# Oracle® Solaris 11.2 安全性規範指南

文件號碼： E53941
2014 年 7 月

ORACLE

# 目錄

# 使用本文件

- **簡介** – 說明如何評估與報告 Oracle Solaris 系統符合指定之安全性基準規範的程度。
- **對象** – 評估 Oracle Solaris 11 系統安全性的安全性管理員和稽核人員。
- **必備知識** – 網站安全性需求。

## 產品文件庫

文件庫中含有關於本產品的最新資訊和已知問題，網址為 http://www.oracle.com/pls/topic/lookup?ctx=E56345。

## 存取 Oracle 支援

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 報告遵循安全性標準規範的情形

本章說明如何評估與報告 Oracle Solaris 系統遵循安全性標準 (亦稱為安全性基準和安全性原則) 規範的情形。本章包含以下主題：



## 關於規範

符合安全性標準的系統可提供較為安全的運算環境，同時也較易於測試、維護及保護。在本發行版本中，Oracle Solaris 提供程序檔來評估與報告 Oracle Solaris 系統遵循兩種安全性基準的程度，包括 Solaris 安全性基準及支付卡產業資料安全標準 (PCI DSS)。

驗證配置以支援系統符合外部和內部安全性原則的規範遵循情形非常重要。處理安全性規範及稽核需求佔 IT 安全性支出很大的比例，包括文件、報告及驗證本身。銀行、醫院及政府之類的組織具有特殊的規範需求。不熟悉作業系統的稽核人員可能難以讓安全性控制符合需求。因此，對應安全性控制與需求的工具可以輔助稽核人員，減少時間和成本。

規範程序檔是根據「安全內容自動化協定 (Security Content Automation Protocol，SCAP)」，使用「開放性弱點和評估語言 (Open Vulnerability and Assessment Language，OVAL)」撰寫。Oracle Solaris 中的 SCAP 實作同時支援符合「程序檔檢查引擎 (Script Check Engine，SCE)」的程序檔。這些程序檔可新增目前 OVAL 綱要和探測器不提供的安全性檢查。其他程序檔可用來符合其他管制環境標準，例如 Gramm-Leach-Bliley Act (GLBA)、Health Insurance Portability and Accountability Act (HIPAA)、Sarbanes Oxley (SOX) 及 Federal Information Security Management Act (FISMA)。如需這些標準的連結，請參閱第 12 頁的「規範參考資料」。

# Oracle Solaris 安全性基準

Oracle Solaris 11 提供兩種標準的規範程序檔，Solaris 與 PCI DSS。

## Solaris 安全性原則基準

Solaris 安全性原則基準是以 Oracle Solaris 之「預設為安全 (SBD)」的預設安裝為基礎的標準。此基準提供兩種設定檔，基準線和建議。這些設定檔詳述於第 8 頁的「規範評量」。

構成 SBD 的功能詳述於「Securing Systems and Attached Devices in Oracle Solaris 11.2 」中的「Using the Secure by Default Configuration」及「Oracle Solaris 11 安全性準則 」中的「Oracle Solaris 可配置安全性」。

這些基準並無法滿足 Oracle Solaris 之 PCI DSS、Center for Internet Security (CIS) 或 Defense Information Systems Agency-Security Technical Information Guides (DISA-STIG) 基準的需求。

## PCI DSS 安全性原則基準

PCI DSS 安全性原則基準是處理持卡人資訊 (主要是簽帳卡和信用卡) 之組織的所有權資訊安全性標準。此標準是由支付卡產業安全標準委員會 (Payment Card Industry Security Standards Council) 所定義。目的是減少信用卡詐騙事件。

必須配置 Oracle Solaris 系統，使其符合 PCI DSS 標準。規範報告會指出那些測試失敗、那些測試通過，並提供修補步驟。

# 規範評量

若要評量安全性規範 (以下稱為規範)，需要有安全性基準或設定檔、對於該基準的規範評量 (稱之為評估)，接著是發現項目的報告。此報告亦可以指南形式例印，以供訓練或存檔之用。

Oracle Solaris 提供評量 Solaris 基準下之兩種安全性設定檔的程序檔。

- Solaris 基準的「基準線」設定檔最符合 Oracle Solaris 的預設 SBD 安裝。
- Solaris「建議」設定檔則可滿足使用較「基準線」設定檔嚴格之安全性需求的組織。

  這些設定檔具有巢狀關係。符合「建議」設定檔的系統可符合「基準線」設定檔。

PCI DSS 基準可評量您的系統遵循 PCI DSS 標準規範的情形。因為 PCI DSS 需求沒有直接的程式碼連結，您必須檢驗規範報告。如需詳細資訊，請參閱 Meeting PCI DSS Compliance with Oracle Solaris 11。

### `compliance` 套裝軟體

規範功能可從 `pkg:/security/compliance` 套裝軟體取得，此套裝軟體已隨 `solaris-small-server` 和 `solaris-large-server` 套裝軟體群組一併安裝。

- 如需有關套裝軟體群組的資訊，請參閱「Oracle Solaris 11 安全性準則 」中的「安裝 Oracle Solaris OS」。
- 如需有關套裝軟體的資訊，請參閱 「Oracle Solaris 11.2 Package Group Lists 」。
- 若要顯示 compliance 套裝軟體的說明，請使用 `pkg info compliance` 指令。

## Oracle Solaris 規範評估

`compliance` 指令是用來評估與報告系統遵循已知基準規範的情形。Oracle Solaris compliance 指令將基準的需求對應至檢驗對特定需求規範的程式碼、檔案或指令輸出。如需有關此指令的資訊，請參閱 `compliance(1M)` 線上手冊。

如需有關支援 `compliance` 指令之 SCAP 工具集的資訊，請參閱 `oscap`(8) 線上手冊。若要顯示 SCAP 工具集的版本，請使用 `oscap -V` 指令。

---

注意 - SCAP 工具集無法將 `oscap` 指令產生的報告本土化，也無法將測試描述本土化。(本土化意指將軟體翻譯為本地語言。)

---

## 第三方規範評估

CIS 第三方標準組織提供針對其基準的自動化規範檢查工具。您可以洽詢 CIS，判斷使用這些工具來評估遵循 CIS 基準規範程度所需的成本。CIS 工具可在 Microsoft Windows 系統上使用，以用於檢查 Oracle Solaris 規範。

# 評估 Oracle Solaris 規範

`compliance` 指令可自動化規範評估，而不是修補。此指令是用來列出、產生以及刪除評估和報告。任何使用者均可存取規範報告。若要管理評估及產生報告則需要權限。如需詳細資訊，請參閱 `compliance(1M)` 線上手冊。

compliance 指令僅能檢查本機檔案。如果您的系統掛載檔案系統，則必須分別測試用戶端和伺服器的規範。例如，如果您從中央伺服器掛載使用者個人目錄，請在使用者系統和匯出該個人目錄的每個伺服器上執行 compliance 指令。

## 執行 compliance 指令的權限

Oracle Solaris 提供兩個權限設定檔來處理規範評估和報告產生作業。

- Compliance Assessor 權限設定檔可讓使用者執行評估、將評估放置在評估存放區、產生報告以及從存放區刪除評估。
- Compliance Reporter 權限設定檔可讓使用者從現有的評估產生新的報告。

compliance 子指令需要下列權限：

- compliance assess 指令 – 需要所有權限，及 solaris.compliance.assess 授權。Compliance Assessor 權限設定檔提供這些權限。
- compliance delete 指令 – 需要評估存放區的寫入存取權，及 solaris.compliance.assess 授權。Compliance Assessor 權限設定檔提供這些權限。
- compliance list 指令 – 具備基本權限的任何人均可執行。此指令提供基準和評估的完整顯示。
- compliance report 指令 – 任何人均可執行，但會根據使用者權限而有不同的功能範圍。受指派 Compliance Assessor 或 Compliance Reporter 設定檔的使用者，可以在評估存放區中產生新的報告。所有使用者均可檢視現有的報告，但僅具備基本權限的使用者則無法產生報告。

## 建立規範評估和報告

已完成規範評估。報告可以包含評估中的每個項目，或是包含評估中某項資訊的子集。定期執行評估，例如使其成為 cron 工作，以監督您系統遵循規範的情形。

### ▼ 如何執行規範報告

依照預設，solaris-small-server 和 solaris-large-server 套裝軟體包含 compliance 套裝軟體。solaris-desktop 和 solaris-minimal 套裝軟體並不包含 compliance 套裝軟體。

開始之前 您必須受指派 Software Installation 權限設定檔才能在系統新增套裝軟體。您必須受指派大部分 compliance 指令的管理權限，如第 10 頁的「執行 compliance 指令的權限」中所述。如需詳細資訊，請參閱「Securing Users and Processes in Oracle Solaris 11.2 」中的「Using Your Assigned Administrative Rights」。

1. 安裝 **compliance** 套裝軟體。

```
# pkg install compliance
```

下列訊息指示已安裝此套裝軟體：

```
No updates necessary for this image.
```

如需詳細資訊，請參閱 pkg(1) 線上手冊。

---

注意 - 在您計畫執行規範測試的每個區域中安裝此套裝軟體。

---

2. 建立評估。

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
 No assessments available
# compliance -p profile -a assessment-directory
```

-p 指示設定檔的名稱。設定檔名稱有區分大小寫。

-a 指示評估的目錄名稱。預設名稱包含時戳。

例如，下列指令會建立使用「建議」設定檔的評估。

```
# compliance -p Recommended -a recommended
```

此指令會在 /var/share/compliance/assessments 中建立名為 recommended 的目錄，並在其中包含評估 (使用三種檔案：記錄檔案、XML 檔案及 HTML 檔案)。

```
# cd /var/share/compliance/assessments/recommended
# ls
recommended.html
recommended.txt
recommended.xml
```

如果再次執行此指令，並不會取代這些檔案。在重複使用評估某個目錄之前，您必須先移除這些檔案。

3. (選用) 建立自訂報告。

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

此指令會使用 HTML 格式，建立包含失敗和未選取之項目的報告。此報告是根據最近的評估來執行。

您可以重複執行自訂報告。不過，您只能在原始目錄中執行一次完整報告，亦即評估。

4. 檢視完整報告。

您可以在文字編輯器中檢視記錄檔案、在瀏覽器中檢視 HTML 檔案，或是在 XML 檢視器中檢視 XML 檔案。

例如，若要從前面的步驟檢視自訂 HTML 報告，請輸入下列瀏覽器項目：

```
file:///var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

5. 修正必須通過安全性原則的任何失敗。

   a. 完成失敗項目的修正。

   b. 如果修正包括重新啟動系統，請在再次執行評估之前重新啟動系統。

6. (選用) 以 **cron** 工作的方式執行 **compliance** 指令。

   ```
   # cron -e
   ```

   如需在每天上午 2:30 執行規範評估，root 便需新增下列項目：

   ```
   30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
   ```

   如需在每週星期天上午 1:15 執行規範評估，root 便需新增下列項目：

   ```
   15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
   ```

   如需在每月 1 日上午 4:00 執行評估，root 便需新增下列項目：

   ```
   0 4 1 * * /usr/bin/compliance assess -b pci-dss
   ```

   如需在每月第一個星期一上午 3:45 執行評估，root 便需新增下列項目：

   ```
   45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
   ```

7. (選用) 針對在您系統上安裝的部分或所有基準建立指南。

   ```
   # compliance guide -a
   ```

   指南包含每項安全性檢查的說明及修正失敗檢查的步驟。指南對於訓練及作為未來測試的準則而言非常有用。依照預設，在安裝時便會建立每個安全性設定檔的指南。如果您新增或變更某基準，您可能會建立新的指南。

# 規範參考資料

電腦安全性規範區域會假設您熟悉許多標準、縮寫及處理程序。為了讓您方便運用，提供下列名詞和參考資料清單。

下列程式實作規範評估和報告：

- 安全內容自動化協定 (Security Content Automation Protocol，SCAP)

- SCAP 工具 (OpenSCAP)
- 開放性弱點和評估語言 (Open Vulnerability and Assessment Language，OVAL)
- 可擴展配置檢查清單描述格式 (eXtensible Configuration Checklist Description Format，XCCDF)

下列主體提供規範標準或法律：

- 網際網路安全中心 (Center for Internet Security，CIS)
- 聯邦資訊安全管理法 (Federal Information Security Management Act，FISMA)
- 金融服務業現代化法案 (Gramm-Leach-Bliley Act，GLBA)
- 健康保險可攜性與責任法案 (Health Insurance Portability and Accountability Act，HIPAA)
- 支付卡產業資料安全標準 (Payment Card Industry-Data Security Standard，PCI DSS)
- 沙賓法案 (Sarbanes Oxley，SOX)