Oracle® Solaris 11 安全性指導方針

文件號碼：E25820–03
2012 年 3 月

ORACLE

120411@25097

目錄

前言

本指南提供 Oracle Solaris 作業系統 (Oracle Solaris 作業系統) 的安全性指導方針。本指南首先描述企業作業系統必須解決的安全性問題。接著描述 Oracle Solaris 作業系統的預設安全性功能。最後提供強化系統及使用 Oracle Solaris 安全性功能來保護您的資料和應用程式所需採取的特定步驟。您可以針對您的網站安全性策略修改本指南中的建議。

對象

「Oracle Solaris 11 安全性指導方針」適合執行下列作業的安全性管理員和其他系統管理員使用：

- 分析安全性需求
- 實作軟體網站安全性策略
- 安裝和配置 Oracle Solaris 作業系統
- 維護系統和網路安全性

若要使用本指南，您必須具備 UNIX 管理的基本知識、良好的軟體安全性基礎，以及熟悉您的網站安全性策略。

存取 Oracle 客戶服務部

Oracle 客戶可以透過 My Oracle Support 存取電子支援。如需相關資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info，如果您有聽力障礙，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

印刷排版慣例

下表說明本書所使用的印刷排版慣例。

表 P–1 印刷排版慣例

字體	說明	範例
`AaBbCc123`	指令、檔案及目錄的名稱；螢幕畫面輸出。	請編輯您的 `.login` 檔案。 請使用 `ls -a` 列出所有檔案。 `machine_name% you have mail.`
`AaBbCc123`	您所鍵入的內容 (與螢幕畫面輸出相區別)。	`machine_name%` **`su`** `Password:`
aabbcc123	預留位置：用實際名稱或值取代	移除檔案的指令是 `rm` *filename*。
AaBbCc123	書名 (通常會加上引號)、新專有名詞以及要強調的專有名詞 (中文以粗體表示)	請參閱「使用者指南」第 6 章。 **快取記憶體**是儲存在本機的副本。 請**不要**儲存此檔案。 **備註**：某些強調項目在線上以粗體顯示。

指令中的 Shell 提示符號範例

下表顯示 Oracle Solaris OS 中包含的與 shell 有關的預設 UNIX 系統提示及超級使用者提示。請注意，顯示在指令範例中的預設系統提示符號視 Oracle Solaris 發行版本而不同。

表 P–2 Shell 提示符號

Shell	提示符號
Bash shell、Korn shell 和 Bourne shell	`$`
適用於超級使用者的 Bash shell、Korn shell 和 Bourne shell	`#`
C shell	`machine_name%`
C shell 超級使用者	`machine_name#`

◆ ◆ ◆ 第 1 章

1 Oracle Solaris 11 安全性簡介

Oracle Solaris 11 是一種非常牢固的最佳企業作業系統，可提供穩固的安全性功能。Oracle Solaris 11 擁有最先進的全網路安全性系統，可控制使用者存取檔案、保護系統資料庫和使用系統資源的方式，以滿足每個層級的安全性需求。傳統作業系統包含既有的安全性弱點，然而 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 11 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 安全性保護

Oracle Solaris 會保護磁碟上和傳輸中的資料，爲公司資料及應用程式提供穩固的基礎。Oracle Solaris Resource Manager (稱爲**資源管理**) 和 Oracle Solaris Zones 提供的功能，可以防止並避免不當使用應用程式。此控制功能與透過權限和 Oracle Solaris 以角色爲基礎的存取控制 (RBAC) 功能實作的最低權限，可以降低侵入者或一般使用者動作的安全性風險。認證和加密的通訊協定，例如 IP 安全性 (IPsec)，可以在網際網路與 LAN 或 WAN 內的通道間提供虛擬私人網路 (VPN)，以進行安全的資料傳遞。此外，Oracle Solaris 的稽核功能可確保記錄任何相關的活動。

Oracle Solaris 11 安全性服務可爲系統和網路提供保護層，因此能提供全面的防禦。Oracle Solaris 是藉由在核心公用程式內限制公用程式可以執行的權限動作以保護核心。預設的網路配置會針對系統和網路提供資料保護。IPsec (Oracle Solaris 的 IP 篩選器功能) 和 Kerberos 可以提供額外的保護。

Oracle Solaris 安全性服務包括：

- 保護核心 – 核心常駐程式與裝置會受檔案權限和特權保護。
- 保護登入 – 登入需要密碼。密碼會經過增強的加密。遠端登入最初會透過 Oracle Solaris 的 Secure Shell 功能限定至加密和認證的通道。`root` 帳戶無法直接登入。
- 保護資料 – 磁碟上的資料會受檔案權限保護。您也可以設定其他的保護層。舉例來說，您可以使用存取控制清單 (ACL)、將資料放在某個區域、加密檔案、加密 Oracle Solaris ZFS 資料集、建立唯讀的 ZFS 資料集，以及裝載檔案系統，使 `setuid` 程式和可執行檔無法執行。

Oracle Solaris 11 安全性技術

Oracle Solaris 的安全性功能可以設定成實作您網站的安全性策略。

下列各節提供 Oracle Solaris 安全性功能的簡介。此描述包含更詳細的說明參考資料，以及本指南和示範這些功能之其他 Oracle Solaris 系統管理指南的程序參考資料。

稽核服務

稽核是收集關於系統資源使用情形的資料。稽核資料可提供安全性相關之系統事件的記錄。此資料可接著用來爲系統上發生的動作指派職責。

稽核是安全性評估、驗證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「Oracle Solaris Administration: Security Services」中的第 29 章「Auditing (Reference)」。
- 如需指導方針，請參閱第 30 頁的 「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「Oracle Solaris Administration: Security Services」中的第 26 章「Auditing (Overview)」。
- 如需稽核作業的資訊，請參閱「Oracle Solaris Administration: Security Services」中的第 28 章「Managing Auditing (Tasks)」。

基本稽核報表工具

Oracle Solaris 的基本稽核報表工具 (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。透過建立 BART 清單，您可以輕鬆可靠地收集安裝在部署系統上之軟體堆疊的元件相關資訊。

BART 是管理系統或系統網路之完整性的實用工具。

如需更多資訊，請參閱：

- 選取的線上手冊包含「bart(1M) 線上手冊」、「bart_rules(4) 線上手冊」以及「bart_manifest(4) 線上手冊」。
- 如需指導方針，請參閱第 42 頁的 「建立系統 BART 快照」、第 45 頁的 「使用基本稽核報告工具」及線上手冊。
- 如需 BART 的簡介，請參閱「Oracle Solaris Administration: Security Services」中的第 6 章「Verifying File Integrity by Using BART」。
- 如需使用 BART 的範例，請參閱「Oracle Solaris Administration: Security Services」中的「Using BART (Tasks)」和線上手冊。

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，爲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。各種公開金鑰基礎架構 (PKI) 不同的儲存機制、管理公用程式及程式設計介面在採用 KMF 介面時，可使用整合的介面。

加密架構透過個別的指令、使用者層級的程式設計介面、核心程式設計介面，以及使用者層級和核心層級的架構，爲使用者和應用程式提供加密服務。加密架構會爲應用程式提供這些加密服務，並以無縫的方式爲一般使用者提供核心模組。加密架構也會爲一般使用者提供直接的加密服務，例如檔案的加密和解密。

KMF 爲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：

- 選取的線上手冊包含「cryptoadm(1M) 線上手冊」、「encrypt(1) 線上手冊」、「mac(1) 線上手冊」、「pktool(1) 線上手冊」以及「kmfcfg(1) 線上手冊」。
- 如需加密服務的簡介，請參閱「Oracle Solaris Administration: Security Services」中的第 11 章「Cryptographic Framework (Overview)」以及「Oracle Solaris Administration: Security Services」中的第 13 章「Key Management Framework」。
- 如需使用加密架構的範例，請參閱「Oracle Solaris Administration: Security Services」中的第 12 章「Cryptographic Framework (Tasks)」和線上手冊。

檔案權限和存取控制項目

檔案系統中用來保護物件的防禦第一線，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，ZFS 也支援存取控制清單 (ACL) (亦稱爲存取控制項目 (ACE))，可以更精細地控制檔案系統物件之個人和群組的存取。

如需更多資訊，請參閱：

- 如需對 ZFS 檔案設定 ACL 的說明，請參閱「chmod(1) 線上手冊」。
- 如需檔案權限的簡介，請參閱「Oracle Solaris Administration: Security Services」中的「Using UNIX Permissions to Protect Files」。
- 如需保護 ZFS 檔案的簡介和範例，請參閱「Oracle Solaris Administration: ZFS File Systems」中的第 8 章「Using ACLs and Attributes to Protect Oracle Solaris ZFS Files」和線上手冊。

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。

IP 篩選器

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

更具體而言，IP 篩選器可以提供有狀態的封包篩選功能，並可依據 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：

- 選取的線上手冊包含「ipfilter(5) 線上手冊」、「ipf(1M) 線上手冊」、「ipnat(1M) 線上手冊」、「svc.ipfd(1M) 線上手冊」以及「ipf(4) 線上手冊」。
- 如需 IP 篩選器的簡介，請參閱「Oracle Solaris Administration: IP Services」中的第 20 章「IP Filter in Oracle Solaris (Overview)」。
- 如需使用 IP 篩選器的範例，請參閱「Oracle Solaris Administration: IP Services」中的第 21 章「IP Filter (Tasks)」和線上手冊。
- 如需 IP 篩選器策略語言之語法的資訊和範例，請參閱「ipnat(4) 線上手冊」。

TCP 包裝程式

TCP 包裝程式會檢查從 ACL 要求特定網路服務的主機位址，以提供進行存取控制的方式。接著會接受或拒絕要求。TCP 包裝程式也會記錄網路服務的主機要求，這是很實用的監視功能。Secure Shell 和 Oracle Solaris 的 `sendmail` 功能會設爲使用 TCP 包裝程式。可以設定存取控制的網路服務包含 `ftpd` 和 `rpcbind`。

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性策略，還可指定以每個服務爲基礎的安全性策略。還可依據主機名稱、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。

如需更多資訊，請參閱：

- 如需 TCP 包裝程式的資訊，請參閱「Oracle Solaris Administration: IP Services」中的「How to Use TCP Wrappers to Control Access to TCP Services」。
- 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」。

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 有數種可用於設定增強式使用者密碼的功能。您可以設定密碼長度、內容、變更頻率及修改需求，以及保存密碼歷程。系統會提供應避免之密碼的密碼字典。並提供數種可使用的密碼演算法。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Security Services」中的「Maintaining Login Control」
- 「Oracle Solaris Administration: Security Services」中的「Securing Logins and Passwords (Tasks)」
- 選取的線上手冊包含「`passwd`(1) 線上手冊」和「`crypt.conf`(4) 線上手冊」。

可插接式驗證模組

可插接式驗證模組 (PAM) 架構可以讓您爲帳戶、認證、階段作業及密碼，協調和設定使用者認證需求。

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 `ftp`) 會使用 PAM 架構以確保系統的所有進入點均已受保護。此架構可取代或修改領域中的認證模組，不需變更使用 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。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Security Services」中的第 14 章「Using PAM」
- 「`pam.conf`(4) 線上手冊」

Oracle Solaris 中的特權

特權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`)。特權可授與指令、使用者、角色或系統。許多 Oracle Solaris 指令和常駐程式只會使用執行其作業所需的特權來執行。特權的使用也稱爲**程序權限管理**。

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。此外，特權也可讓組織限制要將哪些特權授與在其系統上執行的服務和程序。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Security Services」中的「Privileges (Overview)」
- 「Oracle Solaris Administration: Security Services」中的「Using Privileges (Tasks)」
- 「Developer's Guide to Oracle Solaris 11 Security」中的第 2 章「Developing Privileged Applications」
- 選取的線上手冊包含「`ppriv(1)` 線上手冊」和「`privileges(5)` 線上手冊」。

遠端存取

遠端存取攻擊可能會損害系統和網路。保護網路存取在現今的網際網路環境中是必要的，甚至在 WAN 和 LAN 環境中也很有用。

IPsec 和 IKE

IP 安全性 (IPsec) 會透過認證封包、加密封包或同時執行兩者以保護 IP 封包。Oracle Solaris 支援 IPv4 和 IPv6 的 IPsec。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 和其金鑰交換通訊協定 (IKE) 會使用加密架構中的演算法。此外，加密架構還爲使用 metaslot 的應用程式，提供了 softtoken 金鑰庫。當 IKE 設爲使用 metaslot 時，組織可以選擇將金鑰儲存在磁碟、連接的硬體金鑰庫或 softtoken 金鑰庫中。

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：

- 「Oracle Solaris Administration: IP Services」中的第 14 章「IP Security Architecture (Overview)」
- 「Oracle Solaris Administration: IP Services」中的第 15 章「Configuring IPsec (Tasks)」
- 「Oracle Solaris Administration: IP Services」中的第 17 章「Internet Key Exchange (Overview)」
- 「Oracle Solaris Administration: IP Services」中的第 18 章「Configuring IKE (Tasks)」
- 選取的線上手冊包含「`ipsecconf(1M)` 線上手冊」和「`in.iked(1M)` 線上手冊」。

Secure Shell

Oracle Solaris 的 Secure Shell 功能可讓使用者或服務透過加密的通訊通道，在遠端系統之間存取或傳輸檔案。在 Secure Shell 中，會加密所有網路流量。Secure Shell 也可做爲依需求指定的虛擬私有網路 (VPN)，其可轉送 X Window 系統流量，或可經由認證和加密的網路連結，來連線本機系統和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。依照預設，Secure Shell 是新安裝的系統上唯一使用中的遠端存取機制。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Security Services」中的第 15 章「Using Secure Shell」
- 選取的線上手冊包含「`ssh(1)` 線上手冊」、「`sshd(1M)` 線上手冊」、「`sshd_config(4)` 線上手冊」以及「`ssh_config(4)` 線上手冊」。

Kerberos 服務

Oracle Solaris 的 Kerberos 功能可啓用單一登入和安全作業事件，即使是經由執行 Kerberos 服務的異質網路也一樣。

Kerberos 是以在麻省理工學院 (MIT) 開發的 Kerberos V5 網路認證通訊協定爲基礎。Kerberos 服務採用主從式架構，可以保障作業事件在網路上的安全。此服務提供增強式使用者認證，以及整合性和私密性。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：

- 「Oracle Solaris Administration: Security Services」中的第 VI部分「Kerberos Service」
- 選取的線上手冊包含「`kerberos(5)` 線上手冊」和「`kinit(1)` 線上手冊」。

以角色為基礎的存取控制

RBAC 可讓組織選擇性地授與使用者或角色管理權限 (依據他們獨特的需要和需求)，以套用最低權限的安全性原則。

Oracle Solaris 以角色爲基礎的存取控制 (RBAC) 功能可控制使用者對一般限 `root` 角色存取之作業的存取。藉由套用安全性屬性到程序和使用者，RBAC 可在數個管理員之間散發管理權限。RBAC 也稱爲**使用者權限管理**。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Security Services」中的第 III部分「Roles, Rights Profiles, and Privileges」
- 選取的線上手冊包含「`rbac(5)` 線上手冊」、「`roleadd(1M)` 線上手冊」、「`profiles(1)` 線上手冊」以及「`user_attr(4)` 線上手冊」。

服務管理功能

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 會使用 RBAC 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，以及控制如何啓動、停止和重新整理那些服務。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Common Tasks」中的第 6 章「Managing Services (Overview)」
- 「Oracle Solaris Administration: Common Tasks」中的第 7 章「Managing Services (Tasks)」
- 選取的線上手冊包含「`svcadm(1M)` 線上手冊」、「`svcs(1)` 線上手冊」以及「`smf(5)` 線上手冊」。

Oracle Solaris ZFS 檔案系統

ZFS 是 Oracle Solaris 11 預設的檔案系統。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 中建立檔案系統是非常簡易的，您可以輕鬆建立配額和保留的空間。UNIX 權限和 ACE 會保護檔案，而 RBAC 則支援 ZFS 資料集的委任管理。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: ZFS File Systems」中的第 1 章「Oracle Solaris ZFS File System (Introduction)」
- 「Oracle Solaris Administration: ZFS File Systems」中的第 3 章「Oracle Solaris ZFS and Traditional File System Differences」
- 「Oracle Solaris Administration: ZFS File Systems」中的第 6 章「Managing Oracle Solaris ZFS File Systems」
- 選取的線上手冊包含「`zfs(1M)` 線上手冊」和「`zfs(7FS)` 線上手冊」。

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。

如需更多資訊，請參閱：

- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的第 II部分「Oracle Solaris Zones」
- 選取的線上手冊包含「brands(5) 線上手冊」、「zoneadm(1M) 線上手冊」以及「zonecfg(1M) 線上手冊」。

Trusted Extensions

Oracle Solaris 的 Trusted Extensions 功能是選擇性啓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 支援以所有權爲基礎的傳統任意存取控制 (DAC) 策略，以及以標籤爲基礎的必要存取控制 (MAC) 策略。除非啓用 Trusted Extensions 層，否則所有標籤都是相等的，如此核心才不會配置爲強制執行 MAC 策略。啓用以標籤爲基礎的 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。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。

Trusted Extensions 符合 Common Criteria Labeled Security Protection Profile (LSPP)、Role-Based Access Protection Profile (RBACPP) 及 Controlled Access Protection Profile (CAPP) 的需求。不過，Trusted Extensions 實作的獨特性在於提供高度保證，同時最大化相容性，且最小化負荷。

如需更多資訊，請參閱：

- 如需配置和維護 Trusted Extensions 的相關資訊，請參閱「Trusted Extensions Configuration and Administration」。
- 如需使用多層級桌面的相關資訊，請參閱「Trusted Extensions User's Guide」。
- 選取的線上手冊包含「trusted_extensions(5) 線上手冊」和「labeld(1M) 線上手冊」。

Oracle Solaris 11 安全性預設值

安裝之後，在其他安全性功能當中，Oracle Solaris 會保護系統免於遭受入侵，並會監視登入嘗試。

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。這兩個帳戶的密碼最初是相同的。

- 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。

- 初始使用者會被指派 /etc/security/policy.conf 檔案中的預設值。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啓動系統。
- 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爲 6 個字元的長度，並且至少包含一個字母字元和一個數字字元。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。有了加密和認證機制，使用者可以放心地連線系統，不會有資料遭到攔截、修改或詐騙的風險。

記錄的登入嘗試 – 系統會對所有**登入/登出**事件 (登入、登出、切換使用者、啓動和停止 ssh 階段作業，以及螢幕鎖定) 與所有非可歸因 (失敗) 的登入啓用稽核服務。由於 root 角色無法登入，因此可以在稽核記錄中追蹤具有 root 身分的使用者名稱。初始使用者可以透過系統管理員權限設定檔授與的權限來審閱稽核記錄。

具備核心、檔案及桌面保護

在初始使用者登入後，核心、檔案系統以及桌面應用程式都會受最低特權、權限和以角色爲基礎的存取控制 (RBAC) 所保護。

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，所有檔案系統均爲 ZFS 檔案系統。使用者的 umask 是 022，因此當某個使用者建立新檔案或目錄時，只有該使用者才能進行修改。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。目錄權限爲 drwxr-xr-x (755)。檔案權限爲 -rw-r--r-- (644)。

桌面 Applet – 桌面 Applet 受 RBAC 保護。舉例來說，唯有初始使用者或 root 角色可以使用套裝軟體管理員 Applet 安裝新的套裝軟體。沒有被指派使用權限的一般使用者，則看不到套裝軟體管理員。

具備其他安全性功能

Oracle Solaris 11 提供許多安全性功能，可用來設定系統和使用者，以滿足網站安全性需求。

- **以角色為基礎的存取控制 (RBAC)** – Oracle Solaris 提供數種授權、特權及權限設定檔。`root` 是唯一定義的角色。權限設定檔可爲您建立的角色提供良好的基礎。此外，某些管理指令需要 RBAC 授權才能成功。沒有授權的使用者無法執行指令，即使使用者具有必要的特權也一樣。
- **使用者權限** – 使用者會被指派 `/etc/security/policy.conf` 檔案中一組基本的特權、權限設定檔和授權，如同第 17 頁的「系統存取權會受到限制和監視」中所述的初始使用者。使用者登入嘗試不會受到限制，但稽核服務會記錄所有失敗的登入。
- **系統檔案保護** – 系統檔案會受檔案權限保護。唯有 `root` 角色可以修改系統配置檔案。

網站安全性策略和做法

如果要有安全的系統或系統網路，您的網站必須具備安全性策略，以及支援策略的安全做法。

如需更多資訊，請參閱以下內容：

- 「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 11 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 作業系統

當您安裝 Oracle Solaris 作業系統 時，請選擇安裝適當**群組**套裝軟體的媒體：

- **Oracle Solaris Large Server** – 在 [自動安裝程式 (AI)] 安裝的預設清單以及安裝 `group/system/solaris-large-server` 群組之文字安裝程式 (提供 Oracle Solaris 大型伺服器環境) 中的預設清單。
- **Oracle Solaris Desktop** – Live Media 會安裝 `group/system/solaris-desktop` 群組，此群組提供 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` 群組新增至 Oracle Solaris 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 Systems」中的第 III部分「Installing Using an Install Server」。

如需引導您選擇媒體，請參閱下列安裝指南：

- 「Installing Oracle Solaris 11 Systems」
- 「Creating a Custom Oracle Solaris 11 Installation Image」
- 「Adding and Updating Oracle Solaris 11 Software Packages」

保護系統

最好依序執行下列作業。此時，Oracle Solaris 11 作業系統已安裝，只有能夠擔任 root 角色的初始使用者可以存取系統。

作業	說明	相關說明
1. 驗證系統上的套裝軟體。	檢查安裝媒體的套裝軟體是否與已安裝的套裝軟體相同。	第 22 頁的「驗證套裝軟體」
2. 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。	「Oracle Solaris Administration: Security Services」中的「Controlling Access to System Hardware (Tasks)」
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 23 頁的「停用不需要的服務」
4. 需要裝置配置。	避免在沒有明確的授權下使用可移除的媒體。這些裝置包含麥克風、USB 磁碟機以及 CD。	「Oracle Solaris Administration: Security Services」中的「How to Enable Device Allocation」
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 23 頁的「移除使用者的電源管理能力」
6. 建立反映您網站之安全性策略的登入警告訊息。	通知使用者及可能的攻擊者系統已受監控。	第 24 頁的「將安全訊息放置在標題檔案中」 第 24 頁的「將安全訊息放置在桌面登入畫面上」

▼ 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 您必須爲 root 角色。

1. **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
   ```

2. **審閱有任何錯誤的記錄。**

3. **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。

▼ 停用不需要的服務

基於系統考量，使用此程序停用不必要的服務。

開始之前 您必須爲 root 角色。

1. **列出線上服務。**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **停用此系統不需要的服務。**

例如，如果系統不是 NFS 伺服器或 Web 伺服器，但這些服務在線上，請停用這些服務。

```
# 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「Oracle Solaris Administration: Common Tasks」中的第 6 章「Managing Services (Overview)」和「svcs(1) 線上手冊」。

▼ 移除使用者的電源管理能力

使用此程序，可避免此系統的使用者暫停系統或中斷系統的電源。

開始之前 您必須爲 root 角色。

1. **審閱主控台使用者 (Console User) 權限設定檔的內容。**

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;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「Oracle Solaris Administration: Security Services」中的「How to Create or Change a Rights Profile」。

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

   ```
   #CONSOLE_USER=Console User
   ```

4. **將您在步驟 2 建立的權限設定檔指派給使用者。**

   ```
   # usermod -P +new-profile username
   ```

另請參閱 如需更多資訊，請參閱「Oracle Solaris Administration: Security Services」中的「policy.conf File」，以及「policy.conf(4) 線上手冊」和「usermod(1M) 線上手冊」。

▼ 將安全訊息放置在標題檔案中

使用此程序建立反映您網站安全性策略的警告訊息。這些檔案的內容會顯示在本機和遠端登入。

備註 – 此程序中的範例訊息無法滿足美國政府需求，可能也無法滿足您的安全性策略。

開始之前 您必須爲 root 角色。最佳做法是向您公司的法律顧問查詢安全訊息的相關內容。

1. **將安全訊息輸入 /etc/issue 檔案。**

   ```
   # vi /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.
   ```

   如需更多資訊，請參閱「issue(4) 線上手冊」。

   telnet 程式會顯示 /etc/issue 檔案的內容作爲其登入訊息。如需讓其他應用程式使用此檔案的資訊，請參閱第 33 頁的「向 ssh 和 ftp 使用者顯示安全訊息」和第 24 頁的「將安全訊息放置在桌面登入畫面上」。

2. **新增安全訊息至 /etc/motd 檔案。**

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

▼ 將安全訊息放置在桌面登入畫面上

從數種方法中選擇以建立供使用者在登入時審閱的安全訊息。

如需更多資訊，請按一下桌面上的 [系統 > 說明] 功能表啓動 [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。

備註 – 此程序中的範例訊息無法滿足美國政府需求，可能也無法滿足您的安全性策略。

開始之前 您必須爲 `root` 角色。最佳做法是向您公司的法律顧問查詢安全訊息的相關內容。

- **將安全訊息放置在桌面登入畫面上。**

  您有幾個選項可用。建立對話方塊的選項可使用第 24 頁的 「將安全訊息放置在標題檔案中」的步驟 1中的 `/etc/issue` 檔案。

  - **選項 1：建立一個會在登入時於對話方塊中顯示安全訊息的桌面檔案。**

    ```
    # vi /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/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    在登入視窗中認證後，使用者必須關閉對話方塊才能連線工作區。如需 `zenity` 指令選項的資訊，請參閱「`zenity`(1) 線上手冊」。

  - **選項 2：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` 目錄包含三種初始化程序檔，可以在桌面登入之前、登入期間或登入之後立即顯示安全訊息。在 Oracle Solaris 10 發行版本中也有提供這些程序檔。

    - **在登入畫面出現之前顯示安全訊息。**

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

    - **認證之後在登入畫面上顯示安全訊息。**

      在顯示使用者工作區之前會先執行此程序檔。修改 `Default.sample` 程序檔即可建立此程序檔。

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

    - **認證後在使用者的初始工作區中顯示安全訊息。**

      ```
      # vi /etc/gdm/PreSession/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      ```

```
--title="Security Message" \
--filename=/etc/issue
```

備註 – 在使用者的工作區上，視窗可能會覆蓋對話方塊。

- **選項 3：修改登入視窗來於輸入欄位上方顯示安全訊息。**

  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。

  備註 – `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. **(可選擇) 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` 程式會開啓 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. **(可選擇) 在修改登入視窗 GUI 之後，儲存副本。**

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

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爲桌面檔案中 `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。

```
# vi /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。

作業	說明	相關說明
需要增強式密碼，以及經常更換密碼。	加強每個系統的預設密碼限制強度。	第 27 頁的「設定較強的密碼限制」
爲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爲比 022 更具限制性的值。	第 29 頁的「爲一般使用者設定更具限制性的 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，並減少會啓動鎖定的登入次數。	第 28 頁的「設定一般使用者的帳戶鎖定」
預先選取其他稽核類別。	針對系統的潛在威脅提供較佳的監視和記錄。	第 30 頁的「稽核登入/登出以外的重大事件」
將稽核事件的文字摘要傳送到 syslog 公用程式。	提供即時涵蓋重大稽核事件，例如登入和嘗試登入。	第 30 頁的「即時監視 lo 事件」
建立角色。	將特定的管理作業分發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。	「Oracle Solaris Administration: Common Tasks」中的「Setting Up User Accounts」 「Oracle Solaris Administration: Security Services」中的「How to Create a Role」 「Oracle Solaris Administration: Security Services」中的「How to Assign a Role」。
只在使用者的桌面顯示允許的應用程式。	避免使用者看見或使用未授權其使用的應用程式。	請參閱「Trusted Extensions Configuration and Administration」中的「How to Limit a User to Desktop Applications」。
限制使用者的權限。	移除使用者不需要的基本權限。	第 31 頁的「移除使用者不需要的基本權限」

▼ 設定較強的密碼限制

如果預設值無法滿足您的網站安全性需求，則使用此程序。步驟會依照 /etc/default/passwd 檔案中的項目清單來操作。

開始之前 變更預設值前，請確保這些變更可以讓所有使用者驗證應用程式和網路上的其他系統。

您必須爲 root 角色。

- **編輯 /etc/default/passwd 檔案。**

  a. **要求使用者每個月都要變更密碼，但更換的頻率間隔不得少於三個禮拜。**

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  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

- 如需限制密碼建立的變數清單，請參閱 /etc/default/passwd 檔案。檔案會指示預設值。
- 如需安裝後生效的密碼限制，請參閱第 17 頁的「系統存取權會受到限制和監視」。
- 「passwd(1) 線上手冊」

▼ 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。

備註 – 不要爲可以擔任角色的使用者設定帳戶鎖定，因爲您可能會鎖定該角色。

開始之前 您必須爲 root 角色。不要在用來進行管理活動的系統上，將此保護設定爲全系統保護。

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

- **設定全系統。**

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

- **設定每個使用者。**

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

2 **將 RETRIES 安全性屬性設為 3。**

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

另請參閱

- 如需使用者和角色安全性屬性的討論，請參閱「Oracle Solaris Administration: Security Services」中的第 10 章「Security Attributes in Oracle Solaris (Reference)」。
- 選取的線上手冊包含「policy.conf(4) 線上手冊」和「user_attr(4) 線上手冊」。

▼ 為一般使用者設定更具限制性的 umask 值

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 您必須爲 root 角色。

- **針對各種 Shells 修改骨架目錄中登入設定檔的 umask 值。**

  Oracle Solaris 提供可讓管理員自訂使用者 Shell 預設值的目錄。這些骨架目錄包含如 .profile、.bashrc 以及 .kshrc 等等的檔案。

  選擇下列其中一個值：

  - umask 027 – 提供中等檔案保護

    (740) – w 適用於群組，rwx 適用於其他人
  - umask 026 – 提供稍微嚴格的檔案保護

    (741) – w 適用於群組，rw 適用於其他人
  - 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：

- 「Oracle Solaris Administration: Common Tasks」中的「Setting Up User Accounts」
- 「Oracle Solaris Administration: Security Services」中的「Default umask Value」
- 選取的線上手冊包含「usermod(1M) 線上手冊」和「umask(1) 線上手冊」。

▼ 稽核登入/登出以外的重大事件

使用此程序，稽核管理指令、侵入系統的嘗試，以及網站安全性策略指定的其他重大事件。

備註 – 此程序的範例可能無法滿足您的安全性策略。

開始之前 您必須爲 root 角色。您要針對稽核實作網站安全性策略。

1. **稽核使用者與角色對於特權指令的所有用法。**

   若是要稽核所有使用者與角色，請新增 AUE_PFEXEC 稽核事件至 preselection 遮罩。

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. **請記錄稽核指令的引數。**

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

3. **請記錄執行稽核指令的環境。**

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

另請參閱

- 如需稽核策略的資訊，請參閱「Oracle Solaris Administration: Security Services」中的「Audit Policy」。
- 如需有關設定稽核旗號的範例，請參閱「Oracle Solaris Administration: Security Services」中的「Configuring the Audit Service (Tasks)」和「Oracle Solaris Administration: Security Services」中的「Troubleshooting the Audit Service (Tasks)」。
- 若要配置稽核，請參閱「auditconfig(1M) 線上手冊」。

▼ 即時監視 lo 事件

請使用此程序啓動您想要即時監視之事件的 audit_syslog 外掛程式。

開始之前 您必須爲 root 角色才可修改 syslog.conf 檔案。 其他步驟需要將稽核配置權限設定檔指派給您。

1. **將 lo 類別傳送至 audit_syslog 外掛程式，並啓動該外掛程式。**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **將 audit.notice 項目新增至 syslog.conf 檔案。**

   預設的項目包括記錄檔案的位置。

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. **建立記錄檔案。**

   ```
   # touch /var/adm/auditlog
   ```

4. **重新整理 syslog 服務的配置資訊。**

   ```
   # svcadm refresh system/system-log
   ```

5. **重新整理稽核服務。**

   稽核服務會在重新整理時讀取稽核外掛程式的變更。

   ```
   # audit -s
   ```

另請參閱

- 若要將稽核摘要傳送至其他系統，請參閱下列範例「Oracle Solaris Administration: Security Services」中的「How to Configure syslog Audit Logs」。
- 稽核服務可以產生大量輸出。若要管理記錄，請參閱「logadm(1M) 線上手冊」。
- 若要監視輸出，請參閱第 46 頁的「監視 audit_syslog 稽核摘要」。

▼ 移除使用者不需要的基本權限

在特定情況下，可從一般使用者的基本設定中移除三個基本權限中的一個或多個權限。

- file_link_any – 允許程序建立與有效 UID 程序相異，且由 UID 擁有之檔案的強制連結。
- proc_info – 允許程序檢查可傳送訊號以外程序的狀態。無法檢查的程序在 /proc 中不會顯示，而且也不會存在。
- proc_session – 允許程序傳送訊號或追蹤其階段作業以外的程序。

開始之前 您必須爲 root 角色。

1. **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
   ```

2. **防止使用者檢查不屬於使用者的程序。**

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

3. **防止使用者啓動第二個階段作業，例如從使用者目前的階段作業啓動 ssh 階段作業。**

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

4. **從使用者的基本設定移除所有三個權限。**

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

另請參閱 如需更多資訊，請參閱「Oracle Solaris Administration: Security Services」中的第 8 章「Using Roles and Privileges (Overview)」和「privileges(5) 線上手冊」。

保護核心

此時，您可能已建立可擔任角色的使用者，並且建立角色。僅有 root 角色才可以修改系統檔案。

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。	「Oracle Solaris Administration: Security Services」中的「Protecting Executable Files From Compromising Security」
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。	「Oracle Solaris Administration: Common Tasks」中的「How to Enable a Global Core File Path」 「Oracle Solaris Administration: Common Tasks」中的「Managing Core Files (Task Map)」

配置網路

此時，您可能已建立可擔任角色的使用者，並且建立角色。僅有 root 角色才可以修改系統檔案。

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。這些網站作業會通知遠端登入的使用者其系統已受保護以及強化 IP、ARP 及 TCP 通訊協定。

作業	說明	相關說明
顯示反映您網站之安全性策略的警告訊息。	通知使用者及可能的攻擊者系統已受監控。	第 33 頁的 「向 ssh 和 ftp 使用者顯示安全訊息」
停用網路路由常駐程式。	限制可能的網路封包監聽程式存取系統。	第 34 頁的 「停用網路路由常駐程式」

作業	說明	相關說明
防止散播網路拓樸資訊。	防止廣播封包。	第 35 頁的「停用廣播封包轉寄」
	防止回應廣播回應要求和多重播送回應要求。	第 35 頁的「停用對回應要求的回應」
針對做爲其他網域之閘道器的系統 (例如防火牆或 VPN 節點)，開啓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。	第 36 頁的「設定限制多址功能」
控制未完成的系統連線數，防止 DOS 攻擊。	限制 TCP 偵聽程式允許的未完成 TCP 連線數。	第 36 頁的「設定未完成 TCP 的最大連線數」
控制許可的傳入連線數，防止 DOS 攻擊。	指定 TCP 偵聽程式預設的擱置 TCP 最大連線數。	第 37 頁的「設定擱置 TCP 的最大連線數」
產生用於初始 TCP 連線數的強式亂數。	與由 RFC 1948 所指定的順序編號產生值相符。	第 37 頁的「指定用於初始 TCP 連線的強式亂數」
將網路參數回復成安全預設值。	增加因管理動作而降低的安全性。	第 37 頁的「將網路參數重設爲安全值」
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。 依預設，會使用 TCP 包裝程式保護 `sendmail` 應用程式，如「Oracle Solaris Administration: Network Services」中的「Support for TCP Wrappers From Version 8.12 of sendmail」所述。	若要爲所有 `inetd` 服務啓用 TCP 包裝程式，請參閱「Oracle Solaris Administration: IP Services」中的「How to Use TCP Wrappers to Control Access to TCP Services」。 如需 TCP 包裝程式保護 FTP 網路服務的範例，請參閱「Oracle Solaris Administration: Network Services」中的「How to Start an FTP Server Using SMF」。

▼ 向 ssh 和 ftp 使用者顯示安全訊息

在遠端登入和檔案傳輸時會使用此程序來顯示警告。

開始之前 您必須爲 `root` 角色。您已在 第 24 頁的「將安全訊息放置在標題檔案中」 的 步驟 1 中建立 `/etc/issue` 檔案。

1 如果要向使用 `ssh` 登入的使用者顯示安全訊息，請執行下列動作：

a. 取消 `/etc/sshd_config` 檔案中之 [標題] 指令的註釋。

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. 重新整理 `ssh` 服務。

```
# svcadm refresh ssh
```

如需更多資訊，請參閱「issue(4) 線上手冊」和「sshd_config(4) 線上手冊」。

2 **如果要向使用 ftp 登入的使用者顯示安全訊息，請執行下列動作：**

a. **將 DisplayConnect 指令新增至 proftpd.conf 檔案。**

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. **重新啓動 ftp 服務。**

```
# svcadm restart ftp
```

如需更多資訊，請參閱 ProFTPD (http://www.proftpd.org/) 網站。

▼ 停用網路路由常駐程式

使用此程序指定預設路由器以防止在安裝之後執行網路路由。否則，請在手動配置路由之後執行此程序。

備註 – 許多網路配置程序都需要停用路由常駐程式。因此，做爲較大配置程序中的一部分，您可能要停用此常駐程式。

開始之前 您必須被指派網路管理權限設定檔。

1 **確認路由常駐程式是否正在執行。**

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

如果服務未執行，您可進行到此步驟爲止。

2 **停用路由常駐程式。**

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 **確認路由常駐程式是否已停用。**

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

另請參閱 「routeadm(1M) 線上手冊」

▼ 停用廣播封包轉寄

依預設，&OSOL 會轉寄廣播封包。如果您的網站安全性策略需要降低廣播大量湧入的可能性，請使用此程序變更預設。

備註 – 當您停用 _forward_directed_broadcasts 網路特性時，也會停用廣播偵測。

開始之前 您必須被指派網路管理權限設定檔。

1. **將 IP 封包的廣播封包轉寄特性設定為 0。**

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2. **驗證目前的值。**

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                   PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts  rw   0         --           0         0,1
```

另請參閱 「ipadm(1M) 線上手冊」

▼ 停用對回應要求的回應

使用此程序防止網路拓樸資訊的散播。

開始之前 您必須被指派網路管理權限設定檔。

1. **對 IP 封包的廣播回應要求特性的回應設定為 0，然後驗證目前的值。**

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2. **對 IP 封包的多重播送回應要求特性的回應設定為 0，然後驗證目前的值。**

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

另請參閱 如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual」中的「_respond_to_echo_broadcast and _respond_to_echo_multicast (ipv4 or ipv6)」和「ipadm(1M) 線上手冊」。

▼ 設定限制多址功能

針對做爲其他網域之閘道器的系統 (例如防火牆或 VPN 節點)，使用此程序以開啓限制多址功能。

Oracle Solaris 11 發行版本爲 IPv4 和 IPv6 引進了一項新的 `hostmodel` 特性。此特性會控制多址系統上 IP 封包的傳送與接收運作方式。

開始之前 您必須被指派網路管理權限設定檔。

1. **將 IP 封包的 `hostmodel` 特性設定為 `strong`。**

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2. **驗證目前的值並注意可能的值。**

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

另請參閱 如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual 」中的「hostmodel (ipv4 or ipv6)」和「ipadm(1M) 線上手冊」。

如需更多使用限制多址功能的資訊，請參閱「Oracle Solaris Administration: IP Services」中的「How to Protect a VPN With IPsec in Tunnel Mode」。

▼ 設定未完成 TCP 的最大連線數

使用此程序控制未完成擱置連線數，防止組絕服務 (DOS) 攻擊。

開始之前 您必須被指派網路管理權限設定檔。

1. **設定傳入的最大連線數。**

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2. **驗證目前的值。**

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

另請參閱 如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual」中的「_conn_req_max_q0」和「ipadm(1M) 線上手冊」。

▼ 設定擱置 TCP 的最大連線數

使用此程序控制許可的傳入連線數，防止 DOS 攻擊。

開始之前 您必須被指派網路管理權限設定檔。

1. **設定傳入的最大連線數。**

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2. **驗證目前的值。**

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

另請參閱 如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual」中的「_conn_req_max_q」和「ipadm(1M) 線上手冊」。

▼ 指定用於初始 TCP 連線的強式亂數

此程序會設定 TCP 初始順序編號產生參數以遵循 RFC 1948 (http://www.ietf.org/rfc/rfc1948.txt)。

開始之前 您必須是 root 角色才能修改系統檔案。

- **變更 TCP_STRONG_ISS 變數的預設值。**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ 將網路參數重設為安全值

依預設，許多安全的網路參數皆可調整，因此您可進行變更。如果網站條件許可，請將下列可調整的參數回復爲預設值。

開始之前 您必須被指派網路管理權限設定檔。參數目前的值比預設值的安全性低。

1. **將 IP 封包的來源封包轉寄特性設定為 0，然後驗證目前的值。**

   預設值會防止來自詐騙封包的 DOS 攻擊。

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

   如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual」中的「forwarding (ipv4 or ipv6)」。

2. **將 IP 封包的網路遮罩回應特性設定為 0，然後驗證目前的值。**

   預設值會防止網路拓樸資訊的散播。

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3. **將 IP 封包的時間戳記回應特性設定為 0，然後驗證目前的值。**

   預設值會依系統需求移除額外的 CPU，並防止網路資訊的散播。

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp     rw   0         --           0         0,1
```

4. **將 IP 封包的廣播時間戳記特性設定為 0，然後驗證目前的值。**

   預設值會依系統需求移除額外的 CPU，並防止網路資訊的散播。

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast  rw   0         --           0         0,1
```

5. **將 IP 封包的忽略重新導向特性設定為 0，然後驗證目前的值。**

   預設值會依系統需求防止使用額外的 CPU。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6. **防止 IP 來源發送。**

   如果您因診斷目的需要 IP 來源發送，請勿停用此網路參數。

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
```

```
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes  rw   0         --           0         0,1
```

如需更多資訊，請參閱「Oracle Solaris Tunable Parameters Reference Manual」中的「_rev_src_routes」。

7 **將 IP 封包的忽略重新導向特性設定為 0，然後驗證目前的值。**

預設值會依系統需求防止使用額外的 CPU。一般而言，在設計優良的網路上不需要重新導向功能。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY          PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY          PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw    0         --           0         0,1
```

另請參閱 「ipadm(1M) 線上手冊」

保護檔案系統與檔案

ZFS 檔案系統爲簡易的系統，並可進行加密、壓縮及配置保留的空間和磁碟空間限制。

下列作業提供 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「Oracle Solaris Administration: ZFS File Systems」中的「Setting ZFS Quotas and Reservations」和「zfs(1M) 線上手冊」。

作業	說明	相關說明
管理和保留磁碟空間，防止 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。	「Oracle Solaris Administration: ZFS File Systems」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。	「Oracle Solaris Administration: ZFS File Systems」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。	「Oracle Solaris Administration: ZFS File Systems」中的「Encrypting ZFS File Systems」 「Oracle Solaris Administration: ZFS File Systems」中的「Examples of Encrypting ZFS File Systems」

作業	說明	相關說明
指定 ACL 保護檔案，ACL 比一般 UNIX 檔案權限更爲精細。	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)

保護與修改檔案

僅有 root 角色才可以修改系統檔案。

作業	說明	相關說明
爲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爲比 022 更具限制性的值。	第 29 頁的「爲一般使用者設定更具限制性的 umask 值」
防止惡意檔案取代系統檔案。	透過程序檔或使用 BART 找出惡意檔案。	「Oracle Solaris Administration: Security Services」中的「How to Find Files With Special File Permissions」

保護應用程式與服務

您可以配置 Oracle Solaris 安全性功能以保護應用程式。

建立區域以包含重要的應用程式

區域爲隔離程序的容器。它們對應用程式而言是實用的容器，也是應用程式的一部分。例如，區域可用來分隔網站資料庫與網站的 Web 伺服器。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的第 15 章「Introduction to Oracle Solaris Zones」
- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的「Summary of Zones by Function」
- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的「Capabilities Provided by Non-Global Zones」
- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的「Setting Up Zones on Your System (Task Map)」。

- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的第 16 章「Non-Global Zone Configuration (Overview)」。
- Hardening Oracle Database with Oracle Solaris Security Technologies (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

管理區域中的資源

區域會提供一些管理區域資源的工具。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的第 14 章「Resource Management Configuration Example」
- 「Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management」中的第 I部分「Oracle Solaris Resource Management」

配置 IPsec 和 IKE

IPsec 和 IKE 會保護節點與使用 IPsec 和 IKE 共同配置的網路之間的網路傳輸。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: IP Services」中的第 14 章「IP Security Architecture (Overview)」
- 「Oracle Solaris Administration: IP Services」中的第 17 章「Internet Key Exchange (Overview)」
- 「Oracle Solaris Administration: IP Services」中的第 15 章「Configuring IPsec (Tasks)」
- 「Oracle Solaris Administration: IP Services」中的第 18 章「Configuring IKE (Tasks)」

配置 IP 篩選器

IP 篩選器功能會提供防火牆。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: IP Services」中的第 20 章「IP Filter in Oracle Solaris (Overview)」
- 「Oracle Solaris Administration: IP Services」中的第 21 章「IP Filter (Tasks)」

配置 Kerberos

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。身爲 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：

- 「Oracle Solaris Administration: Security Services」中的第 20 章「Planning for the Kerberos Service」
- 「Oracle Solaris Administration: Security Services」中的第 21 章「Configuring the Kerberos Service (Tasks)」
- 選取的線上手冊包括「`kadmin(1M)` 線上手冊」、「`pam_krb5(5)` 線上手冊」和「`kclient(1M)` 線上手冊」。

新增 SMF 至原來的服務

您可以藉由新增應用程式至 Oracle Solaris 的服務管理設備 (SMF) 功能，爲信任的使用者或角色限制應用程式配置。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: Security Services」中的「How to Add RBAC Properties to Legacy Applications」
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`)。
- 選取的線上手冊包含「`smf(5)` 線上手冊」、「`smf_security(5)` 線上手冊」、「`svcadm(1M)` 線上手冊」及「`svccfg(1M)` 線上手冊」。

建立系統 BART 快照

在配置系統之後，您可以建立一個或多個 BART 清單。這些清單會提供系統快照。然後，您就可以排程一般快照和比較。如需更多資訊，請參閱第 45 頁的「使用基本稽核報告工具」。

新增多層級 (標示) 安全性

Trusted Extensions 會藉由強制執行強制性存取控制 (MAC) 策略擴充 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) 之間的關係爲基礎，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：

- 標示網路
- 標籤感知檔案系統的裝載和共用
- 標示桌面
- 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

`group/feature/trusted-desktop` 套裝軟體提供 Oracle Solaris 多層級及信任的桌面環境。

配置 Trusted Extensions

您必須先安裝 Trusted Extensions 套裝軟體，然後再配置系統。安裝套裝軟體之後，系統就可以使用直接連接的點陣式顯示來執行桌面，例如膝上型電腦或工作站。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」

配置標示 IPsec

您可以使用 IPsec 保護標示封包。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: IP Services」中的第 14 章「IP Security Architecture (Overview)」
- 「Trusted Extensions Configuration and Administration」中的「Administration of Labeled IPsec」
- 「Trusted Extensions Configuration and Administration」中的「Configuring Labeled IPsec (Task Map)」

◆ ◆ ◆ 第 3 章

3 監視和維護 Oracle Solaris 11 安全性

Oracle Solaris 提供兩種監視安全性的系統工具：基本稽核報告工具 (BART) 功能和稽核服務。個別的程式與應用程式也可以建立存取和使用記錄。

使用基本稽核報告工具

BART 清單會提供一份系統安裝項目的靜態記錄。隨著時間和系統的改變，您可以比較 BART 清單，追蹤已安裝系統的變更與系統間的差異。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: Security Services」中的「BART (Overview)」
- 「Oracle Solaris Administration: Security Services」中的「Using BART (Tasks)」
- 「Oracle Solaris Administration: Security Services」中的「BART Manifests, Rules Files, and Reports (Reference)」

如需追蹤已安裝系統之變更的特定說明，請參閱「Oracle Solaris Administration: Security Services」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資訊，請參閱「Oracle Solaris Administration: Security Services」中的第 VII部分「Auditing in Oracle Solaris」。

- 「Oracle Solaris Administration: Security Services」中的第 26 章「Auditing (Overview)」
- 「Oracle Solaris Administration: Security Services」中的第 27 章「Planning for Auditing」
- 「Oracle Solaris Administration: Security Services」中的第 28 章「Managing Auditing (Tasks)」
- 「Oracle Solaris Administration: Security Services」中的第 29 章「Auditing (Reference)」

  如需這些資訊之線上手冊和連結的清單，請參閱「Oracle Solaris Administration: Security Services」中的「Audit Service Man Pages」。

若要符合您的網站需求，下列稽核服務程序可能會有幫助：

- 建立個別的角色來配置稽核、審閱稽核以及啓動和停止稽核服務。

  使用稽核配置、稽核審閱以及稽核控制權限設定檔，做爲您角色的基礎。

  若要建立角色，請參閱「Oracle Solaris Administration: Security Services」中的「How to Create a Role」。
- 監視 `syslog` 公用程式中稽核事件的文字摘要。

  啓動 `audit_syslog` 外掛程式，然後監視報告的事件。

  請參閱「Oracle Solaris Administration: Security Services」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` 屬性設爲可用的大小。考慮其他因素中的審閱排程、磁碟空間以及 `cron` 工作頻率。

  例如，請參閱「Oracle Solaris Administration: Security Services」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 池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。

監視 audit_syslog 稽核摘要

`audit_syslog` 外掛程式可以讓您記錄預先選取之稽核事件的摘要。

您可以在執行與下列類似的指令時，於終端機視窗中顯示產生的稽核摘要：

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

審閱和歸檔稽核記錄

您可以用文字格式或在瀏覽器中以 XML 格式檢視稽核記錄。

如需相關資訊和程序，請參閱：

- 「Oracle Solaris Administration: Security Services」中的「Audit Logs」
- 「Oracle Solaris Administration: Security Services」中的「How to Prevent Audit Trail Overflow」
- 「Oracle Solaris Administration: Security Services」中的「Managing Audit Records on Local Systems (Tasks)」

尋找惡意檔案

您可以尋找可能對程式未授權使用 `setuid` 和 `setgid` 權限的情形。可疑的可執行檔會將所有權授與使用者，而非系統帳戶，例如 `root` 或 `bin`。

如需程序和範例，請參閱「Oracle Solaris Administration: Security Services」中的「How to Find Files With Special File Permissions」。

◆ ◆ ◆ 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 作業系統中包含一些實用的安全性資訊，但有些資訊已經過時。

Oracle Solaris 11 參考資料

下列書籍和文章含有關於 Oracle Solaris 11 系統安全性的描述。

- 「Oracle Solaris Administration: Security Services」

  此安全性指南是 Oracle 專爲 Oracle Solaris 11 管理員所發行。此指南說明 Oracle Solaris 的安全性功能，以及配置系統時如何使用這些功能。前言包含其他可能含有安全性資訊之 Oracle Solaris 系統管理員指南的連結。

- Oracle Solaris Security: Oracle Solaris Express (`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)

  此文章提供 Oracle Solaris 安全性功能的快照 (爲此發行版本 2010 年 11 月的版本)。

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  此文章提供 Oracle Solaris 功能的快照 (爲此發行版本 2010 年 11 月的版本)。

如需可能有用的 Oracle Solaris 10 參考資料，請參閱「Oracle Solaris 10 Security Guidelines」。