Oracle® Solaris 10 安全性指導方針

文件號碼：E38846–02
2013 年 6 月

ORACLE

130702@25097

目錄

前言

本指南提供 Oracle Solaris 作業系統 (Oracle Solaris 作業系統) 安全性指導方針的指標和描述。系統強化參考說明如何強化 Oracle Solaris 10 系統，以及如何使用 Oracle Solaris 安全性功能保護您的資料和應用程式。您可以針對您的網站安全性政策修改這些參考中的建議。

此外，本指南提供有關 Oracle Solaris 安全性背景資訊的指標，以及可引導您完成一般實作的白皮書。

對象

「Oracle Solaris 10 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
- 實作軟體安全性政策
- 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。

利用 Oracle 客戶服務部

Oracle 客戶可以透過 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。

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 作業系統中所含與 shell 有關的 UNIX 系統提示及超級使用者提示。在指令範例中，Shell 提示會指示應由一般使用者或擁有權限的使用者來執行指令。

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 10 安全性指導方針

Oracle Solaris 10 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 10 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 10 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 10 系統強化參考

下列兩份文件說明如何強化 Oracle Solaris、如何在新增應用程式和使用者到系統時使用安全性功能配置您的系統以確保作業的安全性，以及如何使用特殊的安全性功能保護網路應用系統。每份文件標題都附有簡短描述。

- CIS Solaris 10 Benchmark v5.0.0 (`http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500`)，2010 年 7 月 9 日。

  本文件的另一個名稱爲「Solaris 10 11/06 至 10/09 的安全配置基準」。此標準是許多參與者超過七年努力的成果，這些參與者包括 Oracle、Defense Information Systems Agency (DISA)、Center for Internet Security (CIS)、National Institute of Standards and Technology (NIST)、National Security Agency (NSA)，以及許多個別企業、學術機構和個人。 此標準建立一組 Oracle、CIS、NSA 和 DISA 同意的基準強化指導方針。

- An Overview of Oracle Solaris 10 Security Controls (`http://www.oracle.com/technetwork/server-storage/solaris/documentation/o11-076-s10-cis-appendix-487450.pdf`)，Glenn Brunette，2011 年 9 月。

  此「Solaris 10 11/06 至 10/09 的安全配置基準」附錄著重在系統強化和安全性配置驗證領域外的 Oracle Solaris 10 安全性控制。此附錄提供安全性功能及 Oracle Solaris 10 功能的完整簡介，並視需要提供特定的建議。

Oracle Solaris 10 的其他安全性參考

下列指南和文章提供上述區段的系統強化指導方針補充說明：

- 「System Administration Guide: Security Services」

  此安全性指南是 Oracle 專爲 Oracle Solaris 10 管理員所發行。此指南說明 Oracle Solaris 10 作業系統的安全性功能，以及配置系統時如何使用這些功能。與「Solaris 10 11/06 至 10/09 的安全配置基準」不同，此指南並不是針對系統強化或最佳做法所設計的文件。

- 「Solaris 10 安全性基本資訊」，Oracle 工程師，2009 年。ISBN 978-0137012336

  Solaris 工程師和技術文件作者提供 12 種 Solaris 安全性技術的說明，並在本書提供範例。與「Solaris 10 11/06 至 10/09 的安全配置基準」不同， 此指南並不是針對系統強化或最佳做法所設計的文件。

- 「Using Oracle® Solaris 10 to Overcome Security Challenges (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf`)」，2010 年 8 月。

  此 Oracle 白皮書的目標對象是需要完整系統安全性功能的組織。需要針對電腦安全性提供高效能與高效率解決方案的 IT 部門，可以使用 Oracle Solaris 10 獨特且強大的安全性功能，保護企業免於潛在威脅、符合公司和法規要求，以及克服安全性挑戰。此白皮書提供 Oracle Solaris 安全性功能的高階說明。這不是針對系統強化或最佳做法所設計的文件。