



網路管理 Webmin

我們可以透過使用 Webmin 來網路管理我們選端的電腦 <http://www.webmin.com/> 是 Webmin 的網址，我們可以在這下載原始碼檔 tar.gz。



1-1-1 原始檔安裝

這是 webmin-1.121.tar.gz 版本的安裝，如果要安裝新的 webmin-1.*.tar.gz 的版本，也是按照同樣的步驟和方法。我們將下載的 Webmin 原始檔複製到 /usr/local 目錄中。

```
# cp webmin-1.121.tar.gz /usr/local
```

解壓檔案

語法

指令：gunzip [-參數] [-S 字尾] [檔名]

我們解壓 webmin-1.121.tar.gz 檔到 /usr/local 中。

```
[root@flash chaiyen]# cd /usr/local
```

```
[root@flash local]# gunzip webmin-1.121.tar.gz
```

我們使用 tar xf webmin-1.121.tar 來將 webmin-1.121.tar 打包的檔案取出。

```
# tar xf webmin-1.121.tar
```

我們到 webmin-1.121 的目錄，並且執行其預設的 shell 指令。我們輸入 ./setup.sh

```
# cd webmin-1.121
```

```
# ./setup.sh
```

這是歡迎我們安裝的畫面。

```
*****
*                               Welcome to the Webmin setup script, version 1.121                               *
*****
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /usr/local/webmin-1.121 ...
```

```
*****
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.
```

我們輸入放置 webmin 組態檔的位置為/etc/good。預設的放置位置為/etc/webmin。
Config file directory [/etc/webmin]: /etc/good

我們輸入放置 webmin 記錄檔的位置為/var/good。預設的放置位置為/var/webmin。
Log file directory [/var/webmin]: /var/good

因為 Webmin 是由 perl 所撰寫，所以我們要輸入 perl 直譯器的路徑。預設為
/usr/bin/perl。輸入完後，它會自動偵測我們的作業系統。

Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.

Full path to perl (default /usr/bin/perl): /usr/bin/perl

Testing Perl ...
Perl seems to be installed ok

我們選取作業系統 Redhat Linux。

```
*****
For Webmin to work properly, it needs to know which operating system
type and version you are running. Please select your system type by
entering the number next to it from the list below
-----
 1) Sun Solaris          2) Caldera OpenLinux eS  3) Caldera OpenLinux
 4) Redhat Linux        5) Slackware Linux      6) Debian Linux
 7) SuSE Linux          8) United Linux        9) Corel Linux
10) TurboLinux         11) Cobalt Linux       12) Mandrake Linux
13) Mandrake Linux Corpo 14) Delix DLD Linux    15) Conectiva Linux
16) ThizLinux Desktop   17) ThizServer         18) MSC Linux
19) MklLinux           20) LinuxPPC          21) XLinux
22) LinuxPL            23) Trustix           24) Cendio LBS Linux
25) Ute Linux          26) Lanthan Linux     27) Yellow Dog Linux
28) Corvus Latinux     29) Immunix Linux     30) Gentoo Linux
31) Lycoris Desktop/LX 32) Secure Linux      33) Generic Linux
34) FreeBSD            35) OpenBSD           36) NetBSD
37) BSDI               38) HP/UX              39) SGI Irix
40) DEC/Compaq OSF/1   41) IBM AIX            42) SCO UnixWare
43) SCO OpenServer     44) Darwin             45) Mac OS X
46) Mac OS X / OS X Serv 47) Cygwin
-----
```

選取 16。

Please choose which version of Redhat Linux you are running, by entering the number next to it from the list below

- ```

1) Redhat Linux 4.0 2) Redhat Linux 4.1
3) Redhat Linux 4.2 4) Redhat Linux 5.0
5) Redhat Linux 5.1 6) Redhat Linux 5.2
7) Redhat Linux 6.0 8) Redhat Linux 6.1
9) Redhat Linux 6.2 10) Redhat Linux 7.0
11) Redhat Linux 7.1 12) Redhat Linux 7.2
13) Redhat Linux 7.3 14) Redhat Linux 8.0
15) Redhat Linux 9.0 16) Redhat Linux Fedora 1
17) Redhat Linux 2.1AS 18) Redhat Linux 2.1ES
19) Redhat Linux 2.1WS 20) Redhat Linux 3.0AS
21) Redhat Linux 3.0ES 22) Redhat Linux 3.0WS

```

Version: 16

Webmin 使用我們自己的密碼來保護網站管理我們的程式。我們需知到這個網路的服務是架在哪一個埠、使用者登錄的名稱、使用者的密碼、這個系統的主機名稱、是否使用 SSL、是否開機時就執行 Webmin。

```
Operating system name: Redhat Linux
Operating system version: Fedora 1
```

```

Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
- What port to run the web server on. There must not be another
 web server already using this port.
- The login name required to access the web server.
- The password required to access the web server.
- If the webserver should use SSL (if your system supports it).
- Whether to start webmin at boot time.
```

我們輸入網路服務的埠為 5000。預設服務的埠為 10000。

```
Web server port (default 10000): 5000
```

我們輸入登錄的名稱為 good。預設為 admin。

```
Login name (default admin): good
```

我們輸入我們登錄的密碼 353766。連續輸入兩次。密碼可以自行設定。

```
Login password:
```

我們主機的名稱。我們的主機是 flash.aasir.com。

```
Web server host name (default flash.aasir.com): flash.aasir.com
```

開機時是否要啟動 Webmin。我們選取 y。

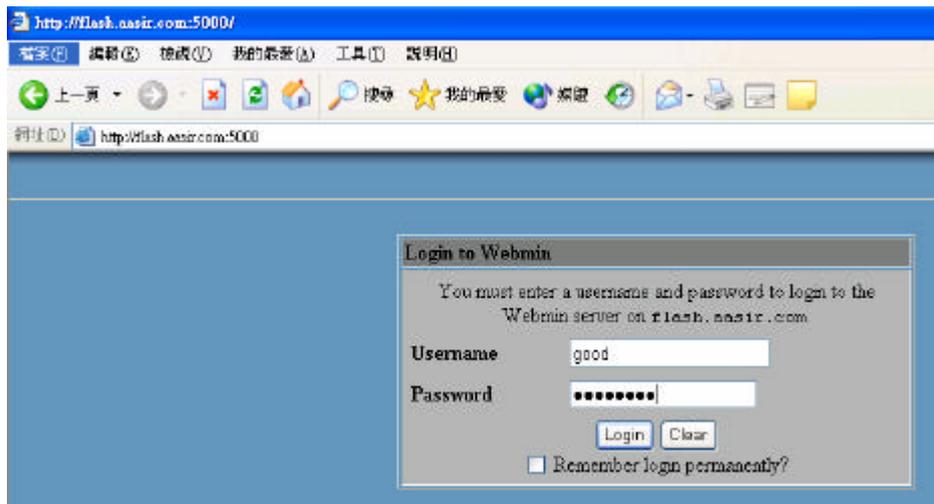
```
The Perl SSLeay library is not installed. SSL not available.
Start Webmin at boot time (y/n): y
```

我們輸入 `http://網址:埠號/` 就可以登錄 Webmin。在這裏我們輸入的是 `http://flash.aasir.com:5000/`。

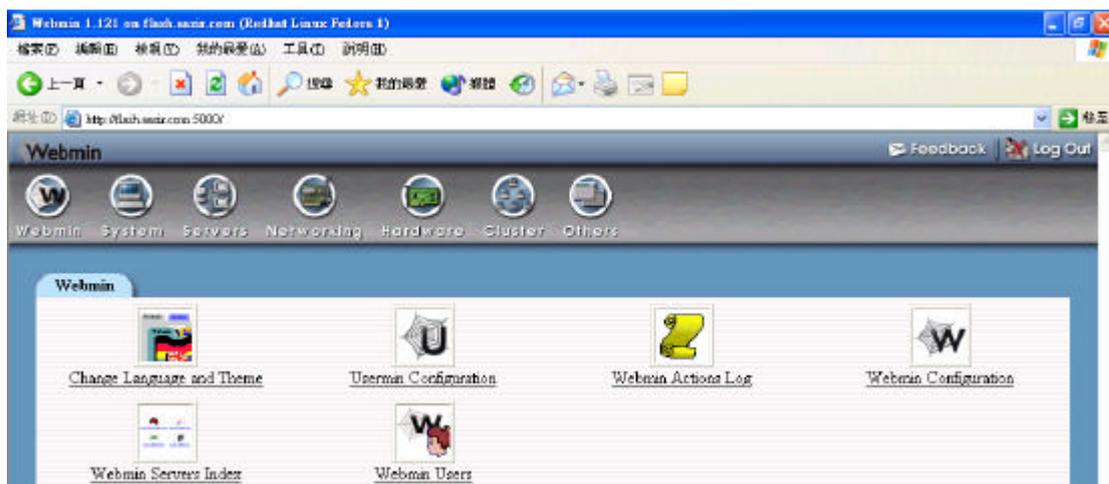
Webmin has been installed and started successfully. Use your web browser to go to

<http://flash.aasir.com:5000/>

我們以我們的帳號 `good` 和密碼 `353766` 登錄。



這樣就進入 Webmin 的畫面。



我們可以停止 Webmin 的執行。我們使用/etc/rc.d/init.d/webmin stop。

```
[root@flash webmin-1.121]# /etc/rc.d/init.d/webmin stop
Stopping Webmin server in /usr/local/webmin-1.121
```

我們可以啟動 Webmin。我們使用/etc/rc.d/init.d/webmin start。

```
/etc/rc.d/init.d/webmin start
```

## 1-2 改變成中文環境

改變中文環境可以分為改變個人的中文環境和改變 Webmin 組態的中文環境。

我們選取 Webmin Webmin 組態 語言。我們將語言設定為 Traditional Chinese (ZH\_TW.BIG5)

我們選取 Webmin 組態。



我們選取語言。



我們設定為繁體中文的語言。

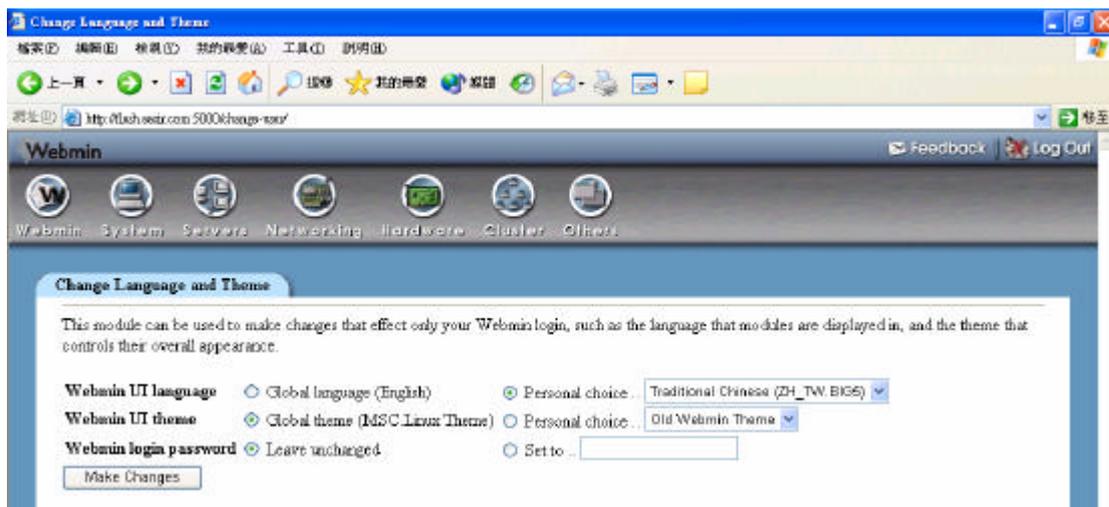


### 1-2-1 改變個人的中文環境

我們進入 Webmin 後選取 Change Language and Theme。



我們選取 Personal choice，並選取繁體中文 Traditional Chinese(ZH\_TW.BIG5)，然後按下 Make Changes，這樣就選取繁體中文了。



### 1-3 增加 Webmin 的使用管理者

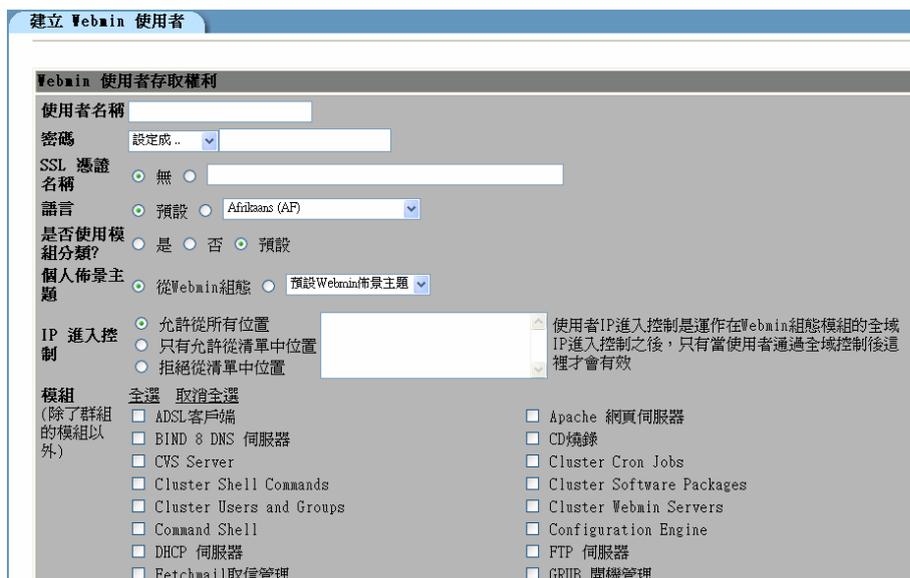
我們可以在 Webmin 新增使用管理者，並設定他的使用權限。我們選取 Webmin->Webmin 使用者。



我們可以建立新的 Webmin 使用者，而在這裏我們可以看到我們在安裝時設定的 good 使用者。我們按下建立新的 Webmin 使用者。



我們輸入我們新增的使用者名稱，並且輸入密碼，也設定語言為繁體中文。



我們可以設定使用者名稱及密碼。我們可以設定使用者為 gogo。



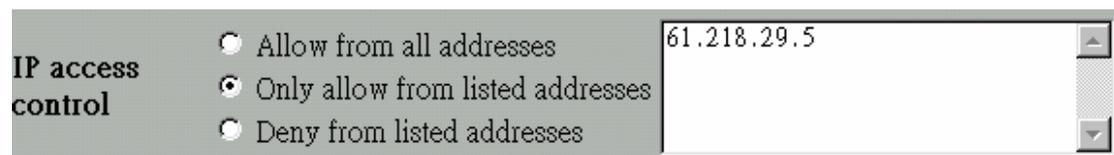
我們也可以設定使用者為 bibo。



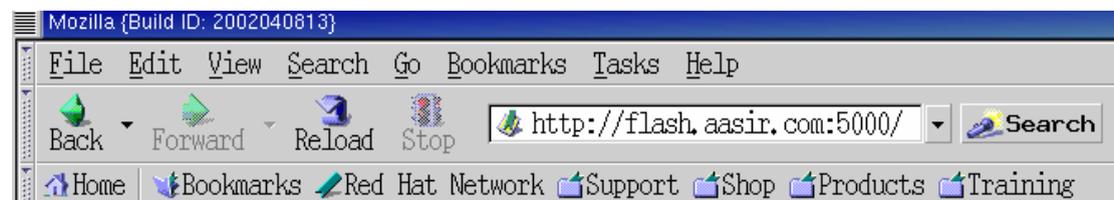
我們可以設定繁體中文 Traditional Chinese(ZH\_TW.BIG5)。



當我們設定 Allow from all addresses 時，則所有網路 IP 位址皆可存取 Webmin。如果我們設定 Only allow from listed addresses，則只有指定的 IP 位址可以存取我們的 Webmin。在這裏我們設定只有網路 IP 位址為 61.218.29.5 的可以存取我們的 Webmin 網路管理程式。當我們設定 Deny form listed addresses 時，將限定我們所指定的網路 IP 位址不可存取我們的 Webmin 管理程式。

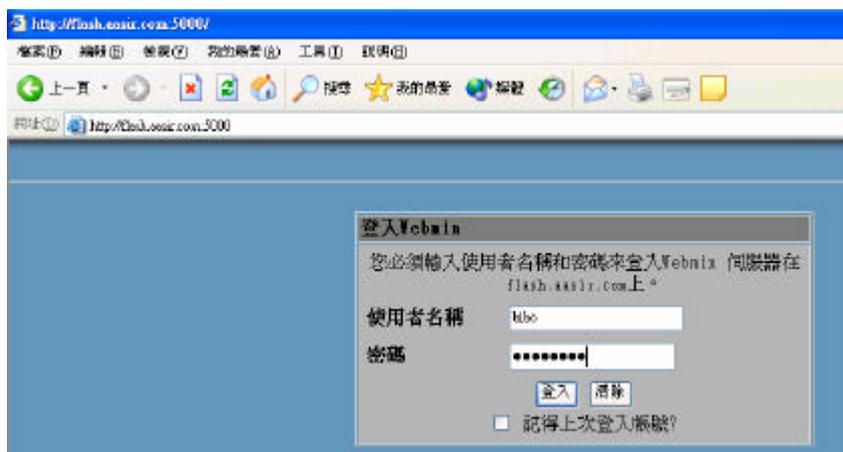


當我們從 IP 位址為 61.218.29.3 的位址要存取 Webmin 時，因為是 Only allow form listed addresse 61.218.29.5，所以只有 61.218.29.5 的才能夠存取我們的 Webmin。

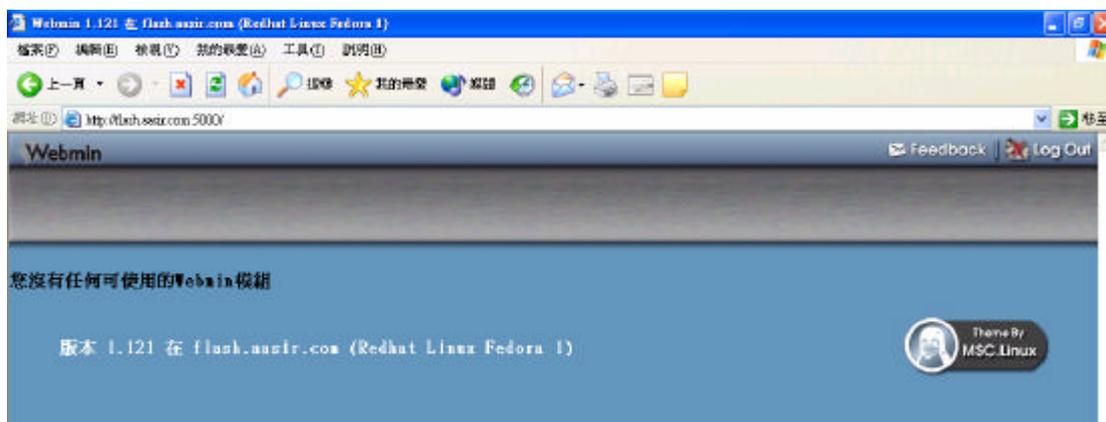


**Error - Access denied for 61.218.29.3**

我們現在輸入使用者名稱及密碼就可以進入 Webmin 網路管理程式了。



因為我們沒有設定可使用的模組，所以並沒有顯示可使用的 Webmin 模組。

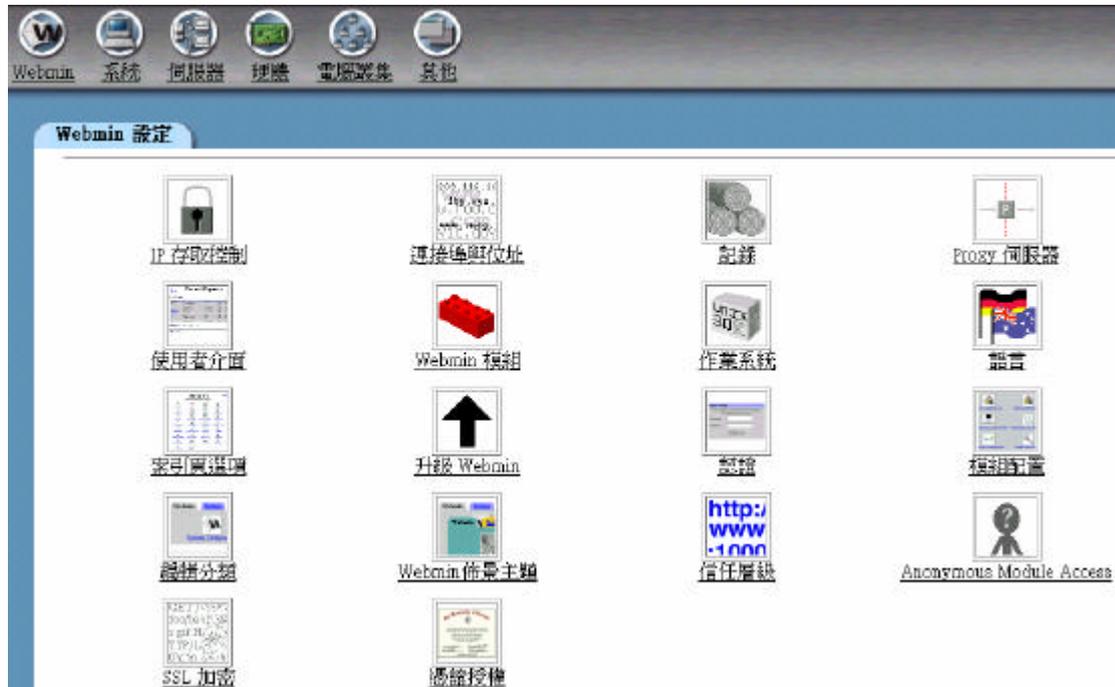


#### 1-4 Webmin 組態管理

我們可以設定我們 Webmin 的組態。我們在 Webmin 選取 Webmin 組態。



這就是 Webmin 的組態設定，有 IP 存取控制、連接埠與位址、記錄、Proxy 伺服器、使用者介面、Webmin 模組、作業系統、語言、索引頁選項、升級 Webmin、認證、模組配置、編輯分類、Webmin 佈景主題、信任層級、Anonymous Module Access、SSL 加密、憑證授權。



## IP 存取控制：



### IP 存取控制

Webmin 伺服器可以設定拒絕或允許使用此格式之特定 IP 位址的存取。主機名稱（例如 flash.aasir.com）與 IP 網路（例如 61.218.29.0 或 61.218.29.0/255.255.255.248）都可以被輸入。只有八個 IP 位址允許輸入。我們應該僅允許讓可信任的位址存取伺服器，特別是在可從 Internet 存取的情況下。否則，只要有人猜對了您的密碼，他就可以完全控制您的系統。

#### IP 存取控制

Webmin 伺服器可以設定拒絕或允許使用此格式之特定 IP 位址的存取。主機名稱（例如 foo.bar.com）與 IP 網路（例如 10.254.3.0 或 10.254.1.0/255.255.255.128）都可以被輸入。您應該僅允許讓可信任的位址存取伺服器，特別是在可從 Internet 存取的情況下。否則，只要有人猜對了您的密碼，他就可以完全控制您的系統。

##### 存取控制

允許所有的位址

僅允許列出的位址

拒絕列出的位址

Resolve hostnames on every request

61.218.29.5

連接埠與位址：



連接埠與位址

我們如果執行 Webmin 的主機上有多個 IP 位址，我們可以使用此格式將伺服器設定成只接聽一個位址。Webmin 接聽的連接埠也是在此設定。注意：我們的 web 瀏覽器可能會在變更連接埠或連結位址後提示我們重新登入。我們設定的接聽連接埠為 5000。

**IP 位址與連接埠**

接聽 IP 位址  全部

接聽連接埠

儲存

記錄：



記錄

Webmin 可以標準 CLF 記錄檔格式設定寫入 web 伺服器使用記錄。如果記錄功能被啟動，我們也可以選擇要記錄 IP 位址或主機名稱、以及多久清除一次記錄檔。啟動時，記錄會被寫入檔案 /var/good/miniserv.log。當紀錄啟用時，Webmin 將會寫入更多關於使用者動作的詳細紀錄到檔案 /var/good/webmin.log。這個紀錄將可以用 Webmin 動作紀錄模組 來瀏覽和分析 Webmin 使用者做過的事情。

**Web 伺服器記錄**

關閉記錄

啟動記錄

記錄解析的主機名稱

每  個小時清除記錄

紀錄所有使用者

只紀錄動作依..

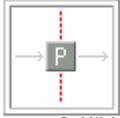
紀錄所有模組動作

只紀錄動作在 ..

依動作紀錄變更產生檔案

- BIND 4 DNS 伺服器
- BIND 8 DNS 伺服器
- CVS Server
- Configuration Engine

Proxy 伺服器：



Proxy 伺服器

我們如果執行 Webmin 的主機隱藏在防火牆或類似的東西之後，我們可能需要 proxy 伺服器以存取 web 或 FTP 站台。某些模組，例如軟體封裝，將會使用 proxy 伺服器以下載檔案或程式。

| proxy 伺服器      |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| HTTP proxy 伺服器 | <input checked="" type="radio"/> 無 <input type="radio"/> <input type="text"/> |
| FTP proxy 伺服器  | <input checked="" type="radio"/> 無 <input type="radio"/> <input type="text"/> |
| 沒有 proxy 伺服器給  | <input type="text"/>                                                          |
| proxy 帳號       | <input type="text"/>                                                          |
| proxy 密碼       | <input type="text"/>                                                          |

使用者介面：

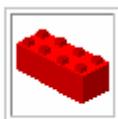


使用者介面

這個格式可以任您編輯所有模組使用的使用者介面選項。輸入顏色時，我們必須使用標準 RGB 系統指定每個顏色，也就是範圍在 00 到 ff 的十六進位數字。

| 使用者介面選項     |                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| 網頁背景        | <input checked="" type="radio"/> 預設值 <input type="radio"/> R <input type="text"/> G <input type="text"/> B <input type="text"/> |
| 一般文字        | <input checked="" type="radio"/> 預設值 <input type="radio"/> R <input type="text"/> G <input type="text"/> B <input type="text"/> |
| 表格背景        | <input checked="" type="radio"/> 預設值 <input type="radio"/> R <input type="text"/> G <input type="text"/> B <input type="text"/> |
| 表格標題        | <input checked="" type="radio"/> 預設值 <input type="radio"/> R <input type="text"/> G <input type="text"/> B <input type="text"/> |
| 連結文字        | <input checked="" type="radio"/> 預設值 <input type="radio"/> R <input type="text"/> G <input type="text"/> B <input type="text"/> |
| 是否將標題顯示成文字? | <input type="radio"/> 是 <input checked="" type="radio"/> 否                                                                      |
| 顯示登入和主機名稱   | <input type="text" value="在瀏覽器下方"/>                                                                                             |
| 傳送回饋到       | <input type="radio"/> feedback@webmin.com <input checked="" type="radio"/> chaiyen@cml.hinet.net                                |

Webmin 模組：



Webmin 模組

作業系統：



作業系統

這個格式允許我們變更 Webmin 認定的作業系統。當我們將電腦升級成新的作業系統版本，這個功能會很有用。注意，即使新舊系統之間有差異，已經安裝的模組設定一樣不會變更。

執行程式、以及將共用程式庫傳給任何程式時，我們也可以變更 Webmin 使用的搜尋路徑。

語言：



語言

索引頁選項：



索引頁選項

這個頁面可以讓我們定義您要在索引頁的每一列顯示多少圖示

| 索引頁選項                       |                                                            |
|-----------------------------|------------------------------------------------------------|
| 欄數                          | <input type="radio"/> 預設 <input type="text" value=""/>     |
| 要分類群組嗎？                     | <input type="radio"/> 是 <input type="radio"/> 否            |
| 預設分類                        | Webmin <input type="text"/>                                |
| 使用其它標題                      | <input type="radio"/> 是 <input checked="" type="radio"/> 否 |
| 顯示版本,主機名稱和作業系統?             | <input type="radio"/> 是 <input type="radio"/> 否            |
| 如果使用者只有一個模組可使用時，是否直接跳到該模組中？ | <input type="radio"/> 是 <input checked="" type="radio"/> 否 |

升級 Webmin :



升級 Webmin

這個表單可以讓您將整個安裝的 Webmin 升級到新的版本。您可以從本機檔案、上傳檔案或從 [www.webmin.com](http://www.webmin.com) 所提供的最新版本安裝。就如同手動升級一樣，所有的設定與協力廠商模組都會被保留。

認證 :



認證

當啟用密碼逾時保護時，使我們的 Webmin 伺服器免於同一使用者連續阻斷服務攻擊而使暴力破解密碼的攻擊者的入侵。

當 session 認證啟用時,Webmin 可以根據使用者的 session 來判斷是否閒置而自動登出使用者，注意當啟用或停用 session 認證時，會迫使所有使用者要重新登

入。

**認證和 session 選項**

- 停用密碼逾時
- 啟用密碼逾時
  - 禁止登入失敗次數超過  次的主機在  秒內再次登入。
  - 在syslog紀錄被禁止的主機, 登入和認證失敗的資料。
- 停用 session 認證
- 啟用 session 認證
  - 在閒置  分鐘後自動登出
  - 顯示記得上次登入?
  - 顯示主機名稱在登入畫面?
  - No pre-login page  Show pre-login file
- 每次均需要輸入帳號和密碼
- 允許本地端不用驗證使用者密碼
- 如果可以的話，使用Unix的PAM認證
- 絕不使用Unix的PAM認證
- 如果PAM無效或是停用的，從檔案  第  到  列讀取使用者和密碼

模組配置：



模組配置

這表單可以讓我們配置哪個模組的分類應顯示在 Webmin 首頁上

| 配置模組分類                    |      |
|---------------------------|------|
| Apache 網頁伺服器              | 伺服器  |
| BIND 8 DNS 伺服器            | 伺服器  |
| CVS Server                | 伺服器  |
| Cluster Users and Groups  | 電腦叢集 |
| Command Shell             | 其他   |
| DHCP 伺服器                  | 伺服器  |
| Fetchmail Mail Retrieval  | 伺服器  |
| Heartbeat Monitor         | 電腦叢集 |
| Linux 開機組態                | 硬體   |
| MON Service Monitor       | 系統   |
| MySQL 資料庫伺服器              | 伺服器  |
| NIS 客戶端和伺服器               | 系統   |
| PPP 使用者與密碼                | 伺服器  |
| Postfix 組態                | 伺服器  |
| ProFTP Server             | 伺服器  |
| QMail Configuration       | 伺服器  |
| SSL Tunnels               | 伺服器  |
| B I N D 伺服器               | 伺服器  |
| CD 燒錄                     | 硬體   |
| Cluster Software Packages | 電腦叢集 |
| Cluster Webmin Servers    | 電腦叢集 |
| Configuration Engine      | 電腦叢集 |
| FTP 伺服器                   | 伺服器  |
| GRUB 開機管理                 | 硬體   |
| Jabber IM Server          | 伺服器  |
| Linux 磁碟陣列                | 硬體   |
| Makrdomo 郵遞列表管理者          | 伺服器  |
| NFS 匯出                    | 系統   |
| PAM 認證                    | 系統   |
| Peri 模組                   | 其他   |
| PostgreSQL 資料庫伺服器         | 伺服器  |
| Procmal Mail Filter       | 伺服器  |
| SSH Server                | 伺服器  |
| Samba 網路檔案分享              | 伺服器  |

編輯分類：



編輯分類

這表單可以讓我們更名應存在的 Webmin 分類和新增一個分配模組，上方的表格可以改變內建分類的描述，而下方的表格可以新增一個分類 ID 和描述。

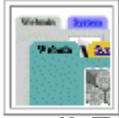
| 分類ID和描述         |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| <b>webmin</b>   | <input checked="" type="radio"/> 預設 (Webmin) <input type="radio"/> <input type="text"/> |
| <b>servers</b>  | <input checked="" type="radio"/> 預設 (伺服器) <input type="radio"/> <input type="text"/>    |
| <b>net</b>      | <input checked="" type="radio"/> 預設 (網路) <input type="radio"/> <input type="text"/>     |
| <b>system</b>   | <input checked="" type="radio"/> 預設 (系統) <input type="radio"/> <input type="text"/>     |
| <b>cluster</b>  | <input checked="" type="radio"/> 預設 (電腦叢集) <input type="radio"/> <input type="text"/>   |
| <b>hardware</b> | <input checked="" type="radio"/> 預設 (硬體) <input type="radio"/> <input type="text"/>     |
| <b>syslet</b>   | <input checked="" type="radio"/> 預設 (網管) <input type="radio"/> <input type="text"/>     |
| <b>info</b>     | <input checked="" type="radio"/> 預設 (資訊) <input type="radio"/> <input type="text"/>     |
| <b>other</b>    | <input checked="" type="radio"/> 預設 (其他) <input type="radio"/> <input type="text"/>     |

| ID                   | Displayed description |
|----------------------|-----------------------|
| <input type="text"/> | <input type="text"/>  |

儲存分類

Webmin 佈景主題；



Webmin 佈景主題

佈景主題是用來控制 Webmin 使用者介面外觀，包含圖示、顏色、背景和有些頁面的版面配置，下方的選單可以用來選一個佈景主題在您的系統上。

我們也可以選取 KDE 的佈景。

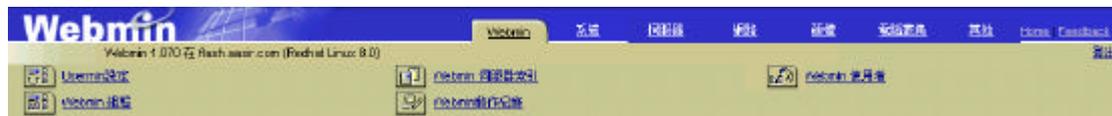
預設 Webmin 佈景主題

Caldera Theme

KDE-style loon Theme

MSC.Linux Theme

這就是修改成 Caldera Theme 的佈景主題。



我們也可以使用下方的表單來安裝一個新的 Webmin 佈景主題在您的系統上，佈景主題套件型態可能是 .wbt 檔案，但如果我們的作業系統支援的話，也可以安裝 RPM 檔案。

從本機檔案  ...

從上傳的檔案  瀏覽...

從 FTP 或 HTTP URL

安裝佈景主題

信任層級：



可以讓我們配置 Webmin 支援的的信任層級，用來預防惡意的連結從其他網站控制我們的瀏覽器在 Webmin 中進行危險行為，不過，如果我們從自己的網站連結，則我們信任下方清單的網址。

啓用來源檢查?  是  否

信任網站

信任未知來源連結

Anonymous Module Access：



Anonymous Module Access

我們可以授權使用者不用登錄就可以使用的模組。我們使用這個時，要小心有人使用這來攻擊我們的系統。

| URL path             | Webmin user          | URL path             | Webmin user          |
|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

儲存

SSL 加密：



SSL 加密

在使用 SSL 加密之前，我們要先安裝 SSL 軟體。

<http://www.openssl.org/> 我們可以到這網站來下載安全加密軟體 它提供我們網路層的安全(Secure Socket Layer)，和傳輸層的安全(Transport Layer)。



這是我們的下載區，我們可以下載 `openssl-0.9.6.g.tar.gz` 的檔案。



下載之後我們可以安裝。

```
$./config
$ make
$ make test
$ make install
```

我們將我們所下載的 openssl-0.9.\*解壓縮。

```
[root@flash webmin]# tar -zxvf openssl-0.9.6g.tar.gz
```

我們可以設定 openssl 的組態。我們使用 ./config。

```
[root@flash openssl-0.9.6g]# ./config
```

我們可以編譯 openssl。我們使用 make。

```
[root@flash openssl-0.9.6g]# make
```

編譯完成後我們要測試編譯的情況，我們使用 make test。

```
[root@flash openssl-0.9.6g]# make test
```

如果測試沒有問題我們就可以安裝 openssl 了。我們使用 make install 來安裝。

```
[root@flash openssl-0.9.6g]# make install
```

我們選取 webmin 組態，再選取 SSL 加密。



SSL 加密

#### SSL 加密

Net::SSLLeay perl 模組似乎沒有安裝在您的系統上，要安裝 OpenSSL 函數庫和 Net::SSLLeay，遵循此資訊頁面 在 Webmin 網站

我們發現 Net::SSLLeay perl 模組沒有安裝在我們的系統上，因此要安裝 OpenSSL 函數庫和 Net::SSLLeay。

因為我們使用瀏覽器來管理遠端的 webmin 伺服器，在這資料的傳遞是沒有使用保密的措施，因此資料容易被人劫取。因此我們使用 SSL 來加密 Webmin 的資料。

我們已經安裝好 OpenSSL 加密軟體，現在我們要下載 Net::SSLLeay perl，

Net::SSLLeay perl 會使用 perl 來呼叫 OpenSSL 加密函數。我們可以從 Webmin 的網站下載 Net\_SSLLeay.pm-1.15.tar.gz，<http://www.webmin.com/download/>。

|                                                                                     |                                            |                   |                              |
|-------------------------------------------------------------------------------------|--------------------------------------------|-------------------|------------------------------|
|  | <a href="#">Parent Directory</a>           | 15-Aug-2002 06:20 | -                            |
|  | <a href="#">Net_SSLLeay.pm-1.15.tar.gz</a> | 23-May-2002 16:32 | 61k GZIP compressed docume>  |
|  | <a href="#">contrib/</a>                   | 20-Aug-2000 21:08 | -                            |
|  | <a href="#">modules/</a>                   | 01-Jul-2002 00:14 | -                            |
|  | <a href="#">saprouter.wbm</a>              | 12-Jan-2001 20:21 | 110k                         |
|  | <a href="#">webmin-0.992.tar.gz</a>        | 08-Jul-2002 19:29 | 5.0M GZIP compressed docume> |

安裝 Net\_SSLeay.pm-1.06.tar.gz。

```
build OpenSSL as per instructions in that package

gunzip <Net_SSLeay.pm-1.06.tar.gz | tar xvf -
cd Net_SSLeay.pm-1.14
./Makefile.PL -t # builds and tests it
make install # You probably have to su to root to do this
perldoc Net::SSLeay # optional, but highly recommended
perldoc Net::SSLeay::Handle
```

我們將我們所下載的 Net\_SSLeay 給解壓縮。

```
[root@flash webmin]# tar zxvf Net_SSLeay.pm-1.15.tar.gz
```

解壓縮後檔案會放到 Net\_SSLeay.pm-1.15。

```
[root@flash webmin]# cd Net_SSLeay.pm-1.15
```

```
[root@flash Net_SSLeay.pm-1.15]# ls
Changes Makefile.PL ptrcasttst.c README SSLeay.xs
Credits MANIFEST ptrtstrun.pl README.Win32 test.pl
examples Net-SSLeay-Handle-0.50 QuickRef SSLeay.pm typemap
[root@flash Net_SSLeay.pm-1.15]# ./Makefile.PL
```

我們現在使用 ./Makefile.PL -t 來建立和測試檔案。

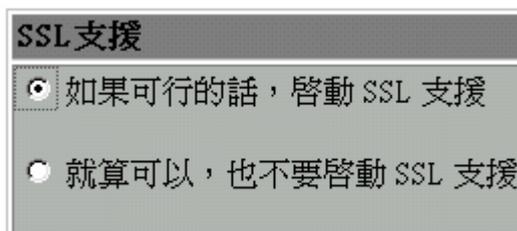
```
[root@flash Net_SSLeay.pm-1.15]# ./Makefile.PL -t
```

我們使用 make install 來安裝。

```
[root@flash Net_SSLeay.pm-1.15]# make install
```

我們重新選取 Webmin 組態，我們選取使用 SSL。如果安裝成功就會顯示 SSL 支援。

如果 Webmin 所使用的主機有安裝 SSLeay Perl 模組。我們使用這個的話，Webmin 將支援在瀏覽器和伺服器間的 SSL 加密通訊。如果我們透過 Internet 存取我們的 Webmin 主機，應該要使用 SSL 以防止駭客擷取到我們的 Webmin 密碼。警告，只有在我們的瀏覽器支援 SSL (例如 Netscape 或 IE)，而且沒有防火牆阻攔瀏覽器和 Webmin 主機之間的 https 要求時，才能打開 SSL 支援。



我們現在使用 <https://flash.aasir.com:5000> 來使用加密通訊來登錄管理 Webmin。



SSL 是密碼協定，它允許兩台電腦來作安全上的溝通，所以只有它們兩台電腦可以傳送接收到雙方的信息。SSL 這是我們目前在最常在網路上運用的保密協定，因此它為瀏覽器和網站的標準。

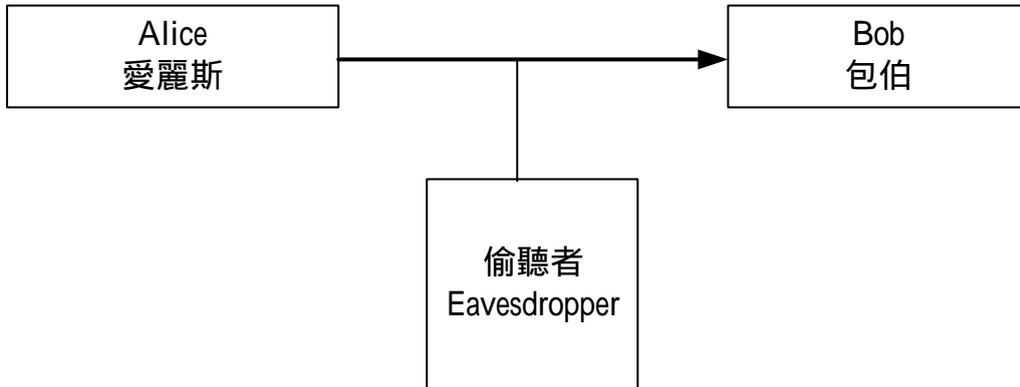
SSL 協定是我們使用者端(Client)和伺服器端(Server)安全溝通的保帳。我們假設我們在伺服器端已經獲得認證，而這認證是從 CA(認證公司所發給)。

認證包含：

獨一無二的網址(DNS)。

伺服器端的編碼演算法 E(ks)。

# SSL安全傳輸訊息概念



E:編碼演算法(Encoding algorithm)

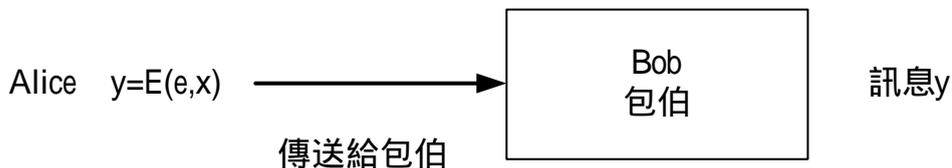
D:解碼演算法(Decoding algorithm)

這兩個是公開給大眾的

e:編碼之鑰 Encoding key

d:解碼之鑰 decoding key

X 訊息是由  $\{0,1\}^*$  二進位所組成。X  $\{0,1\}^*$   
 愛麗斯使用 e 編碼之鑰將 x 訊息編碼成 y，再將它傳送給包伯。



當包伯收到訊息y然後解碼

$$D(d,y)=x$$

$$D(d,E(e,x))=x$$

$$E(e,x)=e \cdot x, D(e,y)=e \cdot y$$

$$((x \cdot e) \cdot e)=x$$

公開之鑰保密機：

愛麗斯藉由計算和傳送  $E(e,x)$  將訊息 x 送給包伯。

$D(E(e,x))=x$  只要解碼就可以得到 x。

這個重點是偷窺者(駭客)很難從 e 來計算求出 d，而且如果不知到 d 將很難計算從 y 來得到 x。

$$y=x^e \pmod{pq}$$

$$e \cdot d=1+k \cdot (pq)$$

在密碼學中未加密的資訊稱為明文，加密過後的資訊叫作密文。我們使用者將明文加密然後將密文傳給收件者，收件者只要有密鑰，就可以將密文轉換成明文，然後得取資訊。竊取者如果竊取傳輸中的密文，但沒有解密的密鑰，也是無法得到明文。簡單的解釋 P 為明文 E 為加密的函數 D 為解密的密鑰， $D(E(P))=P$ 。 $D(E(P))=P$  表示當 P 經 E 加密後再經過 D 解密就可以得到原來的 P 了。

憑證授權：



憑證授權

我們的 Webmin 已經設定成憑證授權。我們可以使用此格式來重新設定，但是所有已經發給使用者的憑證都會失效。

| 建立新的 CA 憑證                            |                      |
|---------------------------------------|----------------------|
| 授權名稱                                  | <input type="text"/> |
| 電子郵件位址                                | <input type="text"/> |
| 部門                                    | <input type="text"/> |
| 組織                                    | <input type="text"/> |
| 州(省)                                  | <input type="text"/> |
| 國家碼                                   | <input type="text"/> |
| <input type="button" value="設定憑證授權"/> |                      |