



Splunk 4.0 安裝手冊

目錄索引

1	安裝前注意事項	2
2	WINDOWS 安裝說明.....	4
3	LINUX 安裝說明	8
4	其他注意事項	9
	註記	10

概要說明

此文件為精誠資訊所提供，目的為使客戶第一次安裝 Splunk 時可快速完成基本配置

用戶請於 www.splunk.com 登錄帳號，以便下載 Splunk 安裝軟體與相關資源。

請注意此份安裝文件依照 Splunk 3.4.6 版本為製作依據，非此最後版本安裝，請參考以下網址查詢最新安裝方式與相關信息。

www.splunk.com/base

最後更新時間: 2009/7



1 安裝前注意事項

安裝前請先確認 Splunk 最低硬體與作業系統配置需求，請參考以下資訊後，配置相關硬體。

以下為硬體配置建議

Splunk 建議的硬件平台是要求大於以下規格：

Non-Windows platforms	2x quad-core Xeon, 3GHz, 8GB RAM, RAID 0 or 1+0, with a 64 bit OS installed.
Windows platforms	2x quad-core Xeon, 3GHz, 8GB RAM, RAID 0 or 1+0, with a 64 bit OS installed.

如果只是單純的轉送數據 (Light Forwarder)，建議配置如下：

Recommended	Dual Core 1.5Ghz+ processor, 1GB+ RAM
Minimum	1.0 Ghz processor, 512MB RAM

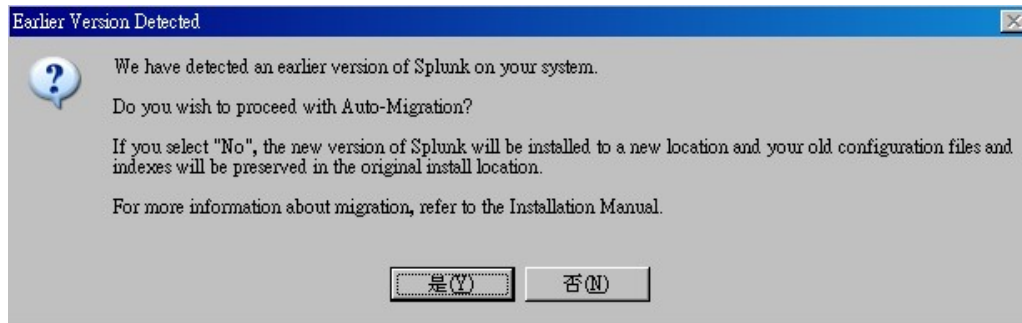
以下為作業系統支援

- Solaris 9, 10 (x86, SPARC)
- Linux Kernel vers 2.6.18 and above (x86)
- FreeBSD 6.1 and 6.2 (x86)
- Windows 2003 (64-bit, supported but not recommended on 32-bit)
- Windows 2008 (64-bit, supported but not recommended on 32-bit)
- WindowsXP (32-bit)
- Vista (32-bit, 64-bit)
- MacOSX 10.5 (32-bit)
- AIX 5.2 5.3

請使用 Firefox 2 and 3.0.x 、Internet Explorer 7 and 8 、Safari 3 以上版本為 Splunk 使用的瀏覽器，並確認有安裝 Adobe Flash 9 功能。

3.X 升級 4.0 特別說明：

直接安裝的過程中，會出現以下畫面，是提醒已經安裝 Splunk 3.X 的用戶，可以透過自動升級程式進行資料轉換，當您選擇 [否] 時，Splunk 4.0 會安裝在另一個目錄與使用其他的 Service Port。



目前已知不能轉換的資訊如下：

1. 3.X 的 Dashboard 不會出現在 4.0 上
2. 3.X 系統設定，在 4.0 上不會生效

2 Windows 安裝說明

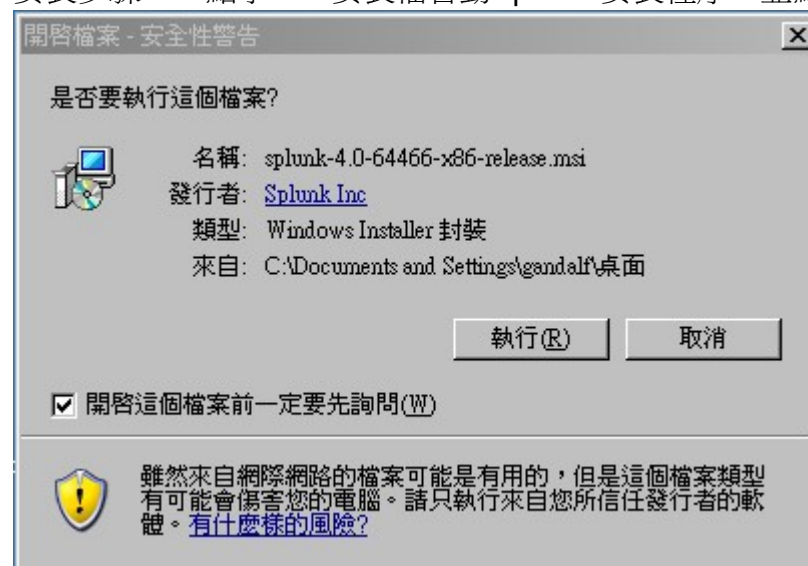
以下為安裝 Windows 前建議與注意事項，請先閱讀並檢視目前平台配置後開始安裝：

1. 建議使用 64bit 硬體與 64bit windows 作業系統
2. 建議使用英文版 windows 作業系統
3. 請確當前使用者為最高管理權限者 Administrator
4. 請確認安裝目的磁碟（一般預設為 C:/）剩餘空間大於 10GB
5. 請確認不必要的服務與程式已經關閉

以下使用 Windows XP 中文版為安裝範例（建議安裝語系仍為英文版）

安裝步驟一、下載最新 Splunk MSI 安裝程式

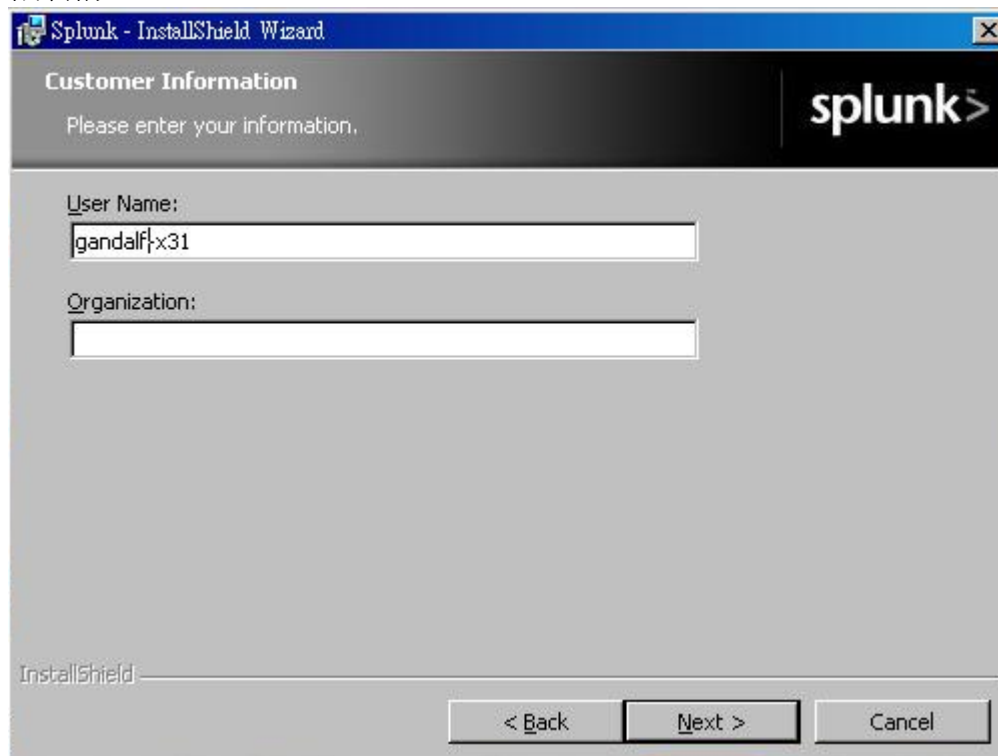
安裝步驟二、點擊 MSI 安裝檔啟動 splunk 安裝程序，並點選<執行>



安裝步驟三、點擊<Next>頁面直至授權說明，確認您以詳讀授權使用後，點擊<Next> 進行下一安裝步驟

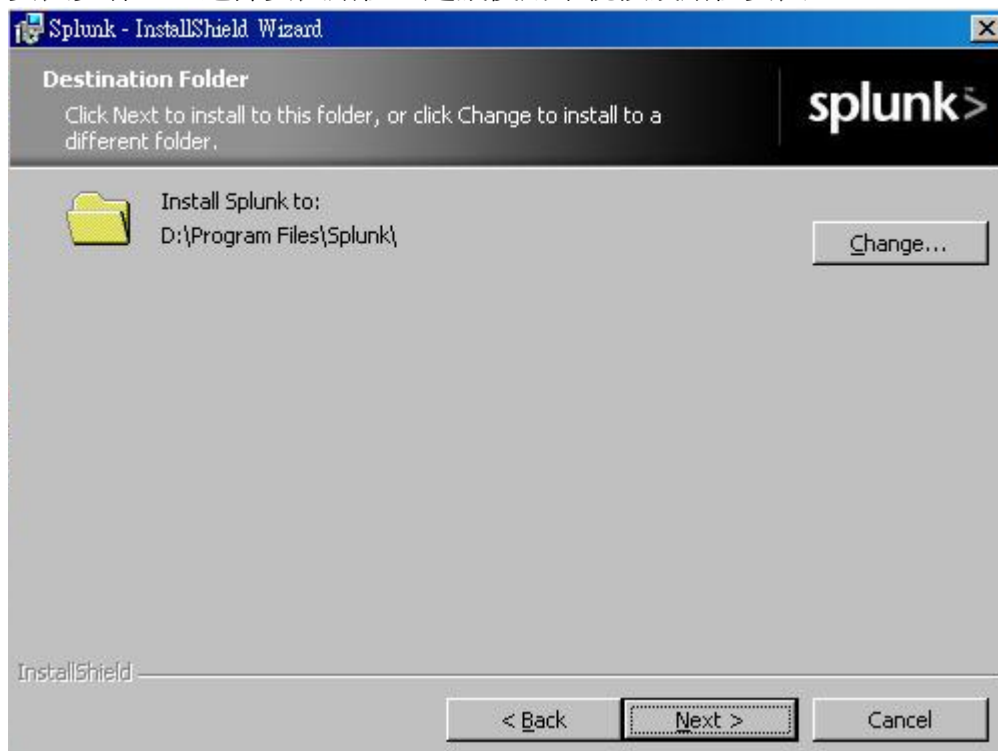


安裝步驟四、請輸入使用者(非 Splunk 使用者帳號，預設為電腦名稱)名稱與組織名稱



The screenshot shows the 'Customer Information' window of the Splunk - InstallShield Wizard. The window has a blue title bar with the text 'Splunk - InstallShield Wizard' and a close button. Below the title bar is a dark header area with the 'splunk' logo. The main content area is light gray and contains the text 'Please enter your information.' followed by two input fields: 'User Name:' with the text 'gandalf-x31' and 'Organization:' which is empty. At the bottom, there is a progress bar labeled 'InstallShield' and three buttons: '< Back', 'Next >', and 'Cancel'.

安裝步驟五、選擇安裝路徑，建議使用系統預設路徑安裝

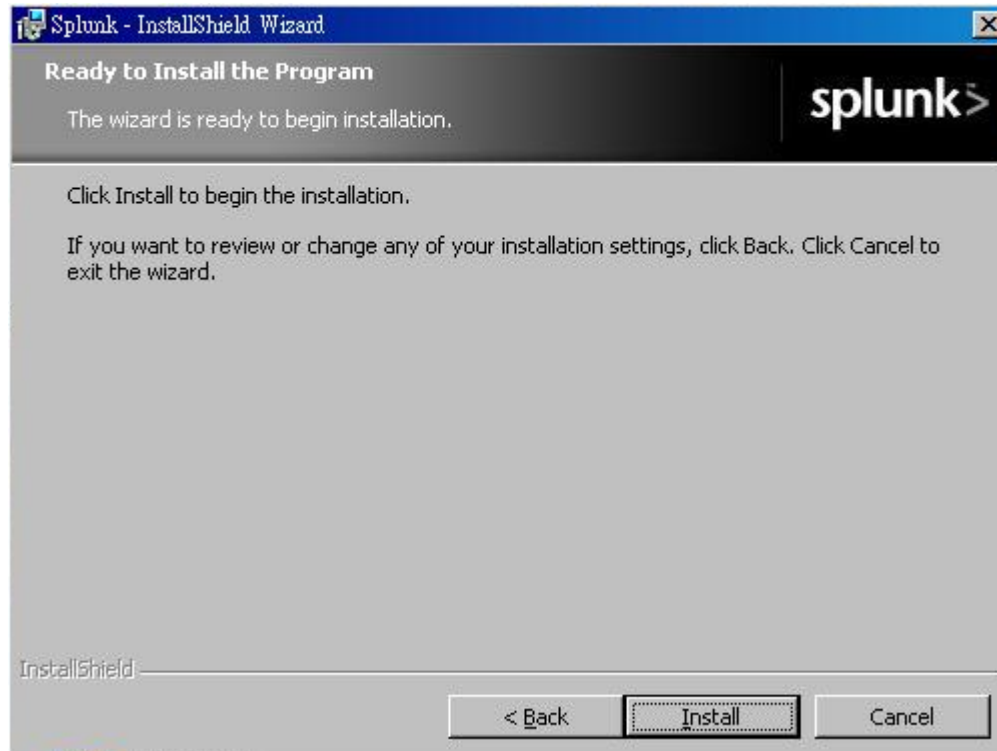


The screenshot shows the 'Destination Folder' window of the Splunk - InstallShield Wizard. The window has a blue title bar with the text 'Splunk - InstallShield Wizard' and a close button. Below the title bar is a dark header area with the 'splunk' logo. The main content area is light gray and contains the text 'Click Next to install to this folder, or click Change to install to a different folder.' followed by a folder icon and the text 'Install Splunk to: D:\Program Files\Splunk\'. To the right of this text is a 'Change...' button. At the bottom, there is a progress bar labeled 'InstallShield' and three buttons: '< Back', 'Next >', and 'Cancel'.

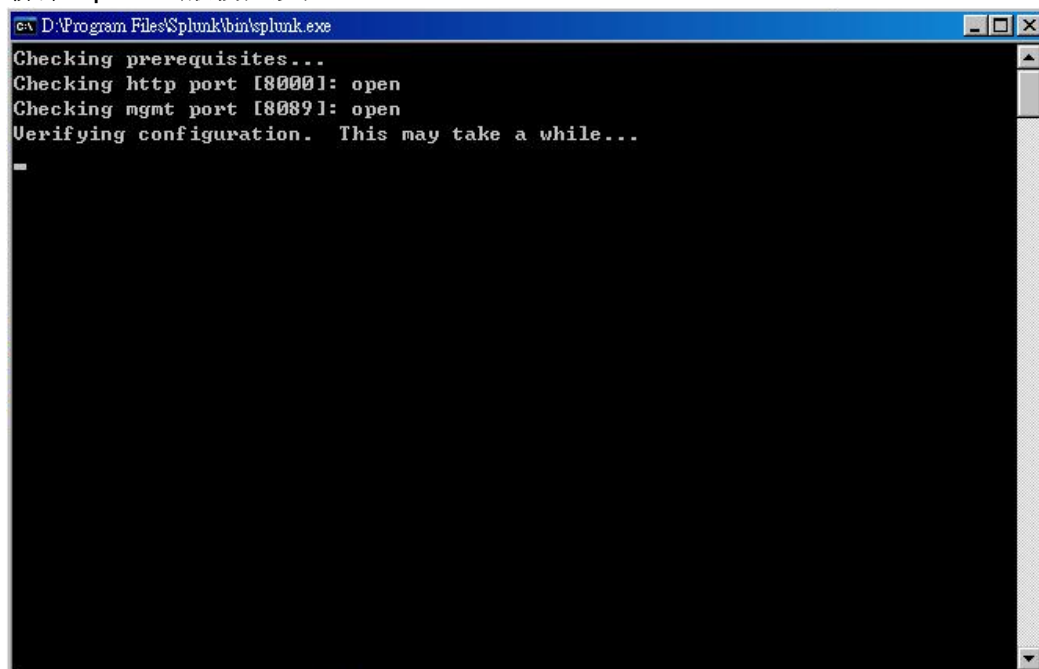
安裝步驟六、splunk 安裝後會啟動兩個服務，一者為 Splunkd 管理服務，另一為 SplunkWeb 服務，如您是系統之最高管理者 Administrator，請選擇 Local system user，如您不確定，請詢問您的系統管理者。



安裝步驟七、確認上述安裝資訊後，進入以下畫面，點擊 <Install>進行安裝



安裝步驟八、安裝過程中會進入 CLI 模式，如您停留在此畫面超過五分鐘，請聯繫 splunk 服務人員

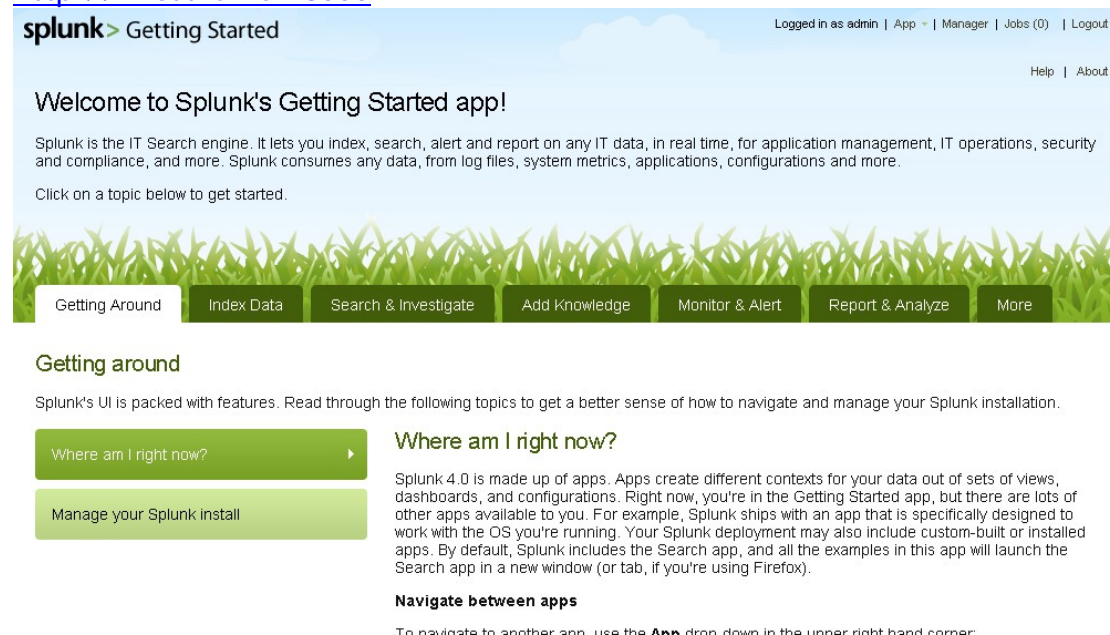


安裝步驟九、在 3.X 的版本中，會開啓 WMI 選項，取得基本資訊(Windows Event Log)、登錄檔監控、CPU 使用狀態、RAM 使用狀態、本地磁碟使用狀態與磁碟剩餘空間檢視。但在 Splunk 4.0 預設是全部開啓，所以使用者不需要額外勾選，比 3.X 方便的是，全部是以 Splunk Web UI 做控制，讓使用者不需要進行額外設定檔設定。

安裝步驟十、當您到達此畫面時，代表您已經成功安裝 Splunk 與您的系統中，請注意整段安裝過程時間應小於 5 分鐘，如安裝時間超過上述時間，請重新檢視您的硬體、作業系統的配置符合 splunk 最低要求。



安裝步驟十一、請確認您的瀏覽器使用 Mozilla FireFox 1.5 以上版本，一般路徑為 <http://localhost:8000> 預設的服務 Port 為 8000 或為 <http://<hostname>:8000>



3 Linux 安裝說明

以下為安裝 Linux 前建議與注意事項，請先閱讀並檢視目前平台配置後開始安裝：

1. 建議使用 64bit 硬體與 64bit Linux 作業系統
2. 建議使用英文版 Linux 作業系統
3. 請確當前使用者為最高管理權限者 root
4. 請確認安裝目的磁碟（一般預設為/opt/）剩餘空間大於 10GB
5. 請確認不必要的服務與程式已經關閉

Splunk 在 Linux 系統上可使用 rpm, deb 與 tarball 方式安裝，以下使用 Redhat rpm 程式為安裝範例

安裝步驟一、下載最新 Splunk rpm 安裝程式，並進行安裝

```
rpm -i splunk_package_name.rpm
```

安裝步驟二、如您需要安裝在不同目錄，請參考以下指令

```
rpm -i --perfix=/opt/new_directory splunk_package_name.rpm
```

安裝步驟三、如您需要於系統開機時自動啟動 splunk，請使用以下指令

```
./splunk start -accept-license  
./splunk enable boot-start
```


安裝步驟四、請確認您的瀏覽器使用 Mozilla FireFox 1.5 以上版本，一般路徑為 <http://localhost:8000> 預設的服務 Port 為 8000 或為 <http://<hostname>:8000>

The screenshot shows the 'Getting Started' app in the Splunk interface. At the top, it says 'splunk > Getting Started' and 'Logged in as admin | App | Manager | Jobs (0) | Logout'. Below this is a 'Welcome to Splunk's Getting Started app!' message. A description states: 'Splunk is the IT Search engine. It lets you index, search, alert and report on any IT data, in real time, for application management, IT operations, security and compliance, and more. Splunk consumes any data, from log files, system metrics, applications, configurations and more. Click on a topic below to get started.' A navigation bar contains buttons: 'Getting Around', 'Index Data', 'Search & Investigate', 'Add Knowledge', 'Monitor & Alert', 'Report & Analyze', and 'More'. Below the navigation bar, the 'Getting around' section is active, showing two buttons: 'Where am I right now?' and 'Manage your Splunk install'. To the right of these buttons, the text reads: 'Where am I right now? Splunk 4.0 is made up of apps. Apps create different contexts for your data out of sets of views, dashboards, and configurations. Right now, you're in the Getting Started app, but there are lots of other apps available to you. For example, Splunk ships with an app that is specifically designed to work with the OS you're running. Your Splunk deployment may also include custom-built or installed apps. By default, Splunk includes the Search app, and all the examples in this app will launch the Search app in a new window (or tab, if you're using Firefox). Navigate between apps To navigate to another app, use the App drop-down in the upper right hand corner.'

4 其他注意事項

此份安裝手冊僅列舉 Windows 與 Linux 安裝方式，如需其他安裝說明，請至 www.splunk.com/base 參考 Installation Manual 進行安裝，或聯繫當地 Splunk 服務供應商取得支援服務。

Happy Splunk

註記

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

此份安裝手冊為基於 Splunk 建議而說明。