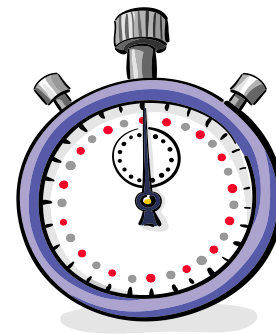


IBM Guardium 教育訓練 Guardium 操作介紹

泰鋒電腦 洪禮育

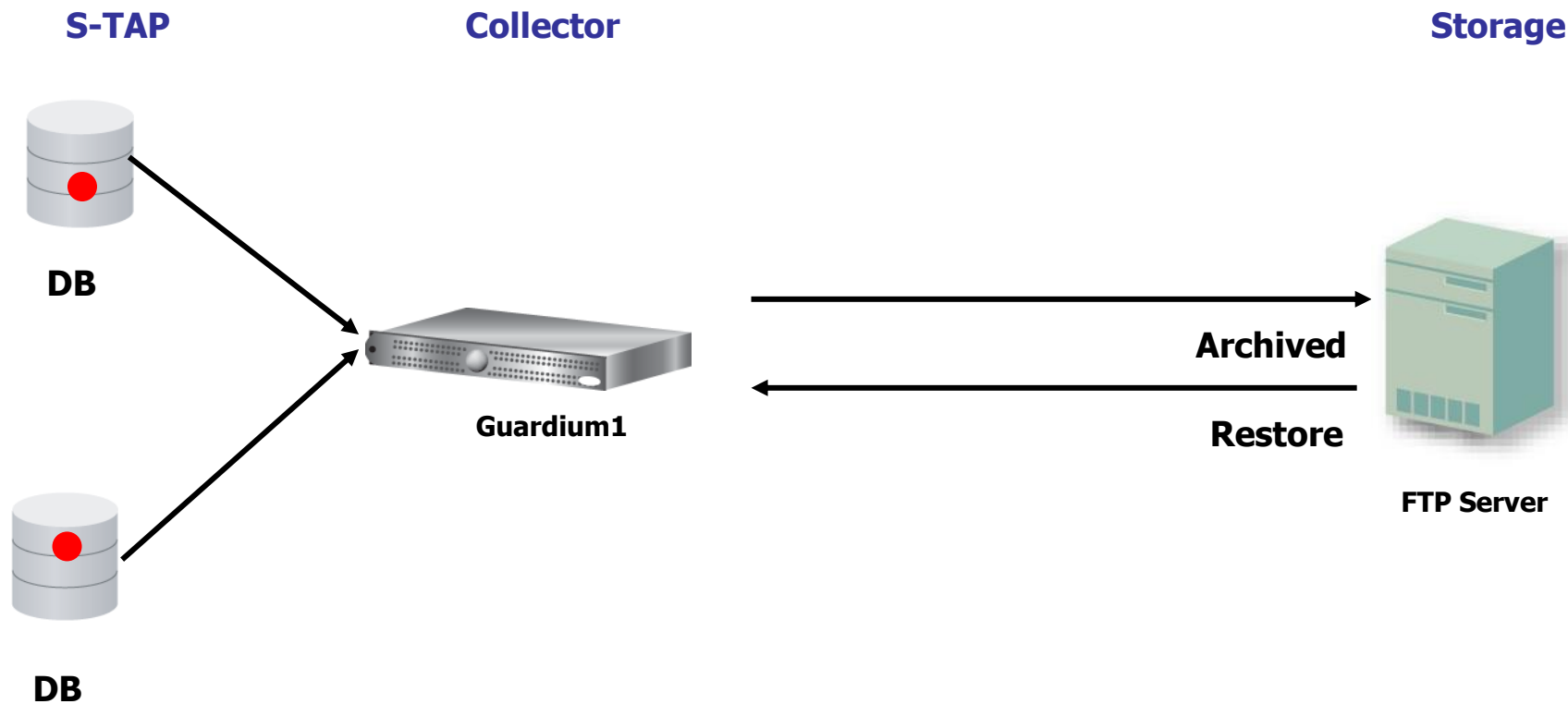
簡報綱要

- ❖ 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



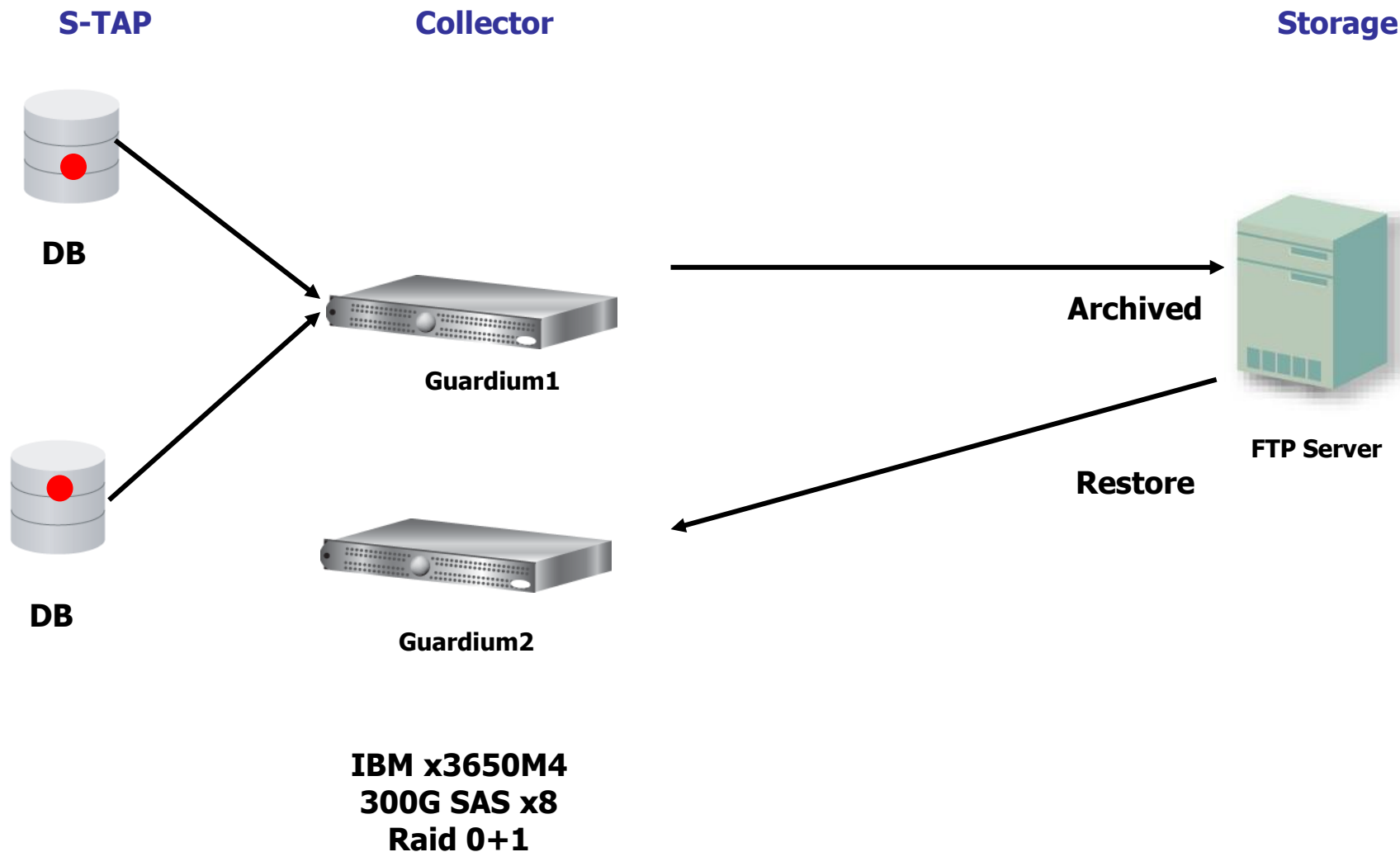
系統基本管理

基本Guardium 建置環境

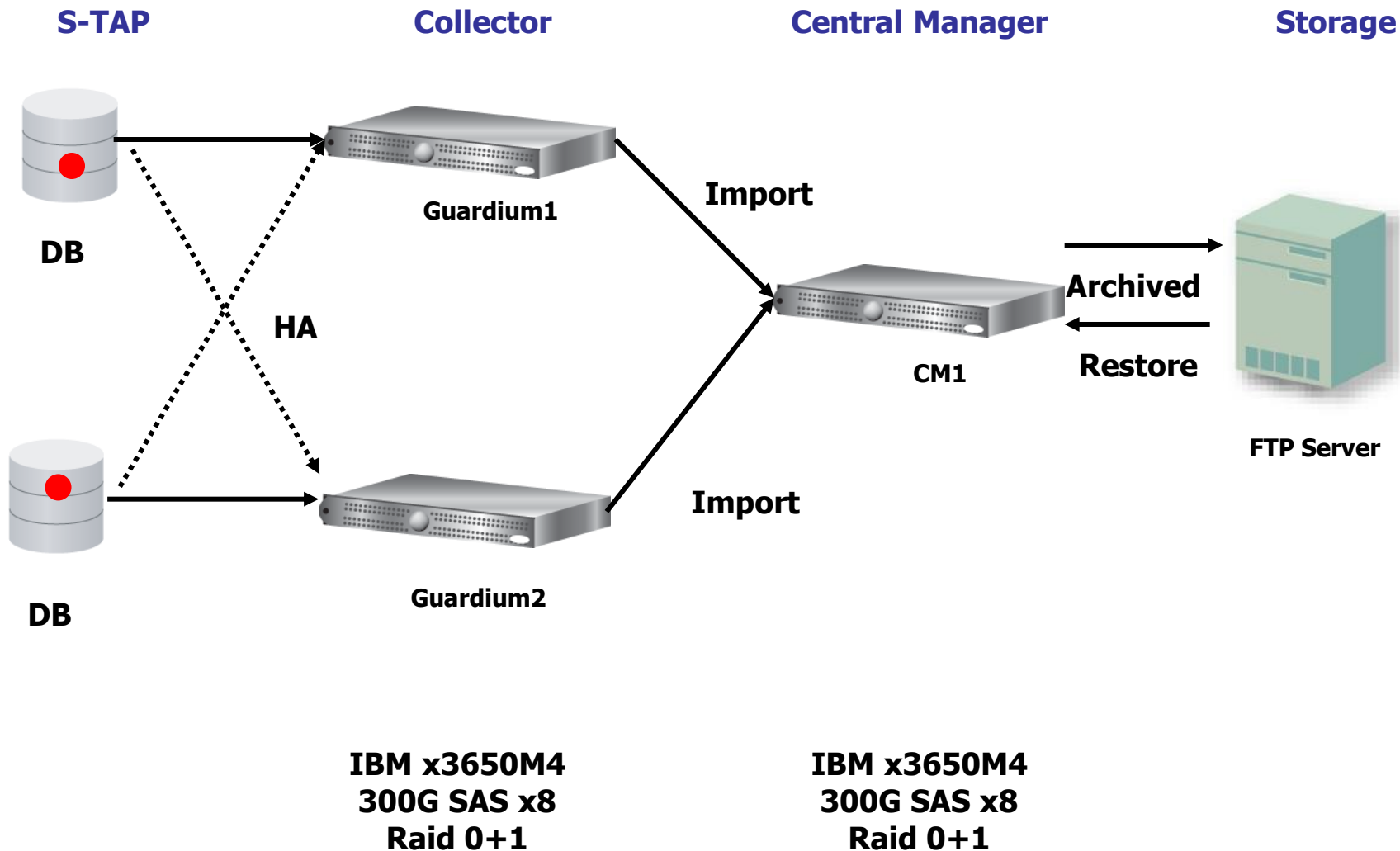


IBM x3650M4
300G SAS x8
Raid 0+1

較佳Guardium 建置環境



建議Guardium 建置環境



IBM x3650M4
300G SAS x8
Raid 0+1

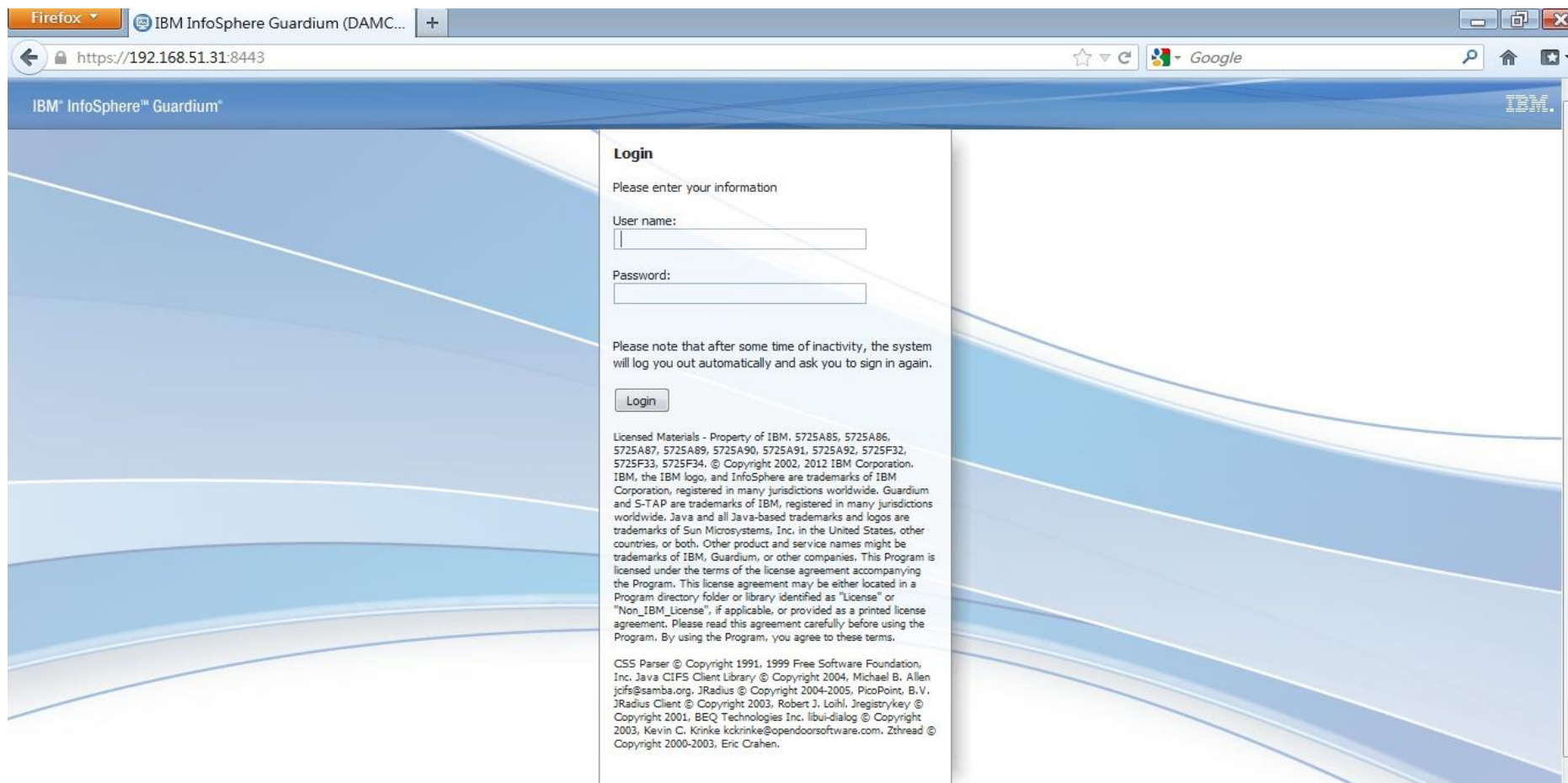
IBM x3650M4
300G SAS x8
Raid 0+1

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

The screenshot displays the IBM InfoSphere Guardium Collector interface. At the top, it shows the system name 'IBM InfoSphere™ Guardium' and the user 'admin'. Below the navigation tabs, the 'S-TAP Status Monitor' window is active, showing a table of 14 database instances. All instances are in an 'Active' state, indicated by green status cells. To the right, the 'Request Rate' window shows a line graph with a peak around 1:45 PM. Below that, the 'CPU Usage' window shows another line graph with multiple peaks. At the bottom, the 'Current Status Monitor' window displays a terminal-style output of system metrics.

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Instance Name	Primary Host Name	KTAP	TEF	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	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 14:19:10	DB2-0	192.168.51.31	Yes	No	No	No	Yes	No	Unencrypted	No		50000	50000

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(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

The screenshot displays the IBM InfoSphere Guardium Central Management interface. The top navigation bar includes 'System View', 'Administration Console', 'Tools', 'Daily Monitor', 'Guardium Monitor', 'Tap Monitor', 'Incident Management', and 'test NAT'. The 'Central Manager - Aggregator' window is highlighted in red.

S-TAP Status Monitor
 Using Merge Period Between 2013-01-14 and 2013-01-28.
 Aliases: OFF

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
Not an STAP UNIT																	

Current Status Monitor

```

procs-----memory-----swap-----io-----system-----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 104 1824048 154356 10489592 0 0 0 276 1036 288 0 0 99 1 0
    
```

Net Inspection → Analysis Engine (N/A) → S-TAP Inspection

SQL Server → Teradata → Oracle → MySQL → DB2 → XML → Sybase → IMS → Free Disk: 662 GB, DB 40% full

Request Rate
 Start Date: 2013-01-28 12:22:08 End Date: 2013-01-28 14:22:08
 Aliases: OFF

CPU Usage
 Start Date: 2013-01-28 12:22:08 End Date: 2013-01-28 14:22:08

Administration Console設定-Alerter

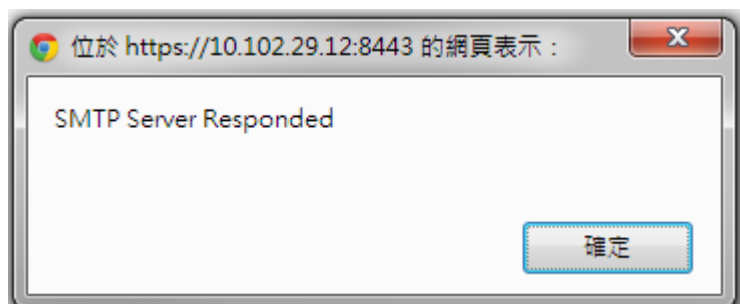
系統發出Alerter
的Mail相關設定

The screenshot shows the Administration Console interface with the Alerter configuration page selected. The left sidebar lists various configuration options, with 'Alerter' highlighted. The main panel displays the Alerter settings, including a checkbox for 'Active on startup', a 'Polling Interval (seconds)' field set to 60, and sections for SMTP and SNMP configurations. The SMTP section includes fields for IP Address/Host Name (10.102.29.201), Port (25), User Name (kevinhung), Password (masked), Re-enter password (masked), and Return Email Address (kevinhung@taifon.com.tw). The Authentication method is set to None. The SNMP section includes fields for IP Address/Host Name, 'Trap' Community, and Retype Community. At the bottom, there are buttons for Stop, Restart, and Apply.

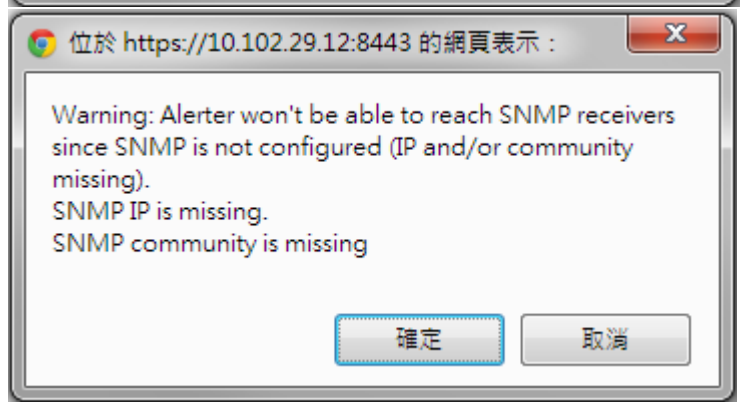
Section	Field	Value
General	Active on startup	<input checked="" type="checkbox"/>
	Polling Interval (seconds)	60
SMTP	IP Address/Host Name	10.102.29.201
	Port	25
	User Name	kevinhung
	Password
	Re-enter password
	Return Email Address	kevinhung@taifon.com.tw
Authentication method	None	
SNMP	IP Address/Host Name	
	"Trap" Community	
	Retype Community	

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

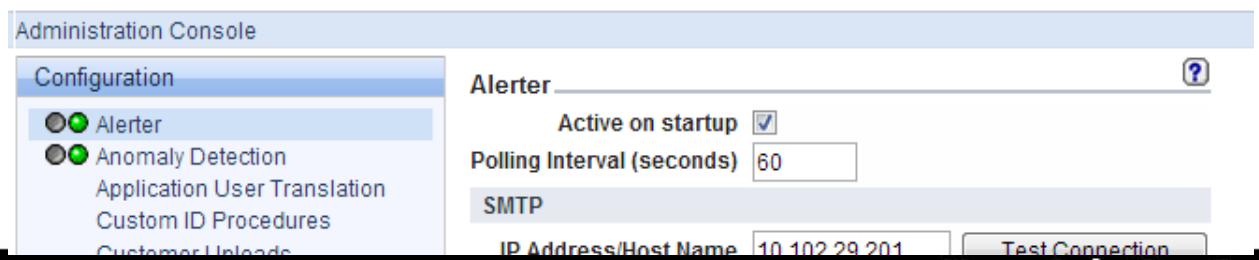
Test Connect For SMTP



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

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

Configuration

- Alerter
- Anomaly Detection
- Application User Translation
- Custom ID Procedures
- Flat Log Process
- Global Profile
- Guardium for z/OS
- Incident Generation
- Inspection Engines
- IP-to-Hostname Aliasing
- Policy Installation
- Portal
- Support Maintenance
- Session Inference
- System
- Upload Key File

Data Management

Central Management

Local Taps

Custom Classes

Module Installation

Inspection Engine Configuration

Default Capture Value	<input checked="" type="checkbox"/>	Default Mark Auto Commit	<input checked="" type="checkbox"/>
Log Request Sql String	<input checked="" type="checkbox"/>	Log Sequencing	<input checked="" type="checkbox"/>
Log Exception Sql String	<input checked="" type="checkbox"/>	Log Records Affected	<input checked="" type="checkbox"/>
Log timestamp per second	<input checked="" type="checkbox"/>	Compute Avg. Response Time	<input checked="" type="checkbox"/>
Inspect Returned Data	<input type="checkbox"/>	Record Empty Sessions	<input type="checkbox"/>
Parse XML	<input type="checkbox"/>		
Logging Granularity	60	Max. Hits per Returned Data	64
Ignored Ports List	<input type="text"/>		
Buffer Free	100 %		

Restart Inspection Engines Add Comments Apply

+ Add Inspection Engine...

Administration Console設定- Portal

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

The screenshot displays the IBM InfoSphere Guardium Administration Console interface. The top navigation bar includes tabs for System View, Administration Console (selected), Tools, Daily Monitor, Guardium Monitor, Tap Monitor, and Incident Management. The main content area is titled "Administration Console" and features a left-hand navigation menu with categories like Configuration, Data Management, Central Management, Local Taps, Custom Classes, and Module Installation. The "Configuration" section is expanded, showing various settings such as Alerter, Anomaly Detection, and Portal. The "Guardium Portal" configuration page is active, showing the "Active on startup" checkbox checked and the "HTTPS Port (1025-65535)" set to 8443. Below this, there are buttons for Restart, Revert, and Apply. The "Authentication Configuration" section is also visible, with radio buttons for Local (selected), RADIUS, and LDAP, and buttons for Test and Apply.

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

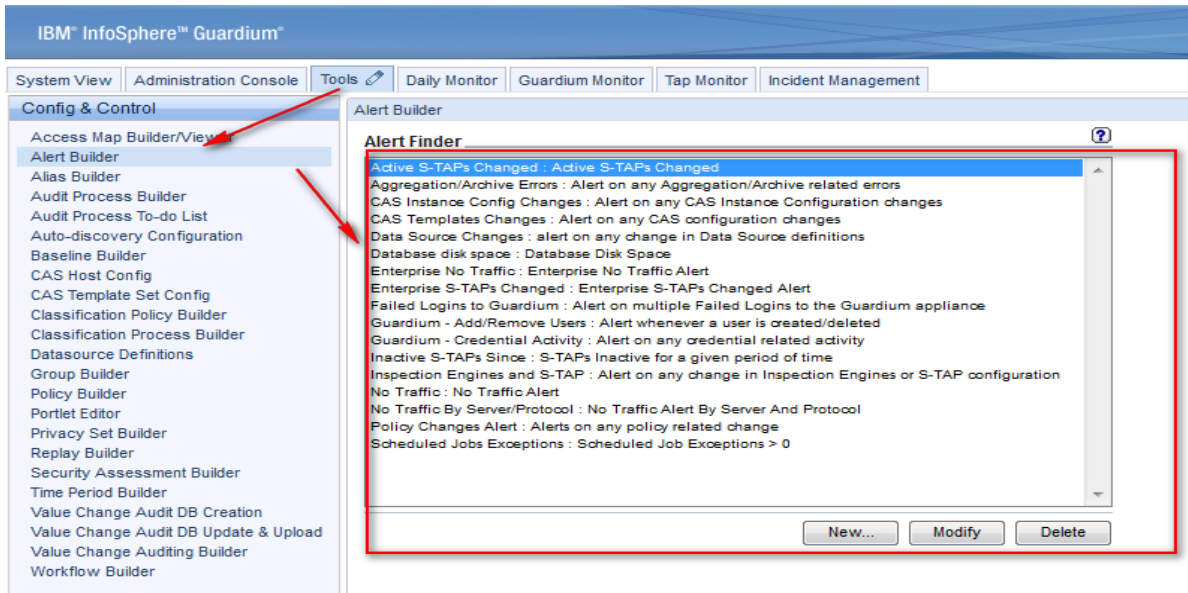
System Shared Secret:各主機需設定相同, CM, 資料還原, Export, Import會用到, 若不相同將影響該功能

The screenshot displays the Administration Console interface with the following configuration details:

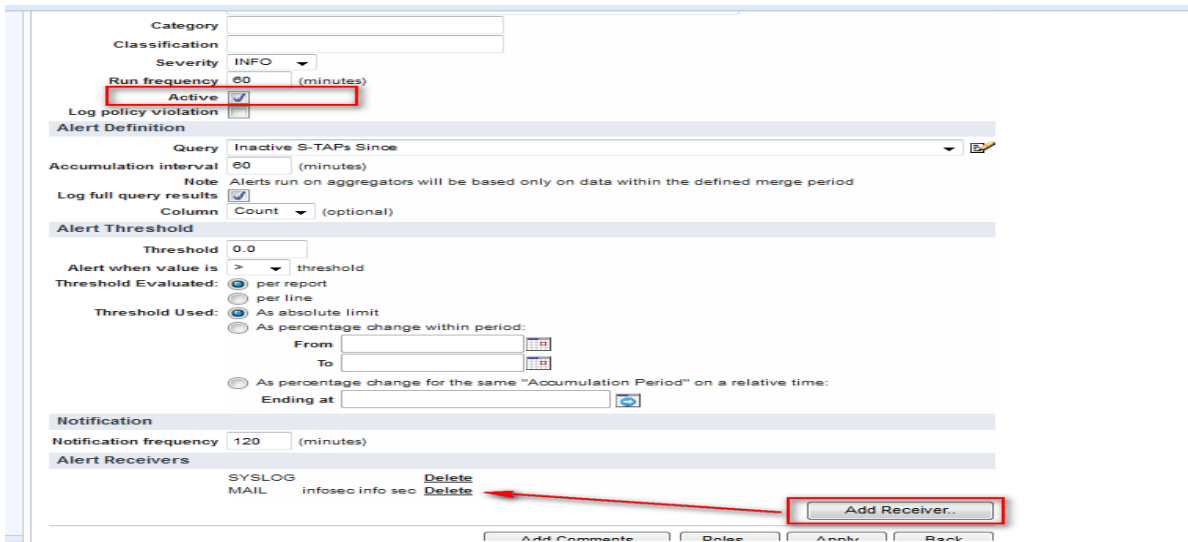
- System Configuration:**
 - Unique global identifier: 186780210
 - System Shared Secret** (highlighted)
 - Retype Secret
 - Number of datasources: -1
 - Metered scans left: -1
 - License valid until: 2099-01-01 00:00:00
 - # of Licenses: 9999
- Network Address:**
 - System Hostname: DAMC01P
 - Domain: vghks.gov.tw
 - System IP Address: 192.168.51.31
 - SubNet Mask: 255.255.255.0
 - Hardware (MAC) Address: 6C:AE:8B:22:0A:32
- Secondary Management Interface:**
 - System IP Address
 - SubNet Mask
- Routing:**
 - Default Route: 192.168.51.254
 - Secondary Route
- DNS:**
 - Primary Resolver: 192.168.97.1 (Test Connection)
 - Secondary Resolver: 192.168.197.1 (Test Connection)
 - Tertiary Resolver (Test Connection)

Buttons at the bottom: Stop, Restart, Apply.

Guardium 系統警示

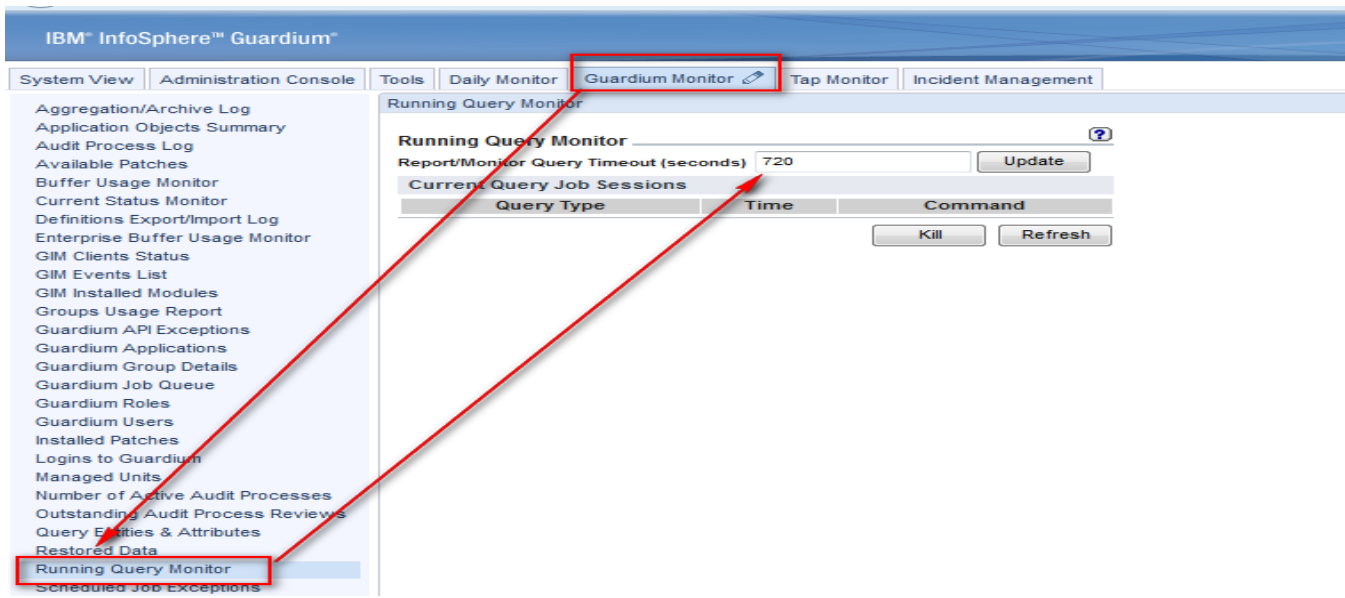


Guardium已內建17種系統異常警示，建議啟動備份異常，STAP異常，Guardium DB空間3個Alert

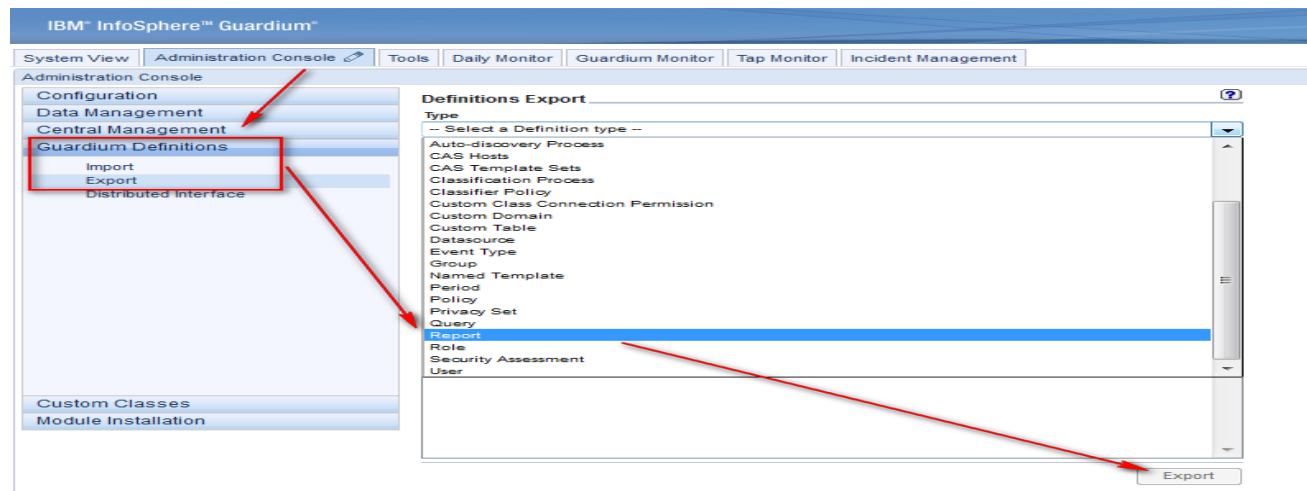


點選進入後，僅要點選Active，與加上Add Receiver，選擇mail，再選收件使用者，其它用預設值即可

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

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

Configuration

Data Management

- Data Archive
- Data Export
 - Data Restore
 - Catalog Archive
 - Catalog Export
 - Catalog Import
 - Patch Backup
- Results Archive (audit)
- Results Export (files)
- System Backup

Central Management

Local Taps

Guardium Definitions

Custom Classes

Module Installation

Data Archive

Configuration

Archive

Archive data older than Day(s)

Ignore data older than Day(s) (optional)

Archive Values

Protocols SCP FTP

Host

Directory

Port

Username

Password

Re-enter password

Purge

Purge data older than Day(s)

Allow purge without exporting or archiving

Scheduling

Data Archive is actively scheduled.

Data Archive : Schedule

Scheduling

●● Data Archive is actively scheduled.

Modify Schedule... Pause Run Once Now



System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

- Configuration
- Data Management
 - Data Archive
 - Data Export
 - Data Restore
 - Catalog Archive
 - Catalog Export
 - Catalog Import
 - Patch Backup
 - Results Archive (audit)
 - Results Export (files)
 - System Backup

Schedule Definition

Start Time 1 a.m. : 00

Restart Run only once

Repeat Do not repeat within the hour

Schedule by... Day/Week

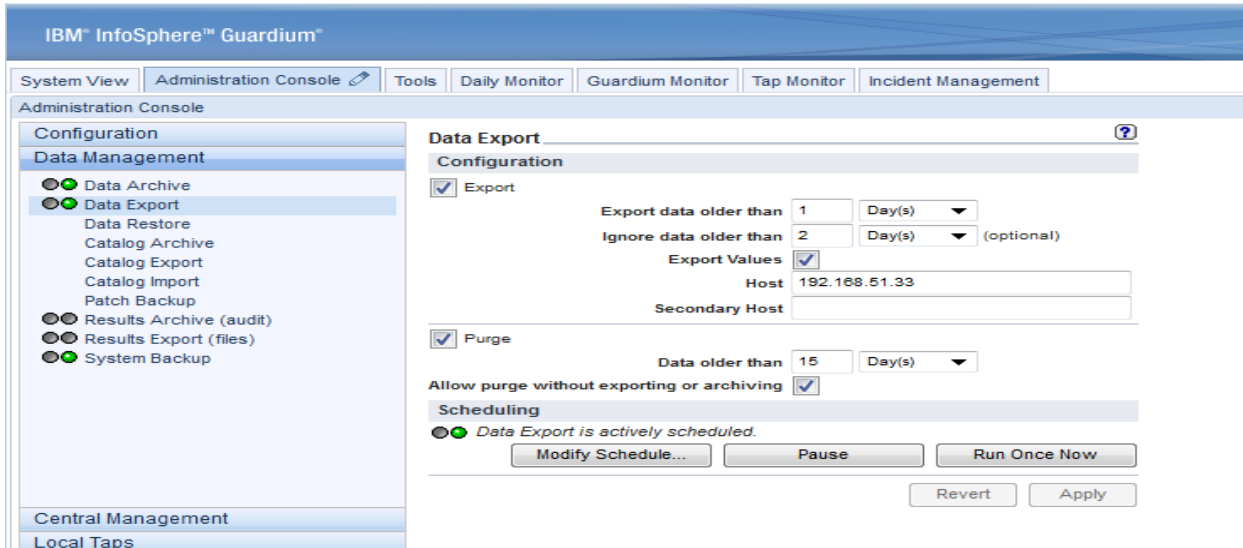
Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Every day

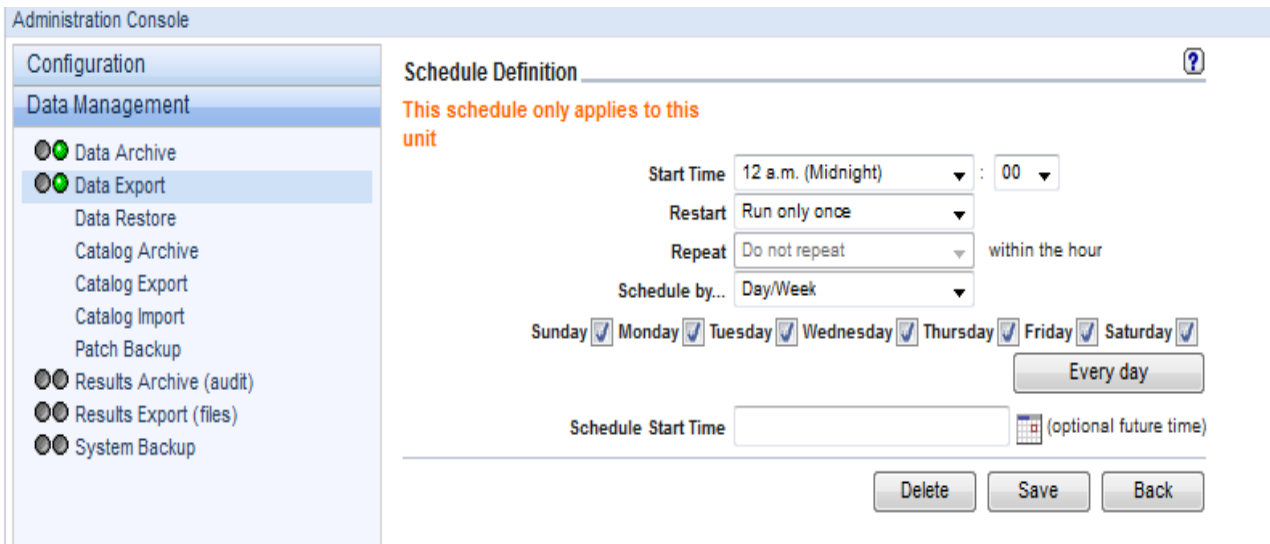
Schedule Start Time (optional future time)

Delete Save Back

Export (Collector -> CM)

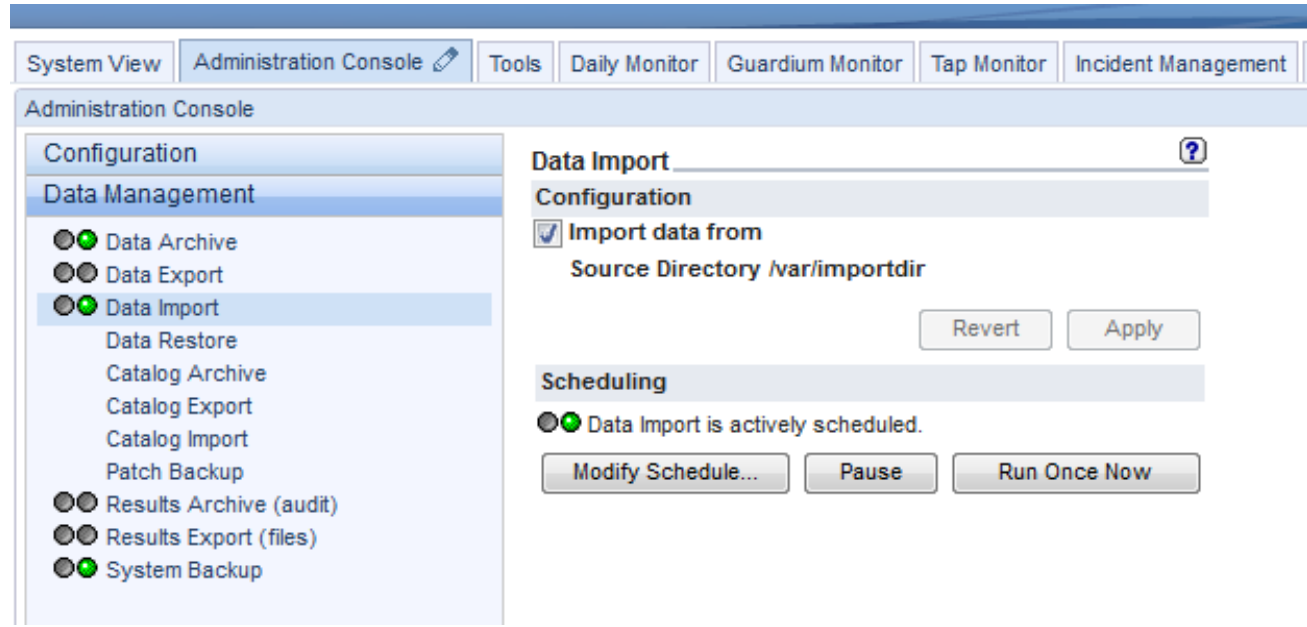


每天匯出資料至
CM主機上, 並刪
除15天(31主機)
與20天(32主機)
前資料

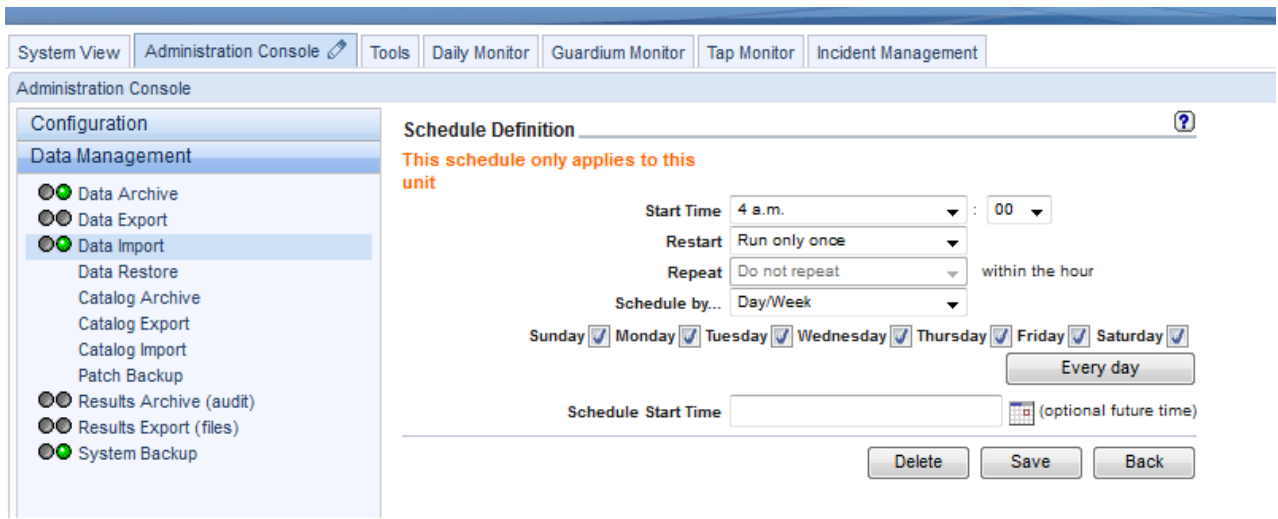


每天清晨12:00
執行

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)

IBM InfoSphere™ Guardium™

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

Configuration

Data Management

- Data Archive
- Data Export
- Data Import
- Data Restore
- Catalog Archive
- Catalog Export
- Catalog Import
- Patch Backup
- Results Archive (audit)
- Results Export (files)
- System Backup

Central Management

Guardium Definitions

Custom Classes

Module Installation

Data Archive

Configuration

Archive

Archive data older than 1 Day(s)

Ignore data older than 2 Day(s) (optional)

Archive Values

Protocols SCP FTP

Host 192.168.226.19

Directory \

Port 21

Username apdam01

Password

Re-enter password

Purge

Purge data older than 20 Day(s)

Allow purge without exporting or archiving

Scheduling

Data Archive is actively scheduled.

Modify Schedule... Pause Run Once Now

Revert Apply

CM主機每天將資料備份到FTP Server上, 並刪除20天前資料

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

Configuration

Data Management

- Data Archive
- Data Export
- Data Import
- Data Restore
- Catalog Archive
- Catalog Export
- Catalog Import
- Patch Backup
- Results Archive (audit)
- Results Export (files)
- System Backup

Schedule Definition

This schedule only applies to this unit

Start Time 5 a.m. : 00

Restart Run only once

Repeat Do not repeat within the hour

Schedule by... Day/Week

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Every day

Schedule Start Time (optional future time)

Delete Save Back

每天清晨5:00執行

System Backup (系統設定備份)

The screenshot shows the 'System Backup' configuration page. On the left is a navigation tree with 'System Backup' selected. The main area is divided into 'Configuration' and 'Scheduling' sections.

Configuration:

- Protocols: SCP FTP
- Host: 192.168.225.59
- Directory: /dam
- Port: 21
- Username: apdam01
- Password: [Empty]
- Re-enter password: [Empty]
- Backup: Configuration Data

Scheduling:

- System Backup is actively scheduled.
- Buttons: Modify Schedule..., Pause, Run Once Now, Revert, Apply

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

The screenshot shows the 'Schedule Definition' page. It includes a warning message and configuration options for the backup schedule.

Schedule Definition:

- Warning: This schedule only applies to this unit
- Start Time: 12 p.m. (Noon) : 00
- Restart: Run only once
- Repeat: Do not repeat within the hour
- Schedule by: Day/Week
- Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday
 - Every day
- Schedule Start Time: [Empty] (optional future time)
- Buttons: Delete, Save, Back

每週日中午
12:00執行

Policy管理

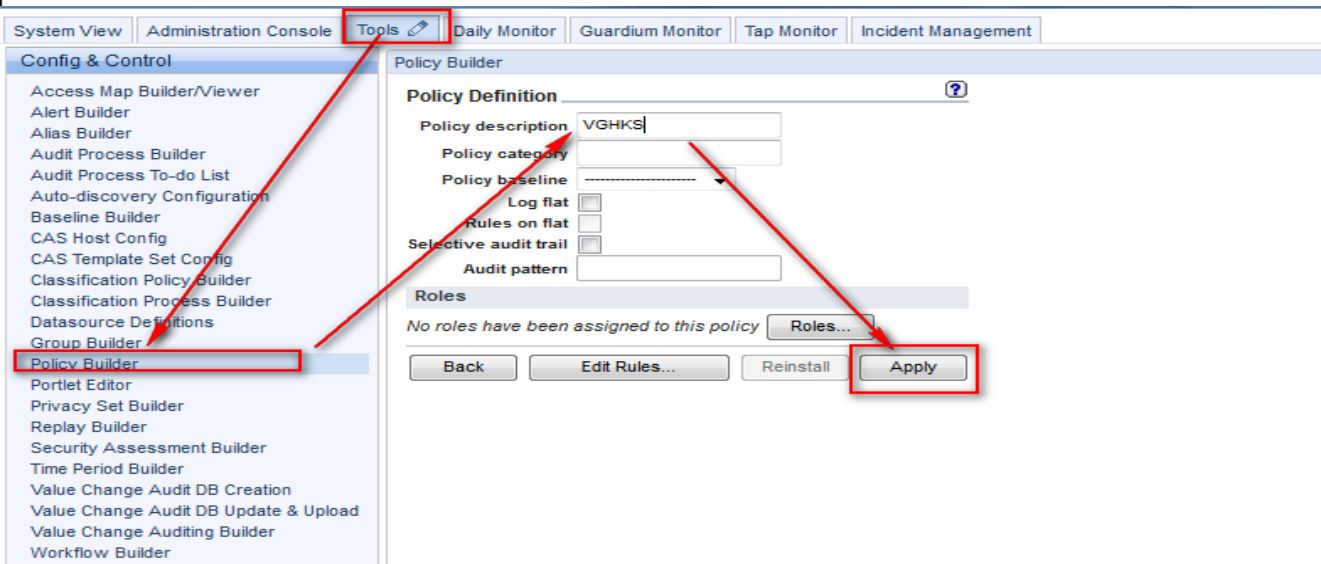
Guardium Policy制定

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.

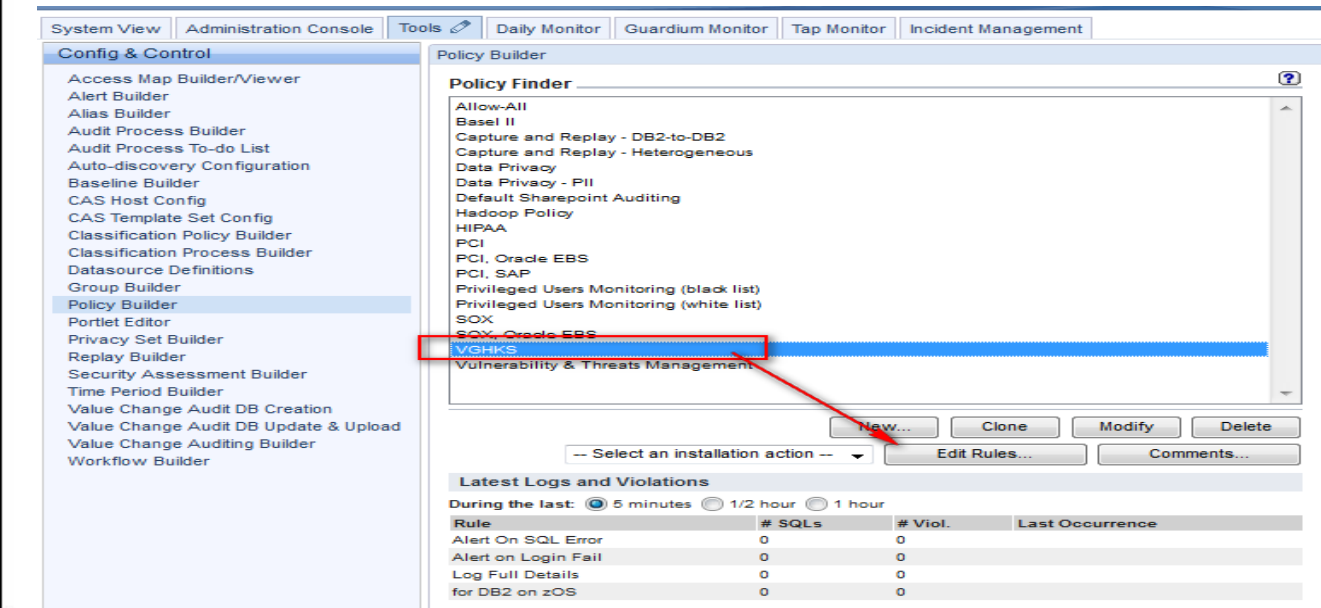
若有CM主機,相關Policy建議於CM主機上制定再派送至Collector

The screenshot displays the Guardium Policy Builder web interface. At the top, there are navigation tabs: System View, Administration Console, Tools, Daily Monitor, Guardium Monitor, Tap Monitor, and Incident Management. The right side of the header shows 'G5000 - C'. The left sidebar, titled 'Config & Control', lists various tools, with 'Policy Builder' highlighted. The main content area, titled 'Policy Builder', features a 'Policy Finder' search box and a list of policies. The 'Allow-All' policy is currently selected. Below the list, there are several action buttons: 'New...', 'Clone', 'Modify', 'Delete', 'Edit Rules...', and 'Comments...'.

Guardium Policy 名稱



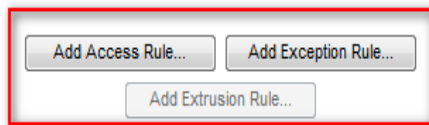
由Tools -> Policy Builder -> New 進入 Policy Definition 新增VGHKS名稱之 Policy



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



Rule Suggestion

Suggest from DB

Rule min. ct. 0

Object Group min. ct. 1

Suggest Rules

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Config & Control Policy Builder

Access Map Builder/Viewer
Alert Builder
Alias Builder
Audit Process Builder
Audit Process To-do List
Auto-discovery Configuration
Baseline Builder
CAS Host Config
CAS Template Set Config
Classification Policy Builder
Classification Process Builder
Datasource Definitions
Group Builder
Policy Builder
Portlet Editor
Privacy Set Builder
Replay Builder
Security Assessment Builder
Time Period Builder
Value Change Audit DB Creation
Value Change Audit DB Update & Upload
Value Change Auditing Builder
Workflow Builder

Policy Rules

VGHKS Filter: [dropdown] [edit] [delete] [refresh]

Expand All Collapse All Select All Unselect All Delete Selected Copy Rules ...

- 1 Access Rule: DB2 on zOS 1 - for DSNP (Installed)
- 2 Access Rule: DB2 on zOS 2 - for DSMT
- 3 Access Rule: Log Full Details (Installed)
- 4 Exception Rule: Alert on Login Fail (Installed)
- 5 Exception Rule: Alert On SQL Error (Installed)

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)

Access Rule Definition ?

Rule #3 of policy VGHKS

Description

Category Classification Severity

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prtcl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User and/or Group

Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Field and/or Group Every

Not Object and/or Group Every

Not Command and/or Group Every

Not Object/Cmd. Group

Not Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern (RE) Replacement Character

Time Period

Minimum Count Reset Interval minutes Trigger Once Per Session

Quarantine for minutes Records Affected Threshold Rec. Vals. Cont. to next rule

Actions

Log Full Details 不設任何條件, 全都錄至主機

Object/Cmd. Group

Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern (RE) Replacement Character

Time Period

Minimum Count Reset Interval minutes

Quarantine for minutes Records Affected Threshold Rec. Vals. Cont. to next rule

Actions

LOG FULL DETAILS

Action

Guardium Policy Rule制定 (續)

Policy Builder

Exception Rule Definition ?

Rule #4 of policy VGHKS

Description Alert on Login Fail

Category Classification Severity INFO

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prctl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB User and/or Group

Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Error Code and/or Group

Not Excpt. Type LOGIN_FAILED

Data Pattern RE Replacement Character *

Time Period

Minimum Count 0 Reset Interval 0 minutes

Quarantine for 0 minutes Rec. Vals. Cont. to next rule

Actions

ALERT PER MATCH

Add Action

Back Add Comments Save

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

Actions

ALERT PER MATCH

Action ALERT PER MATCH

Message Template Default

Notification

Notification Type SYSLOG Alert Receiver SYSLOG

Notification Type SYSLOG

Alert Receiver SYSLOG

Add

Apply

Add Action

Back Add Comments Save

Guardium Policy Rule制定 (續)

Exception Rule Definition [?](#)

Rule #5 of policy VGHKS

Description Alert On SQL Error

Category Classification Severity INFO

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prtol. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User and/or Group

Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Error Code and/or Group

Not Excpt. Type SQL_ERROR

Masking Pattern Replacement Character

Time Period

Minimum Count 0 Reset Interval 0 minutes

Quarantine for 0 minutes Rec. Vals. Cont. to next rule

Actions

ALERT PER MATCH

Add Action

Back Add Comments Save

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

Actions

ALERT PER MATCH

Action ALERT PER MATCH

Message Template Default

Notification

Notification Type SYSLOG Alert Receiver SYSLOG

Notification Type SYSLOG

Alert Receiver SYSLOG

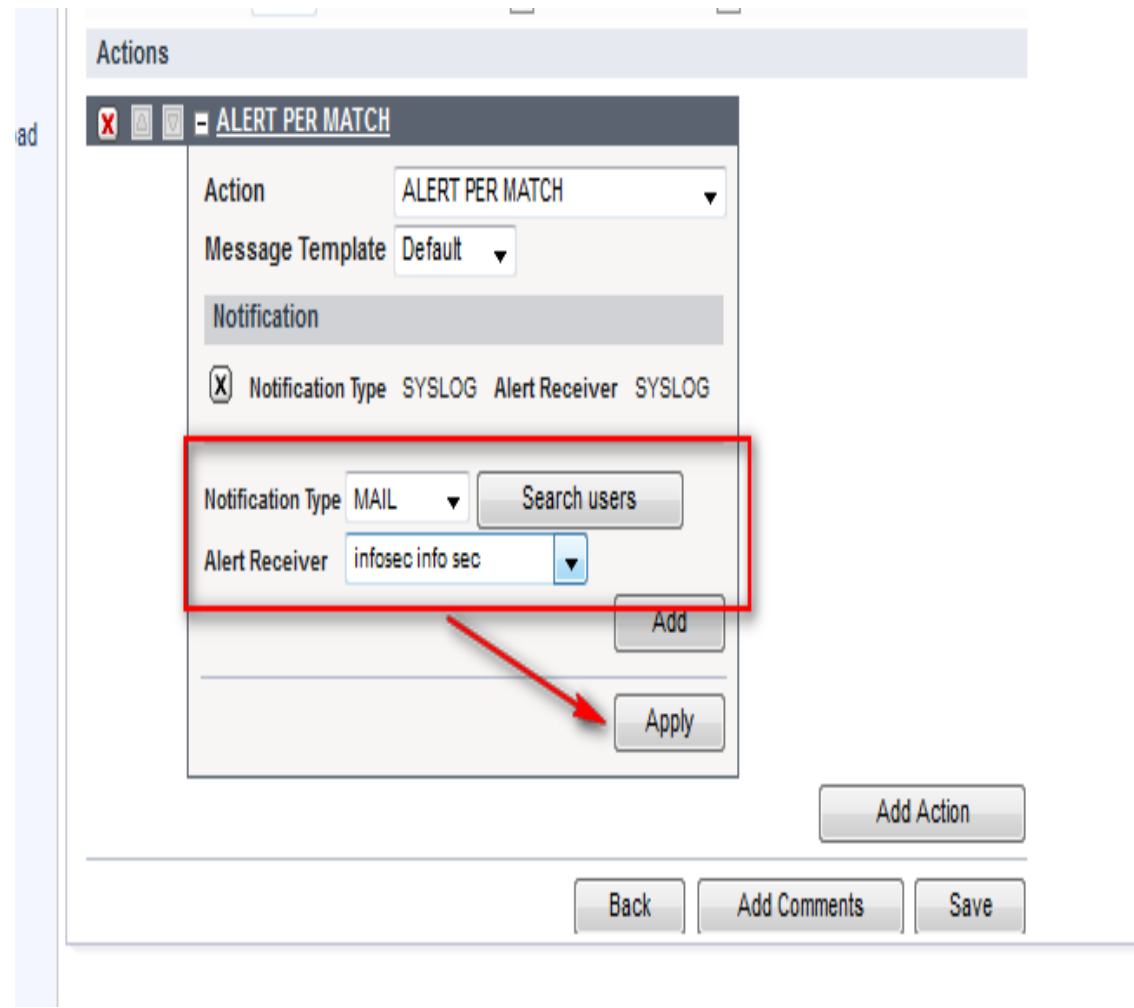
Add

Apply

Add Action

Back Add Comments Save

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

Custom ID Procedures
Flat Log Process
Global Profile
Guardium for z/OS
Incident Generation
Inspection Engines
IP-to-Hostname Aliasing
Policy Installation
Portal
Support Maintenance
Session Inference
System
Upload Key File

Data Management
Central Management
Local Taps
Custom Classes
Module Installation

Policy Installer

Capture and Replay - DB2-to-DB2
Capture and Replay - Heterogeneous
Data Privacy
Data Privacy - PII
Default Sharepoint Auditing
Hadoop Policy
HIPAA
PCI
PCI, Oracle EBS
PCI, SAP
Privileged Users Monitoring (black list)
Privileged Users Monitoring (white list)
SOX
SOX, Oracle EBS
VGHKS
Vulnerability & Threats Management

Installed Rules 5
Baseline records 0

Edit Installed Policy

View Details Report

-- Select an installation action --
Add Comments

-- Select an installation action --
Install & Override
Install before policy: VGHKS
Install last

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

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Administration Console

Configuration
Alerter
Anomaly Detection
Application User Translation
Custom ID Procedures
Flat Log Process
Global Profile
Guardium for z/OS
Incident Generation
Inspection Engines
IP-to-Hostname Aliasing
Policy Installation
Portal
Support Maintenance
Session Inference
System
Upload Key File

Data Management
Central Management
Local Taps
Custom Classes

Currently Installed Policies

Installed Policy #1

Installed Policy VGHKS
Date Installed 1/23/13 11:11 AM
This is not a selective audit policy
Not logging to flat
Rules don't fire on flat
Installed Rules 5
Baseline records 0

Edit Installed Policy

View Details Report

Policy Installer

中央控管機制

Central Management 管理 (CM主機)

IBM® InfoSphere™ Guardium™ 17:17 | Edit Account: admin | Customize | Logout | About

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Central Manager -

Administration Console

Configuration
Data Management
Central Management
Central Management
Portal User Sync.

Central Management

Groups	Unit	Insp. Engines	Installed Policy	Unit Type	Ver.	Last Patch	Last Ping
All Units (2)	DAMC01P vghks.gov.tw	Show	VGHKS	Managed, Collector	9.0	2	1/28/13 5:15 PM
	DAMC02P vghks.gov.tw	Show	VGHKS	Managed, Collector	9.0	2	1/28/13 5:15 PM

Selected Units

Group Setup Unregister

Restarting

Reboot Restart Portal Restart Inspection Engines

Distribution

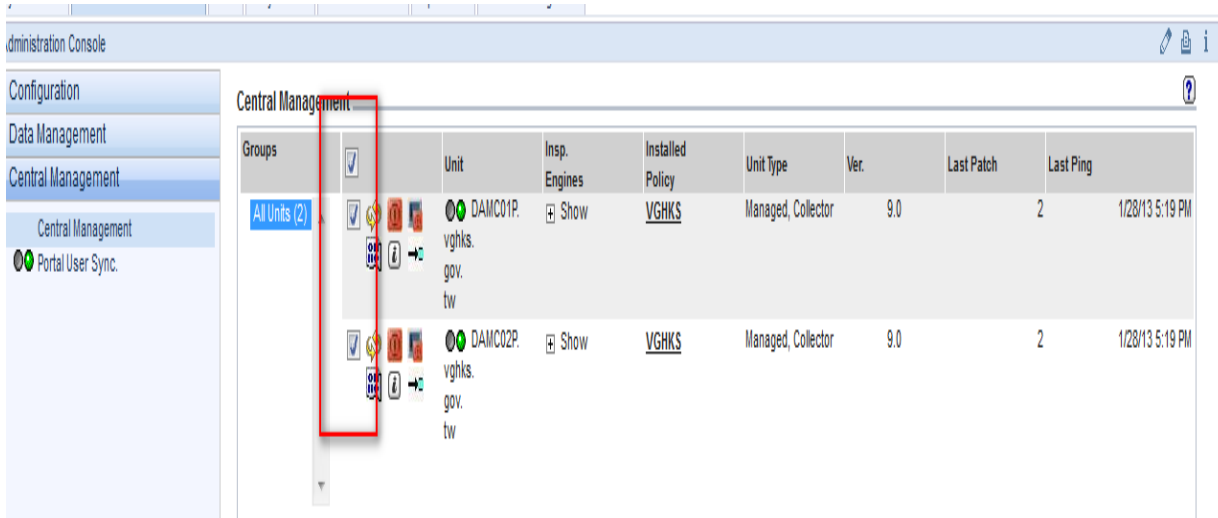
Refresh Install Policy Patch Distribution
Distribute Uploaded Jar Files
Distribute Patch Backup Settings Distribute Authentication Config
Distribute Configurations

Register New... Patch Installation Status Show Distributed Map
Distributed Monitor

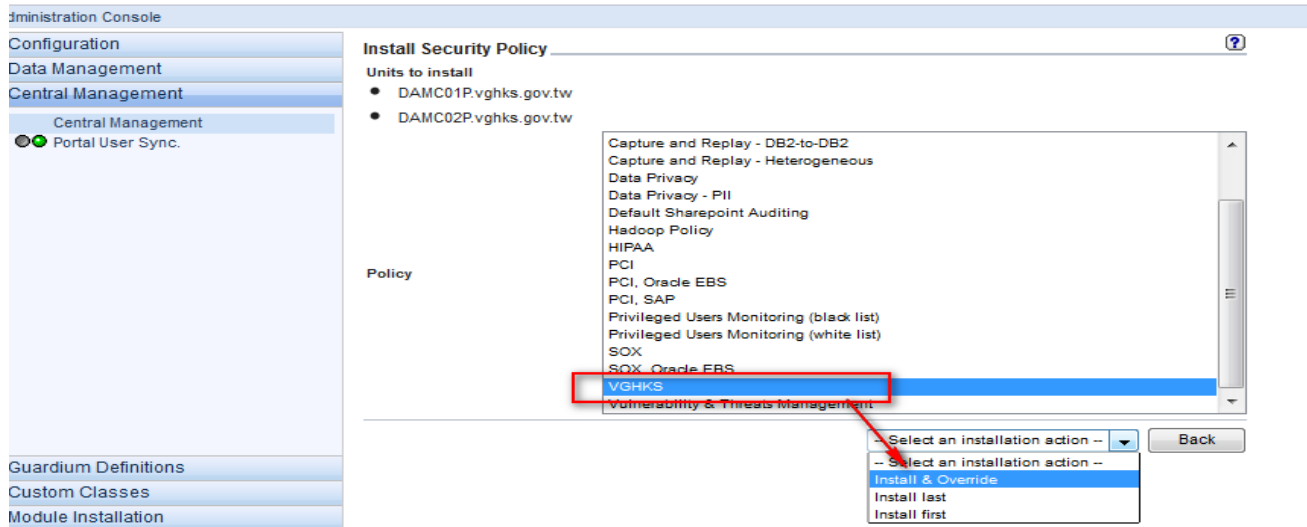
CM目前管理2台
Collector主機

可點選要管理的主
機來重開機, 安裝
Policy , Patch檔等
功能

Central Management 統一派送Policy (CM主機)

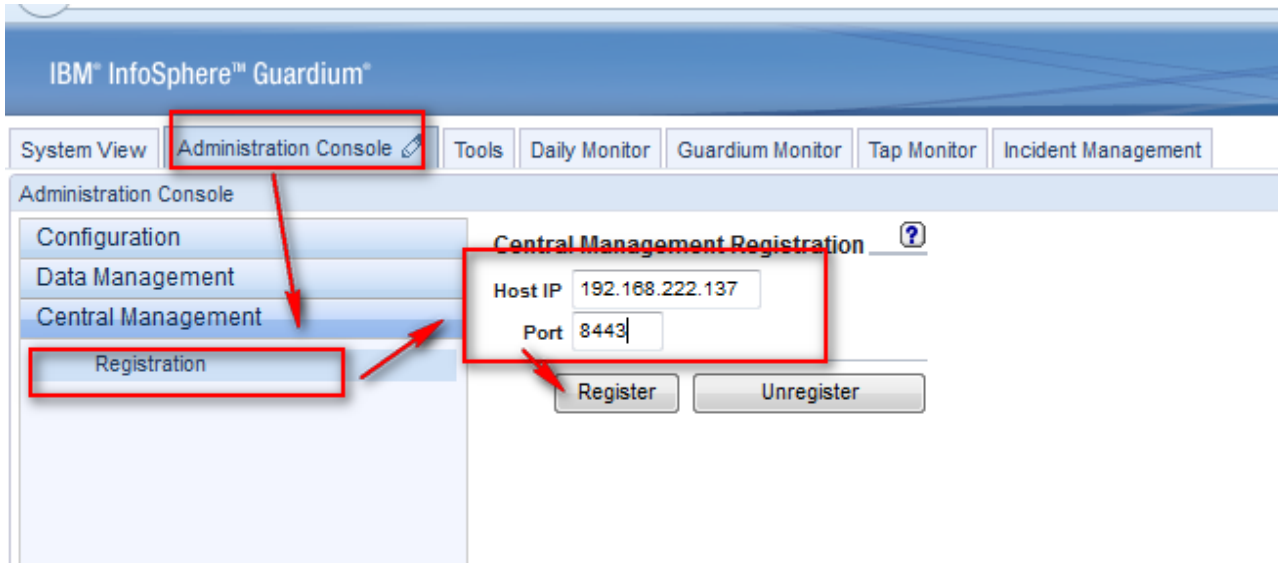


點選要控管的
Collector主機
選Install Policy

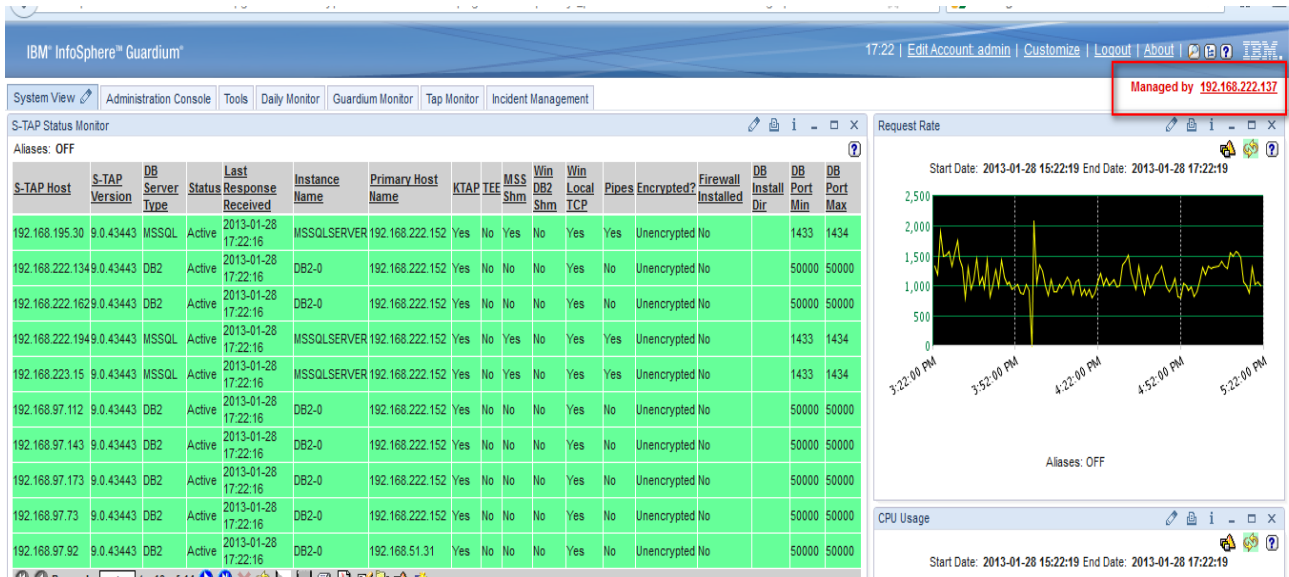


選取要Install
Policy後選
Install&Override

Collector加入Central Management控管 (Collector)



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



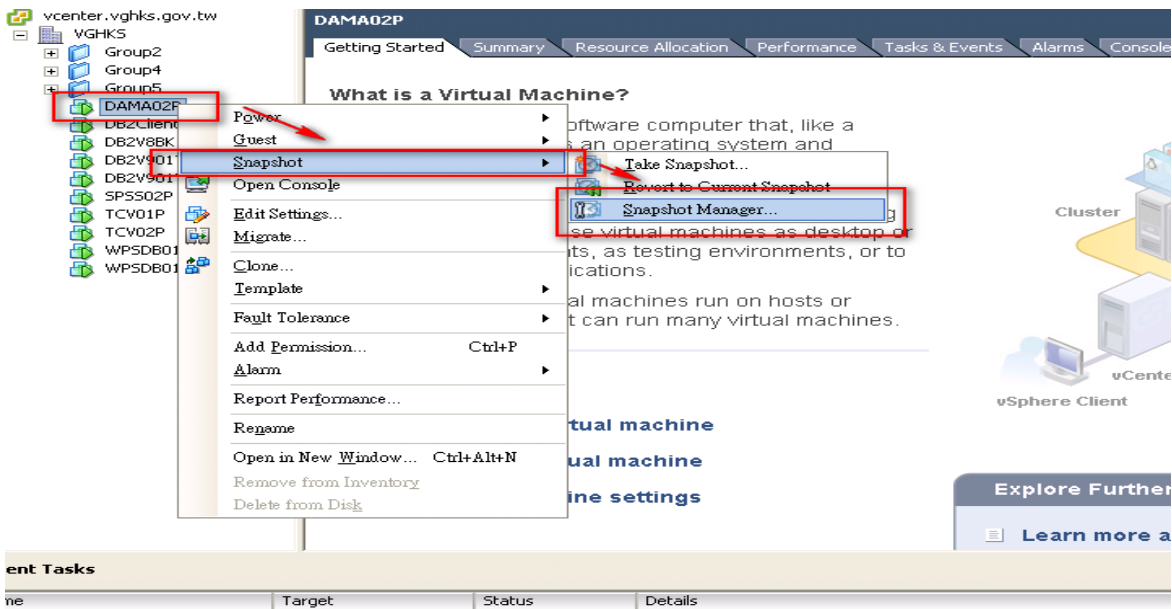
加入後, 重新登錄主機於右上方會出現目前CM主機IP, 成功加入

資料還原

Central Management 上資料還原

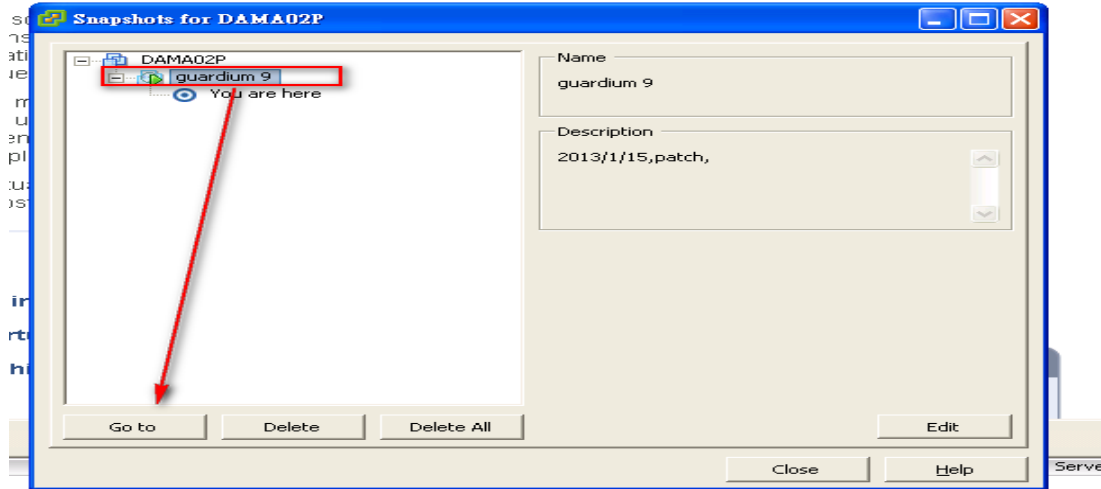
名稱	修改日期	類型	大小
735247-DAMA01P.vghks.gov.tw-w201...	2013/1/15 上午 0...	ENC 檔案	1,979,923 KB
735246-DAMA01P.vghks.gov.tw-w201...	2013/1/14 上午 0...	ENC 檔案	1,231,712 KB
2013-01-13-1200-DAMC01P.vghks.go...	2013/1/13 下午 1...	tgz Archive	7,275 KB
2013-01-13-1200-DAMA01P.vghks.go...	2013/1/13 下午 1...	tgz Archive	6,299 KB
2013-01-13-1200-DAMC02P.vghks.go...	2013/1/13 下午 1...	tgz Archive	7,109 KB
735245-DAMA01P.vghks.gov.tw-w201...	2013/1/13 上午 0...	ENC 檔案	1,427,388 KB
735244-DAMA01P.vghks.gov.tw-w201...	2013/1/12 上午 0...	ENC 檔案	2,112,844 KB
735243-DAMA01P.vghks.gov.tw-w201...	2013/1/11 上午 0...	ENC 檔案	2,189,568 KB
735242-DAMA01P.vghks.gov.tw-w201...	2013/1/10 上午 0...	ENC 檔案	2,076,177 KB
735241-DAMA01P.vghks.gov.tw-w201...	2013/1/9 上午 05...	ENC 檔案	2,486,024 KB
735240-DAMA01P.vghks.gov.tw-w201...	2013/1/8 上午 05...	ENC 檔案	2,564,321 KB
735239-DAMA01P.vghks.gov.tw-w201...	2013/1/7 上午 05...	ENC 檔案	1,740,435 KB
2013-01-06-1200-DAMC01P.vghks.go...	2013/1/6 下午 12...	tgz Archive	7,261 KB
2013-01-06-1200-DAMC02P.vghks.go...	2013/1/6 下午 12...	tgz Archive	6,989 KB
2013-01-06-1200-DAMA01P.vghks.go...	2013/1/6 下午 12...	tgz Archive	6,041 KB
735238-DAMA01P.vghks.gov.tw-w201...	2013/1/6 上午 05...	ENC 檔案	1,365,531 KB
735237-DAMA01P.vghks.gov.tw-w201...	2013/1/5 上午 05...	ENC 檔案	2,198,466 KB
735236-DAMA01P.vghks.gov.tw-w201...	2013/1/4 上午 05...	ENC 檔案	2,495,114 KB

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

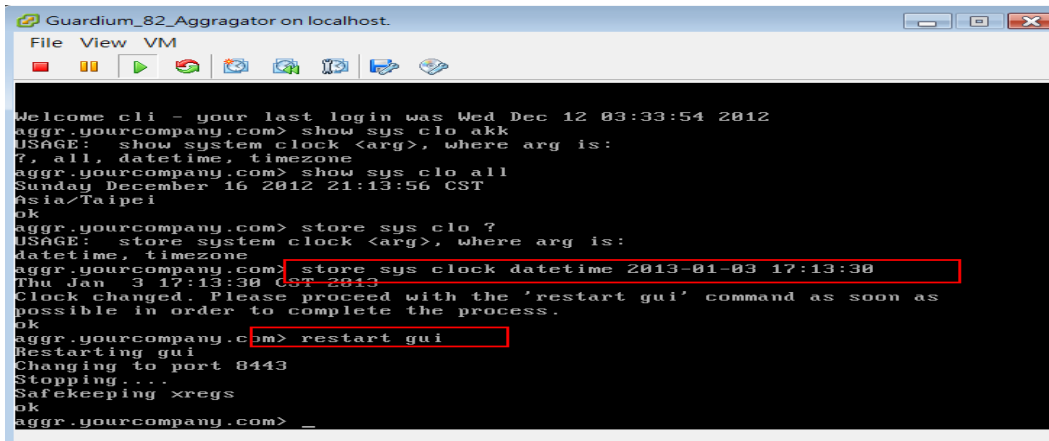


已另建還原專用機
 192.168.222.138是於VM上，目前也做好一Snapshot為初始完整安裝，日後有還原過資料，可使其再回覆到時間點。連到DAMA02P主機機，選取該內的Snapshot功能

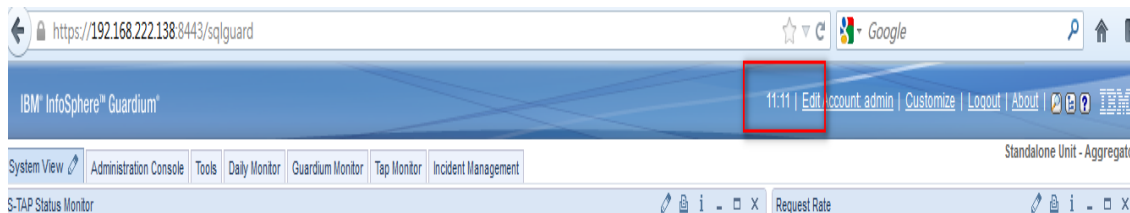
Central Management 上資料還原 (續)



選取Guardium 9此snapshot來還原

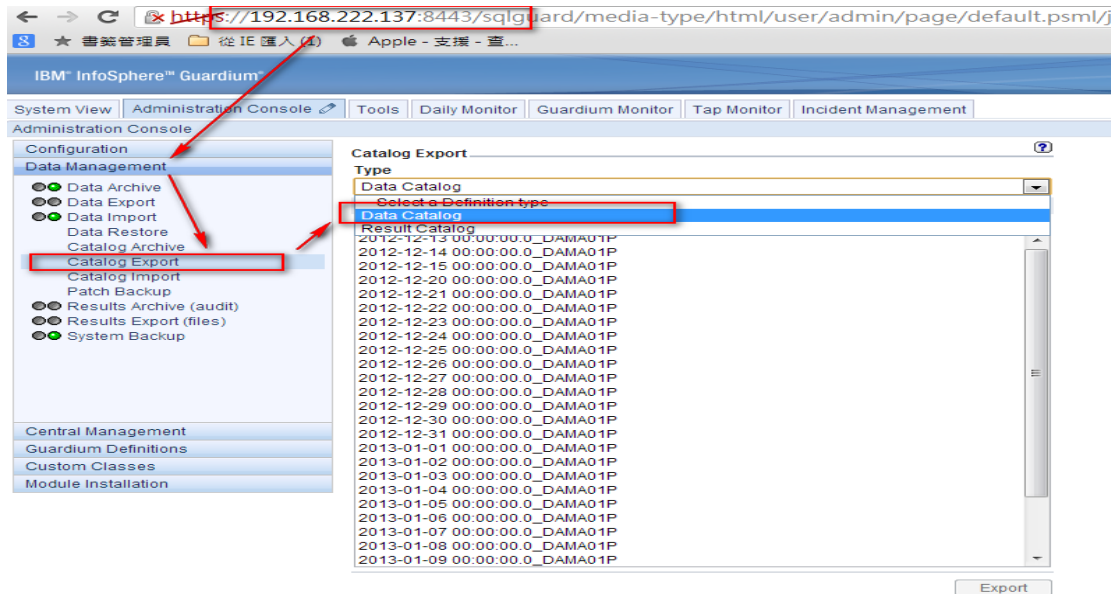


還原後, 因該VM時間點與實際時間不符, 另開啟該VM Console修改系統時間, 下store system clock datetime 來修改, 並restart gui 重新啟動GUI程式

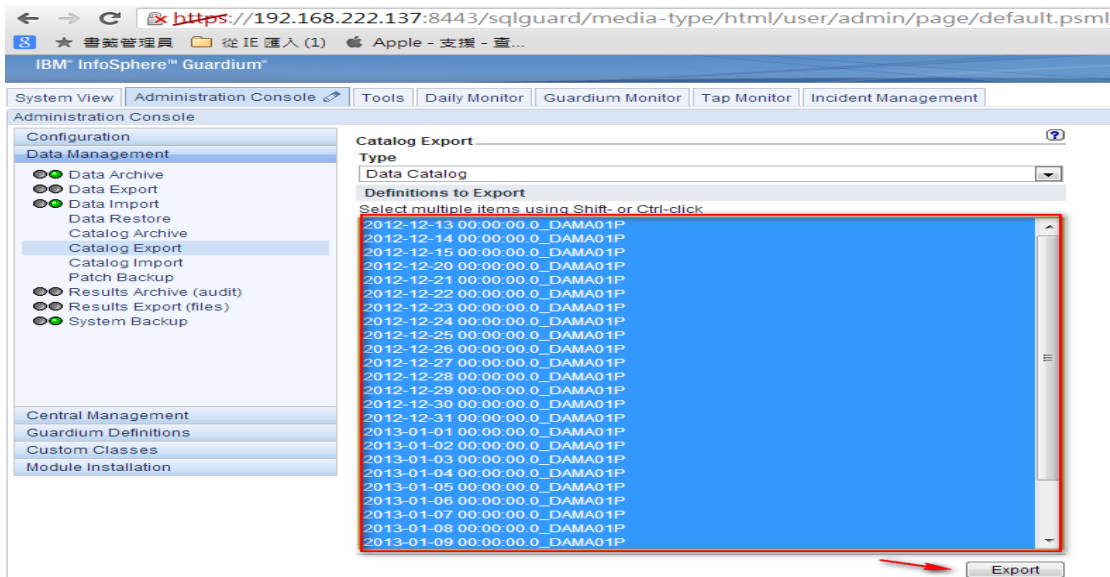


用admin登入192.168.222.138主機, 確認時間與實際時間相同, 再開始還原資料

Central Management 上資料還原 (續)

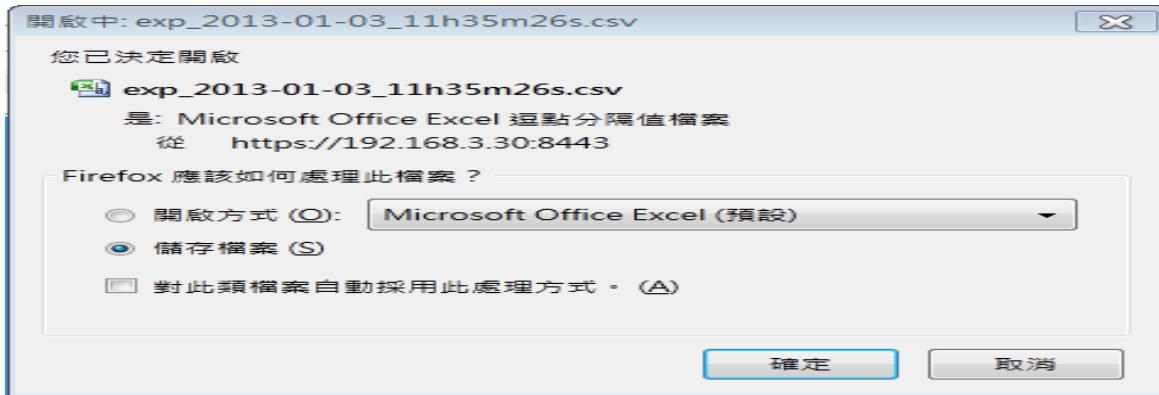


將CM 主機上 Catalog Export 出來, 可選預還原的備份時間點(或全部)即可, 選export後存於操作的PC上

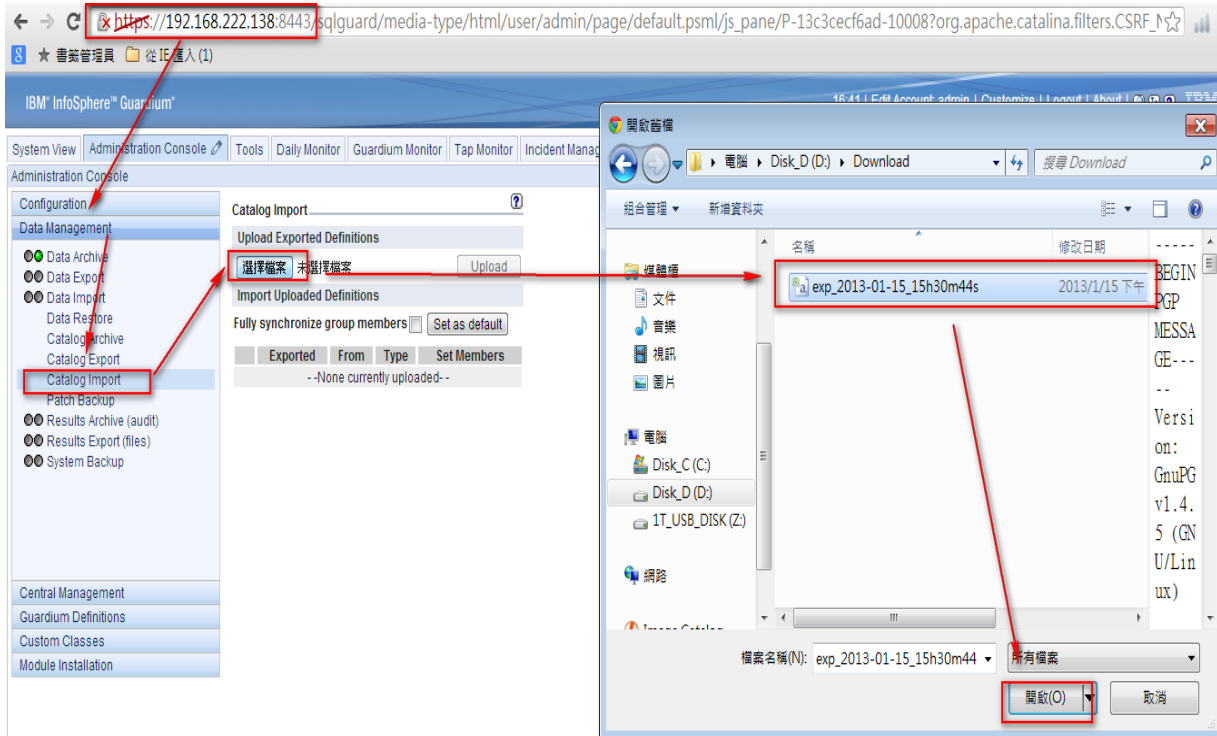


選取要匯出的Data Catalog 日期後選Export

Central Management 上資料還原 (續)

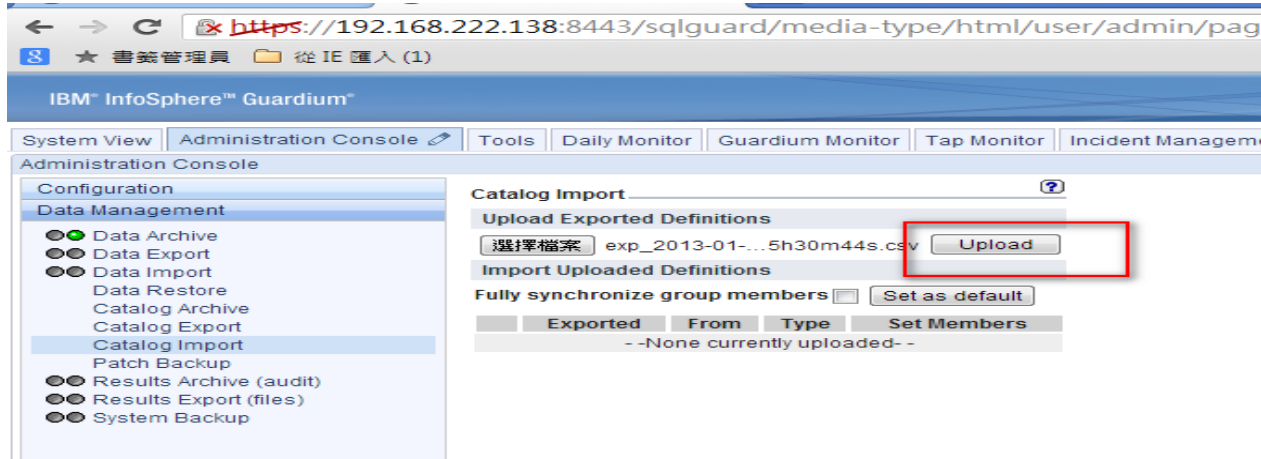


存到本機硬碟上

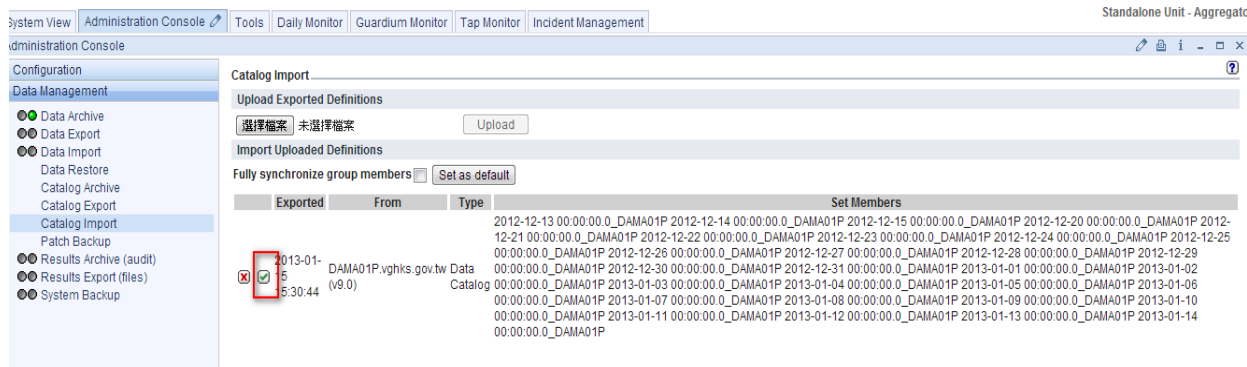


至192.168.222.138還原資料專用機，將剛export的Catalog檔選Catalog Import匯入備份相關資料

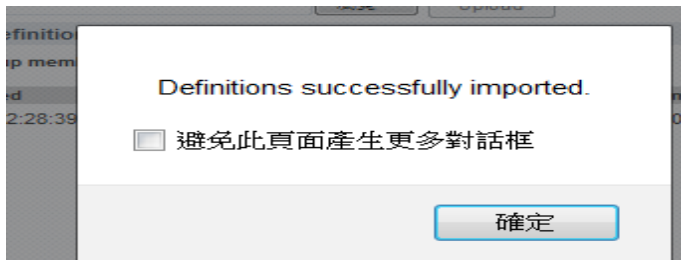
Central Management 上資料還原 (續)



選取剛下載的csv檔，將其upload

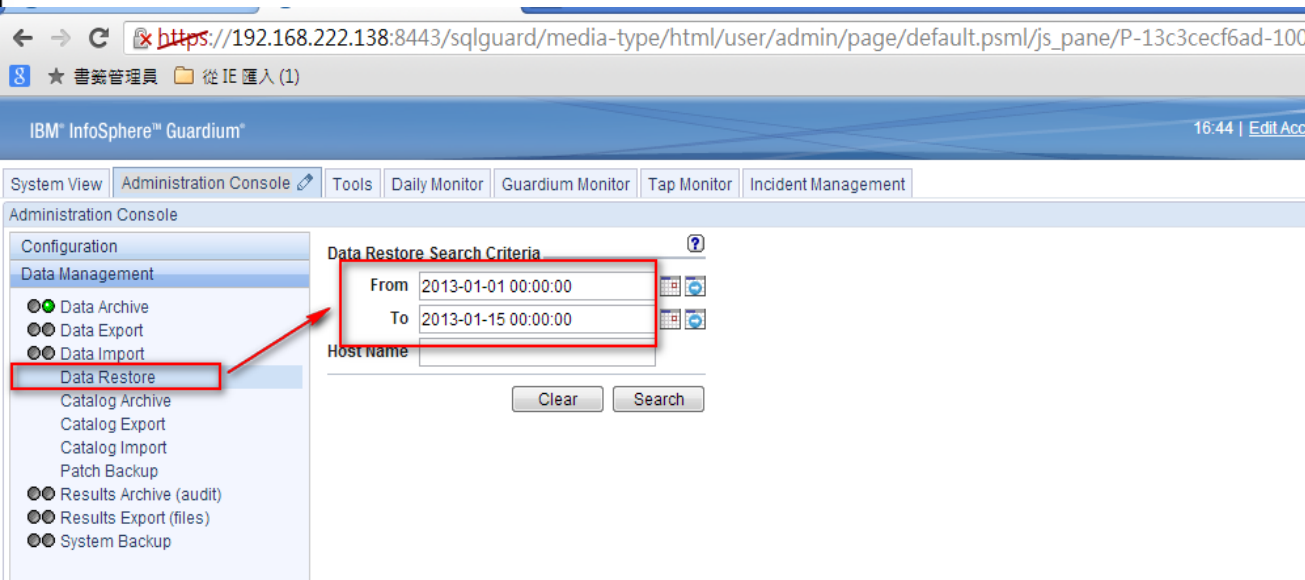


點選”綠色小勾”匯入Catalog

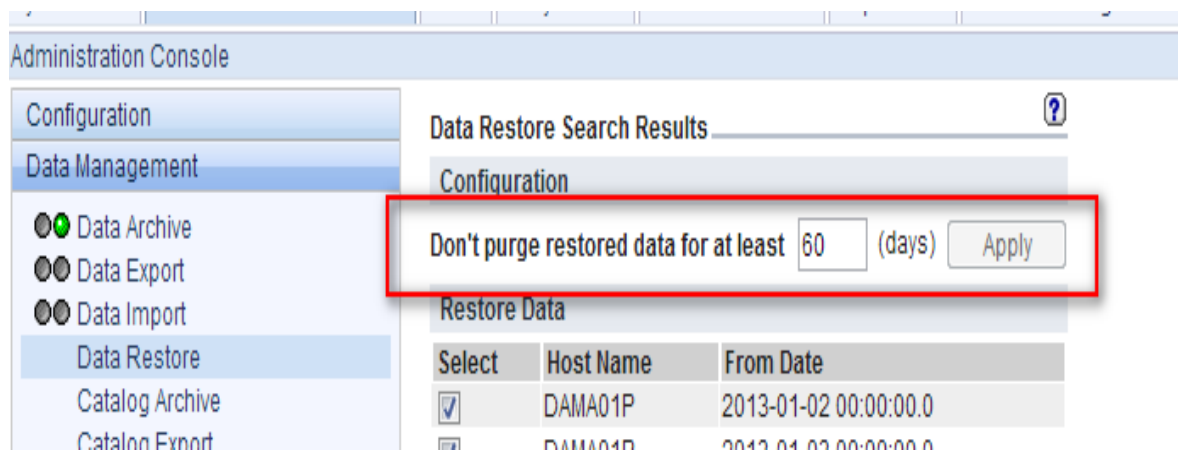


成功 Import

Central Management 上資料還原 (續)

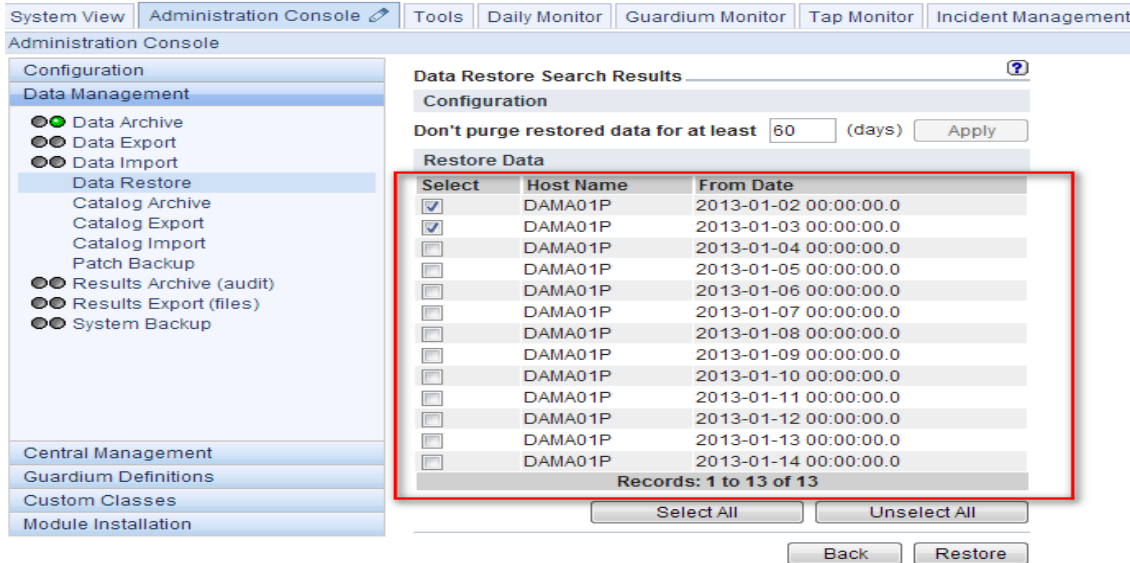


Catalog還原後，選取Data Restore來還原實際資料
選擇要還原資料的時間區段，選擇Search



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

Central 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)

WZ00J042J.040042-02009-04-22.000011P/ TAN T圖

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

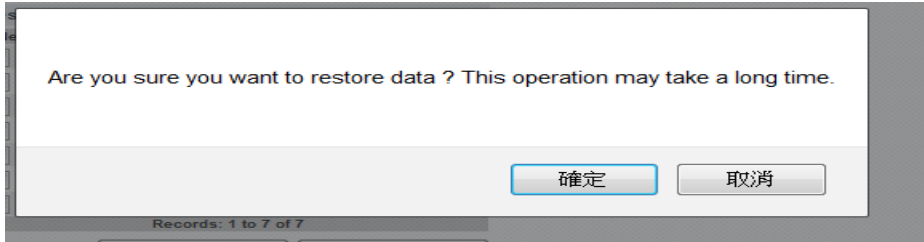
還原想要的日子，然後還原後續月份的第一天

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

Central Management 上資料還原 (續)



確認要開始Restore

Browser address: https://192.168.222.138:8443/sqlguard/media-type/html/user/admin/page/default.psm/js_pane/P-13c3cec6ae-100b67org.apache.catalina.f

System View | Administration Console | Tools | Daily Monitor | **Guardium Monitor** | Tap Monitor | Incident Management | Standalone Unit - Aggreg

Aggregation/Archive Log

Start Date: 2013-01-16 16:09:41 End Date: 2013-01-23 16:09:41
Using Merge Period Between 2013-01-09 and 2013-01-23.
Aliases: OFF SQLGuardHostName: LIKE %

Activity Type	Start Time	File Name	Status	Comment	Guardium Host Name	Records Purged	Period Start	Period End
Restore	2013-01-23 09:38:43.0		Succeeded	Begin restore of 4 entries.	DAMA02P	N/A		
Restore	2013-01-23 09:39:18.0		Succeeded	Entry_id = 01e654b35d35e5e74fd6b092143ab24 files fetched.	DAMA02P	N/A		
Restore	2013-01-23 09:39:51.0		Succeeded	Entry_id = 95c20265384066d5bdec4b230af35ef files fetched.	DAMA02P	N/A		
Restore	2013-01-23 09:40:23.0		Succeeded	Entry_id = e39df1efe4d0d96475176e371d1017c9 files fetched.	DAMA02P	N/A		
Restore	2013-01-23 09:41:08.0		Succeeded	Entry_id = b71597d9d3b582a46bfec9a8705d8576 files fetched.	DAMA02P	N/A		
Restore	2013-01-23 09:41:14.0		Succeeded	Restore - START	DAMA02P	N/A		
Importing file	2013-01-23 09:41:19.0	735234-DAMA01P.vghis.gov.tw-w20130102.050002-d2013-01-01.agg.90.tar.gz	Succeeded	Size: 1.4G	DAMA02P	N/A	2013-01-01 00:00:00	2013-01-02 00:00:00
Importing file	2013-01-23 09:52:18.0	735245-DAMA01P.vghis.gov.tw-w20130113.050002-d2013-01-12.agg.90.tar.gz	Succeeded	Size: 1.4G	DAMA02P	N/A	2013-01-12 00:00:00	2013-01-13 00:00:00
Importing file	2013-01-23 10:03:02.0	735246-DAMA01P.vghis.gov.tw-w20130114.050002-d2013-01-13.agg.90.tar.gz	Succeeded	Size: 1.2G	DAMA02P	N/A	2013-01-13 00:00:00	2013-01-14 00:00:00
Importing file	2013-01-23 10:12:07.0	735247-DAMA01P.vghis.gov.tw-w20130115.050002-d2013-01-14.agg.90.tar.gz	Succeeded	Size: 1.9G	DAMA02P	N/A	2013-01-14 00:00:00	2013-01-15 00:00:00
Restore	2013-01-23 10:26:15.0		Succeeded	Restore - DONE	DAMA02P	N/A		
Restore	2013-01-23 10:26:20.0		Succeeded	loaded to TURBINE database.	DAMA02P	N/A		
Merge process	2013-01-23 10:26:23.0		Succeeded	Merge process - START	DAMA02P	N/A		
Merge	2013-01-23 10:27:10.0		Succeeded	Merge (TURBINE)	DAMA02P	N/A		
Merge	2013-01-23 10:27:19.0		Succeeded	Merge (INV_1)	DAMA02P	N/A		
Merge	2013-01-23 10:27:19.0		Succeeded	Merge (INV_2)	DAMA02P	N/A		
Merge	2013-01-23 10:27:19.0		Succeeded	Merge (INV_3)	DAMA02P	N/A		

於Aggregation/Archive Log內查看Restore還原狀況

Central Management 上資料還原 (續)

https://192.168.222.137:8443/qlguard/media-type/html/user/infosec/page/default.psmi?org.apache.catalina.filters.CSRF_NONCE=1751

IBM InfoSphere™ Guardium

You have 6 items on your To-do list

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

Overview

DB Activities

Activity By Client IP

Database Servers

DML Execution on Sensitive Objects

IMS Access

IMS Data Access Details

IMS Event

IMS Object

Sensitive Objects Usage

Sessions By Server Type

VSAM Detailed Access

VSAM RLM

Servers Accessed

Start Date: 2013-01-13 00:00:00 End Date: 2013-01-14 00:00:00
Using Merge Period Between 2013-01-09 and 2013-01-23.
Aliases: OFF

Server IP	Server Type	Database Name	Service Name	Count of Source Program	Count of Sessions
192.168.195.30	MS SQL	SERVERBREASTSCREEN	MS SQL SERVER4		15
192.168.195.30	MS SQL	SERVERCONSULT	MS SQL SERVER2		7
192.168.195.30	MS SQL	SERVERMASTER	MS SQL SERVER3		340
192.168.195.30	MS SQL	SERVERMSDB	MS SQL SERVER4		13500
192.168.195.30	MS SQL	SERVERRADTRACK	MS SQL SERVER3		2530
192.168.195.30	MS SQL	SERVERREPORT_AGENT	MS SQL SERVER10		3437
192.168.195.30	MS SQL	SERVERREPORT_AGENT	MSSQLSERVER 2		1982
192.168.195.30	MS SQL	SERVERREPORT_HISRPT	MS SQL SERVER2		1156
192.168.195.30	MS SQL	SERVERREPORT_META	MS SQL SERVER3		195
192.168.195.30	MS SQL	SERVERREPORT_META	MSSQLSERVER 1		4205
192.168.195.30	MS SQL	SERVERREPORT_NM	MS SQL SERVER4		376
192.168.195.30	MS SQL	SERVERREPORT_NM	MSSQLSERVER 1		1412
192.168.195.30	MS SQL	SERVERREPORT_PCU	MS SQL SERVER1		1
192.168.195.30	MS SQL	SERVERREPORT_RAD	MS SQL SERVER8		2513
192.168.195.30	MS SQL	SERVERREPORT_RAD	MSSQLSERVER 2		5949
192.168.195.30	MS SQL	SERVERSRREPORT	MS SQL SERVER3		1068
192.168.195.30	MS SQL	SERVERSTUDYPROTOCOL	MS SQL SERVER3		1005
192.168.195.30	MS SQL	SERVERSTUDYPROTOCOL_HISSPMM	MS SQL SERVER1		1
192.168.195.30	MS SQL	SERVERVOICE	MS SQL SERVER2		10
192.168.195.30	MS SQL	SERVERVOICE_LONGTERM	MS SQL SERVER1		1

Records 1 to 20 of 94

Databases Discovered

Start Date: 2013-01-22 15:55:06 End Date: 2013-01-23 15:55:06
Using Merge Period Between 2013-01-09 and 2013-01-23.
Aliases: OFF PortNotLike: NOT LIKE

Time Probed Server IP Server Host Name DB Type Port Port Type #

No data found. Check the aggregation merge period.

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

https://192.168.222.138:8443/qlguard/media-type/html/user/infosec/page/default.psmi?org.apache.catalina.filters.CSRF_NONCE=75_4742E

IBM InfoSphere™ Guardium

You have 6 items on your To-do list

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

Overview

DB Activities

Activity By Client IP

Database Servers

DML Execution on Sensitive Objects

IMS Access

IMS Data Access Details

IMS Event

IMS Object

Sensitive Objects Usage

Sessions By Server Type

VSAM Detailed Access

VSAM RLM

Servers Accessed

Start Date: 2013-01-13 00:00:00 End Date: 2013-01-14 00:00:00
Using Merge Period Between 2013-01-09 and 2013-01-23.
Aliases: OFF

Server IP	Server Type	Database Name	Service Name	Count of Source Program	Count of Sessions
192.168.195.30	MS SQL	SERVERBREASTSCREEN	MS SQL SERVER4		15
192.168.195.30	MS SQL	SERVERCONSULT	MS SQL SERVER2		7
192.168.195.30	MS SQL	SERVERMASTER	MS SQL SERVER3		340
192.168.195.30	MS SQL	SERVERMSDB	MS SQL SERVER4		13500
192.168.195.30	MS SQL	SERVERRADTRACK	MS SQL SERVER3		2530
192.168.195.30	MS SQL	SERVERREPORT_AGENT	MS SQL SERVER10		3437
192.168.195.30	MS SQL	SERVERREPORT_AGENT	MSSQLSERVER 2		1982
192.168.195.30	MS SQL	SERVERREPORT_HISRPT	MS SQL SERVER2		1156
192.168.195.30	MS SQL	SERVERREPORT_META	MS SQL SERVER3		195
192.168.195.30	MS SQL	SERVERREPORT_META	MSSQLSERVER 1		4205
192.168.195.30	MS SQL	SERVERREPORT_NM	MS SQL SERVER4		376
192.168.195.30	MS SQL	SERVERREPORT_NM	MSSQLSERVER 1		1412
192.168.195.30	MS SQL	SERVERREPORT_PCU	MS SQL SERVER1		1
192.168.195.30	MS SQL	SERVERREPORT_RAD	MS SQL SERVER8		2513
192.168.195.30	MS SQL	SERVERREPORT_RAD	MSSQLSERVER 2		5949
192.168.195.30	MS SQL	SERVERSRREPORT	MS SQL SERVER3		1068
192.168.195.30	MS SQL	SERVERSTUDYPROTOCOL	MS SQL SERVER3		1005
192.168.195.30	MS SQL	SERVERSTUDYPROTOCOL_HISSPMM	MS SQL SERVER1		1
192.168.195.30	MS SQL	SERVERVOICE	MS SQL SERVER2		10
192.168.195.30	MS SQL	SERVERVOICE_LONGTERM	MS SQL SERVER1		1

Records 1 to 20 of 94

Databases Discovered

Start Date: 2013-01-22 15:55:24 End Date: 2013-01-23 15:55:24
Using Merge Period Between 2013-01-09 and 2013-01-23.
Aliases: OFF PortNotLike: NOT LIKE

Time Probed Server IP Server Host Name DB Type Port Port Type #

No data found. Check the aggregation merge period.

Records 1 to 20 of 0

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

IBM® InfoSphere™ Guardium® 17:52 | [Edit Account: accessmgr](#) | [Customize](#) | [Logout](#) | [About](#) |

Access Management Data Security Central Manager - Aggregator

User Browser

Filter string (case sensitive): User Name

Username	First Name	Last Name	Email	Actions
2869	fenmei	chang	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
2869mgr	fenmei	chang	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
2869user	fenmei	chang	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
accessmgr	accessmgr	accessmgr		Edit Roles Change Layout
admin	admin	admin	bryan@tfnkh.com.tw	Edit Roles Change Layout
infosec	info	sec	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete

新增帳號與修改

IBM InfoSphere™ Guardium™ 10:46 | [Edit Account accessmgr](#) | [Customize](#)

Access Management | Data Security

User Browser

Filter string (case sensitive): User Name ▾ Filter **Add User** Search Users

Username	First Name	Last Name	Email	Actions
2869	fenmei	chang	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
2869mgr	fenmei	chahg	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
2869user	fenmei	chang	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete
accessmgr	accessmgr	accessmgr		Edit Roles Change Layout
admin	admin	admin	bryan@tfnkh.com.tw	Edit Roles Change Layout
infosec	info	sec	fmchang@vqhks.gov.tw	Edit Roles Change Layout Delete

選add user新增使用者，或編修現有使用者

Data Security

User Form

Username

Password

Password (confirm)

First Name

Last Name

Email

Disabled

*In an effort to provide the highest level security, new passwords must be 8 or more characters in length and must include at least one uppercase letter, lowercase letter, digit, and special character. A special character is considered any of the following:
@#%&.,!+=_*


Add User **Back**

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

IBM InfoSphere Guardium

Access Management  Data Security

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

Role Browser

Role Name	Actions
accessmgr	
admin	
appdev	Delete
audit	Delete
cas	Delete
cli	
datasec-exempt	
dba	Delete
diag	
infosec	Delete
inv	
netadm	Delete
optim-audit	Delete
review-only	
user	

[Add Role](#)

IBM InfoSphere Guardium

Access Management  Data Security


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

Role Form

Role Name


帳號權限修改

新增或刪除使用者所可使用之權限

Access Management  Data Security

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


Edit Application Role Permissions

Assign Roles to Applications 

Access Map Application	Roles...
Access Map Builder/Viewer	Roles...
Access Tracking	Roles...
Administration Console	Roles...
Agg/Archive Activity Tracking	Roles...
Alert Builder	Roles...
Alert Tracking	Roles...
Alias Builder	Roles...
Allow Full SQL Drill Down	Roles...
AME Interface Definition Builder	Roles...
Audit Database Builder	Roles...
Audit Process Builder	Roles...
Audit Process To-Do List	Roles...
Audit Process Tracking	Roles...
Auditing Application	Roles...
Auto-discovery Configuration	Roles...

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

Edit Application Role Permissions

Assign Security Roles 


Owner: admin
Assign Roles for Access Map Application

All Roles

accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
review-only	<input type="checkbox"/>
user	<input type="checkbox"/>

Apply Back

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 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 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, 瀏覽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

IBM InfoSphere™ Guardium™

13:36 | [Edit Account: infosec](#) | [Customize](#) | [Logout](#) | [About](#) |

You have 6 items on your To-do list

Central Manager - Aggregator

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

Overview
DB Activities
Exceptions
DB Administration
Schema Changes
Detailed Activities
Performance
DB Entitlements
Access Map
Hadoop
Hadoop - Biginsights MapReduce Report
Hadoop - Exception Report
Hadoop - Full Message Details report
Hadoop - HBase Report
Hadoop - HDFS Report
Hadoop - Hue/Beeswax Report
Hadoop - MapReduce Report
Hadoop - Unauthorized MapReduce Jobs

View Installed Policy

Currently Installed Policies

Installed Policy #1

Installed Policy VGHKS
Date Installed 12/20/12 3:08 PM
This is not a selective audit policy
Not logging to flat
Rules don't fire on flat
Installed Rules 4
Baseline records 0

[View Details Report](#)

Request Rate

Start Date: 2013-01-29 11:36:08 End Date: 2013-01-29 13:36:08

Aliases: OFF

Number of db per type

Start Date: 2013-01-28 13:33:08 End Date: 2013-01-29 13:33:08

MS SQL SERVER
DB2

Count of Servers
Count of Client Sources

Aliases: OFF

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

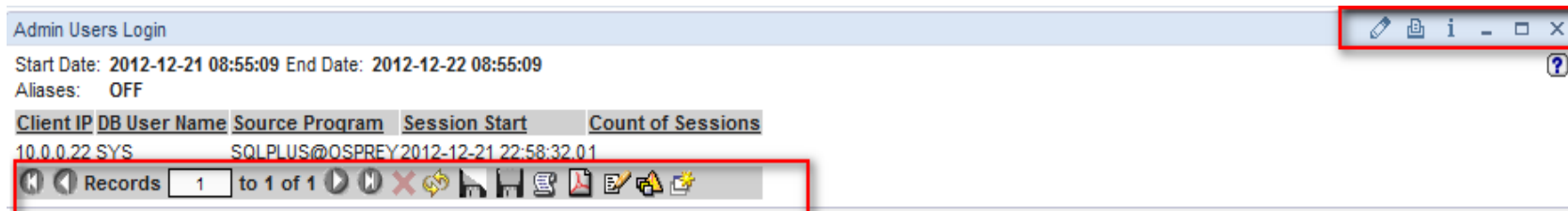
User Failed Login

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

1.1
Start Date: 2012-08-13 12:32:29 End Date: 2012-08-13 13:32:29
Aliases: OFF

Full SQL ID	Timestamp	Client	Full Sql
0:15	2012-08-13 12:55:49.0192.168.0.112	192.168.0.112	HCPPK_QUERY_O
31344961	2012-08-13 12:32:35.0192.168.0.112	192.168.0.112	UG/HCP_ATTENDORY/EXEselect rownum,b,s
31344964	2012-08-13 12:32:30.0192.168.0.112	192.168.0.112	BEGIN hcp_P_CHEC
31344965	2012-08-13 12:32:30.0192.168.0.112	192.168.0.112	BEGIN hcp_P_CHEC
31344966	2012-08-13 12:32:31.0192.168.0.112	192.168.0.112	HCPPK_ATTEND_S
31344967	2012-08-13 12:32:31.0192.168.0.112	192.168.0.112	SELECT CARDING_
31344968	2012-08-13 12:32:31.0192.168.0.112	192.168.0.112	SELECT EMP_NO,E
31344969	2012-08-13 12:32:31.0192.168.0.112	192.168.0.112	SELECT OVERTIME
31344970	2012-08-13 12:32:31.0192.168.0.112	192.168.0.112	SELECT A.USERNA/
31344971	2012-08-13 12:32:32.0192.168.0.112	192.168.0.112	HCPPK_ATTEND_S
31344972	2012-08-13 12:32:32.0192.168.0.112	192.168.0.112	SELECT CARDING_
31344973	2012-08-13 12:32:33.0192.168.0.112	192.168.0.112	BEGIN hcp_P_CHEC
31344974	2012-08-13 12:32:33.0192.168.0.112	192.168.0.112	BEGIN hcp_P_CHEC
31344975	2012-08-13 12:32:34.0192.168.0.112	192.168.0.112	HCPPK_ATTEND_S
31344976	2012-08-13 12:32:34.0192.168.0.112	192.168.0.112	SELECT CARDING_
31344977	2012-08-13 12:32:34.0192.168.0.112	192.168.0.112	select to_char(add
31344978	2012-08-13 12:32:34.0192.168.0.224	GPUSER 2012-08-13 12:07:18.0.JDBC THIN CLIENT	SELECT EMP_NO,E
31344979	2012-08-13 12:32:34.0192.168.0.224	GPUSER 2012-08-13 12:07:18.0.JDBC THIN CLIENT	SELECT OVERTIME
31344980	2012-08-13 12:32:34.0192.168.0.224	GPUSER 2012-08-13 12:07:18.0.JDBC THIN CLIENT	select distinct over
31344981	2012-08-13 12:32:35.0192.168.0.224	GPUSER 2012-08-13 12:30:09.0.JDBC THIN CLIENT	BEGIN hcp_P_INSEI

PDF 報表

1.2 DML
Start Date: 2012-08-12 13:37:26 End Date: 2012-08-12 13:39:28
Aliases: OFF DBUserNameLike: LIKE %
ServerPLike: LIKE % SessionStartAfter: >= NOV

Client IP	Server IP	Server Type	SQL Verb	Count
10.1.13.29	192.168.0.113	ORACLE	DELETE	4
10.1.13.29	192.168.0.113	ORACLE	INSERT	3
10.1.13.29	192.168.0.113	ORACLE	UPDATE	1
192.168.0.112	192.168.0.113	ORACLE	DELETE	16
192.168.0.112	192.168.0.113	ORACLE	INSERT	26
192.168.0.112	192.168.0.113	ORACLE	UPDATE	50
192.168.0.12	192.168.0.113	ORACLE	DELETE	2
192.168.0.12	192.168.0.113	ORACLE	INSERT	6
192.168.0.8	192.168.0.113	ORACLE	DELETE	1
192.168.0.8	192.168.0.113	ORACLE	INSERT	2
192.168.1.27	192.168.0.113	ORACLE	DELETE	1
192.168.1.27	192.168.0.113	ORACLE	INSERT	3
192.168.1.28	192.168.0.113	ORACLE	DELETE	1
192.168.1.28	192.168.0.113	ORACLE	INSERT	4
192.168.2.51	192.168.0.113	ORACLE	DELETE	1
192.168.2.51	192.168.0.113	ORACLE	INSERT	2
192.168.2.99	192.168.0.113	ORACLE	DELETE	2
192.168.2.99	192.168.0.113	ORACLE	INSERT	6
192.168.2.99	192.168.0.113	ORACLE	UPDATE	1
192.168.2.99	192.168.0.113	ORACLE	DELETE	2
192.168.8.41	192.168.0.113	ORACLE	DELETE	2

HTML 報表

IBM InfoSphere Guardium: Report Drilldown - Source: 1.2 DML - Mozilla Firefox
https://192.168.0.157/https://192.168.0.157:8443/reportdrilldown

SessionStartAfter: >= 20120813123928
From: 2012-08-12 13:39:28
DBUserNameLike: LIKE %
ServerPLike: LIKE %
REMOTE_SOURCE: ServerIPLike: LIKE %

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
10.1.13.29	192.168.0.113	ORACLE	DELETE	4	6
10.1.13.29	192.168.0.113	ORACLE	INSERT	3	6
10.1.13.29	192.168.0.113	ORACLE	UPDATE	1	1
192.168.0.12	192.168.0.113	ORACLE	DELETE	16	323
192.168.0.12	192.168.0.113	ORACLE	INSERT	26	493
192.168.0.8	192.168.0.113	ORACLE	UPDATE	60	311
192.168.0.8	192.168.0.113	ORACLE	DELETE	2	7
192.168.1.27	192.168.0.113	ORACLE	INSERT	6	12
192.168.1.27	192.168.0.113	ORACLE	DELETE	1	1
192.168.1.28	192.168.0.113	ORACLE	INSERT	2	2
192.168.1.28	192.168.0.113	ORACLE	INSERT	4	60
192.168.2.51	192.168.0.113	ORACLE	DELETE	1	1
192.168.2.51	192.168.0.113	ORACLE	INSERT	2	2
192.168.2.99	192.168.0.113	ORACLE	DELETE	2	18
192.168.2.99	192.168.0.113	ORACLE	INSERT	6	12464
192.168.2.99	192.168.0.113	ORACLE	UPDATE	1	12
192.168.2.99	192.168.0.113	ORACLE	DELETE	2	14

報表內容操作



圖示可修改內容概覽表

Customize Portlet

Report: **Full_SQL_By_DB User** Based on Query: **Full_SQL_By_DB User**

Title:

Run Time Parameters

ClientIP: LIKE %

Enter Value for Client IP

DBUserName: LIKE %

Enter Value for DB User Name

QUERY_FROM_DATE: >= NOW -3 HOUR

Enter Period From

QUERY_TO_DATE: <= NOW

Enter Period To

REMOTE_SOURCE: -- none --

Remote Data Source

ServerIP: LIKE 192.168.0.35

Enter Value for Server IP

SHOW_ALIASES: On Off Default

Show Aliases

Presentation Parameters

fetchSize:

Max. records per page

refreshRate:

Refresh rate (seconds)

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 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Choose A Group Type Or Sub-Type to Group By</p> <p>Choose A Group Type Or Sub-Type to Group By</p> <p>=====</p> <p>Group Type: COMMANDS</p> <p>Group Type: Server IP</p> <p>Group Type: USERS</p> <p>Group Type: OBJECTS</p> <p>Group Type: SOURCE PROGRAM</p> <p style="padding-left: 20px;">Sub Type: Programs</p> <p style="padding-left: 20px;">Sub Type: fsdf</p> <p>Group Type: Client IP</p> </div>
8	QUERY_FROM_DATE Enter Period From	起始時間 <div style="display: flex; align-items: center;"> <input type="text"/> <input type="button" value="月曆選擇時間"/> </div> <div style="display: flex; align-items: center; margin-top: 5px;"> <input type="text"/> <input type="button" value="條件選擇時間"/> </div>
9	QUERY_TO_DATE Enter Period To	結束時間 <div style="display: flex; align-items: center;"> <input type="text"/> <input type="button" value="月曆選擇時間"/> </div> <div style="display: flex; align-items: center; margin-top: 5px;"> <input type="text"/> <input type="button" value="條件選擇時間"/> </div>

報表內容操作 (續)



圖示可修改內容概覽表

Customize Portlet

Report: **Full_SQL_By_DB User** Based on Query: **Full_SQL_By_DB User**

Title:

Run Time Parameters

ClientIP LIKE %

Enter Value for Client IP

DBUserName LIKE %

Enter Value for DB User Name

QUERY_FROM_DATE >= NOW -3 HOUR

Enter Period From

QUERY_TO_DATE <= NOW

Enter Period To

REMOTE_SOURCE -- none --

Remote Data Source

ServerIP LIKE 192.168.0.35

Enter Value for Server IP

SHOW_ALIASES On Off Default

Show Aliases

Presentation Parameters

fetchSize 20

Max. records per page

refreshRate 0

Refresh rate (seconds)

10	REMOTE_SOURCE Remote Data Source	<input type="text" value="-- 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 <input type="radio"/> On <input type="radio"/> Off <input type="radio"/> default
14	fetchSize Max. records per page	顯示報表筆數(最小 1 最大 100) <input type="text" value="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)

Report: **Full_SQL_By_DB User** Based on Query: **Full_SQL_E**

Title

Run Time Parameters

ClientIP LIKE

Enter Value for Client IP

DBUserName LIKE

Enter Value for DB User Name

QUERY_FROM_DATE >= NOW -1 DAY

Enter Period From

QUERY_TO_DATE <= NOW

Enter Period To

REMOTE_SOURCE -- none --

Remote Data Source

ServerIP LIKE

Enter Value for Server IP

SHOW_ALIASES On Off Default

Show Aliases

Presentation Parameters

fetchSize 20

Max. records per page

refreshRate 0

Refresh rate (seconds)

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主機瀏覽即時資料

QUERY_TO_DATE <= NOW

Enter Period To

REMOTE_SOURCE

Remote Data Source

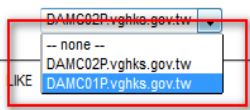
ServerIPLike LIKE

Enter Value for Destination Address

SHOW_ALIASES On Off Default


Show Aliases


Presentation Parameters



選擇Collector主機

報表內容時間條件

>= 2012-12-10 00:00:00 

<= 2012-12-14 

December 2012						
Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

-- none --

LIKE

On Off Default

以日期為單位條件

NOW minus

- Day
- Hour
- Minute
- Week
- Month

以時間為單位條件

QUERY_FROM_DATE
Enter Period From

>= NOW -1 DAY  

QUERY_TO_DATE
Enter Period To

<= NOW  

一般常用時間為單位條件
從現在往前推多久時間

稽核使用者 報表製作

建立報表

You have 1 item 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

Custom Reporting

Track data access

Track exceptions

Track policy violations

Track sent alerts

Track rogue connections

Define how information should be presented

Place report on portal page

- Access tracking builder
- Exceptions tracking builder
- Policy violations tracking builder
- Flat Log tracking builder
- Alert tracking builder
- Rogue connections tracking builder
- Audit Process tracking builder
- Group tracking builder
- Report builder
- Group builder
- Alias builder
- Time period builder

項目	功能簡介
1	報表製作與搜尋。
2	例外報表製作與搜尋。
3	違反策略的報表製作與搜尋。
4	已發過Alert的統計報表製作與搜尋。
5	例外連線狀況報表製作與搜尋。
6	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	新製作報表放置的位置。

You have 1 item 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

Custom Reporting

Query Finder

Query Name -- Select a Query --

Report Title -- Select a Report --

Main Entity -- Select an Entity --

New... Search

選取“New”建立新Report

建立報表(續)

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

Build Audit Policies Build Reports My New Reports Privacy Sets

Custom Reporting

New Query - Overall Details

Query Name Full_SQL_Text

Main Entity FULL SQL

Back Next

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

You have 1 item 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

Custom Reporting

Entity List test

Main Entity: Client/Server By Session

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
------	--------	-----------	------------	----------	-----------	---------

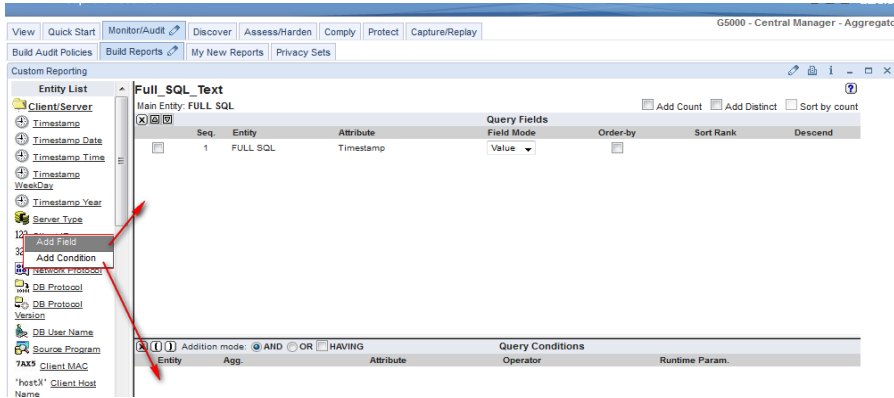
Query Conditions

Addition mode: AND OR HAVING

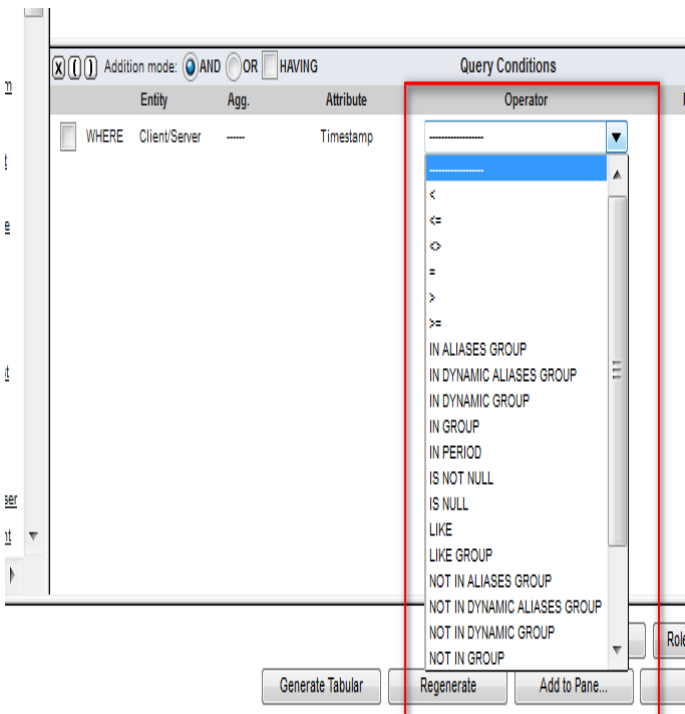
Entity	Agg.	Attribute	Operator	Runtime Param.
--------	------	-----------	----------	----------------

產生一空白報表
左側Entity List
可將其選入報表內

建立報表(續)



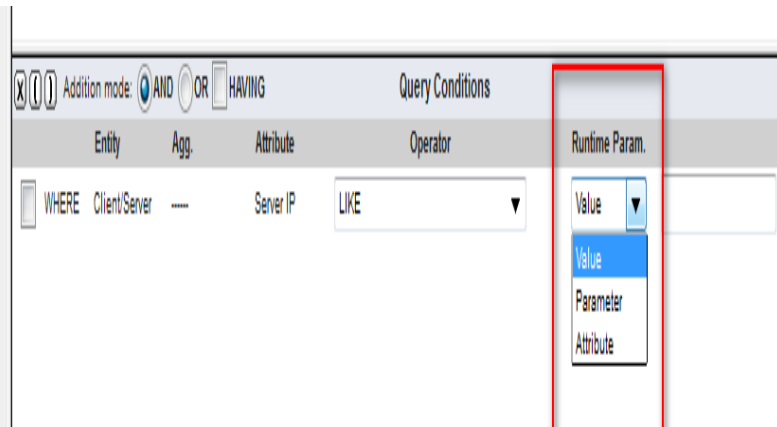
將欲使用Entity選入報表內
 Add Field:報表呈現內容
 Add Condition:條件篩選



於Query Condition中的Operator選單

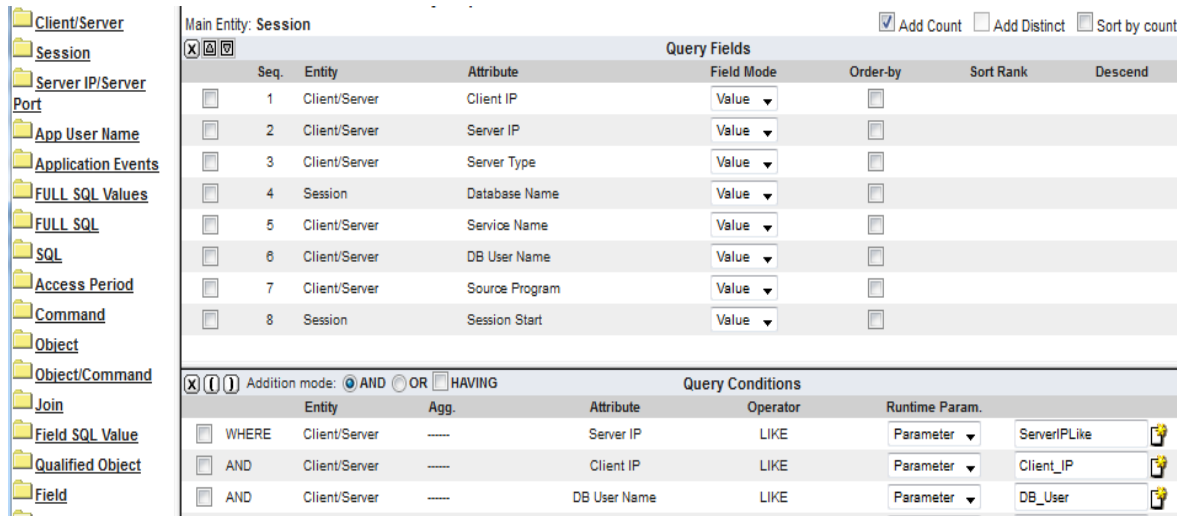
項目	簡介
<	小於空格中的數值。
< =	小於等於空格中的數值。
< >	不等於空格中的數值。
=	等於空格中的數值。
>	大於空格中的數值。
> =	大於等於空格中的數值。
IS NULL	空白的資料。
IS NOT NULL	所有存在的資料。
LIKE	與空格中相似的數值或參數。例如 %tea%，即是包含所有字串中包含 tea 的字串，如： <u>tea</u> 、 <u>Tea</u> 、 <u>tEam</u> 、 <u>steam</u> 。
LIKE GROUP	字串中包含所有相似於 Group 中所設定的數值。
NOT LIKE	不顯示與空格中相似的數值或參數。
REGEXP	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)

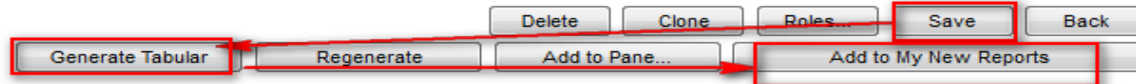


於Query Condition中的Runtime Param選單

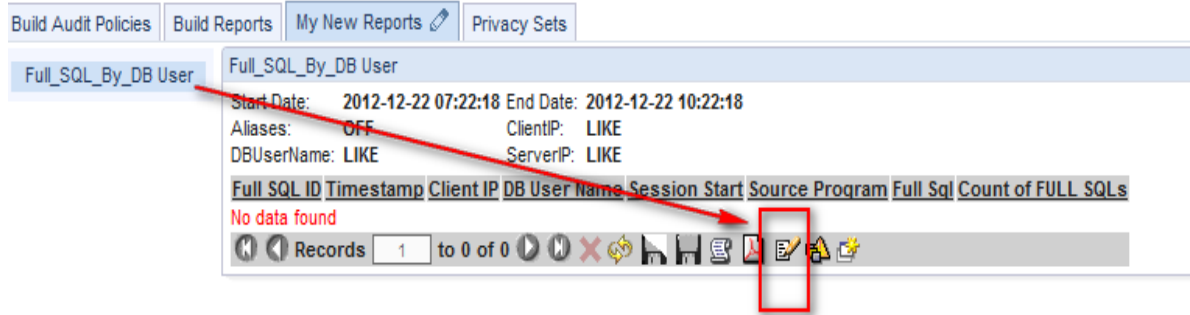
Value	顯現所輸入數值或字串相關的資料
Parameter	輸入欲查詢資料的敘述。
Attribute	顯示該屬性中的資料。



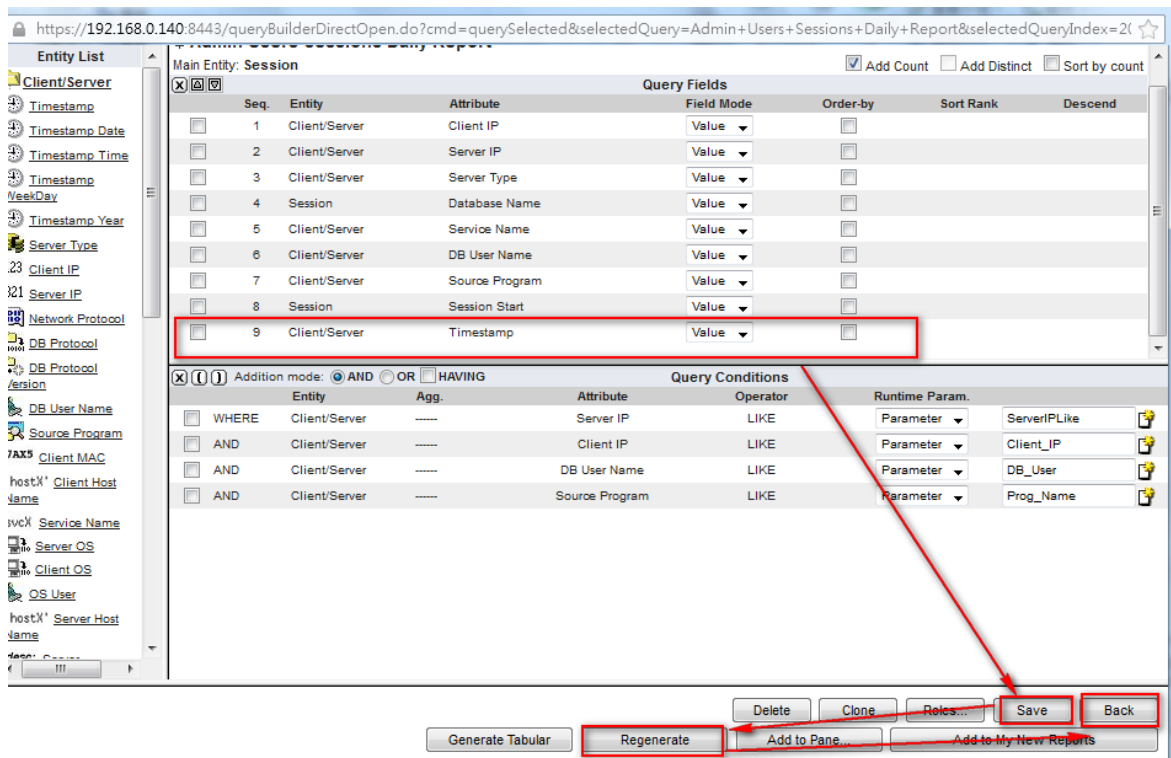
報表完成後，點擊
 Save →
 Generate Tabular →
 Add To My New Reports
 Back 退出



修改報表內容

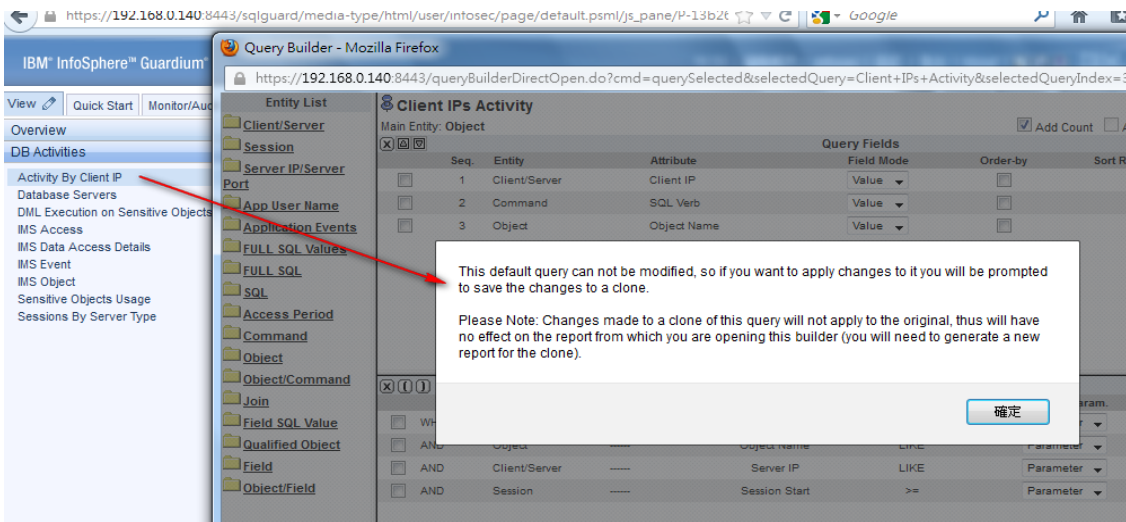


屬於My New Report報表，
可隨時對報表修改內容

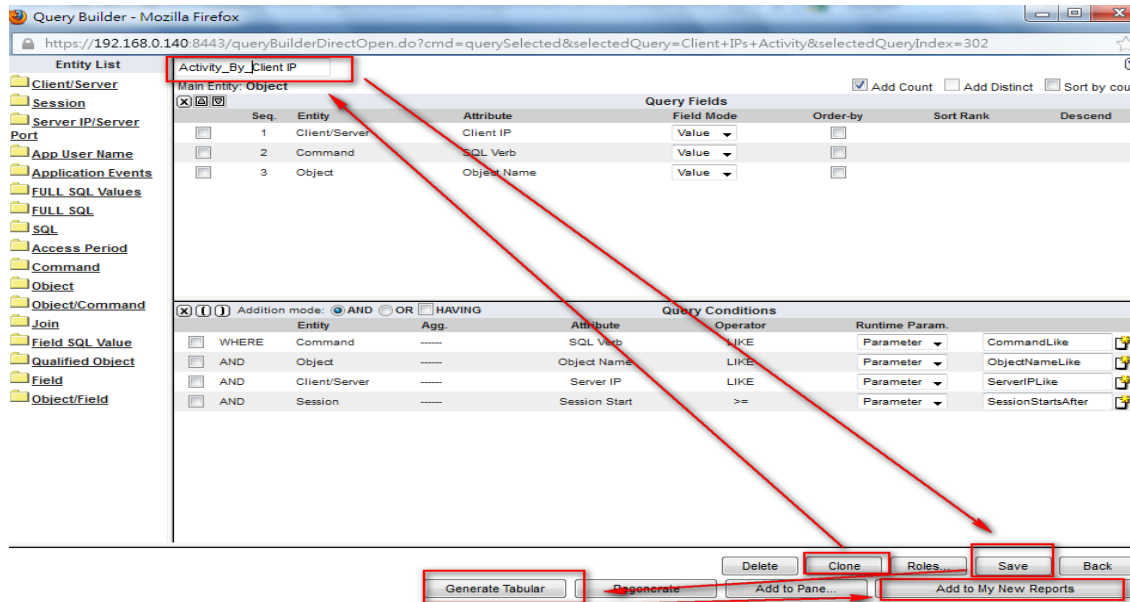


新增或刪除Entity後，
點擊
Save →
Regenerate →
Back 退出

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

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

The screenshot shows the 'Audit Process Builder' interface. The left sidebar has a 'Classification' menu with 'Audit Process Builder' selected. The main area is titled 'Audit Process Finder' and includes a filter section with 'show all' selected. Below the filter is a list of processes, with 'Daily_Audit_Report' highlighted. At the bottom, there is a 'Process Status' table.

Process	Next Run	Last Run		
		Ran At	Receivers Outstanding	Errored Tasks
Appliance Monitoring	Not Scheduled	No prior result found		
Daily_Audit_Report	1/31/13 6:00 AM	1/30/13 6:00 AM	1	0
Guardium To Arcsight Report	1/31/13 7:00 AM	1/30/13 7:00 AM	0	0

稽核報表製作流程

Audit Process Builder

Audit Process Definition

Description: sitive Object Access Detail Daily Report

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: Zip CSV for mail

Email Subject: Sensitive Object Access Detail Daily Report

View Run Once Now Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
Add Receiver					
Receiver name: infosec(info sec)	Action Required: <input checked="" type="radio"/> Review <input type="radio"/> Sign	To-Do List: <input checked="" type="checkbox"/> Add	Email Notification: <input type="radio"/> None <input type="radio"/> Link Only <input checked="" type="radio"/> Full Results		
			<input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV		
	Continuous: <input checked="" type="checkbox"/>				Approve if Empty: <input type="checkbox"/> Yes

View Run Once Now Modify Schedule... **Add**

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> infosec	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> (info sec)			<input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV		

Add Receiver

Receiver name: ----- Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

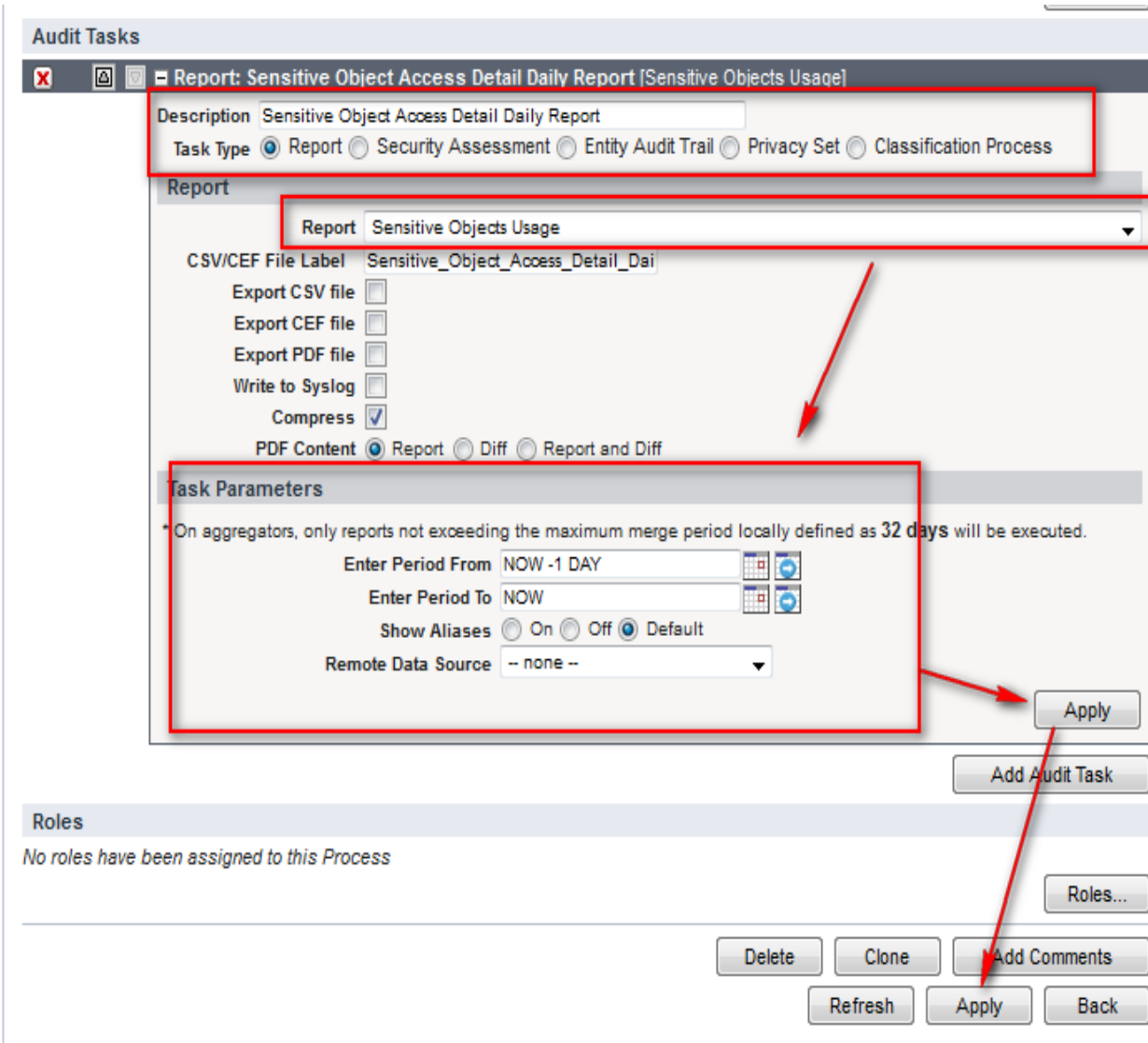
指定稽核報表名稱
Mail標題

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)



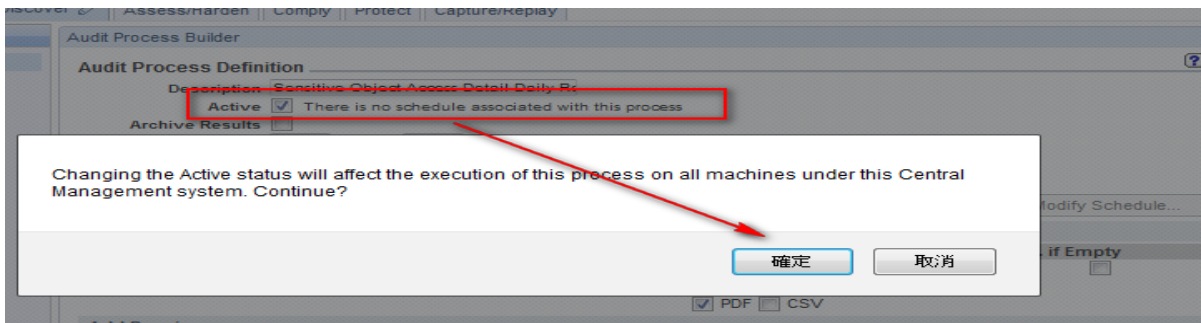
設定Audit Task
 提供Task名稱
 Task Type:Report
 選取要統計之報表

設定該報統計的時間區
 段表
 Apply確定完成此Task

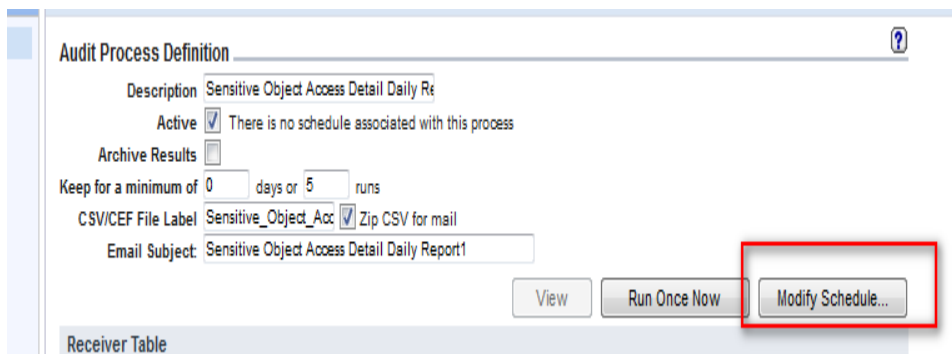
可同時設定許多Task
 選Add Audit Task

設定完成選Apply

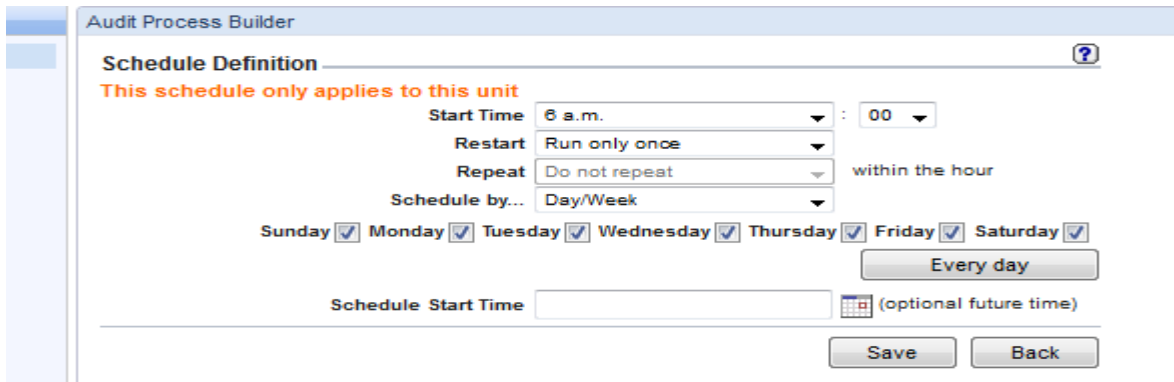
稽核報表製作流程(續)



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

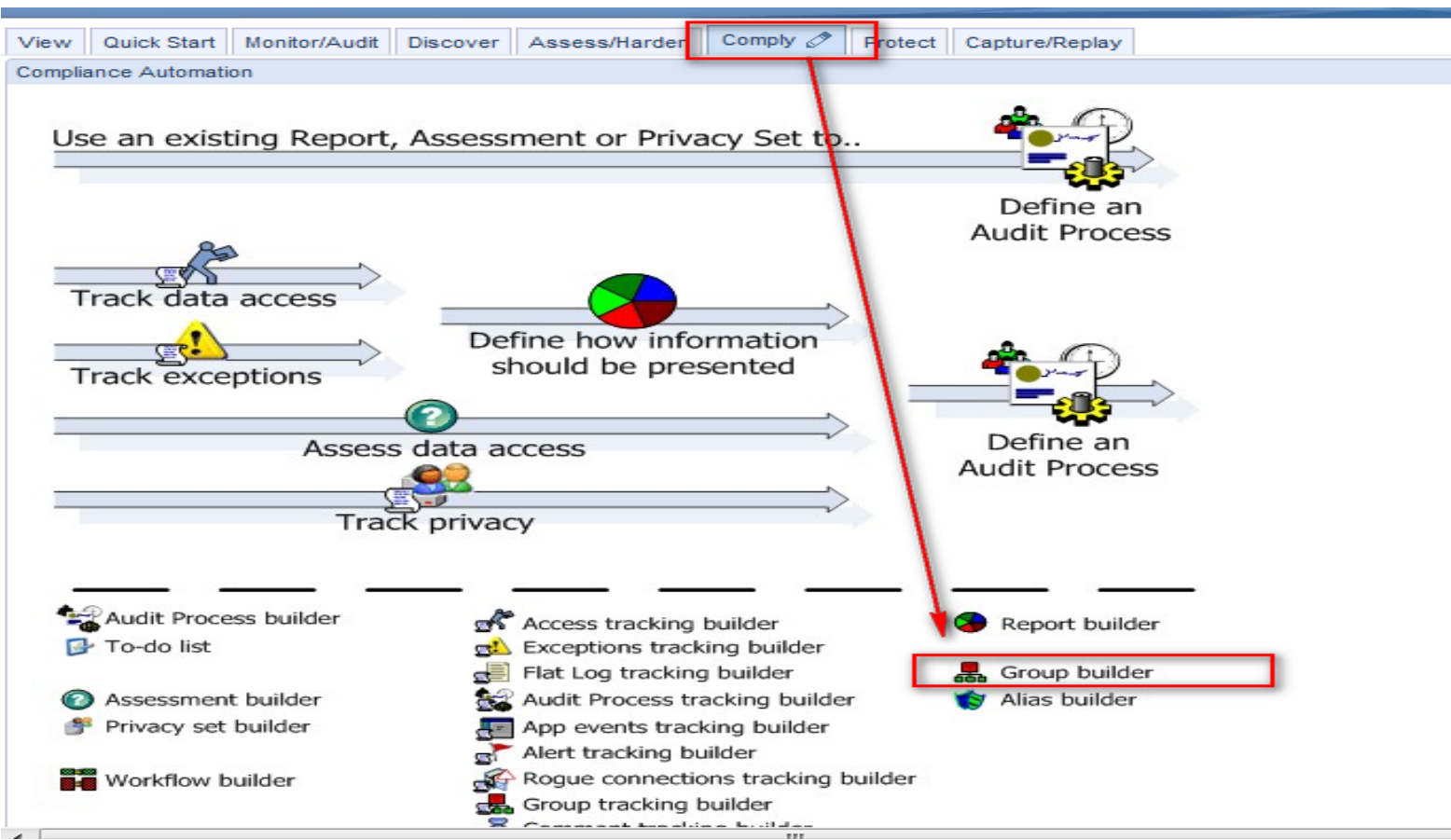


設定寄送時間, 週期

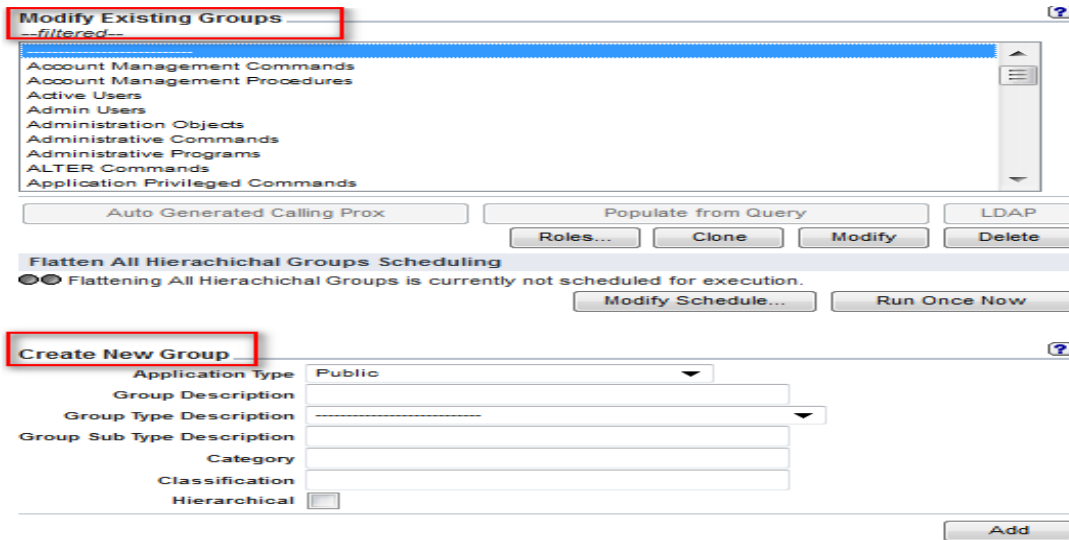
稽核使用者 群組功能操作

製作群組

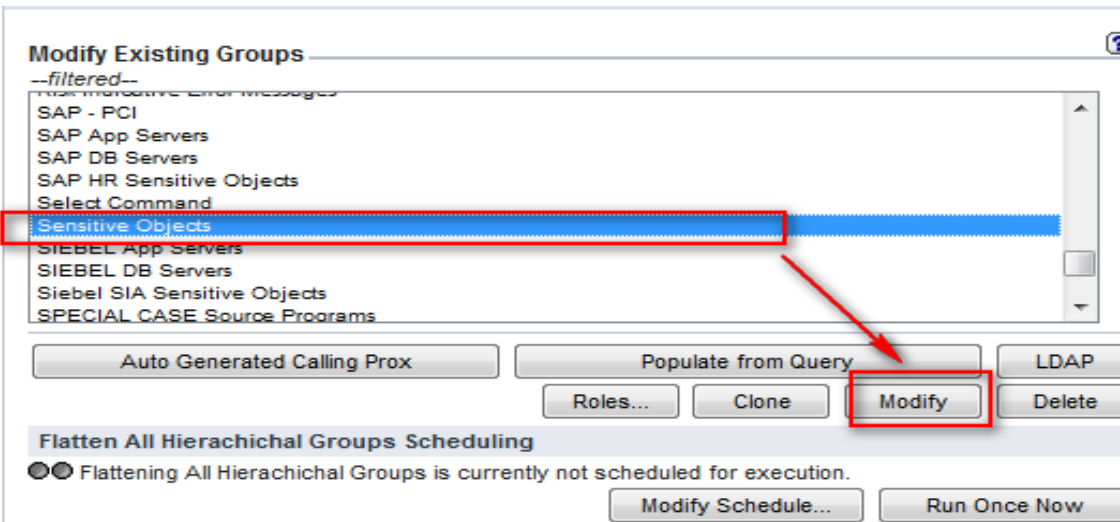
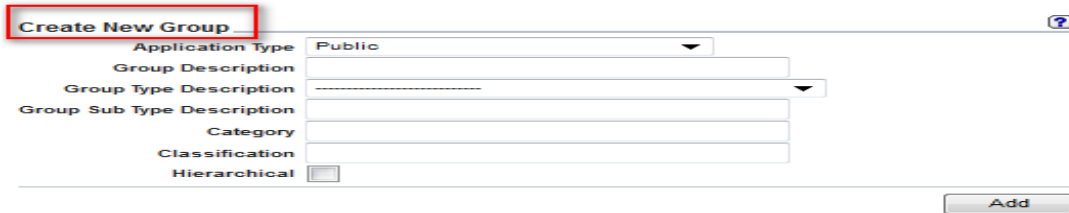
可透過建立群組來管理, 如敏感性資料, 主機群組等等來方便管理與設定
選取Comply → Group Builder



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)

Manage Members for Selected Group ?

Group Name Sensitive Objects
 Group Type OBJECTS
 Category

Group Members Filter

activity
 CARD_ID
 sales

Please select one of the following options

Create & add a new Member named

Rename selected Member to

Delete selected Member

將 Sensitive Objects 名稱輸入
 後選擇 Add
 將所有資料輸入後選 Back 離開

Create New Group ?

Application Type Public

Group Description DCL_Command

Group Type Description COMMANDS

Group Sub Type Description

Category

Classification

Hierarchical

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

