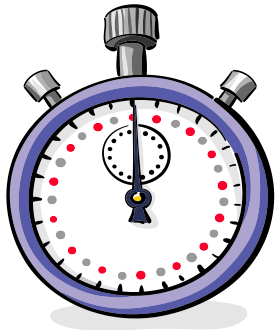
Taifon Your Solution Partner

IBM Guardium 教育訓練
基本安裝

泰鋒電腦 洪禮育

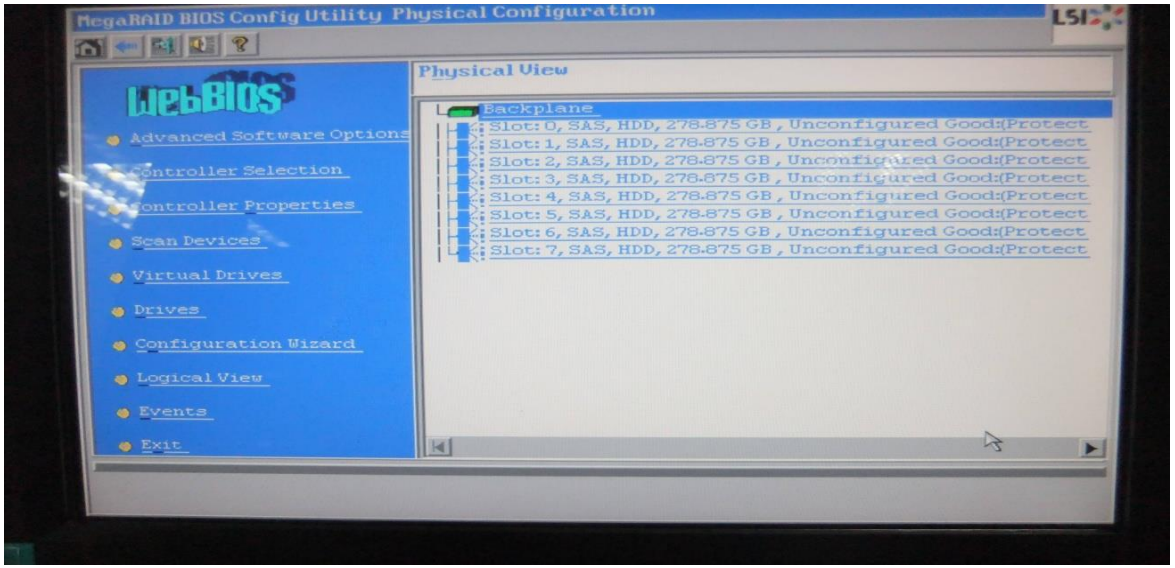
簡報綱要

- IBM X3650 M4 Raid建立
- IBM Guardium 主程式安裝
- IBM Guardium Patch檔更新
- Guardium Collector S-TAP設定
- 問題與討論

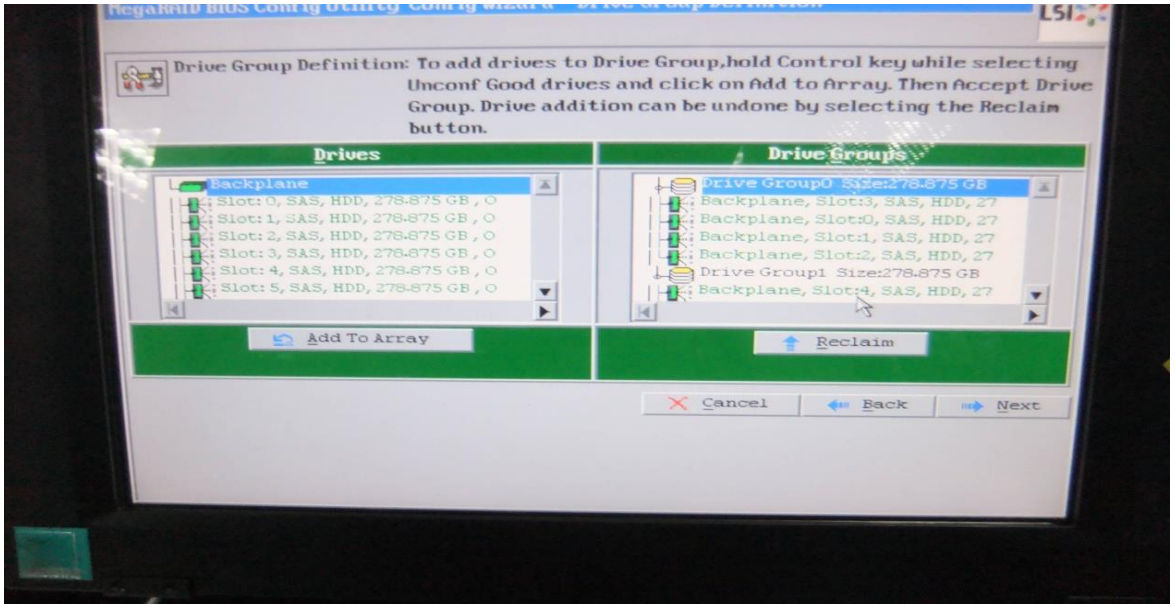


IBM X3650 M4
Raid建立

IBM主機Raid建立

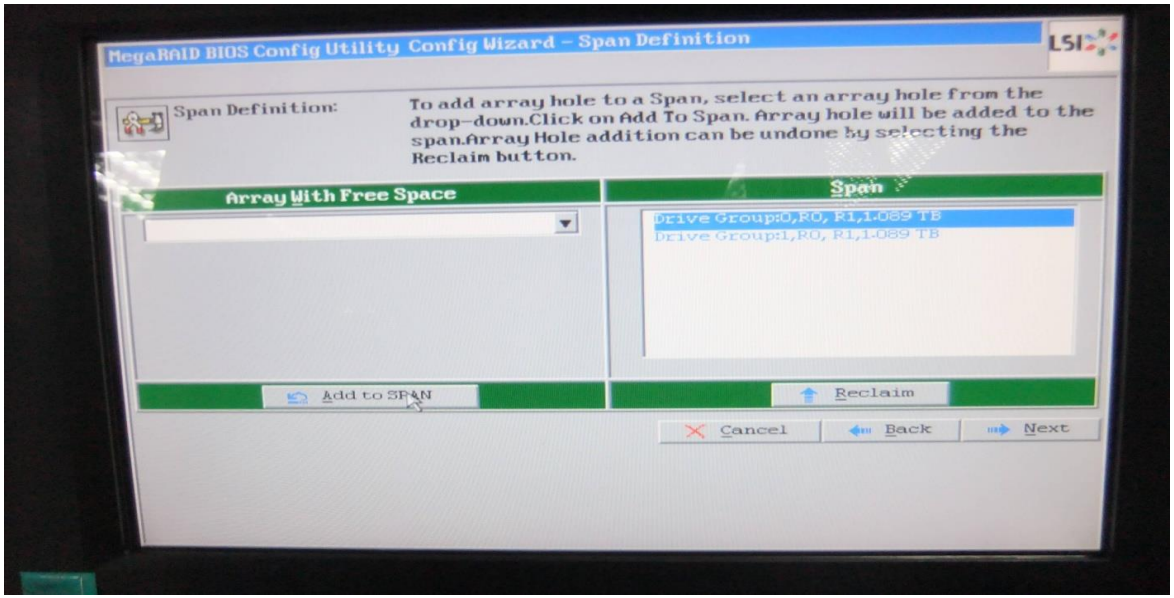


預設8顆未設定
硬碟

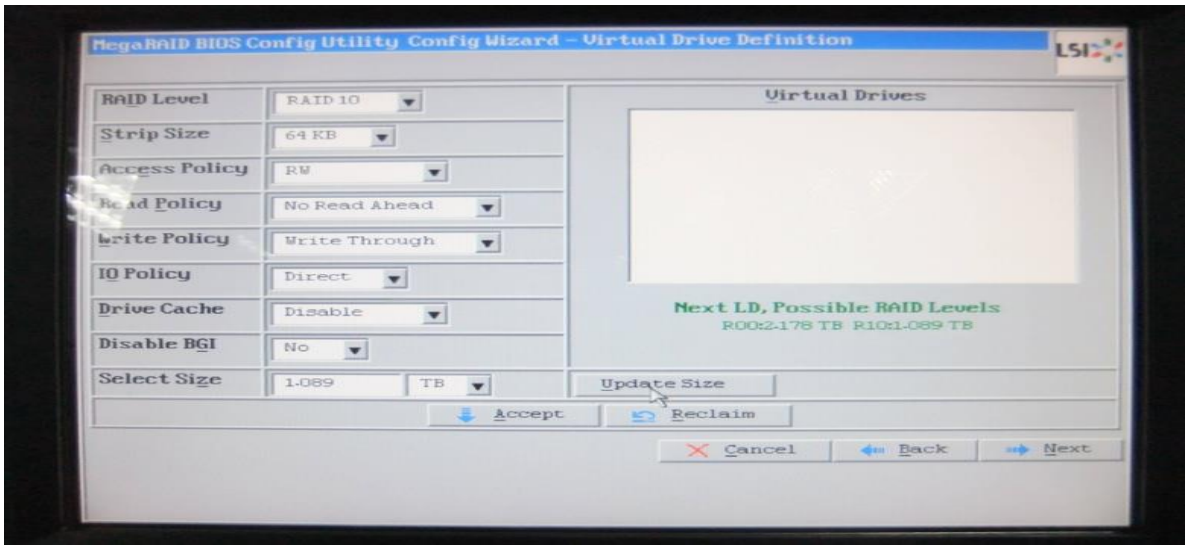


設定2個Disk group
Disk 0-3為Disk Group0
Disk 4-7為Disk Group1

IBM主機Raid建立（續）

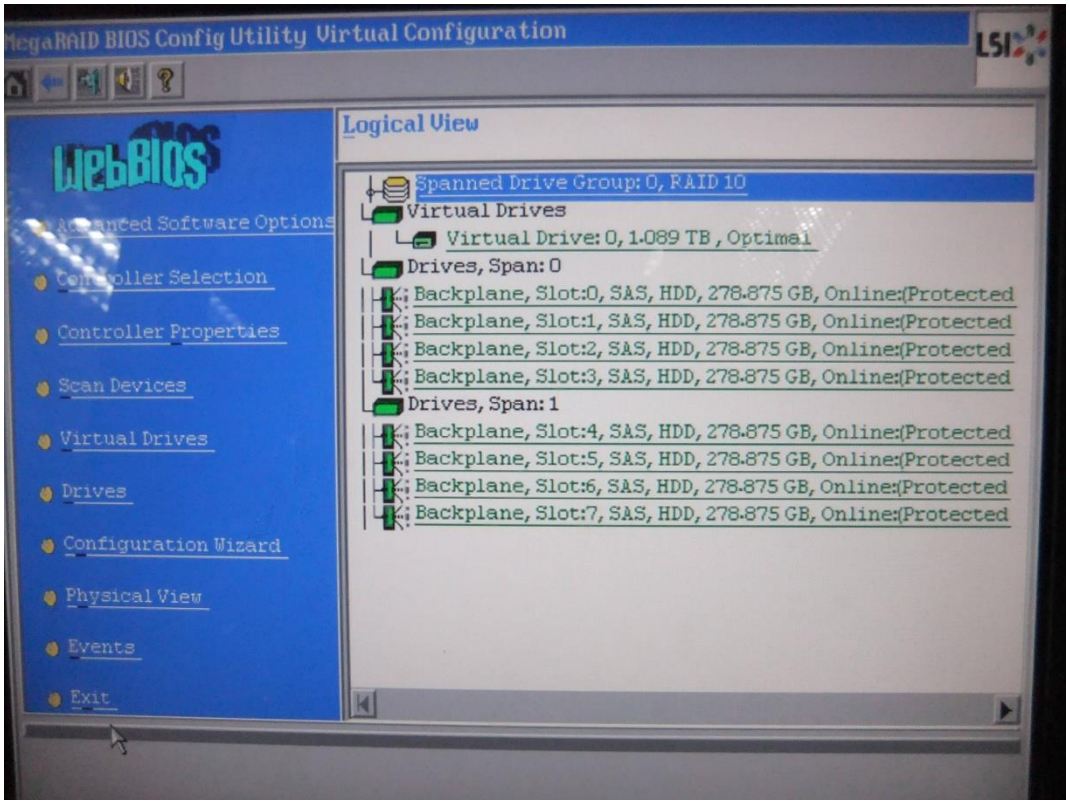


選擇兩個
Disk Group



選擇為Riad 10
Update Size為
1.089TB後確認

IBM主機Raid建立（續）

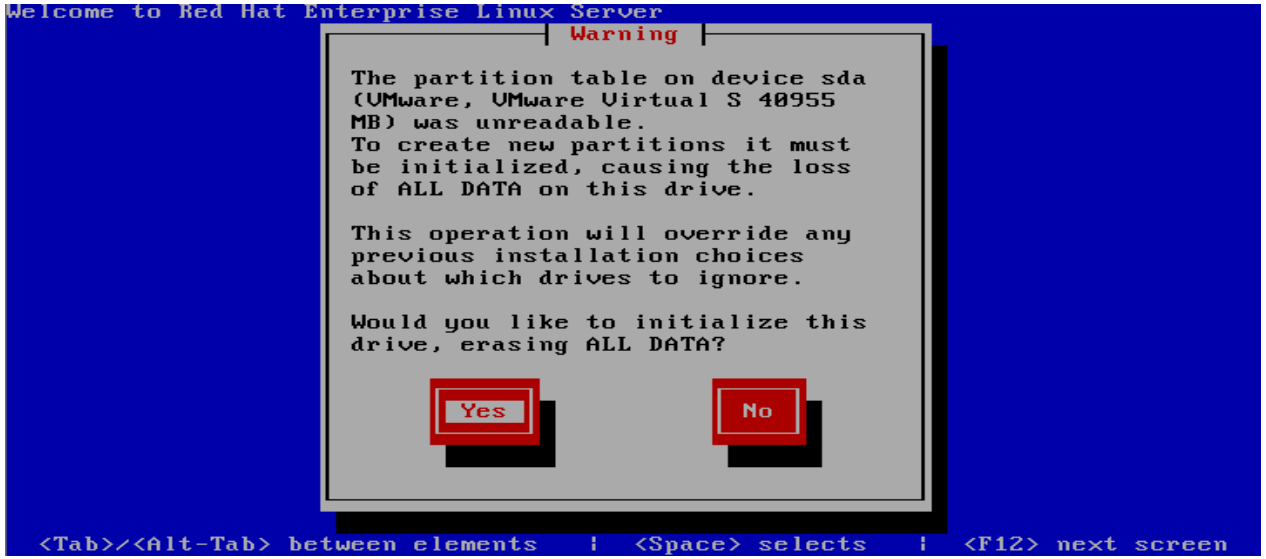


確認Raid 10
設定完成
重新開機

IBM Guardium
主程式安裝

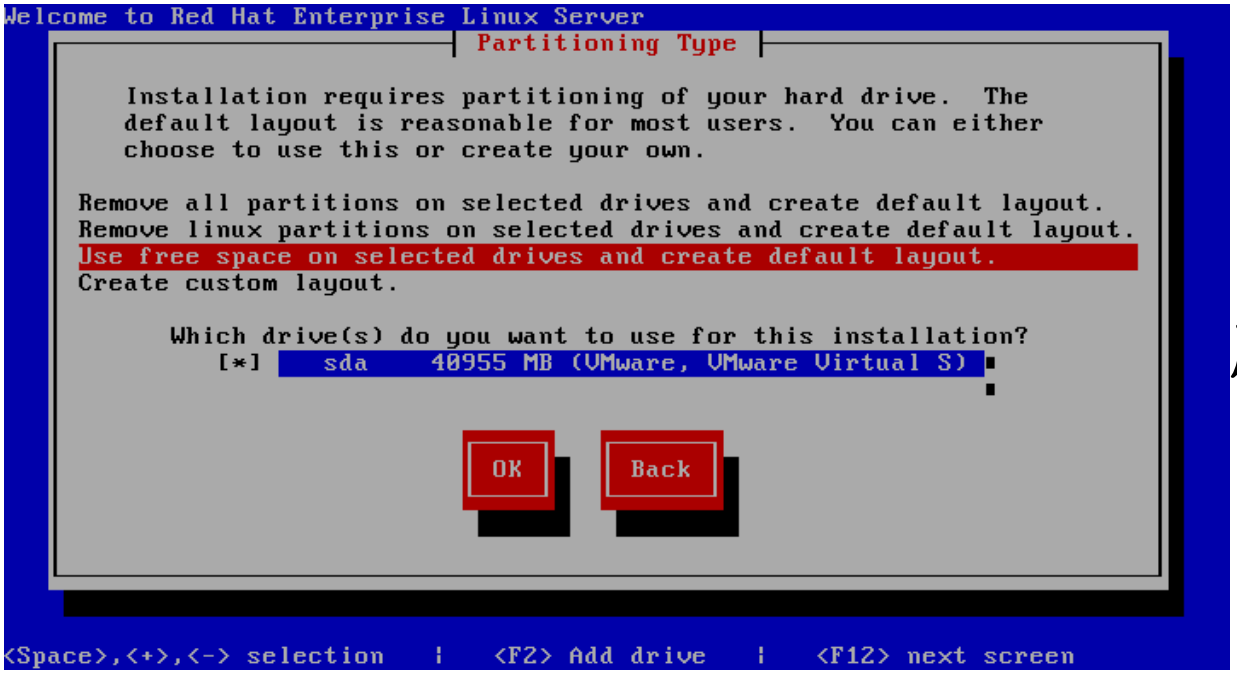
主程式安裝

放入光碟片，由光碟機開機，使用自定安裝

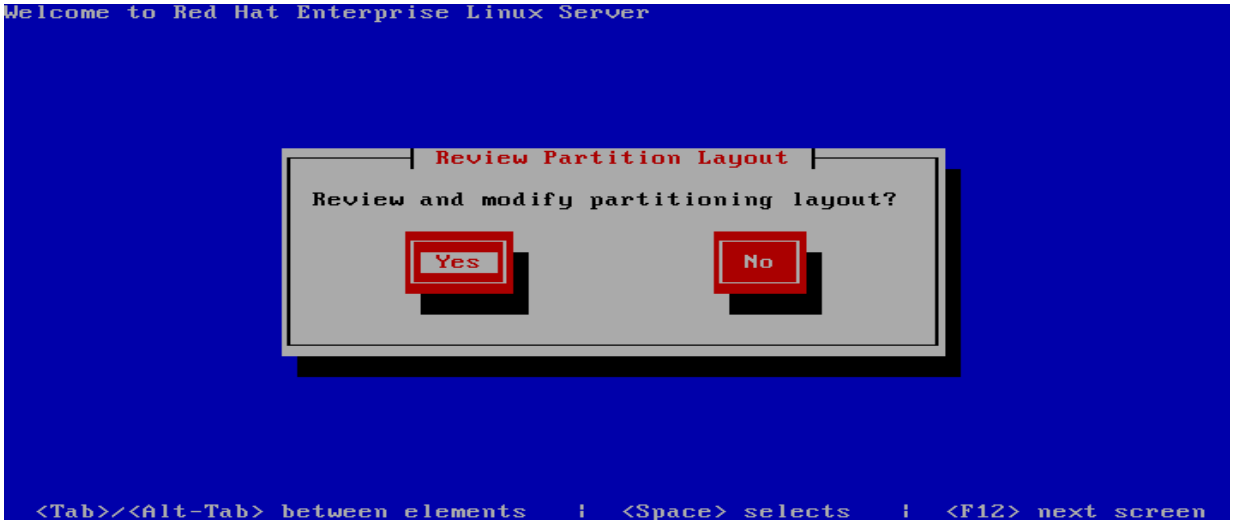


確認會刪所有資料

主程式安裝(續)

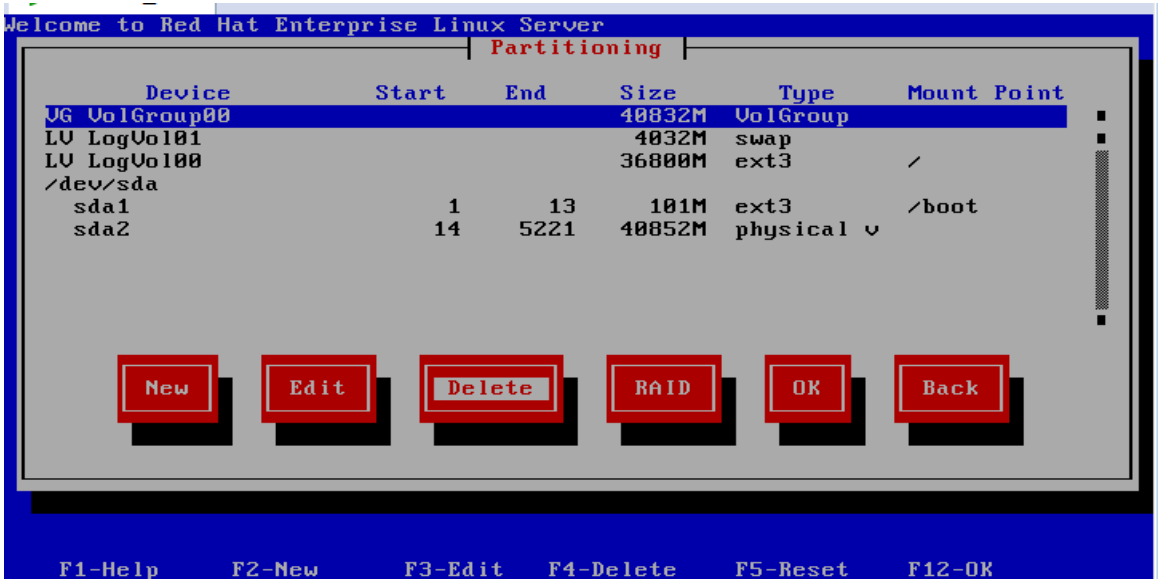


使用現有無使用空間且自定大小

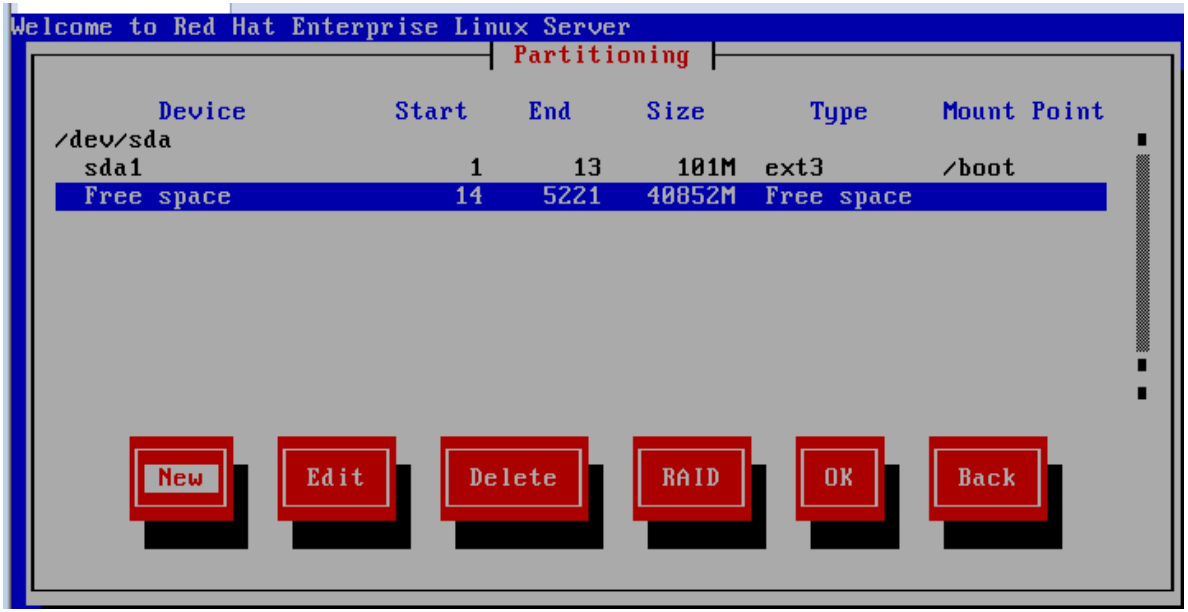


選擇要自訂大小

主程式安裝(續)

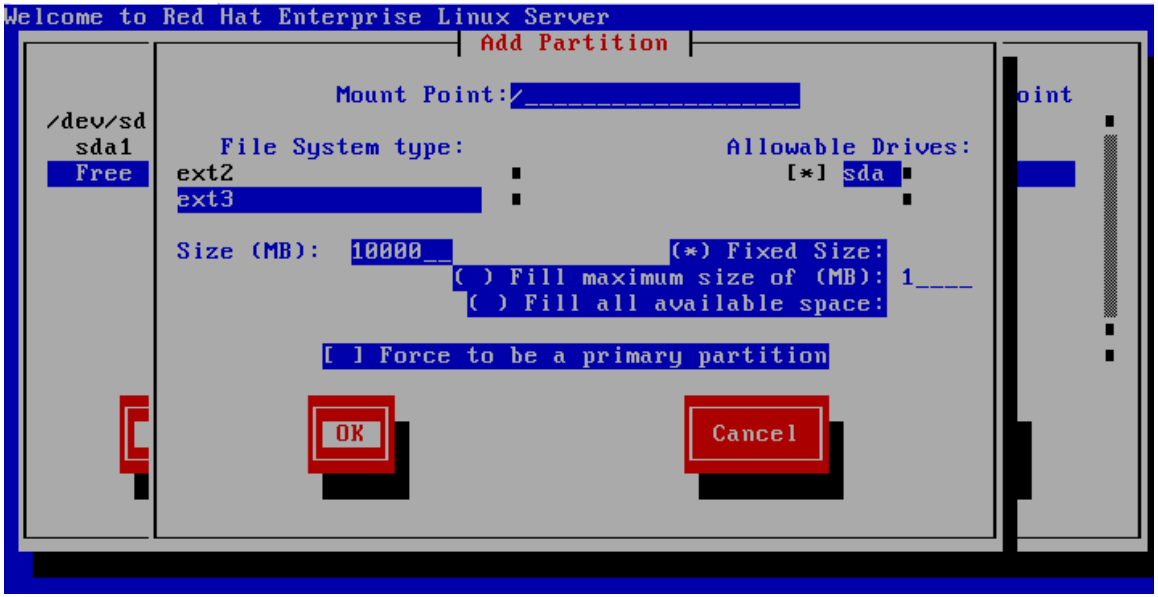


刪除現有LVM格式分割區

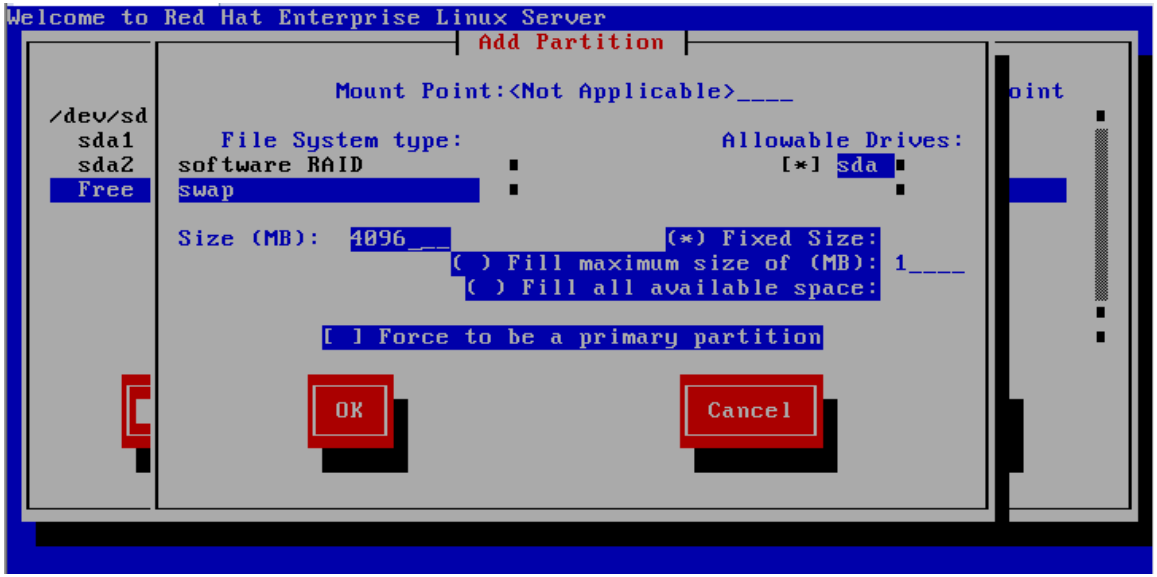


選free space來創建新分割區

主程式安裝(續)

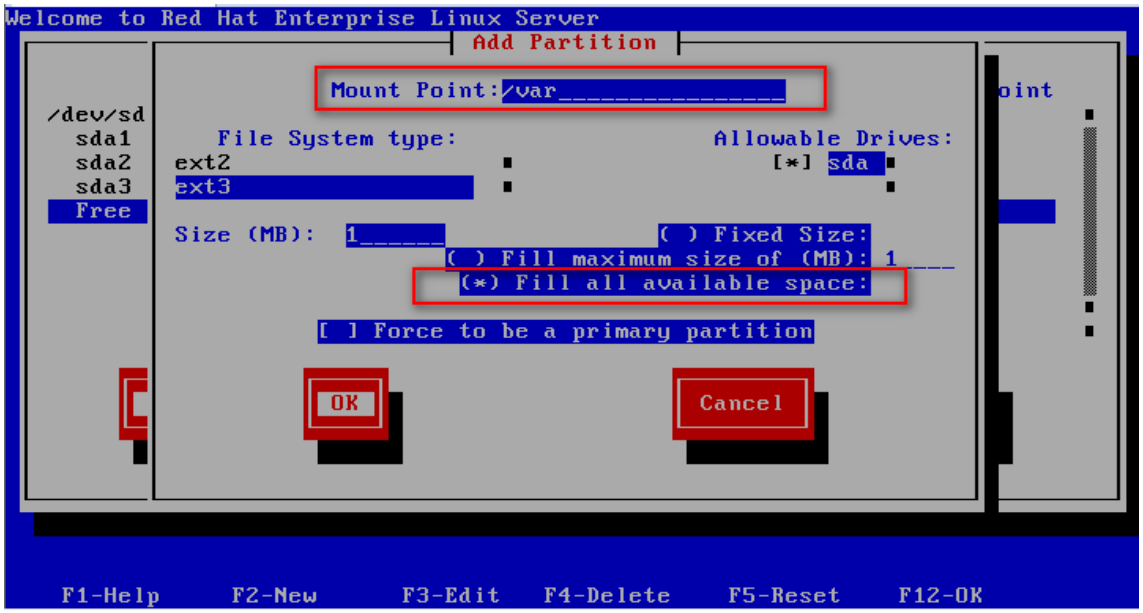


將 / 分割區指定10GB空間,使用ext3檔案格式(目前設定30G)

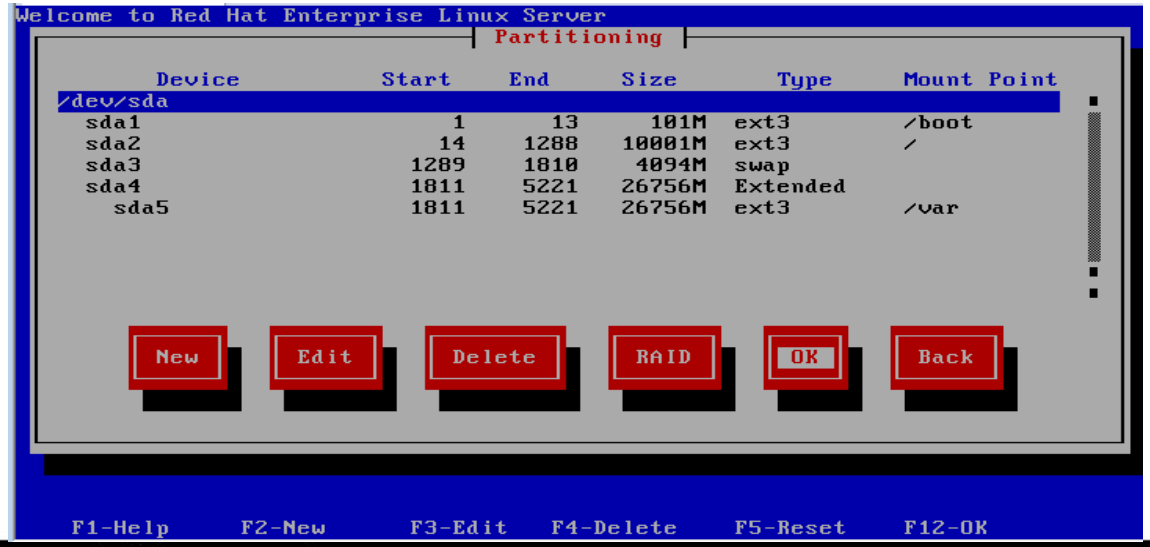


分割swap,指定4GB空間(目前設定20G)

主程式安裝(續)

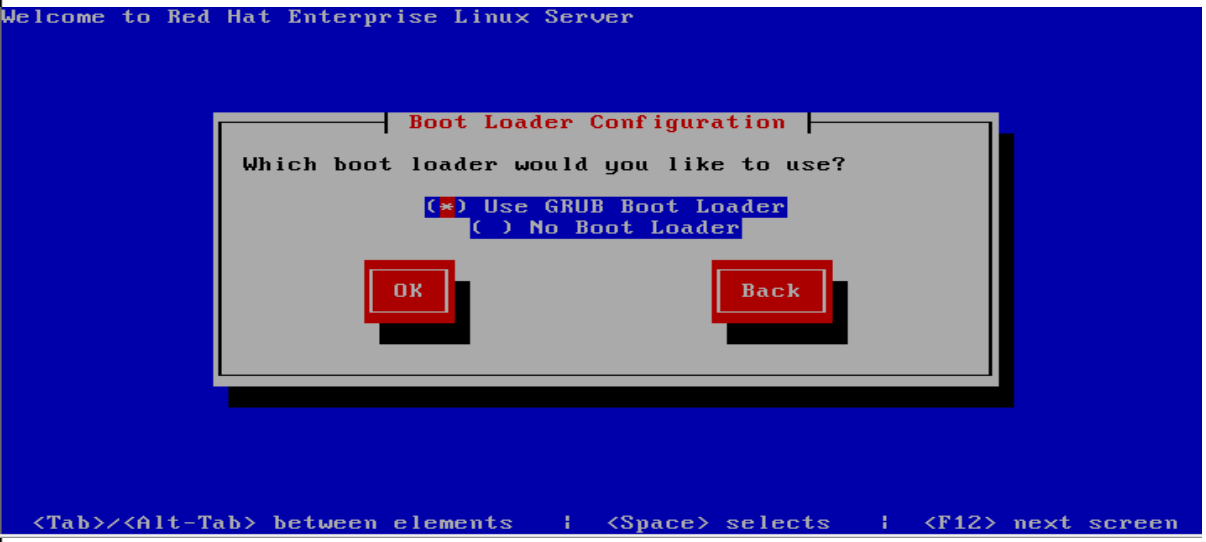


將 /var 分割區指定所有可用空間,使用ext3檔案格式

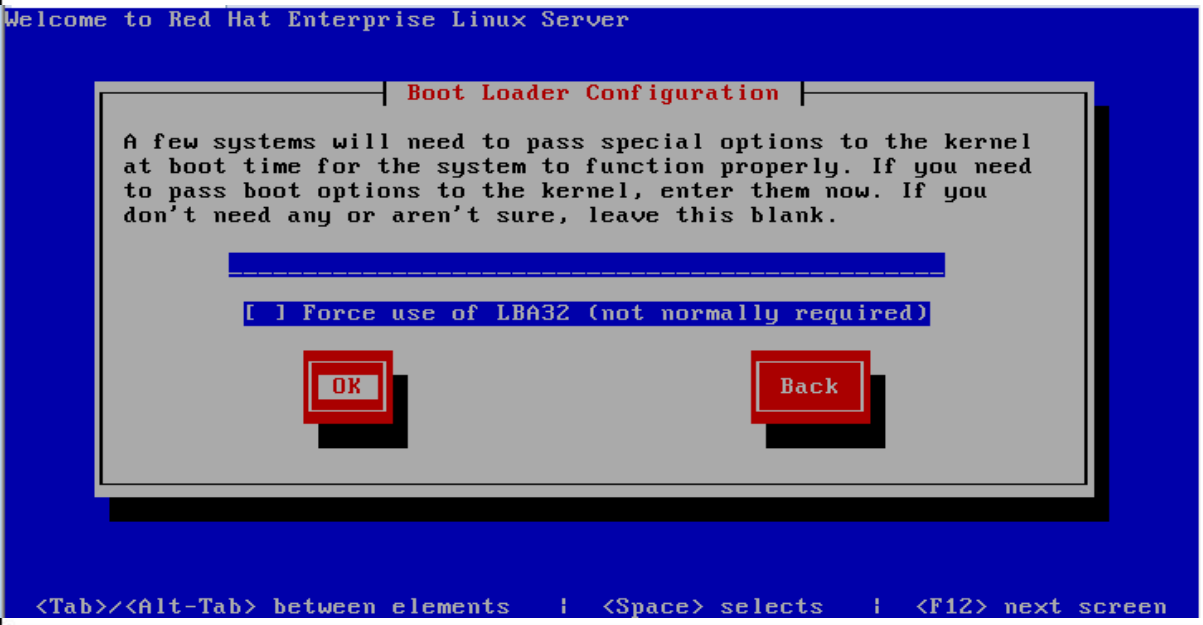


確認一下所有分割區容量無誤

主程式安裝(續)



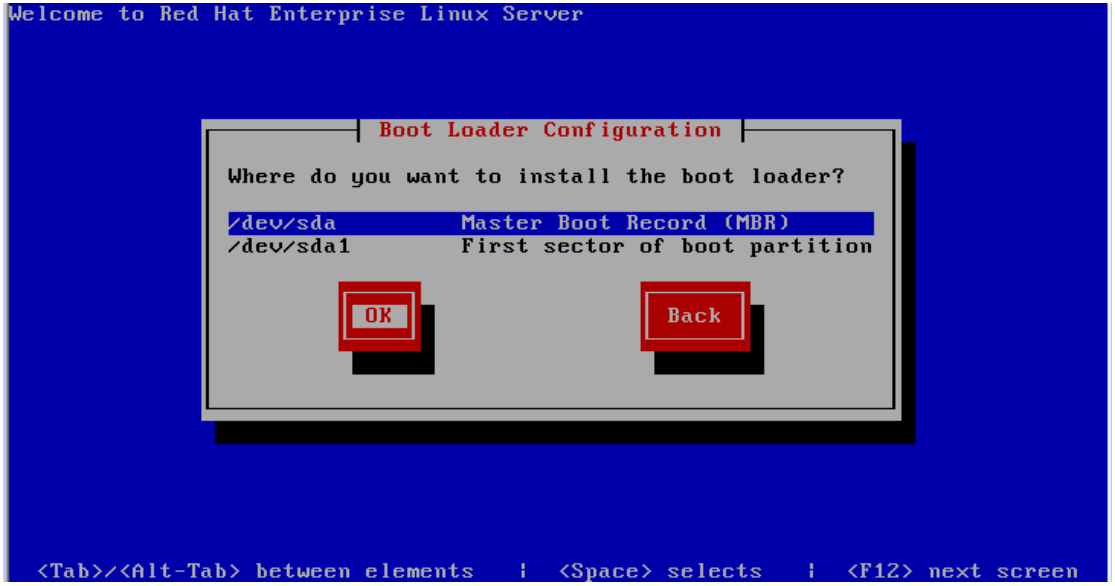
選預設值，直接選ok即可



選預設值，直接選ok即可

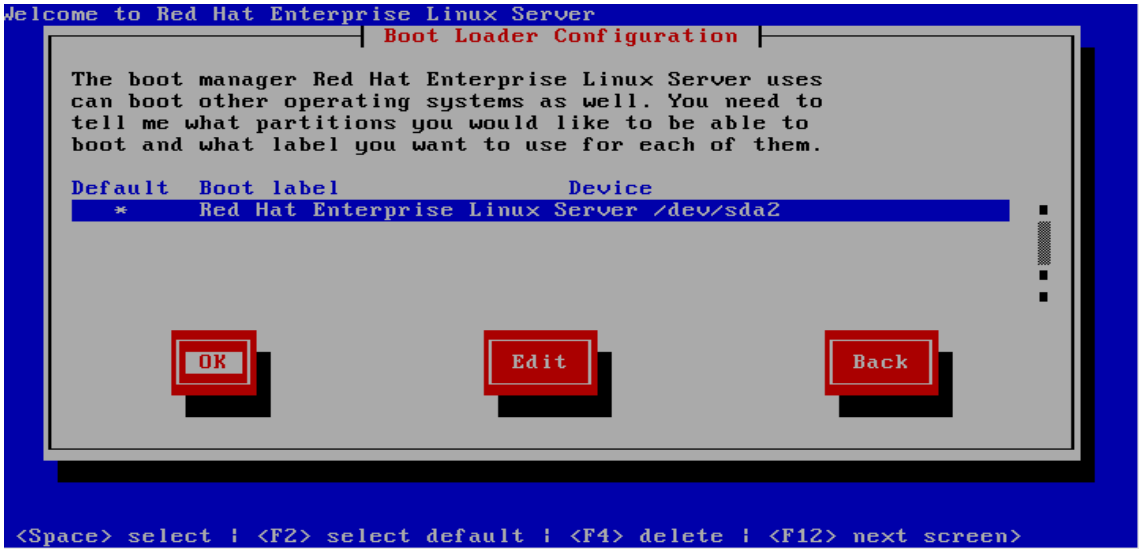
主程式安裝(續)

選預設值, 直接選ok即可

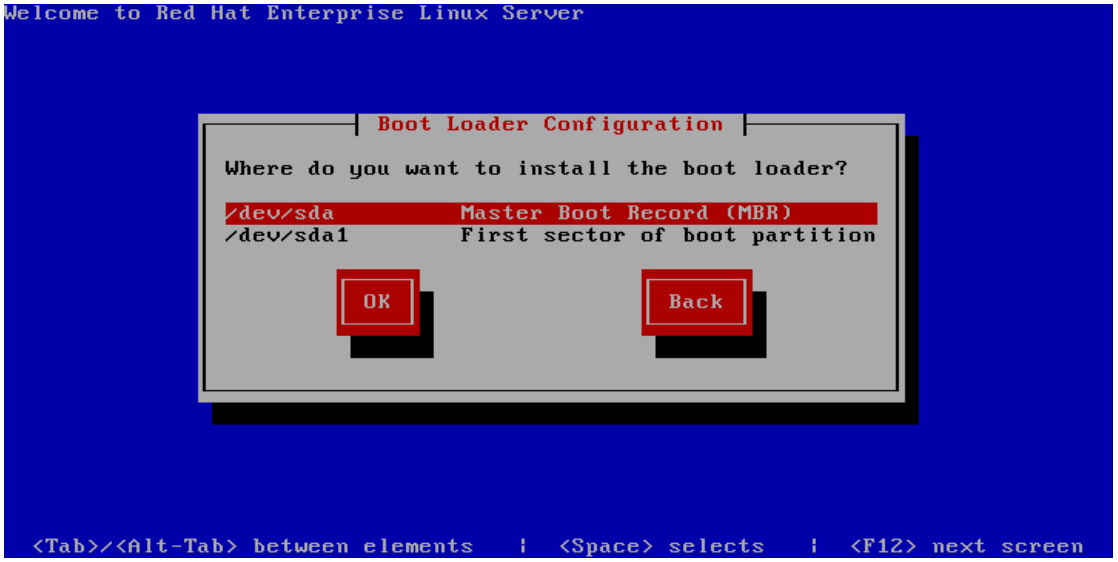


選預設值, 直接選ok即可

主程式安裝(續)

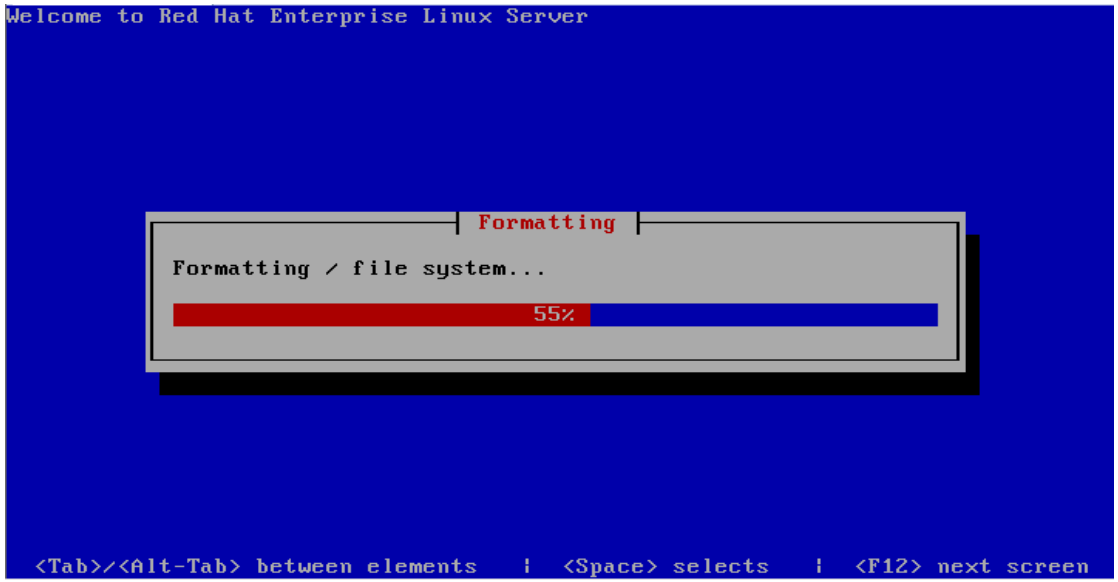


選預設值, 直接選ok即可

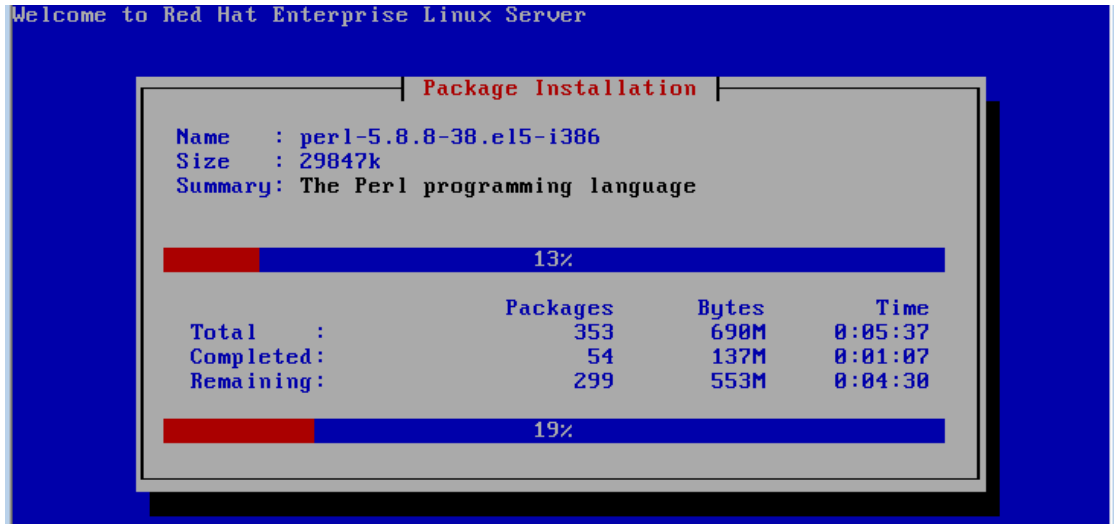


選預設值, 直接選ok即可

主程式安裝(續)

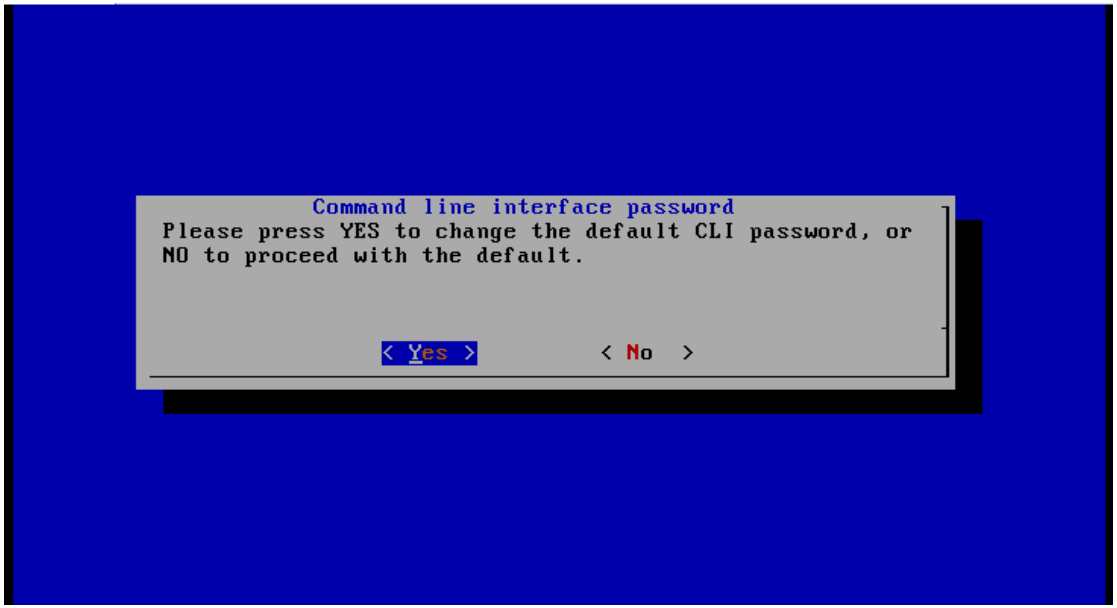


Format Disk中

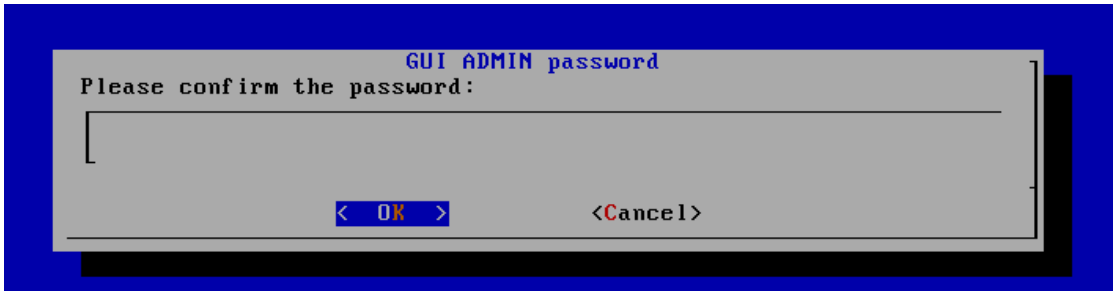


安裝Package

主程式安裝(續)



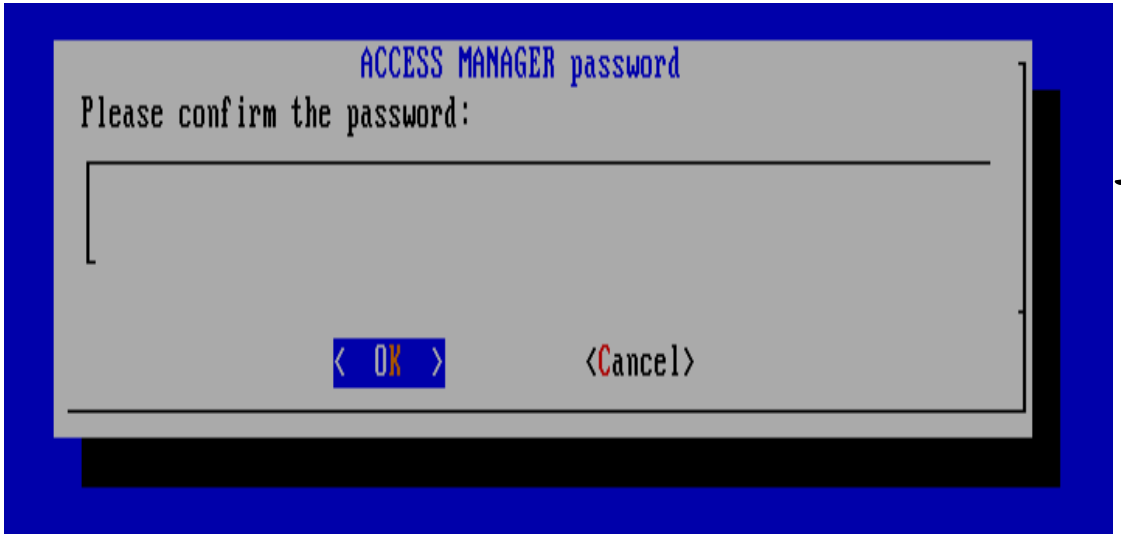
選Yes來更改cli帳號密碼,選No會用預設密碼guardium



若選擇修改,會要求打兩次密碼來確認

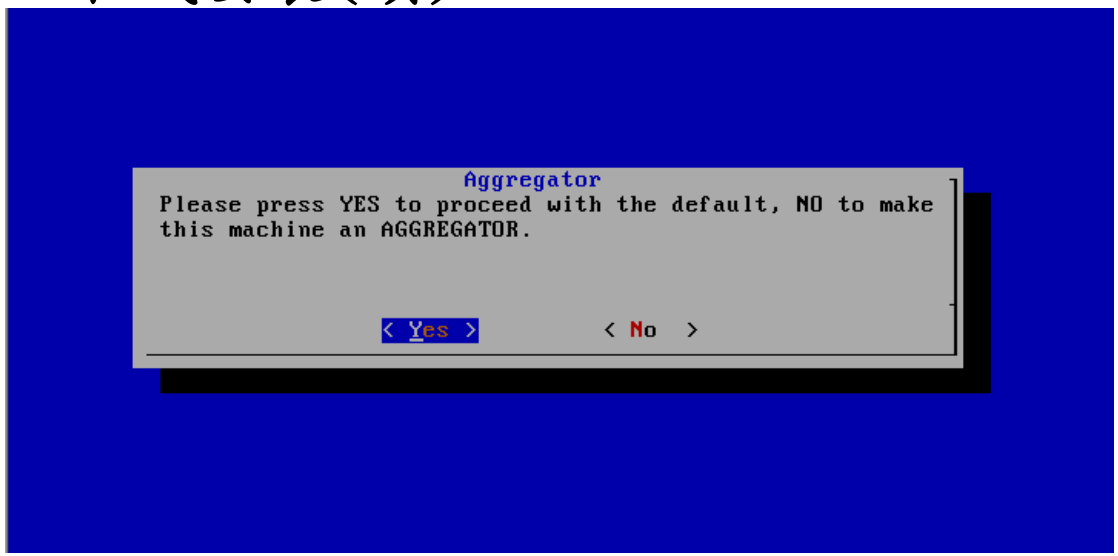
主程式安裝(續)

設定GUI界面的admin帳號密碼,會要求打兩次密碼來確認



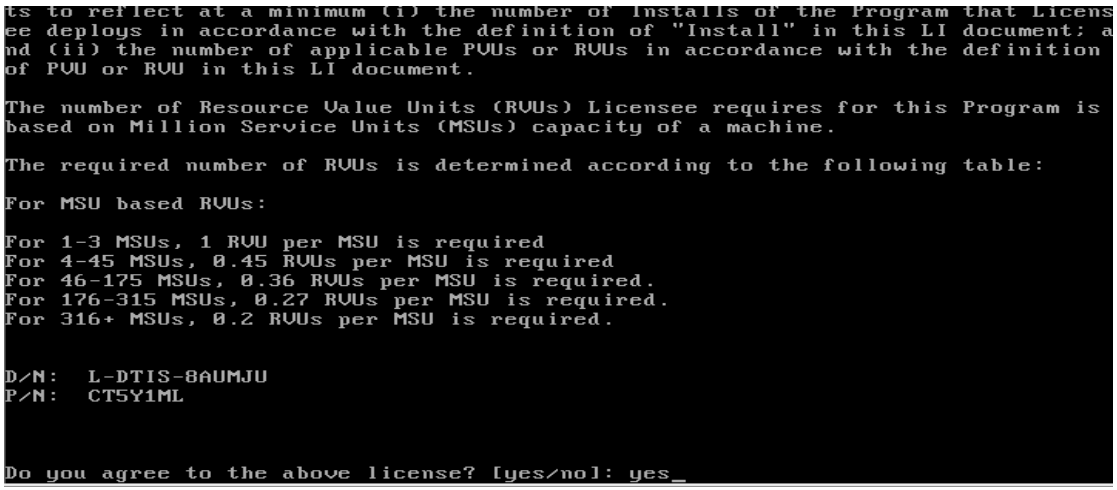
設定帳號管理者accessmgr帳號密碼,會要求打兩次密碼來確認

主程式安裝(續)



設定改主機的角色
YES 為Collector
No 為Aggregator

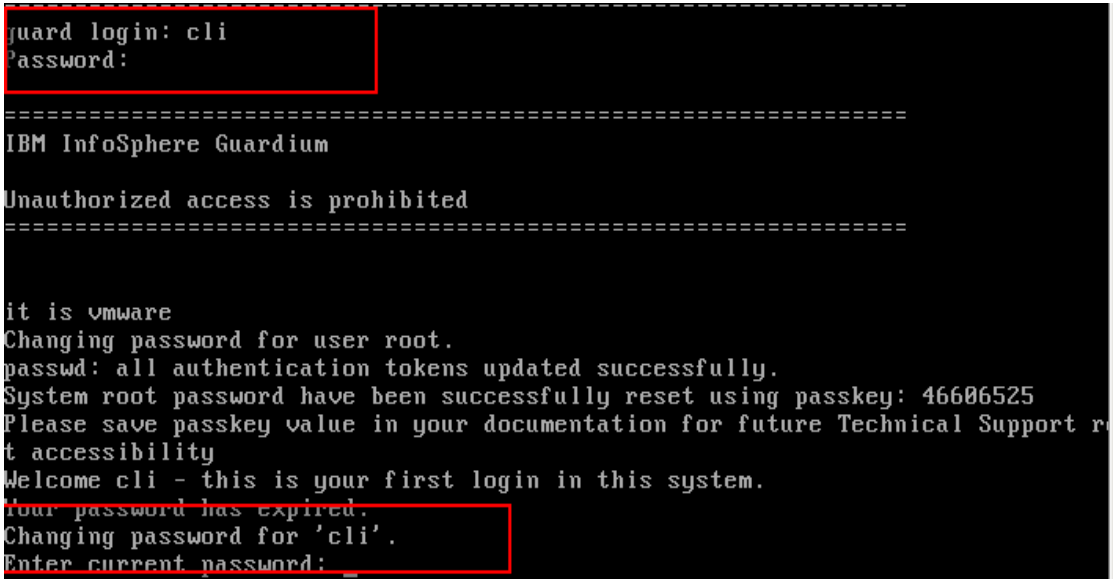
退出光碟片,第一次重開機



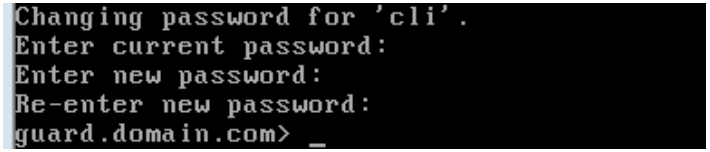
重開機後會出現授權說明,
回答YES接受軟體授權,
系統會第二次重開機

主程式安裝(續)

開機完成, 出現Login畫面進入CLI模式



用cli帳號登入
馬上會要求更改密碼



輸入新的密碼, 若密碼修改完成才會回到cli模式

Guardium基本IP設定

```
vdemop1.1.guardium.com> store network interface ip 10.10.9.242
This change will take effect after the next reboot.
ok
vdemop1.1.guardium.com> _
```

設定本機IP
>store network interface ip xxx.xxx.xxx.xxx

```
vdemop1.1.guardium.com> store network interface mask 255.255.255.0
This change will take effect after the next reboot.
ok
```

設定subnet mask
>store network interface mask xxx.xxx.xxx.xxx

```
vdemop1.1.guardium.com> store network route defaultroute 10.10.9.240
This change will take effect after the next reboot.
ok
```

設定本機閘道
>store network route defaultroute xxx.xxx.xxx.xxx

```
vdemop1.1.guardium.com> store network resolver 2 168.95.1.1
This change will take effect after the next reboot.
ok
```

DNS設定
>store network resolver 1 xxx.xxx.xxx.xxx
[dns1-3] [ip]

```
coll-1.yourcompany.com> store system clock timezone Asia/Taipei
```

系統時區設定為台北,完成後會出現無法連線MySQL DB,不影響
>store system clock timezone Asia/Taipei

設定完後重開機才能生效,執行restart system重開機

Guardium基本設定(續)

重開機網路即可生效,即可由遠端透過SSH方式連線

```
coll-1.yourcompany.com> store system clock datetime 2012-12-06 23:31:30
Thu Dec  6 23:31:30 CST 2012
Clock changed. Please proceed with the 'restart gui' command as soon as
possible in order to complete the process.
ok
```

DateTime設定,設完後執行restart gui
>store system clock datetime yyyy-mm-dd hh:mm:ss

```
ok
coll-1.yourcompany.com> store system host coll-1
ok
```

設定主機名稱
>store system host [host name]

```
coll-1.yourcompany.com> store system domain guardium.com
ok
```

設定網域名稱
>store system domain [domain name]

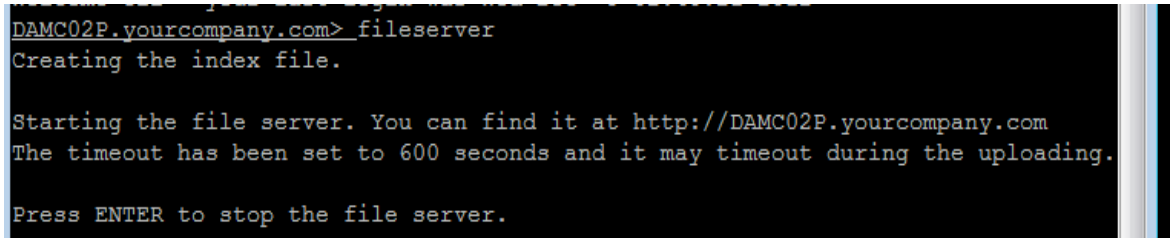
```
coll-1.yourcompany.com> store license console
Please paste the string received from customer services. Then press <ENTER> to c
ontinue.
W1s5OGQwODljMjJmOGNmNmYxNDZmNmJhMzM0ZDYyNmU4Yl1db0pRNh4AAAAAAAAAAAAAACwxLCUsRzIw
MDAgICAgICwtMSwtMSwwLDIwOTktMDEtMDEgMDA6MDA6MDAsMQ==
```

安裝序號
>store license console
系統會重起GUI

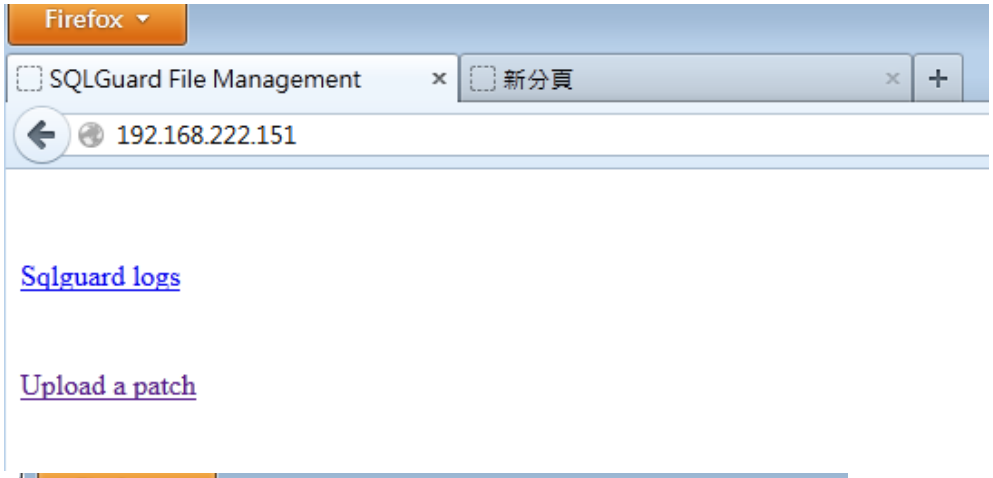
關機指令
重開機 restart system
關機 stop system

IBM Guardium Patch檔更新

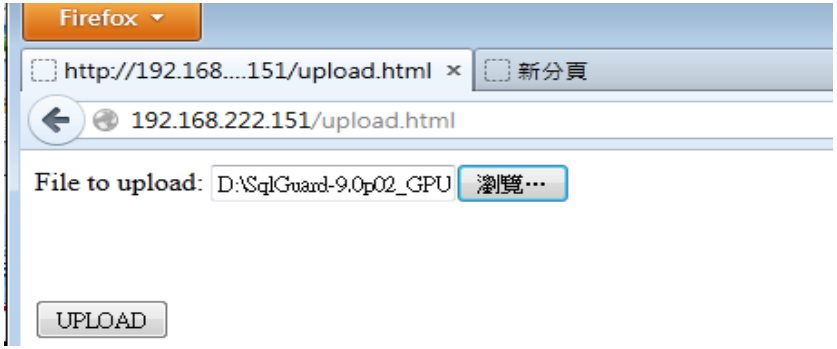
Guardium 更新Patch檔



於cli下執行fileserver會啟動file service



透過瀏覽器 http://IP 選擇upload patch



將欲更新的patch檔sqlguard*.enc檔上傳至主機

Guardium 更新Patch檔（續）

```
DAMC02P.yourcompany.com> fileserver
Creating the index file.

Starting the file server. You can find it at http://DAMC02P.yourcompany.com
The timeout has been set to 600 seconds and it may timeout during the uploading.

Press ENTER to stop the file server.

Stopping process
ok
```

檔案傳輸完成後回到cli下執行ENTER會關閉file service

```
DAMC02P.yourcompany.com> store system patch install sys

The backup profile is not set for saving the backup file when patch installation
 failed.
If you want to save the backup file, please answer "NO" to the question
and run CLI command "store backup profile" to set up the parameters.
Do you want to continue (yes or no)?
yes

List the files in the patches directory:

1. SqlGuard-9.0p02_GPU_October_2012.tgz.enc

Please choose patches to install (1-1, or multiple numbers separated by ",", or
q to quit): 1
```

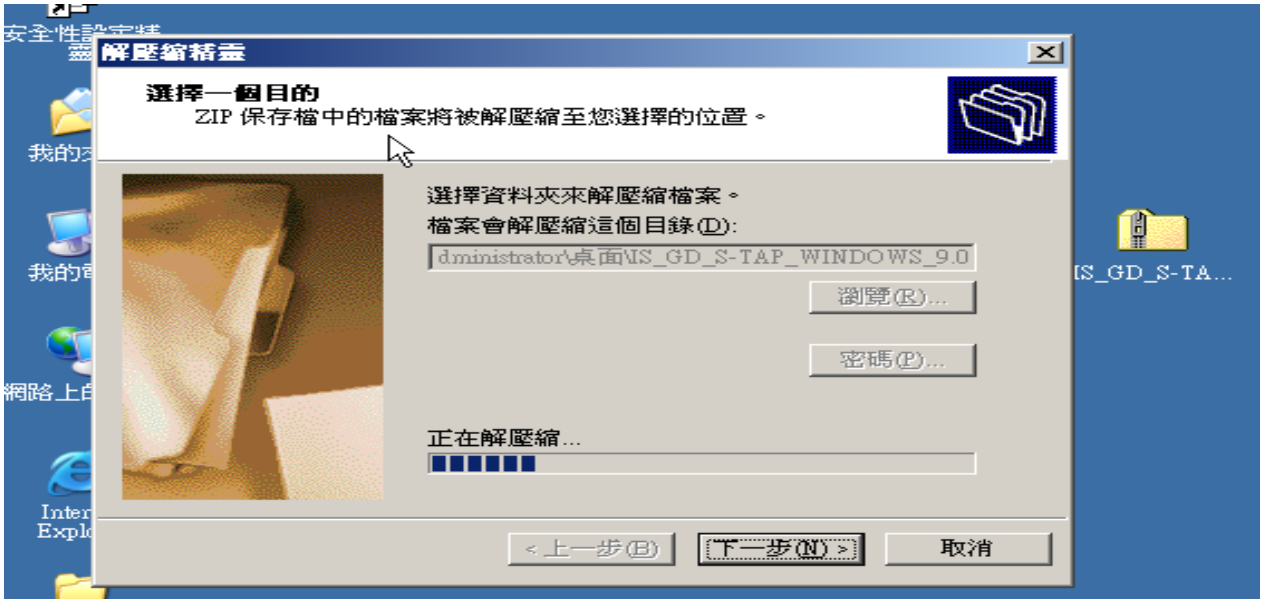
執行store system patch install sys 回答yes後會看到剛上傳的patch檔,選擇要更新的patch檔案,系統開始更新並跳回cli mode

```
DAMC01P.yourcompany.com> show system patch installed
P#      Who       Description                    Request Time         Status
2       CLI       SqlGuard-9.0p02_GPU_October_201 2012-12-04 14:21:46  Preparing
 to install patch.
ok
```

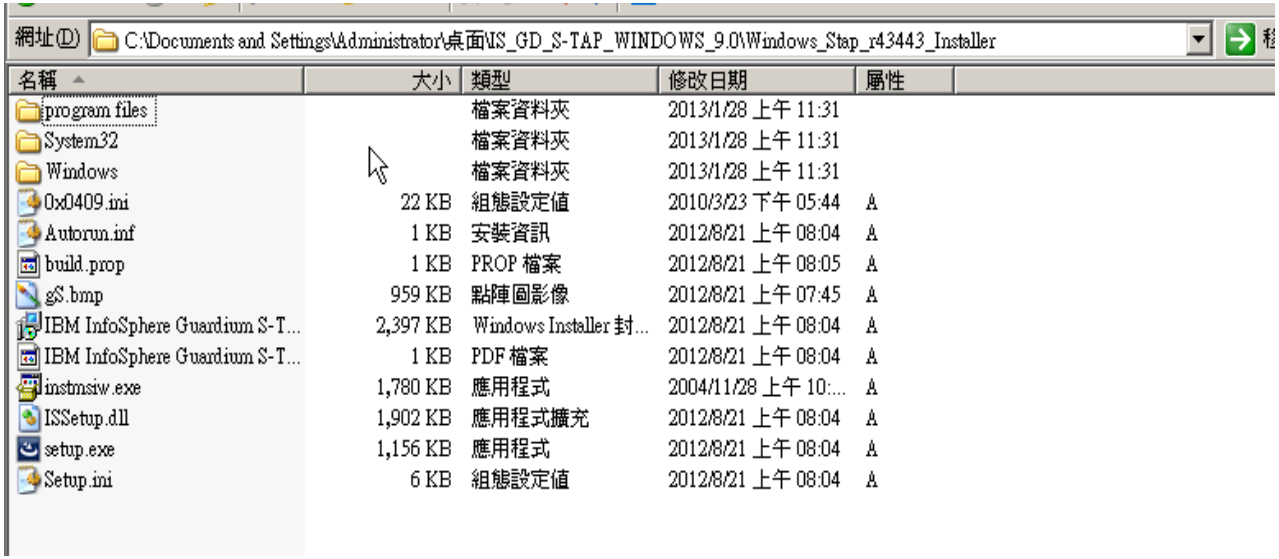
執行show system patch installed 查看更新狀況或已更新之patch檔

IBM Guardium S-TAP For Windows 版安装

Windows 主機安裝STAP

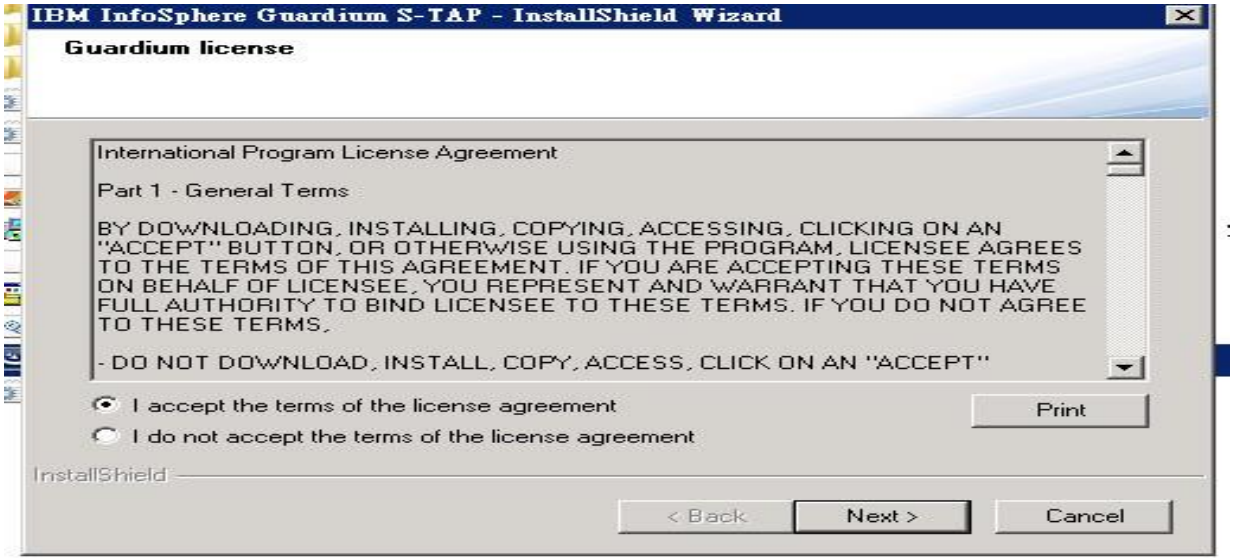


將STAP檔案解壓

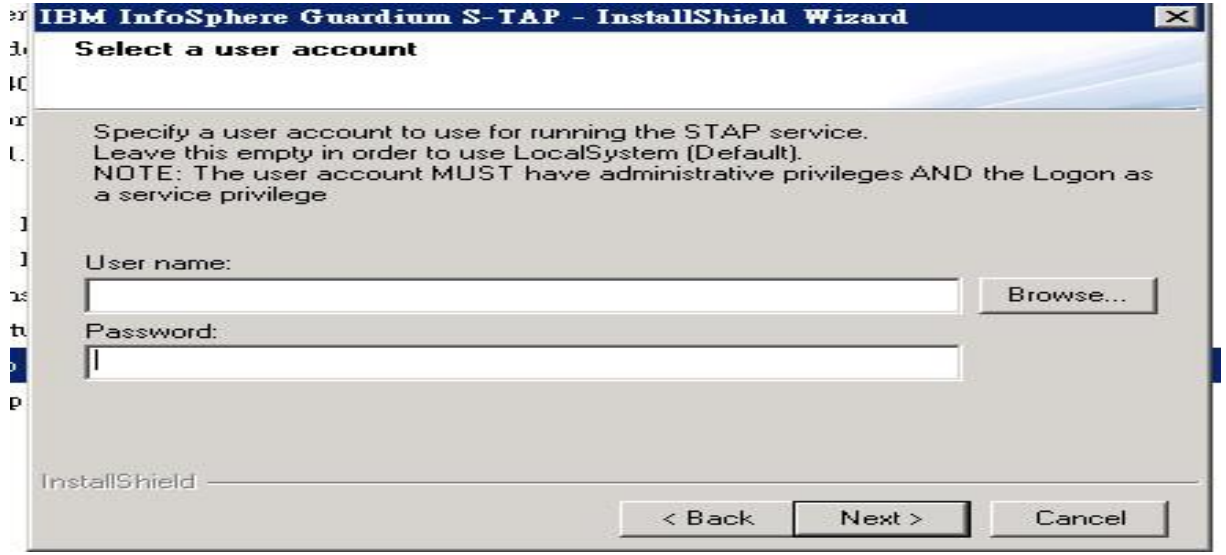


解壓後的檔案

Windows 主機安裝STAP（續）

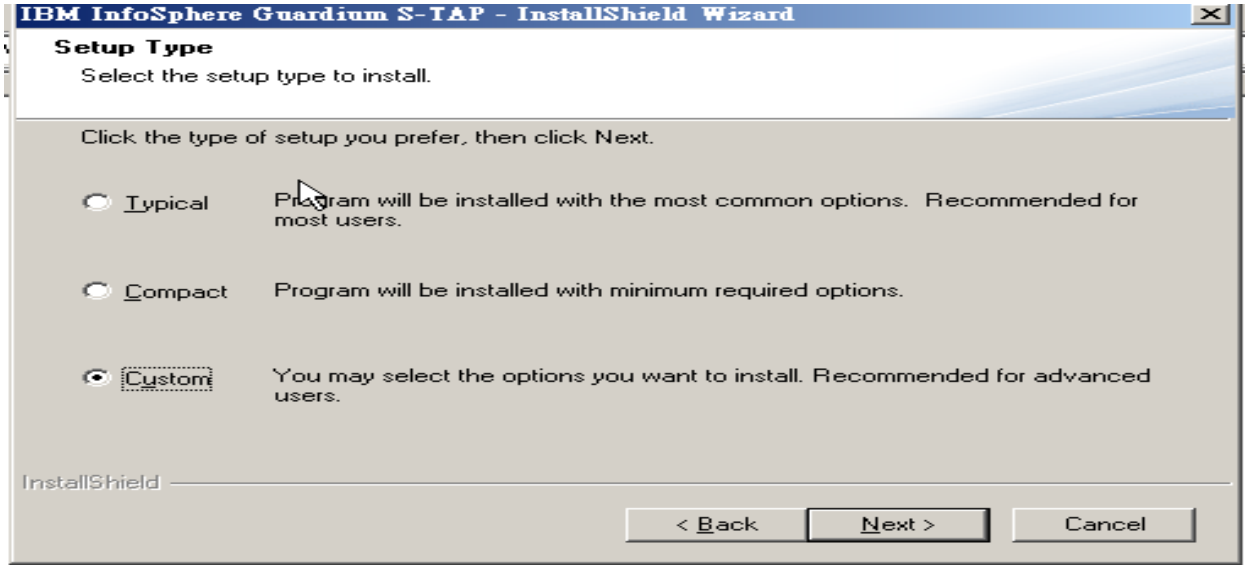


接受軟體授權,下一步

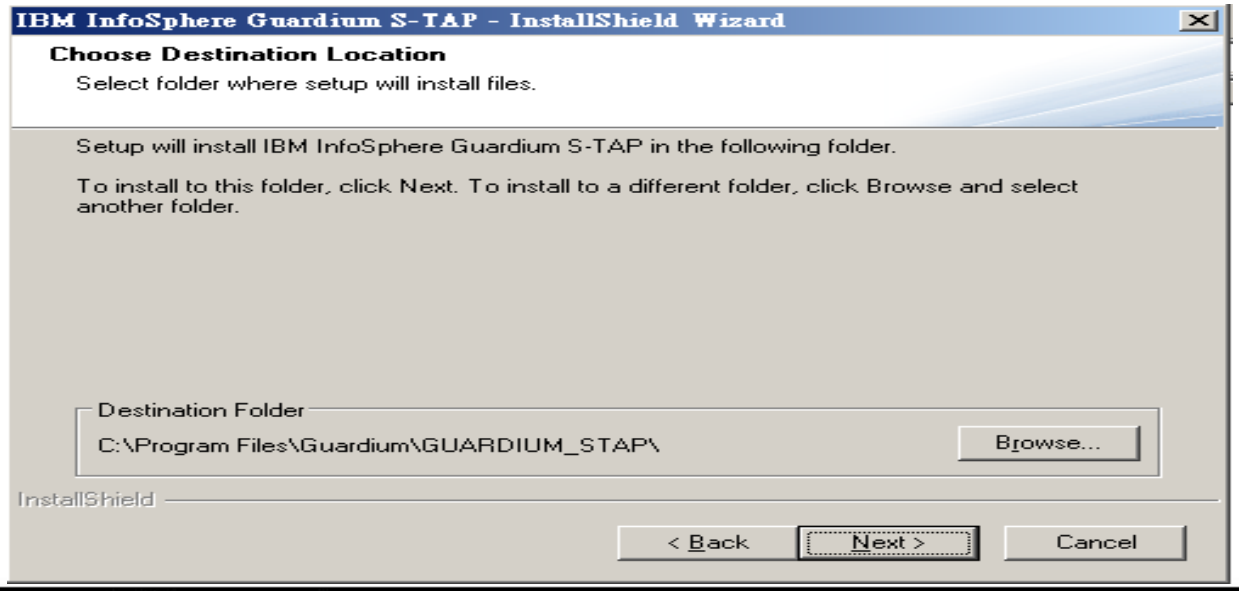


選擇啟動STAP service所使用之帳號,用local system即可,空白不輸入,直接下一步

Windows 主機安裝STAP（續）

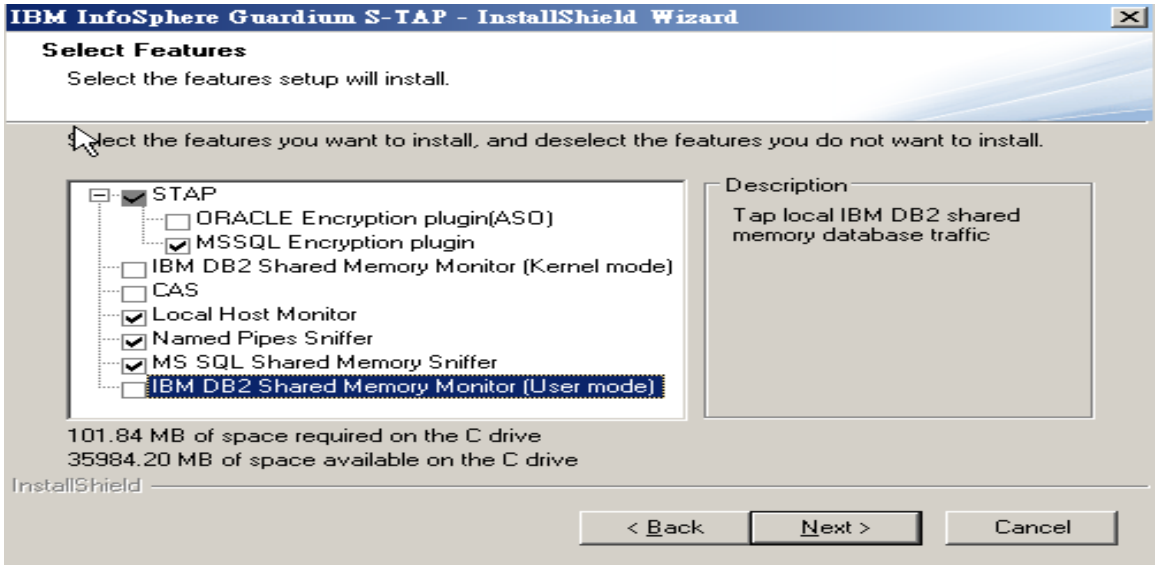


安裝模式,建議選自定,下一步

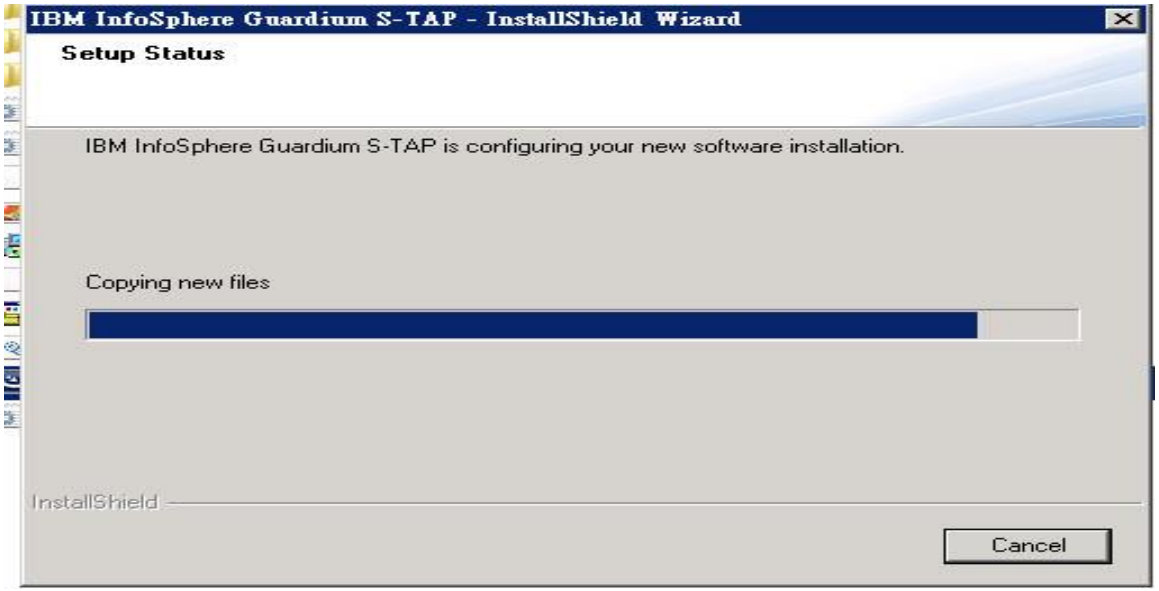


使用預設安裝路徑即可,下一步

Windows 主機安裝STAP（續）



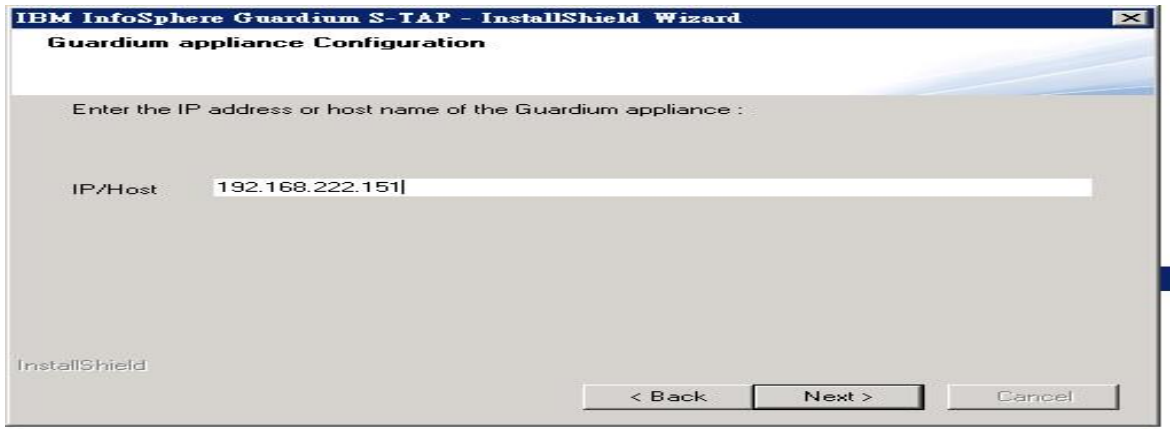
選擇安裝原件,可依欲監控DB種類,選擇安裝項目,CAS建議可不裝(MSSQL為例)



開始安裝軟體

Windows 主機安裝STAP（續）

輸入本機IP



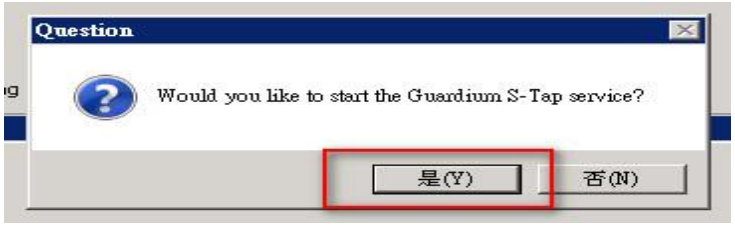
輸入 Guardium Collector 主機IP

若有使用HA模式,回答YES 可指定另一台Guardium IP,若沒有使用HA回答NO

Windows 主機安裝STAP（續）

輸入 Standby Guardium 主機IP

是否還要加其它Guardium主機，已不需要回答No



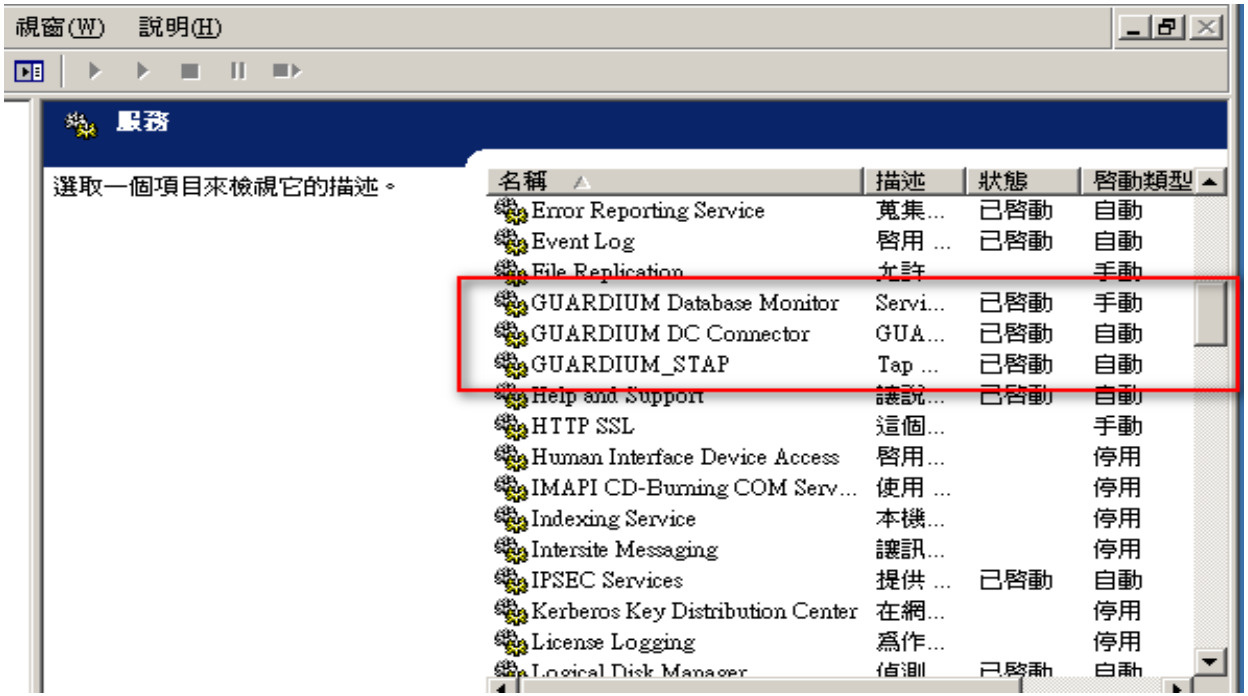
啟動Guardium S-TAP服務

回報設定與服務啟動狀況

Windows 主機安裝STAP（續）

完成安裝

Windows版需重新開機才可收到網路流量

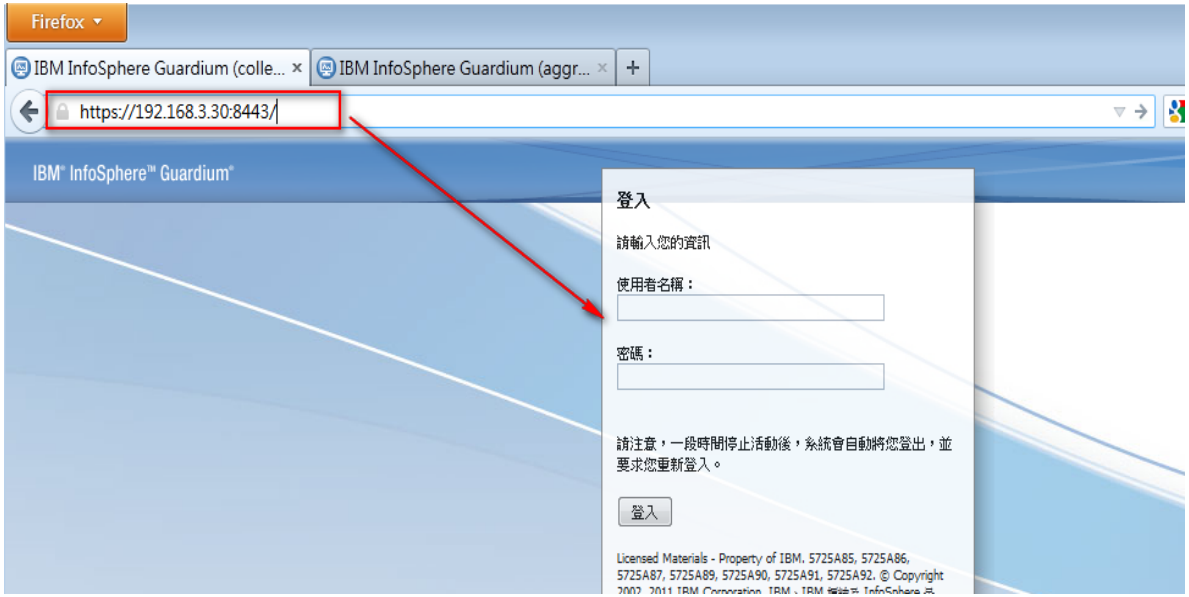


於服務內可看到3條Guardium服務

若要暫停監控可將服務停止

Guardium Collector
S-TAP設定

Guardium 主機登入（Collector）



透過Firefox或IE(另需安裝SVG Viewer)瀏覽器輸入Collector IP

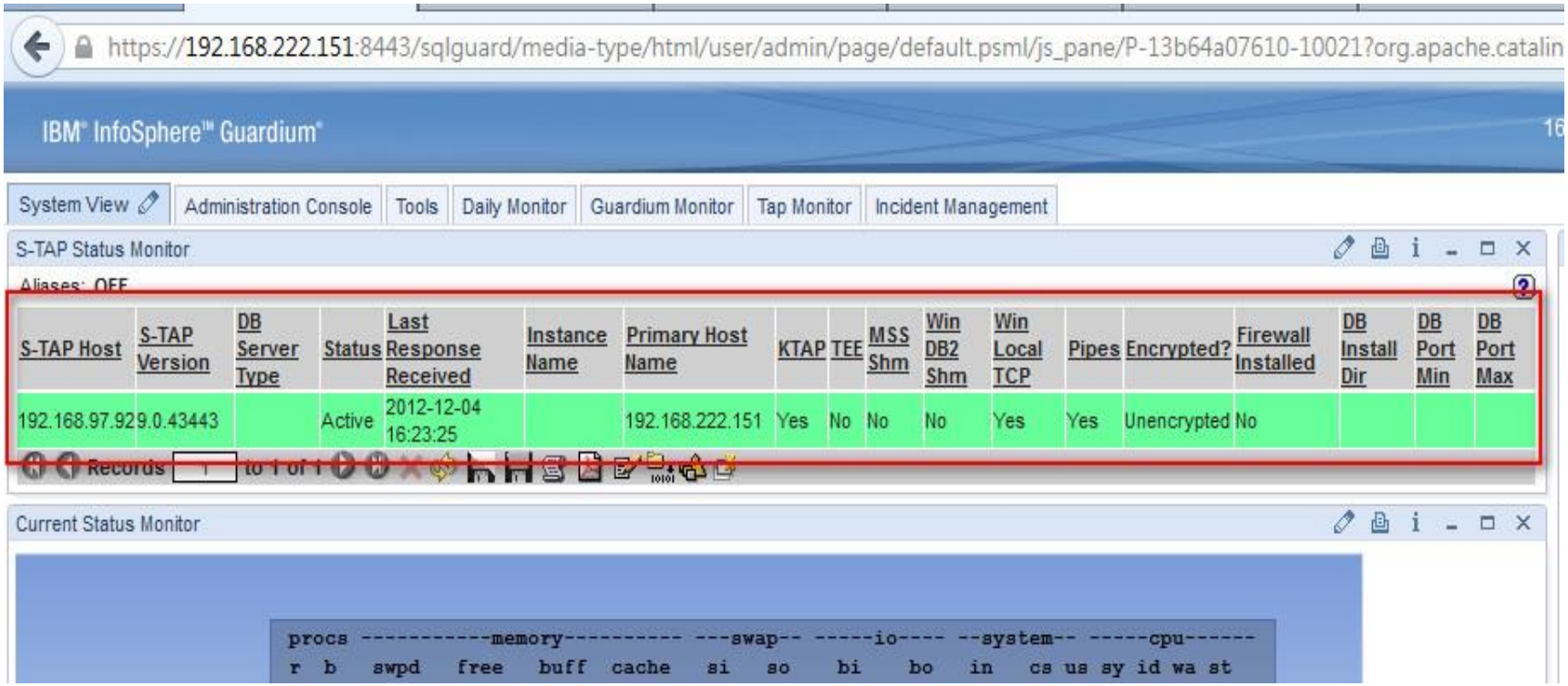
https://IP:8443

輸入登錄帳號

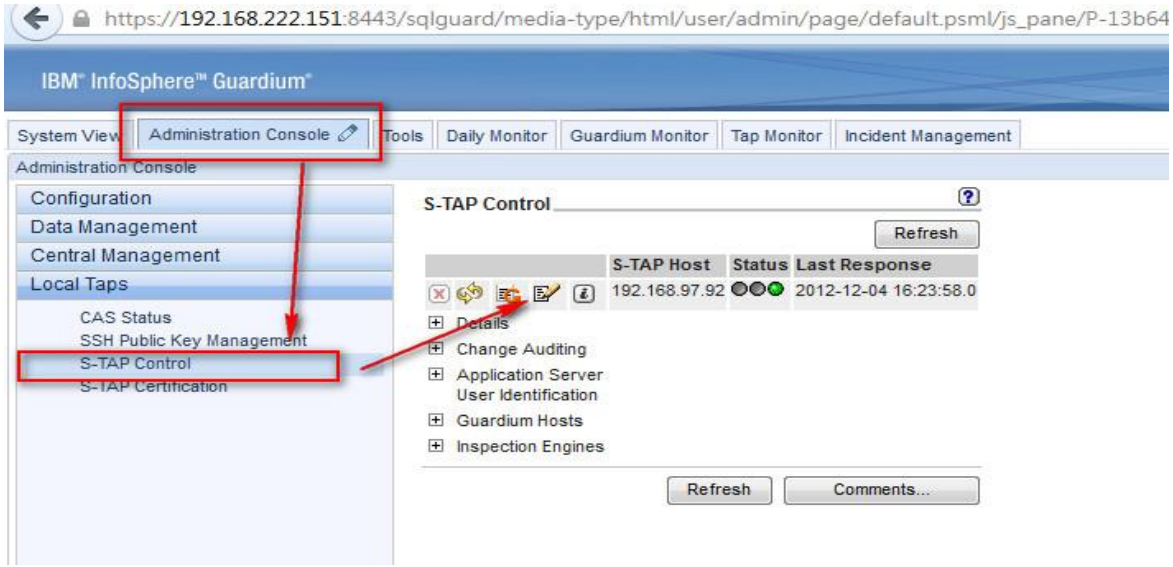
用admin user登入後畫面

Guardium 端S-TAP設定

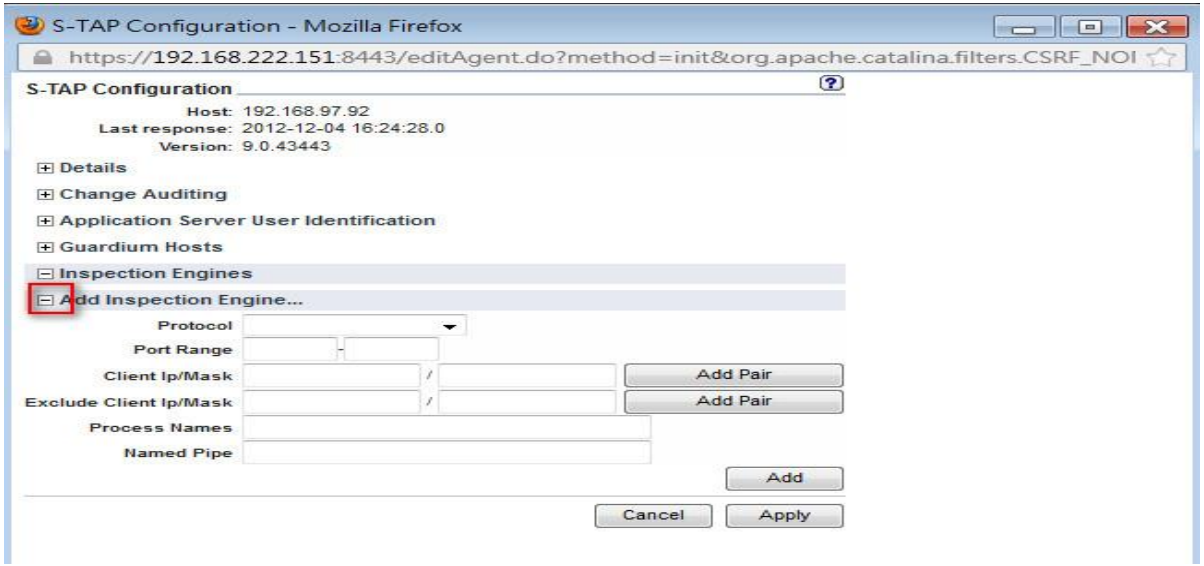
DB端的STAP安裝完後,由Guardium主機上可看到此主機,但另需細部設定



Guardium 端S-TAP設定（續）

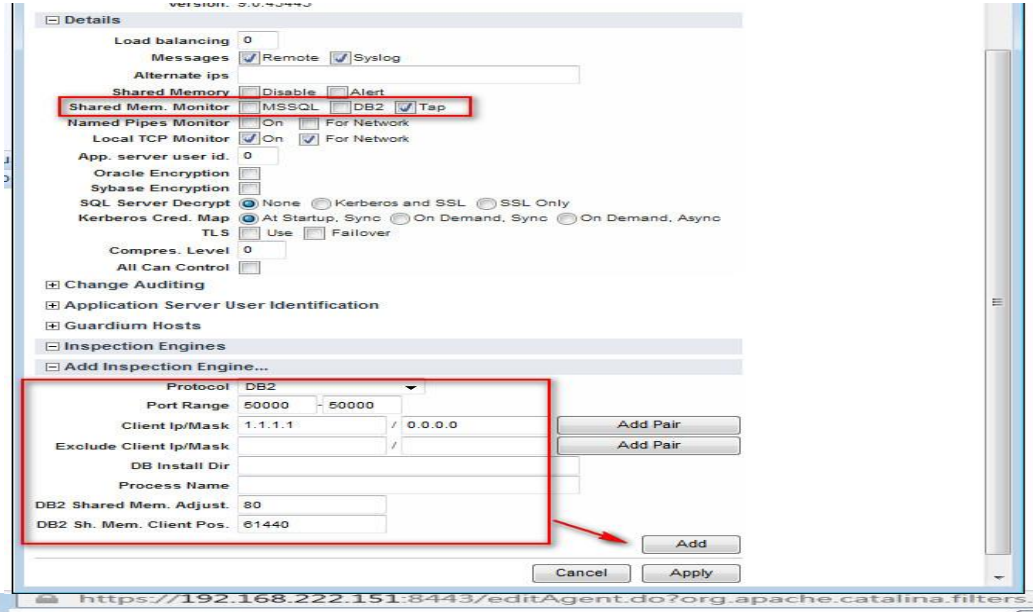


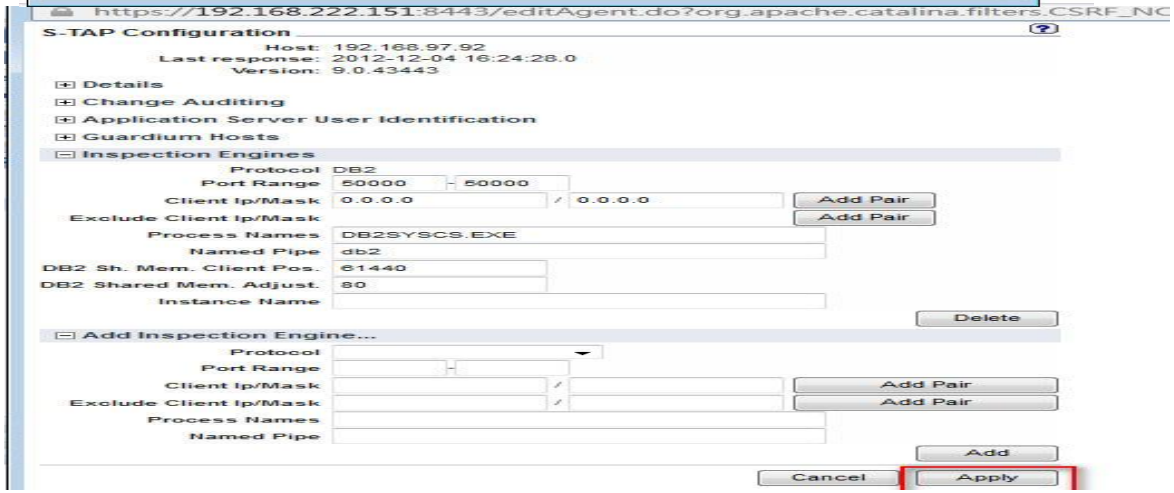
進入S-TAP Control 點選該主機Edit STAP Config



點開Add Inspection Engine, 輸入DB相關資料

Guardium 端S-TAP設定（續）

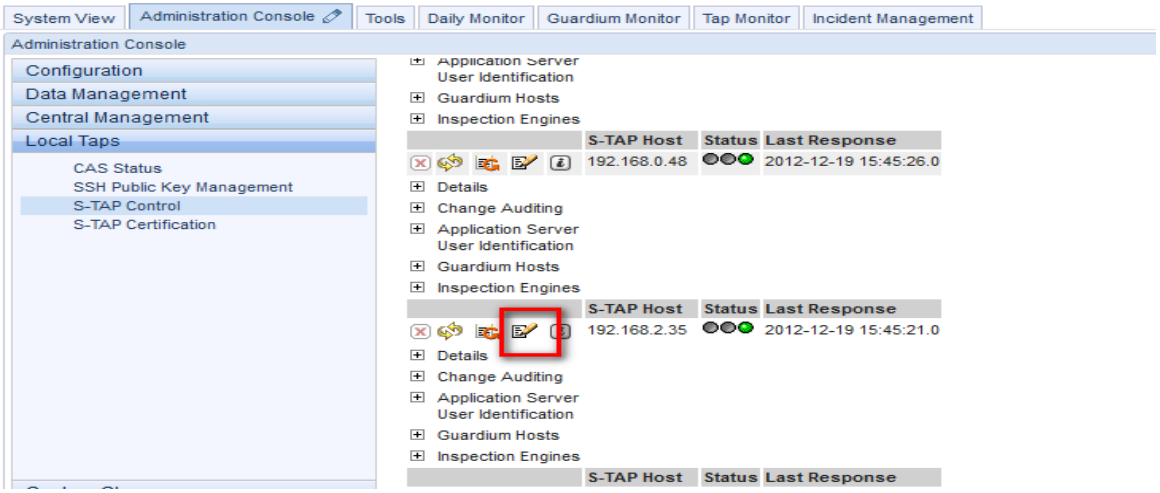




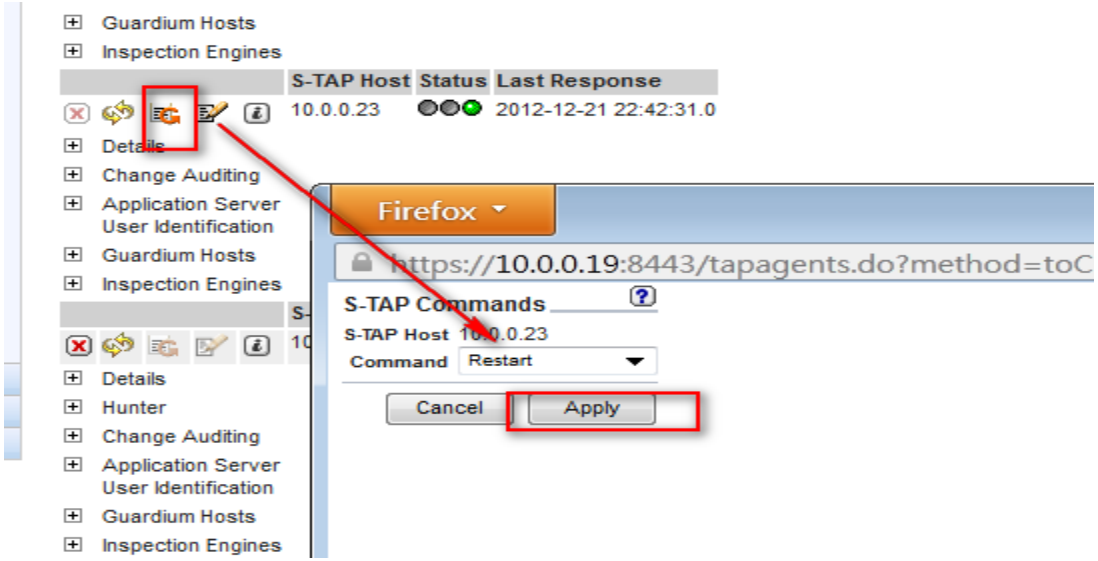
以MSSQL為例
Protocol:DB種類
Port Range:依DB所使用Port
Client Ip/Mask:遠端與本機
一般為0.0.0.0/0.0.0.0
Process Name:MSSQL會自行帶出
或手動輸入
Instance Name:輸入實際使用
名稱
設定完先Add

再新增一欄空白
Inspection Engine
完成後點選Apply
儲存設定

Guardium 端S-TAP設定（續）

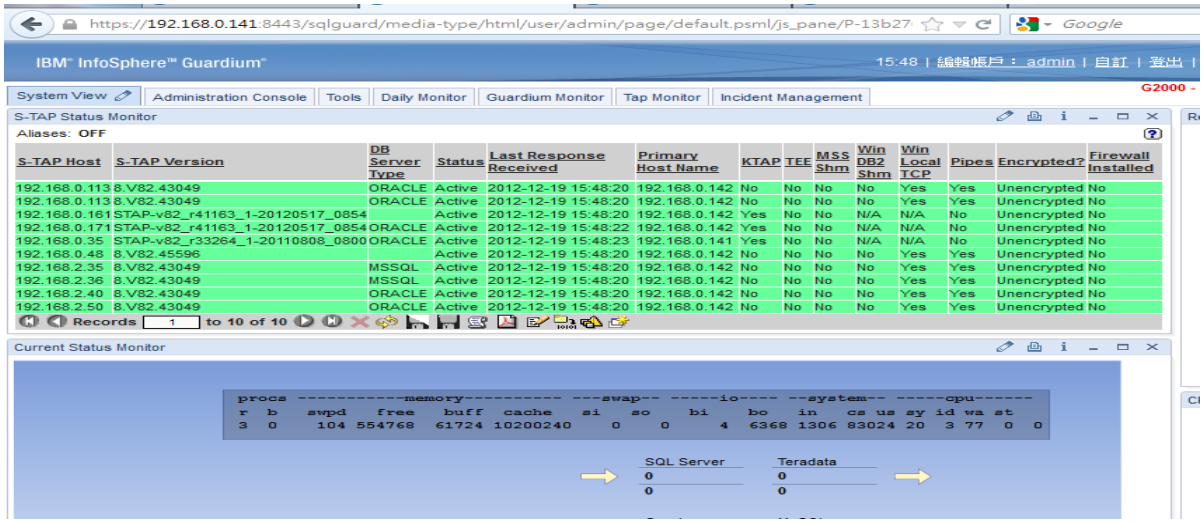


後續若需要修改可再點選該主機,選取”筆”圖示來進行參數設定

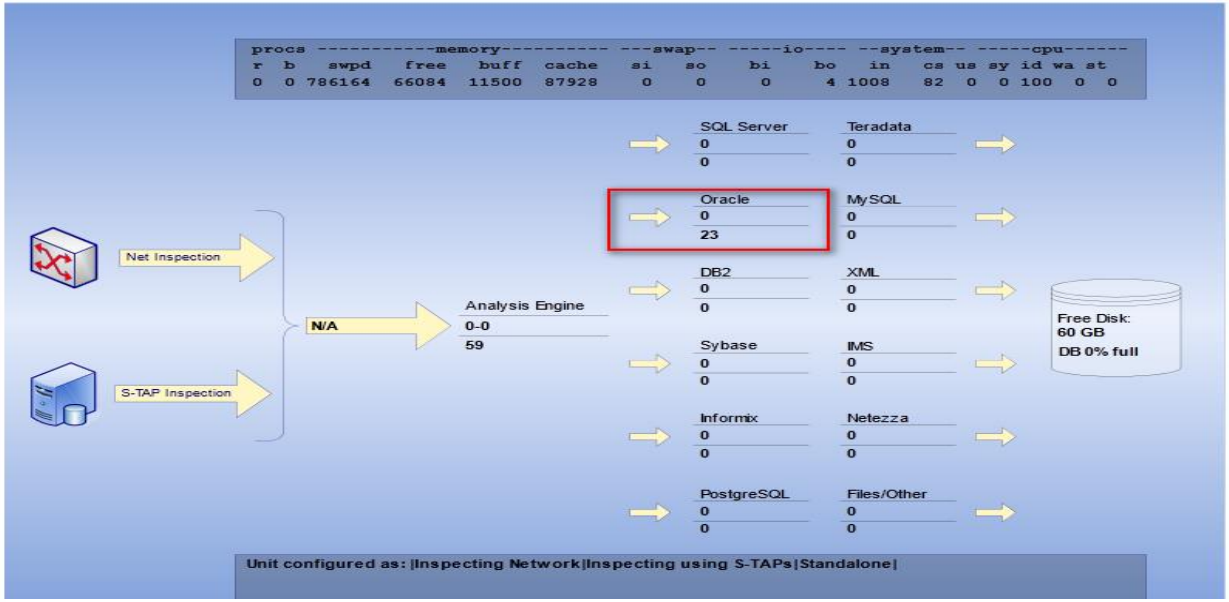


若有修改設定,請重起STAP服務

Guardium 端S-TAP設定（續）

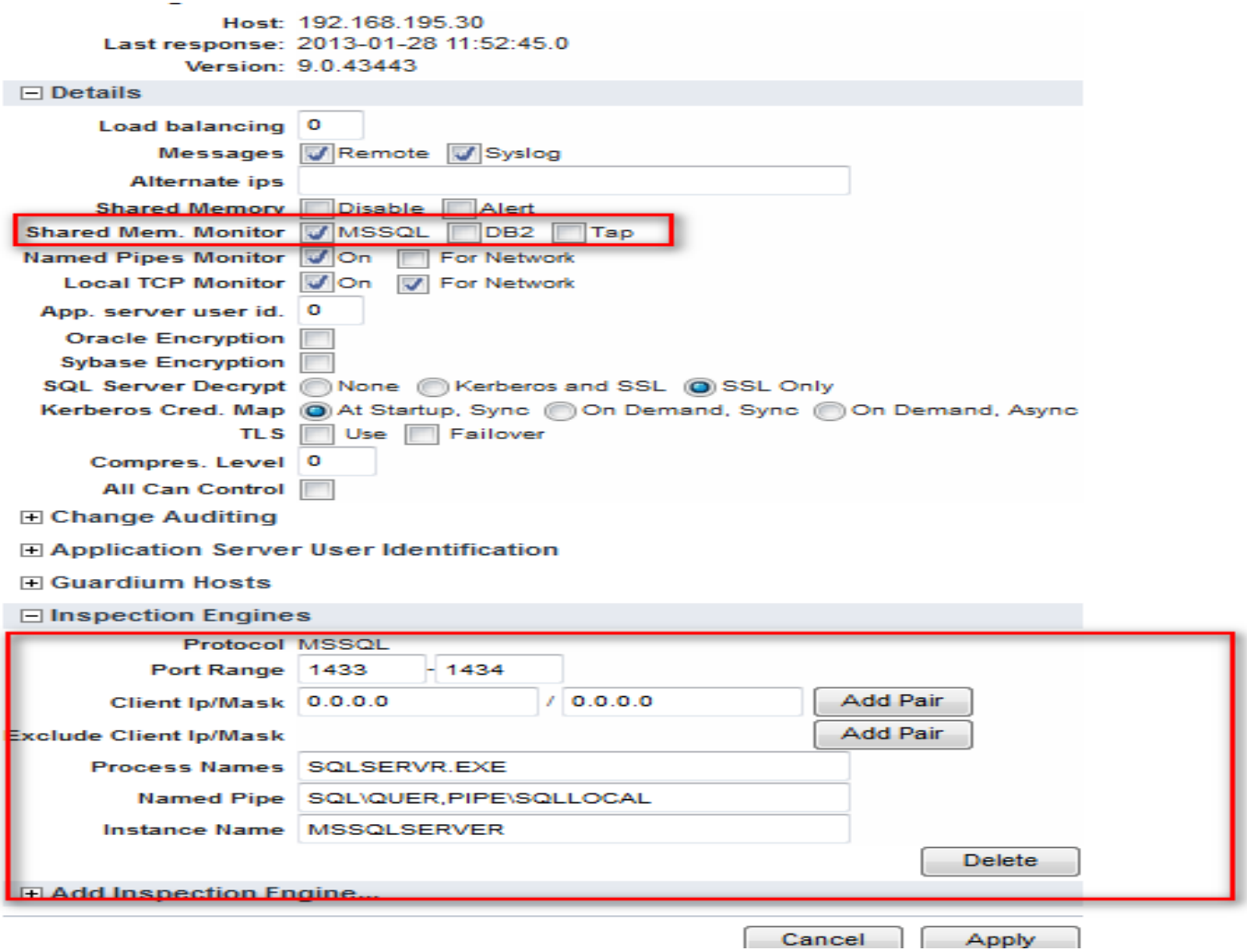


若設定正常，於S-TAP Status Monitor可看到完整訊息

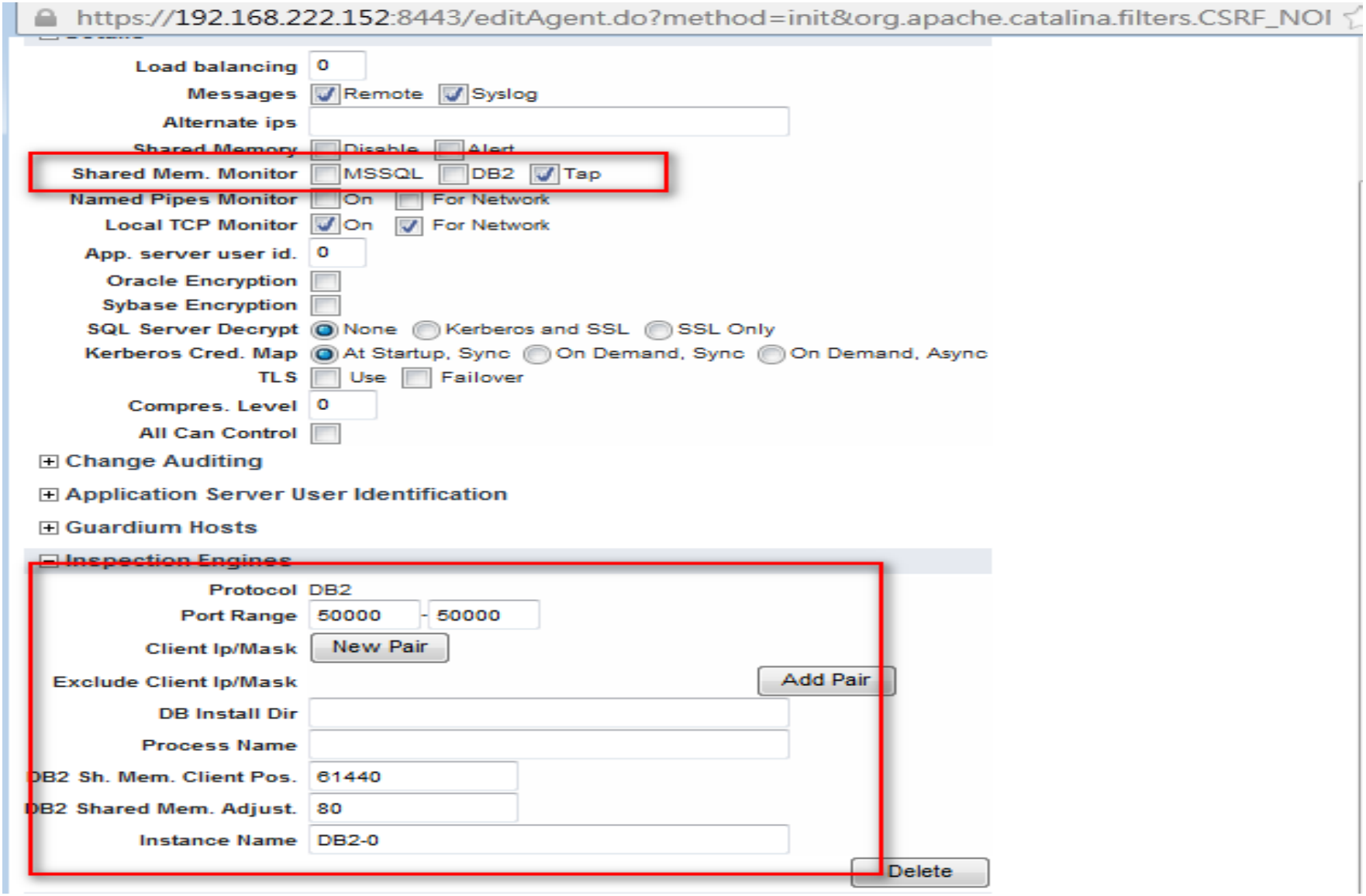


若設定完成，可測試操作DB，是否有流量進入：
下方依DB種類區分
下排流量數字會增長，
上排為待處理流量

現有STAP (S-TAP Control) MS SQL 設定值



現有STAP (S-TAP Control) DB2 設定值



Q & A 問題與討論