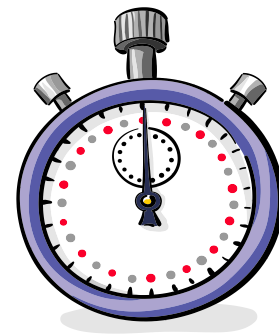


# IBM Guardium 教育訓練 基本安裝

泰鋒電腦 洪禮育

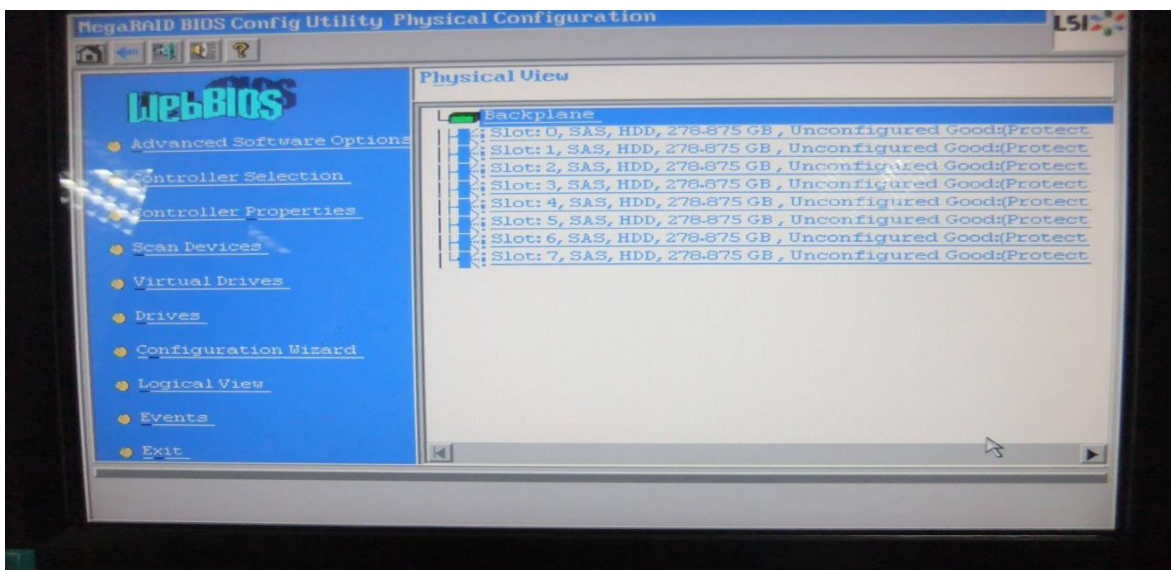
# 簡報綱要

- ❖ 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

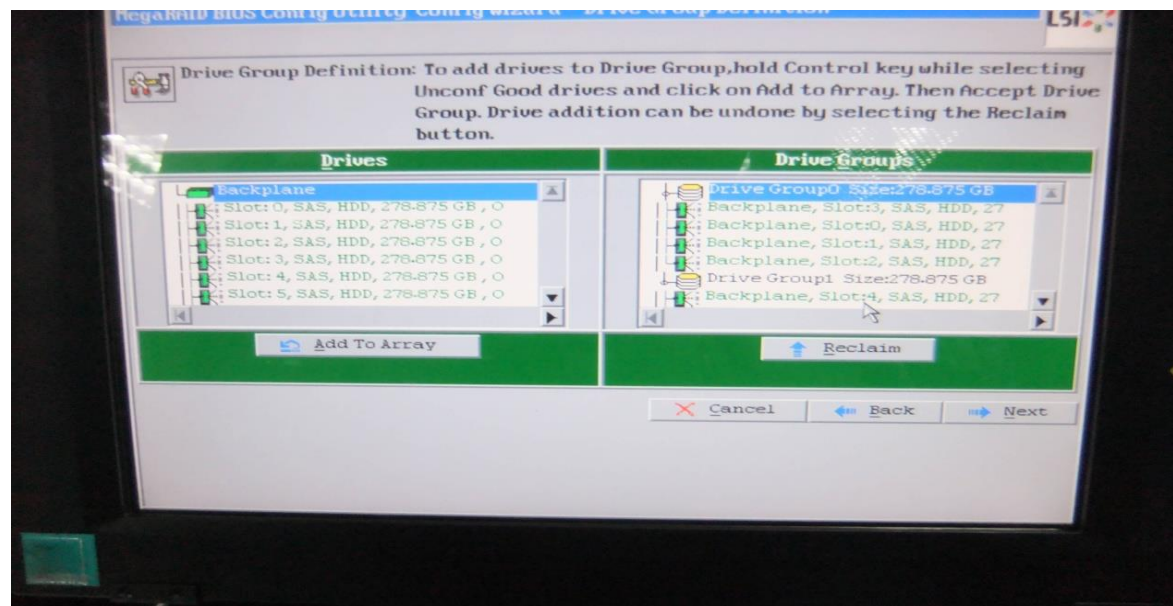


# IBM X3650 M4 Raid建立

# IBM主機Raid建立

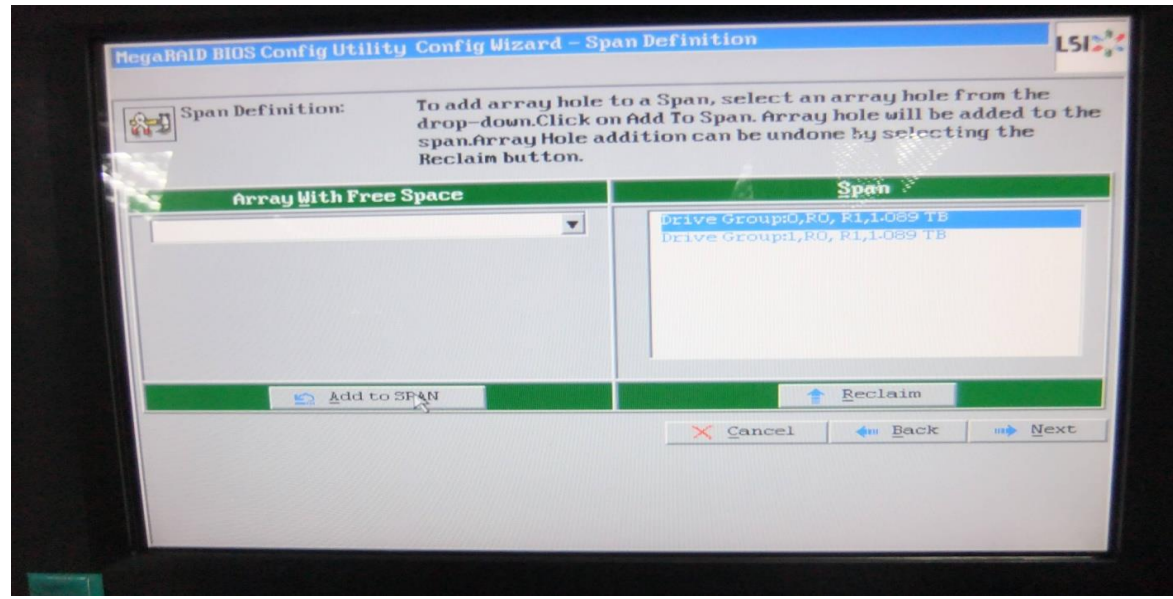


預設8顆未設定  
硬碟

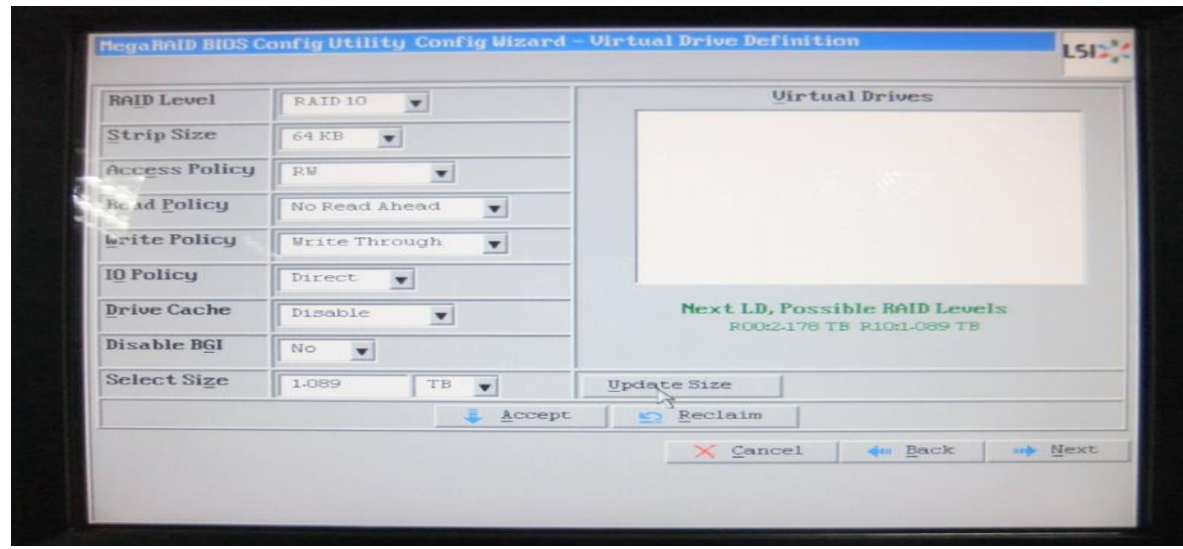


設定2個Disk group  
Disk 0-3為Disk Group0  
Disk 4-7為Disk Group1

# IBM主機Raid建立 (續)



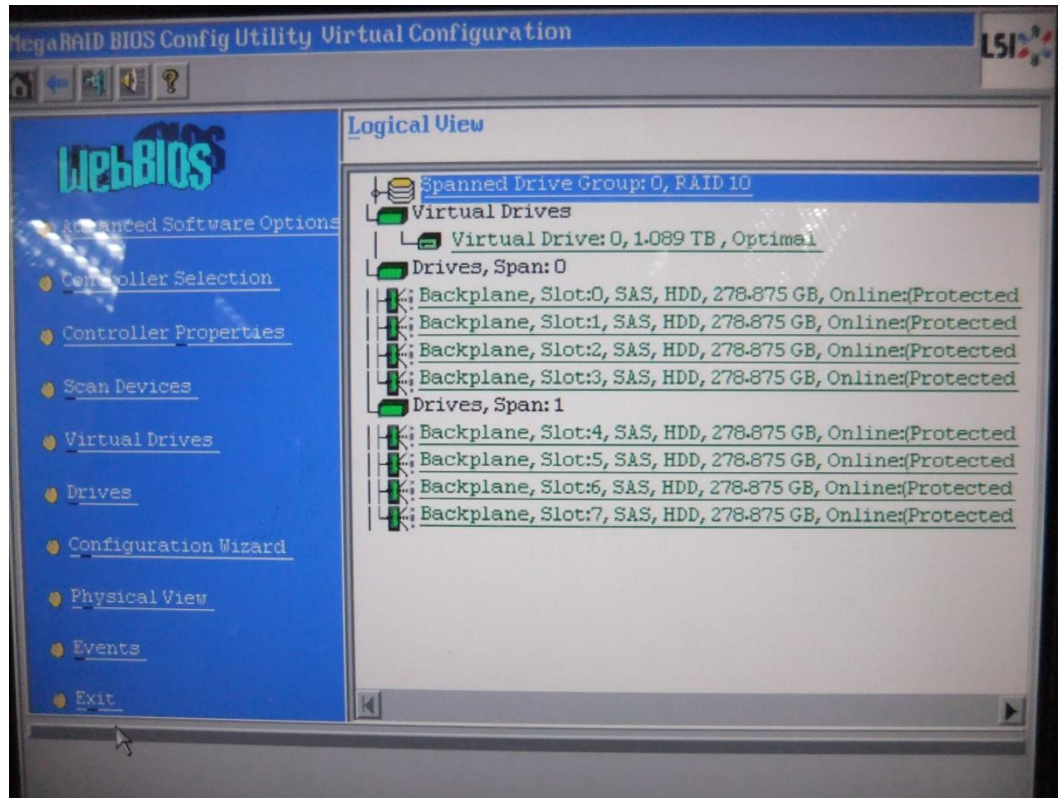
選擇兩個  
Disk Group



選擇為Riad 10  
Update Size為  
1.089TB後確認



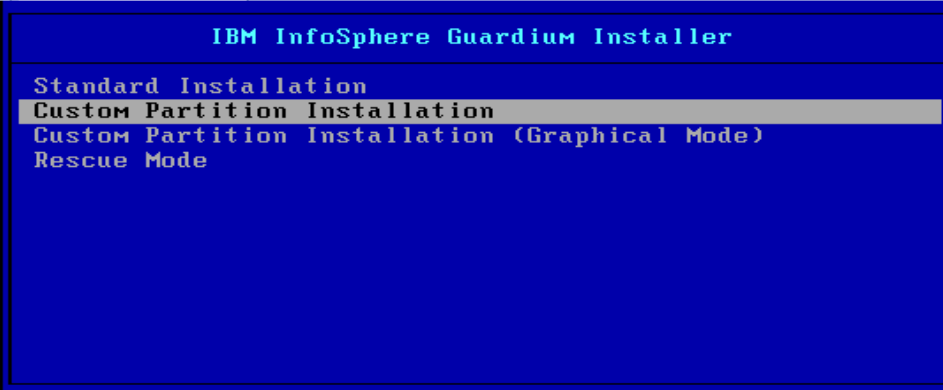
# IBM主機Raid建立 (續)



確認Raid 10  
設定完成  
重新開機

# IBM Guardium 主程式安裝

# 主程式安裝



Press [Tab] to edit options

放入光碟片，由  
光碟機開機，使  
用自定安裝

Welcome to Red Hat Enterprise Linux Server

### Warning

The partition table on device sda  
(UMware, UMware Virtual S 40955  
MB) was unreadable.  
To create new partitions it must  
be initialized, causing the loss  
of ALL DATA on this drive.

This operation will override any  
previous installation choices  
about which drives to ignore.

Would you like to initialize this  
drive, erasing ALL DATA?

Yes

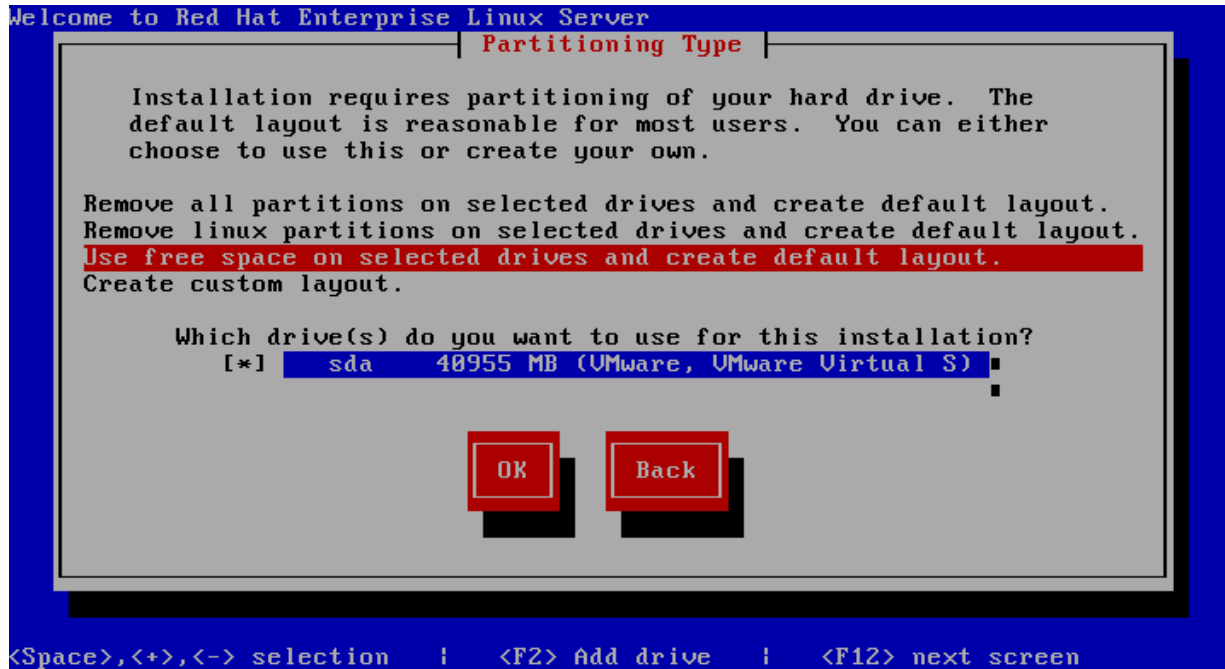
No

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

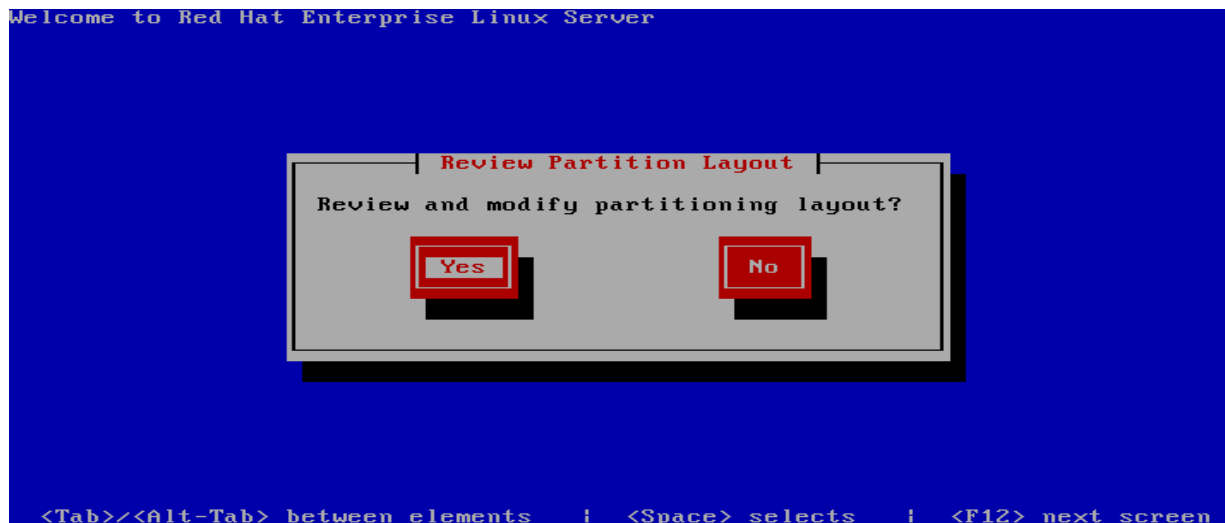
確認會刪所  
有資料



# 主程式安裝(續)

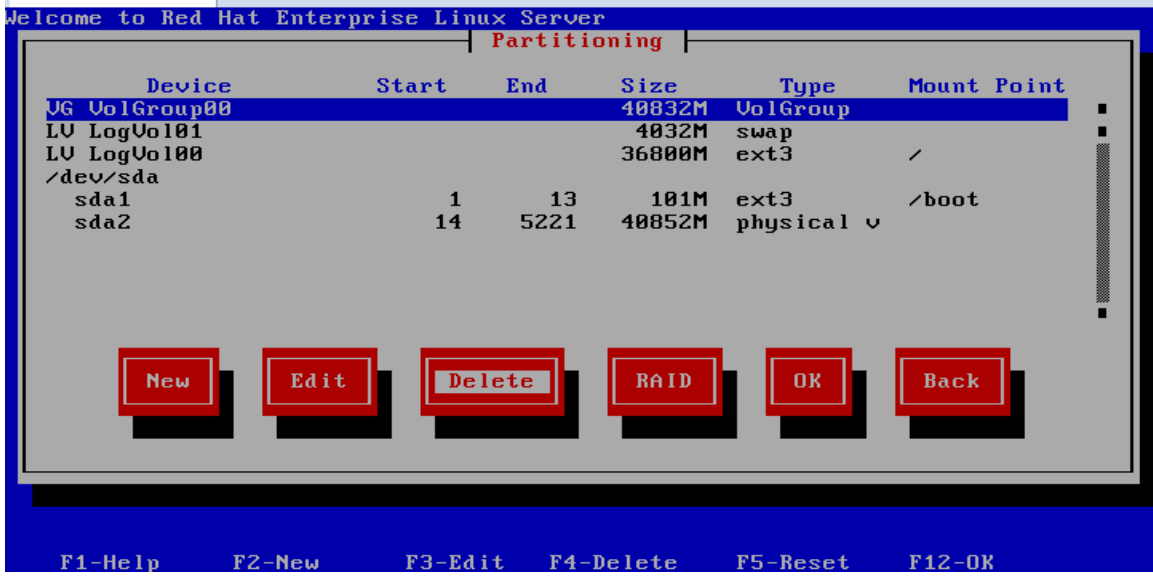


使用現有無使  
用空間且自定大小

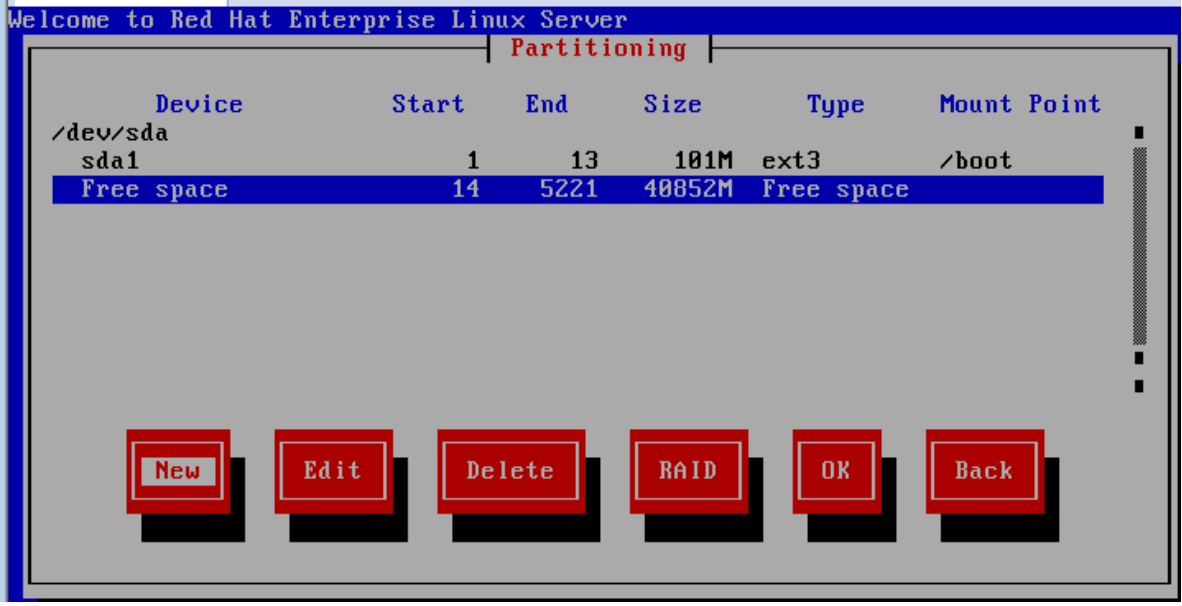


選擇要自訂大小

# 主程式安裝(續)

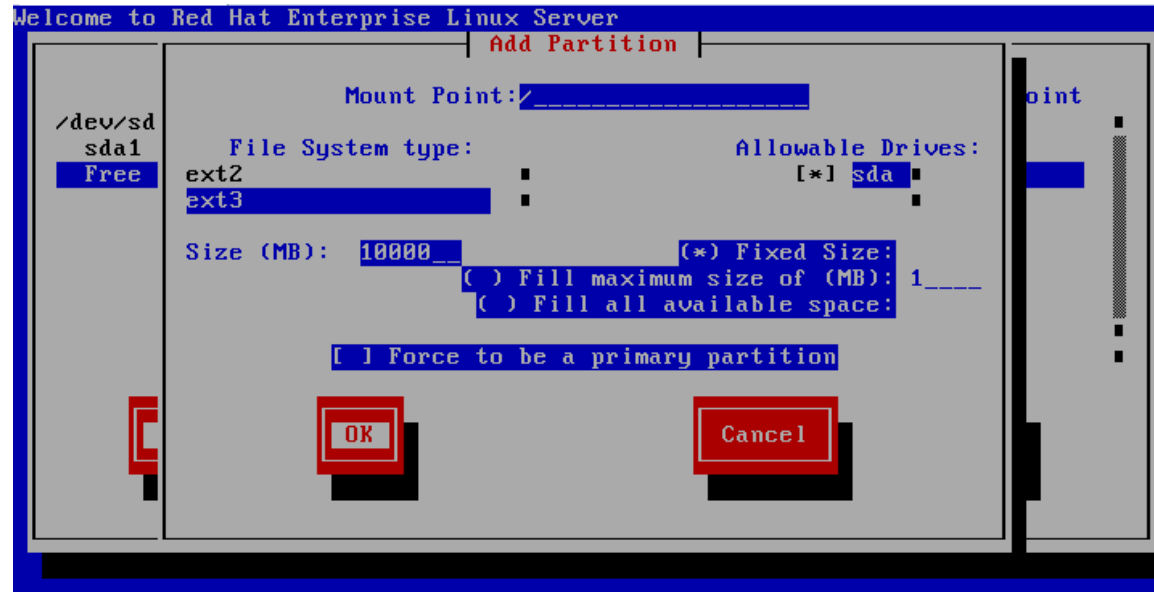


刪除現有LVM格式  
分割區

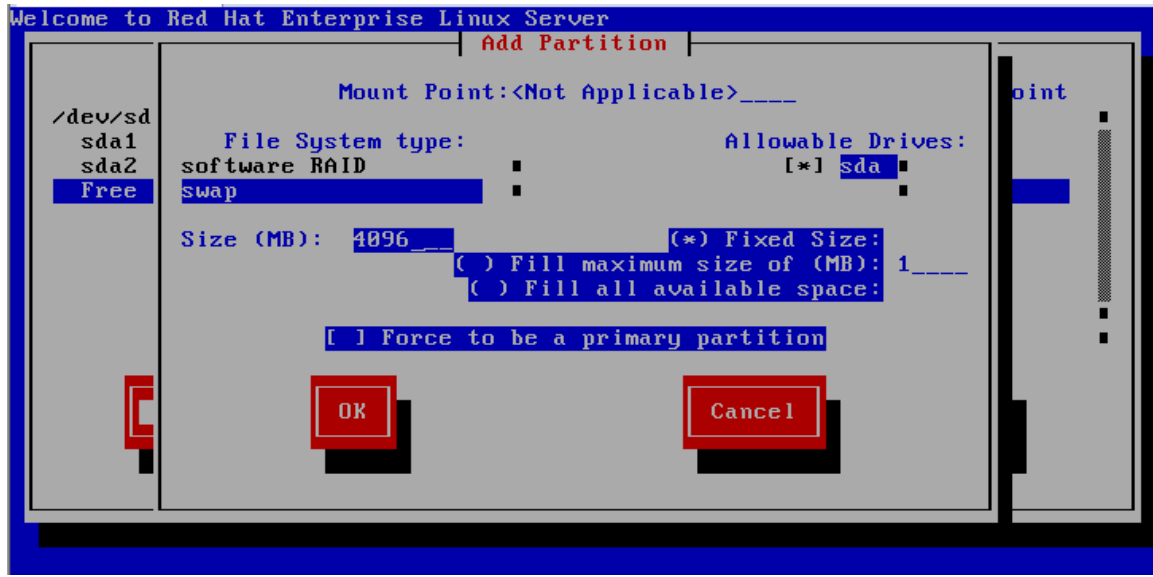


選free space來  
創建新分割區

# 主程式安裝(續)

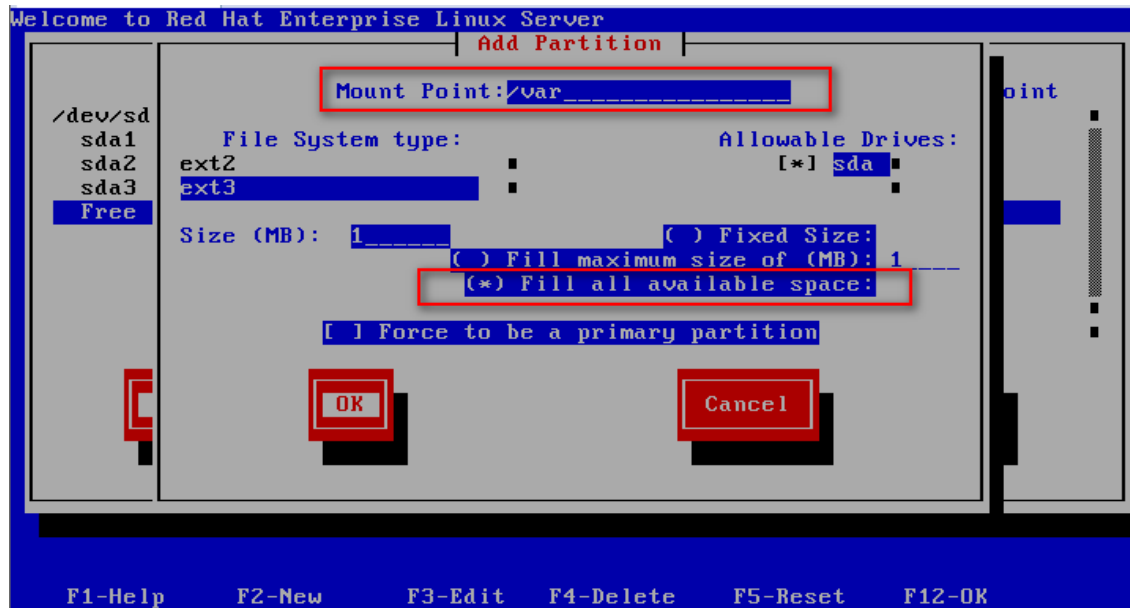


將 / 分割區指定  
10GB空間, 使用  
ext3檔案格式  
(目前設定30G)

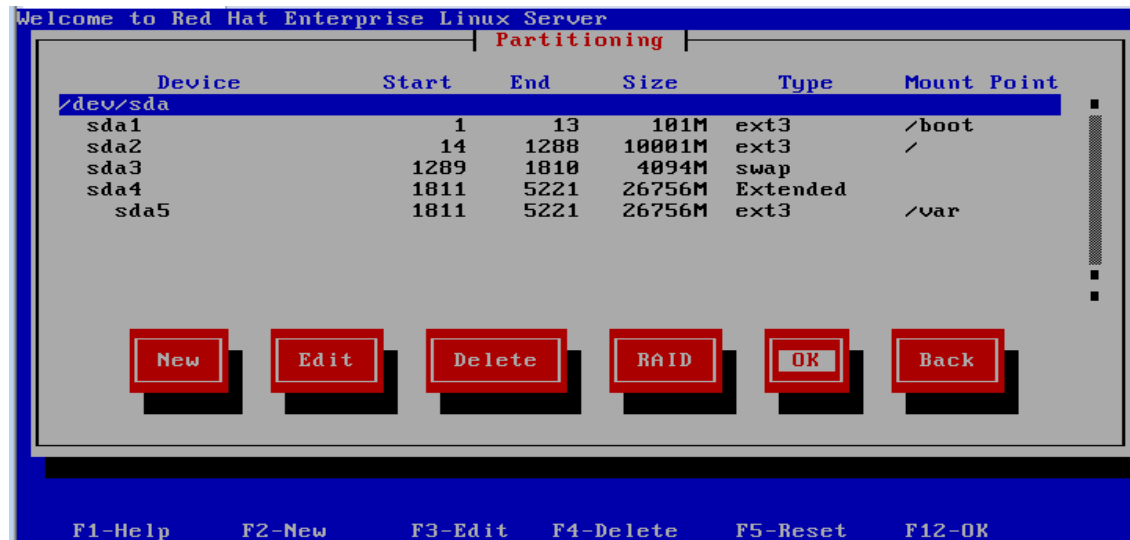


分割swap, 指定  
4GB空間  
(目前設定20G)

# 主程式安裝(續)

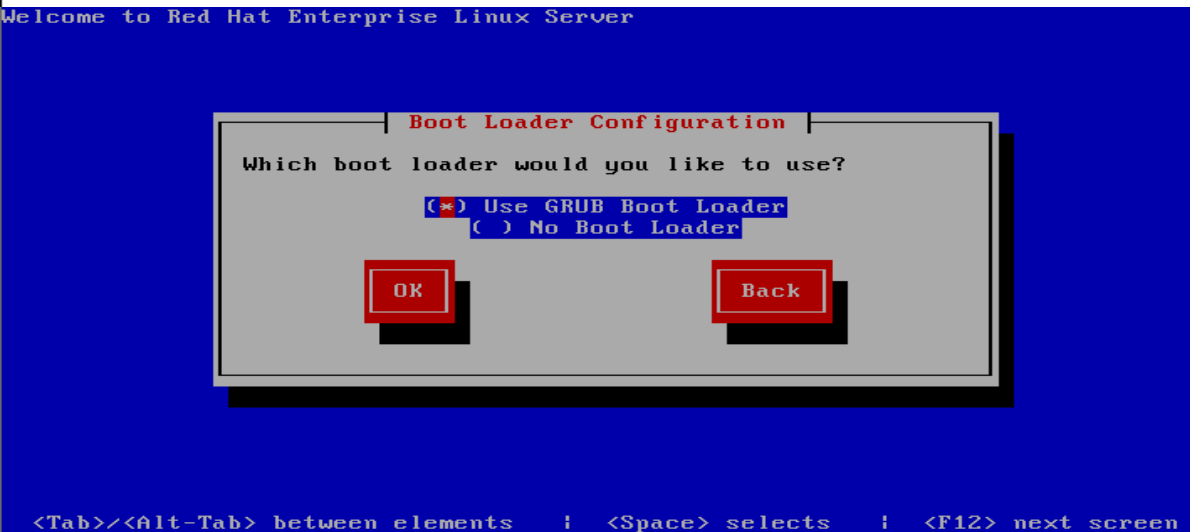


將 /var 分割區指定所有可用空間，使用 ext3 檔案格式

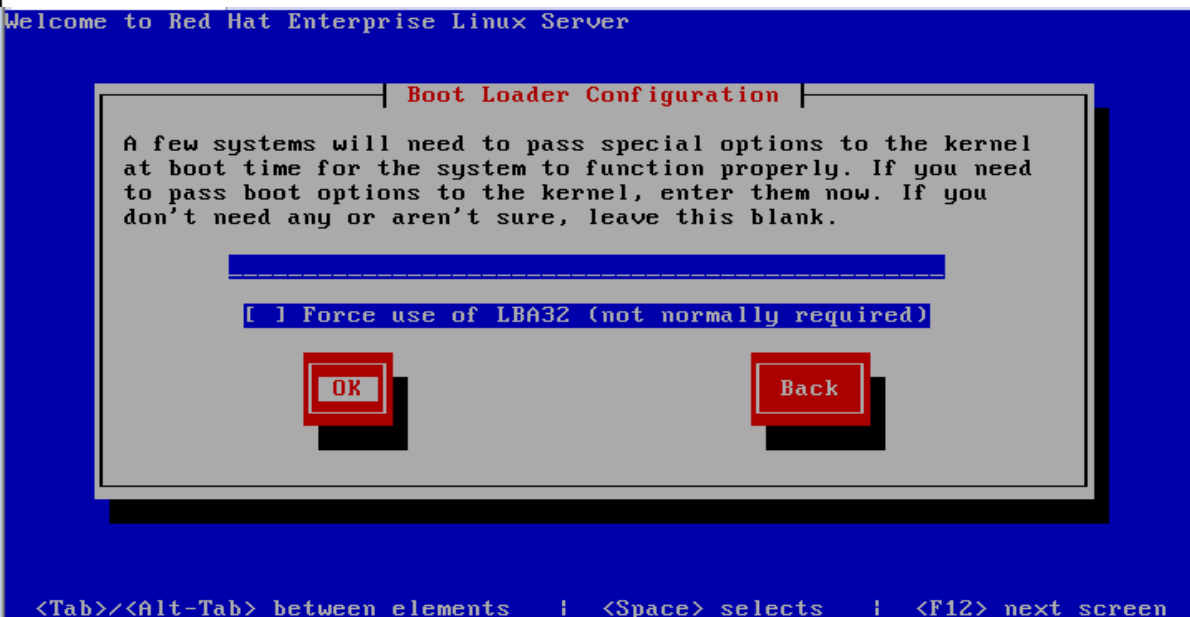


確認一下所有分割區容量無誤

# 主程式安裝(續)

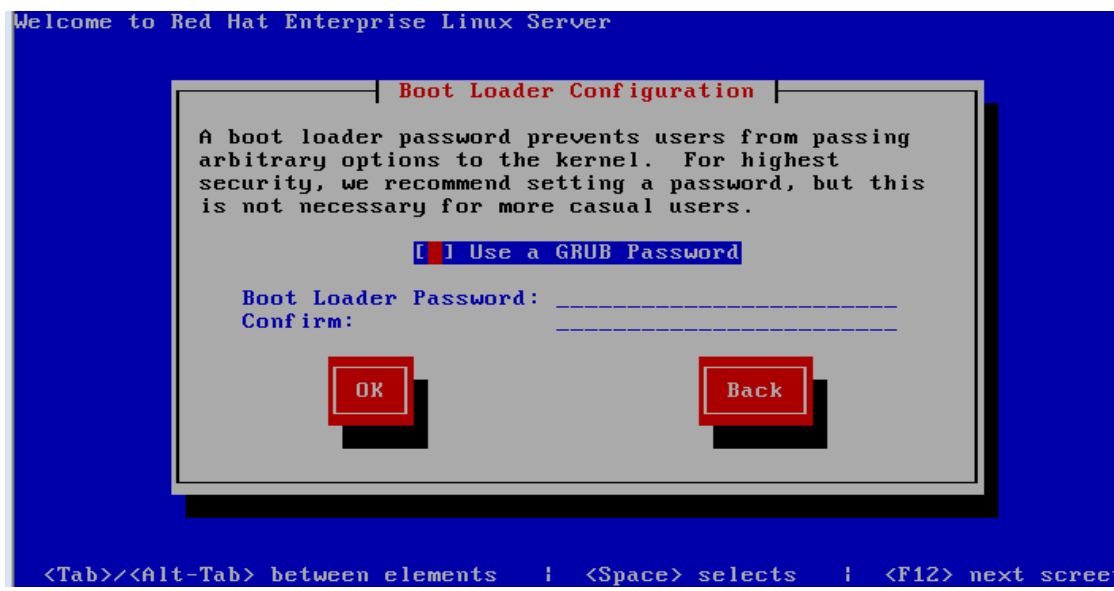


選預設值, 直接  
選ok即可

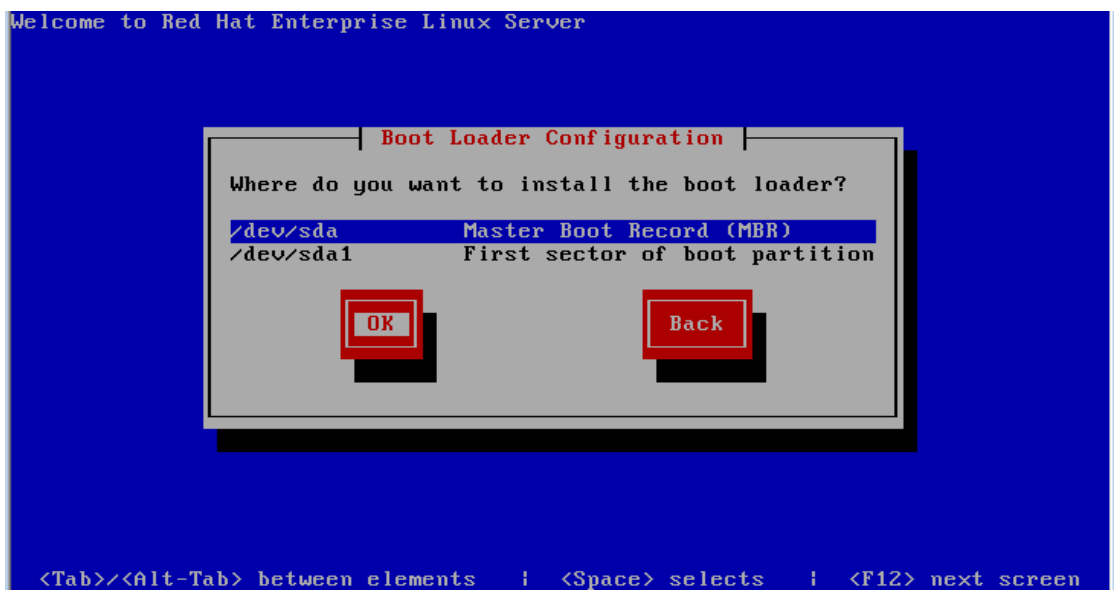


選預設值, 直接  
選ok即可

# 主程式安裝(續)

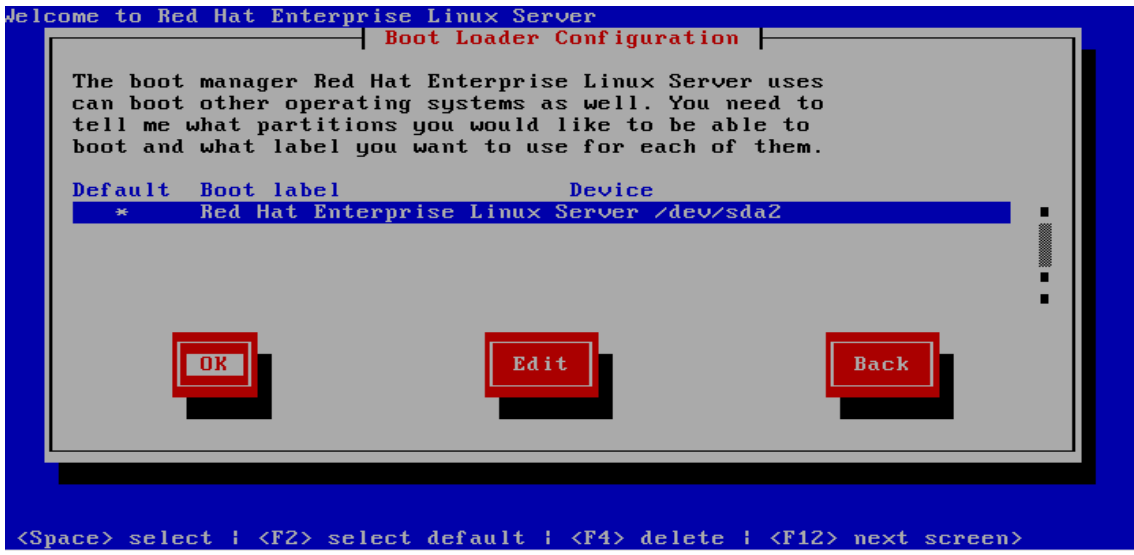


選預設值, 直接  
選ok即可

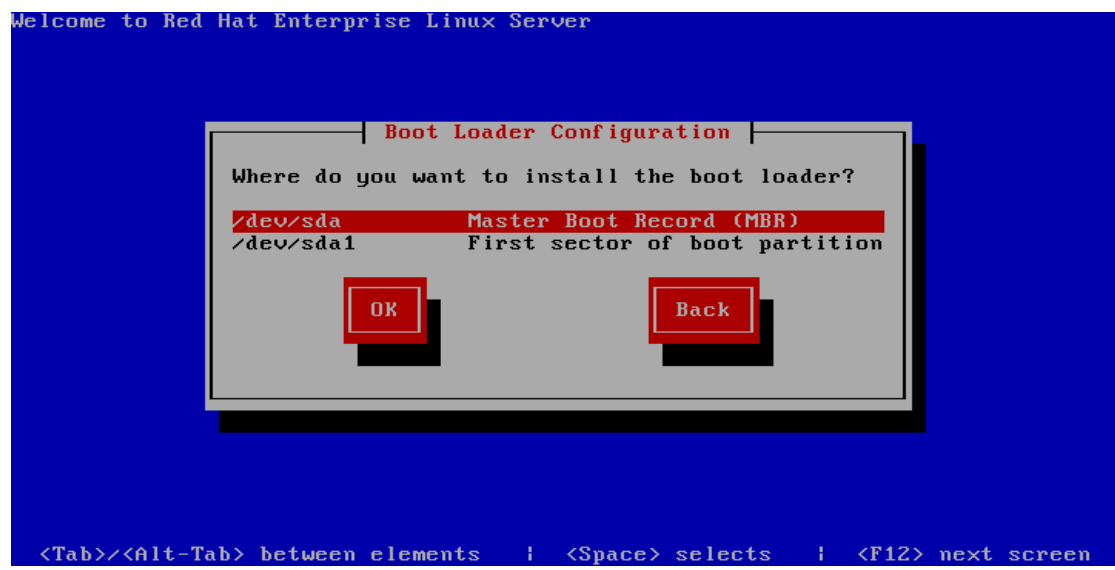


選預設值, 直接  
選ok即可

# 主程式安裝(續)



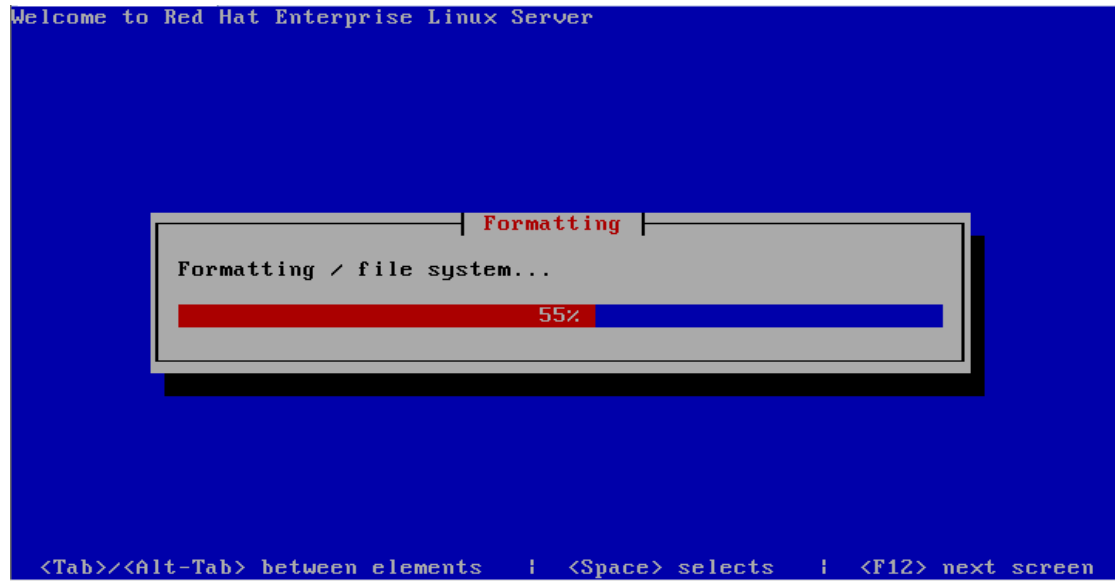
選預設值, 直接  
選ok即可



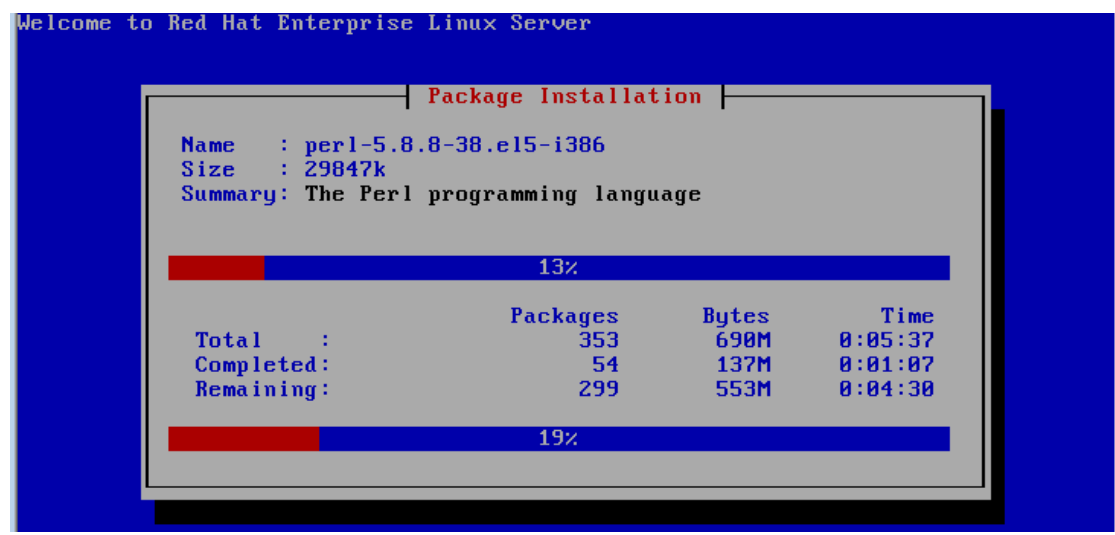
選預設值, 直接  
選ok即可



# 主程式安裝(續)

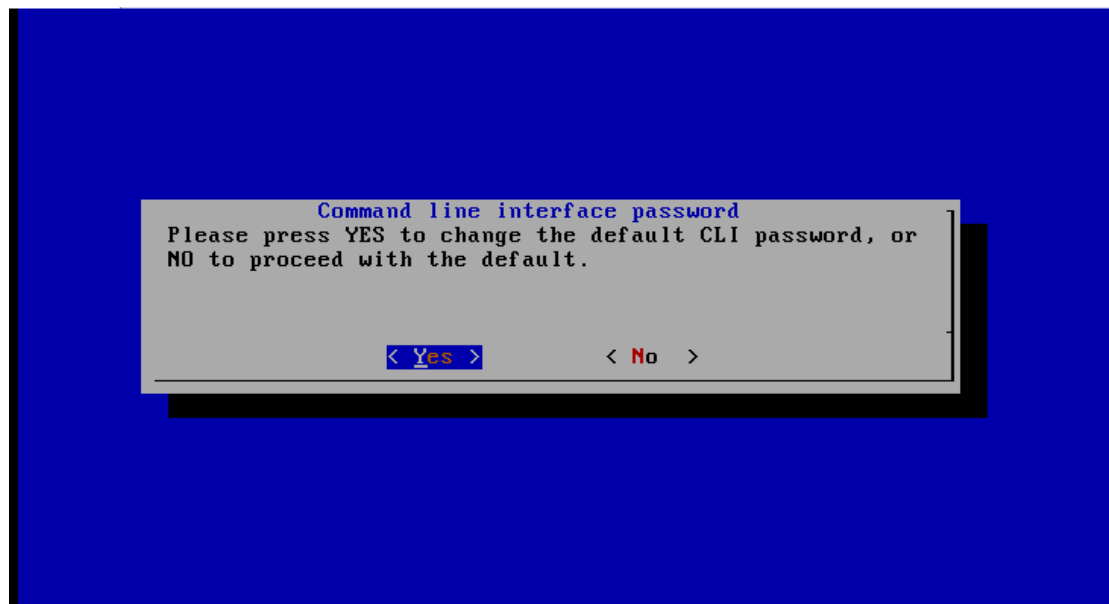


Format Disk 中



安裝Package

# 主程式安裝(續)

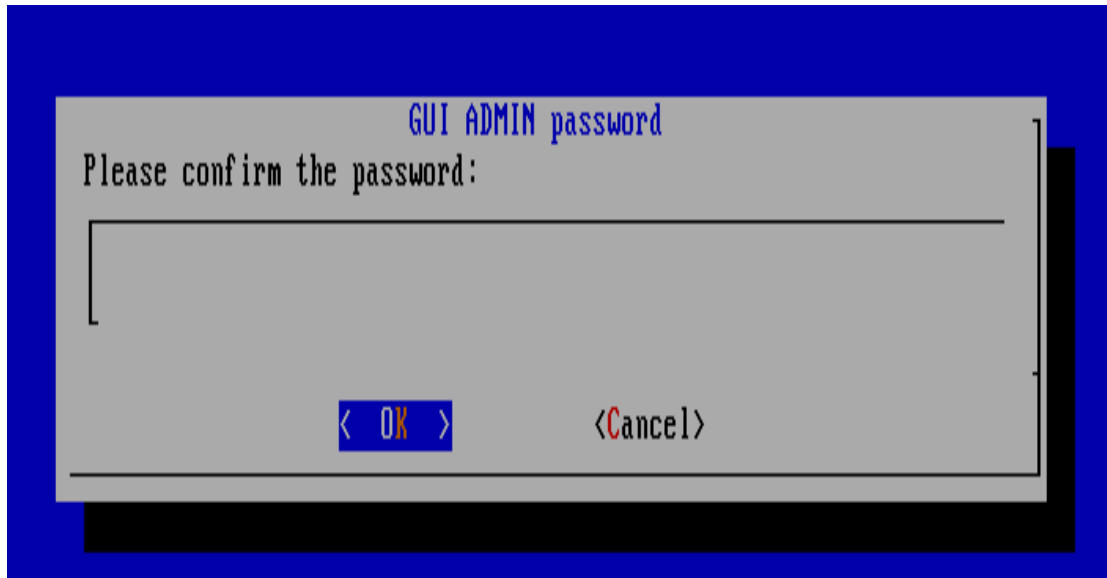


選Yes來更改cli帳號  
密碼, 選No會用預設  
密碼guardium



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

```
netplugd OFF
pcscd OFF
rdisc OFF
restorecond OFF
Rebooting
```

退出光碟片, 第一次重開機

```
ts to reflect at a minimum (i) the number of installs of the Program that Licensee
ee deploys in accordance with the definition of "Install" in this LI document; and
nd (ii) the number of applicable POU or ROU in accordance with the definition
of POU or ROU in this LI document.

The number of Resource Value Units (RVUs) Licensee requires for this Program is
based on Million Service Units (MSUs) capacity of a machine.

The required number of RVUs is determined according to the following table:

For MSU based RVUs:

For 1-3 MSUs, 1 RVU per MSU is required
For 4-45 MSUs, 0.45 RVUs per MSU is required
For 46-175 MSUs, 0.36 RVUs per MSU is required.
For 176-315 MSUs, 0.27 RVUs per MSU is required.
For 316+ MSUs, 0.2 RVUs per MSU is required.

D/N: L-DTIS-8AUMJU
P/N: CT5Y1ML

Do you agree to the above license? [yes/no]: yes_
```

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)

```

=====
IBM InfoSphere Guardium
Unauthorized access is prohibited
=====
guard login: _
    
```

開機完成, 出現Login畫面進入CLI模式

```

guard login: cli
Password:
=====
IBM InfoSphere Guardium
Unauthorized access is prohibited
=====

it is vmware
Changing password for user root.
passwd: all authentication tokens updated successfully.
System root password have been successfully reset using passkey: 46606525
Please save passkey value in your documentation for future Technical Support r
t accessibility
Welcome cli - this is your first login in this system.
Your password has expired.
Changing password for 'cli'.
Enter current password:
    
```

用cli帳號登入  
馬上會要求更改密碼

```

Changing password for 'cli'.
Enter current password:
Enter new password:
Re-enter new password:
guard.domain.com> _
    
```

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

```
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.
Wls5OGQwODljMjJmOGNmNmYxNDZmNmJhMzM0ZDYyNmU4Y1l1db0pRNh4AAAAAAAAAAAAAACwxLCUsRzIw
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

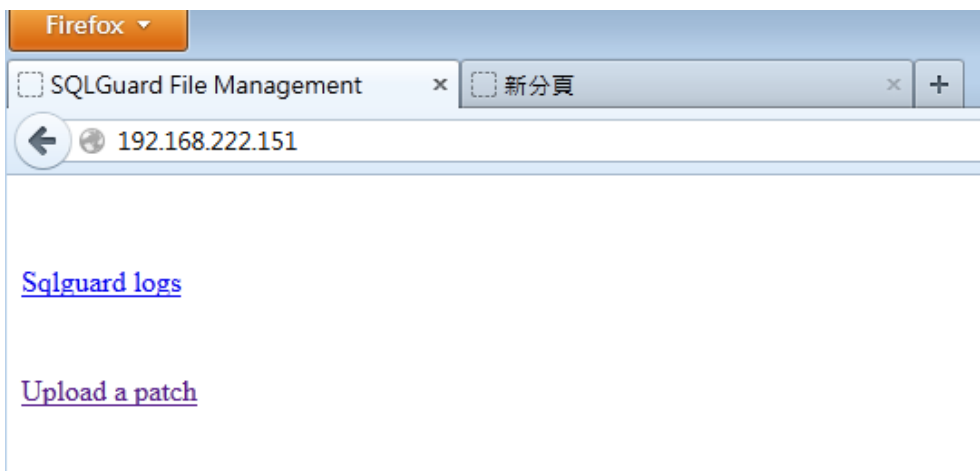
# Guardium 更新Patch檔

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

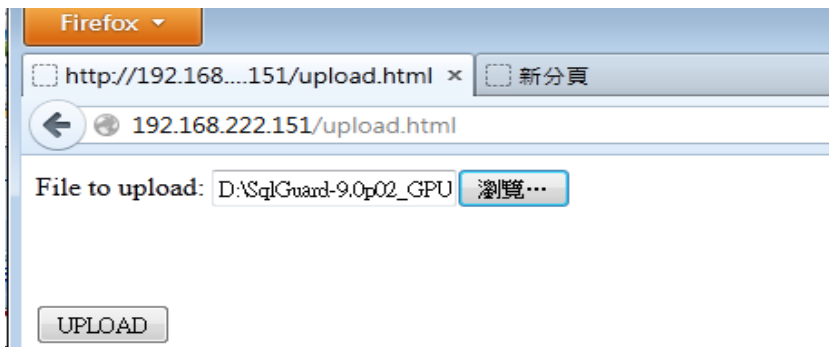
Starting the file server. You can find it at http://DAMC02P.yourcompany.com
The timeout has been set to 600 seconds and it may timeout during the uploading.

Press ENTER to stop the file server.
```

於cli下執行  
fileserv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 檔案，選擇要更新的 patch 檔案，系統開始更新並跳回 cli mode

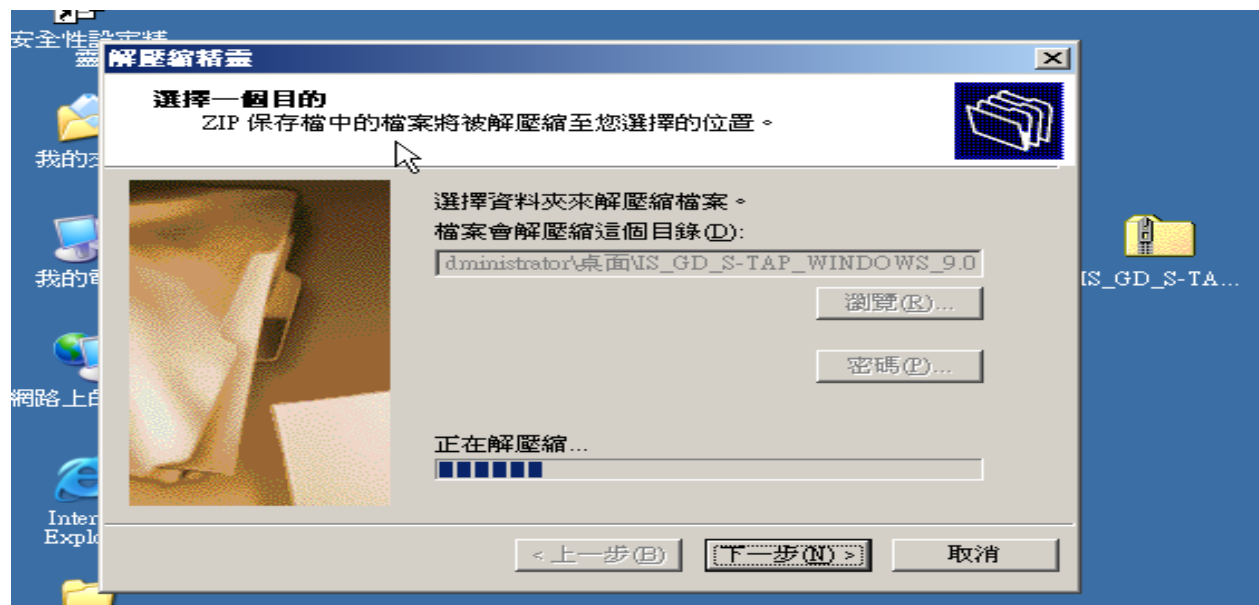
```
DAMC01P.yourcompany.com> show system patch installed

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
```

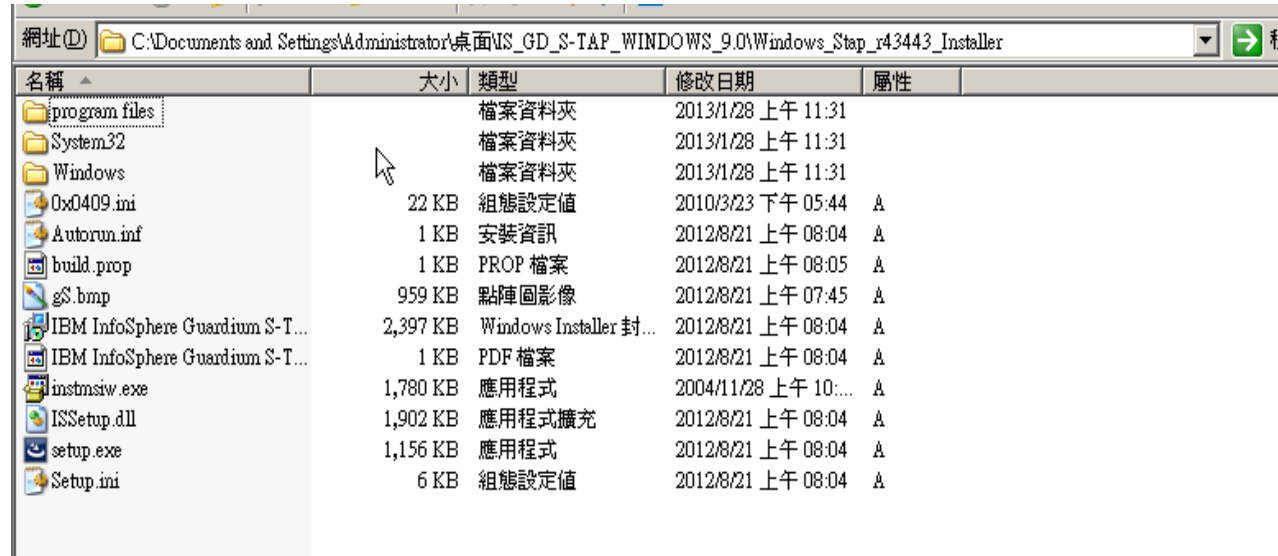
執行 show system patch installed 查看更新狀況或已更新之 patch 檔

IBM Guardium  
S-TAP For Windows  
版安裝

# Windows 主機安裝STAP

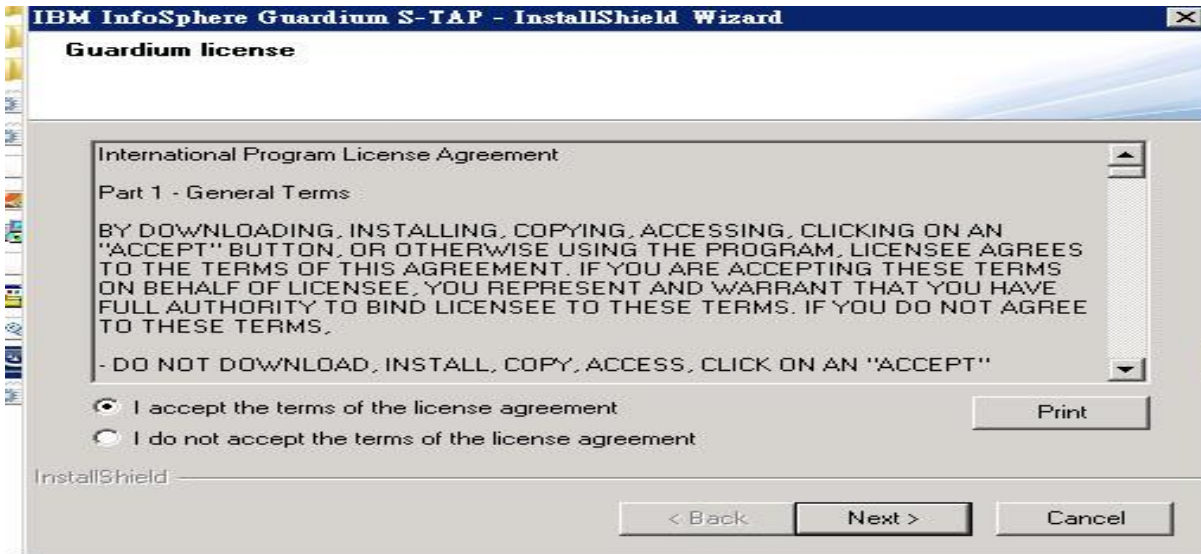


## 將STAP檔案解壓



## 解壓後的檔案

# Windows 主機安裝STAP (續)

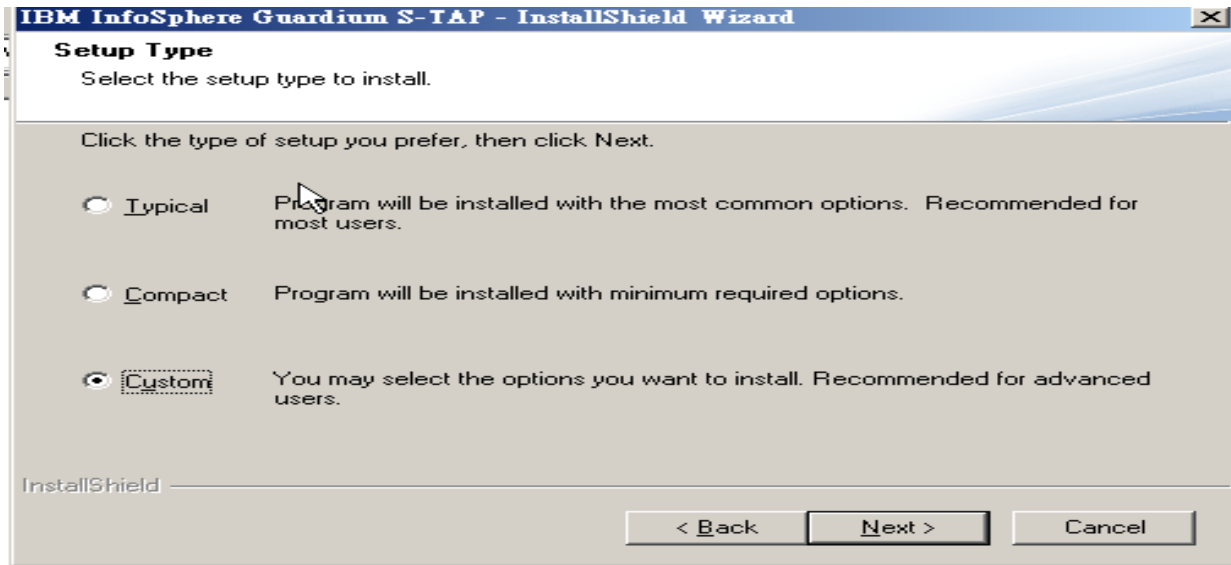


接受軟體授權, 下一步

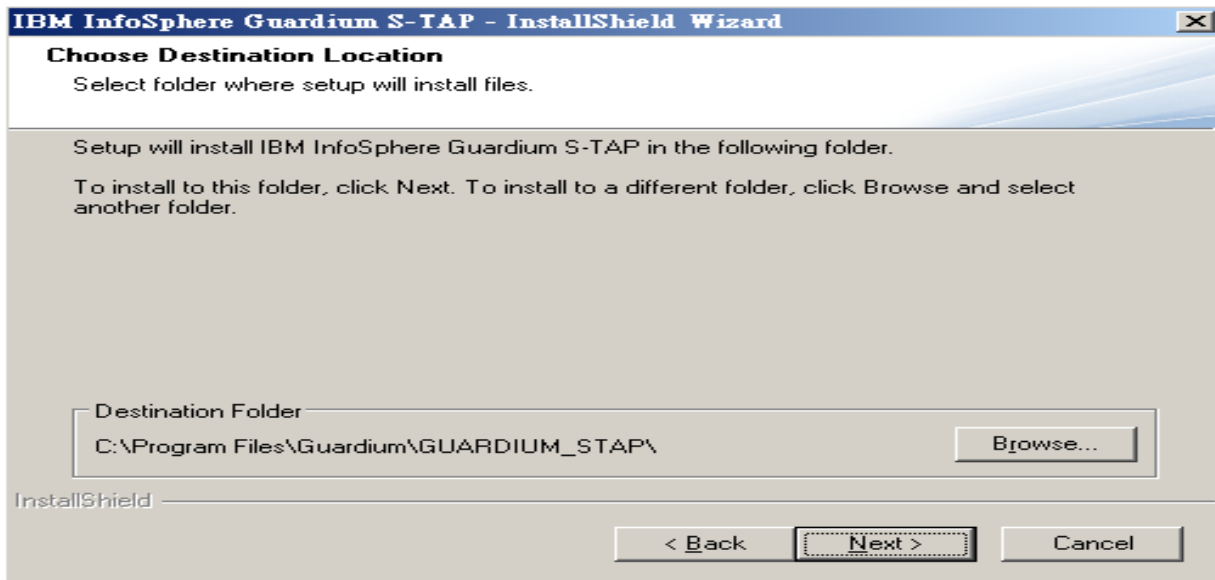


選擇啟動STAP service所使用之帳號, 用local system即可, 空白不輸入, 直接下一步

# Windows 主機安裝STAP (續)



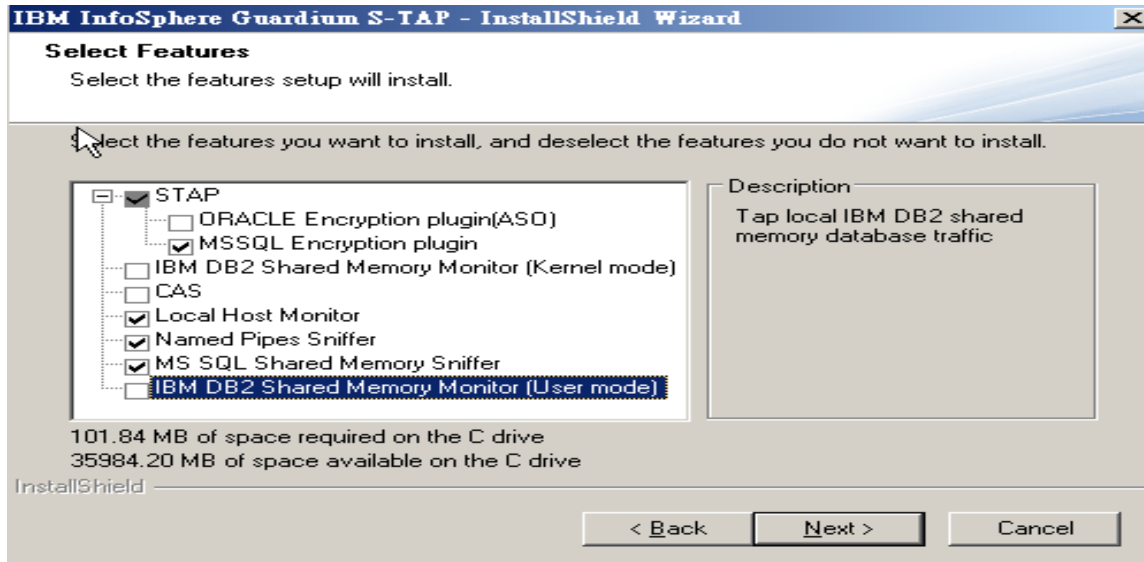
安裝模式, 建議選  
自定, 下一步



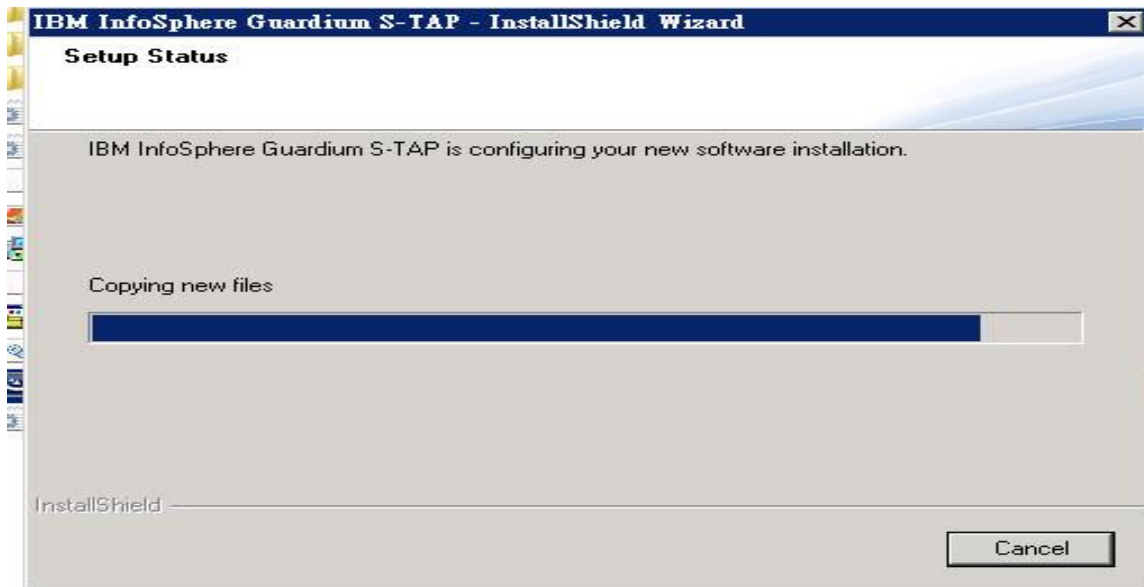
使用預設安裝路  
徑即可, 下一步



# Windows 主機安裝STAP (續)

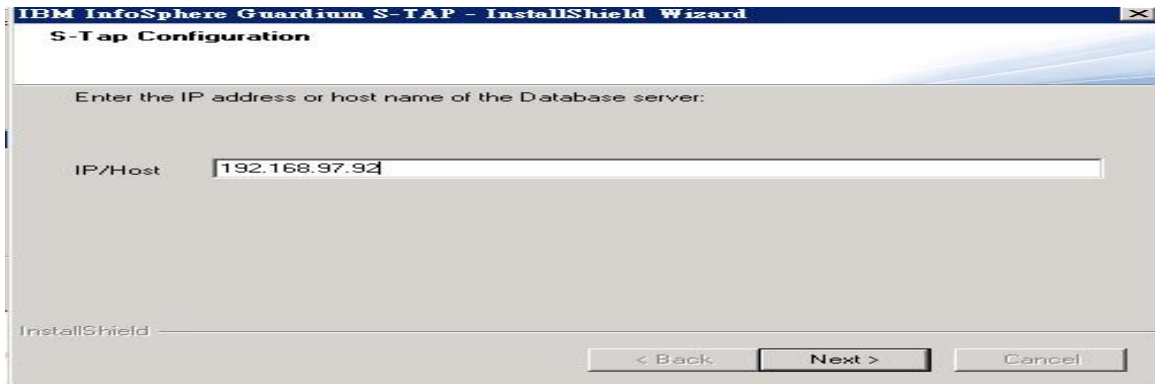


選擇安裝原件, 可依欲  
監控DB種類, 選擇安裝  
項目, CAS建議可不裝  
(MSSQL為例)

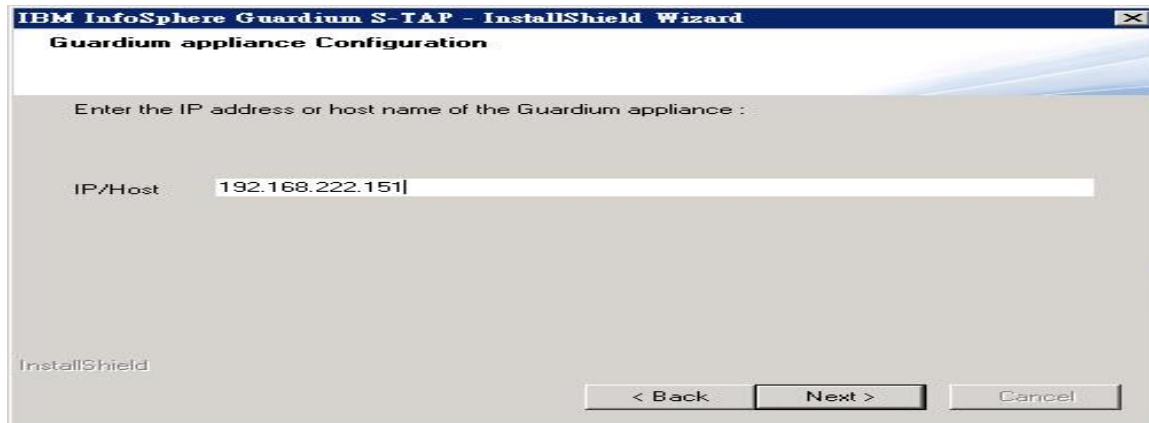


開始安裝軟體

# Windows 主機安裝STAP (續)



輸入本機IP



輸入 Guardium  
Collector 主機IP

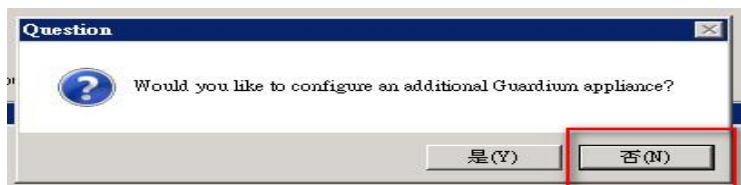


若有使用HA模式, 回答YES 可指定  
另一台Guardium IP, 若沒有使用HA  
回答NO

# Windows 主機安裝STAP (續)



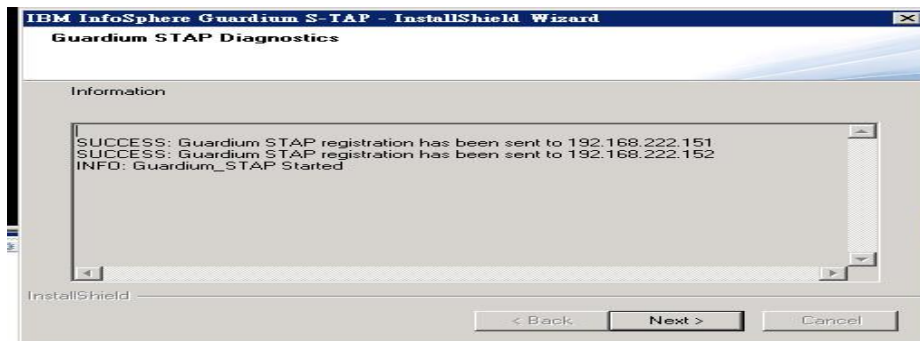
輸入 Standby  
Guardium 主機IP



是否還要加其它Guardium主機  
，已不需要回答No



啟動Guardium S-TAP服務



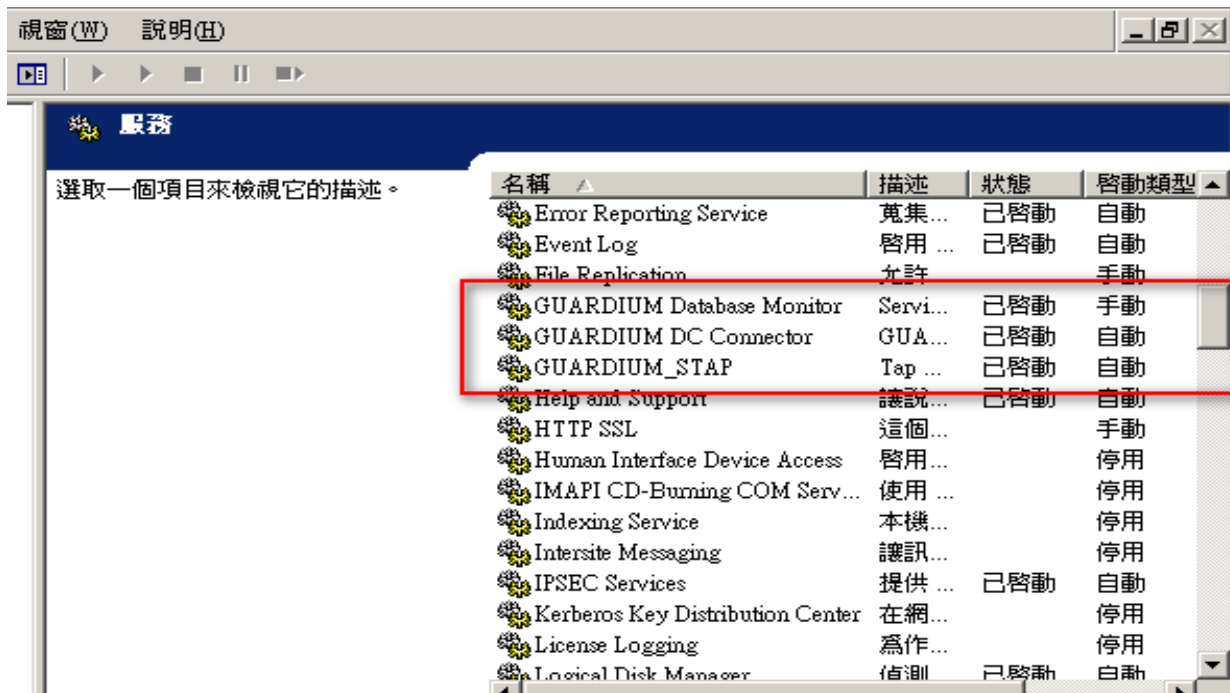
回報設定與服務啟動狀況

# 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

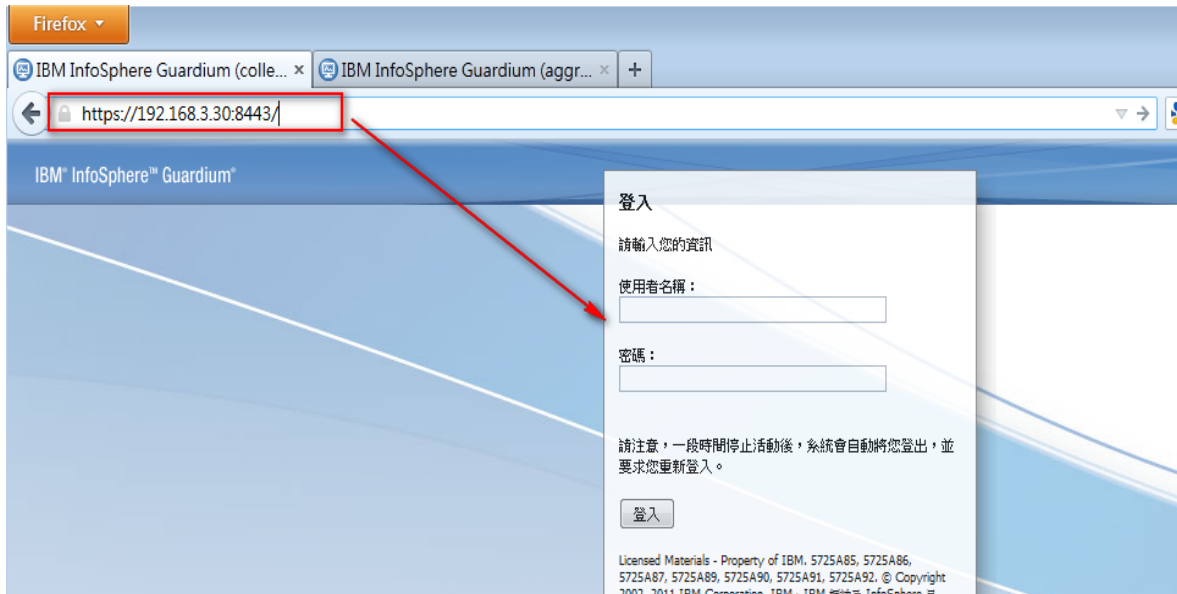


於服務內可看到3條Guardium服務

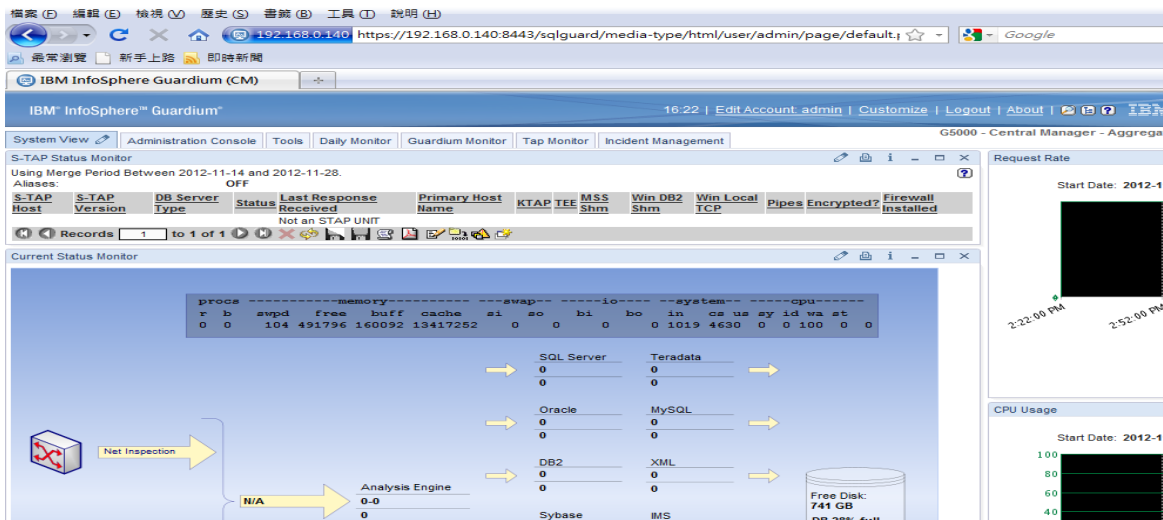
若要暫停監控可將服務停止

# 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

The screenshot shows the IBM InfoSphere Guardium Administration Console. The 'S-TAP Status Monitor' window is active, displaying a table of installed S-TAP instances. The table has the following columns: 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, and DB Port Max. One instance is listed with the following details:

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
192.168.97.929.0.43443			Active	2012-12-04 16:23:25		192.168.222.151	Yes	No	No	No	Yes	Yes	Unencrypted	No			

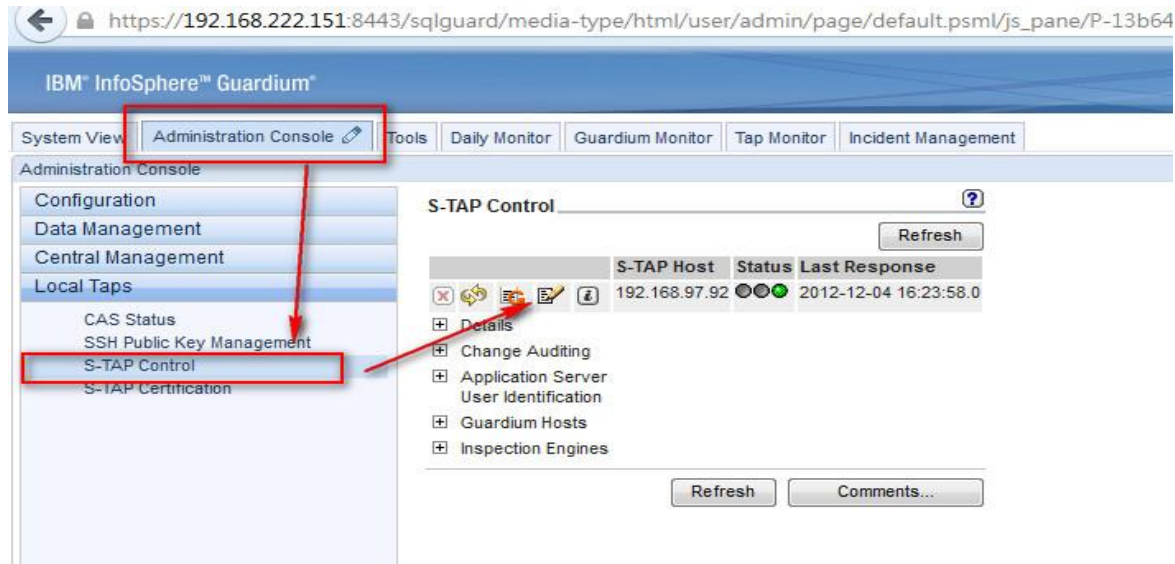
Below the table, there is a 'Records' section and a 'Current Status Monitor' window showing system resource usage statistics.

```

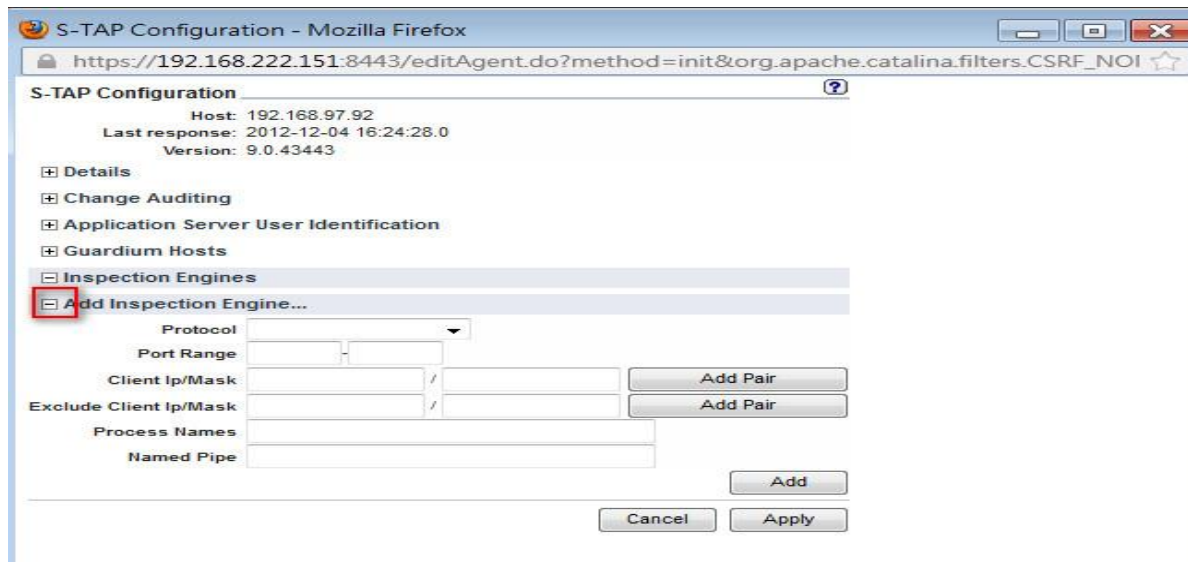
procs -----memory-----swap-----io-----system-----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
  
```



# Guardium 端S-TAP設定 (續)

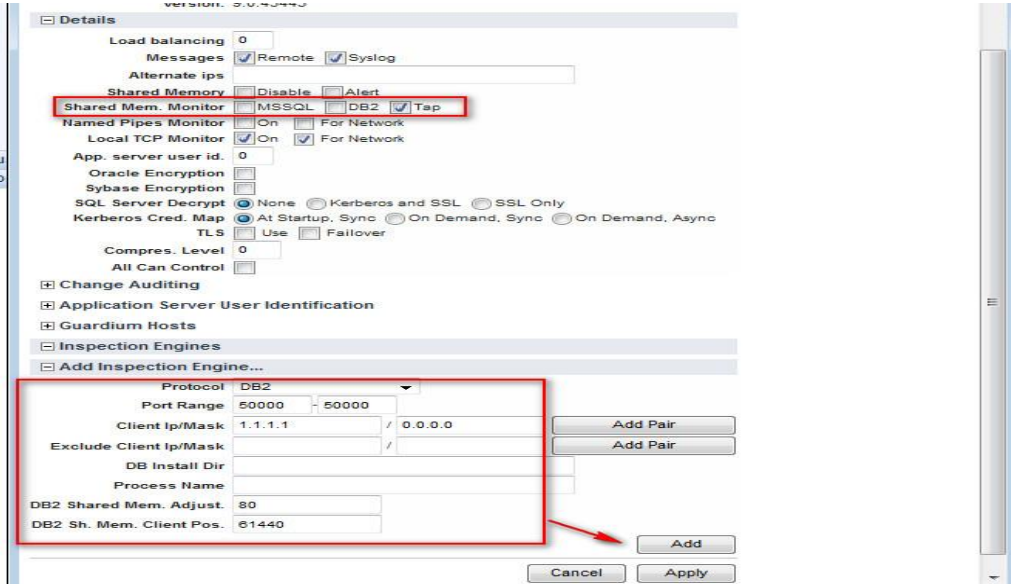


進入S-TAP Control  
點選該主機Edit STAP  
Config



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

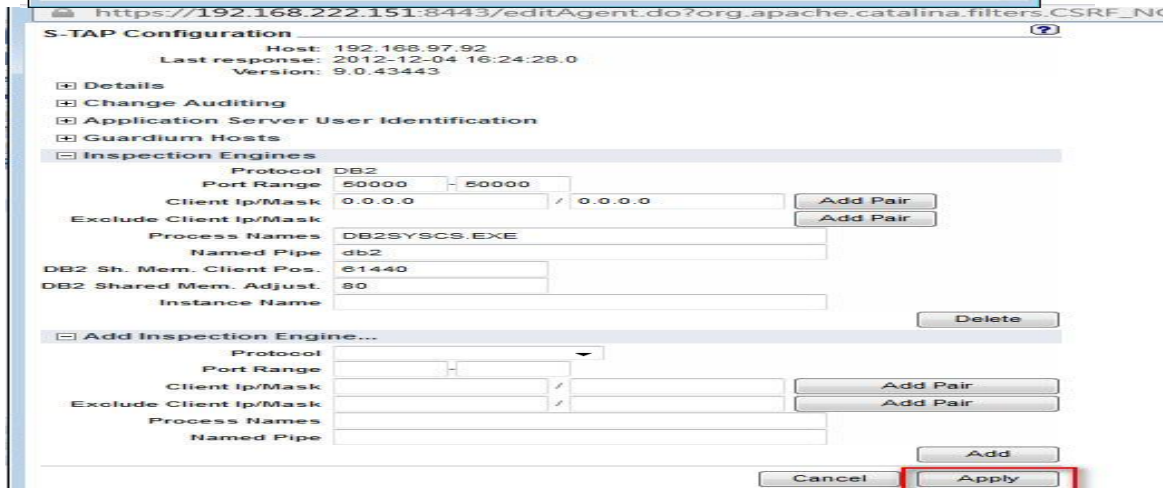
Port Range:依DB所使用Port

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)

Administration Console

- Configuration
- Data Management
- Central Management
- Local Taps
  - CAS Status
  - SSH Public Key Management
  - S-TAP Control
  - S-TAP Certification

S-TAP Host	Status	Last Response
192.168.0.48	●●●●	2012-12-19 15:45:26.0
192.168.2.35	●●●●	2012-12-19 15:45:21.0

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

Guardium Hosts

Inspection Engines

S-TAP Host	Status	Last Response
10.0.0.23	●●●●	2012-12-21 22:42:31.0

Firefox

https://10.0.0.19:8443/tapagents.do?method=toC

S-TAP Commands

S-TAP Host 10.0.0.23

Command Restart

Cancel Apply

若有修改設定，請重起STAP服務

# Guardium 端S-TAP設定 (續)

IBM InfoSphere™ Guardium™ 15:48 | 編輯帳戶: admin | 自訂 | 登出 |

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

S-TAP Status Monitor

Aliases: OFF

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed
192.168.0.113	8.V82.43049	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.0.113	8.V82.43049	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.0.161	STAP-v82_r41163_1-20120517_0854	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	Yes	No	No	N/A	N/A	No	Unencrypted	No
192.168.0.171	STAP-v82_r41163_1-20120517_0854	ORACLE	Active	2012-12-19 15:48:22	192.168.0.142	Yes	No	No	N/A	N/A	No	Unencrypted	No
192.168.0.35	STAP-v82_r33264_1-20110808_0800	ORACLE	Active	2012-12-19 15:48:23	192.168.0.141	Yes	No	No	N/A	N/A	No	Unencrypted	No
192.168.0.48	8.V82.45596	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.2.35	8.V82.43049	MSSQL	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.2.36	8.V82.43049	MSSQL	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.2.40	8.V82.43049	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No
192.168.2.50	8.V82.43049	ORACLE	Active	2012-12-19 15:48:20	192.168.0.142	No	No	No	No	Yes	Yes	Unencrypted	No

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
3  0    104  554768  61724  10200240  0  0  4  6368  1306  83024  20  3  77  0  0
    
```

SQL Server      Teradata

0                      0

0                      0

若設定正常，於S-TAP Status Monitor可看到完整訊息

Net Inspection → Analysis Engine (N/A) → SQL Server, Oracle, DB2, Sybase, Informix, PostgreSQL, Teradata, MySQL, XML, IMS, Netezza, Files/Other

S-TAP Inspection → Analysis Engine (59) → Oracle (23), MySQL, XML, IMS, Netezza, Files/Other

Free Disk: 60 GB, DB 0% full

Unit configured as: [Inspecting Network] [Inspecting using S-TAPs] [Standalone]

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

Host: 192.168.195.30  
Last response: 2013-01-28 11:52:45.0  
Version: 9.0.43443

**Details**

Load balancing

Messages  Remote  Syslog

Alternate ips

Shared Memory  Disable  Alert

**Shared Mem. Monitor**  MSSQL  DB2  Tap

Named Pipes Monitor  On  For Network

Local TCP Monitor  On  For Network

App. server user id.

Oracle Encryption

Sybase Encryption

SQL Server Decrypt  None  Kerberos and SSL  SSL Only

Kerberos Cred. Map  At Startup, Sync  On Demand, Sync  On Demand, Async

TLS  Use  Failover

Compres. Level

All Can Control

**Change Auditing**

**Application Server User Identification**

**Guardium Hosts**

**Inspection Engines**

Protocol	MSSQL	
Port Range	<input type="text" value="1433"/>	<input type="text" value="1434"/>
Client Ip/Mask	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Exclude Client Ip/Mask	<input type="text"/>	
Process Names	<input type="text" value="SQLSERVR.EXE"/>	
Named Pipe	<input type="text" value="SQL\QUER,PIPE\SQLLOCAL"/>	
Instance Name	<input type="text" value="MSSQLSERVER"/>	



# 現有STAP (S-TAP Control) DB2 設定值

https://192.168.222.152:8443/editAgent.do?method=init&org.apache.catalina.filters.CSRF\_NOI

Load balancing

Messages  Remote  Syslog

Alternate ips

Shared Memory  Disable  Alert

**Shared Mem. Monitor**  MSSQL  DB2  Tap

Named Pipes Monitor  On  For Network

Local TCP Monitor  On  For Network

App. server user id.

Oracle Encryption

Sybase Encryption

SQL Server Decrypt  None  Kerberos and SSL  SSL Only

Kerberos Cred. Map  At Startup, Sync  On Demand, Sync  On Demand, Async

TLS  Use  Failover

Compres. Level

All Can Control

+ Change Auditing

+ Application Server User Identification

+ Guardium Hosts

- Inspection Engines

Protocol DB2

Port Range  -

Client Ip/Mask

Exclude Client Ip/Mask

DB Install Dir

Process Name

DB2 Sh. Mem. Client Pos.

DB2 Shared Mem. Adjust.

Instance Name

# Q & A 問題與討論

