Solaris™ Security Toolkit 4.1
管理指南

Sun Microsystems, Inc.
www.sun.com

文件號碼：817-7656-10
2004 年 10 月，修訂版 A

請將您對本文件的意見提交至： http://www.sun.com/hwdocs/feedback

目錄

圖

表

程式碼範例

前言

本手冊包含瞭解與使用 Solaris Security Toolkit 軟體的參考資訊。本手冊主要是針對使用 Solaris Security Toolkit 軟體來鞏固 Solaris™ 作業系統 (OS) 版本 8 到 9 之安全性的人員所撰寫的，例如，管理員、諮詢人員及其他部署新的 Sun 系統或鞏固已部署的系統之安全性的人員。本手冊內的指示適用於在 JumpStart™ 模式或獨立模式下使用本軟體時。

在您閱讀本書之前

您應爲已取得 Sun 認證的 Solaris™ 系統管理員或已取得 Sun 認證的 Solaris™ 作業系統網路管理員。您亦應具備標準網路通訊協定和拓樸方面的知識。

由於本書是設計爲依照使用者對於安全性的經驗或知識的不同程度來提供其個別需求，因此使用者的經驗和知識會決定使用者使用本書的方式。

本書章節組成部分

本手冊是做爲使用者指南，其章節包含使用軟體來鞏固系統安全性的資訊、指示及準則。本書架構如下所示：

第 1 章說明 Solaris Security Toolkit 軟體的設計和用途。其中涵蓋重要元件、功能、優點及支援的平台。

第 2 章提供鞏固系統安全性的方法。其中提供在您使用 Solaris Security Toolkit 軟體鞏固系統安全性之前，可以套用的程序。

第 3 章提供下載、安裝及執行 Solaris Security Toolkit 軟體及其他安全性相關軟體的指示。

第 4 章提供如何反轉（取消）Solaris Security Toolkit 軟體在執行強化期間所做的變更之資訊和程序。

第 5 章提供配置和管理 JumpStart 伺服器以使用 Solaris Security Toolkit 軟體的資訊。

第 6 章說明如何使用 Solaris Security Toolkit 軟體來稽核（驗證）系統的安全性。請使用本章的資訊和程序來維護在強化之後所建立的安全性設定檔。

第 7 章說明如何將前述章節所提供的資訊和專業技術應用於實際的情境，以安裝和鞏固新系統的安全性。

使用 UNIX® 指令

本文件可能不包括有關基本 UNIX® 指令及程序的資訊，例如關閉系統、啓動系統及配置裝置。請參閱以下文件資料以取得相關資訊：

- 系統隨附的軟體文件資料
- Solaris 作業系統文件資料（位於下列網址）：

  `http://docs.sun.com`

Shell 提示符號

Shell	提示符號
C shell	*machine-name*%
C shell 超級使用者	*machine-name*#
Bourne shell 與 Korn shell	$
Bourne shell 與 Korn shell 超級使用者	#

印刷排版慣例

字體*	意義	範例
AaBbCc123	指令、檔案和目錄的名稱；電腦螢幕的輸出	編輯您的 .login 檔案。 使用 ls -a 列出所有檔案。 % You have mail.
AaBbCc123	您鍵入的內容，與電腦螢幕輸出不同	% **su** Password:
AaBbCc123	書名、新字或專有名詞，或是要強調的文字。以實際的名稱或數值取代指令行變數。	請參閱 *「使用者指南」* 中的第六章。 這些是*類別* 選項。 您*必須* 是超級使用者才能執行此項操作。 若要刪除檔案，請鍵入 rm *檔案名稱*。

* 您瀏覽器的設定可能與上述設定不同。

存取 Sun 文件資料

若要檢視、列印或購買各種精選的 Sun 文件資料及其本土化版本，請至：

http://www.sun.com/documentation

協力廠商網站

對於本文件提及的協力廠商網站之可用性，Sun 概不負責。對於可在或透過這類網站或資源取得的任何內容、宣傳、產品或其他資料，Sun 概不提供擔保，亦不承擔任何責任或法律責任。對於可在或透過此類網站或資源取得的任何此類內容、貨品或服務的使用或依賴而導致或相關的實際或據稱損壞或損失，Sun 概不承擔任何責任或法律責任。

相關資源

本節列出相關出版品和網站。

出版品

- Andert, Donna, Wakefield, Robin, and Weise, Joel. "Trust Modeling for Security Architecture Development," Sun BluePrints™ OnLine, December 2002, `http://www.sun.com/blueprints/1202/817-0775.pdf`.
- Dasan, Vasanthan, Noordergraaf, Alex, and Ordica, Lou. "The Solaris Fingerprint Database - A Security Tool for Solaris Software and Files," Sun BluePrints OnLine, May 2001, `http://www.sun.com/blueprints/0501/Fingerprint.pdf`.
- Englund, Martin, "Securing Systems with Host-Based Firewalls - Implemented With SunScreen Lite 3.1 Software," Sun BluePrints OnLine, September 2001, `http://sun.com/blueprints/0901/sunscreenlite.pdf`.
- Garfinkel, Simon, and Spafford, Gene. Practical UNIX and Internet Security, 2nd Edition, O'Reilly & Associates, April 1996.
- Howard, John S., and Noordergraaf, Alex. *JumpStart Technology: Effective Use in the Solaris Operating Environment*, The Official Sun Microsystems Resource Series, Prentice Hall, October 2001.
- Moffat, Darren J., FOCUS on SUN: *Solaris BSM Auditing*, `http://www.securityfocus.com/infocus/1362`
- Noordergraaf, Alex. "Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology Updated for Solaris 8 Operating Environment," Sun BluePrints OnLine, November 2000, `http://sun.com/blueprints/1100/minimize-updt1.pdf`.
- Noordergraaf, Alex. "Minimizing the Solaris Operating Environment for Security: Updated for Solaris 9 Operating Environment," Sun BluePrints OnLine, November 2002,`http://sun.com/blueprints/1102/816-5241.pdf`.
- Noordergraaf, Alex. "Securing the Sun Cluster 3.x Software," Sun BluePrints OnLine article, February 2003, `http://www.sun.com/solutions/blueprints/0203/817-1079.pdf`.
- Noordergraaf, Alex, "Securing the Sun Enterprise 10000 System Service Processors," Sun BluePrints OnLine article, March 2002, `http://www.sun.com/blueprints/0302/securingenter.pdf`
- Noordergraaf, Alex, et. al. *Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*, Sun Microsystems™, Prentice Hall Press, ISBN 0-13-100092-6, June 2002.

- Noordergraaf, Alex and Nimeh, Dina. "Securing the Sun Fire 12K and 15K Domains," Sun BluePrints OnLine article, February 2003, `http://www.sun.com/blueprints/0203/817-1357.pdf`.
- Noordergraaf, Alex and Nimeh, Dina. "Securing the Sun Fire 12K and 15K System Controllers," Sun BluePrints OnLine article, February 2003, `http://www.sun.com/blueprints/0203/817-1358.pdf`.
- Noordergraaf, Alex and Watson, Keith. "Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment," Sun BluePrints OnLine, December 2002, `http://www.sun.com/blueprints/1202/816-5242.pdf`.
- O'Donnell, Nicholas and Noordergraaf, Alex. "Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems," Sun BluePrints OnLine articles, September 2003, `http://www.sun.com/blueprints/0903/817-3340.pdf` [Part I] and `http://www.sun.com/blueprints/0903/817-3628.pdf` [Part II]
- Osser, William and Noordergraaf, Alex. "Auditing in the Solaris 8 Operating Environment," Sun BluePrints OnLine, February 2001 `http://www.sun.com/blueprints/0201/audit_config.pdf`.
- Reid, Jason M. and Watson, Keith. "Building and Deploying OpenSSH in the Solaris Operating Environment," Sun BluePrints OnLine, July 2001, `http://sun.com/blueprints/0701/openSSH.pdf`.
- Reid, Jason M. "Configuring OpenSSH for the Solaris Operating Environment," Sun BluePrints OnLine article, January 2002, `http://www.sun.com/blueprints/0102/configssh.pdf`.
- Reid, Jason. *Secure Shell in the Enterprise*, The Official Sun Microsystems Resource Series, Prentice Hall, June 2003
- *Solaris Advanced Installation Guide*, Sun Microsystems, `http://docs.sun.com`.
- *SunSHIELD Basic Security Module Guide*, Sun Microsystems, Inc., `http://docs.sun.com`.
- Watson, Keith and Noordergraaf, Alex. "Solaris Operating Environment Network Settings for Security: Updated for Solaris 9 Operating Environment," Sun BluePrints OnLine, June 2003, `http://www.sun.com/solutions/blueprints/0603/816-5240.pdf`.
- Weise, Joel, and Martin, Charles R. "Developing a Security Policy," Sun BluePrints OnLine article, December 2001, `http://www.sun.com/solutions/blueprints/1201/secpolicy.pdf`.

網站

- AUSCERT, *UNIX Security Checklist*, `http://www.auscert.org.au/render.html?it=1935&cid=1920`
- CERT/CC — `http://www.cert.org`，此爲由聯邦贊助處理電腦安全性問題的研究與發展中心。

- Chkrootkit, `http://www.chkrootkit.org`
- Galvin, Peter Baer, *The Solaris Security FAQ*, `http://www.itworld.com/Comp/2377/security-faq/`
- HoneyNet Project, "Know Your Enemy:Motives" `http://project.honeynet.org/papers/motives/`
- 列出公開檔案軟體 — `ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/`
- Nmap Port Scanner, `http://www.insecure.org`
- OpenSSH 工具 — `http://www.openssh.com/`
- Pomeranz, Hal, *Solaris Security Step by Step*, `http://www.sans.org/`
- Rhoads, Jason, *Solaris Security Guide*, `http://www.sabernet.net/papers/Solaris.html`
- Security Focus — `http://www.securityfocus.org` 爲專門研討安全性相關問題的網站。
- Sendmail Consortium, `sendmail` 配置資訊 — `http://www.sendmail.org/`
- Spitzner, Lance, *Armoring Solaris*, `http://secinf.net/unix_security/Armoring_Solaris.html`
- SSH Communications Security, Secure Shell (SSH) tool, `http://www.ssh.com/`
- Sun BluePrints OnLine, `http://sun.com/blueprints`
- Sun BluePrints OnLine Tools for FixModes software and MD5 scripts, `http://jsecom15k.sun.com/ECom/EComActionServlet?StoreId=8&PartDetailId=817-0074-10&TransactionId=try&LMLoadBalanced=`
- Sun Enterprise Authentication Mechanism™ 資訊 — `http://www.sun.com/software/solaris/ds/ds-seam`
- SunSolve℠ – `http://sunsolve.sun.com`

聯絡 Sun 技術支援

若本文件無法解決您對本產品相關技術上的疑惑，請至下列網址尋求協助：

`http://www.sun.com/service/contacting`

Sun 歡迎您的指教

Sun 一直致力於改善相關的文件資料，因此歡迎您提出批評和建議。您可至下列網站留下您的意見：

`http://www.sun.com/hwdocs/feedback`

請在您的意見中註明本文件的書名和文件號碼：

「Solaris Security Toolkit 4.1 管理指南」，文件號碼：817-7656-10

第1章

簡介

本章旨在說明 Solaris Security Toolkit 軟體的設計和用途，其中涵蓋重要元件、功能、優點及支援的平台。本章提供關於維護修改和部署的版本控制之準則，並陳述自訂 Solaris Security Toolkit 軟體的重要準則。

本章包含以下主題：

以 Solaris Security Toolkit 軟體鞏固系統安全性

Solaris Security Toolkit 軟體其非正式名稱爲 JASS (JumpStart Architecture and Security Scripts) 工具組提供一種自動、可延伸及可延展的機制來建立和維護 Solaris 作業系統之安全性。藉由 Solaris Security Toolkit 軟體，您可以對系統進行強化、最小化及稽核其安全性。

- **強化** – 修改 Solaris 作業系統配置以改善系統安全性。
- **最小化** – 移除特定系統上不需要的 Solaris 作業系統套裝模組。（由於各個系統的需求皆有差異，因此各個系統認爲不需要的亦會有所不同，且須經過評估。）移除作業將會縮減要修補和鞏固安全性的元件之數量，這也會相對縮減潛在入侵者的可用進入點。
- **稽核** – 判定系統配置是否符合預先定義的安全性設定檔之程序。

- **計分** – 分數爲在稽核執行期間與找到的錯誤數量相關的數值。因此，若找不到任何錯誤（任何類型），出現的分數就會是 0。只要偵測到一個錯誤，Solaris Security Toolkit 就會將分數（又稱爲弱點數值）增加 1 分。

系統安裝和配置應儘可能自動化（理想目標爲百分之百）。此準則包括作業系統的安裝和配置、網路配置、使用者帳號、應用程式及安全性修改。安全性修改可能包括強化和 / 或最小化（依系統用途而異）。JumpStart 軟體爲一種可用來自動化 Solaris 作業系統安裝的技術。JumpStart 軟體提供一種將系統安裝在網路上的機制（需要少量或不需人工介入操作）。Solaris Security Toolkit 軟體提供在以 JumpStart 軟體爲基礎的安裝中，實行及自動化與強化及最小化 Solaris 作業系統有關的大多作業之架構和程序檔。

此外，Solaris Security Toolkit 軟體具有獨立模式。此模式能夠提供執行與 JumpStart 模式中相同的所有強化功能，但僅限於在已部署的系統上。在任一模式中，作出的安全性修改可以且應該自訂以符合您的系統之安全性需求。

無論系統的安裝方式爲何，您皆可初始使用 Solaris Security Toolkit 軟體來強化和最小化您的系統。之後，定期使用 Solaris Security Toolkit 軟體來稽核已鞏固安全性的系統之安全性設定檔是否經過不小心或蓄意修改。

備註：*稽核* 一詞被用來說明 Solaris Security Toolkit 軟體透過比較預先定義的安全性設定檔，來驗證安全性部署的自動程序。此專有名詞在此出版品內的使用不代表保證系統在使用稽核選項後即會安全無虞。

瞭解軟體元件

本節提供 Solaris Security Toolkit 軟體元件架構的簡介。Solaris Security Toolkit 軟體爲一組檔案和目錄。圖 1-1 顯示此架構的圖例。

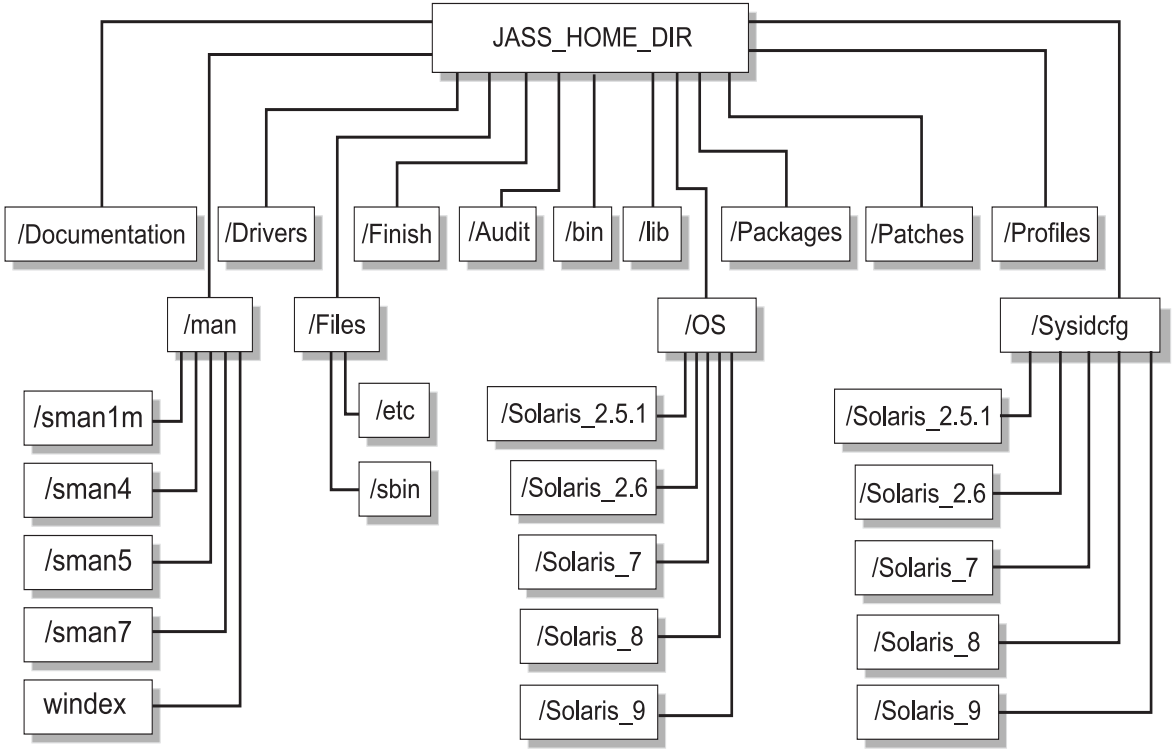

圖 1-1　軟體元件架構

除了這些目錄和子目錄，還包括位於 Solaris Security Toolkit 軟體架構頂層 `/bin` 的以下檔案：

- `add-client` — 將用戶端新增到 JumpStart 環境的 JumpStart 輔助程式。
- `rm-client` — 從 JumpStart 環境移除用戶端的 JumpStart 輔助程式。
- `make-jass-pkg` — 提供能夠從 Solaris Security Toolkit 目錄的內容建立 Solaris 作業系統套裝模組之指令，以簡化自訂 Solaris Security Toolkit 配置的內部分配。
- `jass-check-sum` — 提供能夠根據在各個 Solaris Security Toolkit 執行期間所建立的總合檢查，判定 Solaris Security Toolkit 軟體所修改的任何檔案是否已變更的指令。
- `jass-execute` — 配置 Solaris Security Toolkit 應用程式的指令。

目錄

Solaris Security Toolkit 架構的元件編排爲以下目錄：

- /Audit
- /bin
- /Documentation
- /man
- /Drivers
- /Files
- /Finish
- /lib
- /OS
- /Packages
- /Patches
- /Profiles
- /Sysidcfg

本節說明各個目錄，其中將列出適用的各個程序檔、配置檔或子目錄，及其他章節的參考資料以提供詳細資訊。

Solaris Security Toolkit 目錄架構是基於 Sun BluePrints 手冊 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」中的架構。

Audit 目錄

此目錄含有稽核程序檔，可評估系統是否符合定義的安全性設定檔或稽核程序檔。此目錄中的程序檔編排爲以下類別：

- 停用
- 啓動
- 安裝
- 最小化
- 列印
- 移除
- 設定
- 更新

如需上述各個類別中的程序檔之詳細清單及各個程序檔的說明，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

Documentation 目錄

此目錄包含具有使用者資訊的文字檔，例如 README 檔。

man 目錄

此目錄包含指令、功能和驅動程式之線上說明手冊各節的子目錄。此目錄也包含了 windex 檔，其爲指令的索引且是免費提供。

如需關於這些線上說明手冊的更多資訊，請參閱這些線上說明手冊或 「*Solaris Security Toolkit 4.1 Man Page Guide*」。

Drivers 目錄

此目錄含有配置資訊的檔案，這些配置檔案指出在執行 Solaris Security Toolkit 軟體時會執行和安裝哪些檔案。此目錄含有驅動程式、程序檔及配置檔。

以下爲 Drivers 目錄中的驅動程式和程序檔的範例：

- common_{log|misc}.funcs
- config.driver
- desktop-{config|hardening|secure}.driver
- driver.{funcs|init|run}
- hardening.driver
- finish.init
- install-Sun_ONE-WS.driver
- jumpstart-{config|hardening|secure}.driver
- secure.driver
- starfire-{config|hardening|secure}.driver
- suncluster3x-{config|hardening|secure}.driver
- sunfire_15k_domain-{config|hardening|secure}.driver
- sunfire_15k_sc-{config|hardening|secure}.driver
- sunfire_mf_msp-{config|hardening|secure}.driver
- undo.{funcs|init|run}
- hardening.driver
- user.init.SAMPLE
- user.run.SAMPLE
- audit_{private|public}.funcs

在所有產品專用的驅動程式和某些其他的驅動程式中，每個驅動程式皆包含以下三個檔案：

- *name*-secure.driver
- *name*-config.driver
- *name*-hardening.driver

這三個檔案在先前的清單中是以括號表示，例如：sunfire_15k_sc-{config|hardening|secure}.driver。這些檔案是爲了完整起見所列出的，因此在要執行驅動程式時，請只使用 *name*-secure.driver。該驅動程式會自動呼叫相關的驅動程式。

Solaris Security Toolkit 架構包括在不修改本身的實際程序檔時，啓動驅動程式、結束及用於不同的環境的稽核程序檔之配置資訊。結束和稽核程序檔中使用的所有變數被保留在一組配置檔中 — 這些配置檔是由驅動程式所匯入的，讓變數能夠在受到驅動程式呼叫時即結束並稽核程序檔。

Solaris Security Toolkit 軟體有三個主要的配置檔案，全都儲存於 `Drivers` 目錄中：

- `driver.init`
- `finish.init`
- `user.init`

驅動程式呼叫的結束程序檔位於 Finish 目錄中。驅動程式呼叫的稽核程序檔位於 Audit 目錄中。驅動程式安裝的檔案是從 Files 目錄讀取。要取得更多有關結束和稽核程序檔的資訊，請參閱本書響應章節。

圖 1-2 顯示驅動程式控制流程的流程表。

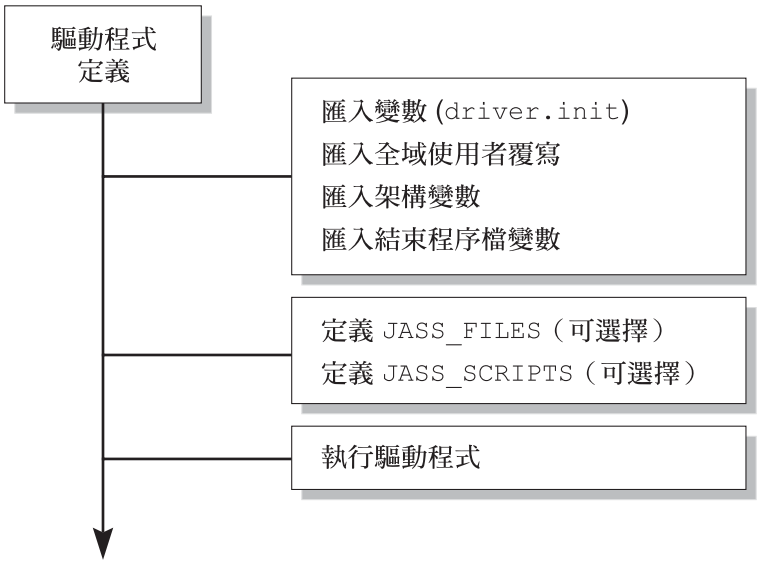

圖 1-2 驅動程式控制流程

各個 `.init` 檔案的所有環境變數都會先匯入。一旦完成之後，驅動程式就會移至第二部分，定義 `JASS_FILES` 和 `JASS_SCRIPTS`。這些定義是選擇使用的；可定義單一環境、或定義兩個環境、或不定義任何環境。驅動程式的第三部分是呼叫 `driver.run` 以執行由 `JASS_FILE` 和 `JASS_SCRIPTS` 環境變數定義的作業。

程式碼範例 1-1 展示驅動程式控制流程。

程式碼範例 1-1 驅動程式控制流程

```
DIR="`/bin/dirname $0`"

export DIR
. ${DIR}/driver.init

JASS_FILES="
                            /etc/cron.d/cron.allow
                            /etc/default/ftpd
                            /etc/default/telnetd
"

JASS_SCRIPTS="
                            install-at-allow.fin
                            remove-unneeded-accounts.fin
"
. ${DIR}/driver.run
```

此程式碼範例會設定並匯出 DIR 環境變數，這樣驅動程式才會辨識到起始目錄。接著，JASS_FILES 環境變數被定義爲含有從 JASS_HOME_DIR/Files 目錄複製到用戶端的檔案。JASS_SCRIPTS 環境變數接著會以 Solaris Security Toolkit 軟體執行的結束程序檔定義。最後，強化運行的執行會由呼叫 driver.run 驅動程式而啓動。一旦被呼叫，driver.run 會複製 JASS_FILES 指定的檔案，然後執行 JASS_SCRIPTS 指定的程序檔。

Files 目錄

此目錄是由 JASS_FILES 環境變數和 driver.run 程序檔所使用。此目錄會儲存複製到 JumpStart 用戶端的檔案。

以下檔案位於本目錄中：

- /.cshrc
- /.profile
- /etc/default/sendmail
- /etc/dt/config/Xaccess
- /etc/hosts.{allow|deny}
- /etc/init.d/nddconfig
- /etc/init.d/set-tmp-permissions
- /etc/init.d/sms_arpconfig
- /etc/init.d/swapadd
- /etc/issue
- /etc/motd
- /etc/notrouter

- /etc/rc2.d/S00set-tmp-permissions
- /etc/rc2.d/S07set-tmp-permissions
- /etc/rc2.d/S70nddconfig
- /etc/rc2.d/S73sms_arpconfig
- /etc/rc2.d/S73swapadd
- /etc/security/audit_class
- /etc/security/audit_control
- /etc/security/audit_event
- /etc/sms_domain_arp
- /etc/sms_sc_arp
- /etc/syslog.conf

Finish 目錄

此目錄含有在安裝期間執行系統修改和更新的結束程序檔。此目錄中的程序檔編排爲以下類別：

- 停用
- 啓動
- 安裝
- 最小化
- 列印
- 移除
- 設定
- 更新

如需上述各個類別中的程序檔之詳細清單及各個程序檔的說明，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

OS 目錄

本目錄只含有 Solaris 作業系統影像。這些是由 JumpStart 軟體安裝程序用來做爲用戶端安裝的原始檔，並且提供 `add_install_client` 和 `rm_install_client` 程序檔。`add_client` 程序檔可接受這些其他目錄名稱。

要取得更多有關載入及修改 Solaris 作業系統影像的資訊，請參閱 Sun BluePrints 文件「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

以下爲標準安裝命名慣例。

Solaris OS

使用以下 Solaris 作業系統的命名標準：

`Solaris_`*`os version_4 digit year_2 digit month of CD release`*

例如，Solaris 8 Operating Environment CD（日期：2001 年 4 月）的目錄名稱爲 `Solaris_8_2001-04`。隔開更新和 Solaris 作業系統的發行版本，可維持測試和部署方面的精密控制。

Trusted Solaris OS

使用以下 Trusted Solaris 的目錄命名標準：

`Trusted_Solaris_`*os version_4 digit year_2 digit month of CD release*

例如，如果 Trusted Solaris 軟體發行版本爲 2000 年 2 月，目錄名稱則爲：`Trusted_Solaris_8_2000-02`。

Solaris OS Intel Platform Edition

對 Solaris OS Intel Platform Edition 使用以下目錄命名規則：

`Solaris_`*os version_4 digit year_2 digit month of CD release*`_ia`

例如，如果 Solaris OS Intel Platform Edition 發行版本爲 2001 年 4 月，目錄名稱則爲：`Solaris_8_2001-04_ia`。

`Packages` 目錄

此目錄含有可用結束程序檔安裝的軟體套裝模組。例如，Sun Java™ System Web Server（之前爲 Sun™ ONE Web Server，更早則爲 iPlanet™ Web Server）軟體套裝模組可儲存於 `Packages` 目錄，讓適用的結束程序檔依照需求安裝軟體。

某些隨附於 Solaris Security Toolkit 軟體的結束程序檔會執行軟體安裝和基本配置功能。從 `Packages` 目錄安裝軟體的程序檔包括：

- `install-fix-modes.fin`
- `install-Sun_ONE-WS.fin`
- `install-jass.fin`
- `install-md5.fin`
- `install-openssh.fin`

`Patches` 目錄

此目錄是用來儲存 Solaris 作業系統的「建議和安全修補程式叢集」。下載需要的修補程式，然後將其解壓縮至此目錄。

藉由將修補程式置放及解壓縮到此目錄，您可以讓安裝更加順利。當修補程式解壓縮到此目錄時，Solaris Security Toolkit 軟體的修補程式安裝程序檔會進行自動化安裝，這樣您就不必爲各個系統安裝手動解壓縮修補程式叢集。

爲各個使用的 Solaris 作業系統版本建立子目錄。例如，您在 Patches 目錄內可能會有 2.5.1_Recommended 和 2.6_Recommended 目錄。

Solaris Security Toolkit 軟體可支援 Solaris OS Intel Platform Edition 修補程式叢集。這些修補程式叢集支援的命名慣例和由 SunSolve OnLine℠ 服務提供的相同。

格式爲 Solaris_<release>_x86_Recommended。Solaris 8 作業系統的 Solaris OS Intel Platform Edition 修補程式叢集會位於名爲 Solaris_8_x86_Recommended 的目錄中。

Profiles 目錄

此目錄包含所有 JumpStart 設定檔。這些設定檔包含 JumpStart 軟體用來判定要執行的安裝的 Solaris 作業系統叢集之配置資訊（例如：核心、一般使用者、開發人員或完整分發）、磁碟佈局及安裝類型（例如：獨立式）。

JumpStart 設定檔是在 rules 檔案中列出及使用，以定義建立的系統或系統群組之特定程度。

Sysidcfg 目錄

類似於 Profiles 目錄、含有僅用於 JumpStart 模式安裝的檔案之 Sysidcfg 目錄。這些檔案會提供所需的安裝資訊來自動化 Solaris 作業系統安裝。會有另一個目錄架構儲存作業系統專用的資訊。

每個 Solaris 作業系統都有其個別的目錄。對於每個發行版本，都會有一個已命名的目錄。
Solaris_*OS Version*。Solaris Security Toolkit 軟體包含用於 Solaris 作業系統版本 2.5.1 到 9 之 sysidcfg 檔案範例。

sysidcfg 檔案範例可以延伸至其他類型，例如：網路、主機等。Solaris Security Toolkit 軟體支援任意 sysidcfg 檔案。

要取得更多有關 sysidcfg 檔案的資訊，請參閱 Sun BluePrints 文件 「*JumpStart Technology:Effective Use in the Solaris Operating Environment*」。

資料儲存庫

資料儲存庫是支援 Solaris Security Toolkit 還原運行的 JASS_REPOSITORY 目錄中的一個環境變數，依照每次執行的運行來儲存資料、維護軟體所修改的明示檔、爲執行日誌儲存資料。還原功能依賴儲存於資料儲存庫中的資訊。

維護版本控制

維護 Solaris Security Toolkit 軟體使用的所有檔案和程序檔之版本控制是非常重要的，原因有二：首先，本環境的其中一個目標爲能夠重建系統安裝。如果沒有安裝時使用的所有檔案版本之快照，此目標就無法達成。第二，由於這些程序檔會執行安全性功能 — 這對許多機構而言都是相當重要的一環 — 因此實行的時候必須格外小心以確保只執行適用和已測試的變更。

Solaris 作業系統 `SUNWsprot` 套裝模組中提供了 Source Code Control System (SCCS) 版本控制套裝模組。您可以使用其他免費的以及商業軟體供應商提供的版本控制軟體以管理版本資訊。無論您使用哪種版本控制產品，請使程序就緒開始管理更新和擷取版本資訊以用於將來的系統重建。

除了版本控制，請使用整合性管理解決方案以判定檔案內容是否有經過修改。雖然系統的特權使用者或許能夠繞過版本控制系統，但他們不會輕易忽略整合性管理系統，其在遠端系統上維持整合性資料庫。整合性管理解決方案在集中化時最爲有用，這是因爲本端儲存的資料庫有可能會遭到蓄意修改。

執行支援的 Solaris 作業系統版本

Solaris Security Toolkit 軟體的 Sun 支援僅可在 Solaris 8 和 Solaris 9 作業系統下使用。雖然此軟體可以在 Solaris 2.5.1、Solaris 2.6 和 Solaris 7 作業系統下使用，但是 Sun 支援卻無法在這些作業系統下使用。

Solaris Security Toolkit 軟體會自動偵測已安裝哪個 Solaris 作業系統軟體，然後執行適用於該作業系統版本的作業。

執行支援的 SMS 版本

若您是使用 System Management Services (SMS) 來管理系統控制器 (SC)，而且使用的 SMS 版本爲 1.3 到 1.4.1，就可以使用 Solaris Security Toolkit 4.1 軟體的 Sun 支援。

配置和自訂 Solaris Security Toolkit 軟體

Solaris Security Toolkit 軟體含有預設程序檔、架構功能及變數，這些變數可實行 Sun BluePrints 文件中標題爲 「*Enterprise Security:Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*」和有關安全性的 Sun BluePrints OnLine 文摘中的所有安全性準則。這些設定並不適用於所有系統，因此您必須自訂 Solaris Security Toolkit 軟體以達到您的系統的安全性需求。

Solaris Security Toolkit 軟體其中一個最顯著的特性就是，您可以輕鬆自訂此軟體以符合您的環境、系統及需求。若要自訂 Solaris Security Toolkit 軟體，請透過驅動程式、結束程序檔、稽核程序檔、架構功能、環境變數及檔案範本來調整它的行動。

大多的使用者不需修改 Solaris Security Toolkit 程式碼。任何變更都有可能會對支援和升級造成負面影響。如果在您的環境中使用 Solaris Security Toolkit 軟體時絕對需要代碼修改，請將代碼複製到一個獨有的檔案或函數名稱，這樣您就可以如第 12 頁「準則」中所述輕鬆追蹤變更。

在這本手冊當中，自訂 Solaris Security Toolkit 軟體的準則和指示會在每章適當之處提供說明。請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」取得關於自訂驅動程式的有用資訊。自訂包括修改和建立檔案或變數。

以下章節提供自訂 Solaris Security Toolkit 軟體的範例。這些範例重點說明您可以自訂 Solaris Security Toolkit 軟體的某些方式，不過仍有多種可能性。

以下章節介紹在試圖自訂 Solaris Security Toolkit 軟體前必須清楚瞭解的資訊。這些資訊是根據從許多部署集結而成的分享經驗，讓您避免陷入一般的陷阱。

策略和需求

在自訂和部署 Solaris Security Toolkit 軟體時，適當的規劃可確保平台配置正確且符合您的機構之期望。

在您的規劃階段中，請務必從各種來源取得輸入，包括安全性策略和標準、企業法規和準則，以及供應商提供的偏好實作。

除了這些資訊以外，您也必須注意應用程式和作業需求，以確保配置不會影響到平台具備其預計的商業功能之能力。

準則

在自訂 Solaris Security Toolkit 軟體時，請注意以下準則。瞭解並觀察這些準則可讓部署程序變得較爲簡易且較具效率。

- 就一般的原則而言，請勿變更任何隨附於 Solaris Security Toolkit 軟體的*原始*檔案（驅動程式、程序檔、檔案等）。變更原始檔案會抑制並限制您的機構升級到新版 Solaris Security Toolkit 軟體的能力，這是因爲對於原始檔案的任何變更可能會被新版檔案覆寫。（您的所有自訂變更將會消失，而您系統的配置可能會變成意料外的結果。）若要自訂任何這些檔案，請先製作備份、然後修改副本、保留原始檔案不作修改。此準則只存有三個例外：`sysidcfg` 檔案、Files 目錄中的範本及當 Sun BluePrints OnLine 文摘提供指示時。
- 適當地命名您的驅動程式或程序檔副本，讓檔名與原檔名有所區別。使用能代表程序檔用途的前綴或關鍵字。例如，含有公司名稱或股票代號的前綴、部門識別碼、甚或是平台或應用程式類型等都是絕佳的命名標準。表 1-1 列出一些命名標準的範例。

表 1-1 自訂檔案的命名標準

目前檔案	命名標準
`abccorp-secure.driver`	公司前綴
`abcc-nj-secure.driver`	公司股票代號、位置
`abbcorp-nj-webserver.driver`	公司、位置、應用程式類型
`abc-nj-trading-webserver.driver`	公司、位置、機構、應用程式類型

- 檢閱以下 Solaris Security Toolkit 檔案，查看是否適用於您的系統。若要自訂這些檔案，請複製原始檔案、將副本重新命名爲 `user.init` 和 `user.run`，然後再對這些副本進行修改或新增內容。

`Drivers/user.init.SAMPLE`	用於自訂全域參數。
`Drivers/user.run.SAMPLE`	用於自訂全域函數。

- 如有需要，修改以下原始檔案。*只有*這些檔案是您應該直接修改的原始 Solaris Security Toolkit 檔案。

`Sysidcfg/*/sysidcfg`	用於 JumpStart 自動配置。
`Files/*`	用來做爲檔案範本並複製到系統上。

備註：請注意，若使用 `pkgrm` 指令移除 `SUNWjass`，`user.init` 和 `user.run` 檔案（如有建立）不會被移除。對於新增到 Solaris Security Toolkit 目錄架構的和未包含於分發中的任何客戶檔案也是如此。隨附於 Solaris Security Toolkit 分發的 Files 目錄中的檔案及 `sysidcfg` 檔案都會存在，因此會被移除。

第2章

系統安全化：套用方法

本章提供一個系統安全化的方法，其中提供在您使用 Solaris Security Toolkit 軟體鞏固系統安全性之前可以套用的程序。

本章包含以下主題：

規劃及準備

正確的規劃是成功使用 Solaris Security Toolkit 軟體以鞏固系統安全性的關鍵。在規劃階段，Solaris Security Toolkit 根據機構的安全性策略與標準，以及系統應用程式與運作需求建立系統的設定檔。此階段可分爲下列作業：

雖然本書並未涵括，本階段的考慮可能包括瞭解風險及曝光、瞭解基礎架構與其安全性需求以及考慮責任、記錄及使用稽核。

考慮風險及利益

本節呈現您在嘗試系統安全化之前必須要清楚理解的顧慮。小心的評量風險與利益，判定何種動作對您的機構是最適合的。

強化系統時，必須以特別預防來協助您確保當執行 Solaris Security Toolkit 軟體後系統仍可發揮功能。更進一步，程序確保將當機時間減少至最低是非常重要的。

備註：當已部署系統執行安全化時，對於某些狀況重新建立是最有效的，安裝期間作強化，然後重新將運作必要的軟體重新載入。

---

1. 瞭解系統服務及應用程式的需求。

   在執行 Solaris Security Toolkit 軟體之前必須辨識系統中執行的服務及應用程式。任何與服務及應用程式相關的依賴性必須列舉出來，如此可以充分的調整 Solaris Security Toolkit 的配置。如果未能如此做，可能導致一開始就會停用或者阻止必要的服務。Solaris Security Toolkit 軟體所作的變更大部分可以復原，安裝之前設定一個正確的設定檔，限制與 Solaris Security Toolkit 實現有關的潛在當機時間。

2. 將系統必須離線及重新開機納入考慮。

   要使 Solaris Security Toolkit 軟體所作的變更生效，系統必須重新開機。根據系統的重要性、所提供的服務以及是否維護視窗的適用性，機構可能面臨實施軟體的困難。仔細衡量過當機的代價相對於不加強安全性的風險之後，再作決定。

3. 系統可能需要多次的重新開機來驗證功能性。

   使系統的關鍵性服務 (mission-critical) 設定生效之前，於非生產性系統上作所有的變更。但這不是永遠可行的。例如，缺乏足夠的硬體或軟體可以正確的作目標環境的鏡射。Solaris Security Toolkit 軟體安裝之前及之後都必須作測試。系統強化之後可能還是會有無法辨識的依賴性，這些依賴性需要作疑難排解。大部分狀況，這些議題使用本章所述的技巧可以很快解決。若安裝 Solaris Security Toolkit 之後發現了功能性問題，要復原 Solaris Security Toolkit 的效果再重新開機可能是必要的，或者更進一步更改系統的安全性配置來支援或者啓用遺漏的功能。

4. 平台的安全性不只是強化及最小化。

   當考慮重塑系統配置來增強安全狀態時，重要的是要瞭解平台強化及最小化是就保護系統、服務及資料而言，只是可以做及應該做的一小部分。其他衡量標準及控制已經超出本文件的範圍，但是鼓勵您考慮與帳號管理、權限管理、檔案系統及資料完整性、主機存取的控制、入侵偵測、脆弱性掃描及分析以及應用程式安全性相關的問題。

5. 系統可能已經被利用或者有可被利用的弱點。

   要被強化的平台可能已經被攻擊者利用。對於已被利用的弱點，要 Solaris Security Toolkit 軟體提供保護可能已經太晚。若是如此，重新安裝系統，然後安裝及使用 Solaris Security Toolkit 軟體來增強安全性。

檢閱安全性策略、標準以及相關文件

系統安全化的第一個工作是瞭解您機構有關平台安全性的相關安全性策略、標準以及準則。使用這些文件來形成 Solaris Security Toolkit 設定檔的基礎，原因是這些文件傳達機構內所有系統的需求及實作。若您的機構沒有這些文件，建立它來增加您自訂 Solaris Security Toolkit 軟體的能力。

備註：尋找這些文件時，要知道有些資料可能列入最佳實作或者其他文件中。

要取得更多有關安全性策略的資訊，請參閱 Sun BluePrints OnLine 文摘「Developing a Security Policy」。此文件可被使用來取得更多對於安全性策略在機構安全性計畫中所扮演的角色的瞭解。

下面兩個範例說明策略聲明可如何直接影響配置 Solaris Security Toolkit 設定檔的方法。

範例 1

- **策略** — 機構必須使用支持使用者嚴格驗證及資料傳輸加密的管理協定。
- **設定檔影響** — 明文 (Clear-text) 協定如 Telnet、FTP、SNMPv1 等不應該被使用。依據預設，Solaris Security Toolkit 停用如此的服務，因此不需要另外的配置。

備註：Telnet 及 FTP 服務兩者皆可延伸使用如 Kerberos 來支援嚴格驗證及加密。這些列舉的服務做爲範例，原因是它們預設的配置並不支持這些安全性附加階層。

範例 2

策略 — 每個使用者每隔 30 天必須更改密碼。

設定檔影響 — Solaris Security Toolkit 軟體可以配置成啓用密碼生命期。依據預設，Solaris Security Toolkit 設定密碼的最大期限爲 8 週（56 天）。要配合安全性策略，Solaris Security Toolkit 軟體的設定檔必須作更改。請參閱「*Solaris Security Toolkit 4.1 Reference Manual*」。

雖然系統執行 Solaris Security Toolkit 軟體之預設值爲啓用密碼生命期，但此變更無法改變現存的使用者。對現存使用者啓用密碼生命期，對每個使用者帳號呼叫 `passwd`(1) 指令。

判定應用程式及服務的需求

此項作業確保系統強化之後服務仍具功能。此項作業由下列步驟所組成：

- 第 18 頁「辨識應用程式及作業服務庫存」
- 第 18 頁「判定服務需求」

辨識應用程式及作業服務庫存

盤點應用程式、服務以及作業或管理功能。要判定軟體是否真正在系統上使用，此份庫存清單是必要的。很多狀況下，系統被配置過多的軟體而且軟體並不支援商業功能。

若有可能，系統應該做最小建構。那就是不需要安裝不支援商業功能的軟體。系統不需要的軟體應用程式會增加攻擊者可以用來利用系統的機會。除此之外，系統上愈多軟體通常代表需要套用愈多的修補程式。要取得簡化 Solaris 作業系統的資訊，請參閱 Sun BluePrints OnLine 文摘「Minimizing the Solaris Operating Environment for Security」。

建立軟體的庫存清單時，除了常駐系統的應用程式，確定要納入內部架構元件，例如管理、監控以及備份軟體。

判定服務需求

當您完成應用程式及服務清單後，請判定元件間的依賴性是否可能因強化程序而影響。很多協力廠商應用程式不直接使用由 Solaris 作業系統所提供的服務。對於那些直接使用的應用程式，下列章節提供有用的資訊。

- 第 18 頁「共享程式庫」
- 第 21 頁「配置檔案」
- 第 21 頁「服務架構」

共享程式庫

瞭解支援一個應用程式需要何種程式庫是非常重要的。這項知識對於除錯情況非常有用，而且對於準備強化系統也是很有用的。當不明瞭系統狀態時，盡可能收集資料（例如軟體間的依賴性），如此才會清楚瞭解。

根據您安裝的 Solaris 作業系統，有三個方法可用來確定應用程式使用的程式庫：

- 第一個是針對檔案系統物件（例如，應用程式二進位碼）。
- 分析執行中的應用程式時使用第二個。
- 第三個用來追蹤程式何時開始。

範例：判定支援 DNS 伺服器軟體所需的程式庫。

若要收集檔案系統相關資訊，請使用 /usr/bin/ldd 指令。

程式碼範例 2-1 取得有關檔案系統物件的資訊

```
# ldd /usr/sbin/in.named
libresolv.so.2 => /usr/lib/libresolv.so.2
libsocket.so.1 => /usr/lib/libsocket.so.1
libnsl.so.1 =>    /usr/lib/libnsl.so.1
libc.so.1 =>      /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1
```

使用 /usr/proc/bin/pldd 指令（Solaris 作業系統版本 8 和 9 適用），自執行的程序中收集資訊。

程式碼範例 2-2 自執行中程序收集資訊

```
# pldd 20307
20307:  /usr/sbin/in.named
/usr/lib/libresolv.so.2
/usr/lib/libsocket.so.1
/usr/lib/libnsl.so.1
/usr/lib/libc.so.1
/usr/lib/libdl.so.1
/usr/lib/libmp.so.2
/usr/platform/sun4u/lib/libc_psr.so.1
/usr/lib/dns/dnssafe.so.1
/usr/lib/dns/cylink.so.1
```

pldd 指令顯示應用程式動態的將共享程式庫載入，除了那些已與應用程式連結的程式。此資訊也可使用下列 truss 指令收集。

備註：爲了簡明起見，下列輸出經過刪略。

程式碼範例 2-3 確認動態載入應用程式

```
# truss -f -topen,open64 /usr/sbin/in.named
20357:  open("/usr/lib/libresolv.so.2", O_RDONLY)        = 3
20357:  open("/usr/lib/libsocket.so.1", O_RDONLY)        = 3
20357:  open("/usr/lib/libnsl.so.1", O_RDONLY)           = 3
20357:  open("/usr/lib/libc.so.1", O_RDONLY)             = 3
20357:  open("/usr/lib/libdl.so.1", O_RDONLY)            = 3
20357:  open("/usr/lib/libmp.so.2", O_RDONLY)            = 3
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)        = 4
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)        = 4
20357:  open("/usr/lib/dns/dnssafe.so.1", O_RDONLY)      = 4
20357:  open("/usr/lib/dns/cylink.so.1", O_RDONLY)       = 4
20357:  open("/usr/lib/dns/sparcv9/cylink.so.1", O_RDONLY) = 4
```

此輸出版本含有程序識別碼，系統呼叫（範例個案：open）及它的引數以及系統呼叫的回傳值。使用回傳值，很清楚的可以知道何時系統呼叫成功地找到及開啓共享程式庫。

一旦已經知道共享程式庫的清單，使用下列指令來判定它們所屬的 Solaris 作業系統套裝模組：

```
# grep '/usr/lib/dns/cylink.so.1' /var/sadm/install/contents
/usr/lib/dns/cylink.so.1 f none 0755 root bin 63532 24346 \
  1018126408 SUNWcsl
```

結果輸出顯示此共享程式庫屬於 SUNWcsl (Core、Shared Libs) 套裝模組。此程序對執行平台最小化時特別有用，原因是此程序協助確認支援應用程式或服務所需要的套裝模組。

配置檔案

另一種方式來收集需求是透過配置檔案。由於配置檔案可以由重新命名或移除來停用服務，此程序對強化系統有更直接的影響。 要取得更多資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

若要判定配置檔案是否正在被使用，請使用 `truss` 指令。

備註：爲了簡明起見，下列輸出經過刪略。

程式碼範例 2-4 判定配置檔案是否使用中

```
# truss -f -topen,open64 /usr/sbin/in.named 2>&1 | \
grep -v "/usr/lib/.*.so.*"
20384:  open("/etc/resolv.conf", O_RDONLY)              = 3
20384:  open("/dev/conslog", O_WRONLY)                  = 3
20384:  open("/usr/share/lib/zoneinfo/US/Eastern", O_RDONLY) = 4
20384:  open("/var/run/syslog_door", O_RDONLY)          = 4
20384:  open("/etc/nsswitch.conf", O_RDONLY)            = 4
20384:  open("/etc/services", O_RDONLY)                 = 4
20384:  open("/etc/protocols", O_RDONLY)                = 4
20384:  open("/etc/named.conf", O_RDONLY)               = 4
20384:  open("named.ca", O_RDONLY)                      = 5
20384:  open("named.local", O_RDONLY)                   = 5
20384:  open("db.192.168.1", O_RDONLY)                  = 5
20384:  open("db.internal.net", O_RDONLY)               = 5
```

此範例中，DNS 服務使用配置檔案，例如 `/etc/named.conf`。如同上個範例，若服務的回傳值爲錯誤，表示可能有問題。小心的記錄強化之前及之後的結果可以協助加速整個驗證程序。

服務架構

此類別包括在其之上建立更大更複雜應用程式的架構或元服務 (meta-services)。通常在此類別中的架構種類有命名服務（例如：NIS、NIS+ 及 LDAP），驗證服務（例如：Kerberos 及 LDAP），以及由 RPC 設備所使用的通訊埠對映器。

不是都很清楚何時應用程式會依賴這些種類的服務。當配置應用程式需要特別的調整時，例如加入至 Kerberos 範圍，依賴性是已知的。有些狀況下，應用程式依賴不需要增加任何工作而且廠商並未記錄實際的依賴。

其中之一的範例是 RPC 通訊埠對映器。依據預設，Solaris Security Toolkit 軟體會停用 RPC 通訊埠對映器。此行動可能導致依賴此服務的其他服務有不可預期的行爲。根據過去的經驗，中斷服務、當機或故障會根據應用程式碼的好壞來判定如何處理意外狀況。要判定應用程式是否使用 RPC 通訊埠對映器，請使用 `rpcinfo` 指令。例如：

程式碼範例 2-5 判定使用 RPC 的應用程式

```
# rpcinfo -p
100000    3   tcp    111  rpcbind
100000    4   udp    111  rpcbind
100000    2   udp    111  rpcbind
100024    1   udp  32777  status
100024    1   tcp  32772  status
100133    1   udp  32777
100133    1   tcp  32772
100021    1   udp   4045  nlockmgr
100021    2   udp   4045  nlockmgr
100021    3   udp   4045  nlockmgr
100021    4   udp   4045  nlockmgr
100021    1   tcp   4045  nlockmgr
```

服務欄位的資訊來自 `/etc/rpc` 檔案和 / 或配置的命名服務如 LDAP。

若檔案內沒有服務的項目，經常是協力廠商的產品，服務欄位可能是空的。這樣使得要確認由其他應用程式註冊的應用程式更加困難。

例如，考慮 `rusers` 指令。此指令會依賴 RPC 通訊埠對映服務。若 RPC 通訊埠對映器不是執行中，`rusers` 指令看起來是當機。此程式最終會逾時，出現下列錯誤訊息：

```
# rusers -a localhost
localhost: RPC: Rpcbind failure
```

此問題會發生，因爲程式不能與服務溝通。自 `/etc/init.d/rpc` 啓動 RPC 通訊埠對映服務之後，程式馬上產生它的結果。

正如另外的範例，考慮 RPC 通訊埠對映服務執行中，而且 rusers 服務並未配置爲執行。這個狀況下，會產生完全不同的反應，相對的比較容易作驗證。

程式碼範例 2-6 驗證 rusers 服務

```
# rusers -a localhost
localhost: RPC: Program not registered
# grep rusers /etc/rpc
rusersd         100002  rusers
# rpcinfo -p | grep rusers
<No output generated>
```

rpcinfo 指令並未註冊 rusers 服務，假設該服務並未配置爲執行是安全的。此假設藉由觀察 /etc/inet/inetd.conf 中的服務項目來驗證。

```
# grep rusers /etc/inet/inetd.conf
# rusersd/2-3   tli     rpc/datagram_v,circuit_v     wait root
/usr/lib/netsvc/rusers/rpc.rusersd     rpc.rusersd
```

服務行開頭的註解標記 (#) 指示 rusers 服務是停用的。要啓用此服務，去除此行的註解標記並且送出一個 SIGHUP 訊號給 /usr/sbin/inetd 程式如下：

```
# pkill -HUP inetd
```

備註：pkill 指令僅適用 Solaris 作業系統版本 7 到 9。對於其他版本，請使用 ps 及 kill 指令，依次爲尋找及用訊號通知程序。

另一個判定應用程式是否使用 RPC 設備的方法是使用先前描述的 ldd 指令。

程式碼範例 2-7 判定使用 RPC 的應用程式的替代方法

```
# ldd /usr/lib/netsvc/rusers/rpc.rusersd
libnsl.so.1 =>   /usr/lib/libnsl.so.1
librpcsvc.so.1 =>        /usr/lib/librpcsvc.so.1
libc.so.1 =>     /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-250/lib/libc_psr.so.1
```

librpcsvc.so.1 項目指示，跟隨檔案名稱，此項服務依賴 RPC 通訊埠對映服務。

除了 RPC 通訊埠對映器，應用程式可能依賴其他一般作業系統服務，如 FTP、SNMP 或 NFS。您可使用相似的技巧來爲這些服務除錯，以及判定它們真的被需要用來支援商業功能。有一個方法與使用 netstat 指令有關，如下：

```
# netstat -a | egrep "ESTABLISHED|TIME_WAIT"
```

此指令傳回一個最近使用的服務清單，例如：

表 2-1 列出最近使用的服務

```
localhost.32827      localhost.32828      49152      0 49152      0
ESTABLISHED

localhost.35044      localhost.32784      49152      0 49152      0
ESTABLISHED

localhost.32784      localhost.35044      49152      0 49152      0
ESTABLISHED

localhost.35047      localhost.35046      49152      0 49152      0
ESTABLISHED

localhost.35046      localhost.35047      49152      0 49152      0
ESTABLISHED

filefly.ssh 192.168.0.3.2969    17615     1 50320     0 ESTABLISHED
```

此範例中，很多服務都在使用中，但是不清楚哪一個服務或應用程式使用哪一個埠。此資訊可藉由使用 pfiles 指令（Solaris 作業系統版本 8 和 9）檢測程序而得知。

程式碼範例 2-8 判定服務及應用程式使用的埠

```
# for pid in `ps -aeo pid | grep -v PID`; do
> pfiles ${pid} | egrep "^${pid}:|sockname:"
> done
```

更有效及有效率來判定依賴性的方法是使用 lsof （列出開啓的檔案）指令。此指令判定什麼程序使用什麼檔案及埠。例如，要判定上述範例中什麼程序使用埠 35047，使用下列指令。

程式碼範例 2-9 判定使用檔案及埠的程序

```
# ./lsof -i | grep 35047
ttsession   600 root 9u  IPv4 0x3000b4d47e8      0t1  TCP
localhost:35047->localhost:35046 (ESTABLISHED)
dtexec     5614 root 9u  IPv4 0x3000b4d59e8      0t0  TCP
localhost:35046->localhost:35047 (ESTABLISHED)
```

lsof 的輸出顯示埠 35047 正用於 dtexec 和 ttsession 程序之間的通訊。

使用 lsof 程式，您可能可以更迅速的判定系統之間或應用程式之依賴性，需要檔案系統或網路使用率。幾乎所有本章內所提起的都可以使用 lsof 程式的不同選項來擷取。

要取得 lsof 程式，自下列網址下載：

ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/

備註：前面描述的判定依賴性的方法可能無法找出那些很少使用的項目。除了使用這些方法，檢閱文件及廠商文件資料。

開發及實現 Solaris Security Toolkit 設定檔

在您完成規劃及準備階段後，請開發及實現安全性設定檔。安全性設定檔包含一個強化驅動程式，例如，*name*-hardening.driver，以及所有相關驅動程式、程序檔，以及可以實現您站台特定安全性策略的檔案。

自訂 Solaris Security Toolkit 軟體隨附的安全性設定檔之一，或是開發您自己的安全性設定檔。每個機構的策略、標準以及應用程式需求皆有不同，雖然可能只有少許。

要自訂一個安全性設定檔，請透過結束程序檔、稽核程序檔、環境變數、架構功能以及檔案範例調整它的行動。

請參閱以下章節取得更多資訊：

- 要取得有關自訂軟體的重要準則，請參閱第 1 章，第 12 頁「配置和自訂 Solaris Security Toolkit 軟體」。
- 要取得安全性設定檔被建立的範例情境，請參閱第 7 章的第 83 頁「建立安全性設定檔」。
- 要取得有關自訂驅動程式的資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

  如有需要，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」的其他適用章節、取得程序檔、架構功能、環境變數以及檔案的資訊。有兩個您也許要自訂的關鍵環境變數：JASS_FILES 及 JASS_SCRIPTS。

要落實大部分平台之間的標準，但仍然提供平台特定的差異，使用一種稱爲巢狀或階層式安全性設定檔的技巧。要取得更多資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。使用您機構的策略、標準及需求比較結果安全性設定檔，以確保變更不是因不慎或錯誤而造成。

安裝軟體

Solaris Security Toolkit 軟體的安裝對於已部署系統或要被安裝的新系統而言是相同的。要取得詳細的指示，請參閱第 3 章。

對於已部署系統，一些特殊狀況會使程序簡單及迅速。這些狀況並不注重強化程序，但是注重安裝前及安裝後的工作。

執行安裝前作業

強化已部署系統之前，考慮及計畫兩個重要的工作 — 備份及確認。這些作業協助判定已部署系統的狀態以及在強化系統之前處理任何潛在的配置問題。

備份資料

此作業著重於偶發性計畫。萬一發生問題時，必須要確保系統配置及資料歸檔於某種形式。您必須備份系統，確定備份媒體是可讀取的，以及驗證它的內容可以復原。對系統作任何重大改變之前進行此步驟。

驗證系統穩定性

驗證作業與備份作業的重要性相同。驗證作業確保在實現任何配置變更（例如強化程序所作的變更）前，系統處於穩定工作狀態。此驗證程序包括重新開機及隨後應用程式或服務的成功測試。期望一個完善定義的測試及接受計畫，但不一定有合適的文件。如果是這種情況，根據系統的情況來作測試。此項努力的目標是確保執行中的配置，事實上，與儲存的配置相符合。

當系統開機或應用程式啓動時，檢視任何顯示的錯誤訊息或警告。若您無法修正錯誤，請記錄它們。如此強化期間它們不會規爲問題的潛在原因。檢查日誌檔時，確定要納入系統、服務、以及應用程式記錄，如：

- `/var/adm/messages`
- `/var/adm/sulog`
- `/var/log/syslog`
- `/var/cron/log`

當您可以重新啓動系統而沒有錯誤或警告訊息時，此項作業已經完成（所有已知的皆已記載）。系統應重新啓動至已知及穩定狀態。如果，驗證期間，您發現執行中與儲存的系統配置不相同，重新評估您機構的變更控制策略以及程序來確認導致不同狀況的差異。

執行安裝後作業

安裝後作業是安裝前工作的延伸。目的是確保強化程序並未導致系統或應用程式的任何新錯誤。此項作業主要由檢閱系統及應用程式日誌檔而達成。強化並重新開機之後建立的日誌檔應當與強化系統之前收集的日誌檔相似。某些狀況下，應該有比較少的訊息（因爲啓動的服務比較少）。最重要的是不應該有新的錯誤或警告訊息。

除了檢閱日誌檔，也請測試功能性（因爲有些應用程式可能失敗但未寫入日誌檔）。參閱下列章節取得詳細驗證資訊。

驗證應用程式及服務功能性

此系統安全化程序中最後的作業包括驗證系統提供的應用程式及服務可以正確的執行功能。此項工作也會驗證安全性設定檔成功地實現安全性設定檔的需求。重新啓動強化後的平台之後完整的執行此項工作，確保偵測到任何不正常或問題後即刻被修正。此項作業分爲兩項子作業：驗證安全性設定檔安裝及驗證應用程式及服務的功能性。

驗證安全性設定檔安裝

要驗證 Solaris Security Toolkit 軟體已正確安裝安全性設定檔且無錯誤，請檢閱安裝日誌檔。此檔案安裝在 `JASS_REPOSITORY/jass-install-log.txt`。

備註：請參閱此日誌檔以瞭解 Solaris Security Toolkit 軟體對系統作了什麼。每當系統執行時，會根據執行的開始時間將新的日誌檔儲存於目錄之中。

除了驗證設定檔已被安裝，也請評估系統的安全性配置。執行手動檢視或使用工具來自動化程序。

驗證應用程式及服務功能性

要驗證程序應用程式及服務，請執行一個完善定義的測試及接受計畫。此計畫使用系統或應用程式的不同元件來判定它們是否處於適用及工作順序中。若沒有適用的計畫，根據系統使用的方式作合理的測試。此努力的目的爲確保強化程序並未影響應用程式或服務執行應有功能的能力。

當強化系統之後，若您發現應用程式或服務有異常，檢閱應用程式日誌檔判定問題所在。很多狀況下，您可使用 `truss` 指令來判定應用程式自何處開始發生困難。瞭解之後，您可將問題做爲目標並回溯至 Solaris Security Toolkit 軟體所作的變更。

維護系統安全性

很多機構會發生的錯誤是只在安裝時注重安全性，之後就很少或不再關切此問題。維護安全性是一個持續的程序。系統安全性必須定期的檢閱及重新查看。

維護一個安全的系統需要心生警惕，原因是任何系統預設的安全配置經過一段時間之後開放度會大增。例如，系統的弱點已被人知道。以下的基本準則提供相關簡介：

- Solaris 作業系統修補程式可能會安裝其他軟體套裝模組做爲安裝的一部分，及可能覆寫系統的配置檔案。確定安裝之前及之後都要檢閱系統的安全狀態。而且，重要的是要使用最新的修補程式來更新系統。

  Solaris Security Toolkit 軟體可以協助您套用修補程式，這是因爲它可以支援系統重複的執行，因此安裝修補程式之後可以保護系統。每次安裝修補程式後要使用適用的驅動程式來執行安全性軟體，確保您的配置與您定義的安全性策略保持一致。除此之外，進行系統的手動檢閱，因爲 Solaris Security Toolkit 軟體所使用的版本可能並不支援修補程式新增的功能。

- 以進行中方式監控系統，確保沒有發生未經授權的運作方式。檢閱系統帳號、密碼以及存取模式，它們會提供大量有關系統動態的資訊。
- 部署及維護一個中央的 `syslog` 儲存庫來收集及剖析 `syslog` 訊息。您可藉由聚集及檢閱日誌檔來取得重要的資訊。
- 建立一個容易瞭解的弱點及稽核策略來監控及維護系統配置。此項需求對於長時間下維護系統於安全配置的情況下是非常重要的。
- 定期使用最新版本的 Solaris Security Toolkit 軟體來更新您的系統。

Solaris Security Toolkit 軟體包含做爲起始點使用的預設安全性設定檔。

第3章

安裝及執行安全性軟體

本章提供下載安裝及執行 Solaris Security Toolkit 軟體的指示以及其他安全性相關軟體。包含將您的環境配置爲獨立或 JumpStart 模式以及取得支援的指示。

遵循本章提供的指示及程序來安裝，配置以及執行軟體。這些指示包括下載其他的安全性軟體，有用的範例以及準則。

雖然 Solaris Security Toolkit 軟體是獨立的產品，但是當它與其他下載的安全性軟體共同使用時最爲有效。此軟體包括來自 SunSolve OnLine 最新的「建議和安全修補程式叢集」、可緊化 Solaris 作業系統及協力廠商軟體權限之權限及所有權修正軟體，及可驗證 Sun 檔案及執行檔的完整性的驗證二進位碼。Solaris 作業系統發行版本的 Secure Shell 軟體並未內含。

本節包含以下作業：

執行規劃及安裝前作業

正確的規劃是成功使用 Solaris Security Toolkit 軟體以鞏固系統安全性的關鍵。安裝軟體之前，請參閱第 2 章取得詳細規劃資訊。

若您要安裝軟體於已部署的系統，請參閱第 26 頁「執行安裝前作業」，取得在安裝軟體於已部署系統之安裝前作業的資訊。

需求

Solaris Security Toolkit 4.1 軟體有一些需求。

硬體需求

請參閱第 11 頁「執行支援的 Solaris 作業系統版本」，以得知 Solaris 作業系統支援版本的相關資訊。

軟體需求

Solaris Security Toolkit 4.1 軟體需要 SUNWloc 套裝模組。若沒有此套裝模組，就會導致 Solaris Security Toolkit 的執行失敗。

請參閱第 11 頁「執行支援的 SMS 版本」，以得知 System Managements Services (SMS) 軟體支援版本的相關資訊。

判定使用何種模式

系統安裝期間或之後要及時強化系統，限制系統處於可能暴露在攻擊的不安全狀態時間。使用 Solaris Security Toolkit 軟體保護系統之前，請配置 Solaris Security Toolkit 軟體以便在您的環境正確執行。

Solaris Security Toolkit 軟體具有模組化架構。若您使用 JumpStart 產品，Solaris Security Toolkit 軟體架構的彈性可以有效的準備您之後使用 JumpStart。若您使用 JumpStart，您可自 Solaris Security Toolkit 軟體可以合至現存 JumpStart 架構的能力中獲益。

下面章節說明獨立模式及 JumpStart 模式。

獨立模式

Solaris Security Toolkit 軟體在獨立模式下，直接自 Solaris 作業系統 shell 提示符號後執行。此模式下，您可於需要更改或更新安全性的系統上使用 Solaris Security Toolkit 軟體，但是不可自原點開始重新安裝作業系統。但是如果可能，系統應改自原點開始重新安裝來保護系統。

當安裝修補程式之後作系統強化，獨立模式特別有用。您可在系統上執行多次 Solaris Security Toolkit 軟體，不會有不良的效果。修補程式可能覆寫或者更改那些 Solaris Security Toolkit 更改過的檔案；藉由執行 Solaris Security Toolkit 軟體，任何因安裝修補程式而取消的安全性更改可以重新被使用。

備註：在生產環境中，於真實環境安裝修補程式之前，請於測試及開發環境呈現修補程式。

獨立模式是用來盡速強化一個已部署的系統的最好選項之一。除了第 31 頁 「下載安全性軟體」中提供的下載及安裝指示外，將 Solaris Security Toolkit 軟體整合至沒有 JumpStart 的架構並不需要特別的步驟。

JumpStart 模式

JumpStart 技術是以網路爲基礎的 Solaris 作業系統安裝機制，可以在安裝期間執行 Security Toolkit 程序檔。本書假設讀者熟悉 JumpStart 技術，而且具備既存的 Jumpstart 環境可供使用。要取得更多有關 JumpStart 技術的資訊，請參閱 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

若是用於 JumpStart 環境，請將位於 `JASS_HOME_DIR`（`tar` 下載）或 `/opt/SUNWjass`（`pkg` 下載）中的 Solaris Security Toolkit 原始碼複製到 JumpStart 伺服器的根目錄。預設爲 JumpStart 伺服器上的 `/jumpstart`。`JASS_HOME_DIR` 成爲 JumpStart 伺服器的根目錄。

整合 Solaris Security Toolkit 軟體至 JumpStart 架構只需要少數步驟。請參閱第 5 章取得如何配置 JumpStart 伺服器的指示。

下載安全性軟體

強化系統的第一階段爲下載其他安全性套裝模組至您要保護的系統。本節涵蓋以下作業：

- 第 32 頁 「下載 Solaris Security Toolkit 軟體」

- 第 33 頁「下載建議的修補程式叢集軟體」
- 第 35 頁「下載 FixModes 軟體」
- 第 36 頁「下載 OpenSSH 軟體」
- 第 37 頁「下載 MD5 軟體」

備註：本節說明的軟體中，Solaris Security Toolkit 軟體、「建議和安全修補程式叢集」、FixModes 及 MD5 軟體都是必要的。您可使用商業版本的 Secure Shell 替代 OpenSSH，不同廠商的軟體皆可適用。安裝及使用 Secure Shell 產品至所有的系統。若使用 Solaris 9 作業系統，請使用內含的 Secure Shell 版本。

下載 Solaris Security Toolkit 軟體

首先下載 Solaris Security Toolkit 軟體。然後，如果您使用獨立模式 Solaris Security Toolkit 軟體，請安裝至伺服器上；或者，如果您使用 JumpStart 模式，請安裝至 JumpStart 伺服器上。

備註：下列指示使用的檔案名稱與版本號碼無關。請務必下載網站上的最新版本。

在本手冊的其他部分中，環境變數 `JASS_HOME_DIR` 指的是 Solaris Security Toolkit 軟體的根目錄。當 Solaris Security Toolkit 軟體自 `tar` 歸檔中安裝時，`JASS_HOME_DIR` 被定義爲直至及包含 `jass-`*n.n* 的路徑。若您安裝 `/opt` 目錄內的 `tar` 版本，`JASS_HOME_DIR` 環境變數則會定義爲 `/opt/jass-`*n.n*。

Solaris Security Toolkit 軟體除了傳統的壓縮 `tar` 歸檔以外，還以 Solaris 作業系統套裝模組格式發行。二者歸檔皆含有相同的軟體。

選擇最適合您的狀況的格式。`pkg` 格式最適合用戶端，而 `tar` 最適合 JumpStart 系統及開發自訂套裝之用。

以下章節提供下載及安裝兩個不同歸檔類型的程序。

▼ 下載 tar 版本

1. **下載軟體發行檔案 (**`jass-`*n.n*`.tar.Z`**)。**

   原始檔位於以下網站：

   `http://www.sun.com/security/jass`

2. **使用** `zcat` **及** `tar` **指令將軟體發行檔案解壓縮至伺服器的目錄，如下所示：**

```
# zcat jass-n.n.tar.Z | tar xvf -
```

其中，*n.n* 爲您下載時的最新版本。

執行此指令，建立目前工作目錄中的 jass-*n.n* 子目錄。此子目錄包含所有 Solaris Security Toolkit 目錄及相關檔案。

▼ 下載 pkg 版本

1. **下載軟體發行檔案 (**SUNWjass-*n.n*.pkg.Z**)。**

   此原始檔位於：

   http://www.sun.com/security/jass

備註：若您下載軟體時遇到困難，請使用瀏覽器的 [Save As] 選項。

---

2. **使用 uncompress 指令，將軟體發行檔案解壓縮至伺服器上的目錄：**

```
# uncompress SUNWjass-n.n.pkg.Z
```

3. **使用 pkgadd 指令，安裝軟體發行檔案至伺服器上的目錄，如下所示：**

```
# pkgadd -d SUNWjass-n.n.pkg SUNWjass
```

其中，*n.n* 爲您下載時的最新版本。

執行此指令會在 /opt 中建立 SUNWjass 目錄。此子目錄包含所有 Solaris Security Toolkit 目錄及相關檔案。

下載建議的修補程式叢集軟體

Sun 發行的修補程式提供 Solaris 作業系統修補效能、穩定性、功能性以及安全性。對於系統安全性而言，安裝最新的修補程式叢集非常重要。要確保安裝於您系統上的是 Solaris 作業系統「建議和安全修補程式叢集」最新版本，本節說明如何下載最新修補程式叢集。

備註：安裝修補程式之前，在未上線系統或維護排程期間作評估及測試。

▼ 下載建議的修補程式叢集軟體

安裝修補程式叢集之前，檢閱個別修補程式讀我檔案及其他提供的資訊。資訊通常包含安裝修補程式叢集之前需要瞭解的建議以及有用的資訊。

1. **自 SunSolve OnLine Web 網站下載最新修補程式叢集，位於：**

   `http://sunsolve.sun.com`

2. **於左端瀏覽位址列之頂端按下 [Patches] 連結。**

3. **按下 [Recommended Patches Clusters] 連結。**

   顯示授權合約。

4. **選擇 [Recommended Solaris Patch Clusters] 方塊內適當的 Solaris 作業系統版本。**

   本範例中，選擇 Solaris 8 作業系統。

5. **選擇最佳下載選項，HTTP 或是 FTP 的單選按鈕，然後按 [Go]。**

   瀏覽器視窗顯示一個 [Save As] 對話方塊。

6. **本機儲存檔案。**

7. **安全地移動檔案至強化的系統。**

   使用 `scp`（`scp(1)` — 安全複製（遠端複製程式））指令，或者使用另一個傳輸安全檔的方法。

   使用 `scp` 指令如下：

```
# scp 8_Recommended.zip target01:
```

8. **移動檔案至 `/opt/SUNWjass/Patches` 目錄，然後解壓縮。**

   例如：

程式碼範例 3-1 移動修補程式至 `/opt/SUNWjass/Patches` 目錄

```
# cd /opt/SUNWjass/Patches
# mv /directory in which file was saved/8_Recommended.zip .
# unzip 8_Recommended.zip
Archive:     8_Recommended.zip
   creating: 8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

當您下載其他安全性套裝模組以及執行 Solaris Security Toolkit 軟體之後，修補程式會自動安裝。

備註：若您未將「建議和安全修補程式叢集」軟體放置於 /opt/SUNWjass/Patches 目錄，當您執行 Solaris Security Toolkit 軟體時會出現警告訊息。若無修補程式叢集適用，忽略此訊息是安全的。此狀況通常發生在新發行版本的作業系統。

下載 FixModes 軟體

FixModes 是可緊化預設 Solaris 作業系統目錄及檔案權限的套裝模組。緊化這些權限可以大幅改善整體的安全性。更具限制性的權限使得惡意使用者要取得系統權限變爲更加困難。

備註：Solaris 9 作業系統發行版本，對那些曾被 FixModes 軟體更改過的物件作了修改，來改進預設權限。但是 FixModes 軟體還是有必要，原因是協力廠商及非隨附的軟體需要緊化檔案及目錄的權限。

▼ 下載 FixModes 軟體

1. **自下列網址下載 FixModes 預先編譯之二進位碼：**

   http://www.sun.com/security/jass

   FixModes 軟體以 Solaris 作業系統系統之預先編譯及壓縮套裝模組版本檔案格式做爲發行。檔案名稱爲 SUNBEfixm.pkg.Z。

2. **使用 scp 指令或其他安全傳送檔案的方法，安全地移動檔案至強化的系統。**

   使用 scp 指令如下：

   ```
   # scp SUNBEfixm.pkg.Z target01:
   ```

3. **透過以下指令，解壓縮並儲存 /opt/SUNWjass/Packages 中的 Solaris Security Toolkit Packages 目錄的 SUNBEfixm.pkg.Z 檔案：**

   ```
   # uncompress SUNBEfixm.pkg.Z
   # mv SUNBEfixm.pkg /opt/SUNWjass/Packages/
   ```

   接下來，當下載完所有其他安全性套裝模組後，FixModes 軟體會自動安裝並且執行 Solaris Security Toolkit 軟體。

下載 OpenSSH 軟體

任何安全環境下，要保護使用者互動階段作業，使用加密結合增強驗證是必要的。至少，網路存取必須是加密的。

最通常被用來做爲加密工具的是 Secure Shell 軟體，不論是與 Solaris 作業系統搭售的版本、協力廠商的商業版本或是免費軟體版本皆可。要實現所有由 Solaris Security Toolkit 軟體所作的安全性更改，您必須納入一個 Secure Shell 軟體產品。

備註：若使用 Solaris 9 作業系統，請使用軟體提供的 Secure Shell 。此版本的 Secure Shell 可與其他 Solaris 作業系統安全功能，如 Basic Security Module (BSM) 以及 Sun 支援中心的支援作整合。

第 xx 頁 「相關資源」有提供關於取得商業版本的 Secure Shell 的位置之資訊。

Solaris Security Toolkit 軟體會停用所有未加密的使用者互動服務及系統的常駐程式，特別是如 `in.telnetd`、 `in.ftpd`、`in.rshd` 及 `in.rlogind` 等常駐程式。

Secure Shell 可讓您如使用 Telnet 和 FTP 一般地存取系統。

▼ 下載 OpenSSH 軟體

備註：若伺服器執行 Solaris 9 作業系統，您可使用搭售的 Secure Shell 軟體，跳過本節所述的 OpenSSH 安裝步驟。

- **取得 Sun BluePrints OnLine 文摘，遵循文章中的指示下載軟體。**

  一篇標題爲 「Building and Deploying OpenSSH on the Solaris Operating Environment」的 Sun BluePrints OnLine 文摘，說明了如何編譯及部署 OpenSSH，可在下列網站中找到：

  `http://www.sun.com/blueprints`

  或者設法取得 Sun BluePrints 出版之 *「Secure Shell in the Enterprise」*，應可於書店找到。

  下載完所有其他安全性套裝模組及執行 Solaris Security Toolkit 軟體後，OpenSSH 軟體會自動安裝。

注意：不要在需強化的系統上編譯 OpenSSH 而且不要安裝編譯器至需強化的系統。使用另一個 Solaris 作業系統 — 執行相同 Solaris 作業系統版本、架構及模式的系統（例如：Solaris 8 作業系統、Sun4U (sun4u) 及 64 位元）— 來編譯 OpenSSH。若您使用 SSH 的商業版本，則不需要編譯。此目的爲限制編譯器爲潛在入侵者的可能性。但是，限制系統於本機安裝編譯器並不能保證系統無法遭惡意入侵，原因是仍要安裝預先編譯的工具。

下載 MD5 軟體

MD5 軟體在強化系統上產生 MD5 數位指紋。產生數位指紋後，與 Sun 所發表之正確指紋作比較，可以偵測被更改過的二進位程式碼或未被授權使用者的*特洛伊木馬入侵*（安全下內藏危險程式）。藉由更改系統二進位碼，入侵者開了系統的後門可作存取、隱瞞入侵者的存在並且導致系統的不穩定。

▼ 下載 MD5 軟體

1. **從以下網站下載 MD5 二進位碼：**

   `http://www.sun.com/security/jass`

   MD5 程式以壓縮套裝模組版本檔案做爲發行。

2. **使用 `scp` 指令強化，或使用提供安全檔案傳輸的另一種方法，將檔案 `SUNBEmd5.pkg.Z` 安全地移動到系統。**

   使用 `scp` 指令如下：

```
# scp SUNBEmd5.pkg.Z target01:
```

3. **解壓縮並移動檔案至 `/opt/SUNWjass/Packages` 內的 Solaris Security Toolkit 之 `Packages` 目錄內。使用如下的指令：**

```
# uncompress SUNBEmd5.pkg.Z
# mv SUNBEmd5.pkg /opt/SUNWjass/Packages/
```

   在 MD5 軟體儲存到 `/opt/SUNWjass/Packages` 目錄之後，執行 Solaris Security Toolkit 軟體時就會安裝該軟體。

當 MD5 二進位碼已安裝完畢，您可透過 Solaris 指紋資料庫，使用它來確認系統執行檔的完整性。Sun BluePrints OnLine 文摘，標題爲「The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files」中可取得更多有關 Solaris 指紋資料庫的資訊。

4. **（選擇使用）自 Sun BluePrint 網站下載及安裝 Solaris Fingerprint Database Companion 以及 Solaris Fingerprint Database Sidekick 軟體：**

   `http://www.sun.com/blueprints/tools`

   安裝及使用 MD5 軟體的選用工具。這些工具簡化了驗證系統二進位碼與 MD5 檢查總和資料庫作對照的程序。經常使用這些工具來驗證安全系統上，Solaris 作業系統二進位碼及檔案的完整性。

   如何下載這些工具及指示可以在標題爲「The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files」的 Sun BluePrints OnLine 文摘中找到。

   應該驗證下載的安全性工具的完整性。安裝及執行 Solaris Security Toolkit 軟體及其他安全性軟體之前，請使用 MD5 總和檢查來驗證完整性。Solaris Security Toolkit 的下載頁上，可以取得 MD5 總和檢查。

自訂安全性設定檔

Solaris Security Toolkit 軟體內含，如驅動程式，很多不同的安全性設定檔範例。 如前章所述，預設安全性設定檔及這些驅動程式的更改可能不適合您的系統。這些驅動程式所使用的安全性設定檔將停用不需要的服務，並啓用遭預設爲停用的安全功能選項。

執行 Solaris Security Toolkit 軟體之前，爲您的環境檢閱及自訂，或是建立一個新的預設安全性設定檔。「*Solaris Security Toolkit 4.1 Reference Manual*」中提供了自訂安全性設定檔的技巧及準則。

安裝及執行軟體

在執行 Solaris Security Toolkit 軟體之前完成下列準備作業是重要的。當您執行 Solaris Security Toolkit 軟體時，大部分強化動作是自動完成的。

- 將 Solaris Security Toolkit 軟體及其他安全性軟體下載至您要強化的系統或是 JumpStart 伺服器上。請參閱第 31 頁「下載安全性軟體」。
- 將您的系統配置爲獨立模式或是 JumpStart 模式。請參閱第 30 頁「判定使用何種模式」。
- 如果適用，爲您的環境自訂 Solaris Security Toolkit 軟體。

■ 安裝及執行 Solaris Security Toolkit 軟體及其他安全性軟體之前，透過使用 MD5 總和檢查來驗證完整性。

您可自 JumpStart 伺服器或指令行執行 Solaris Security Toolkit 軟體。

對於指令行選項及執行軟體的其他資訊，請參閱下列章節：

■ 第 39 頁「在獨立模式下執行軟體」
■ 第 47 頁「在 JumpStart 模式下執行軟體」

在獨立模式下執行軟體

程式碼範例 3-2 顯示獨立模式指令行用法範例。

程式碼範例 3-2 獨立模式指令行用法範例

```
# ./jass-execute -h

usage:

To apply this Toolkit to a system, using the syntax:
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
   jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
   jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
      [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
   jass-execute -H

To display the last application of the Toolkit on a system:
   jass-execute -l

To display this help message:
   jass-execute -h
   jass-execute -?

To display version information for this program:
   jass-execute -v

#
```

表 3-1 列出指令行選項並逐一說明。

表 3-1 使用 jass-execute 的指令行選項

選項	說明
-a	判定系統是否與安全性設定檔相符。
-b	與 -u 選項搭配使用。備份自最後一次強化執行以來手動變更的所有檔案，然後將系統復原其原始狀態。
-d	指定獨立模式下執行驅動程式。
-f	與 -u 選項搭配使用。逆轉在強化執行期間所做的變更，而不詢問您是否有任何例外，即使檔案是在強化執行之後才手動變更的也一樣。
-h	顯示 jass-execute 的說明訊息，提供適用選項的簡介。
-H	提供系統上 Solaris Security Toolkit 軟體的歷程。
-k	與 -u 選項搭配使用。保留自最後一次強化執行以來所做的任何手動變更。
-l	顯示系統上 Solaris Security Toolkit 的最後一個應用程式。
-m	傳送輸出至指定的電子郵件地址。
-o	導引輸出至指定檔案。
-p	與 -r *root_directory* 選項搭配使用。 指定 Solaris 作業系統的作業系統版本。格式與 uname -r 使用的相同。
-q	阻止將輸出顯示至螢幕。也稱作無訊息選項。
-r	必須與 -p *os_version* 搭配使用。 指定 jass-execute 執行期間使用的根目錄。依據預設，root 檔案系統爲 /。此根目錄是由 Solaris Security Toolkit (JASS) 環境變數 JASS_ROOT_DIR 所定義。被鞏固安全性的 Solaris 作業系統可透過 / 找到。例如，您想要鞏固個別作業系統目錄的安全性，就暫時掛載到 /mnt 下，然後再使用 -r 選項來指定 /mnt。
-u	互動提示詢問您意外發生要採取何種行動時，執行還原選項。無法與 -d、-a、-h、-l 或 -H 選項搭配使用。
-v	顯示此程式的版本資訊。
-V	指定訊息輸入的詳情層級。
-?	顯示 jass-execute 的說明訊息，提供適用選項的簡介。

要取得獨立模式下執行 jass-execute 指令及其可用選項的詳細資訊，請參閱下面章節：

- 第 42 頁「稽核選項」
- 第 42 頁「顯示說明選項」
- 第 43 頁「驅動程式選項」
- 第 44 頁「電子郵件通知選項」
- 第 44 頁「執行歷程選項」

若要取得適用驅動程式的完整清單，請參閱 Drivers 目錄。新版軟體可能包含更多驅動程式。

▼ 在獨立模式下執行軟體

1. **執行 `secure.driver`（或者產品專用程序檔，例如：`sunfire_15k_sc-secure.driver`）如下。**

程式碼範例 3-3 在獨立模式下執行軟體

```
# cd /opt/SUNWjass
# ./jass-execute -d secure.driver

[NOTE] The following prompt can be disabled by setting
JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured,
it is both possible and likely that by default all remote shell
and file transfer access to this system will be disabled upon
reboot effectively locking out any user without console access to
the system.

Are you sure that you want to continue? (YES/NO) [NO]
y

[NOTE] Executing driver, secure.driver

================================================================
secure.driver: Driver started.
================================================================

================================================================
Solaris Security Toolkit Version: 4.1.0
Node name:                        ufudu
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.9
Date:                             Tue May 4 16:28:24 EST 2004
================================================================
[...]
```

若要取得適用驅動程式的完整清單，請參閱 Drivers 目錄。新版軟體可能包含更多驅動程式。

2. **執行 Solaris Security Toolkit 軟體之後，請重新啓動系統使變更生效。**

   強化期間，用戶端配置作不同的更改。這些更改可能包括伺服器停用起始程序檔，服務的停用選項，以及透過修補程式安裝新二進位碼或程式庫。 在用戶端重新啓動之前，這些更改不會生效。

3. **重新啓動系統之後，確認更改的正確性及完整性。**

   請參閱第 48 頁「驗證系統修改」。

4. **若發生任何錯誤，處理錯誤之後重新在獨立模式下執行 Solaris Security Toolkit 軟體。**

稽核選項

透過 -a 選項，Solaris Security Toolkit 可執行稽核，來判定系統是否與安全性設定檔相符。稽核不僅驗證更改過的系統檔案是否仍然使用中，還要確認已經遭停用的程序是否仍然執行或者已移除的套裝模組是否被重新安裝。 要取得更多此項功能的資訊，請參閱第 6 章。

對照安全性設定檔稽核系統的用法範例：

```
# jass-execute -a driver [ -V [0-4] ] [ -q | -o output-file ]
[ -m email-address ]
```

顯示說明選項

jass-execute 的 -h 選項顯示說明訊息，提供適用選項的簡介。

-h 選項之輸出與下列輸出相似：

程式碼範例 3-4 -h 選項輸出範例

```
# ./jass-execute -h
To apply this Toolkit to a system, using the syntax:
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
   jass-execute -u [ -b| -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
```

程式碼範例 3-4 -h 選項輸出範例 *（續上頁）*

```
    jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
       [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
   jass-execute -H

To display the last application of the Toolkit on a system:
   jass-execute -l

To display this help message:
   jass-execute -h
   jass-execute -?

To display version information for this program:
   jass-execute -v

Note that just the driver name should be specified when using the
'-d' or '-a' options. A path need not be specified as the script
is assumed to exist in the Drivers directory.

The '-u' undo option is mutually exclusive with the '-d' and '-a'
options. The default undo behavior is to ask the user what to do if
a file to be restored has been modified as the checksum is
incorrect.

The -u option can be combined with the '-k', '-b', or '-f' to
override the default interactive behavior. The use of one of these
options is required when run in quiet mode ('-q').

The '-k' option can be used to always keep the current file and
backup if checksum is incorrect. The 'b' can be used to backup the
current file and restore original if the checksum is incorrect.
The 'f' option will always overwrite the original if the checksum
is incorrect, without saving the modified original.
```

驅動程式選項

`-d` *driver* 選項指定驅動程式在獨立模式下執行。

您必須指定驅動程式的 `-d` 選項。Solaris Security Toolkit 軟體會將 `Drivers/` 加在程序檔名稱之前。您只需要在指令行輸入程序檔名稱。

備註：不可以同時使用 `-d` 及 `-u`、`-H`、`-h` 或 `-a` 選項。

---

jass-execute 強化指令使用 -d *driver* 選項之輸出與下列輸出相似：

程式碼範例 3-5 -d *driver* 選項輸出範例

```
# ./jass-execute -d secure.driver
[...]
[NOTE] Executing driver, secure.driver

============================================================
secure.driver: Driver started.
============================================================

============================================================
Solaris Security Toolkit Version: 4.1.0
Node name:                        ufudu
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.9
Date:                             Tue Oct 4 16:28:24 EST 2004
============================================================
[...]
```

電子郵件通知選項

-m *email-address* 選項提供當程式執行完畢時，Solaris Security Toolkit 軟體會自動傳送獨立強化或還原輸出的電子郵件機制。電子郵件報告爲使用其他選項時系統產生的日誌檔之外的報告。

Solaris Security Toolkit 透過電子郵件選項執行呼叫 sunfire_15k_sc-config.driver 應與下列輸出相似：

```
# ./jass-execute -m root -d sunfire_15k_sc-config.driver
[...]
```

執行歷程選項

-H 選項提供判定 Solaris Security Toolkit 軟體在系統上的執行次數的簡單機制。不論是否做過還原，所有的執行皆被列出。

-H 選項之輸出與下列輸出相似：

程式碼範例 3-6 -H 選項輸出範例

```
# ./jass-execute -H
Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 0.3.

The following is a listing of the applications of the Solaris
Security Toolkit on this system.  This list is provided in
reverse chronological order:

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
2.   June 31, 2004 at 12:10:29 (20040631121029)
3.   June 31, 2004 at 12:04:15 (20040631120415)
```

此輸出顯示 Solaris Security Toolkit 軟體執行了 3 次，最後一次作了還原。

最近執行的選項

-l 選項提供判定最近執行的機制。這總是 -H 選項列出的最後一項。

-l 選項提供類似下列的輸出：

程式碼範例 3-7 -l 選項輸出範例

```
# ./jass-execute -l

Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 4.1.0.

The last application of the Solaris Security Toolkit was:

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
```

輸出檔案選項

-o *output-file* 選項重導 jass-execute 螢幕輸出至檔案 *output-file*。

此選項對於 JASS_REPOSITORY 目錄中保存的記錄不發生作用。此選項對於執行在一台慢終端機上時非常有幫助，因爲執行 Solaris Security Toolkit 會產生大量的輸出。

此選項可同時與 -d、-u 或 -a 選項同時使用。

-o 選項之輸出與下列輸出相似：

程式碼範例 3-8 -o 選項輸出範例

```
# ./jass-execute -o jass-output.txt -d secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
```

無訊息輸出選項

-q 選項停止將強化執行之 Solaris Security Toolkit 輸出到標準輸入輸出 (stdio) 資料流。

此選項對於 JASS_REPOSITORY 目錄中保存的記錄不發生作用。與 -o 選項相似，此選項對於執行 cron 工作或在緩慢網路上執行 Solaris Security Toolkit 軟體非常有幫助。

此選項可同時與 -d、-u 或 -a 選項同時使用。

-q 選項之輸出與下列輸出相似：

程式碼範例 3-9 -q 選項輸出範例

```
# ./jass-execute -q -d secure.driver
[NOTE] Executing driver, secure.driver
```

根目錄選項

-r *root-directory* 選項指定執行 jass-execute 時會使用到根目錄。使用 -r 選項需要使用 -p 選項來指定平台（作業系統）版本。-p 選項的格式與 uname -r 產生的格式相同。

依據預設，檔案系統的根目錄爲 /。此根目錄被 Solaris Security Toolkit 的環境變數 JASS_ROOT_DIR 定義。要安全化的 Solaris 作業系統可透過 / 取得。例如，一個單獨的作業系統目錄要安全化，暫時掛載至 /mnt，然後使用 -r 選項來指定 /mnt。所有的程序檔套用到該作業系統影像。

還原選項

透過 -u 選項，Solaris Security Toolkit 軟體可以還原強化期間的系統修改。每個結束的程序檔可以使用 -u 選項作還原。除此之外，Solaris Security Toolkit 的還原能力與每次執行時產生的總和檢查作緊密的整合。要取得此能力的更多資訊，請參閱第 4 章。

還原指令的用法範例：

```
# jass-execute -u [ -f | -b | -k ] [ -q | -o output_file ]
        [ -m e-mail_address ] [ -V [3|4] ]
```

在 JumpStart 模式下執行軟體

JumpStart 模式由將 Solaris Security Toolkit 驅動程式加入 JumpStart 伺服器的 `rules` 檔案內來控制。

若您尚未將您的環境配置爲使用 JumpStart 模式，請參閱第 5 章。

要取得更多有關 JumpStart 技術的資訊，參考 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

▼ 在 JumpStart 模式下執行軟體

要在 JumpStart 模式下執行 Solaris Security Toolkit 軟體，則必須將它整合至您的 JumpStart 環境。做爲 JumpStart 安裝結束程序檔的一部分可被呼叫。要取得如何將 Solaris Security Toolkt 軟體整合至您的環境的資訊，請參閱第 5 章。

1. **當作完驅動程式所有必要的修改時，使用 JumpStart 基礎架構安裝用戶端。**

   於用戶端 `ok` 提示符號下，使用下列指令來完成此項作業。

   ```
   ok> boot net - install
   ```

   一旦安裝完成，JumpStart 軟體會重新啓動系統。

   系統應該處於正確配置中。強化期間，用戶端的配置作了不同的修改。這些修改包括停用服務起始程序，停用服務選項及透過修補程式安裝新的二進位碼或者程式庫。直至用戶端重新啓動，這些修改才會生效。

2. **系統重新啓動後，確認修改的正確性及完整性。**

   請參閱第 48 頁「驗證系統修改」。

3. **若發生任何錯誤，請修復錯誤，然後重新安裝用戶端作業系統。**

驗證系統修改

重新啓動系統後，依照下面章節所述，驗證修改的正確性及完整性。

執行品質保證 (QA) 檢核服務

安全系統中一個重要的挑戰是判定什麼作業系統服務必須保留使用，才能使系統正常運作。Solaris 作業系統服務可能是需要的，由於它們直接被（如 Secure Shell）用來登入系統。或者，它們也可間接被使用，例如：協力廠商的圖形化使用者介面則使用 Remote Procedure Call (RPC) 常駐程式。

執行 Solaris Security Toolkit 軟體之前，要先判定大多數的需求 （請參閱第 18 頁「判定應用程式及服務的需求」。）但是，唯一確定的機制是安裝及保護系統，然後透過品質保證 (QA) 測試來測試系統所需要的功能。當系統強化後，任何要部署的新系統必須要執行 QA 計畫。同樣地，要強化已部署的系統，必須透過測試確保所有需要的及期待的功能都存在。

若 QA 程序發現任何不一致性，請執行下列步驟：

1. 根據第 2 章中的準則判定問題區域。
2. 驗證應用程式在修改過的配置中可執行。
3. 還原 Solaris Security Toolkit 運作。
4. 根據問題的解析，修改安全性設定檔（驅動程式）。
5. 重新執行 Solaris Security Toolkit 軟體。

最終結果必須是，安全性設定檔的執行不會影響任何系統需求的功能。

執行配置的安全性評估

驗證系統是否執行所有需要的功能時，也要評估安全配置是否達到系統預想的安全等級。根據系統所作的強化或最小化，可能牽涉不同的狀況。

最基本的，系統配置必須依下列方式檢閱：

- 確定已經安裝所有適用的「安全性和建議的修補程式」。
- 驗證只有執行需要和適用的程序，而且是以適用的引數執行。
- 確定只有執行需要的常駐程式，而且是以適用的引數執行。

- 確定系統僅開啓需要的埠，可以透過本機檢查（例如，`netstat -a`）及使用遠端 Nmap 埠掃描器來判定網路介面何者埠是可用的。
- 若系統已最小化，請確定只有安裝需要的 Solaris 作業系統套裝模組。

對於新建立及安全化的系統，此項檢視應當做最低限度的檢核。強化老舊的系統時，底層的作業系統應該確認是否有未經授權的更改。完整性的檢查最好藉由掛載系統至唯讀模式，然後自已知的作業系統實例中執行完整性檢核軟體。Sun BluePrints OnLine 文摘「The Solaris Fingerprint Database — Security Tool for Solaris Software and Files」中所述的工具在這些情境中十分有用。

驗證安全性設定檔

在系統安全化及驗證完需要的服務及能力之後，請使用稽核功能確定安全檔案正確及完整地被套用。這個作業重要的原因有兩個。首先確保系統如需求般做好強化。第二要確保系統定義的安全性設定檔安全性設定檔可以正確的反映在 Solaris Security Toolkit 配置中。由於配置資訊在整個部署的生命週期內，要用來維護系統的安全性設定檔，因此這項檢核非常重要。

要取得更多有關稽核功能的資訊，參閱第 6 章。

執行安裝後作業

若您在已部署的系統上安裝軟體，請參閱第 27 頁「執行安裝後作業」，以取得相關資訊。

第4章

逆轉系統變更

本章提供資訊及程序，有關如何逆轉（還原）強化運行時由 Solaris Security Toolkit 軟體所作的變更。此選項提供一個自動化的機制，您可將系統返回到 Solaris Security Toolkit 強化安全運作之前的狀態。

本章包含以下主題：

瞭解變更如何被記錄及逆轉

每次 Solaris Security Toolkit 強化運作會建立一個 `JASS_REPOSITORY` 運作目錄。此目錄的名稱根據起始的日期及時間而定。除了將結果顯示在螢幕上，Solaris Security Toolkit 軟體在目錄中建立一組檔案來追蹤變更及記錄作業。

這些儲存在目錄中的檔案追蹤系統所作的變更以及啓用還原功能來工作。

注意：`JASS_REPOSITORY` 中的檔案內容絕對不可被系統管理員變更。

當您使用 Solaris Security Toolkit 軟體來強化系統，不論是 JumpStart 或獨立模式，軟體將所作的變更記錄在 `JASS_REPOSITORY/jass-manifest.txt` 日誌檔。此檔案列舉可被還原功能用來逆轉所作變更的作業。檔案含有因 Solaris Security Toolkit 軟體而生效的強化作業資訊，包括被建立、複製、移動或移除的檔案。除此之外，此檔案可能含有若要逆轉更複雜的變更時，例如套裝軟體安裝，所需要的標準及自訂項目。一個強化運行就建立一個 `jass-manifest.txt` 檔案。

備註：Solaris Security Toolkit 軟體還原功能僅還原那些明示檔案 (manifest file) 中有項目存在的變更。

還原運行瀏覽因 Solaris Security Toolkit 執行而產生並儲存在 JASS_REPOSITORY 的明示檔案。還原運行將備份檔案還原至原先的位置。若檔案未曾備份，還原功能即不適用。

當 Solaris Security Toolkit 的作業被還原後，相關的目錄並不會被移除。相反地，JASS_REPOSITORY 目錄中會建立兩個檔案：jass-undo-log.txt 及 reverse-jass-manifest.txt。之後，下次再執行 jass-execute -u 指令時，被還原的作業不會再被列出。強化運作只可以被還原一次。

還原系統變更的需求

使用 Solaris Security Toolkit 軟體的還原功能，必須瞭解下列限制及需求：

- 在 Solaris Security Toolkit 版本 0.3 到 4.1 中，您可針對獨立或 JumpStart 模式起始的運行使用還原功能。但是您只能還原獨立模式下的變更。JumpStart 安裝期間不可使用還原功能。
- 若您選擇 Solaris Security Toolkit 中不建立備份的選項，不論是透過獨立模式或 JumpStart 模式，還原功能不適用。設定 JASS_SAVE_BACKUP 參數爲 0，建立備份檔案副本的功能即被停用。
- 一次運行只能還原一次。
- 若您建立一個結束程序檔，它不使用 Solaris Security Toolkit 架構功能，您必須建立一個對應的稽核程序檔並使用 add_to_manifest 函數，將項目加入明示檔案中。否則，Solaris Security Toolkit 無法知道您自訂的進度。
- 任何狀況下都不要變更 JASS_REPOSITORY 目錄內的內容。變更這些檔案，當您使用還原功能時會導致內容毀損、錯誤或系統毀損。

自訂程序檔還原變更

Solaris Security Toolkit 架構提供彈性，可供設計及建立結束程序檔。架構允許您延伸 Solaris Security Toolkit 軟體的能力來符合機構的需要，同時協助您在生命期內作系統配置上更好的管理。

當您自訂程序檔時，很重要的是要瞭解什麼行動會影響還原功能。要簡化自訂程序檔，輔助程式函數會對明示檔案作適當的變更。（還原功能根據明示檔案的內容來逆轉強化運行。）大多數狀況下，這些輔助程式函數提供您自訂程序檔時所需要的資訊。

要取得如何使用輔助程式函數的資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。使用這些輔助程式函數代替相對應的系統指令，如此還原運行可以參照明示檔案內的相關項目。

有些狀況下，若沒有輔助程式功能時，您可能需要執行一個函數。在這樣的狀況下，使用名爲 `add_to_manifest` 的特殊函數。使用此函數，您可手動的新增項目至明示檔案中，不需要呼叫輔助程式函數。小心的使用此項特殊的函數，如此您可以保護系統及 Solaris Security Toolkit 儲存庫的完整性。範例中顯示當您想要加入那些不是 Sun `pkg` 格式的套裝軟體時，可使用此特殊函數。範例中，您必須告訴還原功能如何移除強化運行期間以它種格式加入的套裝軟體。

藉由輔助程式函數及特殊 `add_to_manifest` 函數，Solaris Security Toolkit 軟體提供簡單及彈性的方法來自訂程序檔以及可以使變更延伸至還原運行。

若您未使用這些函數來變更結束程序檔的運作方式，Solaris Security Toolkit 軟體無從知道已經作了變更。因此您必須手動還原那些明示檔案內沒有參照的變更。

另一個範例是系統變更檔案之前，首先必須先儲存原先的版本的檔案。Solaris Security Toolkit 軟體環境之外，使用者一般可以執行 `/user/bin/cp` 指令來達成此項工作。但是在 Solaris Security Toolkit 環境之下，若您直接使用此指令，Solaris Security Toolkit 無從知道需要建立一個項目在明示檔案中。使用 `backup_file` 輔助程式函數，而不使用 `cp` 指令。此函數儲存原先的檔案的副本，使用 `JASS_SUFFIX` 作後綴，而且加入一個明示檔的項目，指示 Solaris Security Toolkit 軟體已經複製了一個檔案。而且此函數計算檔案的總和檢查。檔案的總和檢查被還原功能及 `jass-check-sum` 指令所使用。

檢查曾經手動變更的檔案

雖然使用 `jass-execute -u` 指令可以自動檢查強化運行之後曾被手動變更過的檔案，但有時您會發現使用 `jass-check-sum` 指令列舉及檢視檔案是非常有用的。

此指令可使您檢視 `JASS_REPOSITORY` 的內容以及執行列入明示檔中所有檔案的總和檢查。判定清單上的檔案在強化期間作總和檢查記錄之後是否遭變更。進行強制還原運行之前進行此項檢查，可提供有價值的資訊，如此可以節省長時間不需要的疑難排解。

下面是輸出的範例。

程式碼範例 4-1 手動變更檔案輸入的範例

```
# ./jass-check-sum
File Name              Saved CkSum              Current CkSum
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
/etc/inet/inetd.con    1643619259:6883          2801102257:6879
/etc/logadm.conf       2362963540:1042          640364414:1071
/etc/default/inetd     3677377803:719           2078997873:720
```

輸出指出三個檔案在強化運行完成之後被變更。

使用還原功能選項

本節描述 `jass-execute -u` 指令及選項，您可於執行還原運行時使用。

備註：您不可以與還原功能同時使用 `-d`、`-a`、`-h`、`-l` 或 `-H` 選項。在無訊息模式中執行 `undo` 時，您必須提供 `-b`、`-k` 或 `-f` 選項。

`jass-execute -u` 指令是執行還原運行的標準。此指令會自動發現自上次強化後任何曾遭變更的檔案。若 Solaris Security Toolkit 軟體發現強化運行之後檔案曾遭手動變更，它會要求您選擇一個回應：

1. 在回復至原先的（強化運行之前已經存在）檔案之前先備份目前的檔案。
2. 保留最新的檔案，不要回復原先的檔案。
3. 強制覆寫至任何手動變更的檔案（可能遺失資料）以及回復原先的檔案。

若您要變更預設的還原運作方式，執行還原指令時可使用 `-b`、`-k` 及 `-f` 選項。

表 4-1 列出您可與還原一同使用的指令行選項。要取得有關每個選項的更詳細的資訊，請參閱下面章節。

表 4-1 使用還原指令的指令行選項

選項	說明
`-b`	備份自強化運行之後所有曾遭手動變更的檔案，重新回復系統至原來的狀態。
`-f`	強化運行期間逆轉變更；不詢問您有關異常狀況，即使在強化運行之後檔案曾遭手動變更。
`-k`	保留所有在強化運行之後您所作的手動變更檔案。

表 4-1 使用還原指令的指令行選項 *（續上頁）*

選項	說明
-m	傳送輸出至電子信箱。
-o	導引輸出至檔案。
-q	阻止將輸出顯示至螢幕。也稱作無訊息選項。輸出被儲存在 JASS_REPOSITORY/jass-undo-log.txt。

備份選項

-b 選項自動備份自上次強化運行後所有曾遭手動變更的檔案，然後回復檔案至強化運行之前的原來狀態。要使這些手動變更生效，您需要比較回復的檔案及備份檔案，然後手動調整差異。若檔案使用此項選項作備份，它與下列範例相似。

```
/etc/motd.BACKUP.JASS_SUFFIX
```

強制選項

-f 選項，沒有例外地，逆轉強化運行間的所作的所有變更，即使檔案在強化運行之後遭手動變更。還原運行不比較儲存檔案及目前版本檔案的總和檢查。結果是，強化運行之後若您曾手動變更過檔案，還原運行之後變更會被覆寫及遺失。

還原運行結束之後可能需要手動重新使變更生效。更進一步，根據所作的變更種類可能需要調整檔案組之間的差異。要協助阻止此問題發生，使用 jass-check-sum 指令或上面所述 -b 指令行選項。

保留選項

-k 選項自動保留強化運行之後您所作的檔案手動變更而不回復回原來的檔案。-k 選項發現檔案間任何的不匹配，導致產生一個通知以及作日誌記錄，並不以原來的檔案覆蓋。只針對那些 jass-checksums.txt 內儲存的總和檢查是正確的檔案，才會逆轉變更。

此選項並不全是沒缺點的。例如，若檔案子集被結束程序檔變更之後被變更，使得系統即可能成爲不一致狀態。

考慮 `remove-unneeded-accounts.fin` 結束程序檔。此程序檔修改系統的 `/etc/passwd` 及 `/etc/shadow` 檔案。若使用者在強化運行結束之後手動變更密碼，`/etc/shadow` 檔案的總和檢查與 Solaris Security Toolkit 軟體所儲存的值無法配合。結果是，如果使用保留選項，`/etc/passwd` 檔案複製回原來的狀態。`/etc/shadow` 檔案保留目前的形式。兩個檔案不再一致。

輸出檔案選項

`-o` *output-file* 選項重新導引 `jass-execute` 執行的螢幕輸出至一個檔案 *output-file*。

此選項對於保留在 `JASS_REPOSITORY` 目錄的記錄沒有作用。此選項對於使用連接緩慢終端機進行時特別有用，原因是 Solaris Security Toolkit 還原運行會產生大量的輸出。

無訊息輸出選項

`-q` 選項阻止 Solaris Security Toolkit 軟體顯示輸出至螢幕。此選項對於保留在 `JASS_REPOSITORY` 目錄的記錄沒有作用。與 `-o` 選項相似，透過緩慢網路執行 Solaris Securiyt Toolkit `cron` 工作時非常有幫助。

電子郵件通知選項

`-m` *email-address* 選項指引 Solaris Security Toolkit 軟體傳送完整運行的副本至一個電子郵件地址。電子信箱報告爲使用其他選項所產生之系統日誌檔之外的報告。

還原系統變更

有時候要逆轉一個或多個 Solaris Security Toolkit 強化運行時所作的變更是必要的。若您發現強化運行時所作的變更對您的系統有負面的影響，請還原變更。

例如，強化之後若您發現需要的服務如 NFS 遭停用，還原強化運行。然後，啓用 NFS 以及使用調整過的安全性設定檔案重複強化運行。

本節提供逆轉一個或多個強化運行期間變更的指示。請注意，有效的逆轉強化運行是有限制及需求的。請參閱第 52 頁 「還原系統變更的需求」。

▼ 還原 Solaris Security Toolkit 運行

1. **備份及重新啓動系統。**

   每次還原運作之前要重新開機及備份系統，來確保可以返回或可被帶回至已知的而且是工作的狀態。

2. **判定您要使用** `jass-execute -u` **指令的何種選項。**

   請參閱第 54 頁「使用還原功能選項」。

   下面指示假設您使用 `jass-execute -u` 指令。

3. **要還原一個或多個強化運行使用標準** `-u` **選項，自** `JASS_HOME_DIR` **中輸入指令：**

```
# ./jass-execute -u
```

   Solaris Security Toolkit 軟體藉由尋找位於 `JASS_REPOSITORY` 的所有明示檔來收集每次強化運行的資訊。若明示檔是空的或是不存在，可以假定沒有必要還原變更而且該運行可被省略。除此之外，若名爲 `jass-undo-log.txt` 檔案存在於明示檔案所在的目錄內，可以假定該運行已被逆轉，因此運行可被省略。當收集程序已經完成，將顯示輸出。下面是輸出的範例。

程式碼範例 4-2 還原可用之運行的輸出範例

```
# ./jass-execute -u
[NOTE] Executing driver, undo.driver
Please select a JASS run to restore through:
1. January 24, 2003 at 13:57:27
(/var/opt/SUNWjass/run/20030124135727)
2. January 24, 2003 at 13:44:18
(/var/opt/SUNWjass/run/20030124134418)
3. January 24, 2003 at 13:42:45
(/var/opt/SUNWjass/run/20030124134245)
4. January 24, 2003 at 12:57:30
(/var/opt/SUNWjass/run/20030124125730)

Choice? ('q' to exit)?
```

   範例中，發現四個獨立的強化運行。這些運行對系統作了改變而且尚未還原。強化運行的清單以相反的時間順序呈現。清單中的第一個項目是最近的強化運行。

4. **檢視輸出來判定您要還原的運行，然後輸入對應的編號。**

對於所選擇的項目，Solaris Security Toolkit 軟體將逆轉那些等於或小於選定值的運行。也就是，還原運行以相反順序來逆轉運行，以最近的強化做開始然後繼續至您所選擇的項目。使用上面範例做爲準則，若您選擇運行 3，還原運行會首先逆轉運行 1，然後移動至運行 2 的變更，最後逆轉運行 3 的變更。

下列範例顯示當還原運行處理兩個明示檔案項目的輸出。

程式碼範例 4-3 還原處理多個明示檔案項目的運行之輸出範例

```
[...]

================================================================
undo.driver: Performing UNDO of
//var/opt/SUNWjass/run/20030124135727.
================================================================

[...]

================================================================
undo.driver: Undoing Finish Script: update-cron-allow.fin
================================================================

[NOTE] Undoing operation COPY.
cp -p /etc/cron.d/cron.allow.JASS.20030125223417
/etc/cron.d/cron.allow
rm -f /etc/cron.d/cron.allow.JASS.20030125223417

[NOTE] Removing a JASS-created file.
rm -f /etc/cron.d/cron.allow

[...]
```

本範例中，Solaris Security Toolkit 軟體還原了複製作業以及移除強化期間所加入的檔案。還原運行的輸出記錄用來回復系統所使用的真實指令，如此若您需要作系統配置疑難排解時，程序可被清楚的瞭解及參考。

還原運行繼續進行，直至所有的運行及對應的明示檔案被處理而且變更已被逆轉。

除了 Solaris Security Toolkit 軟體藉由尋找位於 `JASS_REPOSITORY` 的所有明示檔案來收集每次強化運行的資訊之外，Solaris Security Toolkit 軟體比較每個已變更檔案的總和檢查。任何總和檢查檔案的不合，會產生一個通知及被記錄下來。對於這些檔案，還原運行會詢問您要採取何種行動。

5. **若還原運作發現異常（強化運作之後檔案被手動變更），請輸入其中一個選項。**

下面是輸出範例顯示異常及處理異常的選擇。

程式碼範例 4-4 還原異常的輸出範例

```
[...]

================================================================
undo.driver: Undoing Finish Script: install-templates.fin
================================================================

[NOTE] Undoing operation COPY.
cp -p /etc/skel/local.login.JASS.20030125223413
/etc/skel/local.login
rm -f /etc/skel/local.login.JASS.20030125223413

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]    filename = /etc/.login
[WARN]    current = 3198795829:585, saved = 1288382808:584

Please select the course of action:

1. Backup.  Save current file before restoring original.
2. Keep.    Keep the current file, making no changes.
3. Force.   Ignore manual changes and overwrite current file.

Enter 1, 2, or 3:
```

範例中，若我們選擇項目 1，顯示下列輸出。

程式碼範例 4-5 還原期間選擇備份選項的輸出範例

```
Enter 1, 2, or 3: 1

[NOTE] BACKUP specified, creating backup copy of /etc/.login.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /etc/.login to /etc.login.BACKUP.JASS.20030125224926
cp -p /etc/.login.JASS.20030125223413 /etc/.login
rm -f /etc/.login.JASS.20030125223413

[...]
```

對於那些強化之後的手動變更過的檔案採取適當的行動。

當還原動作遇上您不要覆寫的已變更檔案，請在重新開機之前調整它們。

備註：範例之中，被變更的檔案使用新名稱作儲存：
/etc/.login.BACKUP.JASS.20030125224926。當還原已完成，比較該檔案與
/etc/.login 來判定是否需要進一步的調整。

6. **繼續之前調整異常。**

7. **調整異常之後，重新開機。**

   在強化之前對於系統停止及啓動可用的服務，重新開機是必要的。

第5章

配置及管理 JumpStart 伺服器

本章提供用於配置及管理 JumpStart 伺服器的資訊，以使用 Solaris Security Toolkit 軟體。JumpStart 技術爲 Sun 網路基礎的 Solaris 作業系統安裝機制，安裝過程可以使用 Solaris Security Toolkit 軟體。

Solaris Security Toolkit JumpStart 模式根據 JumpStart 技術，自 Solaris 作業系統版本 2.1 後即可用。JumpStart 技術藉由完全自動化 Solaris 作業系統及系統軟體安裝、提供修正及系統標準化功能來協助您管理複雜的事務。它提供一種符合快速安裝及部署系統的方法。

使用 JumpStart 技術的優點於系統安全領域是很明顯的。藉由使用 JumpStart 技術及 Solaris Security Toolkit 軟體，自動化安裝 Solaris 作業系統期間，安全化您的系統。此動作協助確保系統安裝時系統安全是標準化的。要取得有關 JumpStart 技術的資訊，請參閱 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

本章包含以下主題：

配置 JumpStart 伺服器及環境

要在 JumpStart 環境中使用，您必須複製在 `JASS_HOME_DIR`（`tar` 下載）或 `/opt/SUNWjass`（`pkg` 下載）中的 Solaris Security Toolkit 原始程式至 JumpStart 伺服器的根目錄。預設目錄在 JumpStart 伺服器上的 `/jumpstart`。當完成此作業，`JASS_HOME_DIR` 即成爲 JumpStart 伺服器的根目錄。

本章節假設讀者熟悉 JumpStart 技術而且有現存的 JumpStart 環境可使用。

要整合 Solaris Security Toolkit 軟體至 JumpStart 架構只需要幾個步驟。

▼ 配置 JumpStart 模式

1. **複製 Solaris Security Toolkit 原始程式至 JumpStart 伺服器的根目錄。**

   例如，若 Solaris Security Toolkit 歸檔解壓縮至 JASS_REPOSITORY，而 JumpStart 伺服器根目錄是 /jumpstart，下列指令則會複製 Solaris Security Toolkit 原始程式：

```
# pwd
/opt/SUNWjass
# tar cf - . | (cd /jumpstart; tar xf -)
```

   一般來說，Solaris Security Toolkit 軟體被安裝在 JumpStart 伺服器的 SI_CONFIG_DIR，它通常也會是 JASS_HOME_DIR。

2. **若您作了 Solaris 2.5.1 作業系統 sysidcfg 檔案的任何修改，確定它們在 JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1 目錄中。**

   若您使用 Solaris 2.5.1 作業系統，JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1 中的 sysidcfg 檔案不能直接被使用，原因是此版本的 Solaris 僅支援 SI_CONFIG_DIR 中的 sysidcfg 檔案而非子目錄中的檔案。要免於此項限制 Solaris 2.5.1 作業系統，Solaris Security Toolkit 軟體有 SI_CONFIG_DIR/sysidcfg，它連結至 JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1/sysidcfg 檔案。

3. **利用下列指令複製 JASS_HOME_DIR/Drivers/user.init.SAMPLE 至 JASS_HOME_DIR/Drivers/user.init：**

```
# pwd
/jumpstart/Drivers
# cp user.init.SAMPLE user.init
```

4. **若您遇到多宿主 (multihomed) JumpStart 伺服器的問題，請將 JASS_PACKAGE_MOUNT 及 JASS_PATCH_MOUNT 這兩個項目修改爲正確的路徑 JASS_HOME_DIR/Patches 及 JASS_HOME_DIR/Packages 目錄。**

5. **若您要安裝 Solaris Security Toolkit 軟體於 SI_CONFIG_DIR 子目錄下，如 SI_CONFIG_DIR/path/to/JASS，然後加入下列至 user.init 檔案：**

```
if [ -z "${JASS_HOME_DIR}" ]; then
       if [ "${JASS_STANDALONE}" = 0 ]; then
              JASS_HOME_DIR="${SI_CONFIG_DIR}/path/to/JASS"
       fi
fi
export JASS_HOME_DIR
```

6. **選擇或建立 Solaris Security Toolkit 驅動程式（例如預設的 secure.driver）。**

- 若所有 `hardening.driver` 及 `config.driver` 中列出的程序檔要被使用，則請加入 `Drivers/secure.driver` 路徑至 `rules` 檔案。
- 若僅使用被選定之程序檔，請複製那些檔案，然後修改複製檔。

7. 當完成驅動程式後，製作適當的 `rules` 檔案項目。

項目應相似於下列：

```
hostname imbulu - Profiles/core.profile Drivers/secure.driver
```

注意：切勿變更 Solaris Security Toolkit 軟體內含的程序檔。要允許更有效率的移植到 Solaris Security Toolkit 軟體之新發行版本，分開維護原始檔案及您的自訂檔案。

要成功地整合 Solaris Security Toolkit 軟體至現存 JumpStart 環境，還需要一處的更改。

8. 若您使用 Solaris Security Toolkit 軟體所提供的 `sysidcfg` 檔案來自動化 JumpStart 用戶端的安裝，請檢閱它們的適用性。

當剖析 `sysidcfg` 檔案時，若 JumpStart 伺服器發生任何錯誤，整個檔案的內容會被忽略。

當完成本章節中所有配置步驟後，您可以於用戶端使用 JumpStart 技術，安裝過程中可以成功地強化或最小化作業系統。

使用 JumpStart 設定檔範本

JumpStart 設定檔範本是只可於 JumpStart 模式下使用的檔案。需要的或選用的設定檔內容描述於 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

使用 JumpStart 設定檔範本如同您個人站台的修改的範例一般。檢查設定檔來判定您的環境中什麼更改（如有需要）是必要的。

複製設定檔，然後自您的站台作修改。不要修改原始檔案，原因是 Solaris Security Toolkit 軟體更新可會覆寫您的自訂檔案。

下列 JumpStart 設定檔爲 Solaris Security Toolkit 軟體內含的檔案：

- `32-bit-minimal.profile`
- `core.profile`
- `end-user.profile`
- `developer.profile`
- `entire-distribution.profile`

- oem.profile
- minimal-Sun_ONE-WS-Solaris*.profile
- minimal-SunFire_Domain*.profile

下列章節中說明這些設定檔。

32-bit-minimal.profile

對於 32 位於最小化系統，JumpStart 設定檔是一個相當通用的 JumpStart 設定檔。它是一個發展最小化系統的合理起始點，被用來做爲 minimal-Sun_ONE-WS-Solaris*.profile 最小化程序檔的起始點。

core.profile

此 JumpStart 設定檔會安裝最小的 Solaris 作業系統叢集 (SUNWCreq)。除了指定磁碟的分割包括 root 及交換分割區，沒有修改其他的配置。

end-user.profile

此 JumpStart 設定檔會安裝「一般使用者 Solaris 作業系統」叢集 (SUNWCuser) 以及爲程序記錄正常運作所需的兩個 Solaris 作業系統套裝模組。除此之外，磁碟分割被定義爲只包含 root 及交換分割區。

developer.profile

此 JumpStart 設定檔會安裝「開發人員 Solaris 作業系統」叢集 (SUNWCprog) 以及爲程序記錄正常運作所需的兩個 Solaris 作業系統套裝模組。如同 core.profile 的定義，除了 Solaris 作業系統叢集，只定義另外一個配置是包含 root 及交換的磁碟分割。

entire-distribution.profile

此 JumpStart 設定檔會安裝「完整分發 Solaris 作業系統」叢集 (SUNWCall)。如同其他的設定檔，磁碟分割定義含 root 及交換分割區。

oem.profile

此 JumpStart 設定檔會安裝「OEM Solaris 作業系統」叢集 (SUNWCXall)。此叢集爲「完整分發」叢集的超集合，它安裝由 OEM 提供的軟體。

minimal-Sun_ONE-WS-Solaris*.profile

所有下列設定檔依據 Sun BluePrints OnLine 文摘，其標題爲 *「Minimizing the Solaris Operating Environment for Security」*。所有文章內提到的 Solaris 作業系統版本都有特定的設定檔。下列 JumpStart 設定檔與文章內參照的相同。

- minimal-Sun_ONE-WS-Solaris.26.profile
- minimal-Sun_ONE-WS-Solaris7-32bit.profile
- minimal-Sun_ONE-WS-Solaris7-64bit.profile
- minimal-Sun_ONE-WS-Solaris8-32bit.profile
- minimal-Sun_ONE-WS-Solaris8-64bit.profile
- minimal-Sun_ONE-WS-Solaris9-64bit.profile

minimal-SunFire_Domain*.profile

所有下列設定檔依據 Sun BluePrints OnLine 文摘，其標題爲 *「Minimizing Domains for Sun Fire V1280, 12K, and 15K Systems」*。下列 JumpStart 設定檔與文章內參照的相同。

- minimal-SunFire_Domain-Apps-Solaris8.profile
- minimal-SunFire_Domain-Apps-Solaris9.profile
- minimal-SunFire_Domain-NoX-Solaris8.profile
- minimal-SunFire_Domain-NoX-Solaris9.profile
- minimal-SunFire_Domain-X-Solaris8.profile
- minimal-SunFire_Domain-X-Solaris9.profile

新增及移除用戶端

下面資訊說明 JumpStart 模式可用的程序檔。此模式由 Solaris Security Toolkit 驅動程式新增至 JumpStart 伺服器的 rules 而控制。

若您尚未將您的環境配置爲使用 JumpStart 模式，請參閱第 61 頁「配置 JumpStart 伺服器及環境」。

add-client 程序檔

自 JumpStart 伺服器，要簡化 新增用戶端，請使用此 Solaris Security Toolkit 軟體內含的程序檔。下面段落說明了指令及選項，但是尚未說明底層的 JumpStart 技術。請參閱 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」，以取得有關 JumpStart 技術的資訊。

add-client 程序檔是一個 add_install_client 指令的包裝函式，它接受下列引數。

用法範例：

```
# add-client -c client -i server -m client-class -o client-OS -s sysidcfg
```

表 5-1 說明 add-client 指令的有效輸入。

表 5-1 JumpStart add-client 指令

值	說明
-c *client*	JumpStart 用戶端可分解的主機名稱。
-h	顯示用法資訊。不需搭配其他選項使用。其他選項都將被忽略。
-i *server*	JumpStart 用戶端的 IP 位址或可分解之主機名稱 JumpStart 伺服器介面。若沒有指定值，會顯示本機主機可用的介面清單。
-m *client-class*	JumpStart 用戶端的機器類別。它的格式如同 uname -m 指令的輸出格式。
-o *client-OS*	Solaris 作業系統的修訂版，可於 JASS_HOME_DIR/OS 目錄取得，必須安裝到用戶端。若未指定特定的值，將顯示 JASS_HOME_DIR/OS 目錄內可用 Solaris 作業系統的版本清單。
-s *sysidcfg*	指向替代目錄的可選擇路徑名稱，包含一個您要用作系統辨識及配置的 sysidcfg 檔案。依照預設值，此值設定爲 JASS_HOME_DIR/Sysidcfg/Solaris_version/ 目錄，由用戶端指定的作業系統的版本進行解壓縮。若有指定，必須使用相對於 JASS_HOME_DIR 目錄的路徑名稱。只需指定至 sysidcfg 檔案的路徑名稱。
-v	此程式的版本資訊。
-?	顯示用法資訊。不需搭配其他選項使用。其他選項都將被忽略。

新增一個名爲 jordan JumpStart 用戶端至名爲 nomexJumpStart 伺服器。使用 Solaris 8 作業系統 (4/01) 名爲 nomex-jumpstart 的介面，您可使用下列 add-client 指令：

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart
updating /etc/bootparams
```

要使用 sysidcfg 選項來新增相同的 JumpStart 用戶端 (jordan) ，您可使用下列指令：

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart -s
Hosts/jordan
updating /etc/bootparams
```

rm-client 程序檔

要簡化自 JumpStart 伺服器上移除用戶端，使用 Solaris Security Toolkit 軟體內含的程序檔。下面段落說明了指令及選項，但是並未說明底層的 JumpStart 技術。請參閱「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」，以取得有關 JumpStart 技術的資訊。

rm-client 程序檔是一個 rm_install_client 指令的包裝函式，與 add-client 近似：

用法範例：**rm-client** [-c] *client*

其中，*client* 是 JumpStart 用戶端可分解的主機名稱。

表 5-2 說明 rm-client 指令的有效輸入。

表 5-2 JumpStart rm-client 指令

值	說明
-c *client*	JumpStart 用戶端可分析的主機名稱。
-h	顯示用法資訊。不需搭配其他選項使用。其他選項都將被忽略。
-v	此程式的版本資訊。
-?	顯示用法資訊。不需搭配其他選項使用。其他選項都將被忽略。

要移除一個名爲 jordan 的 JumpStart 用戶端，您可使用以下的 rm-client 指令：

```
# ./rm-client -c jordan
removing jordan from bootparams
```

第6章

稽核系統安全性

本章說明如何使用 Solaris Security Toolkit 稽核（驗證）系統的安全性。請使用本章的資訊和程序來維護在強化之後所建立的安全性設定檔。對於已部署的系統，在強化之前您可使用本章的資訊來評估系統的安全性。

備註：本章及本書中的*稽核*一詞是用來定義透過比較預先定義的安全性設定檔，Solaris Security Toolkit 軟體驗證安全性部署的自動化程序。此專有名詞在此出版品內的使用不保證系統在使用稽核選項後即會安全無虞。

本章包含以下主題：

維護安全性

維護安全性是一個持續的程序，必須經常檢閱及重複查看。維護一個安全的系統需要心生警惕，原因是任何系統預設的安全配置經過一段時間之後開放度會大增（要取得維護安全的資訊，請參閱第 28 頁「維護系統安全性」。）

根據使用者經驗及要求，我們爲 Solaris Security Toolkit 軟體開發了自動化方法，藉由判定與特定安全性設定檔案相符的程度來稽核系統的安全狀態。

備註：此方法僅適用於獨立模式下使用 `jass-execute -a` 指令，而且不可在 JumpStart 安裝期間使用。

定期的稽核系統的安全狀態，手動或自動（例如：透過 cron 工作或 rc 程序檔）皆可。例如，強化一個新安裝的系統之後，5 天之後執行 Solaris Security Toolkit 軟體稽核指令 (jass-execute -a *driver-name*) 判定系統的安全性已經改變，脫離安全性設定檔所定義的狀態。

多久作一次稽核在於系統的重要性及您的安全策略。有些使用者每個小時、每天或一個月一次作稽核。有些使用者每個小時執行 mini-scan（限定數量的檢核），以及每一天執行全部掃描（所有可能的檢核）。

要維護已部署系統的安全狀態，稽核是重要的元件。若系統狀態沒有定期的稽核，然後隨著時間配置會偏移，原因可能是隨機變化 (entropy) 或者不明狀況或惡意的更改預定的系統安全狀態。若沒有定期的檢閱，這些變更會變成無法偵測而且無法進行修正。結果就是系統會不安全及更脆弱。

除了定期稽核之外，升級、修補及其他大型系統配置更改後都要做稽核。

強化之前檢視安全性

有些狀況下，您會發現在強化*之前* 檢閱已部署系統的安全狀態是有用的。例如，若您接掌由他人所管理的已部署系統，檢閱系統的狀態，如此您知道它們的狀態以及，若有需要，可以帶領系統進入依從您系統所使用的相同安全性設定檔。

自訂安全性稽核

稽核選項提供高彈性及可延伸的機制來評估系統的狀態。使用強化程序檔，您可自訂稽核程序檔的動作。例如，您可自訂環境變數、自訂架構及輔助程式函數、加入新的檢查、及加入新的功能至稽核架構。

大部分使用者發現標準及產品特定程序檔適合做爲自訂環境稽核的範本。對於此情境，透過驅動程式、結束程序、檔環境變數、及檔案範本自訂稽核程序檔行動。這些自訂的更改只需少許工作而且不需更改程式碼來達成。不論您爲強化系統作了什麼改變，當您執行稽核 Solaris Security Toolkit 軟體會自動知道。

偶而，使用者發現須新增 Solaris Security Toolkit 軟體未提供的檢查或功能是有必要的。對於此情境，加入檢查或新的功能至稽核程序檔。（對應的結束程序檔要做相關的修改。）有些狀況下可能需要更改程式碼。當進行新增或修改程式碼時要特別小心，以避免帶入錯誤及失敗。

有些使用者需要建立全新的專屬系統或者站台特定的，驅動程式及程序檔。當您編碼新的驅動程式及程序檔時，使用範本及樣品做爲準則。當您使用稽核選項時，站台特定驅動程式、結束程序檔、變數、及函數並*不會* 自動的被 Solaris Security Toolkit 軟體知

道。例如，若您新增一個名爲 abcc-nj-secure.driver 站台特定的驅動程式，它包括一個站台特定結束程序檔，abcc-nj-install-foo.fin，然後您需要建立一個站台特定的稽核程序檔，abcc-nj-install-foo.aud。同樣地，若您以稽核程序檔做開始，您應該建立對應的結束程序檔。

要自訂或建立一個新的驅動程式、程序檔、變數、及函數，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

例如，您可能需要新增一個 Solaris Security Toolkit 未安裝的修補程式。您可將標準或產品特定的範本作延伸，或者建立您自己的範本。若您建立自己的範本，建立一個結束程序檔來新增修補程式，然後建立一個對應的修補程式安裝的稽核程序檔來作檢查。

準備稽核安全性

要使用本章的指示及準則，您需要一個安全性設定檔。要取得有關建立及使安全性設定檔生效，請參閱第 2 章。

Solaris Security Toolkit 發行內包含不同的安全性設定檔範本做爲驅動程式。如同本書前面章節所描述，預設安全性設定檔及被這些驅動程式所作的更改可能並不適合您的系統。通常，由這些驅動程式所實現的安全性設定檔爲系統的 「高值參數」標記。因此我們認爲停用的服務是不需要的，而且它們的預設選用安全功能爲停用。

很多 Solaris Security Toolkit 軟體使用者發現，它們的環境可以接受標準及特定產品安全性設定檔的範本。若您的狀況可以套用，判定那一個安全性設定檔是最接近您要的安全狀態，然後使用它們評估及強化您的系統。

爲您的環境檢視或自訂安全性設定檔範本，或者建立一個新的範本。「*Solaris Security Toolkit 4.1 Reference Manual*」提供自訂安全性設定檔的技巧及準則。這個方法提供爲您的機構量身訂做適合的安全性狀態，而且作安全性評估時會減少回傳的假錯誤數量。例如，若您知道 Telnet 需要被啓用，您可自訂安全性設定檔，如此當進行安全評估時，軟體不會認爲 Telnet 是弱點。例如，系統使用 Telnet 和 Kerberos 作驗證及加密，即不會認爲 Telnet 是弱點。

使用選項及控制稽核輸出

本節說明執行稽核運轉之可用選項及用來控制輸出的選項。本節包含以下主題：

指令行選項

範例對照安全性設定檔來稽核系統的方法：

```
# jass-execute -a driver [ -V [0-4] ] [ -q | -o output-file ]
[ -m email-address ]
```

當執行 Solaris Security Toolkit 軟體稽核指令，您可使用表 6-1 中所列出的選項。

表 6-1 使用稽核指令的指令行選項

選項	說明
-a	判定系統是否符合其安全性設定檔。
-h	顯示 jass-execute 說明訊息，提供可用選項的簡介。
-m	傳送輸出至電子郵件位址。
-o	導引輸出至檔案。
-q	阻止主控台顯示輸出。也稱作無訊息選項。
-V	指定稽核運行的詳細程度。

要取得有關 jass-execute -a 指令可用選項的詳細資訊，請參閱以下章節：

- 第 73 頁「顯示說明選項」
- 第 73 頁「電子郵件通知選項」
- 第 74 頁「輸出檔案選項」
- 第 74 頁「無訊息選項」
- 第 74 頁「詳細度選項」

顯示說明選項

jass-execute 的 -h 選項顯示說明訊息，提供適用選項的簡介。

-h 選項之輸出與下列輸出相似：

程式碼範例 6-1 -h 選項輸出範例

```
# ./jass-execute -h

To apply this Toolkit to a system, using the syntax:
  jass-execute [-r root_directory -p os_version ]
  [ -q | -o output_file ] [ -m e-mail_address ]
  [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
  jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
     [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
  jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
     [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
  jass-execute -H

To display the last application of the Toolkit on a system:
  jass-execute -l

To display this help message:
  jass-execute -h
  jass-execute -?

To display version information for this program:
  jass-execute -v
```

電子郵件通知選項

-m *email-address* 選項提供當執行完畢，Solaris Security Toolkit 軟體自動將輸出寄出的機制。電子信箱報告爲使用其他選項所產生之系統日誌檔之外的報告。

Solaris Security Toolkit 透過電子郵件選項執行呼叫 sunfire_15k_sc-config.driver 應與下列輸出相似：

```
# ./jass-execute -m root -a sunfire_15k_sc-config.driver
[...]
```

輸出檔案選項

-o *output-file* 選項重導 jass-execute 螢幕輸出至檔案 *output-file*。

此選項對保留在 JASS_REPOSITORY 目錄的日誌檔沒有任何效用。此選項對於執行在一台慢終端機上時非常有幫助，因爲執行 Solaris Security Toolkit 會產生大量的輸出。

此選項可同時與 -d、-u 或 -a 選項同時使用。

-o 選項之輸出與下列輸出相似：

程式碼範例 6-2 -o 選項輸出範例

```
# ./jass-execute -o jass-output.txt -a secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
#
```

無訊息選項

-q 選項停止將強化執行之 Solaris Security Toolkit 輸出到標準輸入 / 輸出 (stdio) 資料流。

此選項對保留在 JASS_REPOSITORY 目錄的日誌檔沒有任何效用。與 -o 選項相似，此選項對於執行 cron 工作或在緩慢網路上執行 Solaris Security Toolkit 軟體非常有幫助。

此選項可同時與 -d、-u 或 -a 選項同時使用。

-q 選項之輸出與下列輸出相似：

程式碼範例 6-3 -q 選項輸出範例

```
# ./jass-execute -q -a secure.driver
[NOTE] Executing driver, secure.driver
```

詳細度選項

-V 選項指定稽核運行時的詳細度等級。此選項只適用稽核。詳細度等級提供高彈性的方法來顯示稽核的結果。例如，若您有 100 台電腦作稽核，您可能希望限制輸出爲：以每台電腦一行來判定那台電腦通過或沒有通過。然後對於那些沒有通過的電腦，您可能會想要執行稽核，它可產生擴展性的輸出以便著重於問題所在區域。

五個詳細度等級（0 至 4）由 -V 選項來控制。每個增加的等級提供您可用來更瞭解何者已通過檢查以及何者沒有通過的更多資訊。表 6-2 說明詳細度等級。

表 6-2 稽核詳細度等級

等級	輸出
0	一行表示通過或失敗。
1	對於每個程序檔而言，一行表示通過或失敗。所有程序檔行下有一個總合分數行。
2	對於每個程序檔，提供所有檢查的結果。
3	多行提供全部輸出，包含標題及標頭訊息。
4	多行（等級 3 的所有資料）加上由 logDebug 日誌函數產生的所有項目。此等級作除錯之用。

備註：jass-execute -V 指令的預設詳細度等級是 3。

要取得詳細度的完整說明，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

標題及訊息輸出

您可配置 Solaris Security Toolkit 稽核選項至報告或者省略標題及訊息。JASS_LOG_BANNER 變數不可用在詳細度 0 至 2。這些輸出選項適用詳細度 3 及 4。例如，您可能想要去除輸出的通過訊息（JASS_LOG_SUCCESS 變數），如此您可報導和集焦於失敗訊息（JASS_LOG_FAILURE 變數）。

表 6-3 列舉您可透過記錄變數控制的標題及訊息。（要取得有關記錄變數的詳細資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。）若記錄變數設定爲 0，該種類的訊息不產生輸出。相反地，若記錄變數設定爲 1，訊息就會顯示。每一個變數的預設行動爲顯示輸出。表 6-3 說明記錄變數。

表 6-3 顯示稽核輸出的標題與訊息

記錄變數	日誌檔前綴	說明
JASS_LOG_BANNER	所有標題輸出	此參數控制標題訊息的顯示。這些訊息通常由等號（「=」）或者破折號（「-」）字元所組成的分隔符號圍繞。
JASS_LOG_ERROR	[ERR]	此參數控制錯誤訊息的顯示。若設定爲 0，將不產生錯誤訊息。
JASS_LOG_FAILURE	[FAIL]	此參數控制所有失敗訊息的顯示。若設定爲 0，將不產生失敗訊息。

表 6-3 顯示稽核輸出的標題與訊息 *（續上頁）*

記錄變數	日誌檔前綴	說明
JASS_LOG_NOTICE	[NOTE]	此參數控制所有提示的顯示。若設定爲 0，不產生提示訊息。
JASS_LOG_SUCCESS	[PASS]	此參數控制成功或通過狀態訊息的顯示。若設定爲 0，不產生成功訊息。
JASS_LOG_WARNING	[WARN]	此參數控制警告訊息的顯示。若設定爲 0，不產生警告訊息。

當您只需檢視特定訊息時，使用這些選項非常有用。藉由設定這些選項，您可最小化輸出，但仍可著重於您認爲重要的範圍。例如，藉由設定除了 JASS_LOG_FAILURE（保留預設值 1）之外的所有的記錄變數爲 0，稽核只報告由 logFailure 函數所產生的失敗訊息。

程式碼範例 6-4 僅報告稽核失敗之輸出範例

```
# JASS_LOG_FAILURE=1
# export JASS_LOG_FAILURE
[setting of other parameters to 0 omitted]
# ./jass-execute -a secure.driver -V 2
update-at-deny        [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
update-at-deny        [FAIL] Audit Check Total : 1 Error(s)
update-inetd-conf     [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Audit Check Total : 3 Error(s)
```

主機名稱、程序檔名稱、以及時間戳記輸出

您可配置 Solaris Security Toolkit 稽核選項，包括主機名稱、程序檔名稱以及詳細度 0 至 2 的資訊。例如，若您要稽核多台電腦，您也許想要根據主機，程序檔名稱或者時間戳記來排序。表 6-4 列舉出變數。

表 6-4 顯示主機名稱、程序檔名稱、及時間戳記稽核輸出

變數名稱	變數描述
JASS_DISPLAY_HOSTNAME	設定此參數爲 1 導致 Solaris Security Toolkit 軟體置系統主機名稱至每個記錄項目之前。此資訊根據 JASS_HOSTNAME 參數而來。依據預設，此參數是空的，因此 Toolkit 不會顯示此資訊。
JASS_DISPLAY_SCRIPTNAME	依據預設，此參數設定爲 1，如此 Solaris Security Toolkit 軟體將目前開始執行的稽核程序檔的名稱置於每個記錄之前。設定任何值給此參數會導致 Toolkit 不顯示資訊。
JASS_DISPLAY_TIMESTAMP	設定此參數爲 1 導致 Solaris Security Toolkit 軟體將執行稽核的時間戳記置於每個記錄項目之前。此資訊根據 JASS_TIMESTAMP 參數而定。依據預設，此參數是空的，因此軟體不顯示此資訊。

藉由配置 Solaris Security Toolkit 軟體將主機、程序檔、時間戳記資訊作前置，您可結合不論是單一系統或一組系統的執行結果，然後根據關鍵資料來作排序。您可使用這些資訊來尋找跨越數個系統或是部署程序症狀性的問題。例如，系統管理員可以知道若建立系統時使用特定的程序，檢查則一定會失敗。

例如，設定 JASS_DISPLAY_TIMESTAMP 參數爲 1 以及設定 JASS_DISPLAY_SCRIPTNAME 值爲 0 的輸出與下列輸出相似。

程式碼範例 6-5 稽核記錄項目輸出範例

```
# JASS_DISPLAY_SCRIPTNAME=0
# JASS_DISPLAY_TIMESTAMP=1
# export JASS_DISPLAY_SCRIPTNAME JASS_DISPLAY_TIMESTAMP
# ./jass-execute -a secure.driver -V 2
20030101233525 [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
20030101233525 [FAIL] Audit Check Total : 1 Error(s)
20030101233525 [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Audit Check Total : 3 Error(s)
```

執行安全性稽核

定期執行系統安全性評估，可以提供一個系統的安全性是否貼近安全性設定檔的基準。最普遍的場景是強化新安裝之後，進行安全評估做爲維護安全的作業。我們設計了安全評估選項，因此您可以單純的執行與您作系統強化相同的強化驅動程式。但是現在您可使用 `-a` 選項來檢查目前的狀態與強化期生效的安全性設定檔作比較。這項設計去除了複雜性而且提供彈性。例如，當您更新您的安全性設定檔，接下來使用更新的安全性設定檔作安全評估。

另一個可能的情境是，您必須負責已部署系統的安全。在強化之前，您想要進行安全性評估。這樣的情境下，您要定義自己的安全性設定檔，自訂 Solaris Security Toolkit 安全性設定檔範本，或者不加更動的使用安全檔案範本。

▼ 執行安全性稽核

執行稽核之前，您需要定義或選擇一個安全性設定檔。要取得更多資訊，請參閱第 71 頁「準備稽核安全性」。

注意：若您在已部署但尚未強化的系統上執行安全評估，首先備份系統、重新開機，來確定它的配置是已知的、運作中的和一致的。任何預先開機期間偵測到的錯誤或警告，在進行安全評估之前應該被修正或作記錄。

1. **選擇您想要使用的安全性設定檔（強化驅動程式）：**
   - 若您曾做過系統強化，使用相同的安全性設定檔。

     例如，`secure.driver`。
   - 若您尚未強化系統，使用標準安全性設定檔或您自訂的檔案。

     例如，`secure.driver` 或 `abccorp-secure.driver`。

   若要完整及新的可用驅動程式清單，自下列網站下載最新版本的 Solaris Security Toolkit 軟體：

   `http://www.sun.com/security/jass`

   請參閱「*Solaris Security Toolkit 4.1 Reference Manual*」取得標準及產品專用驅動程式的資訊。對於最近的驅動程式清單，請參閱 Drivers 目錄。
2. **判定您要的指令行選項以及您想要如何控制輸出。**

   請參閱第 71 頁「使用選項及控制稽核輸出」。
3. **輸入 `jass-execute -a` 指令、安全性設定檔的名稱以及您想要的選項。**

下列是使用 sunfire_15k_sc-secure.driver 執行稽核的範例。

程式碼範例 6-6 執行稽核的輸出範例

```
# ./jass-execute -a sunfire_15k_sc-secure.driver
[NOTE] Executing driver, sunfire_15k_sc-secure.driver

[...]

================================================================
sunfire_15k_sc-secure.driver: Audit script: enable-rfc1948.aud
================================================================

#----------------------------------------------------------------
# RFC 1948 Sequence Number Generation
#
# Rationale for Audit:
#
# The purpose of this script is to audit that the system is
# configured and is in fact using RFC 1948 for its TCP sequence
# number generation algorithm (unique-per-connection ID). This is
# configured by setting the 'TCP_STRONG_ISS' parameter to '2' in
# the /etc/default/inetinit file.
#
# Determination of Compliance:
#
[...]
#----------------------------------------------------------------

[PASS] TCP_STRONG_ISS is set to '2' in /etc/default/inetinit.
[PASS] System is running with tcp_strong_iss=2.

# The following is the vulnerability total for this audit script.

[PASS] Audit Check Total : 0 Error(s)

================================================================

# The following is the vulnerability total for this driver profile.

[PASS] Driver Total : 0 Error(s)

================================================================
sunfire_15k_sc-secure.driver: Driver finished.
================================================================

[PASS] Grand Total : 0 Error(s)
```

當稽核運行已經啓始，Solaris Security Toolkit 軟體自 JASS_HOME_DIR/Audit 目錄中存取檔案。雖然所有的檔案存在於 JASS_HOME_DIR/Audit 及 JASS_HOME_DIR/Finish 目錄，共享相同的基本檔案名稱，它們的字尾不同。driver.run 程序檔自動的翻譯結束程序檔定義的 JASS_SCRIPTS 變數至稽核程序檔，藉由改變它們的字尾自 .fin 改爲 .aud。

稽核運行啓動及起始 Solaris Security Toolkit 軟體的狀態。每個運行期間驅動程式的存取會評估所有的檔案範本及稽核程序檔的狀態。每個檢查的結果是成功或失敗的狀態，由零或非零來表現。大多數狀況下，失敗由 1 來表示。每個執行的程序檔產生一個安全分數的小計，根據程序檔包含的每一個檢查的弱點的總計。更進一步，每個驅動程式的弱點小計值在完成驅動程式評估之後顯示。總合值在執行結束後顯示。

安全性評估選項提供一個容易瞭解的，起始安全評估時點的系統狀態。Solaris Security Toolkit 軟體藉由檢視配置檔案來檢查系統的儲存狀態，以及藉由檢視表格資訊、裝置驅動程式資訊及其他來檢查系統的執行狀態。Solaris Security Toolkit 軟體檢查每個檔案及服務是否存在以及檢查與服務相連的軟體是否已安裝、配置、啓用及執行。這個方法產生目前系統狀態的正確快照。

第7章

系統安全化

本章描述如何套用前章所提供之資訊及專業知識至真實情境內，安裝及安全化一個新的系統。本章說明如何使用 Solaris 8 作業系統的 Check PointFirewall-1 NG 來部署 Solaris Security Toolkit 軟體。

使用本章之資訊做爲新系統及應用程式安全化之準則及個案情境。

Sun BluePrint 文件以及線上文摘可用來引導您執行最小化以及強化 Sun 系統的過程。請參閱下列網站取得最新產品專用的書籍及文章：

`http://www.sun.com/blueprints`

本章包含以下主題：

規劃及準備

要有效用及有效率的部署最小化的以及安全化的系統，如同個案研究所描述，規劃及準備非常重要。底層之網路內部架構，策略以及程序必須就位。除此之外，系統的支援及維護必須已被定義及作好溝通。要取得更多有關規劃及準備的資訊，請參閱第 2 章。本章所描述的情境記錄了要達成一個防火牆系統的最小化及強化後的 Solaris 作業系統影像，系統管理員 (SA) 必須執行的程序及作業。

在此情境中，SA 爲服務提供者 (xSP)，它提供防火牆服務給它的客戶，建立一個自動化以及可延展的方案來建立及部署 Check PointFirewall-1 NG 系統。針對此情境，xSP 的需求以及考慮如下：

- 由於 xSP 計劃部署很多系統，建立及部署每一個系統的時程很重要而且必須符合效率。
- 系統由使用專屬管理網路連接至每個系統的內部乙太網路介面來作安裝。網路只可被 xSP 人員而非服務申請者使用。
- 所有其他介面位於分離的實體網路介面，而且已經過篩選。
- 管理網路的安全性對於已部署防火牆系統的全面安全性而言很重要。

根據上述需求，SA 決定使用 JumpStart 技術及 Solaris Security Toolkit 軟體來自動安裝、簡化以及強化作業系統影像。

假設及限制

本章假設我們使用已經運作正常的 Solaris Security Toolkit 軟體以及 JumpStart 技術安裝。本書的其他章節提供安裝軟體的指示及準則，請參閱該資訊適用的章節。

本章假設我們爲最小化及強化特定應用程式而發展一個自訂的配置。Solaris Security Toolkit 軟體沒有任何該應用程式專用之驅動程式或 JumpStart 設定檔。因此，我們需要建立此應用程式自訂驅動程式以及設定檔。此項作業可由複製現存驅動程式及設定檔，然後依照應用程式修改它而完成。

對於此個案情境，SA 的技術層次如下：

- 有足夠的知識及經驗配置作業系統以及應用程式。
- 知道如何測試配置及作調整來微調。
- 知道如何自安裝好的用戶端系統建立一個 JumpStart 環境。請參閱 Sun BluePrint 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。
- 熟悉作業系統的最小化技巧。請參閱 「*Enterprise Security:Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*」。

- 熟悉 Solaris Security Toolkit 軟體基礎而且已準備好使用最小化和強化技巧及準則來建立一個自訂配置。請參閱第 1 章。

系統環境

情境範例乃根據下列硬體及軟體環境：

- Check PointFirewall-1 NG
- Solaris 8 作業系統
- JumpStart 技術
- Solaris 作業系統叢集 (`SUNWCreq`)
- Solaris Security Toolkit 軟體
- 基於 SPARC 技術的平台
- 至少兩個乙太網路介面

安全性需求

對於此情境，高層次需求以及軟體套裝模組已確認，但是所有套裝模組之特定元件及服務需要認定。而且，需要用來處理管理系統之 Solaris 作業系統能力也需要被認定。

下列清單提供軟體元件如何被使用的詳細說明：

- 用於遠端管理的 Secure Shell
- 用來複製檔案的 FTP
- 用來鏡射磁碟的 Solstice DiskSuite™ 軟體
- SYSLOG 訊息轉送至中央儲存庫

根據此清單，您可建立一個安全性設定檔。要取得建立安全性設定檔以及使用設定檔範本的詳細資訊，請參閱第 25 頁「開發及實現 Solaris Security Toolkit 設定檔」。

建立安全性設定檔

安全性設定檔定義出當系統安全配置強化及最小化時，Solaris Security Toolkit 軟體所作的更改。沒有一個 Solaris Security Toolkit 軟體內含的標準安全性設定檔或驅動程式符合最小化 Check PointFirewall-1 NG 系統的需求。因此，您必須建立一個自訂的安全性設定檔來使適當的系統更改生效。

對於此情境，建立安全性設定檔的程序將於本章數個章節內說明。首先，我們根據現存的驅動程式建立新的驅動程式檔案。然後我們修改新的驅動程式來符合前面所描述的安全需求。第 84 頁「安裝軟體」中描述最小化，而強化則在第 91 頁「自訂強化配置」中說明。

安裝軟體

本節示範安裝軟體的程序。對於情境範例，我們提供所有例外或特定情境的指示。要取得有關安裝軟體的一般指示，使用本手冊其他部分的參考文獻。

備註：您可使用如下列的指示做爲處理相關狀況的範本。

本節包含以下作業：

下載及安裝安全性軟體

於 JumpStart 伺服器上，下載及安裝 Solaris Security Toolkit 以及其他軟體，包括修補程式。如下所示。

▼ 下載及安裝安全性軟體

1. **下載及安裝 Solaris Security Toolkit 軟體及其他安全性軟體。**

   請參閱第 31 頁「下載安全性軟體」。

2. **安裝下載的 Solaris Security Toolkit 軟體及其他安全性軟體。**

   請參閱第 38 頁「安裝及執行軟體」。

注意：還不要執行 Solaris Security Toolkit 軟體。首先進行下面段落說明的其他配置及自訂。

安裝修補程式

作業系統修補程式可能針對弱點、可用性問題、效能考慮及其他系統的狀況。當安裝一個新的作業系統時，以及安裝之後的持續進行基礎上，要檢查來確保已經安裝了適當的修補程式。

Solaris Security Toolkit 軟體提供安裝 SunSolve Online 之「建議和安全修補程式叢集」的機制。此特定作業系統的修補程式叢集包含大部分需要的修補程式。

▼ 安裝修補程式

1. **最低限度，下載「建議和安全修補程式叢集」至 `Patches` 檔案後解壓縮。**

   若強化驅動程式內含 `install-recommended-patches.fin` 程序檔，修補叢集會自動安裝。

   Check PointFirewall-1 NG 有另一個問題。此程式需要一個「建議和安全修補程式叢集」並未內含的特定修補程式。Check PointFirewall-1 NG 需要下列修補程式：

   - 108434
   - 108435

2. **要自動安裝修補程式 108434 及 108435，自 SunSolve OnLine 下載最新的版本至 `Patches` 目錄。**

3. **建立一個新的結束程序檔（例如：`fw1-patch-install.fin`）使用修補程式的名稱來呼叫 `add_patch` 輔助程式函數。**

   此結束程序檔使用兩個 Check PointFirewall-1 NG 所需要的修補程式 ID 呼叫適當的輔助程式函數。例如：

```
# !/bin/sh

# add_patch 108434-10

# add_patch 108435-10
```

指定及安裝作業系統叢集

定義完要安裝作業系統的磁碟佈局後，下一個作業是指定要安裝的作業系統叢集。選擇 Solaris 作業系統適用的五個安裝叢集之中的一個：`SUNWCreq`、`SUNWCuser`、`SUNWCprog`、`SUNWCall` 及 `SUNWCXall`。

▼ 指定及安裝作業系統叢集

1. **指定要安裝的作業系統叢集。**

   由於此個案情境的目的是建立一個最小化及專屬的防火牆裝置，Solaris 作業系統可使用叢集內最小的一個 (`SUNWCreq`)，此叢集也就是 Core。

由於此叢集包括較少的套裝模組，可能還需要其他的套裝模組軟體。這些其他需要的套裝模組與 Solaris 作業系統叢集的定義需要納入設定檔內。

基準設定檔定義將下列加入前面所定義的設定檔內。

```
cluster           SUNWCreq
```

SUNWCreq 安裝叢集內含防火牆 Sun 伺服器正常運轉時不需要的套裝模組。當您有一個運作基準之後，請移除這些多餘的套裝模組。請參閱 Sun BluePrints OnLine 文摘「Minimizing the Solaris Operating Environment for Security:Updated for the Solaris 9 Operating Environment」。

2. **使用適當定義的安全性設定檔執行完整的安裝，判定是否有套裝模組互相依賴的問題。**

   有些套裝模組依賴性發生於安裝期間，而我們判定 Check PointFirewall-1 NG 需要下列 Solaris 作業系統套裝模組：

   - SUNWter — 終端機資訊
   - SUNWadmc — 系統管理核心程式庫
   - SUNWadmfw — 系統及網路管理架構
   - SUNWlibC 及 SUNWlibCx — Check PointNG 應用程式所需

   設定檔內套裝模組的完整清單如下：

```
cluster           SUNWCreq
package           SUNWter          add
package           SUNWlibC         add
package           SUNWlibCx        add
package           SUNWadmc         add
package           SUNWadmfw        add
```

   雖然此清單對於本個案是完整的，根據實際環境所部署的配置，其他套裝模組可能被加入或移除。

   直到系統功能及安全性觀點兩者皆可驗證之前，如第 96 頁「品質保證測試」所述，套裝模組的最終清單可能需要作修改。若有需要，修改設定檔、重新安裝系統，然後重複作測試。

3. **依據前面兩個步驟中的套裝模組依賴性，建立一個 minimize-firewall.fin 程序檔。**

配置 JumpStart 伺服器及用戶端

本節示範如何配置 JumpStart 伺服器及用戶端來使用自訂安全設計檔作最小化。要取得有關在 JumpStart 環境下使用 Solaris Security Toolkit 軟體的詳細資訊，請參閱第 5 章。

本節包含以下作業：

準備基礎架構

進行下列作業來準備基礎架構。下列作業示範使用現存的驅動程式，設定檔及結束程序檔來建立用戶端配置基準線的程序。當此配置基準線已經就定位，確定它可以正常地工作，然後爲選定的應用程式將它改造成爲自訂配置。

▼ 準備基礎架構

1. **配置您的 JumpStart 伺服器及環境。**

   請參閱第 5 章取得詳細指示。

2. **使用 `add-client` 指令新增用戶端至 JumpStart 伺服器。**

   程式碼範例 7-1 新增用戶端至 JumpStart 伺服器

```
# pwd
/jumpstart
# bin/add-client -c jordan -o Solaris_8_2002-02 -m sun4u
-s nomex-jumpstart
cleaning up preexisting install client "jordan"
removing jordan from bootparams
updating /etc/bootparams
```

3. **爲用戶端建立一個 `rules` 檔案項目，指定適當的 JumpStart 設定檔及結束程序檔。例如：**

```
hostname jordan - Profiles/xsp-minimal-firewall.profile \
  Drivers/xsp-firewall-secure.driver
```

4. **藉由複製 Solaris Security Toolkit 軟體所提供的檔案，來建立一個名爲** `xsp-minimal-firewall.profile` **的設定檔以及名爲** `xsp-firewall-secure.driver` **的驅動程式。**

   您必須在成功完成下面步驟之前建立這些檔案。最初這些檔案可以是 Solaris Security Toolkit 軟體所發行的檔案的備份。切勿修改 Solaris Security Toolkit 軟體所發行的原始檔案。下面範例說明如何建立檔案。

程式碼範例 7-2 建立設定檔

```
# pwd
/jumpstart/Drivers
# cp install-Sun_ONE-WS.driver xsp-firewall-secure.driver
# cp hardening.driver xsp-firewall-hardening.driver
[...]
# pwd
/jumpstart/Profiles
# cp minimal-Sun_ONE-WS-Solaris8-64bit.profile \
     xsp-minimal-firewall.profile
```

   此範例是根據一個專屬網路伺服器的配置，因爲它是使用它來開發專屬防火牆的良好基準。

5. **建立設定檔及驅動程式檔案之後，更改檔案如下：**

   a. **使用** `xsp-firewall-hardening.driver` **來取代參照到** `hardening.driver` **的** `xsp-firewall-secure.driver`。

   b. **以** `minimize-firewall.fin` **以及您的結束程序檔（例如：**`fw1-patch-install.fin`**）來取代** `JASS_SCRIPTS` **中定義的兩個結束程序檔。**

      修改過的程序檔應當與下列顯示相似。

程式碼範例 7-3 修改過程序檔的輸出範例

```
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
                minimize-firewall.fin
                fw1-patch-install.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

6. **使用下列指令檢查 `rules` 檔案項目的正確性。**

程式碼範例 7-4 檢查 `rules` 檔案的正確性

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/end-user.profile...
Validating profile Profiles/xsp-minimal-firewall.profile...
Validating profile Profiles/test.profile...
Validating profile Profiles/entire-distribution.profile...
Validating profile Profiles/oem.profile...
The custom JumpStart configuration is ok.
```

此時，應當可以開始於用戶端安裝 JumpStart，此範例爲 `jordan`。使用 JumpStart 配置及 Solaris Security Toolkit 驅動程式、結束程序檔、以及您建立的設定檔。

7. **若您檢查 `rules` 檔案時發生問題，請參閱第 89 頁「驗證及檢核規則檔案」。**

8. **在用戶端 `ok` 提示符號下，輸入下列指令來安裝使用 JumpStart 基礎架構的用戶端。**

```
ok> boot net - install
```

若用戶端無法建立，檢視配置以及修改它直至它可以正常地工作。請注意，本節中並未涉及所有 JumpStart 配置之狀況。請參閱 Sun BluePrint 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」，以取得詳細資訊。

達成 `rules` 檔案正常運轉以及正確地安裝修補程式後，您可啓動用戶端系統的基層安裝以及進行用戶端最小化及強化。

驗證及檢核規則檔案

驗證 `rules` 檔案的正確性時，您可能會遇上各種不同的問題。本節內提出一些最常見的問題。

rules 檔案的第一次運行結果如下列輸出所示。

程式碼範例 7-5 rules 檔案的輸出範例

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/xsp-minimal-firewall.profile...
Error in file "rules", line 20
hostname jordan - Profiles/xsp-minimal-firewall.profile
Drivers/xsp-firewall-secure.driver
ERROR: Profile missing:
   Profiles/xsp-minimal-firewall.profile
```

此範例中，rules 中所指定的 jordan 設定檔項目並不存在。設定檔 xsp-minimal-firewall.profile 並未存在於設定檔目錄。通常此錯誤的原因是檔案名稱拼字錯誤，忘記指定設定檔的正確目錄，或者尚未建立設定檔。修正這個問題後重新執行檢查。

第二次執行發現兩個問題。第一個問題是要被 xsp-firewall-secure.driver 呼叫的驅動程式。應該要呼叫 xsp-firewall-hardening.driver，但 xsp-firewall-secure.driver 仍然呼叫 hardening.driver。

第二個問題是 JASS_SCRIPTS 變數設定爲不正確的 minimize-Sun_ONE-WS.fin 而非 minimize-firewall.fin。

下面是不正確的程序檔。

程式碼範例 7-6 不正確程序檔範例

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="minimize-Sun_ONE-WS.fin"
. ${DIR}/driver.run
. ${DIR}/hardening.driver
```

下面是正確程序檔的範例。

程式碼範例 7-7 正確程序檔範例

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
minimize-firewall.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

自訂強化配置

預定計畫的防火牆強化配置已經做好自訂及微調的準備。起始的程序檔是根據 `hardening.driver` 作成的。意思是系統成爲「warm-brick」，也就是停用所有的服務。

由於 Solaris 8 作業系統並未內含 Secure Shell 用戶端軟體，您必須作修改來允許防火牆的遠端，網路基礎式管理。對於本個案情境中的防火牆，需求中指定 FTP 服務必須保持啓用狀態以及必須安裝一個 Secure Shell 用戶端作遠端管理。限制上述兩種服務僅在私有管理網路內，因此並未啓用自任何其他網路介面作監聽。要取得有關限制服務的資訊，請參閱 Sun BluePrints OnLine 文摘，標題爲「Solaris Operating Environment Security: Updated for Solaris 9 Operating Environment」。

除了保留啓用上述兩種服務，RPC 服務是啓用的。如此我們可以使用 Solstice DiskSuite 圖形化使用者介面 (GUI) 來配置做爲磁碟鏡射的 Solstice DiskSuite。若沒有打算使用 Solstice DiskSuite GUI，那麼則不需要 RPC。本範例中，GUI 是需要的，所以 RPC 服務需要保留啓用。請注意，Solstice DiskSuite 的安裝及配置已經超出本書的範圍。

用戶端的最後一項必須要做的更改是打造使用 xSP 的 中央 SYSLOG 伺服器，自訂的 `syslog.conf`。此自訂的 `syslog.conf` 檔案必須安裝至每一個防火牆系統。

這些更改需要針對各種不同 Solaris Security Toolkit 配置選項作變更。下面章節顯示每個所需更改的詳細資訊。

- 第 92 頁「啓用 FTP 服務」
- 第 92 頁「安裝 Secure Shell 軟體」
- 第 93 頁「啓用 RPC 服務」
- 第 94 頁「自訂 syslog.conf 檔案」

啓用 FTP 服務

對於本個案的防火牆，保留 FTP 服務啓用。

▼ 啓用 FTP 服務

1. **要保留啓用 FTP，請修改** `update-inetd-conf.fin` **檔案的預設運作方式。設定** `JASS_SVCS_DISABLE` **及** `JASS_SVCS_ENABLE` **變數。**

   要停用除了 FTP 外所有標準的 Solaris 作業系統服務，此個案的最好方法是定義 `JASS_SVCS_ENABLE` 爲 `ftp`，同時確保 `finish.init` 程序檔中的 `JASS_SVCS_DISABLE` 保留爲預設值。請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

2. **要透過環境變數來使更改生效，呼叫** `xsp-firewall-hardening.driver` **之前，新增一個類似下列的項目至** `xsp-firewall-secure.driver`**。**

   ```
   JASS_SVCS_ENABLE="ftp"
   ```

3. **確保 FTP 僅適用在 xSP 的管理網路上，藉由防火牆軟體使它生效。**

   另外一個需求是 FTP 應該僅適用於 xSP 的管理網路。Solaris 8 作業系統上，您可以透過系統上的 TCP 包裝函式或者透過防火牆軟體本身來使此需求生效。本個案中，透過防火牆軟體來使它生效。

安裝 Secure Shell 軟體

由於 Solaris 8 作業系統並未納入 Secure Shell 用戶端，安裝一個作遠端管理的 Secure Shell 用戶端。

您可以配置 Solaris Security Toolkit 軟體來安裝 OpenSSH 工具。使用 `install-openssh.fin` 程序檔，它被列入 `config.driver` 檔案中並由 `xsp-firewall-secure.driver` 所使用。

▼ 安裝 Secure Shell

1. **複製預設** `config.driver` **至** `xsp-firewall-config.driver`**。**
2. **於複製檔案內，爲** `install-openssh.fin` **項目解除註解。**
3. **修改** `xsp-firewall-secure.driver` **中的項目，它呼叫** `config.driver` **來取代呼叫** `xsp-firewall-config.driver`**。**

4. **取得最新版本的 OpenSSH。**

   如同修補程式及作業系統版本，使用最新版本的 OpenSSH。請參閱 OpenSSH 網頁取得最新發行版本的資訊：

   `http://www.openssh.org`

5. **編譯最新的 OpenSSH 套裝模組，正確地爲它命名，然後安裝至 `Packages` 目錄。**

   要取得更多此套裝模組的資訊，請參閱 Sun BluePrints OnLine 文摘，標題爲「Configuring OpenSSH for the Solaris Operating Environment」。

6. **更新 `install-openssh.fin` 程序檔來反映 OpenSSH 套裝模組名稱。**

   可能需要修改 `install-openssh.fin` 程序檔。此程序檔定義 OpenSSH 套裝模組名稱如同下列格式：

   ```
   OBSDssh-3.5p1-sparc-sun4u-5.8.pkg
   ```

   套裝模組名稱後加上版本編號 (`3.5p1`)、架構 (`sparc`)、架構的版本 (`sun4u`)、在哪個作業系統上作編譯 (`5.8`) 以及一個 `pkg` 的後綴。

7. **藉由防火牆軟體確保 SSH 僅適用 xSP 的管理網路。**

   另外一個需求是 Secure Shell 僅適用於 xSP 的管理網路。Solaris 8 作業系統下，您可以結合 TCP 包裝函式至系統或者透過防火牆軟體本身來達成這個需求。本個案中，我們透過防火牆軟體來實現。請注意，此需求也可藉由更改 Secure Shell 伺服器的配置來達成。

啓用 RPC 服務

保留 RPC 服務啓用，如此您可使用需要 RPC 的 SDS 作磁碟鏡射。

此項修改相當容易，原因是結束程序檔 `disable-rpc.fin` 在 Solaris Security Toolkit 執行期間可以用來停用 RPC 服務。

備註：系統的遠端存取 RPC 服務應該清楚的被系統防火牆配置所定義。

▼ 啓用 RPC

- **將 `xsp-firewall-hardening.driver` 中的項目 `disable-rpc.fin` 作成註解。**

  藉由將其改爲註解方式自驅動程式中停用程序檔，而非移除它們。當將 `JASS_SCRIPTS` 中定義的項目改爲註解時要小心，因爲只有某註解值的組合是可以接受的。

下列是包含於 driver.funcs 程序檔的註解，Solaris Security Toolkit 軟體接受爲 JASS_SCRIPTS 定義的註解標記。

```
#Very rudimentary comment handler. This code will only recognize
#comments where a single '#' is placed before the file name
#(separated by white space or not). It then will only skip the
#very next argument.
```

自訂 syslog.conf 檔案

此用戶端所需要作的最後更改是打造使用 xSP 中央 SYSLOG 伺服器的自訂 syslog.conf。此自訂 syslog.conf 檔案必須安裝至每一個防火牆系統。

▼ 自訂 syslog.conf 檔案

1. **複製 xSP 標準 syslog.conf 檔案、重新命名爲 syslog.conf.jordan，然後置於 Files/etc 目錄中。**

   Solaris Security Toolkit 軟體支援數種不同模式複製檔案。此配置的最佳選項是將系統的主機名稱做爲後綴附加至檔案，如此 syslog.conf 檔案只會複製到 jordan，因爲它有唯一的防火牆特定修改。此種情況下，用戶端被稱爲 jordan，因此 Files/etc 中使用的驗證檔案名稱爲 syslog.conf.jordan。重要的是要注意 JASS_FILES 定義必須沒有此後綴。要取得後綴的資訊，請參閱 「*Solaris Security Toolkit 4.1 Reference Manual*」。

2. **若 xSP 標準 syslog.conf 檔案不適用，建立一個自訂 syslog.conf 檔案如下：**

   a. **複製 Solaris Security Toolkit 軟體內含的 syslog.conf 檔案，然後重新命名爲 syslog.conf.jordan，將它放在 Files/etc 目錄。**

   b. **修改 syslog.conf.jordan 來配合 xSP 標準 SYSLOG。**

3. **驗證 /etc/syslog.conf 檔案列入 xsp-firewall-hardening.driver 的 JASS_FILES 定義內。**

依據預設，xsp-firewall-hardening.driver 內修正過的 JASS_FILE 定義如下：

程式碼範例 7-8 已修改過的 xsp-firewall-hardening.driver 輸出範例

```
JASS_FILES="
                    /etc/dt/config/Xaccess
                    /etc/init.d/inetsvc
                    /etc/init.d/nddconfig
                    /etc/init.d/set-tmp-permissions
                    /etc/issue
                    /etc/motd
                    /etc/notrouter
                    /etc/rc2.d/S00set-tmp-permissions
                    /etc/rc2.d/S07set-tmp-permissions
                    /etc/rc2.d/S70nddconfig
                    /etc/syslog.conf
"
```

現在，所有的修改皆已完成。特定應用程式的作業系統安裝，最小化及強化已經自訂完成而且完全自動化。唯一沒有自動化的程序是防火牆軟體及 Solstice DiskSuite 的安裝及配置。雖然可以使用 JumpStart 技術來進行配置，但已超出本書範圍。請參閱 Sun BluePrints 文件 「*JumpStart Technology: Effective Use in the Solaris Operating Environment*」。

安裝用戶端

完成驅動程式的所有修改之後，如本節所述般安裝用戶端。

▼ 安裝用戶端

1. **完成驅動程式的所有修改後，使用 JumpStart 基本架構來安裝用戶端。**

   在用戶端 ok 提示符號下使用下列指令。

```
ok> boot net - install
```

2. **若發生任何錯誤，將錯誤修正並重新安裝作業系統。**

品質保證測試

程序中的最後作業包括確定系統提供的應用程式及服務正確的運作。而且，此作業會驗證安全性設定檔成功地使需要的修改生效。

重要的是此項作業完全完成，以及重新啓動已強化及最小化平台之後，確保偵測到任何不正常及問題後，可迅速的將它修正。此程序可分爲兩個作業：驗證設定檔安裝及驗證應用程式及服務的功能性。

▼ 驗證設定檔安裝

要驗證 Solaris Security Toolkit 軟體正確無誤地安裝安全性設定檔，並且檢閱及評估下列事項。

1. **檢閱安裝日誌檔。**

   此檔案安裝在 `JASS_REPOSITORY/jass-install-log.txt`。

   備註：此日誌檔被使用爲一個可清楚瞭解 Solaris Security Toolkit 軟體曾對系統所作的參考來源。每當系統執行時，會根據執行的開始時間將新的日誌檔儲存於目錄之中。這些檔案以及任何其他在 `JASS_REPOSITORY` 目錄中的檔案，絕對不可以直接更改。

2. **使用稽核選項來評估系統的配置。**

   要取得有關稽核選項的詳細資訊，請參閱第 6 章。此個案中，我們使用目錄中的檔案至用戶端安裝的 Solaris Security Toolkit 軟體。

程式碼範例 7-9 評估安全性配置

```
# ./jass-execute -a xsp-firewall-secure.driver
[NOTE] Executing driver, xsp-firewall-secure.driver
================================================================
===
xsp-firewall-secure.driver: Driver started.
================================================================
===

================================================================
===
Solaris Security Toolkit Version:   4.1.0
[...]
```

若 Solaris Security Toolkit 驗證運作發生任何不一致性，它們會被記錄下來。運行報告的結尾摘要了被發現的不一致數目。此運作的全部輸出位於 JASS_REPOSITORY 目錄中。

▼ 驗證應用程式及服務的功能性

應用程式及服務的驗證程序包括執行完善的測試及接受計畫。此計畫使用系統或應用程式的不同元件來判定它們是否處於適用及工作順序中。若沒有適用的計畫，根據系統使用的方式作合理的測試。目的爲確保強化程序並未影響應用程式或服務執行應有功能的能力。

1. **若您發現系統強化後應用程式及服務的異常，請使用第 2 章中所述的技巧來判定問題的所在。**

   例如，使用 truss 指令。此指令通常被使用來判定應用程式於何時發生困難。一旦知道時間點，問題可被當成目標並可追溯至 Solaris Security Toolkit 軟體所作的更改。

   備註：根據安裝過 Solaris Security Toolkit 軟體的共同經驗，使用本書的方法可以避免大部分的問題。

   ---

2. **以同樣的方式，測試 Check PointFirewall-1 NG 軟體，追溯問體返回至 Solaris Security Toolkit 軟體的修改點，然後修正該問題。**
3. **若套裝模組的最終清單需要修改，請修改設定檔、重新安裝系統，然後重複測試。**

字彙表

本表說明 Solaris Security Toolkit 中的縮寫和首字母縮略。

A

ab2 AnswerBook2

ABI 應用程式二進位介面 (Application Binary Interface)

ARP 位址解析協定 (Address Resolution Protocol)

ASPPP 非同步點對點通訊協定 (Asynchronous Point-to-Point Protocol)

B

BIND Berkeley 網際網路名稱網域 (Berkeley Internet Name Domain)

BSD Berkeley 軟體發行版 (Berkeley Software Distribution)

BSM 基本安全模型 (Basic Security Model) *(Solaris)*

C

CD 光碟

CD-ROM 光碟唯讀記憶體

CDE 共用桌面環境 (Common Desktop Environment)

cp(1) 複製檔案

cron(1M) 時脈常駐程式

D

DHCP 動態主機配置協定 (Dynamic Host Configuration Protocol)

DMI 桌面管理介面 (Desktop Management Interface)

DMTF 分散式管理任務小組 (Distributed Management Task Force)

DNS 網域名稱系統 (Domain Name System)

E

EEPROM 電子抹除式唯讀記憶體

F

FTP 檔案傳輸通訊協定 (File Transfer Protocol)

G

GID 群組識別碼

H

HTTP 超文字傳輸通訊協定 (HyperText Transfer Protocol)

I

ID 識別碼

IETF 網際網路工程工作特別小組 (Internet Engineering Task Force)

INETD 網際網路服務常駐程式

IP 網際網路通訊協定 (Internet Protocol)

ISA 指示集架構

J

JASS JumpStart 架構和安全程序檔 (JumpStart Architecture and Security Script)，*現爲* Solaris Security Toolkit

K

KDC Kerberos 金鑰分發 (Kerberos Key Distribution)

L

LDAP 簡易目錄存取協定 (Lightweight Directory Access Protocol)

`lp`**(1)** 列式印表機 *（提交列印請求）*

M

MAN 管理網路 *（Sun Fire 高階系統內部 I1 網路）*

MD5 訊息摘要 5 演算法

MIP 行動網際網路協定 (Mobile Internet Protocol)

MSP 中階服務處理器

`mv`**(1)** 移動檔案

N

NFS 網路檔案系統 (Network File System)

NG 下一代 (Next Generation)

NIS, NIS+ 網路資訊服務 (Network Information Services)

NSCD 名稱服務快取常駐程式

O

OE 作業環境，*以前 Solaris 中的舊用法*

OEM 原始設備代工製造商 (Original Equipment Manufacturer)

OS 作業系統，*現在 Solaris 中的用法*

P

PAM 可插入認證模組 (Pluggable Authentication Module)

PDF 可攜式文件格式 (Portable Document Format)

PICL 平台資訊和控制程式庫 (Platform Information and Control Library)

PPP 點對點通訊協定 (Point-to-Point Protocol)

PROM 可程式化唯讀記憶體

Q

QA 品質保證

R

RBAC 以角色爲基礎的存取控制

rc run-control *（檔案或程序檔）*

`rlogin`**(1)** 遠端登入

RFC 遠端功能呼叫 (Remote Function Call)

RPC 遠端程序呼叫 (Remote Procedure Call)

`rsh`**(1)** 遠端 shell

S

SA 系統管理員

SC 系統控制器 *（Sun Fire 高階和中階系統）*

`scp`**(1)** 安全複製（遠端檔案複製程式）

SCCS 原始碼控制系統 (Source Code Control System)

SLP 服務位置協定 (Service Location Protocol)

SMA 系統管理代理程式 (System Management Agent)

SMC Solaris 管理主控台 (Solaris Management Console)

SNMP 簡易網路管理協定 (Simple Network Management Protocol)

SP 服務供應商

SPARC 可擴充式處理器架構 (Scalable Processor Architecture)

SPC SunSoft Print Client

SSH Secure Shell *(Solaris)*

SSP 系統服務處理器 *（Sun Enterprise 10000 伺服器）*

`stdio` 標準輸入 / 輸出

Sun ONE Sun 開放式網路環境 (Sun Open Network Environment)，*目前爲* Sun Java System，*之前則爲* iPlanet

T

TCP 傳輸控制通訊協定 (Transmission Control Protocol)

`tftp`**(1)** 簡單檔案傳輸程式

`ttl` 存活時間

U

U.S. 美國 (United States)

UDP 使用者圖解協定 (User Diagram Protocol)

UID 使用者識別碼

UUCP UNIX 到 UNIX 複製 (UNIX-to-UNIX Copy)

V

VOLD 磁碟區管理常駐程式

W

WBEM 以網路爲基礎的企業管理 (Web-based Enterprise Management)

索引

一劃

七劃

八劃

九劃

十劃

十一劃

十二劃

十三劃

十四劃

十五劃

十六劃

二十二劃

二十三劃