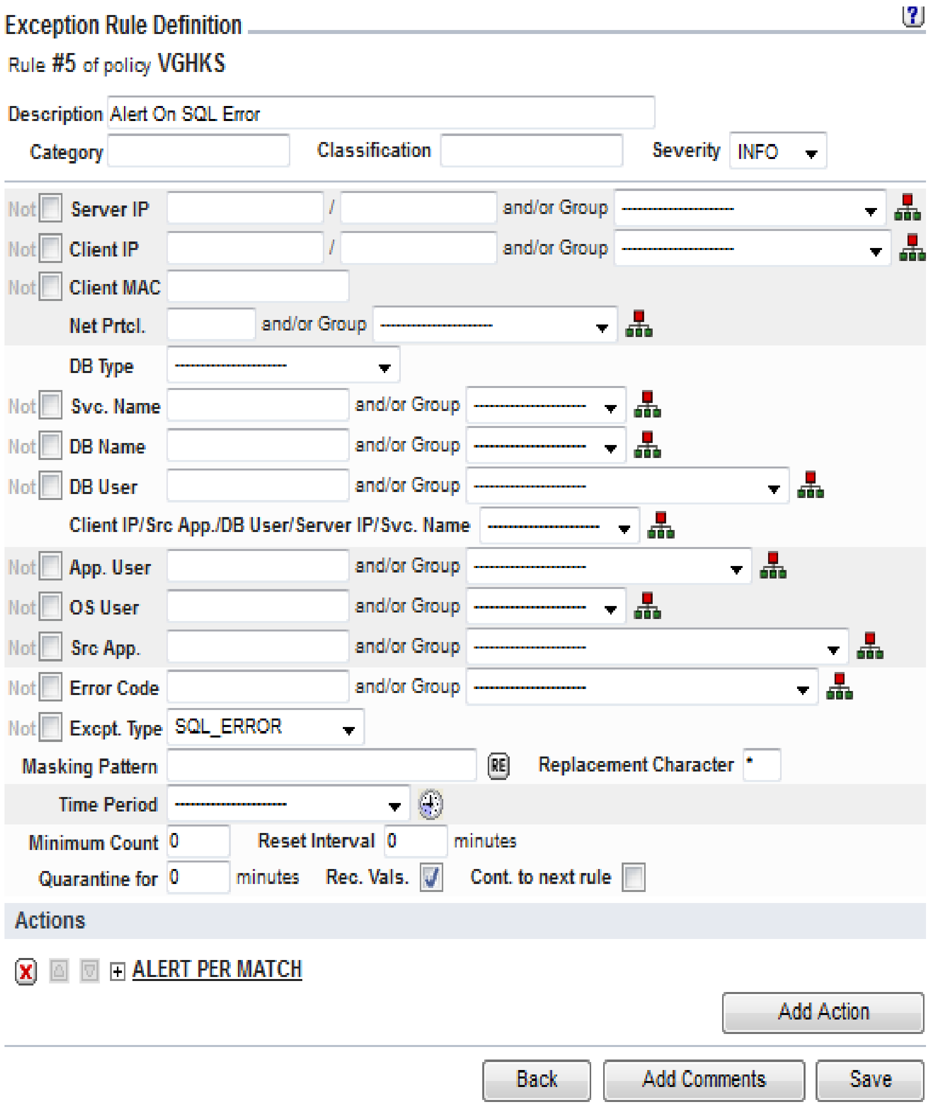


Guardium Policy Rule制定（續）

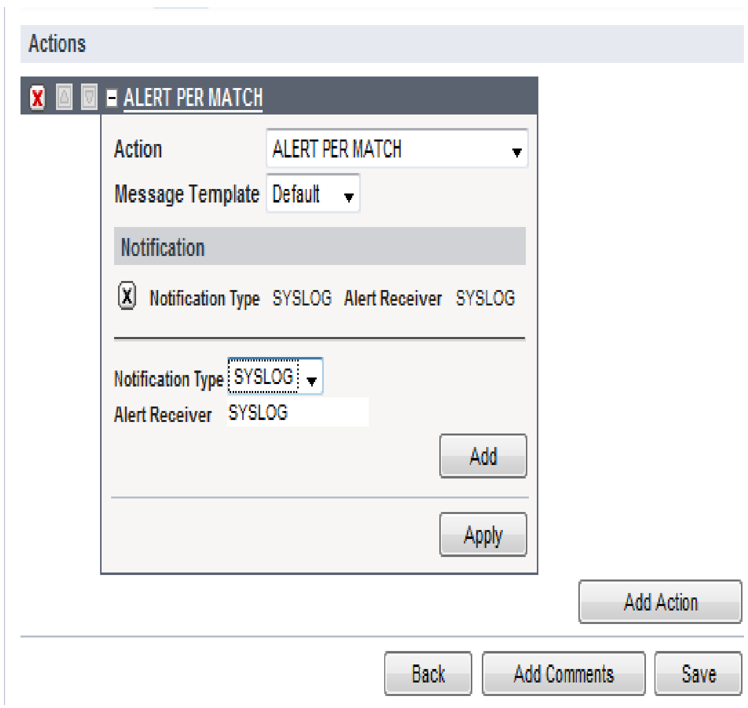


Alert on Login Fail, 當有偵測到登入失敗, 將其寫入Syslog內

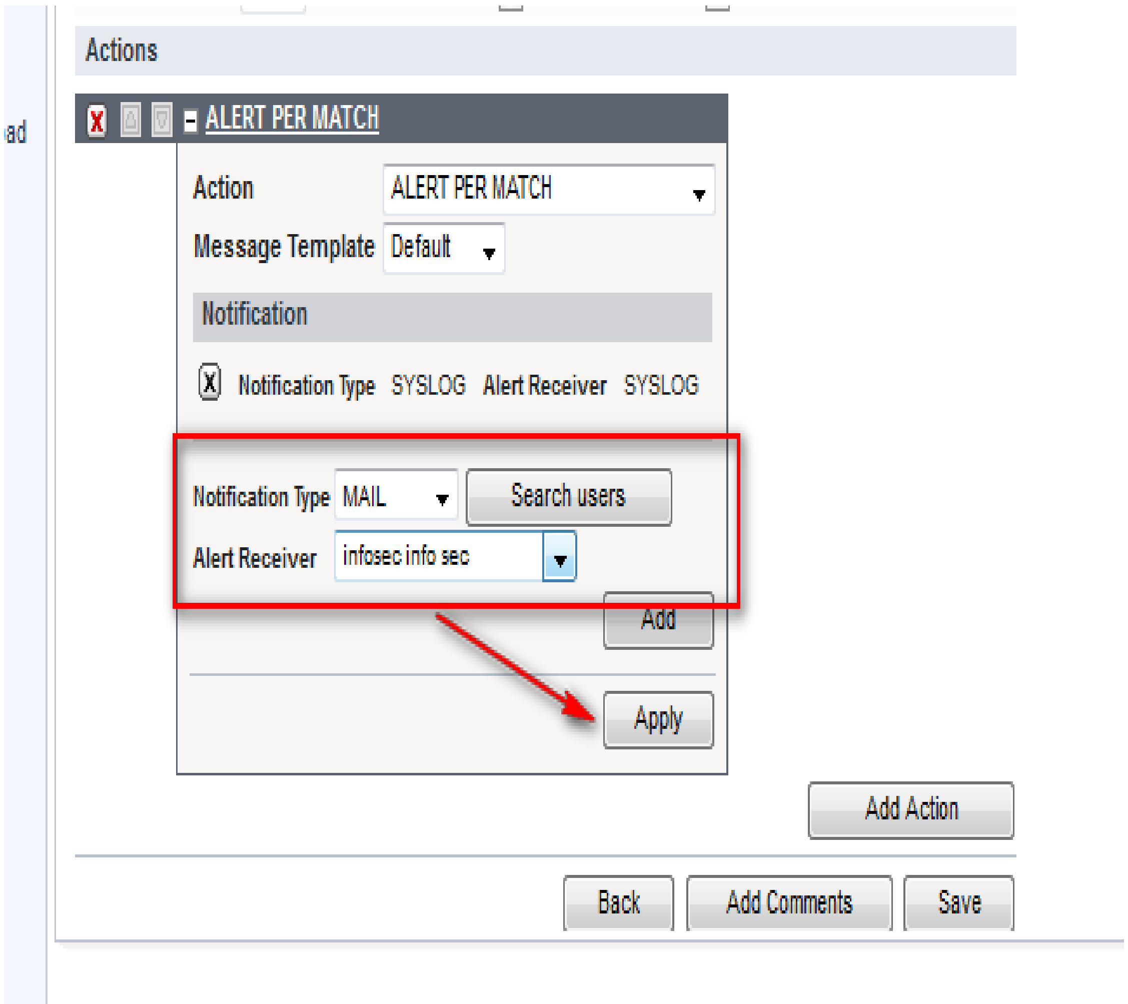
Guardium Policy Rule制定（續）



Alert on SQL Error,當有偵測到SQL Error時,將其寫入Syslog內

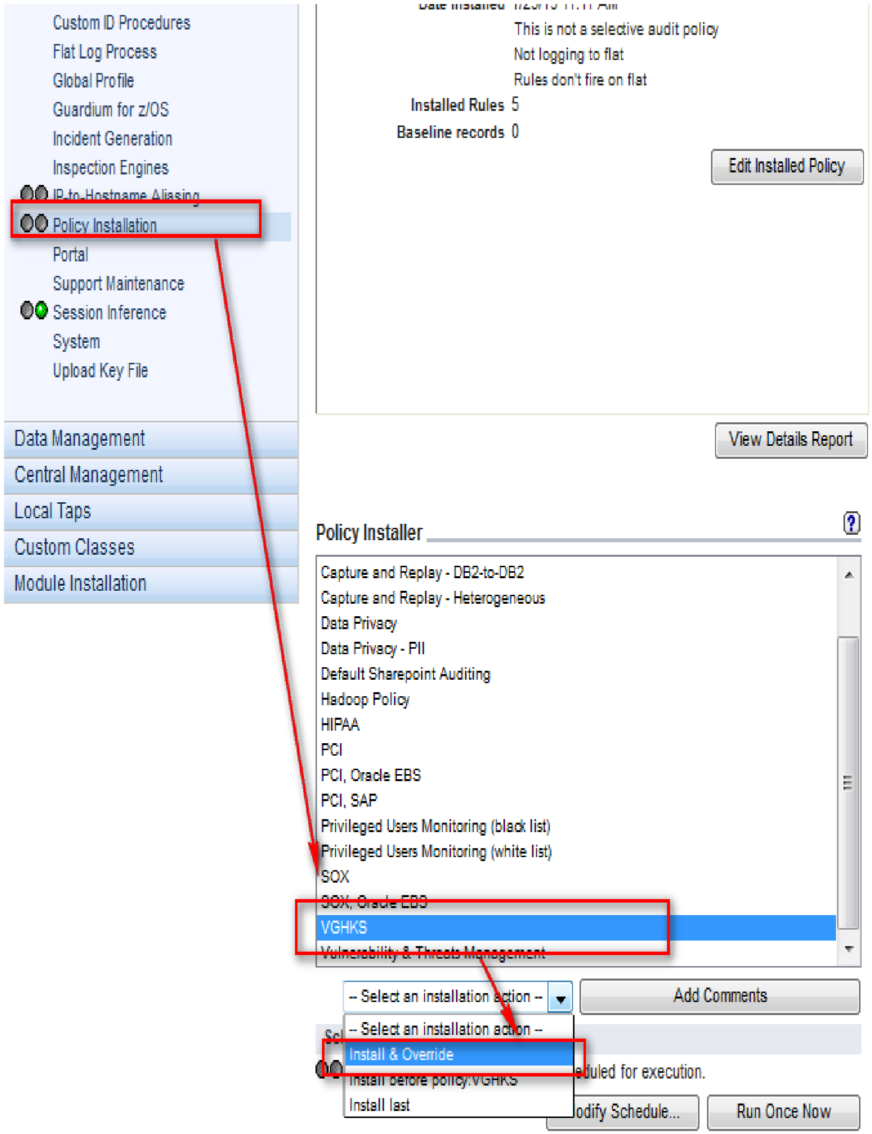


即時警訊告知



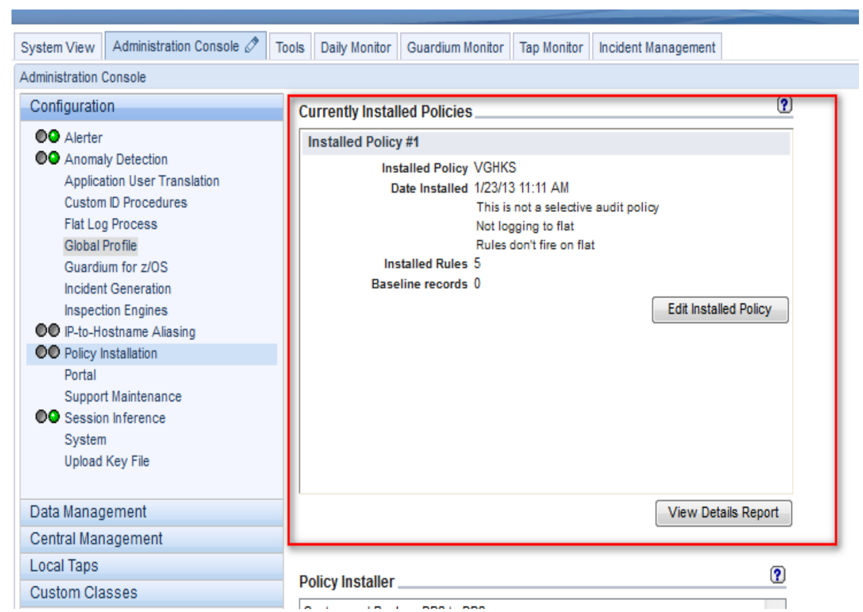
如Alert on SQL Error或Login Fail,可於Alert Per Match條件內,加入Mail通知(Guardium需有此帳號),當有偵測到相關Error時,會將其即時mail給設定人員

Guardium Policy-Install



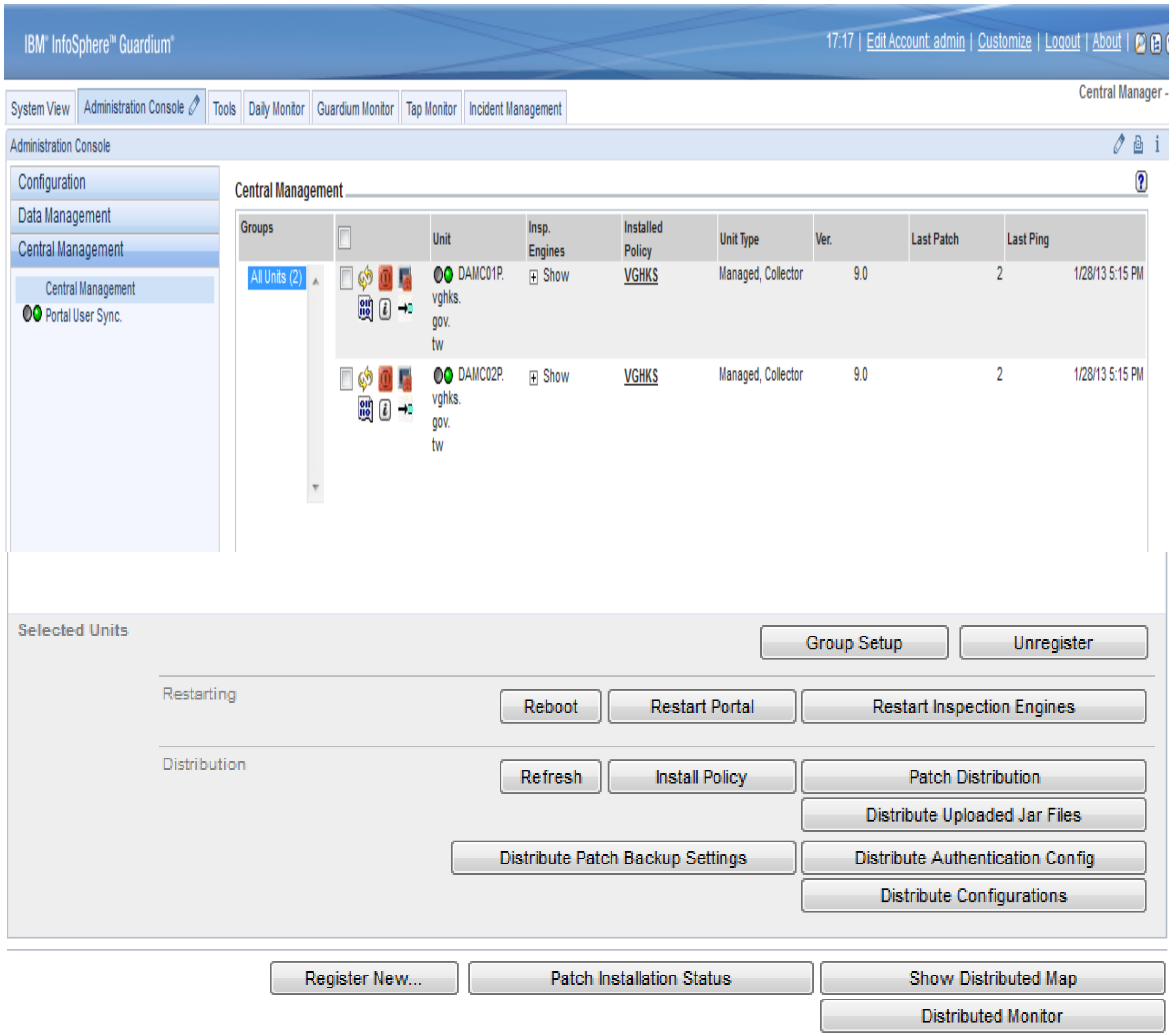
於Policy Installation選擇自訂的Policy名稱，選擇Install & Override 安裝

可由Currently Installed Policies 查詢目前所使用之Policy



中央控管機制

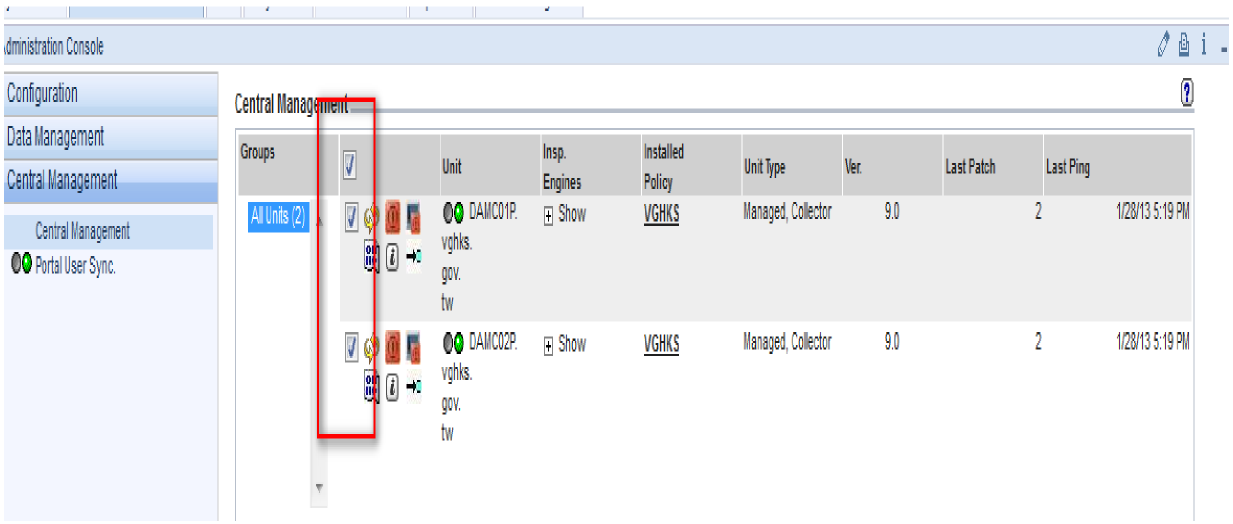
Centeral Management 管理 (CM主機)



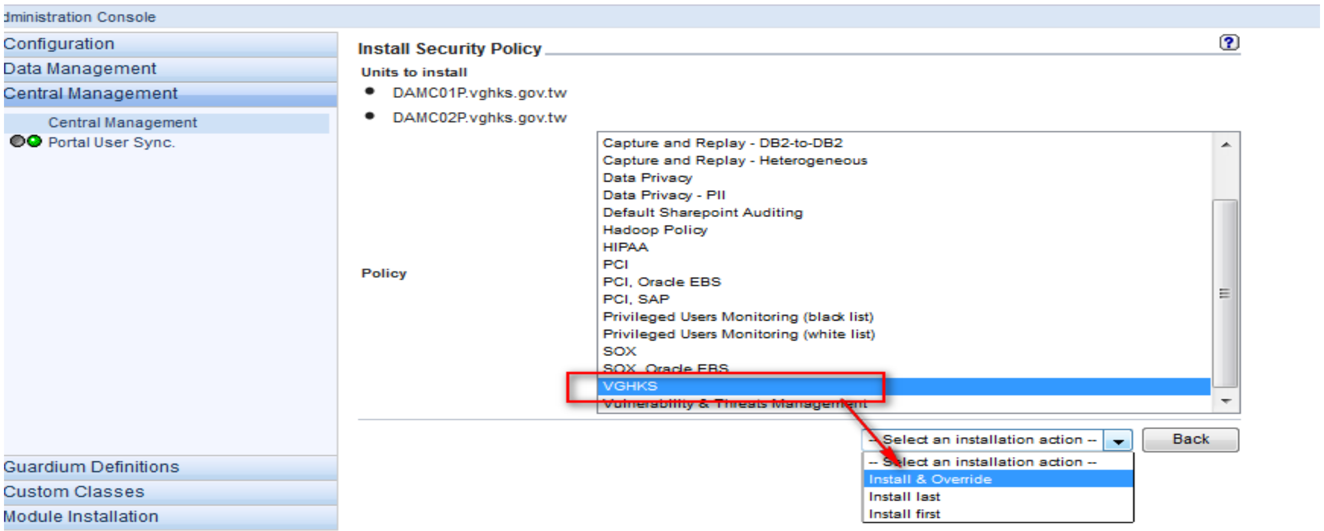
CM目前管理2台Collector主機

可點選要管理的主機來重開機,安裝Policy ,Patch檔等功能

Centeral Management 統一派送Policy (CM主機)

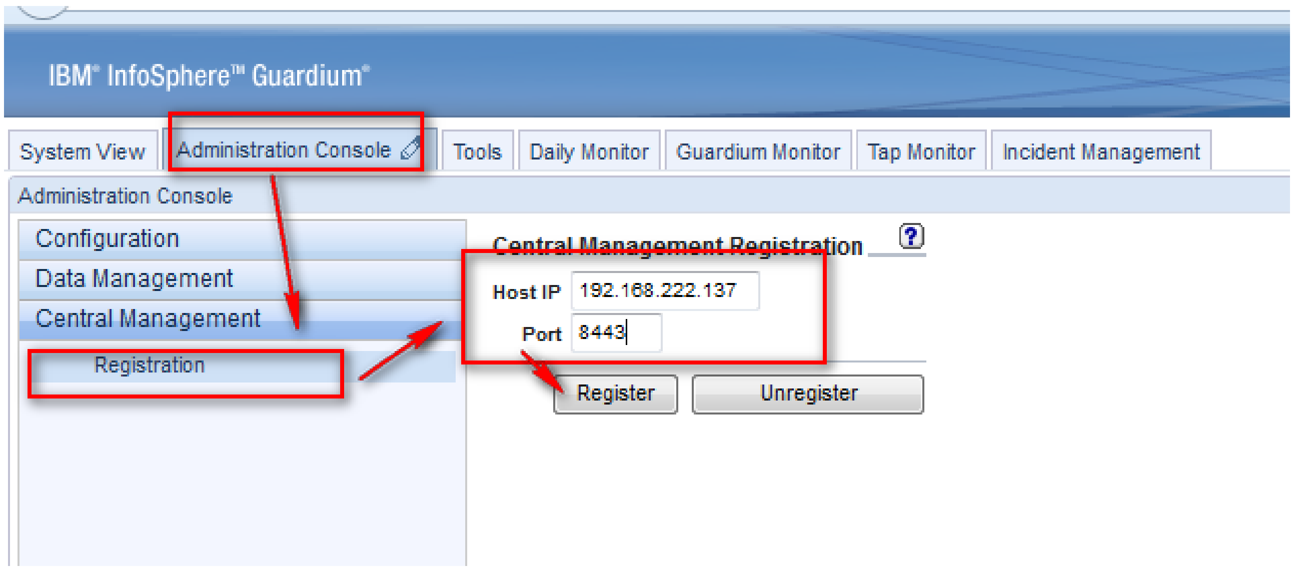


點選要控管的Collector主機選Install Policy

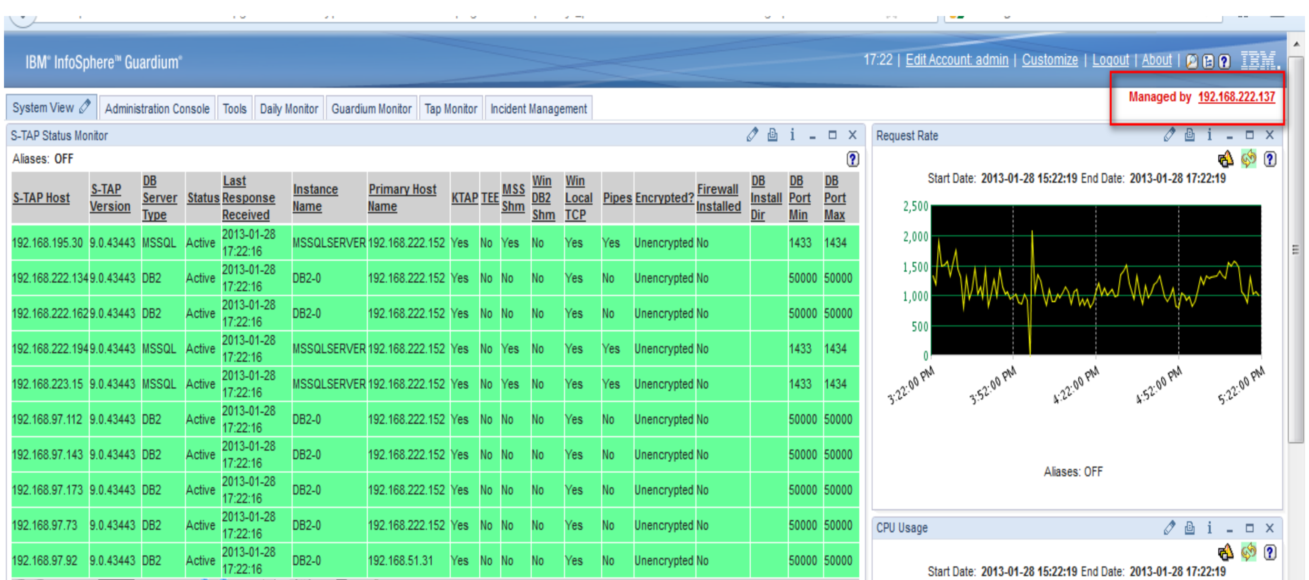


選取要Install Policy後選Install&Override

Collector加入Centeral Management控管 (Collector)



Centeral Management
內 Registration輸入
CM主機IP,Port為8443

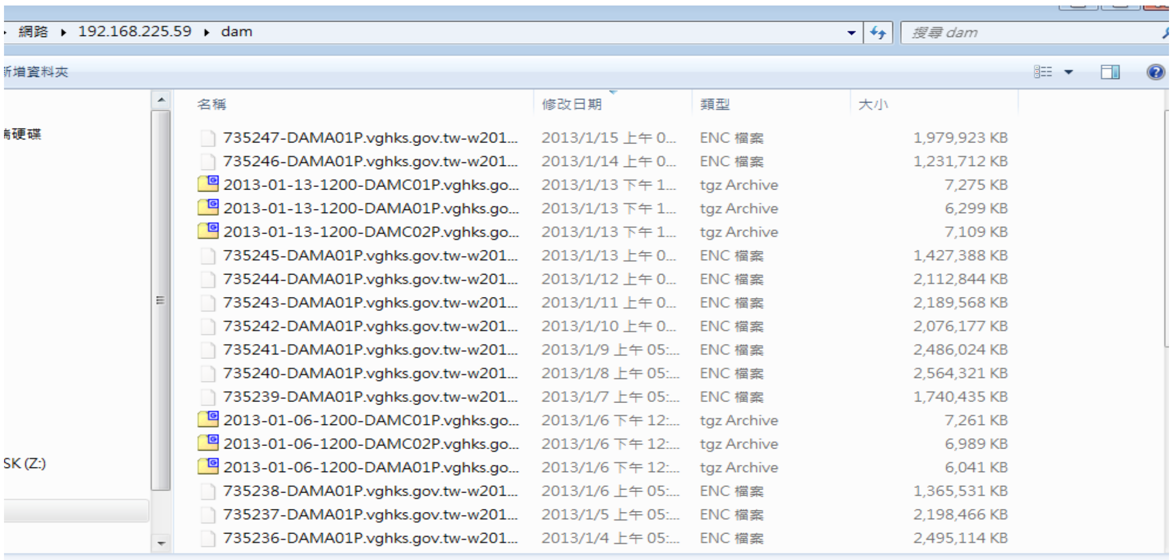


S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Instance Name	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed	DB Install Dir	DB Port Min	DB Port Max
192.168.195.30	9.0.43443	MSSQL	Active	2013-01-28 17:22:16	MSSQLSERVER	192.168.222.152	Yes	No	Yes	No	Yes	Yes	Unencrypted	No		1433	1434
192.168.222.134	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.222.162	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.222.194	9.0.43443	MSSQL	Active	2013-01-28 17:22:16	MSSQLSERVER	192.168.222.152	Yes	No	Yes	No	Yes	Yes	Unencrypted	No		1433	1434
192.168.223.15	9.0.43443	MSSQL	Active	2013-01-28 17:22:16	MSSQLSERVER	192.168.222.152	Yes	No	Yes	No	Yes	Yes	Unencrypted	No		1433	1434
192.168.97.112	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.97.143	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.97.173	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.97.73	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.222.152	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000
192.168.97.92	9.0.43443	DB2	Active	2013-01-28 17:22:16	DB2-0	192.168.51.31	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000

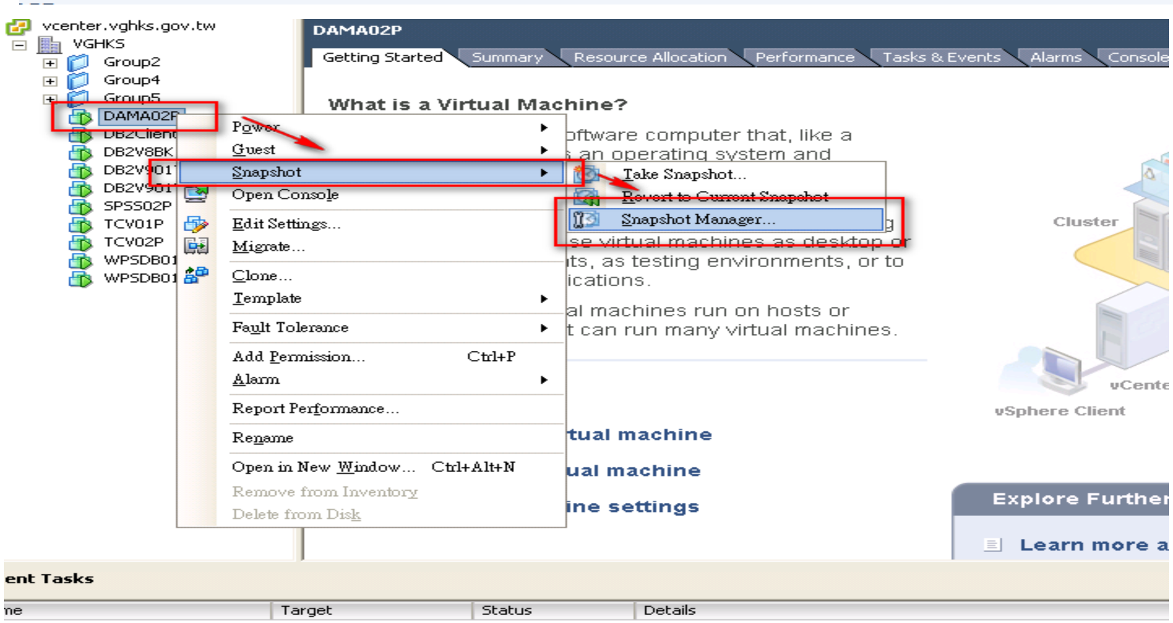
加入後,重新登錄主機
於右上方會出現目前
CM主機IP,成功加入

資料還原

Centeral Management 上資料還原

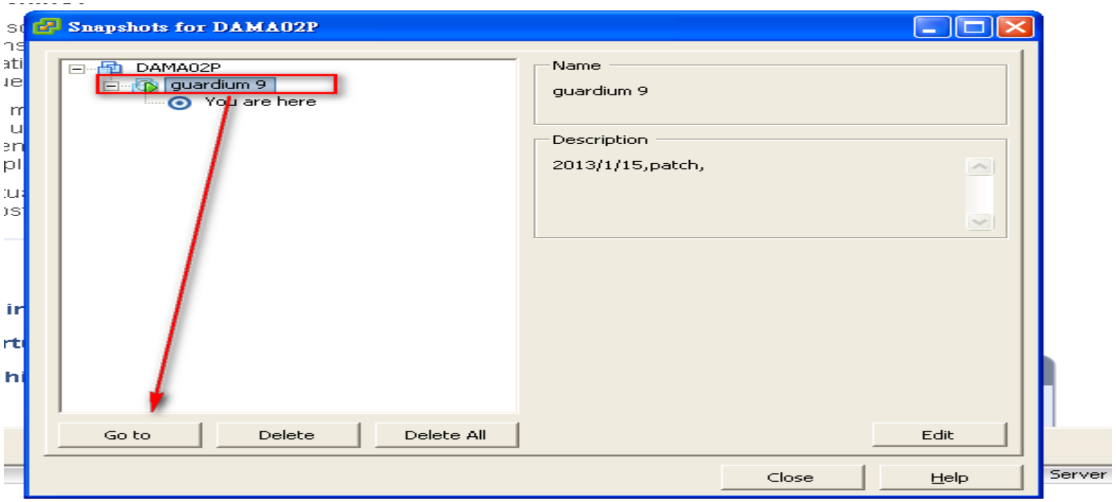


現有資料於CM主機上定期
備份至FTP Server
於FTP Server上可查看到每日
壓縮並加密備份檔案,其格式
為:
主機名稱-備份日期-實際資料
日期.dbdump.enc

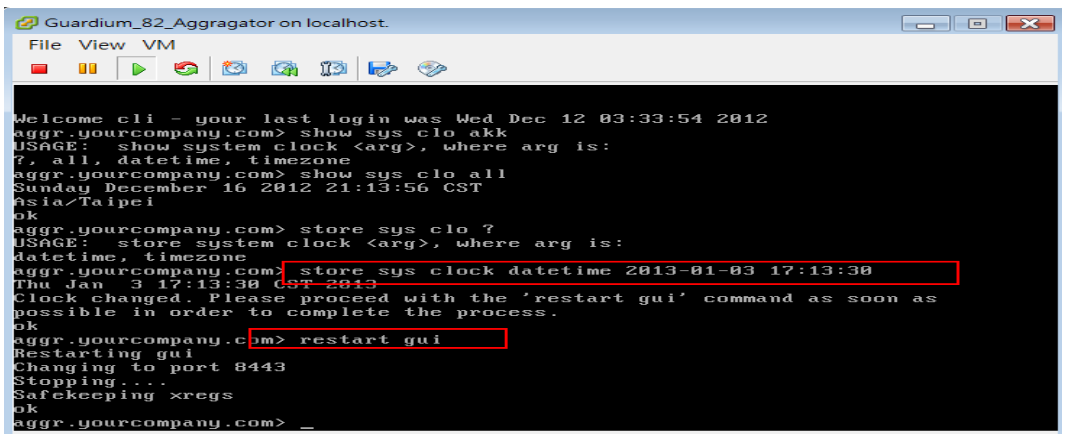


已另建還原專用機
192.168.222.138是於VM上,目
前也做好一Snapshot為初始完
整安裝,日後有還原過資料,可
使其再回覆到時間點.連到
DAMA02P主機機,選取該內的
Snapshot功能

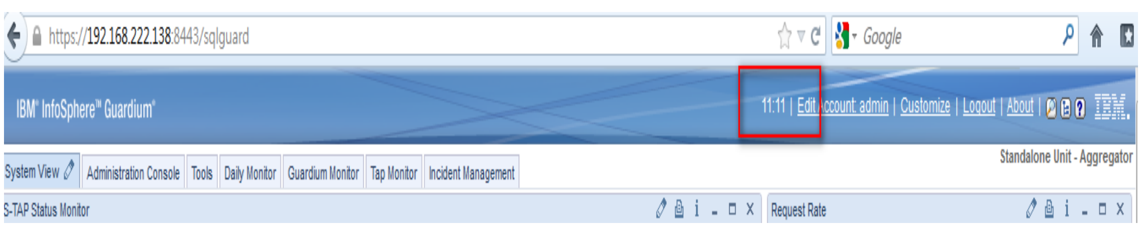
Centeral Management 上資料還原（續）



選取Guardium 9此snapshot來還原

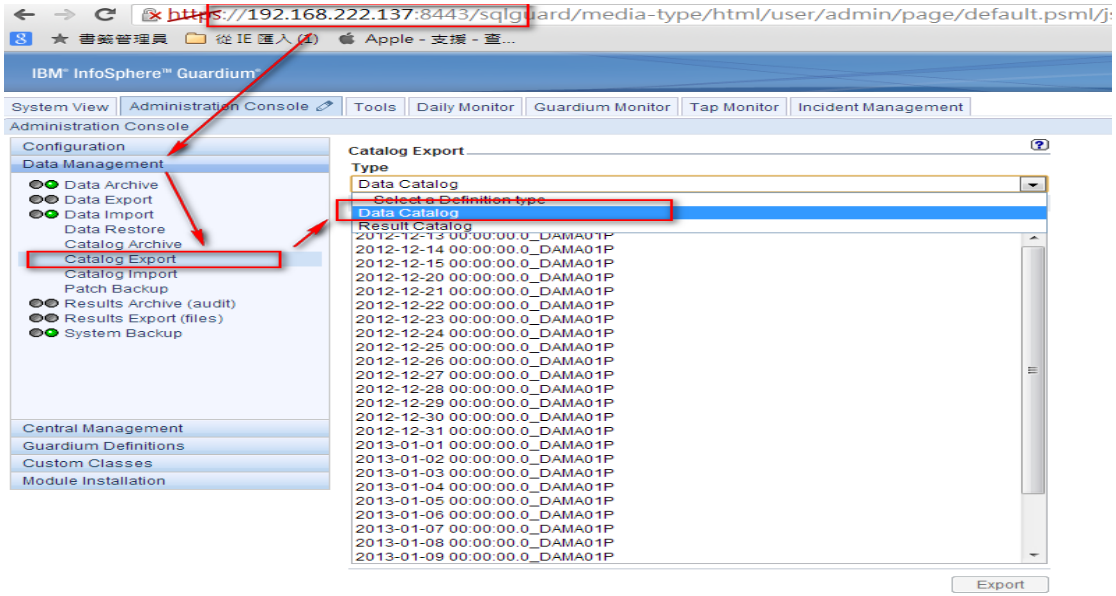


還原後，因該VM時間點與實際時間不符，另開啟該VM Console修改系統時間，下**store system clock datetime** 來修改，並restart gui 重新啟動GUI程式

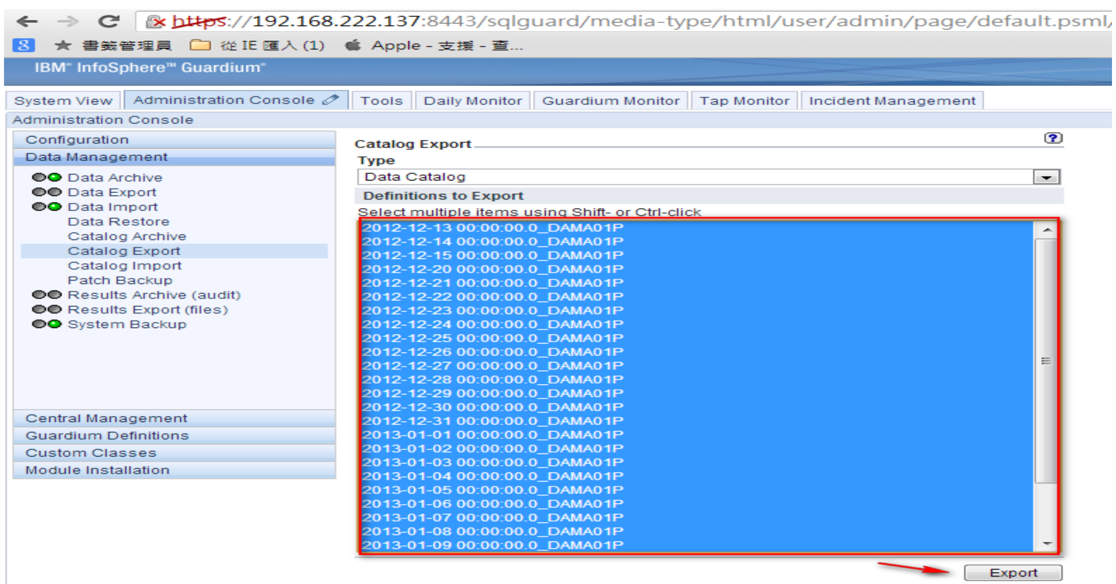


用admin登入192.168.222.138主機，確認時間與實際時間相同，再開始還原資料

Centeral Management 上資料還原（續）

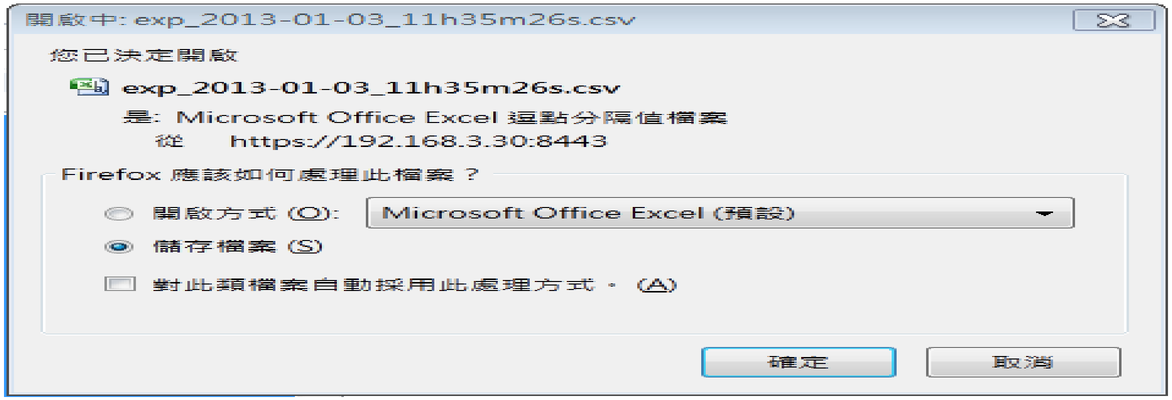


將CM 主機上 Catalog Export出來,可選預還原的備份時間點(或全部)即可,選export後存於操作的PC上

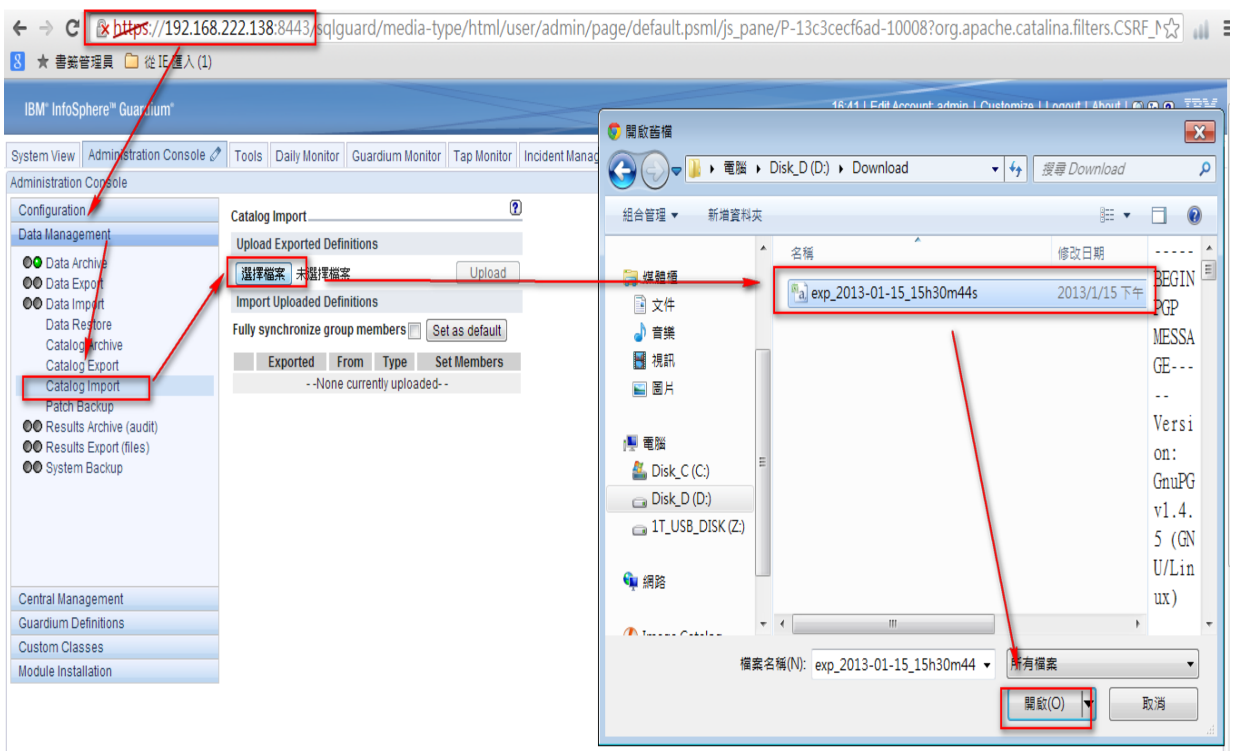


選取要匯出的Data Catalog日期後選Export

Centeral Management 上資料還原（續）

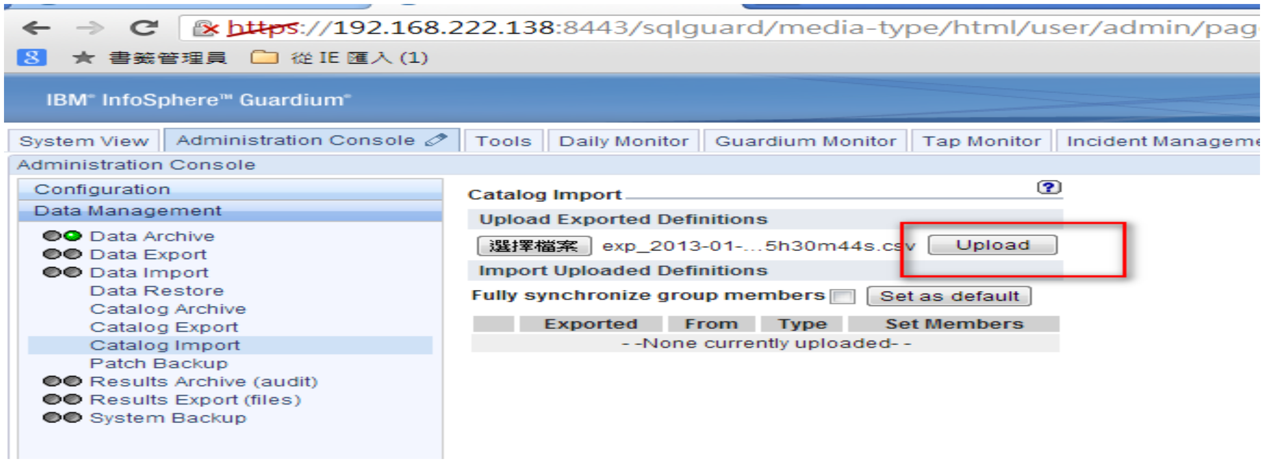


存到本機硬碟上

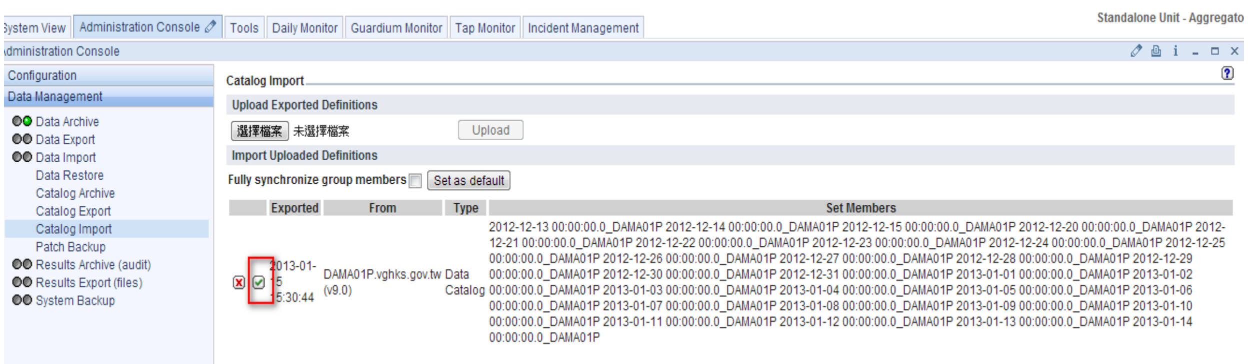


至192.168.222.138還原資料專用機，將剛export的Catalog檔選Catalog Import匯入備份相關資料

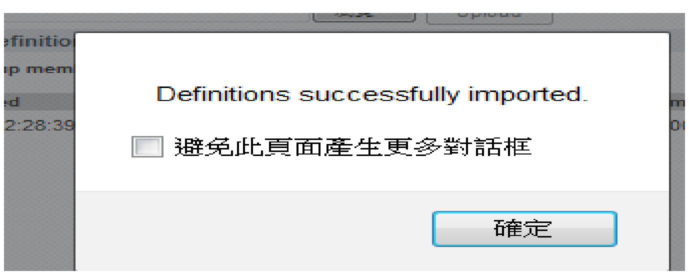
Centeral Management 上資料還原（續）



選取剛下載的csv檔，將其upload

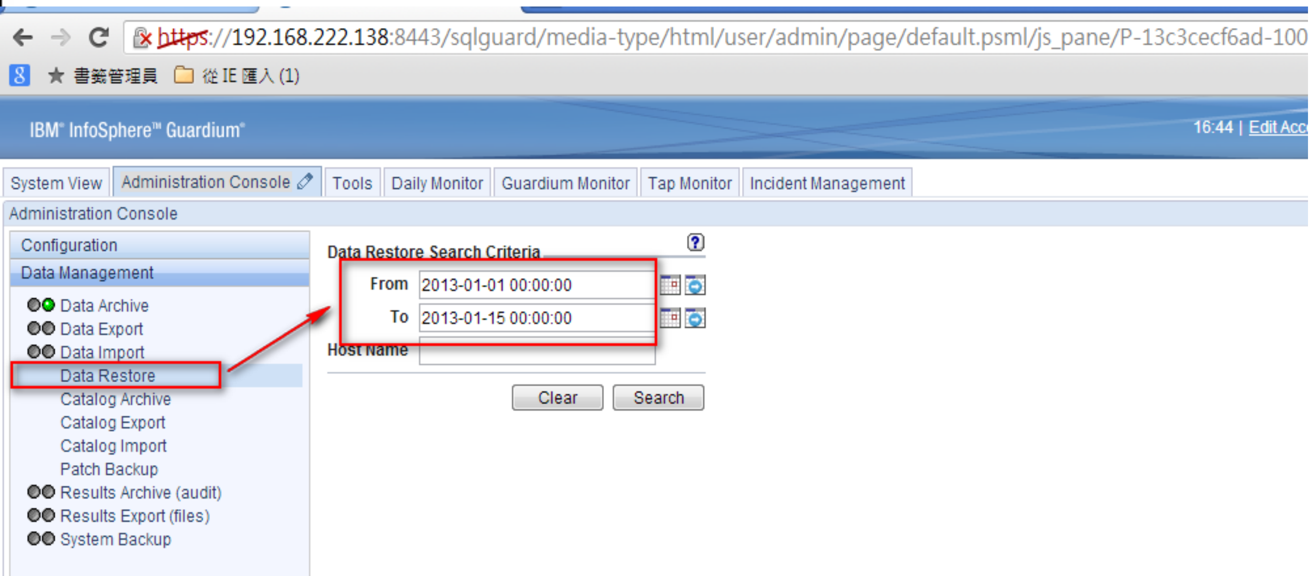


點選”綠色小勾”匯入Catalog

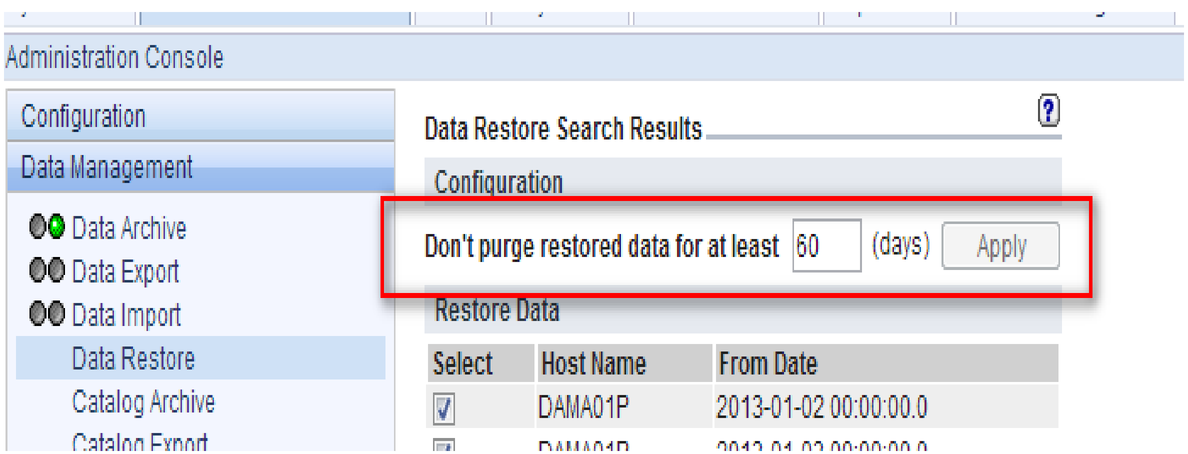


成功Import

Centeral Management 上資料還原（續）

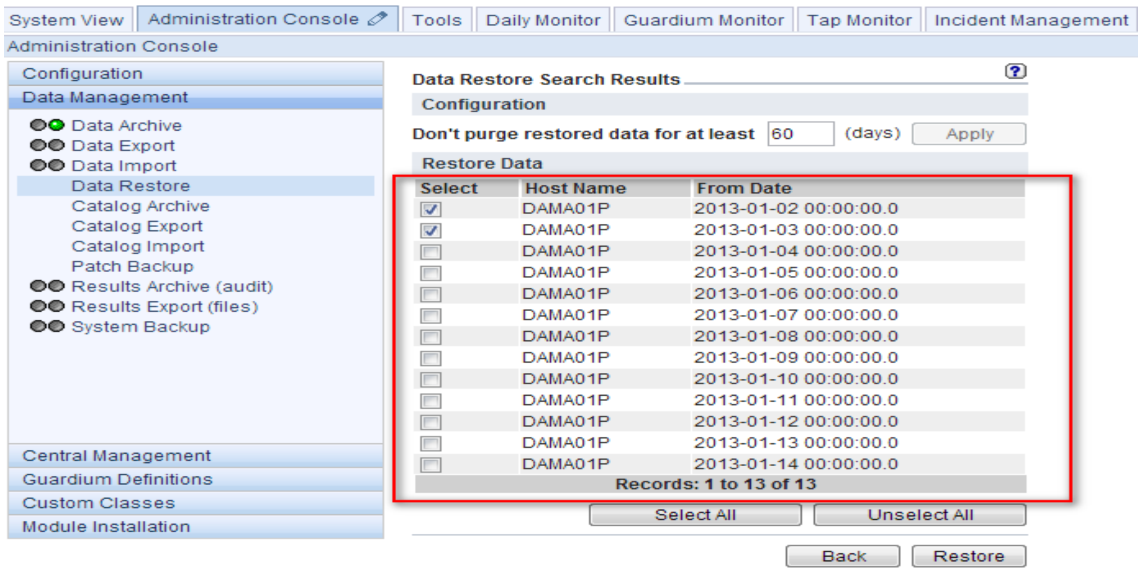


Catalog還原後，選取Data Restore來還原實際資料
選擇要還原資料的時間區段，選擇Search



於 “Don’t purge restored data” 中的天數要大於記錄檔距離今天的天數

Centeral Management 上資料還原（續）



選取還原的資料時時間點後選Restore（注意時間點選擇）

除非您要還原這個月內第一個建立的保存中的資料，否則必須還原多天的資料。這是因為還原資料時，Guardium
必須具備它在保存還原的資料時所擁有的所有資訊。建立保存後，其中部分資訊可能會因沒有使用而清除。還原作業的所有必要資訊都會自動保存，所以每個月的第一次會保存該資料。因此，在還原資料時，您有兩個選擇：

還原該月的第一天及所有後續日子，直到您想要的日子為止

或

還原想要的日子，然後還原後續月份的第一天

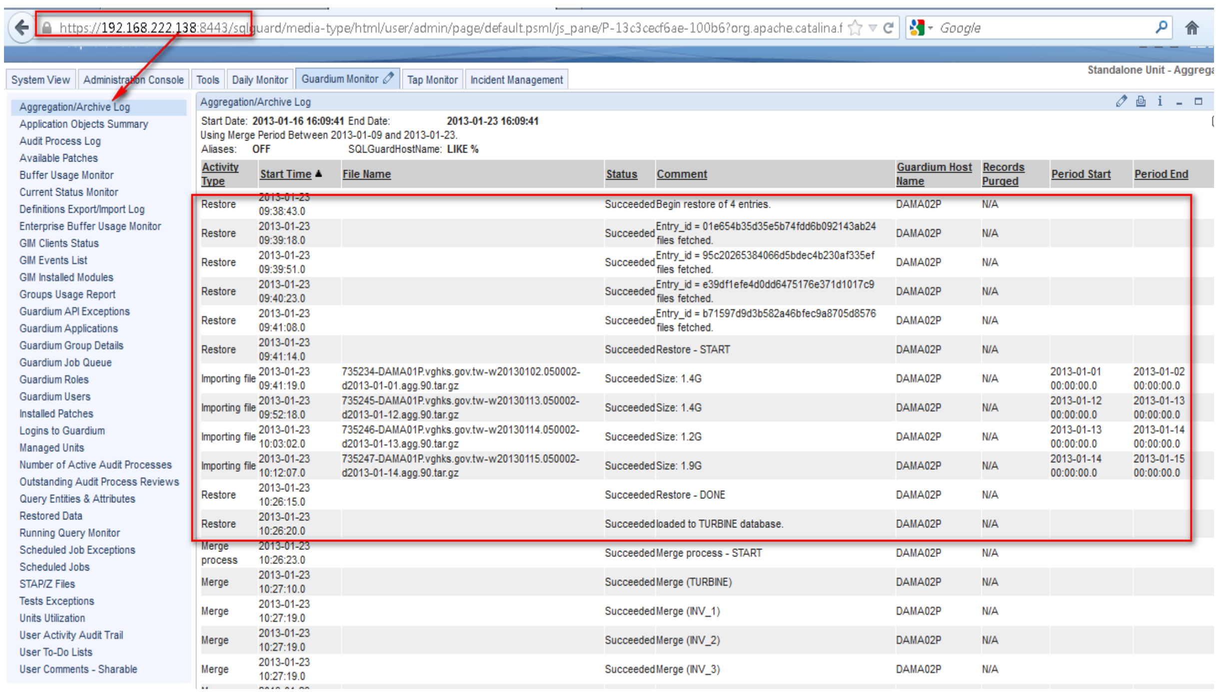
例如，若要還原 6 月 28 日，可以還原 6 月 1 日到 6 月 28 日，或還原 6 月 28 日和 7 月 1 日。

因原廠文件說明還原方式要包含該月1日(或下月1日)的資料，要依此方式還原不能只單獨還原單日資料，可能會有筆數不足產生

建議還原日期除每月一日，加上前後一天資料一併還原

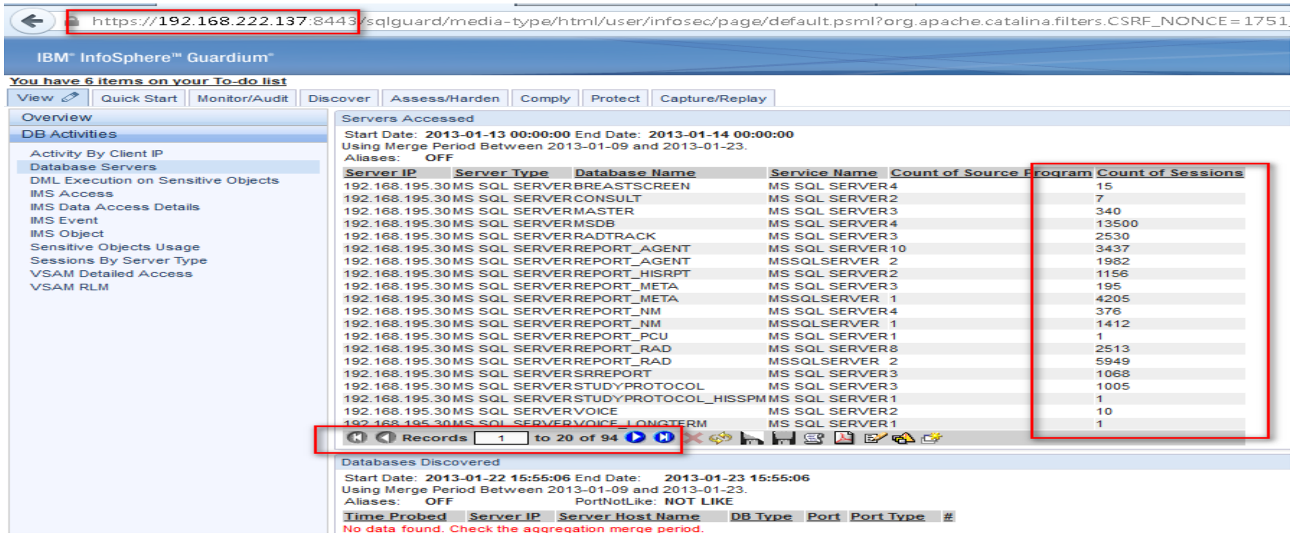
Centeral Management 上資料還原（續）

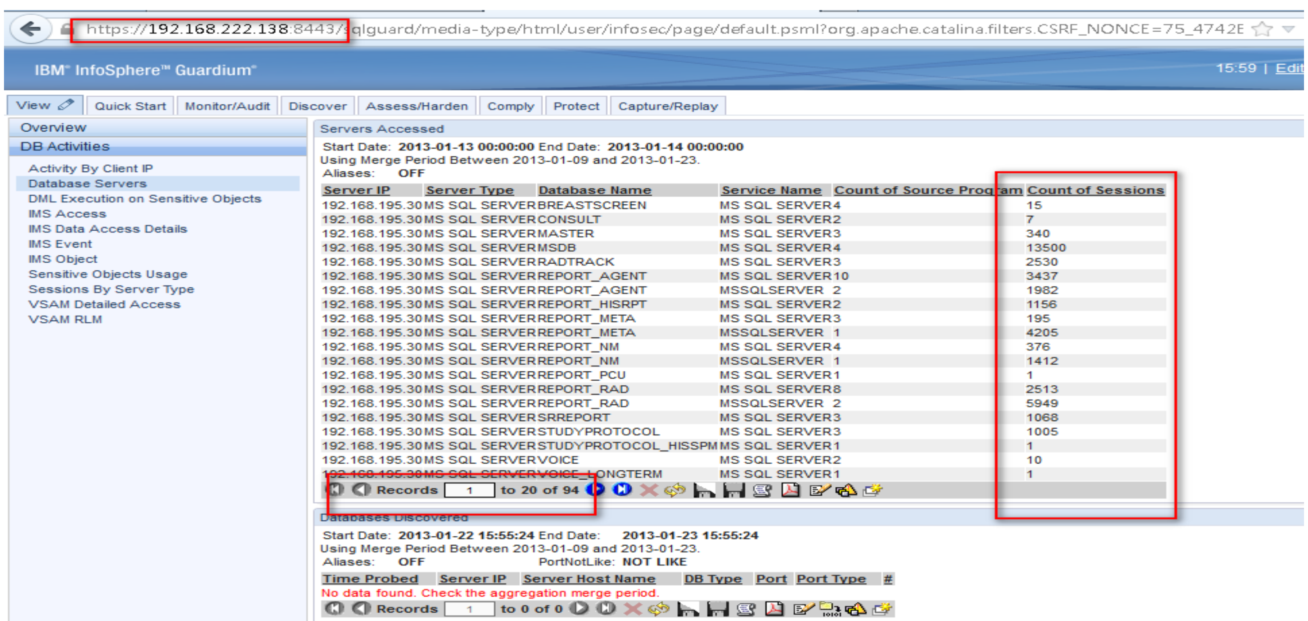
確認要開始Restore



於Aggregation/Archive Log內查看Restore還原狀況

Centeral Management 上資料還原（續）



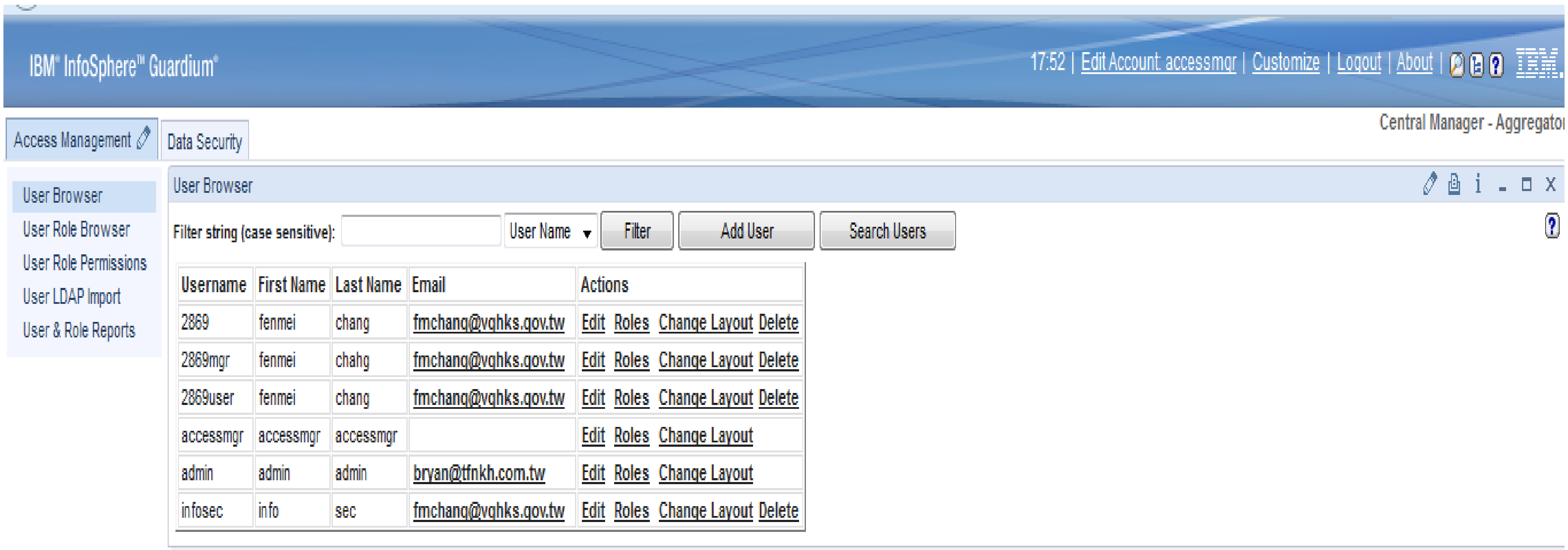


137（舊CM IP)為線上主機，資料還原到138主機
於Database Server Report報表內容筆數皆為94筆，還原資料穩合

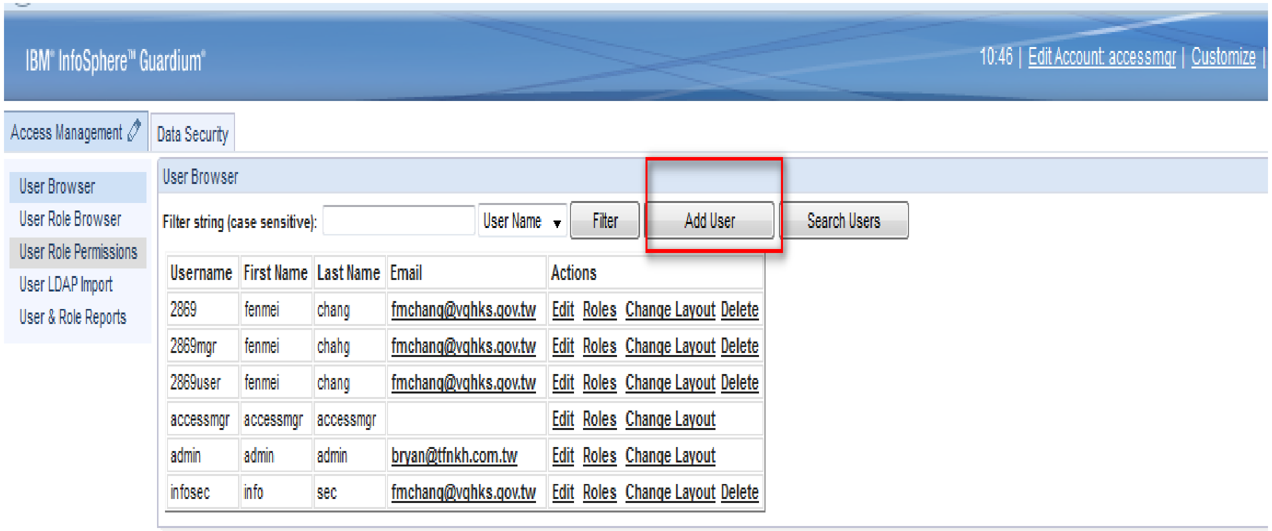
帳號管理

帳號管理者登入Guardium首頁

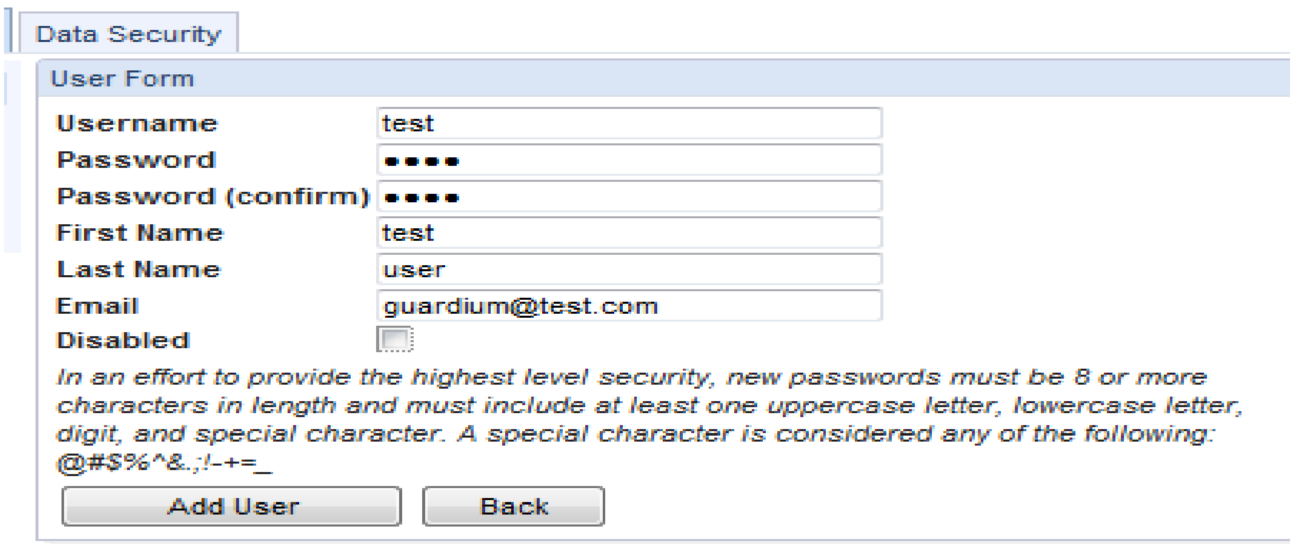
用accessmgr帳號登入，可對Guardium主機使用者帳號來管理
系統預設有accessmgr與admin為預設帳號
一般會另建infosec帳號做為稽核者帳號



新增帳號與修改



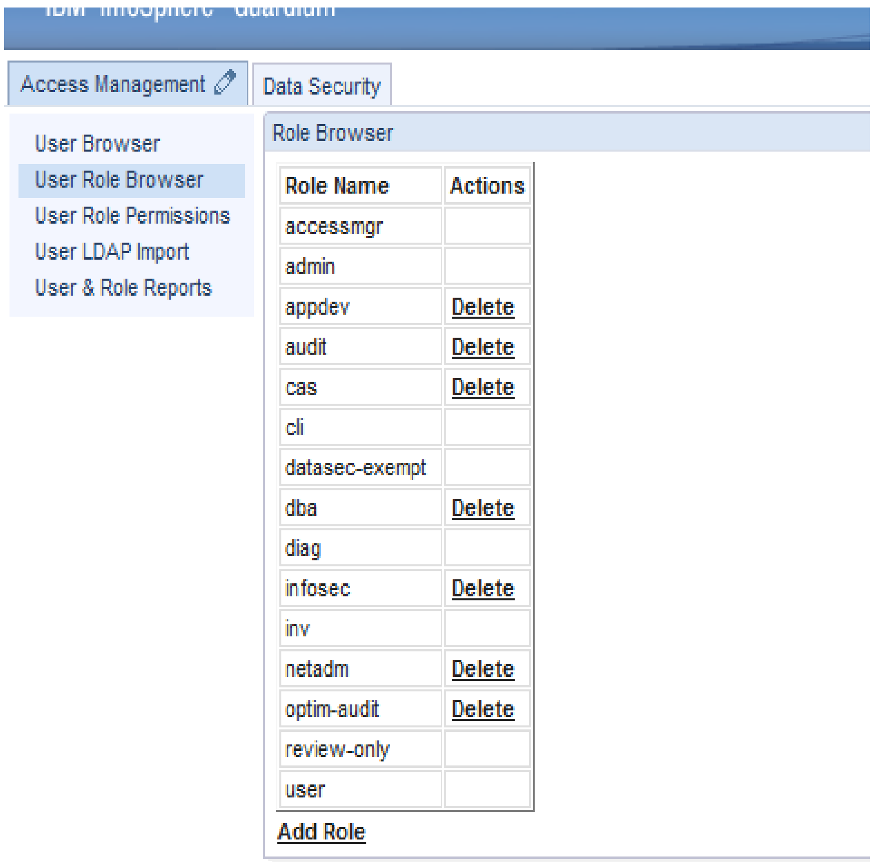
選add user新增使用者，或編修現有使用者

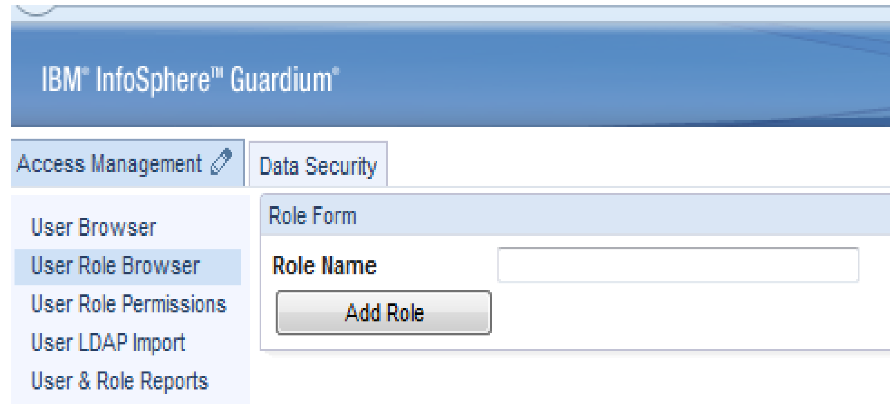


新增使用者，輸入相關資料，將Disabled點選移除

使用者角色管理

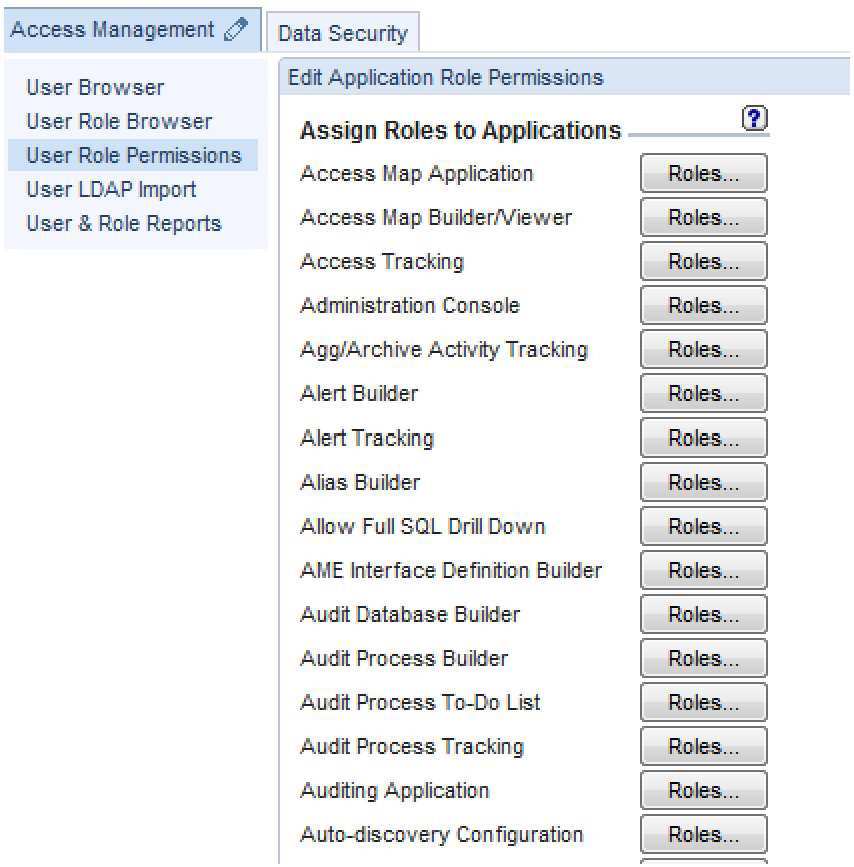
現有使用者角色管理, 新增或刪除

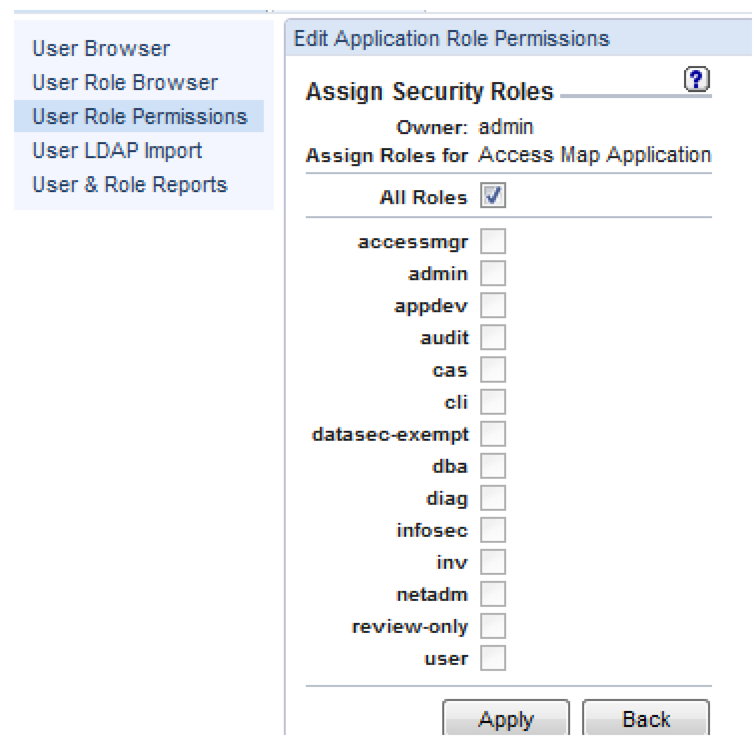




帳號權限修改

新增或刪除使用者所可使用之權限





帳號與角色報告

Access Management | Data Security

- User Browser
- User Role Browser
- User Role Permissions
- User LDAP Import
- User & Role Reports

User - Role

Start Date: **2012-11-27 17:14:59** End Date: **2012-11-28 17:14:59**
Using Merge Period Between 2012-11-14 and 2012-11-28.
Aliases: **OFF**

Login Name	Last Active	# of Role	# of Users
accessmgr	2012-11-28 17:09:20.0	1	1
admin	2012-11-28 16:24:10.0	1	1
infosec	2012-11-28 15:46:02.0	1	1

Records 1 to 3 of 3

All Roles - User

Start Date: **2012-11-27 17:14:59** End Date: **2012-11-28 17:14:59**
Using Merge Period Between 2012-11-14 and 2012-11-28.
Aliases: **OFF**

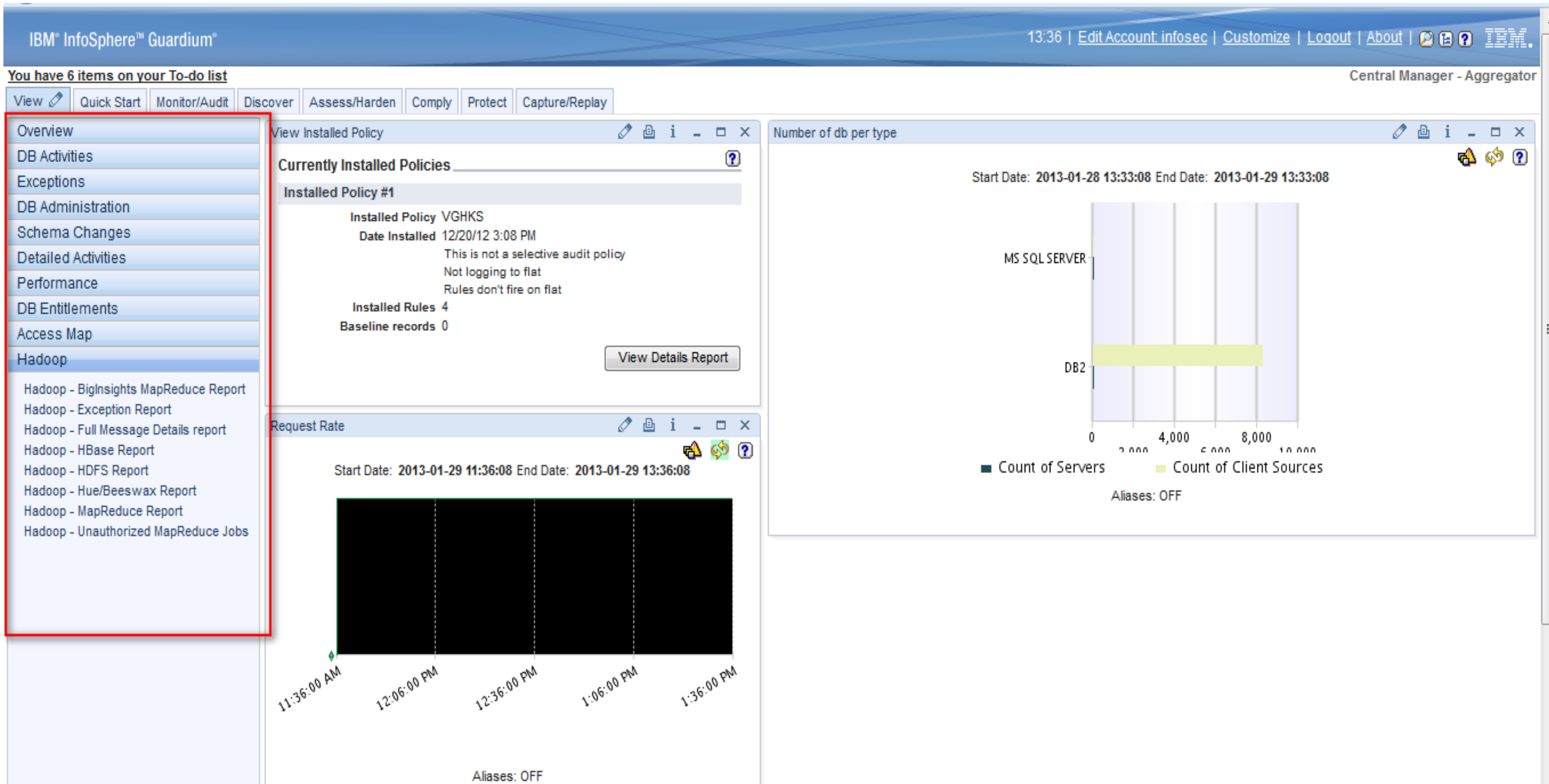
Role	Users Belong	# of Roles
accessmgr	1	1
admin	1	1
appdev	0	1
audit	0	1
cas	0	1
cli	0	1
datasec-exempt	0	1
dba	0	1
diag	0	1
infosec	0	1
inv	0	1
netadm	0	1
review-only	0	1
user	1	1

Records 1 to 14 of 14

稽核使用者報表操作

稽核使用者登入Guardium首頁

以infosec 登入帳號,瀏灠Guardium預設Report與建立自訂Report
每日稽核報表等工作
Guardium於View內已內建近70種基本報表



自訂之Report

除系統預設報告外,於My New Report內可自訂屬客制化Report

IBM® InfoSphere™ Guardium®

You have 6 items on your To-do list

View | Quick Start | Monitor/Audit | Discover | Assess/Harden | Comply | Protect | Capture/Replay

Build Audit Policies | Build Reports | My New Reports | Privacy Sets

- User Failed Login
- SQL Errors Returned
- Full SQL Time
- Admin_Users_Sessions
- Access Sensitive Objects
- Full_SQL_Response_Time
- Full SQL Time with AP user
- DDL Commands Execution
- DML Commands Execution
- DCL_Commands Execution
- SQL_Average_Execution_Time

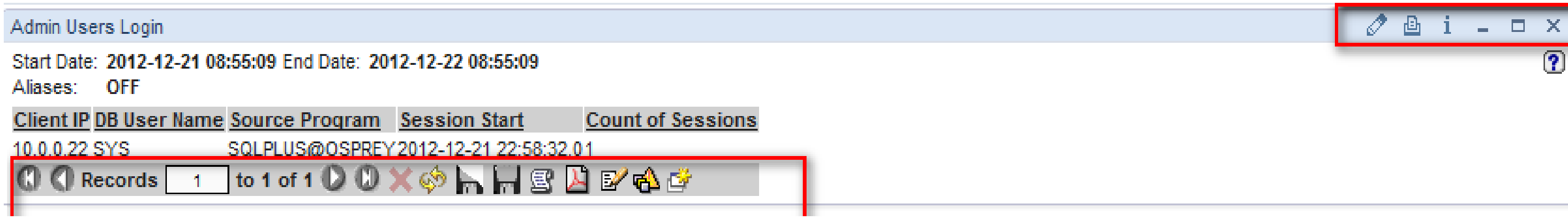
User Failed Login

Start Date: 2013-01-28 13:38:03 End Date: 2013-01-29 13:38:03
Using Merge Period Between 2013-01-15 and 2013-01-29.
Aliases: OFF Remote Source: DAMC02P.vghks.gov.tw
ServerIPLike: LIKE %

Exception Timestamp	DB User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions
2013-01-28 13:55:09.0	2681	192.168.222.162	192.168.222.162	DB2	2
2013-01-28 13:59:17.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 13:59:55.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 14:29:25.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 14:29:53.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 15:29:17.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 15:29:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 15:59:16.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 15:59:53.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 16:29:16.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 16:29:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 16:59:15.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 16:59:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 17:29:15.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 17:29:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 17:59:17.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 17:59:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 18:29:17.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1
2013-01-28 18:29:54.0	BATADMIN	192.168.222.194	192.168.222.194	MS SQL SERVER	1
2013-01-28 18:59:14.0	DB2SERVI	192.168.97.79	192.168.97.73	DB2	1

Records 1 to 20 of 96

報表操作

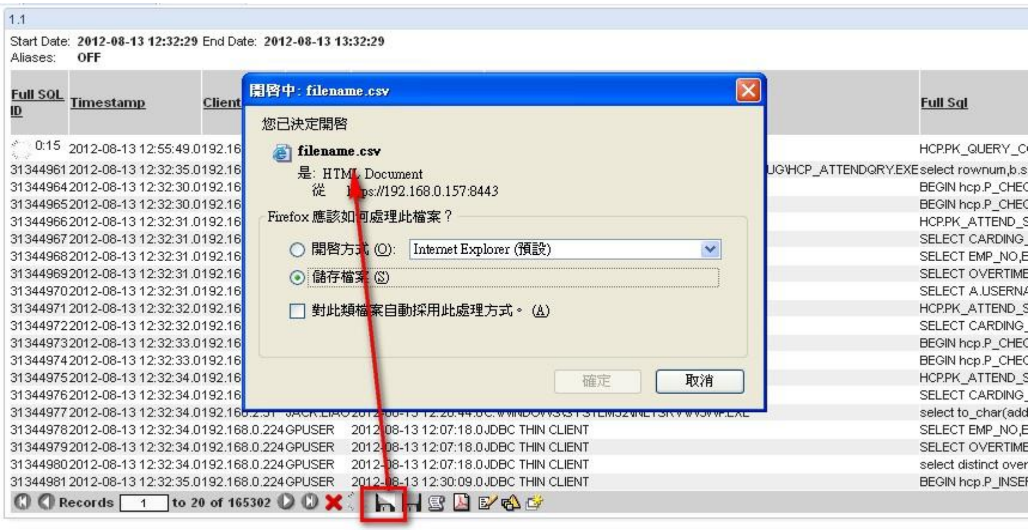


1		擷取資料範圍修改範圍、時間
2		印出該頁整報表資訊
3		顯示報表設置時間與報表編號
4		關閉報表　　　*警告此選項不可輕易更動*
5		縮小報表
6		放大報表
7		前往下一頁面
8		前往最後頁面
9		更新資料
10		另存 CSV 格式(目前報表頁面資料)
11		另存 CSV 格式(報表全部資料)
12		開新視窗顯示全部資料
13		產出 PDF 檔案
14		樹狀圖表陳列資料
15		新增修改報表定義條件

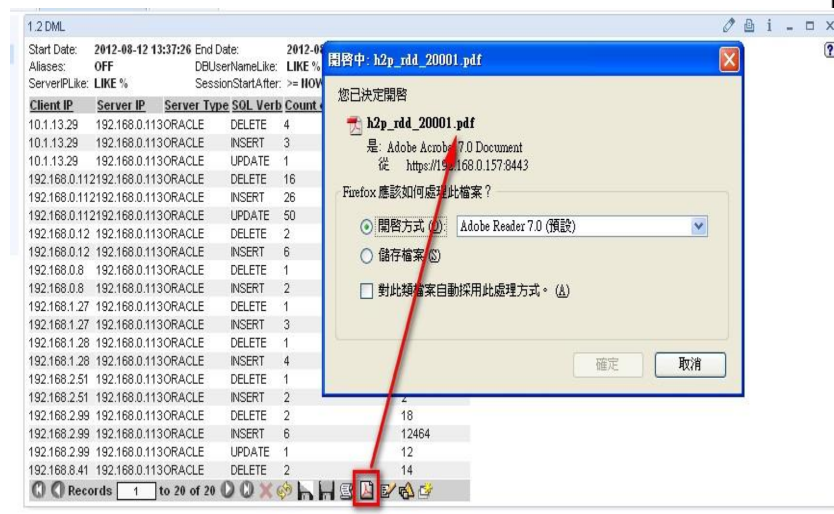
報表儲存

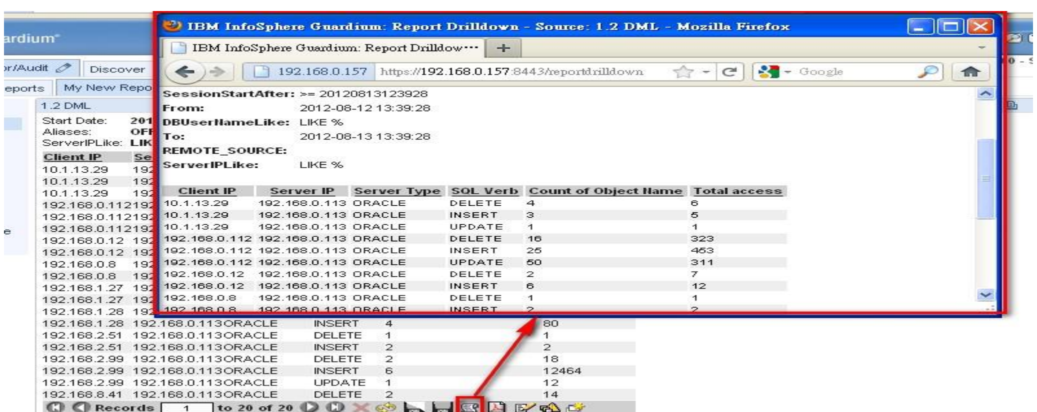
可以將報表另存成: CSV/HTML/PDF 等格式

CSV 報表



PDF 報表

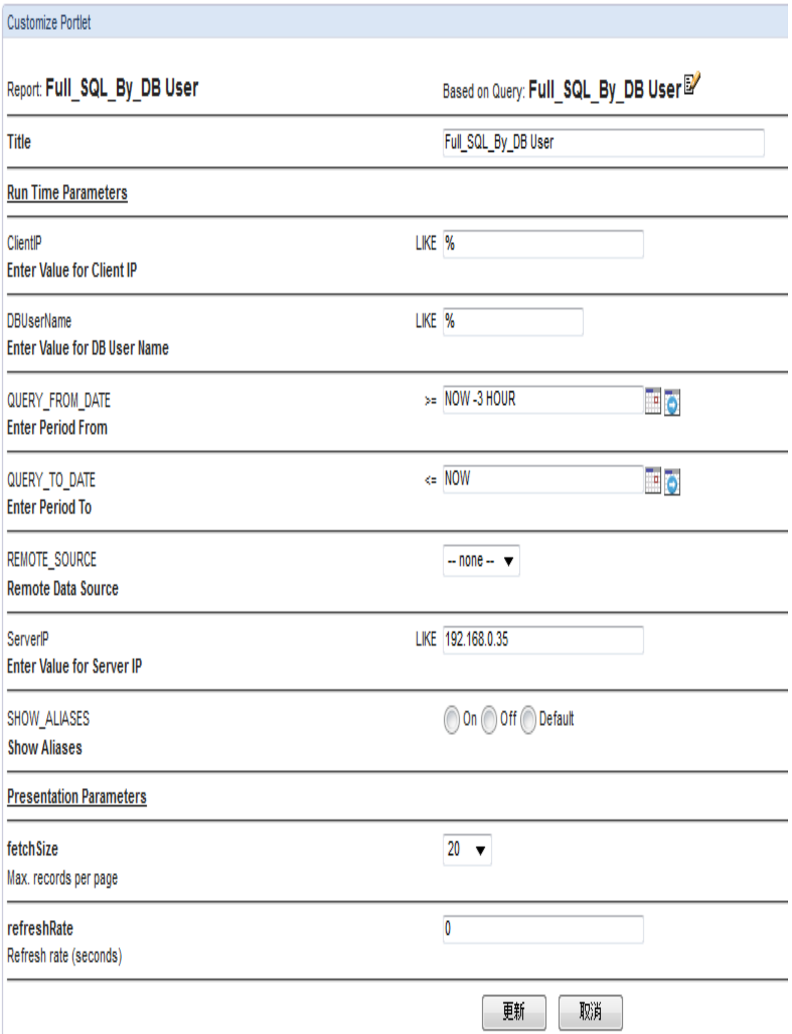




HTML 報表

報表內容操作

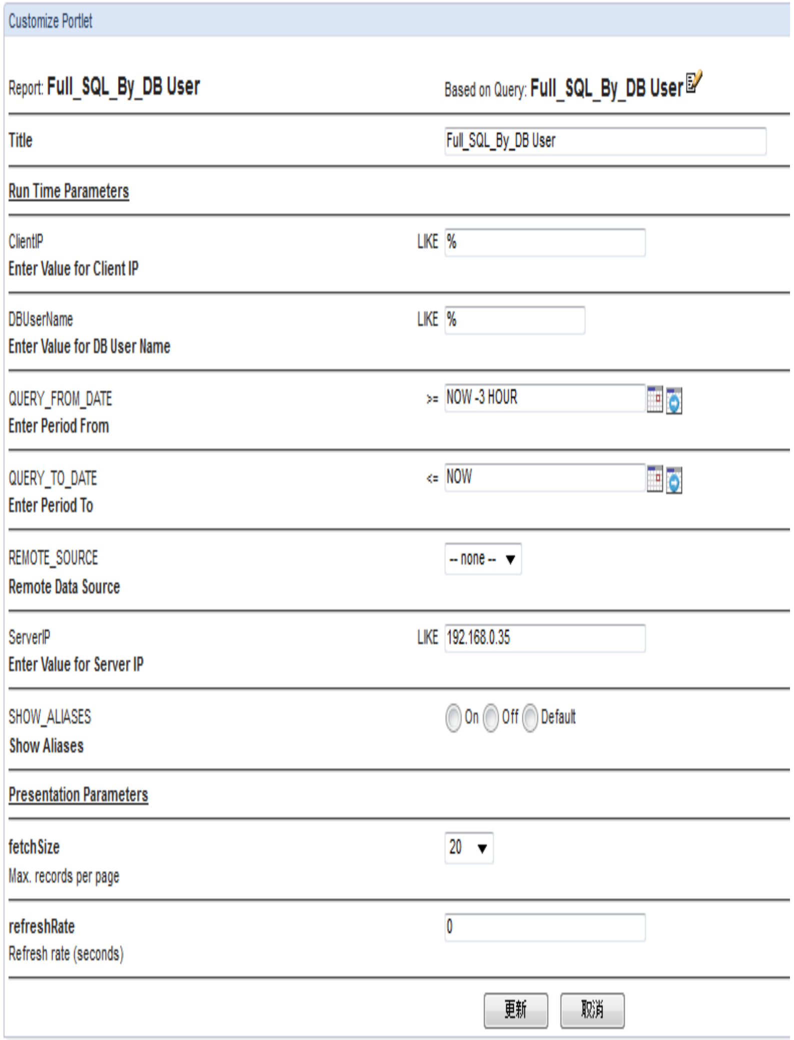
圖示可修改內容概覽表



1	Report:	報表名稱	
2	Based on Query:	新增修改報表定義條件	
3	Title	修改報表抬頭名稱	
4	Skin	修改報表顏色調整	
5	ClientIPAddress Enter Value for Client IP	1. 鎖定 IP，例：192.168.2.1 2. 擷取全部，例： 可用【%】或【*】代表所有	
6	DBUserName Enter Value for DB User Name	1. 鎖定 DB User，例：ADMINISTRATOR 2. 擷取全部，例： 可用【%】或【*】代表所有	
7	GROUPING_SUB_TYPE Choose Grouping Type	相同群組方式顯示資料 Choose A Group Type Or Sub-Type to Group By Choose A Group Type Or Sub-Type to Group By ================================== Group Type: COMMANDS Group Type: Server IP Group Type: USERS Group Type: OBJECTS Group Type: SOURCE PROGRAM Sub Type: Programs Sub Type: fsdf Group Type: Client IP	
8	QUERY_FROM_DATE Enter Period From	起始時間	月曆選擇時間 條件選擇時間
9	QUERY_TO_DATE Enter Period To	結束時間	月曆選擇時間 條件選擇時間

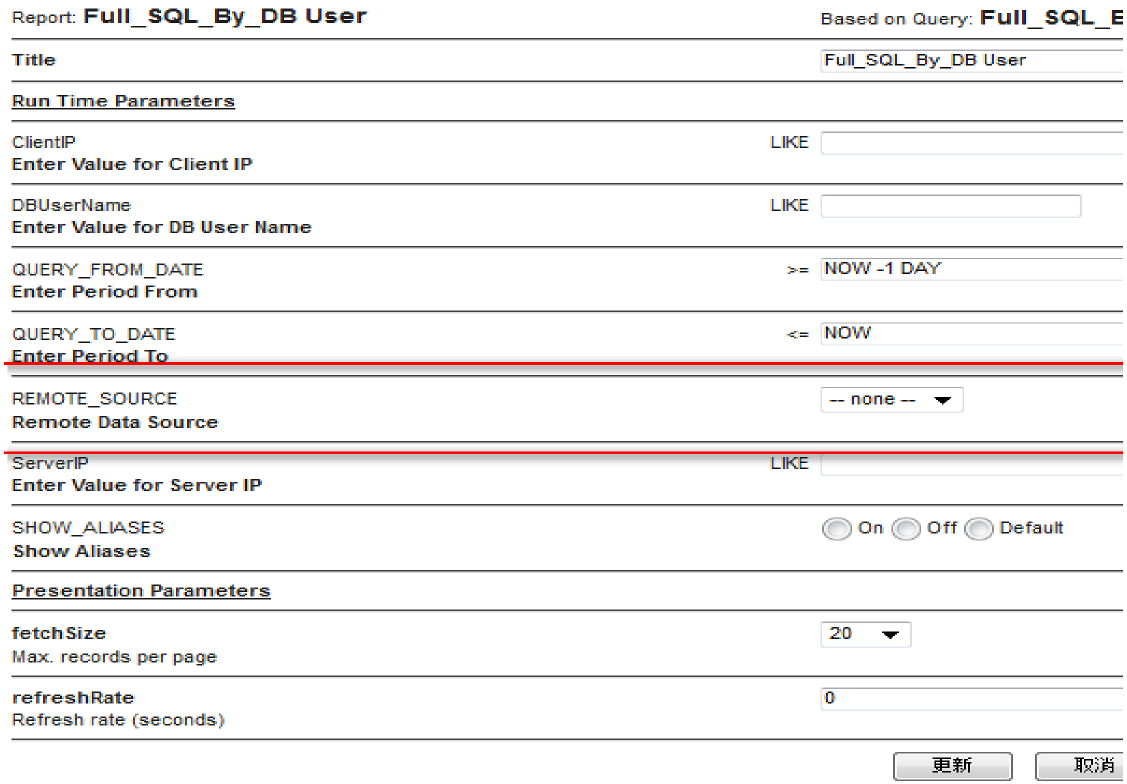
報表內容操作（續）

圖示可修改內容概覽表

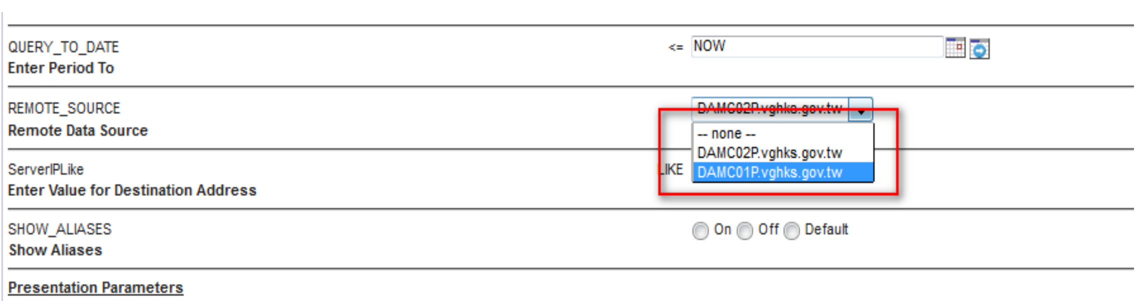


10	REMOTE_SOURCE Remote Data Source	-- none -- -- none -- none
11	ServerIPLike Enter Value for Server IP	1. 鎖定 Server IP，例：10.10.2.9 2. 擷取全部，例： 可用【%】或【*】代表所有
12	SessionStartAfter Enter Value for Session Start	設定 Session 時間
13	SHOW_ALIASES Show Aliases	設定別名呈現 On Off default
14	fetchSize Max. records per page	顯示報表筆數(最小 1 最大 100) 20 1 2 4 5 10 20 50 100
15	refreshRate Refresh rate (seconds)	設定報表更新頻率(0 不更新 3600 最大更新頻率)

報表內容操作（續）

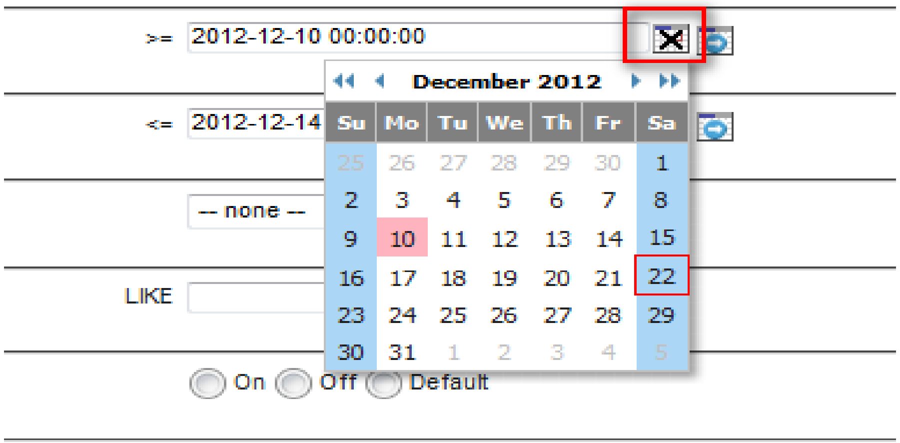


若有CM環境時，大多於CM下操作報表，但CM資料通常為一天前資料，可於Remote_Source內選擇，直接到該Collector主機瀏灠即時資料

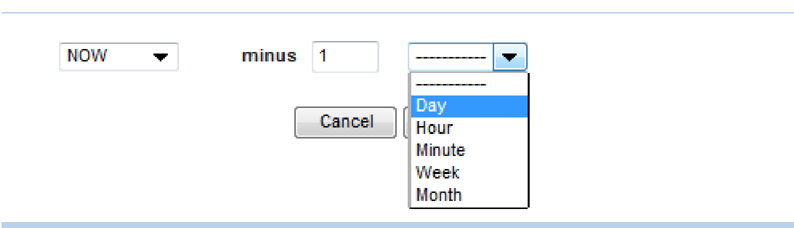


選擇Collector主機

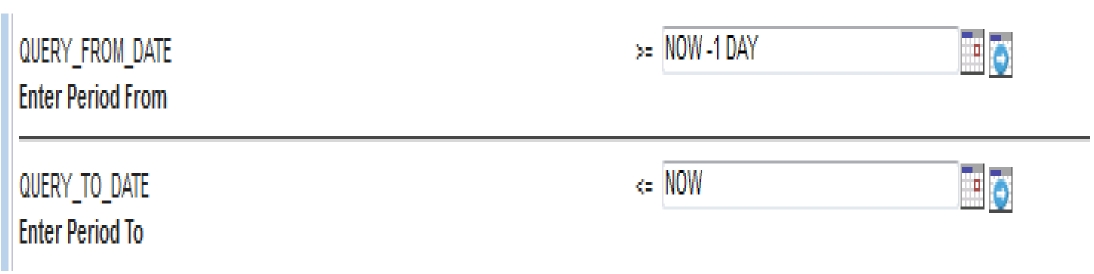
報表內容時間條件



以日期為單位條件



以時間為單位條件

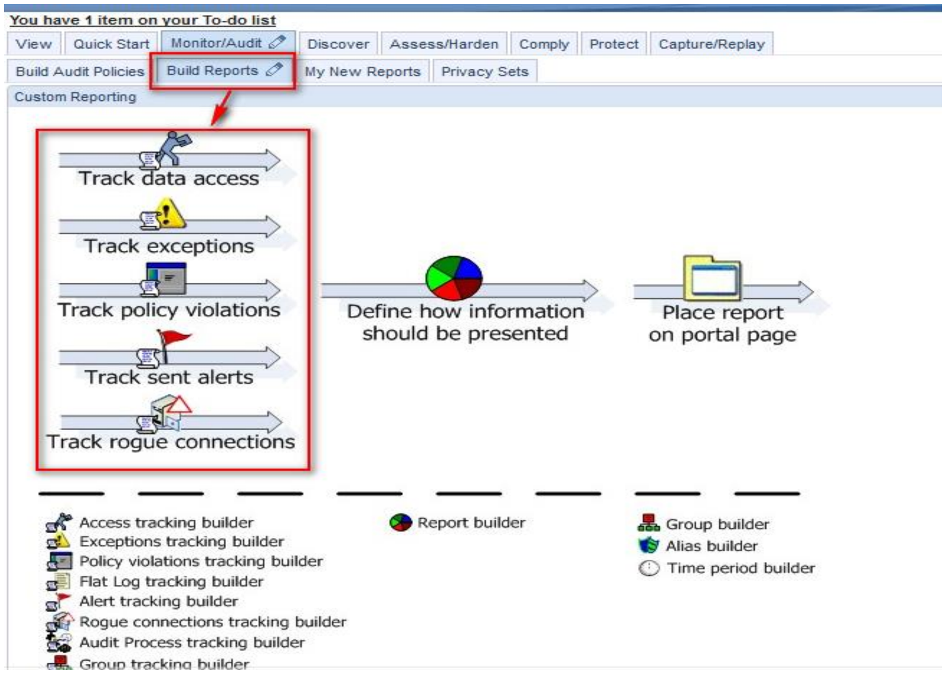


一般常用時間為單位條件
從現在往前推多久時間

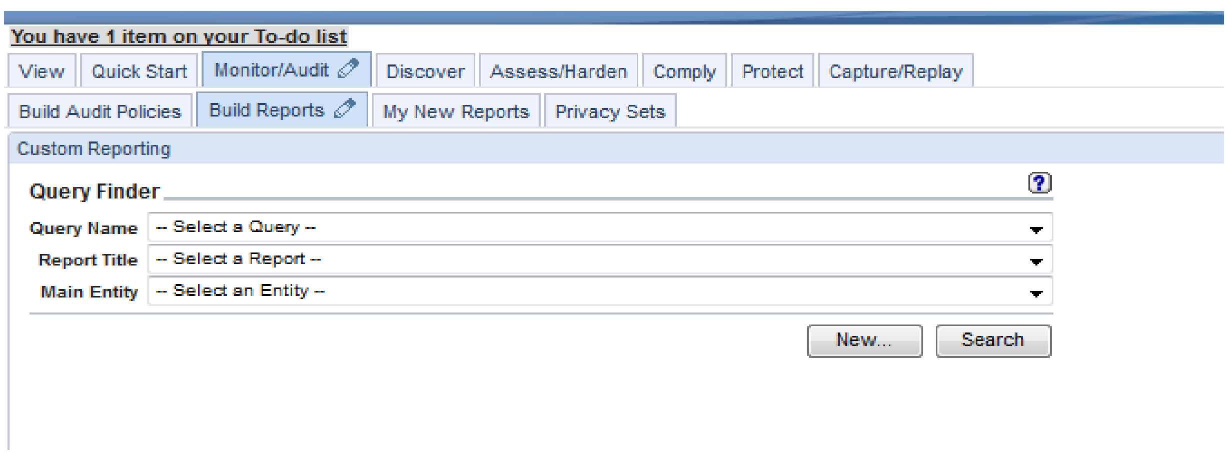
Your Solution Partner

稽核使用者報表製作

建立報表

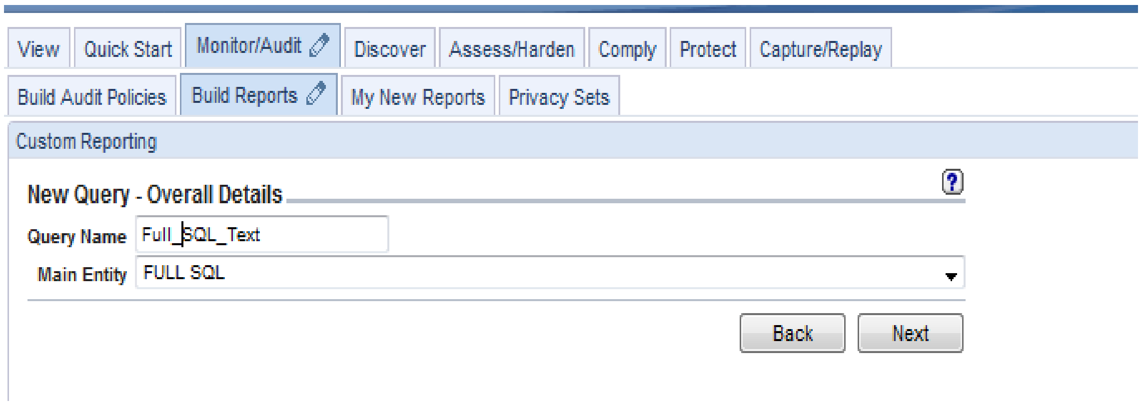


	項目	功能簡介
1	Track data access	報表製作與搜尋。
2	Track exceptions	例外報表製作與搜尋。 。
3	Track policy violations	違反策略的報表製作與搜尋。
4	Track sent alerts	已發過Alert的統計報表製作與搜尋。
5	Track rogue connections	例外連線狀況報表製作與搜尋。
6	Define how information should be presented	已製作報表內容設定修改與報表呈現方式轉換。例如：可利用本功能將報表轉換成圓餅圖、長條圖等其他的方式呈現。
7	Place report on portal page	新製作報表放置的位置。

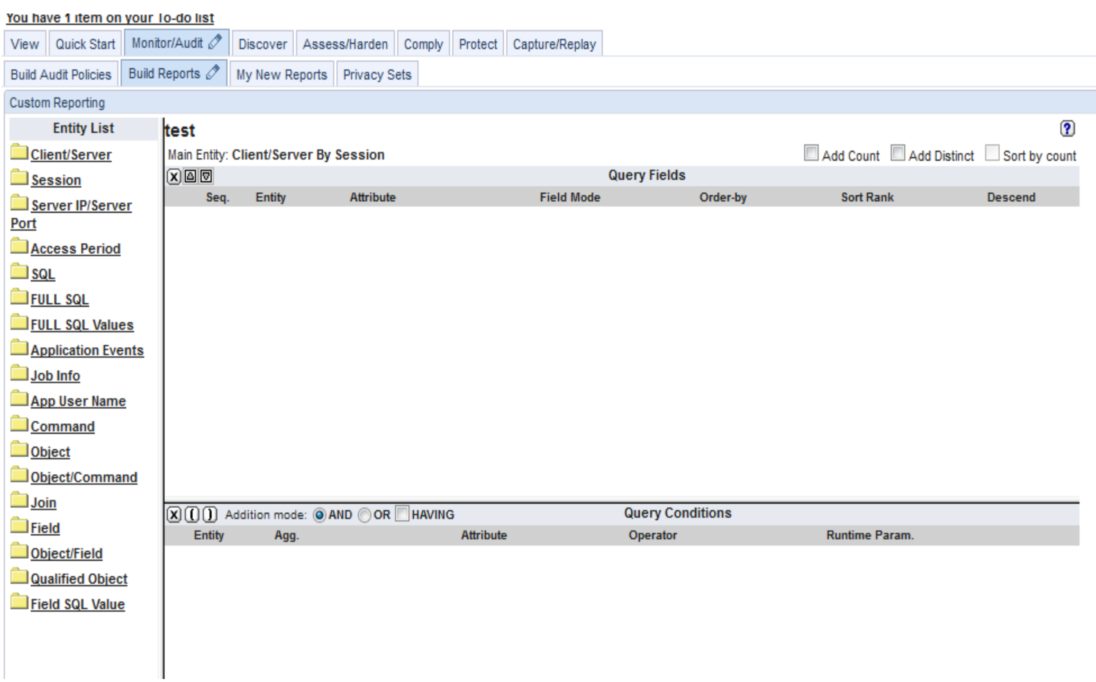


選取"New"建立新Report

建立報表(續)

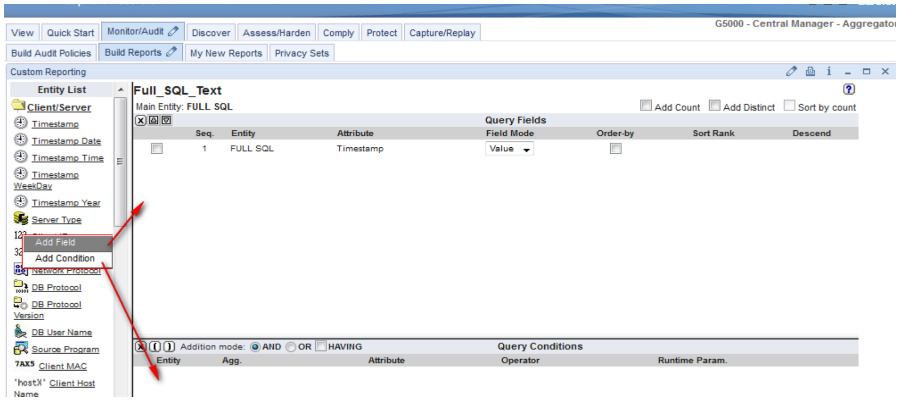


於Query Name中輸入
Report欲定名稱
Main Entity選擇實體種類(以何種觀點來檢視報表)
選取Next

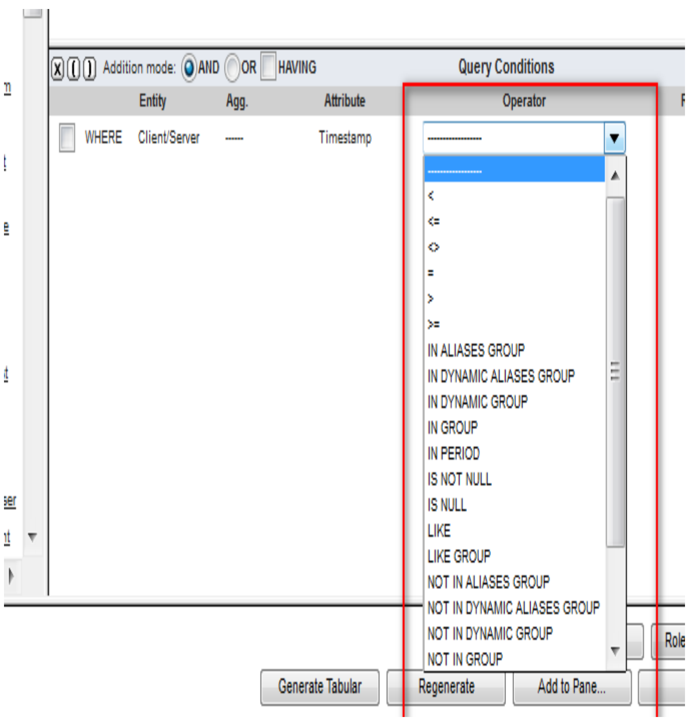


產生一空白報表
左側**Entity List**
可將其選入報表內

建立報表(續)



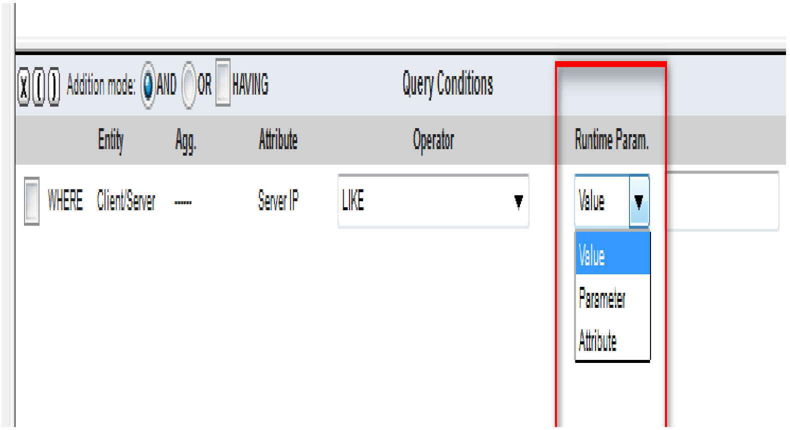
將欲使用Entity選入報表內
Add Field:報表呈現內容
Add Condition:條件篩選



於Query Condition中的Operator選單

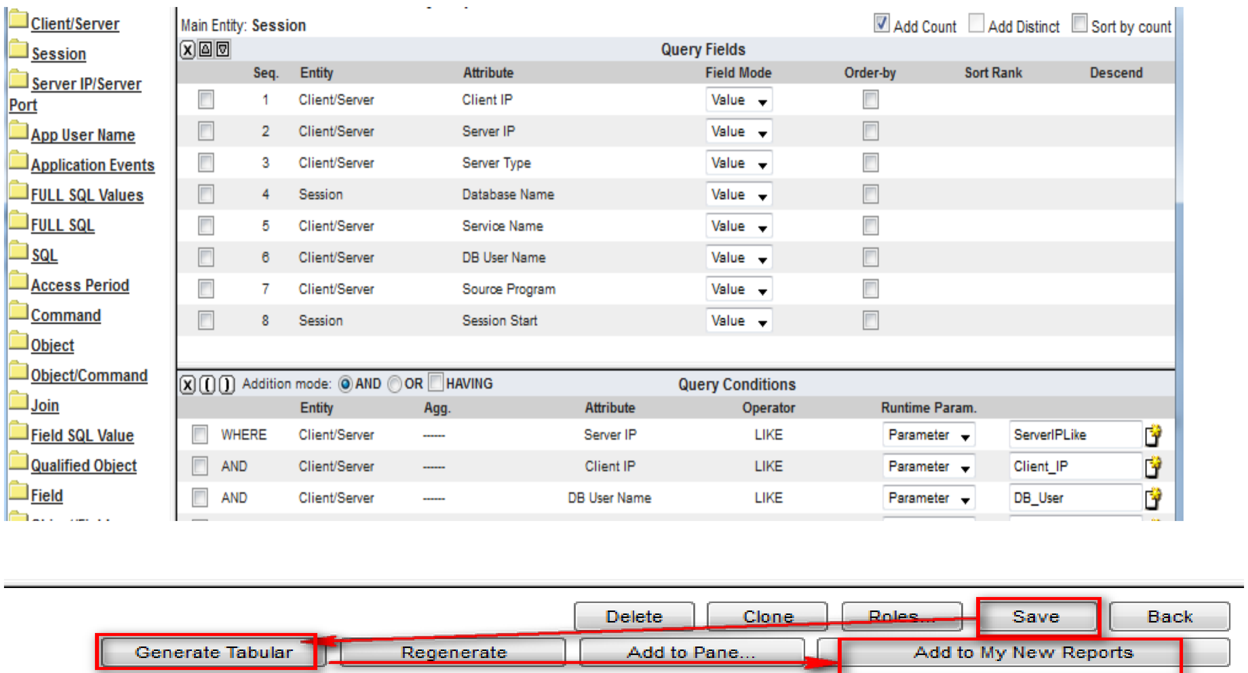
項目	簡介
<	小於空格中的數值
< =	小於等於空格中的數值
< >	不等於空格中的數值
=	等於空格中的數值
>	大於空格中的數值
> =	大於等於空格中的數值
IS NULL	空白的資料
IS NOT NULL	所有存在的資料
LIKE	與空格中相似的數值或參數。例如%tea%，即是包含所有字串中包含 tea 的字串，如：*tea*, *TeA*, *tEam*, *steam*
LIKE GROUP	字串中包含所有相似於 Group 中所設定的數值。
NOT LIKE	不顯示與空格中相似的數值或參數。
REGEXP	顯示所設定的字串。
IN PERIOD or NOT IN PERIOD	顯示在所設定的時間內或不顯示所設定時間內的資料。
IN GROUP or NOT IN GROUP or CATAGORIZED AS or CLASSIFIED AS	所有於 Group 中所設定數值的資料或不顯示於 Group 中所設定數值的資料。

建立報表(續)



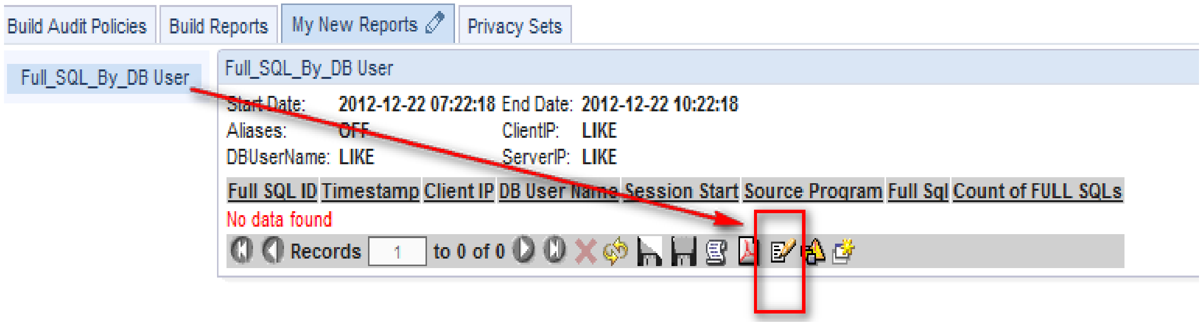
於Query Condition中的Runtime Param選單

Value	顯現所輸入數值或字串相關的資料
Parameter	輸入欲查詢資料的敘述。
Attribute	顯示該屬性中的資料。

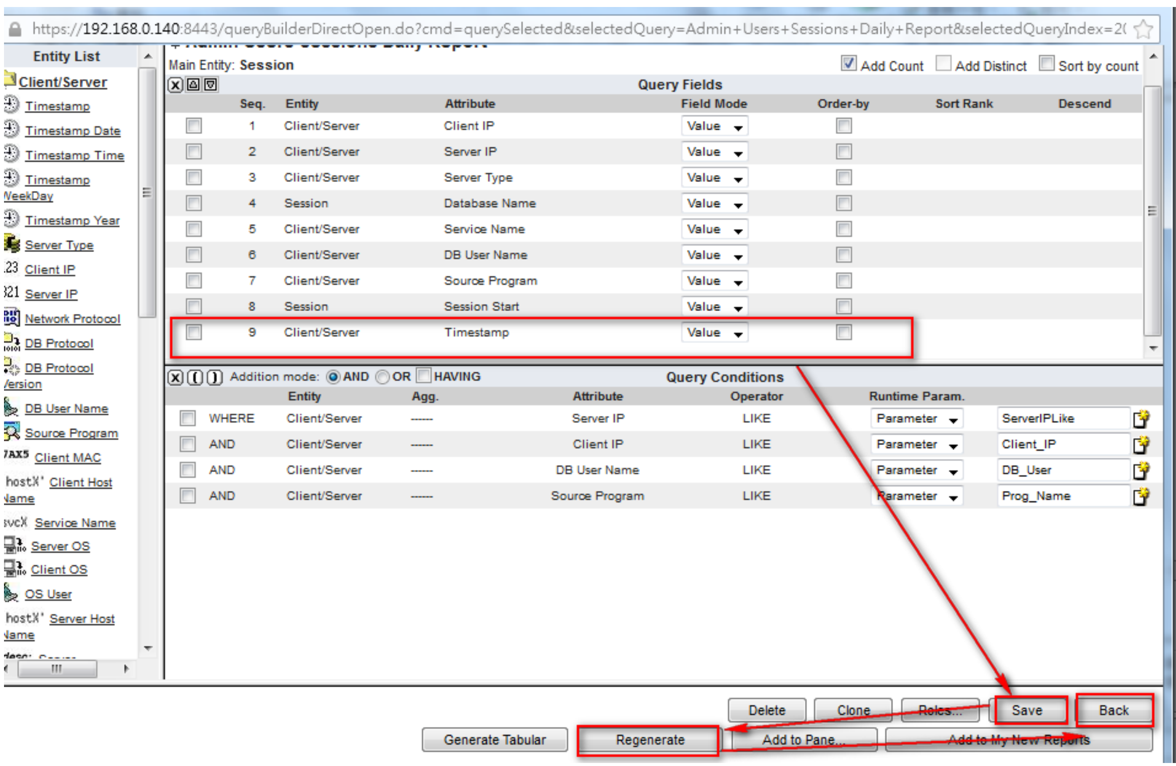


報表完成後,點擊
Save →
Generate Tabular →
Add To My New Reports
Back 退出

修改報表內容

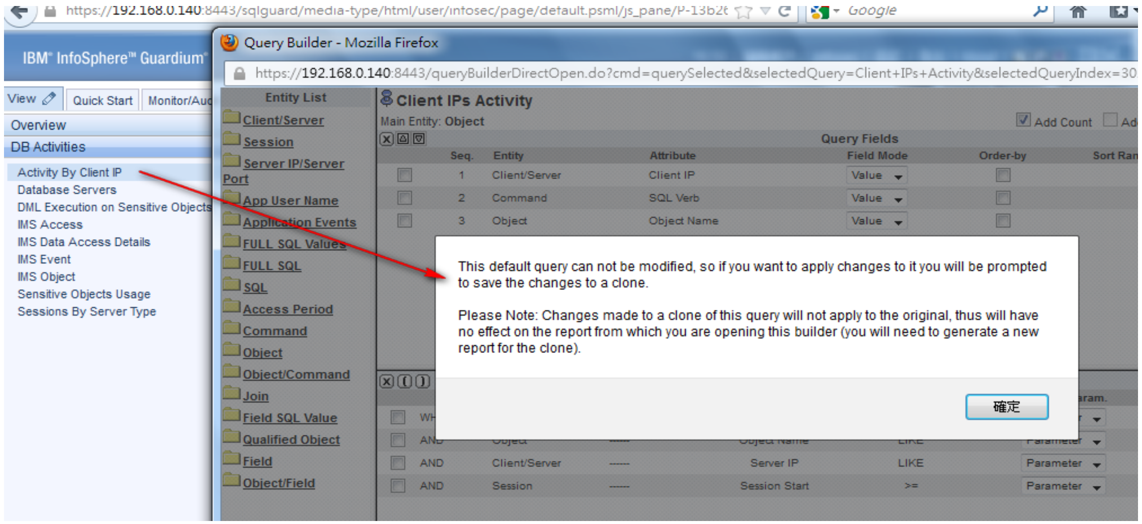


屬於My New Report報表，
可隨時對報表修改內容

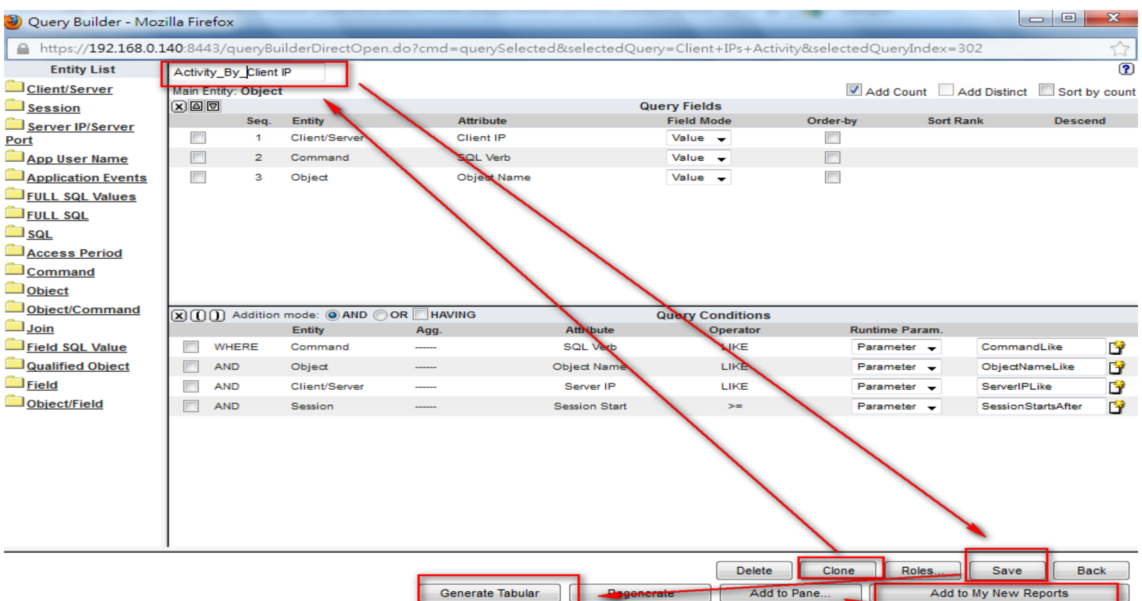


新增或刪除Entity後，
點擊
Save→
Regenerate →
Back 退出

使用現有系統報表修改



另可使用系統所提供之Report來修改，再將存於My New Report中
但預設報表，選取修改時會出現不允許修改，需先做Clone動作



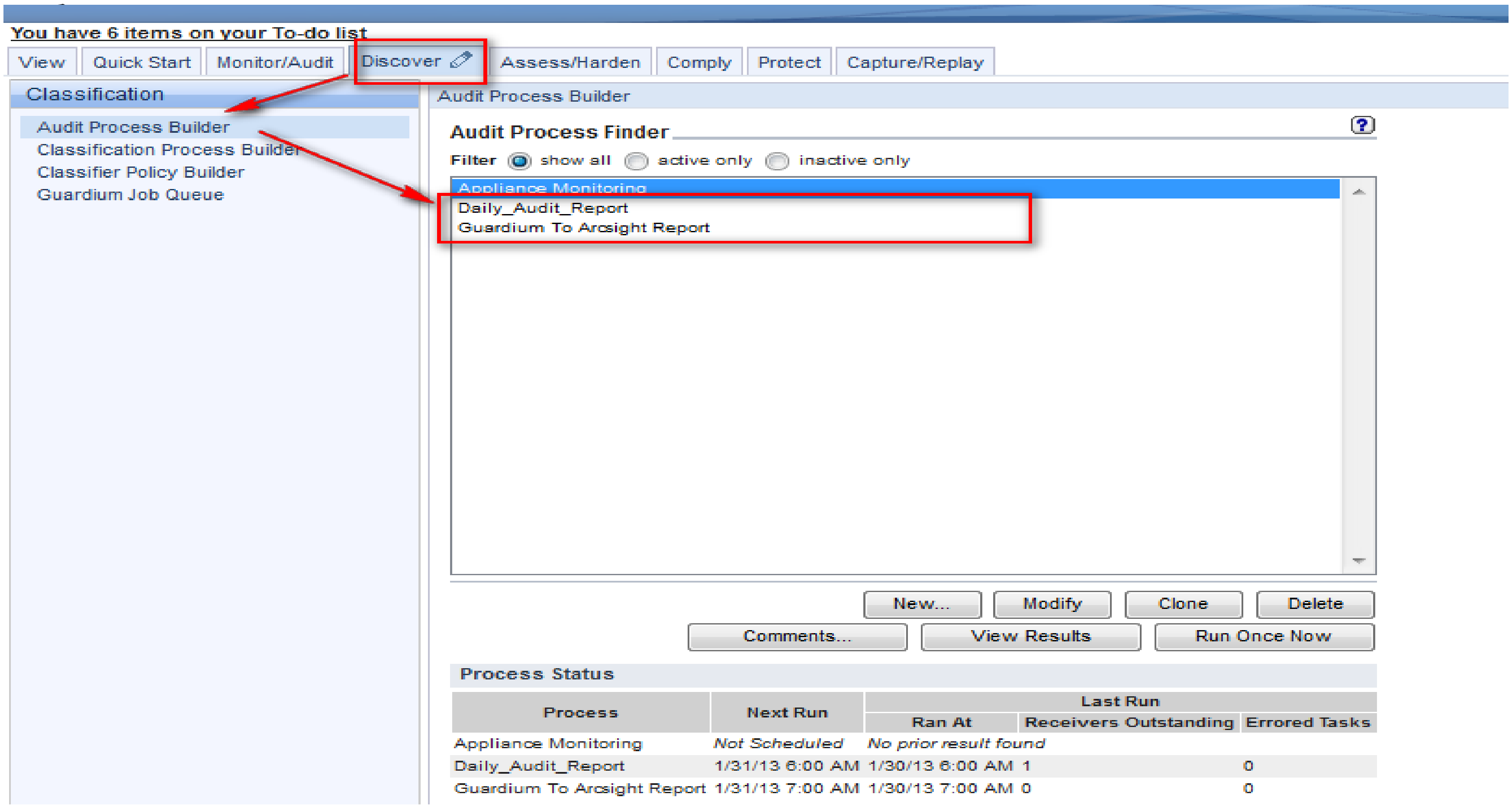
選取Clone→
提供新報表名稱→
Save→
新增或刪除Entity→
Save→
Generate Tabular→
Add To My New Reports
Back 退出

Taifon Your Solution Partner

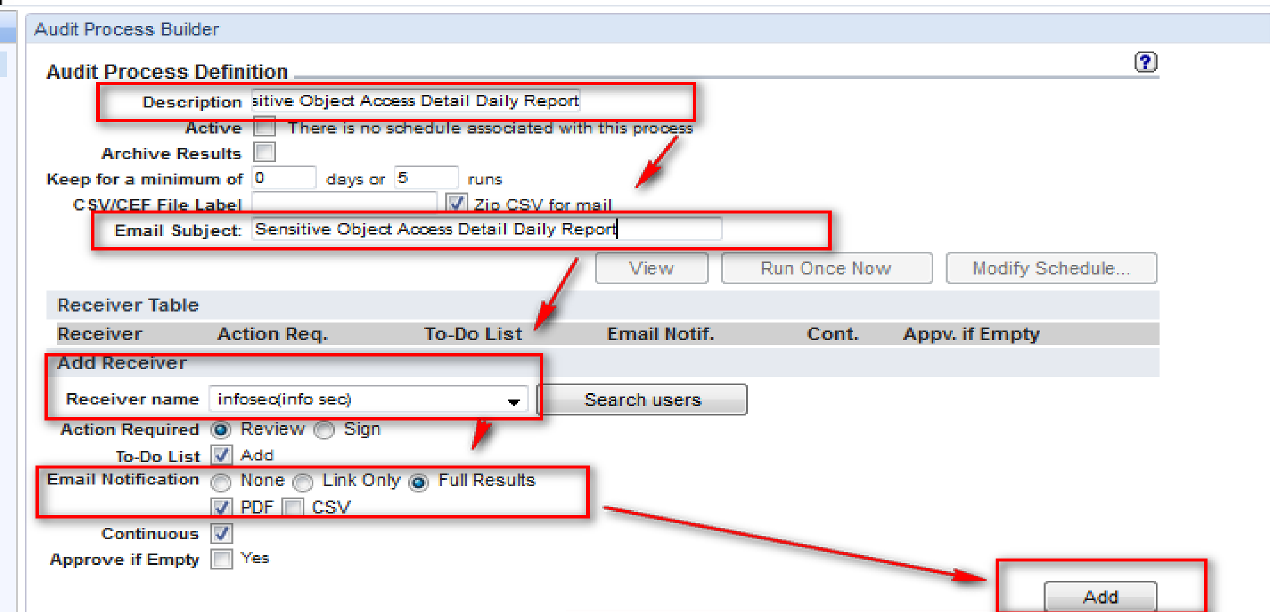
稽核使用者
每日稽核報表

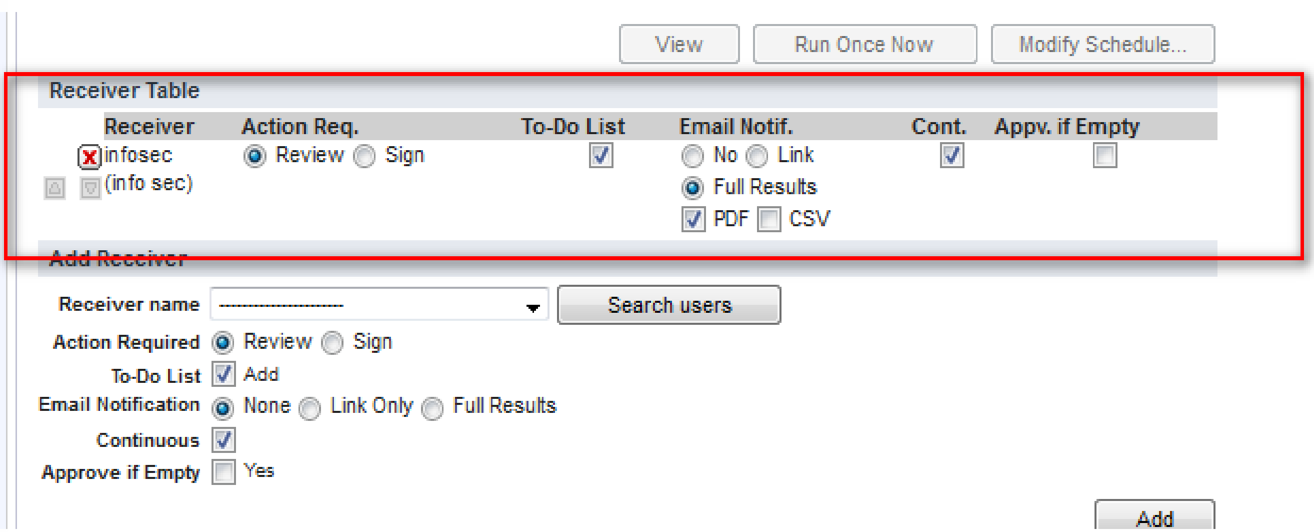
稽核報表製作

可用infosec user登入,Discovery->Audit Process Builder,製作屬於每日的稽核報表,可將指定報表依時間寄送給稽核人



稽核報表製作流程





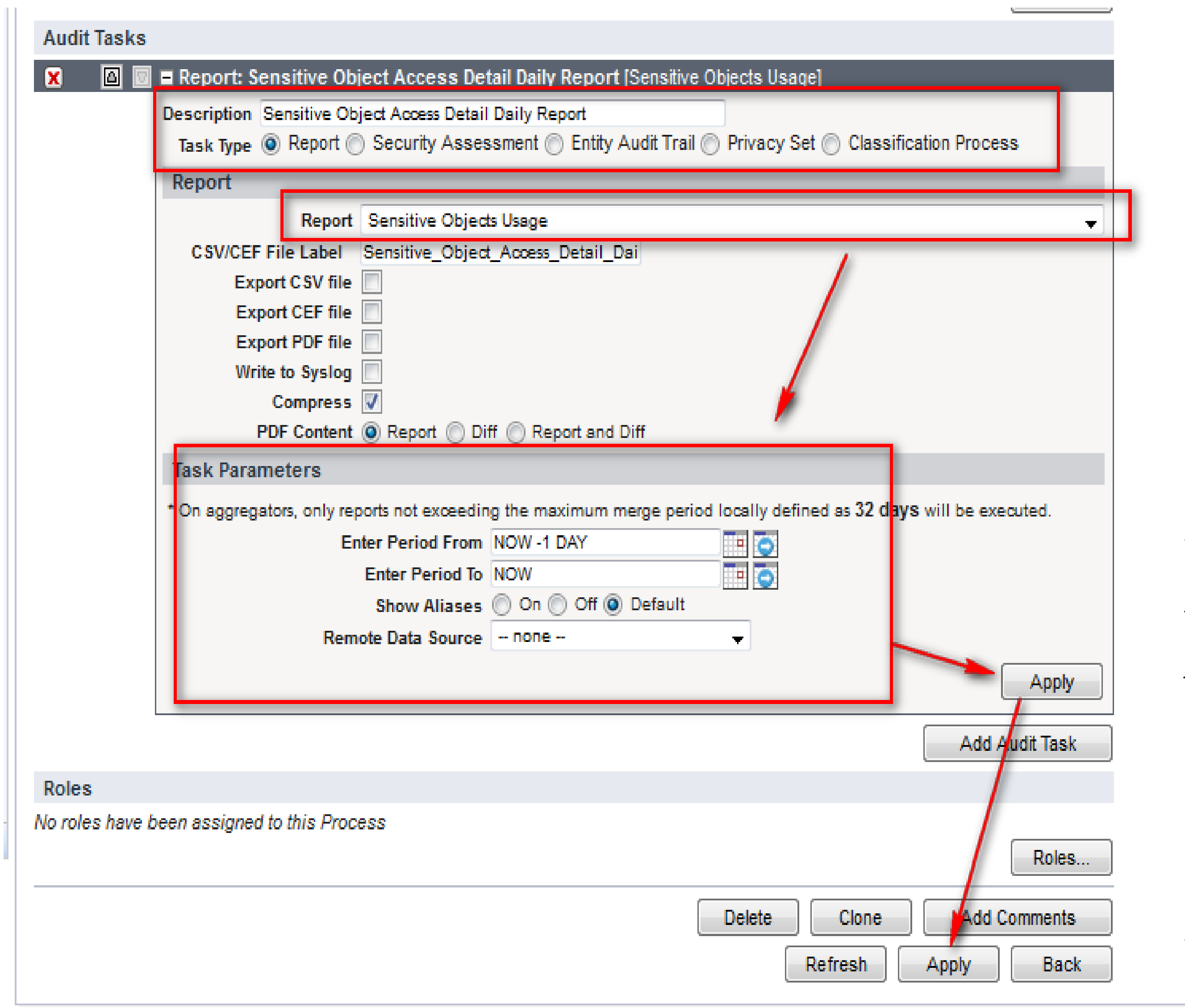
指定稽核報表名稱
Mail標題

Add Receiver
加入收件人
選擇報表格式,內容

確定收件人後add加入

後續可隨時新增或刪除報表收件人與報表格式

稽核報表製作流程(續)



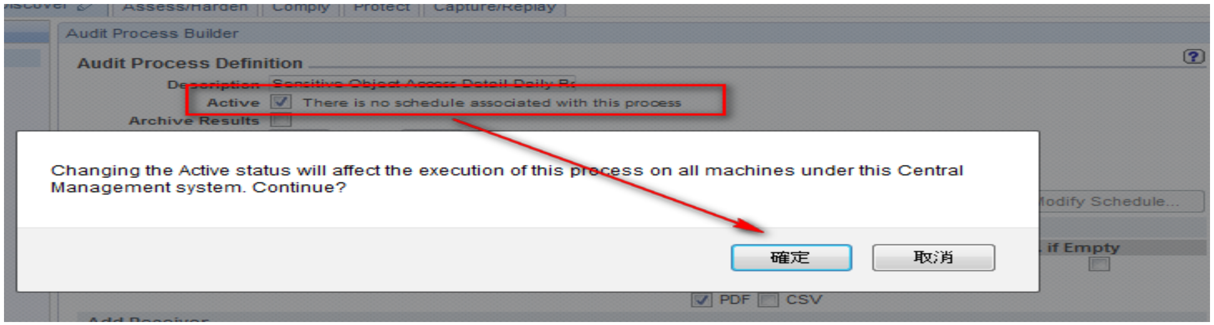
設定Audit Task
提供Task名稱
Task Type:Report
選取要統計之報表

設定該報統計的時間區段表
Apply確定完成此Task

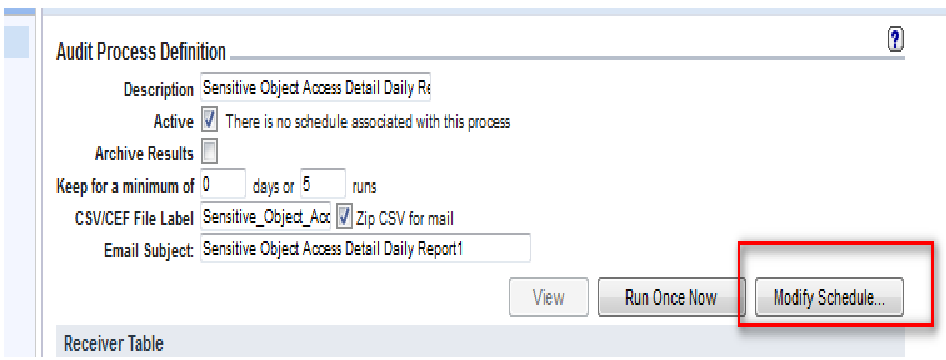
可同時設定許多Task
選Add Audit Task

設定完成選Apply

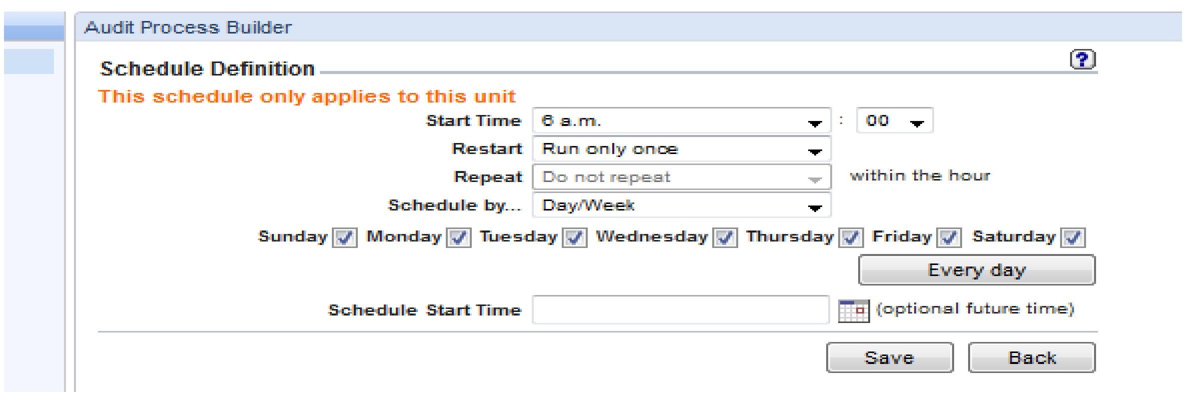
稽核報表製作流程(續)



設定完成後,勾選上方
Active 啟動該報表
選Active後會提醒要
Save後才能修改工作排程
點選最下方的Apply



可馬上測試 Run Once Now
或設定報表寄送時間排程

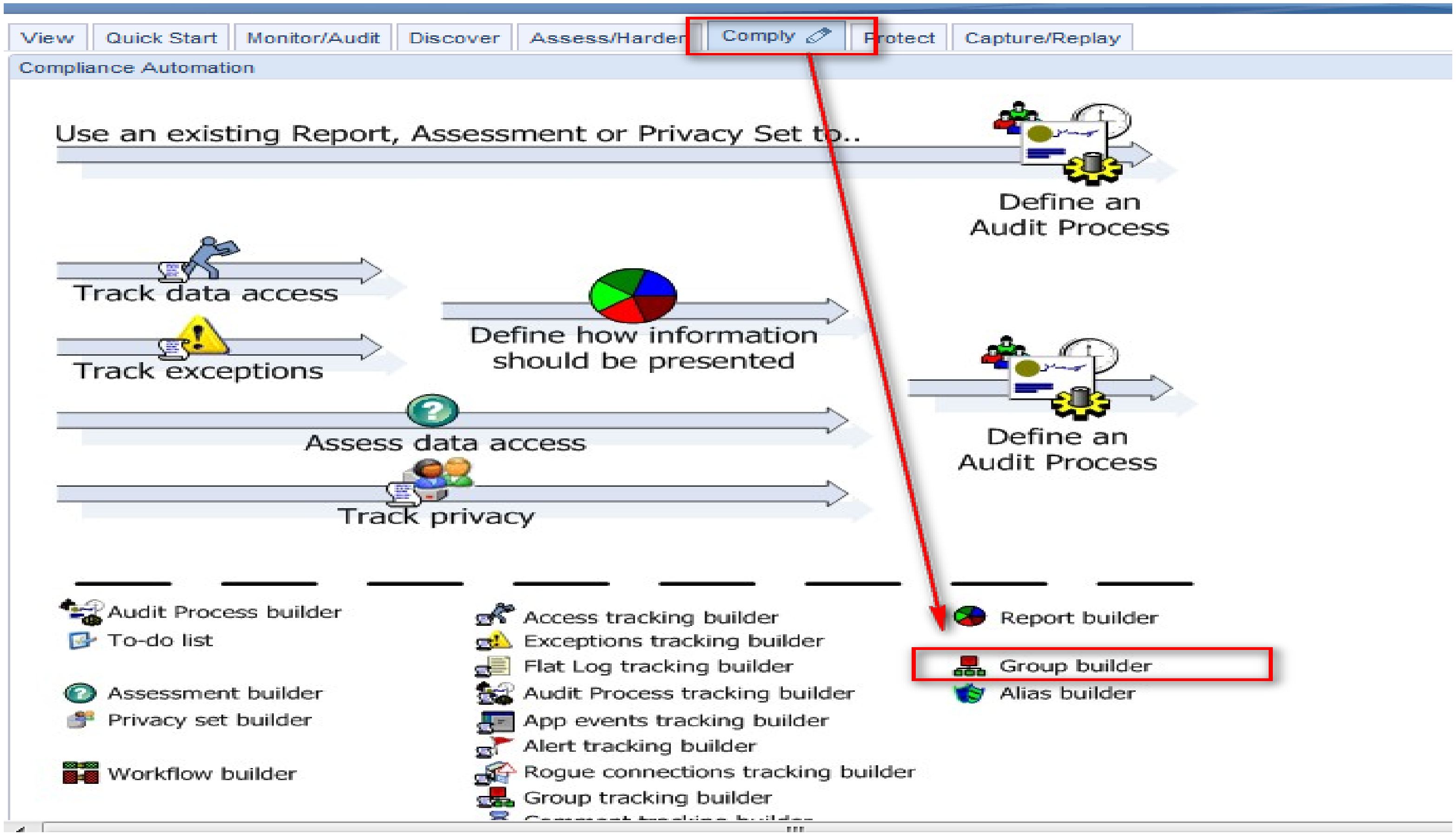


設定寄送時間,週期

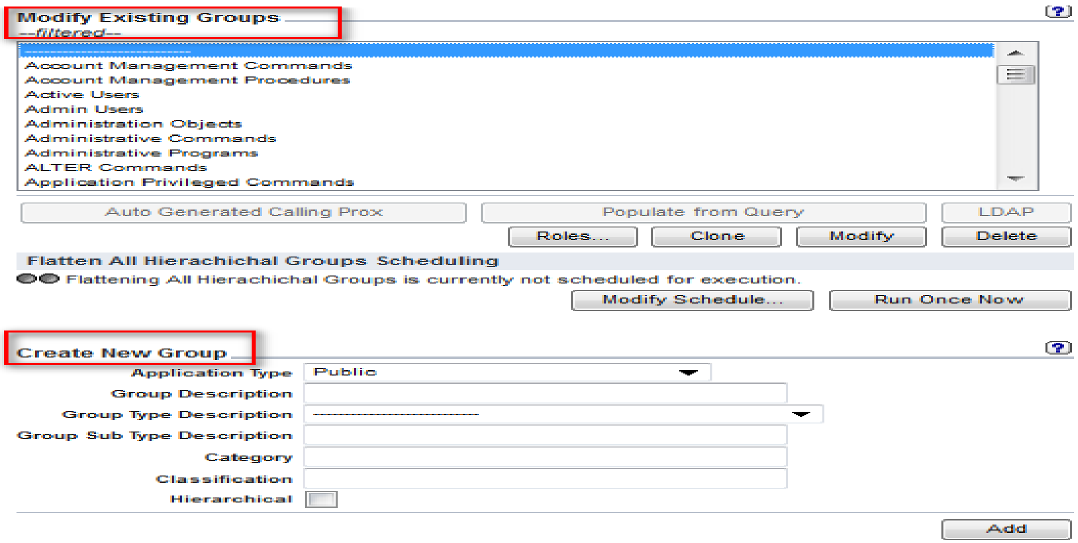
稽核使用者
群組功能操作

製作群組

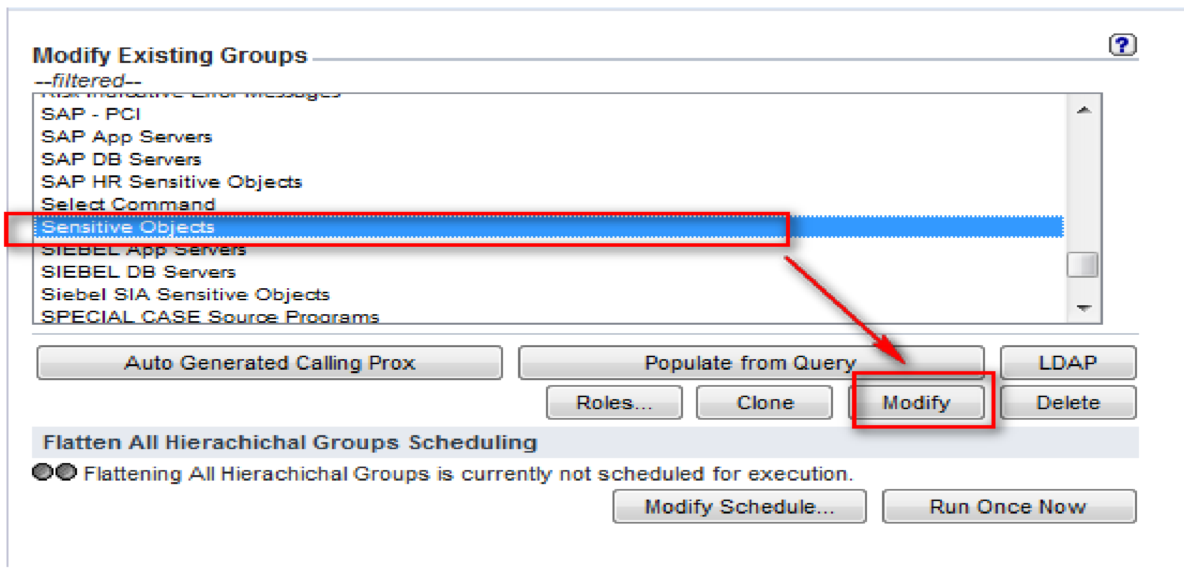
可透過建立群組來管理,如敏感性資料,主機群組等等來方便管理與設定
選取Comply→ Group Builder



群組修改與新增

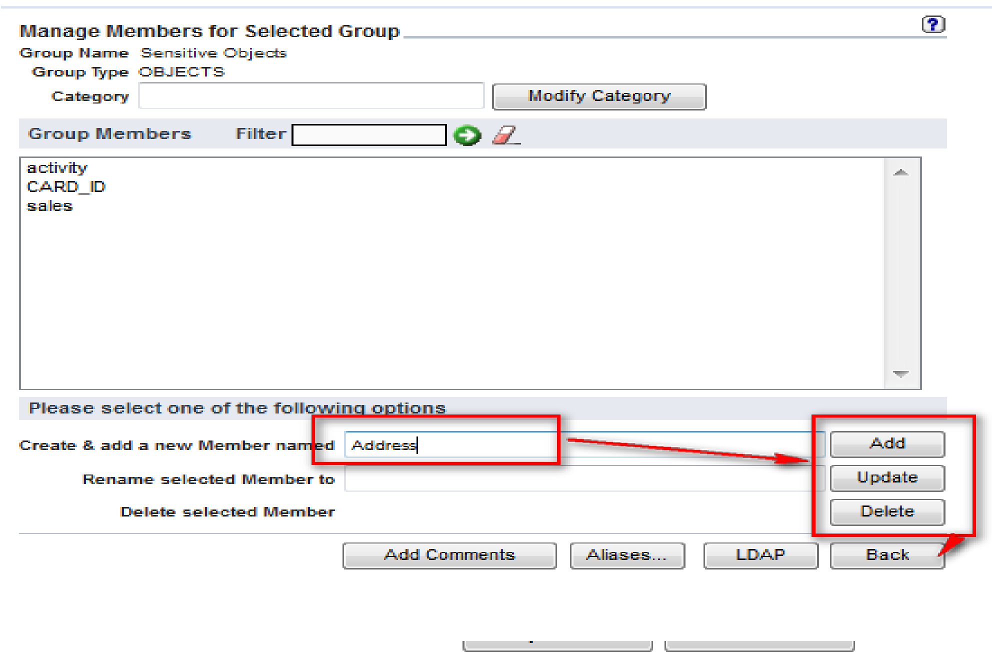


上方可修改現有的Group
下方可新增Group



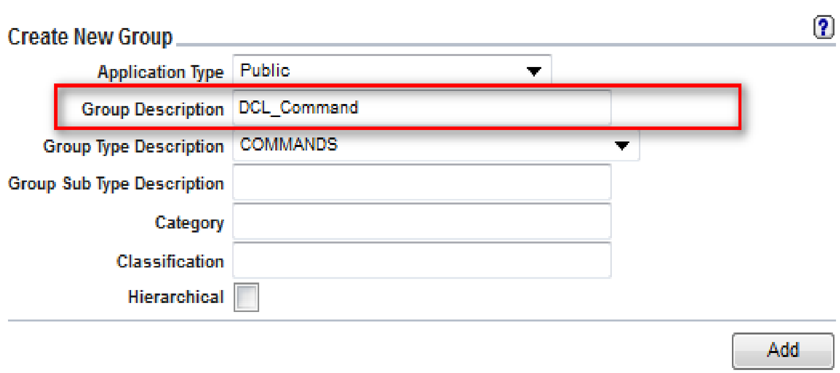
若要修改Sensitive Objects
清單選擇到Sensitive Objects
後選擇Modify

群組修改與新增（續）



將Sensitive Objects名稱輸入後選擇Add

將所有資料輸入後選Back離開



新增Group

如新增一屬於DCL Command 的群組

輸入Group名稱

Group Type 選擇此Group類型

選擇Add

再用Modify來增加內容

Q & A 問題與討論