Oracle® Solaris 11 安全性準則

文件號碼： E53932-02
2014 年 9 月

ORACLE

目錄

表清單

使用本文件

- **簡介** – 提供 Oracle Solaris 安全功能的簡介，以及使用這些功能來強化及保護已安裝系統與其應用程式的準則。
- **對象** – 開發、部署或評估 Oracle Solaris 11 系統安全性的系統管理員、安全性管理員、應用程式開發人員以及稽核人員。
- **必備知識** – 網站安全需求。

產品文件庫

位於 http://www.oracle.com/pls/topic/lookup?ctx=E56345 的文件庫中包含本產品的最新資訊與已知問題。

取用 Oracle Support

Oracle 客戶可透過 My Oracle Support 取用電子支援。如需相關資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info，如果您在聽力上需要特殊服務，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

意見

如果您對本文件有任何意見，歡迎您至以下網址提供意見：http://www.oracle.com/goto/docfeedback。

♦ ♦ ♦ 第 1 章

1 關於 Oracle Solaris 安全性

Oracle Solaris 是一種非常牢固的最佳企業作業系統，可提供穩固的安全功能。Oracle Solaris 11 擁有最先進的全方位網路安全系統，可控制使用者存取檔案、保護系統資料庫及使用系統資源的方式，以滿足各個層級的安全需求。傳統的作業系統包含既有的安全性弱點，而 Oracle Solaris 11 的彈性卻可讓它滿足從企業伺服器到桌面用戶端的各種安全性目標。Oracle Solaris 經過完整測試，可支援 Oracle 的各種 SPARC 和 x86 系統，以及協力廠商的其他硬體平台。

Oracle Solaris 11.2 的新安全功能

本節提供客戶關於本發行版本中重要之新安全功能的重點資訊。

- 您可以使用新的 `compliance` 指令，評估系統的安全標準規範程度。它能夠評估並報告系統相對於業界標準安全基準 (包括 PCI-DSS) 的規範程度。如需詳細資訊，請參閱「Oracle Solaris 11.2 安全性規範指南 」和 `compliance(1M)` 線上手冊。
- Oracle Solaris 的加密架構功能在 Oracle Solaris 11.1 SRU 5.5 和 Oracle Solaris 11.1 SRU 3 發行版本中的 userland 與核心功能通過 FIPS 140-2 第 1 級認證。
  - 如需經 Oracle FIPS 140 驗證的產品清單，請參閱 Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html)。
  - 如需在您的系統上啟用 FIPS 140 模式 的相關資訊，請參閱「Using a FIPS 140 Enabled System in Oracle Solaris 11.2 」。

- Oracle Solaris 11.1 通過加拿大通用標準計畫 (Canadian Common Criteria Scheme) 認證。請參閱第 26 頁的「Oracle Solaris 11 Common Criteria EAL4+ 認證」。
- 稽核服務可以使用 Oracle Audit Vault 來儲存、審閱以及分析稽核記錄。請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「Using Oracle Audit Vault and Database Firewall for Storage and Analysis of Audit Records」。
- 經過驗證的啟動可保護 Oracle SPARC T5 系列伺服器與 Oracle SPARC T7 系列伺服器的啟動程序免於遭受威脅。如需更多資訊，請參閱「Securing Systems and Attached Devices in Oracle Solaris 11.2 」中的「Using Verified Boot」。
- 對於安裝伺服器、特定用戶端系統、特定安裝服務的所有用戶端以及任何其他 AI 用戶端，可以使用憑證與金鑰保護「自動安裝 (AI)」的安裝作業。安全 AI 可保護 Oracle Solaris 套裝軟體與系統的傳輸安全。請參閱「Installing Oracle Solaris 11.2 Systems 」中的「Increasing Security for Automated Installations」。
- 有可用的新群組安裝套裝軟體 `pkg:/group/system/solaris-minimal-server`。如需群組套裝軟體內容的說明與比較，請參閱「Oracle Solaris 11.2 Package Group Lists 」。
- 您可以使用 AI 安裝 Kerberos 用戶端，讓用戶端在首次啟動時成為經過 Kerberos 加密的系統。請參閱「Installing Oracle Solaris 11.2 Systems 」中的「How to Configure Kerberos Clients Using AI」。
- 在本發行版本中，實體全域區域 (稱為「不可變全域區域」) 和虛擬全域區域 (稱為「Oracle Solaris 核心區域」) 可以是唯讀狀態。不可變全域區域比核心區域稍為強大一些，但二者均無法永久變更系統的硬體或配置。唯讀區域的啟動速度較快，而且也比允許寫入的區域安全。

  不可變全域區域定義了一組稱為信任運算基準 (Trusted Computing Base, TCB) 的特別程序，可以透過稱為「信任的路徑」的受保護登入配置。如需更多資訊，請參閱「Creating and Using Oracle Solaris Zones 」中的第 12 章「Configuring and Administering Immutable Zones」。如需區域配置資源的相關資訊，請參閱「Introduction to Oracle Solaris Zones 」。另請參閱 `mwac(5)` 和 `tpd(5)` 線上手冊。

  Oracle Solaris 核心區域對於部署相容系統十分有用。例如，您可以配置相容系統、建立「整合歸檔」，然後將影像部署為核心區域。如需更多資訊，請參閱 `solaris-kz(5)` 線上手冊、「Creating and Using Oracle Solaris Kernel Zones 」、「Introduction to Oracle Solaris 11.2 Virtualization Environments 」中的「Oracle Solaris Zones Overview」以及「Using Unified Archives for System Recovery and Cloning in Oracle Solaris 11.2 」。
- 使用者權限與程序權限的新功能包括：
  - 以時間為基礎與以位置為基礎的 PAM 服務存取控制
  - RBAC 管理的授權角色 (ARMOR) 預先定義角色
  - 運用權限設定檔強制使用者必須先提供密碼後才能執行授權的動作
  - 用於執行 `ipstat`、`tcpstat`、`snoop` 及 `intrstat` 等診斷指令的「網路可觀察性」和「系統可觀察性」權限設定檔已具備權限，無須以 `root` 身分執行

  如需詳細資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「What's New in Rights in Oracle Solaris 11.2」。

- IKE 版本 2 (IKEv2) 提供最新的 IKE 通訊協定，可自動管理 IPsec 保護之網路封包的金鑰。如需詳細資訊，請參閱「Securing the Network in Oracle Solaris 11.2 」中的「What's New in Network Security in Oracle Solaris 11.2」。
- Oracle Hardware Management Pack (HMP) 提供用於配置及更新韌體的指令行工具。如需在其他 Oracle 硬體產品 (例如網路交換器和網路介面卡) 安全地使用 HMP 的相關資訊，請參閱「Oracle Hardware Management Pack for Oracle Solaris 安全指南 」。

安裝後的 Oracle Solaris 11 安全性

Oracle Solaris 使用「安全的預設設定 (secure by default, SBD)」 安裝。在其他安全功能當中，這項安全設定可保護系統免於遭受入侵，並且可監控登入嘗試。

系統存取權會受到限制和監視

初始使用者和 `root` 角色帳戶 – 初始使用者帳戶可以從主控台登入。此帳戶會被指派 `root` 角色。初始使用者與 `root` 帳號的密碼在安裝時為同一個。

- 登入之後，初始使用者可取得 `root` 角色，以進一步配置系統。取得角色之後，系統會提示使用者變更 `root` 密碼。請注意，任何角色均無法直接登入，包括 `root` 角色。
- 系統會將 `/etc/security/policy.conf` 檔案中的預設值指派給初始使用者。預設值包含基本 Solaris 使用者 (Basic Solaris User) 權限設定檔和主控台使用者 (Console User) 權限設定檔。這些權限設定檔可讓使用者讀取和寫入 CD 或 DVD、在沒有特權的情況下於系統上執行任何指令，以及在主控台停止並重新啟動系統。
- 初始使用者帳戶也會被指派系統管理員權限設定檔。因此，在未取得 `root` 角色的情況下，初始使用者會擁有部分管理權限，例如安裝軟體和管理命名服務的權限。

密碼需求 – 使用者密碼必須至少為 6 個字元的長度，並且至少包含兩個字母字元和一個非字母字元。密碼會使用 `SHA256` 演算法進行雜湊。所有使用者 (包含 `root` 角色) 在變更密碼時，都必須符合這些密碼需求。

有限的網路存取 – 在安裝之後，系統會受保護，以避免經由網路的入侵威脅。初始使用者可以使用 `ssh` 通訊協定，經由認證和加密的連線進行遠端登入。這是唯一接受內送封包的網路通訊協定。`ssh` 金鑰會使用 `AES128` 演算法進行包裝。有了加密與認證機制，使用者可以放心地連線遠端系統，無須擔心會有資料遭到攔截、修改或詐騙的風險。

記錄的登入嘗試 – 系統會對所有 `login/logout` 事件 (登入、登出、切換使用者、啟動及停止 `ssh` 階段作業以及螢幕鎖定) 與所有無法歸類 (失敗) 的登入啟用稽核服務。由於 `root` 角色無法登入，因此會在稽核記錄中記錄具有 `root` 身分之使用者的名稱。初始使用者可以透過系統管理員權限設定檔授予的權限來審閱稽核記錄。

具備核心、檔案及桌面保護

初始使用者登入之後，核心、檔案系統、系統檔案以及桌面應用程式都會受到檔案權限、特權以及使用者權限的保護。使用者權限亦稱為以角色為基礎的存取控制 (RBAC)。

核心保護 – 許多常駐程式和管理指令只會被指派讓它們可以成功執行的特權。許多常駐程式是從不具備 `root` (`UID=0`) 特權的特殊管理帳戶執行，因此無法加以奪取以執行其他作業。這些特殊的管理帳戶無法登入。裝置受特權保護。

檔案系統 – 依照預設，所有檔案系統均為 ZFS 檔案系統。使用者的 `umask` 為 `022`，如此若使用者建立新的檔案或目錄，只有該使用者能夠修改。該使用者群組的成員可以讀取並搜尋目錄，以及讀取檔案。使用者群組以外的登入可以列示目錄和讀取檔案。預設的目錄權限為 `drwxr-xr-x` (`755`)。檔案權限為 `-rw-r--r--` (`644`)。

系統檔案 – 系統配置檔案由檔案權限保護。唯有 `root` 角色或具備編輯特定系統檔案之權限的使用者，才能夠修改系統檔案。

桌面 Applet – 桌面 Applet 由權限管理保護。因此，像是在「列印管理員」中新增遠端印表機這類的管理動作，只有具備列印管理權限的使用者和角色能夠執行。

Oracle 硬體管理套裝軟體

Oracle 硬體管理套裝軟體 提供一組供用於配置、管理以及監控 Oracle 伺服器的公用程式。一律提供專用於 Oracle 硬體的加值工具組。它可以自動將某些硬體相關資訊傳遞給 ILOM，以完成其對系統硬體的檢視。如需公用程式與安全性的相關資訊，請參閱 Systems Management and Diagnostics Documentation (http://www.oracle.com/goto/ohmp/docs)。

Oracle Solaris 可配置安全性

除了 Oracle Solaris 安全性預設值提供的穩固基礎之外，Oracle Solaris 系統的安全性設定也具有高度的可配置性，以滿足不同的安全需求。

下列各節提供 Oracle Solaris 安全功能的簡介。描述中包含更詳盡說明的參考資料，以及本指南和示範這些功能之其他 Oracle Solaris 系統管理指南中的程序參考資料。

保護資料

Oracle Solaris 從啟動到安裝、使用以及歸檔，都會持續保護資料。

檔案權限和存取控制項目

檔案系統中用來保護物件的第一道防線，是指派給每個檔案系統物件的預設 UNIX 權限。UNIX 權限支援將唯一存取權指派給物件的擁有者、已指派給物件的群組以及其他的任何人。此外，預設的檔案系統 (即 ZFS) 也支援存取控制清單 (ACL)，可以更精細地控制個別或群組的檔案系統物件存取。

如需更多資訊，請參閱：

- 如需檔案權限的簡介，請參閱「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「Using UNIX Permissions to Protect Files」。
- 如需保護 ZFS 檔案的簡介與範例，請參閱「Managing ZFS File Systems in Oracle Solaris 11.2 」中的第 7 章「Using ACLs and Attributes to Protect Oracle Solaris ZFS Files」和線上手冊。
- 如需設定 ZFS 檔案之 ACL 的相關說明，請參閱 `chmod(1)` 線上手冊。

加密服務

Oracle Solaris 的加密架構功能和 Oracle Solaris 的金鑰管理架構 (KMF) 功能，為加密服務與金鑰管理提供中央儲存庫。硬體、軟體及一般使用者可以無縫存取最佳化演算法。KMF 為各種公開金鑰基礎架構 (KPI) 提供了不同儲存機制、管理公用程式以及程式設計介面的統一介面。

「加密架構」提供儲存通用演算法和 PKCS #11 程式庫，以處理加密的需求。PKCS #11 程式庫根據 RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) 標準實作。加密服務 (例如檔案的加密與解密) 可供一般使用者使用。

KMF 為集中管理公開金鑰物件 (例如 X.509 憑證和公開/私密金鑰對) 提供工具與程式設計介面。儲存這些物件的格式可能會不同。KMF 也提供管理策略的工具，以定義應用程式使用 X.509 憑證的方式。KMF 支援協力廠商外掛程式。

如需更多資訊，請參閱：

- 相關線上手冊：包括 `cryptoadm(1M)`、`encrypt(1)`、`mac(1)`、`pktool(1)` 以及 `kmfcfg(1)`。
- 如需加密服務的簡介，請參閱「Managing Encryption and Certificates in Oracle Solaris 11.2 」中的第 1 章「Cryptographic Framework」和「Managing Encryption and Certificates in Oracle Solaris 11.2 」中的第 4 章「Key Management Framework」。
- 如需使用加密架構的範例，請參閱「Managing Encryption and Certificates in Oracle Solaris 11.2 」中的第 3 章「Cryptographic Framework」和線上手冊。
- 若要啟用加密架構 FIPS 140 提供者，請參閱「Managing Encryption and Certificates in Oracle Solaris 11.2 」中的「How to Create a Boot Environment with FIPS 140 Enabled」。

Oracle Solaris ZFS 檔案系統

ZFS 是 Oracle Solaris 11 的預設檔案系統。ZFS 檔案系統基本上變更了管理 Oracle Solaris 檔案系統的方式。ZFS 是牢固、可擴充且易於管理的系統。由於在 ZFS 中建立檔案系統非常簡易，您可以輕鬆建立配額和保留的空間。UNIX 權限與 ACL 會保護檔案，您可於建立資料集時將整個資料集加密。Oracle Solaris 權限管理支援委任管理 ZFS 資料集，亦即具備有限之一組權限的使用者可以管理 ZFS 資料集。

如需更多資訊，請參閱：

- 「Securing Users and Processes in Oracle Solaris 11.2 」中的「User Rights Management」
- 「Managing ZFS File Systems in Oracle Solaris 11.2 」中的第 1 章「Oracle Solaris ZFS File System (Introduction)」
- 「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Oracle Solaris ZFS and Traditional File System Differences」
- 「Managing ZFS File Systems in Oracle Solaris 11.2 」中的第 5 章「Managing Oracle Solaris ZFS File Systems」
- 「Managing Secure Shell Access in Oracle Solaris 11.2 」中的「How to Remotely Administer ZFS With Secure Shell」
- 相關線上手冊：包括 `zfs(1M)` 和 `zfs(7FS)`。

Java Cryptography Extension

Java 為 Java 應用程式開發人員提供了 Java Cryptography Extension (JCE)。如需更多資訊，請參閱 Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html)。

保護及隔離應用程式

應用程式有可能成為惡意軟體和惡意使用者的進入點。在 Oracle Solaris 中，這些威脅可藉由使用權限與控制區域內的應用程式來降低。僅以應用程式所需的權限執行應用程式，讓惡意使用者沒有 root 特權可存取系統的其他部分。區域可以限制攻擊的範圍。攻擊非全域區域中的應用程式只會影響該區域中的程序，而非該區域的主機系統。

位址空間配置隨機化 (ASLR) 和服務管理功能 (SMF) 是保護應用程式的額外功能。ASLR 讓侵入者難以奪取可執行檔，SMF 功能則讓管理員能夠限制對應用程式的啟動、停止以及使用。

Oracle Solaris 中的特權

特權指的是在核心中對程序強制的細部、特定權限。Oracle Solaris 定義了 80 種以上的特權，範圍涵蓋從基本特權 (像是 `file_read`) 到更具體的特權 (像是 `proc_clock_highres`)。特權可授予程序、使用者或角色。許多 Oracle Solaris 指令和常駐程式只會以執行其作業所需的特權來執行。特權感知的程式可防止侵入者取得超過程式本身所用的特權。

特權的使用也稱為程序權限管理。特權也可讓組織指定進而限制要將哪些特權授予在其系統上執行的服務和程序。

如需更多資訊，請參閱：

- 「Securing Users and Processes in Oracle Solaris 11.2 」中的「Process Rights Management」
- 「Developer's Guide to Oracle Solaris 11 Security 」中的第 2 章「Developing Privileged Applications」
- 相關線上手冊：包括 `ppriv(1)` 和 `privileges(5)`。

Oracle Solaris Zones

Oracle Solaris Zones 軟體分割技術可讓您維護每個伺服器一個應用程式的部署模型，同時共用硬體資源。

Zones 是虛擬的作業環境，可讓多個應用程式在相同的實體硬體上以隔離的方式個別執行。此隔離技術可避免監視一個區域中執行的程序或影響在其他區域執行的程序、檢視彼此的資料，或是操控基礎的硬體。Zones 也可提供抽象層，以分隔應用程式和部署應用程式之系統的實體屬性，例如實體裝置路徑和網路介面名稱。

在 Oracle Solaris 11.2 中，您可以配置不可變的根檔案系統。

如需更多資訊，請參閱：

- 「Creating and Using Oracle Solaris Zones 」中的「Configuring Read-Only Zones」
- 「Introduction to Oracle Solaris Zones 」
- 相關線上手冊：包括 `brands(5)`、`zoneadm(1M)` 以及 `zonecfg(1M)`。

位址空間配置隨機化

位址空間配置隨機化 (ASLR) 會隨機挑選指定之程式使用的位址。ASLR 可以防止因為知道某些記憶體範圍的確切位置而發動的攻擊類型，並且可偵測可能停止程式的嘗試。如需更多資訊，請參閱「Securing Systems and Attached Devices in Oracle Solaris

11.2 」中的「Address Space Layout Randomization」和第 31 頁的「如何驗證 ASLR 是否啟用」。

服務管理功能

服務指的是持續不斷執行的應用程式。服務可以代表執行中的應用程式、裝置的軟體狀態或一組其他服務。Oracle Solaris 的服務管理設備 (SMF) 功能是用來新增、移除、設定和管理服務。SMF 使用權限管理來控制系統上服務管理功能的存取。特別是 SMF 會使用授權來決定誰可以管理服務，以及該人員可以執行的功能。

SMF 可讓組織控制對服務的存取，以及控制如何啟動、停止和重新整理那些服務。

如需更多資訊，請參閱：

- 「Managing System Services in Oracle Solaris 11.2 」
- 「Securing Users and Processes in Oracle Solaris 11.2 」中的「How to Assign Specific Privileges to the Apache Web Server」
- 相關線上手冊：包括 `svcadm(1M)`、`svcs(1)` 以及 `smf(5)`。

保護使用者與指派其他權限

使用者具有 `/etc/security/policy.conf` 檔案中的一組基本權限、權限設定檔以及授權，類似第 13 頁的「系統存取權會受到限制和監視」中所述的初始使用者。這些是可配置的權限。您可以拒絕基本權限，以及增加使用者權限。

Oracle Solaris 保護使用者的方法包括具有彈性的密碼複雜度需求，可針對不同網站需求而配置的認證，以及使用權限設定檔、授權和特權來限制及分發管理權限給信任使用者的使用者權限管理。此外，特殊的共用帳號 (稱為角色)，也只授予使用者所具備之角色的管理權限。Authorization Rules Managed On RBAC (ARMOR) 套裝軟體提供預先定義的角色。

密碼和密碼限制

增強式使用者密碼有助於防禦和暴力密碼破解相關的攻擊。

Oracle Solaris 具有許多可供您根據網站需求配置使用者密碼的功能。您可以指定密碼長度、內容、變更頻率與修改需求，以及保留密碼歷程記錄。系統提供有應避免使用之密碼的字典。另外，也提供數種可使用的密碼雜湊演算法。預設使用 SHA256。

如需更多資訊，請參閱：

- 「Securing Systems and Attached Devices in Oracle Solaris 11.2 」中的「Maintaining Login Control」

- 「Securing Systems and Attached Devices in Oracle Solaris 11.2 」中的「Securing Logins and Passwords」
- 相關線上手冊：包括 passwd(1) 和 crypt.conf(4)。

可插接式驗證模組

可插接式驗證模組 (PAM) 架構讓管理員無須修改需要驗證的服務，即可協調及配置帳號、認證、階段作業以及密碼的使用者驗證需求。

PAM 架構可讓組織自訂使用者認證體驗，以及帳戶、階段作業和密碼管理功能。系統進入服務 (例如 login 和 ssh) 使用 PAM 架構來保護新安裝之系統的所有進入點。PAM 可取代或修改領域中的驗證模組，無須變更使用 PAM 架構的任何系統服務，即可保護系統不受新發現之弱點的影響。

Oracle Solaris 提供涵蓋範圍甚廣的 PAM 模組和配置組合，可符合大多數的網站策略需求。如需更多資訊，請參閱：

- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」中的第 1 章「Using Pluggable Authentication Modules」
- 「Developer's Guide to Oracle Solaris 11 Security 」中的「Writing Applications That Use PAM Services」
- pam.conf(4) 線上手冊

使用者權限管理

Oracle Solaris 中的使用者權限由最低特權的安全性原則管理。組織可依據其獨特的需要與需求，選擇性地授予使用者或角色管理權限。同時也可拒絕使用者所要求的權限。權限可實作為程序的特權與使用者的授權，或是 SMF 方法。權限設定檔提供了將特權與授權收集成一個相關權限組合的便利方式。

如需更多資訊，請參閱：

- 「Securing Users and Processes in Oracle Solaris 11.2 」
- 相關線上手冊：包括 auths(1)、privileges(5)、profiles(1)、rbac(5)、roleadd(1M)、roles(1) 以及 user_attr(4)。

保護網路通訊安全

保護網路的通訊安全有數種方式，例如防火牆、網路應用程式的 TCP 包裝程式，以及加密和認證的遠端連線。

封包篩選

封包篩選可針對網路攻擊提供基本的保護。Oracle Solaris 包含 IP 篩選器功能和 TCP 包裝程式。

防火牆

Oracle Solaris 的 IP 篩選器功能會建立防火牆以避開網路攻擊。

尤其 IP 篩選器可以提供有狀態的封包篩選功能，可依據 IP 位址或網路、連接埠、通訊協定、網路介面及流量方向來篩選封包。IP 篩選也含有無狀態的封包篩選功能，以及建立與管理位址集區的能力。此外，IP 篩選器也具備執行網路位址轉譯 (NAT) 和連接埠位址轉譯 (PAT) 的能力。

如需更多資訊，請參閱：

- 如需 IP 篩選器的簡介，請參閱「Securing the Network in Oracle Solaris 11.2 」中的第 4 章「About IP Filter in Oracle Solaris」。
- 如需使用 IP 篩選器的範例，請參閱「Securing the Network in Oracle Solaris 11.2 」中的第 5 章「Configuring IP Filter」和線上手冊。
- 如需 IP 篩選器策略語言之語法的相關資訊與範例，請參閱 `ipnat(4)` 線上手冊。
- 相關線上手冊：包括 `ipfilter(5)`、`ipf(1M)`、`ipnat(1M)`、`svc.ipfd(1M)` 以及 `ipf(4)`。

TCP 包裝程式

TCP 包裝程式提供網際網路服務的存取控制。當各種網際網路 (`inetd`) 服務啟用之後，`tcpd` 常駐程式會依據 ACL 檢查要求特定網路服務的主機位址。接著會接受或拒絕要求。TCP 包裝程式也會在 `syslog` 中記錄網路服務的主機要求，這是很實用的監控功能。

Secure Shell (`ssh`) 和 Oracle Solaris 的 `sendmail` 功能配置為使用 TCP 包裝程式。與可執行檔案為一對一對應關係的網路服務 (例如 `proftpd` 和 `rpcbind`)，可以使用 TCP 包裝程式。

TCP 包裝程式支援豐富的配置策略語言，不僅可讓組織指定全域的安全策略，還可指定以每個服務為基礎的安全策略。並可依據主機名稱、IPv4 或 IPv6 位址、網路群組名稱、網路甚至是 DNS 網域，來允許或限制對服務的進一步存取。

如需 TCP 包裝程式的相關資訊，請參閱：

- 第 44 頁的「如何使用 TCP 包裝程式」

- 如需 TCP 包裝程式之存取控制語言的語法資訊和範例，請參閱 `hosts_access`(4) 線上手冊。
- 相關線上手冊：包括 `tcpd`(1M) 和 `inetd`(1M)。

遠端存取

遠端存取攻擊可能會損害系統和網路。Oracle Solaris 為網路傳輸提供了全面的防禦。防禦功能包括針對資料傳輸進行加密和認證檢查、登入認證、停用不必要的遠端服務。

IPsec 和 IKE

IP 安全性 (IPsec) 會透過認證 IP 封包、加密 IP 封包或同時執行二者來保護網路傳輸。由於 IPsec 是在應用程式層底下實作，因此網際網路應用程式不需修改其程式碼即可使用 IPsec。

IPsec 與其自動金鑰交換通訊協定 (IKE) 都使用加密架構中的演算法。此外，「加密架構」也提供中央金鑰庫。如果 IKE 配置為使用 metaslot，組織可以選擇將金鑰儲存在磁碟、連附的硬體金鑰庫或稱為 *softtoken* 的軟體金鑰庫中。

IPsec 和 IKE 均需配置，因此預設為安裝但未啟用。如果正確地管理，IPsec 會是保護網路流量的有效工具。

如需更多資訊，請參閱：

- 「Securing the Network in Oracle Solaris 11.2 」中的第 6 章「About IP Security Architecture」
- 「Securing the Network in Oracle Solaris 11.2 」中的第 7 章「Configuring IPsec」
- 「Securing the Network in Oracle Solaris 11.2 」中的「IPsec and FIPS 140」
- 「Securing the Network in Oracle Solaris 11.2 」中的第 8 章「About Internet Key Exchange」
- 「Securing the Network in Oracle Solaris 11.2 」中的第 9 章「Configuring IKEv2」
- 相關線上手冊：包括 `ipsecconf`(1M) 和 `in.iked`(1M)。

Secure Shell

依照預設，Oracle Solaris 的 Secure Shell 功能是新安裝系統之唯一使用中的遠端存取機制。所有其他網路服務均為停用中狀態或僅監聽模式。

Secure Shell 會建立系統之間的加密通訊通道。Secure Shell 也可作為依需求指定的虛擬私有網路 (VPN)，可以轉送 X Window 系統流量，或者可經由認證且加密的網路連結來連線本機系統與遠端系統之間的個別連接埠號碼。

因此，Secure Shell 可防止可能的侵入者讀取遭到攔截的通訊，並能防止惡意使用者詐騙系統。

如需更多資訊，請參閱：

- 「Managing Secure Shell Access in Oracle Solaris 11.2 」中的第 1 章「Using Secure Shell (Tasks)」
- 「Managing Secure Shell Access in Oracle Solaris 11.2 」中的「Secure Shell and FIPS 140」
- 相關線上手冊：包括 ssh(1)、sshd(1M)、sshd_config(4) 以及 ssh_config(4)。

Kerberos 服務

Oracle Solaris 的 Kerberos 功能讓系統為執行不同作業系統且執行 Kerberos 服務的異質網路，也能夠啟用單一登入和安全作業事件。

Kerberos 是以在麻省理工學院 (MIT) 開發的 Kerberos V5 網路認證通訊協定為基礎。Kerberos 服務提供增強式使用者認證，以及整合性與私密性。使用 Kerberos 服務時，只要登入一次，您就能存取其他系統、執行指令、交換資料以及安全地傳輸檔案。此外，管理員也可以使用此服務來限制對服務和系統的存取。

如需更多資訊，請參閱：

- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」
- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」中的「FIPS 140 Algorithms and Kerberos Encryption Types」
- 相關線上手冊：包括 kadmin(1M)、kdcmgr(1M)、kerberos(5)、kinit(1) 以及 krb5.conf(4)。

維護系統安全

Oracle Solaris 提供下列維護系統安全的功能：

- 經過驗證的啟動 – 保護啟動程序的安全。預設停用經過驗證的啟動。
- 套裝軟體驗證 – 確認安裝的套裝軟體與來源儲存庫中的套裝軟體相同。
- 稽核服務 – 稽核系統的存取與使用。預設啟用稽核功能。
- 檔案完整性驗證 – BART 清單可列出系統上的每個檔案，然後使用清單比較來驗證是否維持檔案完整性。
- 記錄檔 – SMF 提供每項服務的記錄檔。syslog 公用程式提供了一個可用於命名及配置系統服務記錄的中央檔案，並且可選擇性地向管理員通報重要事件。其他功能 (例如稽核) 也會建立自己的記錄。
- 規範報告 – Oracle Solaris 提供數種評估系統的安全基準。這些評估項目會產生報告，幫助您評估系統的安全性狀態。

經過驗證的啟動

經過驗證的啟動是一項 Oracle Solaris 功能，可保護系統的啟動程序安全。這項功能可保護系統免於遭受像安裝未授權之核心模組和木馬程式的威脅。預設會停用經過驗證的啟動。

如需更多資訊，請參閱「Securing Systems and Attached Devices in Oracle Solaris 11.2 」中的第 2 章「Protecting Oracle Solaris Systems Integrity」。

套裝軟體完整性驗證

安裝或更新套裝軟體之後，您可以執行 `pkg verify` 指令，確認系統上的套裝軟體與來源儲存庫中的套裝軟體相同。

如需更多資訊，請參閱 pkg(1) 線上手冊和第 30 頁的「如何驗證套裝軟體」。

稽核服務

Oracle Solaris 提供收集系統存取與使用資料的稽核服務。稽核資料提供可靠之安全性相關系統事件的時間戳記記錄。此資料可接著用來為系統上發生的動作指派職責。

稽核是安全性評估、驗證、規範以及憑證主體的基本需求。稽核也有助於遏止潛在的侵入者。

如需更多資訊，請參閱：

- 如需稽核相關線上手冊的清單，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的第 7 章「Auditing Reference」。
- 如需相關準則，請參閱第 40 頁的「如何稽核登入/登出以外的重大事件」和線上手冊。
- 如需稽核的簡介，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的第 1 章「About Auditing in Oracle Solaris」。
- 如需稽核作業的相關資訊，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的第 3 章「Managing the Audit Service」。

檔案完整性驗證

Oracle Solaris 的 BART 功能可對系統執行長期的檔案層級檢查，讓您可以全面地驗證系統。完成安裝之後，`pkg verify` 指令可確認來源套裝軟體內容與目的地套裝軟體內容是否相同。套裝軟體驗證之後，您可以使用 BART 清單，輕鬆且可靠地收集系統上檔案的相關資訊。

BART 是管理系統或系統網路之完整性的實用工具。系統的檔案可與系統的原始檔案和其他系統的檔案做比較。可由報告得知系統尚未經過修補、侵入者安裝了未經允許的檔案，或者侵入者變更了機密檔案 (例如 root 擁有的檔案) 的權限或內容。

如需更多資訊，請參閱：

- 如需相關準則，請參閱第 51 頁的「使用 BART 驗證檔案完整性」、第 51 頁的「使用 BART 驗證檔案完整性」和線上手冊。
- 如需 BART 的簡介，請參閱「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的第 2 章「Verifying File Integrity by Using BART」。
- 如需使用 BART 的範例，請參閱「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「About Using BART」和線上手冊。
- 相關線上手冊：包括 bart(1M)、bart_rules(4) 以及 bart_manifest(4)。

記錄檔

Oracle Solaris 的「服務管理功能 (SMF)」功能會記錄其每項服務的狀態。許多服務 (例如稽核和 Secure Shell) 都會寫入自己的記錄。syslog 或 rsyslog 常駐程式寫入一個集中的記錄，可向管理員通報並警告許多服務中的嚴重情況。舉例來說，可以配置讓稽核將摘要稽核記錄寫入 syslog。請參閱 syslogd(1M) 和 syslog.conf(4) 線上手冊。

安全性標準規範

compliance assess 指令可提供系統之安全性狀態的快照。評估項目所產生的報告會根據業界安全性基準，提出需要對系統進行的特定變更。如需更多資訊，請參閱「Oracle Solaris 11.2 安全性規範指南 」和 compliance(1M) 線上手冊。

標籤式安全性

Oracle Solaris 中的標籤式安全性由 Trusted Extensions 功能提供。

Oracle Solaris 中的 Trusted Extensions 功能

Oracle Solaris 的 Trusted Extensions 功能是選擇性啟用的安全標籤技術層，可以分隔資料安全策略和資料所有權。Trusted Extensions 支援以所有權為基礎的傳統任意存取控制 (DAC) 策略，以及以標籤為基礎的必要存取控制 (MAC) 策略。除非啟用 Trusted Extensions 層，否則所有標籤都是相等的，如此核心才不會配置為強制執行 MAC 策

略。啟用以標籤為基礎的 MAC 策略時，會比較要求存取的程序 (主體) 和包含資料之物件相關聯的標籤，以限制所有資料流程。

Trusted Extensions 實作的獨特性在於提供高度保證，同時將相容性最大化及將負荷最小化。Trusted Extensions 屬於第 26 頁的「Oracle Solaris 11 Common Criteria EAL4+ 認證」的一部分。

Trusted Extensions 符合 Common Criteria Labeled Security Package (LSP) 的需求。請參閱第 26 頁的「Oracle Solaris 11 Common Criteria EAL4+ 認證」。

如需更多資訊，請參閱：

- 如需配置及維護 Trusted Extensions 的相關資訊，請參閱「Trusted Extensions Configuration and Administration 」。
- 相關線上手冊：包括 `trusted_extensions(5)`、`labeladm(1M)` 以及 `labeld(1M)`。

標籤式檔案系統

依照預設，檔案系統 (標籤相同者) 在區域中會有一個指派的單一標籤。您可以建立多層級的 ZFS 資料集並將其掛載至 Trusted Extensions 系統，若有適當權限，還可升級或降級該資料集中的檔案。如需更多資訊，請參閱「Trusted Extensions Configuration and Administration 」中的「Multilevel Datasets for Relabeling Files」。

標籤式網路通訊

Trusted Extensions 會標記網路通訊。系統會根據比較起始網路端點之標籤與接收網路端點之標籤的結果來限制資料流程。必須同時標記閘道器和之間的躍點，才能傳送通訊之標籤的資訊。NFS 和多層級 ZFS 資料集都提供網路的其他功能。

如需更多資訊，請參閱：

- 「Trusted Extensions Configuration and Administration 」中的「Configuring the Network Interfaces in Trusted Extensions」
- 「Trusted Extensions Configuration and Administration 」中的第 15 章「Trusted Networking」
- 「Trusted Extensions Configuration and Administration 」中的第 16 章「Managing Networks in Trusted Extensions」

Trusted Extensions 多層級桌面

與大多數的其他多層級作業系統不同，Trusted Extensions 包含多層級桌面。可以配置讓使用者只見到允許的標籤。可以將每個標籤配置為需要提供個別的密碼。

如需更多資訊，請參閱「Trusted Extensions User's Guide 」。若要配置使用者，請參閱「Trusted Extensions Configuration and Administration 」中的第 11 章「Managing Users, Rights, and Roles in Trusted Extensions」。

Oracle Solaris 11 Common Criteria EAL4+ 認證

Oracle Solaris 11 通過加拿大通用標準計畫的評估保證等級第四級 (Evaluation Assurance Level 4, EAL4) 的認證，並增加了缺點修補 (EAL4+)。EAL4 是獲得 26 個國家承認的共同標準承認協定 (Common Criteria Recognition Arrangement, CCRA) 中最高的評估等級。

這是針對作業系統保護規範 (Operating System Protection Profile, OSPP) 的認證，包含下列的延伸規範：

- 進階管理
- 擴充身分識別與認證
- 標籤式安全性
- 虛擬化

如需認證的相關資訊，請參閱：

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

網站安全策略和做法

如果要有安全的系統或系統網路，您的網站必須具備安全策略，以及支援策略的安全做法。若您正在開發程式或安裝協力廠商程式，您必須安全地開發和安裝那些程式。

如需更多資訊，請參閱以下內容：

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- 「Developer's Guide to Oracle Solaris 11 Security 」中的附錄 A「Secure Coding Guidelines for Developers」
- 「Trusted Extensions Configuration and Administration 」中的附錄 A「Site Security Policy」
- 「Trusted Extensions Configuration and Administration 」中的「Security Requirements Enforcement」

- Keeping Your Code Secure (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ 第 2 章

2 配置 Oracle Solaris 安全性

本章說明設定系統安全性需採取的動作。本章內容涵蓋安裝套裝軟體、設定系統本身，然後設定各種您可能需要的子系統和其他應用程式，例如 IPsec。

安裝 Oracle Solaris OS

Oracle Solaris OS 主要透過從套裝軟體儲存庫選取一組稱之為群組的套裝軟體方式安裝。不同群組所提供的套裝軟體分別支援不同的用途，例如多用途伺服器、最小安裝系統以及桌面系統。套裝軟體均經過簽署，其安全傳輸可加以驗證。

安裝 Oracle Solaris OS 時，請選擇安裝適當群組套裝軟體的媒體，如下所述：

- **Oracle Solaris 大型伺服器** –「自動安裝程式 (AI)」安裝中的預設清單和文字安裝程式均會安裝 `group/system/solaris-large-server` 群組，以提供 Oracle Solaris 大型伺服器環境。
- **Oracle Solaris 小型伺服器** –「自動安裝程式 (AI)」和文字安裝程式會選擇性地安裝 `group/system/solaris-small-server` 群組，以提供有用的指令行環境供您新增套裝軟體。
- **Oracle Solaris 最小型伺服器** –「自動安裝程式 (AI)」和文字安裝程式會選擇性地安裝 `group/system/solaris-minimal-server` 群組，以提供最小型的指令行環境供您新增想要安裝的套裝軟體。
- **Oracle Solaris 桌面** – Live Media 會安裝 `group/system/solaris-desktop` 群組，以提供 Oracle Solaris 11 桌面環境。

若要建立用於集中使用的桌面系統，請將 `group/feature/multi-user-desktop` 群組加到桌面伺服器。如需更多資訊，請參閱「Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment」文章。

如需使用「自動安裝程式 (AI)」執行自動安裝的資訊，請參閱「Installing Oracle Solaris 11.2 Systems」中的第 III部分「Installing Using an Install Server」。

如需引導您選擇媒體，請參閱下列安裝與套裝軟體內容指南：

- 「Installing Oracle Solaris 11.2 Systems」
- 「Creating a Custom Oracle Solaris 11.2 Installation Image」
- 「Adding and Updating Software in Oracle Solaris 11.2」
- 「Oracle Solaris 11.2 Package Group Lists」

最初的系統保護

最好依序執行下列作業。此時，Oracle Solaris 已經安裝好，只有具備 `root` 角色的初始使用者可以存取系統。

表 2-1 系統保護作業說明

作業	說明	相關說明
1. 驗證系統上的套裝軟體。	確認安裝來源的套裝軟體與已安裝的套裝軟體相同。	第 30 頁的「如何驗證套裝軟體」
2. 確認可執行檔受到保護。	確定 ASLR 已經啟用。	第 31 頁的「如何驗證 ASLR 是否啟用」
3. 保護系統的硬碟設定。	變更硬體設定時需要提供密碼，以保護硬體。在 x86 上，存取 GRUB 功能表由系統控制。在 SPARC 上，由 `eeprom` 指令保護硬體。	「Securing Systems and Attached Devices in Oracle Solaris 11.2」中的「Controlling Access to System Hardware」
3. 停用不需要的服務。	避免執行不屬於系統必要功能的處理程序。	第 32 頁的「如何停用不需要的服務」
5. 避免工作站所有者中斷系統的電源。	避免主控台使用者關閉或暫停系統。	第 32 頁的「如何移除使用者的電源管理能力」
6. 建立反映您網站之安全策略的登入警告訊息。	在認證前後通知使用者系統受到監控。	第 33 頁的「如何將安全訊息放置在標題檔案中」 第 34 頁的「如何將安全訊息放置在桌面登入畫面上」

▼ 如何驗證套裝軟體

安裝後會立即驗證套裝軟體以驗證安裝。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 審閱安裝記錄。
2. 執行 **pkg verify** 指令。
   若要保留記錄，可將指令輸出傳送至檔案。

   ```
   # pkg verify > /var/pkgverifylog
   ```

3. 審閱有任何錯誤的記錄。
4. 如果您找到錯誤，請從媒體重新安裝或修正錯誤。

另請參閱 如需更多資訊，請參閱 pkg(1) 線上手冊和 pkg(5) 線上手冊。這些線上手冊包含使用 pkg verify 指令的範例。

▼ 如何驗證 ASLR 是否啟用

標記的可執行指令預設會寫入未連線的位址空間，以降低侵入者在可執行堆疊插入指令的能力。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 確定 ASLR 已經啟用。

   ```
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (all)           enabled (all)
   ```

   all 值的強度大於預設值，但是可能會導致需要使用記憶體中連續堆疊的應用程式發生錯誤。例如，資料庫可能需要使用記憶體中的連續堆疊。

2. 如果 ASLR 停用，請啟用預設值並確認其為作用中。

   ```
   # sxadm delcust aslr
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (tagged-files)  system default (default)
   ```

另請參閱 若要進行除錯，您可以在某個特定的二進位檔呼叫 sxadm 指令將 ASLR 關閉。如需範例，請參閱 sxadm(1M) 線上手冊。

▼ 如何停用不需要的服務

請使用此程序停用系統上不需要的服務。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 列出線上網路服務。

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server:default
...
online         Sep_07   svc:/network/ssh:default
```

2. 停用此系統不需要的服務。
例如，假設系統並不是 NFS 伺服器或 Web 伺服器，但其服務為線上狀態，請將它們停用。

```
# svcadm disable svc:/network/nfs/server:default
# svcadm disable svc:/network/http:apache22
```

另請參閱 如需更多資訊，請參閱「Managing System Services in Oracle Solaris 11.2 」中的第 1 章「Introduction to the Service Management Facility」 和 svcs(1) 線上手冊。

▼ 如何移除使用者的電源管理能力

此程序可讓系統主控台的使用者不能暫停系統或中斷系統的電源。如果主控台使用者能夠拔除系統硬體，此軟體解決方案即無作用。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 審閱主控台使用者 (Console User) 權限設定檔的內容。

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 help=RtConsUser.html
```

2. 建立權限設定檔，其中包含您要使用者保留的任何主控台使用者 (Console User) 設定檔權限。

如需相關說明，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「How to Create a Rights Profile」。

3. 在 **/etc/security/policy.conf** 檔案中註釋主控台使用者權限設定檔。

```
#CONSOLE_USER=Console User
```

4. 指派您在步驟 2 所建立的權限設定檔。

   - 若是多位使用者共用一個權限設定檔的情況，可在權限設定檔中設定這個值，作為具備可擴充性的解決方案。

     ```
     # usermod -P shared-profile username
     ```

   - 您也可以在 `policy.conf` 檔案中個別指派每個系統的設定檔。

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

另請參閱 如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「policy.conf File」，以及 `policy.conf`(4) 線上手冊和 `usermod`(1M) 線上手冊。

▼ 如何將安全訊息放置在標題檔案中

使用此程序，在兩個標題檔案中建立反映您的網站安全策略的安全訊息。認證之前會顯示 `/etc/issue` 檔案，認證之後則顯示 `/etc/motd` 檔案。

注意 - 此程序中的範例訊息無法滿足美國政府的要求，可能也無法滿足您的安全策略。請向您公司的法律顧問查詢安全訊息的相關內容。

開始之前 您必須成為被指派「編輯管理員訊息」權限設定檔的管理員。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 建立 **/etc/issue** 檔案並新增安全訊息。

```
# pfedit /etc/issue
ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

login 指令會在認證前顯示 /etc/issue 的內容，就像 ssh、telnet 以及 FTP 服務一樣。若要在桌面登入顯示 /etc/issue 的內容，請參閱第 34 頁的「如何將安全訊息放置在桌面登入畫面上」。

如需更多資訊，請參閱 issue(4) 線上手冊和 pfedit(1M) 線上手冊。

2. 新增安全訊息至 **/etc/motd** 檔案。

```
# pfedit /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

在 Oracle Solaris 中，使用者的初始 Shell 會顯示 /etc/motd 檔案的內容。

▼ 如何將安全訊息放置在桌面登入畫面上

從數種方法中選擇建立安全訊息的方法，供使用者在認證前、認證後或認證前後審閱。認證之前會顯示 /etc/issue 檔案，認證之後則顯示 /etc/motd 檔案。

如需更多資訊，請按一下桌面上的「系統 -> 說明「功能表啟動「GNOME 說明瀏覽器」。您也可以使用 yelp 指令。在 gdm(1M) 線上手冊的「GDM Login Scripts and Session Files」小節中有關於桌面登入程序檔的討論。

注意 - 此程序中的範例訊息無法滿足美國政府的要求，可能也無法滿足您的安全策略。請向您公司的法律顧問查詢安全訊息的相關內容。

開始之前 若要建立檔案，您必須擔任 root 角色。若要修改現有的檔案，您必須成為被指派 solaris.admin.edit/*path-to-existing-file* 授權的管理員。

1. 使用下列其中一個選項，在認證前於桌面登入畫面顯示安全訊息。

   在認證前建立對話方塊的選項，使用來自第 33 頁的「如何將安全訊息放置在標題檔案中」之步驟 1的 /etc/issue 檔案中的安全訊息。

   - 選項 1：修改 GDM 初始化程序檔即可在對話方塊中顯示安全訊息。

     /etc/gdm 目錄包含三種可於認證前和認證後顯示安全訊息的初始化程序檔。

     ```
     # pfedit /etc/gdm/Init/Default
     /usr/bin/zenity --text-info --width=800 --height=300 \
     --title="Security Message"  --filename=/etc/issue
     ```

     如需以非 root 使用者身分編輯系統檔案的相關資訊，請參閱 pfedit(1M) 線上手冊。

   - 選項 2：修改登入視窗，使安全訊息顯示在輸入欄位上方。

登入視窗會展開以配合您的訊息長度。此方法未指向 `/etc/issue` 檔案。您必須將文字輸入至 GUI 中。

注意 - `pkg fix` 與 `pkg update` 指令已覆寫登入視窗 (`gdm-greeter-login-window.ui`)。如果要保留變更，請將檔案複製到配置檔案目錄中，然後在升級系統之後將此其變更與新檔案合併。如需更多資訊，請參閱 pkg(5) 線上手冊。

---

a. 將目錄變更為登入視窗使用者介面。

```
# cd /usr/share/gdm
```

b. (選用) 儲存原始登入視窗使用者介面的副本。

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
```

c. 使用「GNOME 工具套件」介面設計程式將標籤新增至登入視窗。

`glade-3` 程式會開啟 GTK+ 介面設計程式。在使用者輸入欄位上方所顯示的標籤中輸入安全訊息。

```
# /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
```

若要審閱介面設計程式的指南，請按一下「GNOME 說明瀏覽器」中的「開發」。就會在「線上手冊」中的「應用程式」底下列示 `glade-3`(1) 線上手冊。

d. (選用) 儲存已修改的登入視窗使用者介面的副本。

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
```

2. 使用下列其中一個選項，在認證後於桌面登入畫面顯示安全訊息。

在認證後建立對話方塊的檔案，使用來自第 33 頁的「如何將安全訊息放置在標題檔案中」之步驟 2的 `/etc/motd` 檔案中的安全訊息。

- 選項 1：在認證之後於桌面顯示安全訊息。

```
# pfedit /etc/gdm/PreSession/Default
/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message"  --filename=/etc/motd
```

注意 - 在使用者的工作區上，視窗可能會覆蓋對話方塊。

- 選項 2：建立一個在認證後於另一個視窗中顯示安全訊息的桌面檔案。

```
# pfedit /usr/share/gdm/autostart/LoginWindow/banner.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
```

```
Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message" \
--filename=/etc/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

在登入視窗中認證後，使用者必須將安全訊息視窗關閉，才能連線工作區。如需 `zenity` 指令選項的資訊，請參閱 `zenity`(1) 線上手冊。

範例 2-1 在桌面登入建立簡短警告訊息

在此範例中，管理員會輸入簡短的訊息作為桌面檔案中 `zenity` 指令的引數。管理員也會使用 `--warning` 選項，來顯示含有該訊息的警告圖示。

```
# pfedit /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

保護使用者

此時，只有能夠擔任 `root` 角色的初始使用者可以存取系統。最好依序執行下列作業，才能讓一般使用者登入。

表 2-2 保護使用者作業說明

作業	說明	相關說明
需要提供增強式密碼，並且定期更換密碼。	加強每個系統的預設密碼限制強度。	第 37 頁的「如何設定較強的密碼限制」
為一般使用者配置限制檔案權限。	將一般使用者的檔案權限設定為比 `022` 更具限制性的值。	第 40 頁的「如何設定更具限制性的一般使用者 `umask` 值」
設定一般使用者的帳戶鎖定。	在不是用來管理的系統上，設定全系統帳戶鎖定，並減少會啟動鎖定的登入次數。	第 38 頁的「如何設定一般使用者的帳戶鎖定」
替所有使用者預先選取 `cusa` 稽核類別。	針對系統的潛在威脅提供較佳的監視和記錄。	第 40 頁的「如何稽核登入/登出以外的重大事件」
建立角色。	將特定的管理作業分散給數個可信任的使用者，如此就沒有某個使用者可以損毀系統。 您可以使用預先定義的 ARMOR 角色、建立自己的角色，或者在自己的角色延伸 ARMOR。	「Managing User Accounts and User Environments in Oracle Solaris 11.2 」中的「Managing User Accounts by Using the CLI」 「Securing Users and Processes in Oracle Solaris 11.2 」中的「Assigning Rights to Users」

作業	說明	相關說明
減少可見的 GNOME 桌面應用程式數目。	防止使用者使用會影響安全的桌面應用程式。	請參閱「Oracle Solaris 11.2 Desktop Administrator's Guide 」中的第 11 章「Disabling Features in the Oracle Solaris Desktop System」。
限制使用者的權限。	移除使用者不需要的基本權限。	第 41 頁的「如何移除使用者不需要的基本權限」

▼ 如何設定較強的密碼限制

如果預設值無法滿足您的網站安全需求，則使用此程序。步驟順序以 `/etc/default/passwd` 檔案中的變數項目為準。

開始之前 您必須是具備 `solaris.admin.edit/etc/default/passwd` 授權的管理員。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

- 使用 **`pfedit`** 指令對 **`/etc/default/passwd`** 檔案進行下列變更：

  a. 要求使用者每隔四個月必須更換一次密碼，但更換的間隔頻率要在三個禮拜以上。

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  MINWEEKS=3
  ```

  b. 要求密碼至少要有 8 個字元。

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. 保留密碼歷程記錄。

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. 要求與上個密碼的最小差異。

  ```
  #MINDIFF=3
  MINDIFF=4
  ```

  e. 要求至少要有一個大寫字母。

  ```
  #MINUPPER=0
  MINUPPER=1
  ```

f. 要求至少要有一個數字。

```
#MINDIGIT=0
MINDIGIT=1
```

另請參閱
- 如需可用於限制密碼建立的變數清單，請參閱 passwd(1) 線上手冊。
- 如需安裝後生效的密碼限制，請參閱第 13 頁的「系統存取權會受到限制和監視」。

▼ 如何設定一般使用者的帳戶鎖定

使用此程序，在嘗試登入失敗達特定次數後會鎖定一般使用者帳戶。

注意 - 角色為共用的帳號。請不要針對可被授予角色的使用者或針對角色設定帳號鎖定，因為鎖定一位使用者就會鎖定角色。

開始之前 不要在用來進行管理活動的系統上，將此保護設定為全系統保護。而是應該監控管理系統是否有不尋常的使用，並使其維持可供管理員使用的狀態。

您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 將 **LOCK_AFTER_RETRIES** 安全性屬性設為 **YES**。

   選擇屬性值的範圍。

   - 設定全系統。

     此類保護適用於嘗試使用系統的所有使用者。

     ```
     # pfedit /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - 設定每個使用者。

     此類保護只適用於您對其執行此指令的使用者。如果有許多使用者，這並非具備可擴充性的解決方案。

     ```
     # usermod -K lock_after_retries=yes username
     ```

   - 建立並指派權限設定檔。

     此類保護適用於您指派此權限設定檔的所有使用者或系統。

a. 建立權限設定檔。

```
# profiles -p shared-profile -S ldap
shared-profile: set lock_after_retries=yes
...
```

如需更多建立權限設定檔的資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Creating Rights Profiles and Authorizations」。

b. 將權限設定檔指派給使用者或全系統。

若是多位使用者共用一個權限設定檔的情況，可在權限設定檔中設定這個值，作為具備可擴充性的解決方案。

```
# usermod -P shared-profile username
```

您也可以在 `policy.conf` 檔案中個別指派每個系統的設定檔。

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. 將 **RETRIES** 安全性屬性設為 **3**。

選擇屬性值的範圍。

- 設定全系統。

```
# pfedit /etc/default/login
...
#RETRIES=5
RETRIES=3
...
```

- 設定每個使用者。

```
# usermod -K lock_after_retries=3 username
```

- 建立並指派權限設定檔。

請依照步驟 1.3中的步驟，建立一個包含 `lock_after_retries=3` 的權限設定檔。

另請參閱

- 如需使用者和角色安全性屬性的討論內容，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的第 8 章「Reference for Oracle Solaris Rights」。
- 相關線上手冊：包括 `policy.conf(4)`、`profiles(1)`、`user_attr(4)` 以及 `usermod(1M)`。

▼ 如何設定更具限制性的一般使用者 umask 值

umask 公用程式可設定使用者建立檔案的檔案權限位元。如果預設 umask 值 022 的限制性不夠，請使用此程序設定更具限制性的遮罩。

開始之前 您必須是能夠編輯骨架檔案的管理員。root 角色具有這些授權。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 檢視 Oracle Solaris 針對使用者 Shell 預設值所提供的範例檔案。

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. 在要指派給使用者的 **/etc/skel** 檔案中設定 **umask** 值。

   選擇下列其中一個值：

   - umask 026 – 提供中等檔案保護

     (751) – 群組設為 r，其他人設為 x
   - umask 027 – 提供嚴格的檔案保護

     (750) – 群組設為 r，其他人禁止存取
   - umask 077 – 提供完整的檔案保護

     (700) – 不提供群組或其他人存取權

另請參閱 如需更多資訊，請參閱：

- 「Managing User Accounts and User Environments in Oracle Solaris 11.2 」中的「Managing User Accounts by Using the CLI」
- 「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「Default umask Value」
- 相關線上手冊：包括 useradd(1M) 和 umask(1)。

▼ 如何稽核登入/登出以外的重大事件

此程序可稽核管理指令、系統存取權以及網站安全策略所指定的其他重大事件。

注意 - 此程序的範例可能無法滿足您的安全策略。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 稽核被指派管理權限設定檔之使用者和角色所使用的全部授權指令。

   將 cusa 稽核類別加到其預先選取的遮罩。

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   cusa 中介類別所包括的稽核類別列於 /etc/security/audit_class 檔案中。

2. 記錄稽核指令的引數。

   ```
   # auditconfig -setpolicy +argv
   ```

3. (選用) 記錄執行稽核指令的環境。

   ```
   # auditconfig -setpolicy +arge
   ```

   注意 - 此策略選項有助於疑難排解。

另請參閱
- 如需稽核策略的相關資訊，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「Audit Policy」。
- 如需設定稽核旗號的範例，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「Configuring the Audit Service」和「Managing Auditing in Oracle Solaris 11.2 」中的「Troubleshooting the Audit Service」。
- auditconfig(1M) 線上手冊

▼ 如何移除使用者不需要的基本權限

在特定情況下，可以移除一般使用者或來賓使用者之基本設定中的部分基本權限。例如，讓 Sun Ray 使用者無法檢查不屬於他們的程序狀態。

開始之前 您必須擔任 root 角色。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 列出基本權限設定的完整定義。

   以下是三種可以移除的基本權限。

   ```
   % ppriv -lv basic
   file_link_any
    Allows a process to create hardlinks to files owned by a uid
    different from the process' effective uid.
   ...
   ```

```
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. 選擇權限的移除範圍。

   - 設定全系統。

     嘗試使用系統的所有使用者將無這些權限。此權限移除方法適用於公用電腦。

     ```
     # pfedit /etc/security/policy.conf
     ...
     #PRIV_DEFAULT=basic
     PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
     ```

   - 移除個別使用者的權限。

     - 防止使用者連結至不屬於使用者的檔案。

       ```
       # usermod -K 'defaultpriv=basic,!file_link_any' user
       ```

     - 防止使用者檢查不屬於使用者的程序。

       ```
       # usermod -K 'defaultpriv=basic,!proc_info' user
       ```

     - 防止使用者啟動第二個階段作業，例如從使用者目前的階段作業啟動 **ssh** 階段作業。

       ```
       # usermod -K 'defaultpriv=basic,!proc_session' user
       ```

     - 移除使用者之基本設定中的這三種權限。

       ```
       # usermod -K 'defaultpriv=basic,!file_link_any,!proc_info,!proc_session' user
       ```

   - 建立並指派權限設定檔。

     此類保護適用於您指派此權限設定檔的所有使用者或系統。

     a. 建立權限設定檔。

        ```
        # profiles -p shared-profile -S ldap
        shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
        ...
        ```

        如需更多建立權限設定檔的資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Creating Rights Profiles and Authorizations」。

b. 將權限設定檔指派給使用者或全系統。

如果許多使用者共用一個權限設定檔 (例如 Sun Ray 使用者或遠端使用者)，可以在權限設定檔中設定這個值，作為具備可擴充性的解決方案。

```
# usermod -P shared-profile username
```

您也可以在 `policy.conf` 檔案中個別指派每個系統的設定檔。

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

另請參閱 如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的第 1 章「About Using Rights to Control Users and Processes」和 `privileges(5)` 線上手冊。

保護網路

此時，您可能已建立可擔任角色的使用者，並且建立角色。

根據您的網站需求，從下列網路作業執行能夠提供額外安全性的作業。這些網路作業可強化 IP、ARP 以及 TCP 通訊協定。

表 2-3 配置網路作業說明

作業	說明	相關說明
停用網路路由常駐程式。	限制可能的網路封包監聽程式對系統的存取。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Disable the Network Routing Daemon」
防止散播網路拓樸資訊。	防止廣播封包。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Disable Broadcast Packet Forwarding」
	防止回應廣播回應要求和多重播送回應要求。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Disable Responses to Echo Requests」
針對作為其他網域之閘道器的系統 (例如防火牆或 VPN 節點)，開啟限制嚴格的來源和目標多址功能。	防止將標頭沒有閘道器位址的封包移出閘道器。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Set Strict Multihoming」
透過控制未完成的系統連線數目，避免阻絕服務 (DoS) 攻擊。	限制 TCP 偵聽程式允許的未完成 TCP 連線數。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Set Maximum Number of Incomplete TCP Connections」
透過控制許可的傳入連線數，避免 DoS 攻擊。	指定 TCP 偵聽程式預設的擱置 TCP 最大連線數。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Set Maximum Number of Pending TCP Connections」

作業	說明	相關說明
將網路參數回復成安全預設值。	提高因管理動作而降低的安全性。	「Securing the Network in Oracle Solaris 11.2 」中的「How to Reset Network Parameters to Secure Values」
將 TCP 包裝程式增加到網路服務，以限制合法使用者的應用程式。	指定允許存取網路服務的系統，例如 FTP。	如何使用 TCP 包裝程式
配置防火牆。	使用 IP 篩選器功能提供防火牆。	「Securing the Network in Oracle Solaris 11.2 」中的第 4 章「About IP Filter in Oracle Solaris」 「Securing the Network in Oracle Solaris 11.2 」中的第 5 章「Configuring IP Filter」
配置加密且經過認證的網路連線。	使用 IPsec 和 IKE 保護連帶配置 IPsec 和 IKE 之節點與網路之間的網路傳輸。	「Securing the Network in Oracle Solaris 11.2 」中的第 7 章「Configuring IPsec」 「Securing the Network in Oracle Solaris 11.2 」中的第 9 章「Configuring IKEv2」

▼ 如何使用 TCP 包裝程式

下列步驟顯示 TCP 包裝程式可在 Oracle Solaris 中使用的三種使用方式。

開始之前 您必須是 `root` 角色才能修改程式，以使用 TCP 包裝程式。

1. 您不需要使用 TCP 包裝程式來保護 **`sendmail`** 應用程式。

   此應用程式預設使用 TCP 包裝程式保護，如「Managing sendmail Services in Oracle Solaris 11.2 」中的「Support for TCP Wrappers From Version 8.12 of sendmail」所述。

2. 若要針對所有 **`inetd`** 服務啟用 TCP 包裝程式，請參閱「Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2 」中的「How to Use TCP Wrappers to Control Access to TCP Services」。

3. 使用 TCP 包裝程式保護 FTP 網路。

   a. 依照 **`/usr/share/doc/proftpd/modules/mod_wrap.html`** 模組中的說明。

      因為這個模組是動態的，所以您必須將它載入才能將 TCP 包裝程式與 FTP 搭配使用。

   b. 將下列指令加到 **`proftpd.conf`** 檔案中以載入模組：

      ```
      # pfedit /etc/proftpd.conf
      <IfModule mod_dso.c>
          LoadModule mod_wrap.c
      </IfModule>
      ```

c. 重新啟動 FTP 服務。

```
# svcadm restart svc:/network/ftp
```

保護檔案系統

ZFS 檔案系統為簡易的系統，可以進行加密、壓縮並且配置保留空間和磁碟空間配額。

tmpfs 檔案系統可能會無限制成長。為避免阻絕服務 (DoS) 攻擊，請完成第 45 頁的「如何限制 tmpfs 檔案系統的大小」。

下列作業會配置 tmpfs 的大小限制，並提供 ZFS (Oracle Solaris 的預設檔案系統) 可用的保護快速瀏覽。如需其他資訊，請參閱「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Setting ZFS Quotas and Reservations」和 zfs(1M) 線上手冊。

表 2-4 保護檔案系統作業說明

作業	說明	相關說明
透過管理及保留磁碟空間，避免 DoS 攻擊。	請依照檔案系統、使用者或群組、或是專案，指定使用的磁碟空間。	「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Setting ZFS Quotas and Reservations」
保證資料集和其子系的最小磁碟空間。	依照檔案系統、使用者或群組、或是專案，保證磁碟空間。	「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Setting Reservations on ZFS File Systems」
加密檔案系統上的資料。	資料集建立時，使用加密和通行密碼存取資料集，以保護資料集。	「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Encrypting ZFS File Systems」 「Managing ZFS File Systems in Oracle Solaris 11.2 」中的「Examples of Encrypting ZFS File Systems」
限制 tmpfs 檔案系統的大小。	防止惡意使用者在 /tmp 中建立大型檔案，以致於拖慢系統效能。	第 45 頁的「如何限制 tmpfs 檔案系統的大小」

▼ 如何限制 tmpfs 檔案系統的大小

tmpfs 檔案系統的大小預設為沒有限制。因此，tmpfs 可能會成長到填滿可用的系統記憶體和交換空間。/tmp 目錄是所有應用程式和使用者都能夠使用的目錄，因此某個應用程式就可能佔滿所有可用的系統記憶體。同樣的，有不良意圖的未授權使用者可能會在 /tmp 目錄中建立大型檔案，因而導致系統變慢。為避免效能影響，您可以限制每個 tmpfs 掛載的大小。

您可以嘗試數個不同的值，以獲取最佳系統效能。

開始之前 若要編輯 vfstab 檔案，您必須是具備 solaris.admin.edit/etc/vfstab 授權的管理員。若要重新啟動系統，您必須要被指派「維護與修復」權限設定檔。root 角色具有所有這些權限。如需更多資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 判斷您系統上的記憶體數量。

   注意 - 以下範例所使用的 SPARC T3 系列系統配備有可加快 I/O 速度的固態磁碟 (ssd) 和八顆 279.40 MB 硬碟。系統擁有約 500 GB 的記憶體。

   ```
   % prtconf | head
   System Configuration:  Oracle Corporation  sun4v
   Memory size: 523776 Megabytes
   System Peripherals (Software Nodes):

   ORCL,SPARC-T3-4
   scsi_vhci, instance #0
   disk, instance #4
   disk, instance #5
   disk, instance #6
   disk, instance #8
   ```

2. 計算 **tmpfs** 的記憶體限制。

   視系統記憶體大小而定，若為大型系統，您可能想要以大約 20% 來計算記憶體限制，若為較小的系統，您可能要以大約 30% 來計算記憶體限制。

   因此，對於較小的系統，請使用 .30 作為乘數。

   ```
   10240M x .30 ≈ 340M
   ```

   對於較大的系統，請使用 .20 作為乘數。

   ```
   523776M x .20 ≈ 10475M
   ```

3. 將 **/etc/vfstab** 檔案中的 **swap** 項目修改為限制的大小。

   ```
   # pfedit /etc/vfstab
   #device     device       mount       FS      fsck    mount mount
   #to mount   to fsck      point       type    pass    at boot options
   #
   ...
   #swap       -            /tmp        tmpfs   -       yes     -
   swap        -            /tmp        tmpfs   -       yes     size=10400m
   /dev/zvol/dsk/rpool/swap   -      -   swap    -       no      -
   ```

4. 重新啟動系統。

   ```
   # reboot
   ```

5. 驗證大小限制是否生效。

```
% mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. 監視記憶體使用量，並依據您的網站需求調整。
   `df` 命令有時會很有用。而 `swap` 命令可提供最有用的統計資料。

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

   如需更多資訊，請參閱 `tmpfs(7FS)`、`mount_tmpfs(1M)`、`df(1M)` 以及 `swap(1M)` 等線上手冊。

保護與修改檔案

預設只有 `root` 角色能夠修改系統檔案權限。具備 `solaris.admin.edit/`*path-to-system-file* 授權的角色和使用者才能夠修改該 *system-file*。唯有 `root` 角色能夠搜尋所有檔案。

表 2-5 保護及修改檔案作業說明

作業	說明	相關說明
為一般使用者配置限制檔案權限。	將一般使用者的檔案權限設定為比 `022` 更具限制性的值。	第 40 頁的「如何設定更具限制性的一般使用者 `umask` 值」
指定 ACL 保護檔案，ACL 比一般 UNIX 檔案權限更為精細。	延伸的安全性屬性對於保護檔案而言非常有用。 如需使用 ACL 的注意事項，請參閱 Hiding Within the Trees (http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf)。	ZFS End-to-End Data Integrity (http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data)
維護系統檔案完整性。	透過程序檔或使用 BART 找出惡意檔案。	「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「How to Find Files With Special File Permissions」

保護系統存取與使用

您可以配置 Oracle Solaris 安全功能以保護系統使用上的安全，包括系統上和網路上的應用程式與服務。

表 2-6 保護系統存取與使用作業說明

作業	說明	相關說明
防止程式惡意安裝可執行的堆疊。	設定系統變數，以防止緩衝區溢位惡意安裝可執行的堆疊。	「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「Protecting Executable Files From Compromising Security」
確定標記供位址空間配置隨機化 (ASLR) 使用的二進位檔可以使用 ASLR。	針對標記的二進位檔啟用 ASLR。	第 31 頁的「如何驗證 ASLR 是否啟用」
配置稽核。	自訂涵蓋範圍與檔案完整性的稽核配置。	第 52 頁的「使用稽核服務」
保護可能包含機密資訊的核心檔案。	建立具有核心檔案專用之限制存取的目錄。	「Troubleshooting System Administration Issues in Oracle Solaris 11.2 」中的「Enabling File Paths」 「Troubleshooting System Administration Issues in Oracle Solaris 11.2 」中的「Administering Your Core File Specifications」
使用 SSL 核心代理伺服器 保護 Web 伺服器。	可以使用安全通訊端層 (SSL) 通訊協定加密並加速 Web 伺服器通訊。	「Securing the Network in Oracle Solaris 11.2 」中的第 3 章「Web Servers and the Secure Sockets Layer Protocol」
建立包含應用程式的區域。	區域為隔離程序的容器。它們可以隔離應用程式與應用程式的部分。例如，區域可用來分隔網站資料庫與網站的 Web 伺服器。	「Introduction to Oracle Solaris Zones 」
管理區域中的資源。	區域會提供一些管理區域資源的工具。	「Administering Resource Management in Oracle Solaris 11.2 」

使用 SMF 保護原來的服務

您可以將應用程式加到 Oracle Solaris 的「服務管理功能 (SMF)」功能，然後要求啟動、重新整理以及停止服務的權限，將應用程式配置限於僅供信任的使用者或角色使用。

如需相關資訊和程序，請參閱：

- 「Securing Users and Processes in Oracle Solaris 11.2 」中的「Locking Down Resources by Using Extended Privileges」
- Securing MySQL using SMF - the Ultimate Manifest (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the)。
- 相關線上手冊：包括 `smf(5)`、`smf_security(5)`、`svcadm(1M)`、`svcbundle(1M)` 以及 `svccfg(1M)`。

配置 Kerberos 網路

您可以使用 Kerberos 服務保護您的網路。此主從式架構提供作業事件在網路上的安全性。此服務提供增強式使用者認證，以及整合性和私密性。您可以使用 Kerberos 服務安全地登入其他系統、執行指令、交換資料以及傳輸檔案。此外，管理員也可以使用此服務來限制對服務和系統的存取。身為 Kerberos 使用者，您可以管理其他人對您帳戶的存取。

如需相關資訊和程序，請參閱：

- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」中的第 3 章「Planning for the Kerberos Service」
- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」中的第 4 章「Configuring the Kerberos Service」
- 相關線上手冊：包括 kadmin(1M)、pam_krb5(5) 以及 kclient(1M)。

新增標籤式多層級安全性

Trusted Extensions 藉由強制執行標籤式強制性存取控制 (MAC) 策略來擴充 Oracle Solaris 的安全性。敏感度標籤會自動套用於所有資料來源 (網路、檔案系統及視窗) 和資料使用者 (使用者和程序)。並會以資料標籤 (物件) 與使用者 (主體) 之間的關係為基礎，限制存取所有資料。分層功能包括一組標籤感知服務。

Trusted Extensions 服務的部分清單包括：

- 標籤式網路
- 標籤感知檔案系統的掛載和共用
- 標籤式桌面
- 標籤配置和轉換
- 標籤感知系統管理工具
- 標籤感知裝置配置

system/trusted 和 system/trusted/trusted-global-zone 這兩個套裝軟體已可滿足無周邊系統或不需要多層級桌面之伺服器的需求。system/trusted/trusted-extensions 套裝軟體提供 Oracle Solaris 多層級的信任桌面環境。

配置 Trusted Extensions

您必須先安裝 Trusted Extensions 套裝軟體，然後再配置系統。安裝 trusted-extensions 套裝軟體之後，系統就可以使用直接連接的點陣式顯示執行桌面，例如筆記型電腦或工作站。與其他系統通訊需要網路配置。

如需相關資訊和程序，請參閱：

- 「Trusted Extensions Configuration and Administration 」中的第 I部分「Initial Configuration of Trusted Extensions」
- 「Trusted Extensions Configuration and Administration 」中的第 II部分「Administration of Trusted Extensions」

配置標籤式 IPsec

您可以使用 IPsec 保護標籤式封包。

如需相關資訊和程序，請參閱：

- 「Securing the Network in Oracle Solaris 11.2 」中的第 6 章「About IP Security Architecture」
- 「Trusted Extensions Configuration and Administration 」中的「Administration of Labeled IPsec」
- 「Trusted Extensions Configuration and Administration 」中的「Configuring Labeled IPsec」

♦ ♦ ♦ 第 3 章

3 維護及監控 Oracle Solaris 安全性

初始安裝及配置之後，您可以依照下述各種目的的程序，維護及監控系統的安全性狀態：

- 定期審閱稽核記錄
- 執行套裝軟體與檔案完整性檢查
- 監控網路活動
- 執行規範檢查

維護及監控系統安全性

下列作業可以依據網站的安全需求維護及監控系統、資料的存取與使用。

表 3-1 維護及監控系統作業說明

作業	說明	相關說明
驗證系統上的套裝軟體。	確認更新後的套裝軟體與來源套裝軟體相同。	第 30 頁的「如何驗證套裝軟體」
驗證檔案完整性。	配置之後，需要定期比較 BART 清單，確定只變更需要變更的檔案。	第 51 頁的「使用 BART 驗證檔案完整性」
尋找惡意檔案。	找出可能未授權使用程式之 `setuid` 和 `setgid` 權限的情形。	「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「How to Find Files With Special File Permissions」
定期審閱稽核記錄。	找出異常存取與使用系統的情形。	第 52 頁的「使用稽核服務」
即時審閱登入和登出事件的稽核記錄。	識別出嘗試發生之時間前後的嘗試違反情形。	第 53 頁的「即時監控稽核記錄」
執行規範測試。	評估系統的安全基準規範程度。	「Oracle Solaris 11.2 安全性規範指南 」和 `compliance(1M)` 線上手冊

使用 BART 驗證檔案完整性

BART 是一種使用加密強度雜湊和檔案系統中介資料來報告變更的規則型檔案完整性掃描與報告工具。

如需相關資訊和程序，請參閱：

- 「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「About BART」
- 「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「About Using BART」
- 「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「BART Manifests, Rules Files, and Reports」

如需追蹤已安裝系統之變更的特定說明，請參閱「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」中的「How to Compare Manifests for the Same System Over Time」。

使用稽核服務

稽核會持續記錄系統的使用狀況。稽核服務包含協助分析稽核資料的工具。

如需稽核服務的相關說明，請參閱「Managing Auditing in Oracle Solaris 11.2 」。如需線上手冊的清單與其連結，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「Audit Service Man Pages」。

下列稽核服務程序適用於許多安全環境：

- 建立個別的角色來配置稽核、審閱稽核以及啟動和停止稽核服務。指派角色給信任的使用者。

  使用稽核配置、稽核審閱以及稽核控制權限設定檔，作為您角色的基礎。

  若要建立角色或使用預先定義的 ARMOR 角色，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Assigning Rights to Users」。
- 使用 `cusa` 稽核類別稽核所有管理員。

  `cusa` 稽核類別中的事件涵蓋影響系統之安全性狀態的管理動作。如需相關說明，請參閱 `/etc/security/audit_class` 檔案。如需此程序的相關資訊，請參閱第 40 頁的「如何稽核登入/登出以外的重大事件」。
- 將稽核記錄傳送至中央伺服器。
  - 配置「稽核遠端伺服器 (ARS)」使用的稽核。

    請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「How to Send Audit Files to a Remote Repository」。
  - 將完整的稽核檔案安全傳輸排程到個別 ZFS 集區上的稽核審閱檔案系統。
- 監控 `syslog` 公用程式中所選稽核事件的文字摘要。

  啟動 `audit_syslog` 外掛程式，然後監視報告的事件。

  請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「How to Configure syslog Audit Logs」。
- 限制稽核檔案的大小。

將 audit_binfile 外掛程式的 p_fsize 屬性設為可用的大小。考慮其他因素中的審閱排程、磁碟空間以及 cron 工作頻率。

如需相關範例，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「How to Assign Audit Space for the Audit Trail」。

- 將完整的稽核檔案安全傳輸排程到個別 ZFS 集區上的稽核審閱檔案系統。
- 審閱稽核審閱檔案系統上的完整稽核檔案。

即時監控稽核記錄

audit_syslog 外掛程式可以讓您記錄預先選取之稽核事件的摘要。若要在終端機視窗中顯示產生的稽核摘要，請執行與下列類似的指令：

```
# tail -0f  /var/adm/auditlog
```

若要配置稽核記錄，請參閱「Managing Auditing in Oracle Solaris 11.2 」中的「How to Configure syslog Audit Logs」。

審閱和歸檔稽核記錄

您可以檢視文字格式的稽核記錄，或在瀏覽器中以 XML 格式檢視稽核記錄。

如需相關資訊和程序，請參閱：

- 「Managing Auditing in Oracle Solaris 11.2 」中的「Audit Logs」
- 「Managing Auditing in Oracle Solaris 11.2 」中的「Preventing Audit Trail Overflow」
- 「Managing Auditing in Oracle Solaris 11.2 」中的「Displaying Audit Trail Data」

♦ ♦ ♦ 附 錄 A

Oracle Solaris 安全性的參考書目

下列參考資料包含實用的 Oracle Solaris 系統安全性資訊。舊版 Oracle Solaris 中包含一些實用的安全性資訊，但有些資訊已經過時。

Oracle Technology Network 上的安全性參考資料

Oracle Technology Network 網站上的下列書籍與文章含有 Oracle Solaris 11 系統安全性的相關描述：

- 「Securing Systems and Attached Devices in Oracle Solaris 11.2 」
- 「Securing Files and Verifying File Integrity in Oracle Solaris 11.2 」
- 「Securing the Network in Oracle Solaris 11.2 」
- 「Securing Users and Processes in Oracle Solaris 11.2 」
- 「Managing Encryption and Certificates in Oracle Solaris 11.2 」
- 「Managing Auditing in Oracle Solaris 11.2 」
- 「Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 」
- 「Managing Secure Shell Access in Oracle Solaris 11.2 」
- 「Oracle Solaris 11.2 安全性規範指南 」
- 「Using a FIPS 140 Enabled System in Oracle Solaris 11.2 」

協力廠商出版物中的 Oracle Solaris 安全性參考資料

下列書籍包含 Oracle Solaris 11 系統安全性的相關描述：

- *Solaris 11 11/11* 版本 *1.0.0 2012* 年 *6* 月 *11* 日的安全配置基準

  此安全配置基準是由 Center for Internet Security (CIS) http://cisecurity.org/ 針對安全性社群所發行。本文件提供建議的 Oracle Solaris 作業系統 安全性設定。目標使用者包含開發、安裝、評估 Oracle Solaris 或為 Oracle Solaris 提供安全性解決方案的系統與應用程式管理員、安全性專家、稽核人員、客服工程師、安裝人員及開發人員。若要取得文件副本，請造訪 CIS Security Benchmarks (http://benchmarks.cisecurity.org/)。

- *Oracle Solaris 11 System Administration: The Complete Reference*.Michael Jang, Harry Foxwell, Christine Tran, and Alan Formy-Duval. 2012.McGraw-Hill.ISBN 978007179042.

  本書內容涵蓋 Oracle Solaris 的安全性相關事項。
- *Oracle Solaris 11: First Look*.Philip P.Brown. 2013.Packt Publishing.ISBN 9781849688307.

  本書為適合管理員閱讀的 Oracle Solaris 與其安全性介紹。
- *Oracle Solaris 11 System Administration*, Bill Calkins. 2013.Prentice Hall.ISBN 9780133007114.

  本書內容涵蓋包括安全功能在內的 Oracle Solaris 新功能。