SPARC T8 系列伺服器安全指南

文件號碼： **E91706-01**
2017 年 9 月

文件號碼： E91706-01

說明文件協助工具

如需有關 Oracle 對於協助工具的承諾資訊，請瀏覽 Oracle Accessibility Program 網站，網址為 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

存取 Oracle 支援

已經購買客戶支援的Oracle 客戶可從 My Oracle Support 取得網路支援。如需資訊，請瀏覽 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如您有聽力障礙，請瀏覽 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

目錄

瞭解硬體安全 7
存取限制 7
序號 7
硬碟 8

瞭解軟體安全 9
▼ 防止未經授權的存取 (Oracle Solaris 作業系統) 9
▼ 防止未經授權的存取 (Oracle ILOM) 9
▼ 防止未經授權的存取 (Oracle VM Server for SPARC) 9
限制存取 (OpenBoot) 10
▼ 實作密碼保護 10
▼ 啟用安全模式 10
▼ 停用安全模式 11
▼ 查看失敗的登入 11
▼ 提供開啟電源系統資訊 12
Oracle 系統韌體 12
安全的 WAN Boot 12

瞭解硬體安全

您的安全架構必須建立在實體隔離和存取控制的基礎上。確實將實體伺服器安置在安全的環境中，保護伺服器免於未經授權的接觸使用。同樣地，記錄所有序號有助於避免硬體遭到竊取、轉售或承擔供應鏈風險 (亦即，盜版或偽造的元件流入組織供應鏈的情況)。

下列小節提供 SPARC T8-1、T8-2 與 T8-4 伺服器的一般硬體安全準則。

- 「存取限制」[7]
- 「序號」[7]
- 「硬碟」[8]

存取限制

- 將伺服器及相關設備安置在上鎖且限制人員進出的房間內。
- 如果設備安置在有門可以上鎖的機架內，除非必須維護或操作機架內的元件，否則請讓機架門隨時保持上鎖狀態。將門上鎖也可以有效限制熱插式或熱抽換式裝置的使用。
- 將備用的現場可更換單元 (FRU) 或客戶可更換單元 (CRU) 存放在上鎖的機櫃中。限制只有獲得授權的人員才能使用上鎖的機櫃。
- 定期檢查機架鎖和備用機櫃鎖是否確實上鎖且未受損，以避免 (或察覺) 鎖被人破壞或不小心未將門鎖上的情況。
- 將機櫃鑰匙放置在限制人員進出的安全位置。
- 限制使用 USB 主控台。系統控制器、電源分配器 (PDU) 及網路交換器等裝置都具有 USB 連線。實際取用元件是較為安全的存取方法，因為比較不易受到網路攻擊。
- 將主控台連線外部 KVM 以啟用遠端主控台存取。KVM 裝置通常支援雙因素認證、集中式存取控制及稽核功能。如需有關 KVM 之安全準則和最佳措施的詳細資訊，請參閱 KVM 裝置提供的文件。

序號

- 記錄所有硬體的序號。

- 為所有重要的電腦硬體項目 (例如替換零件) 加上安全標誌。使用特殊的紫外線筆或浮水印標籤來加註安全標誌。
- 將硬體啟動金鑰與授權文件存放在安全的位置。發生系統緊急狀況時，系統管理人員必須能夠方便取用。書面文件可能會是擁有權的唯一證明。

無線電頻率識別 (RFID) 讀取器可進一步簡化資產的追蹤。您可以從下列網址取得「如何使用 *RFID* 追蹤您的 *Oracle Sun* 系統資產」Oracle 白皮書：

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

硬碟

硬碟經常用來儲存機密資訊。如果要防止此資訊受到未經授權的存取，硬碟在重新使用、退役或丟棄之前必須先經妥善處理。

- 您可以使用磁碟清除工具 (例如 Oracle Solarisformat(1M) 指令) 來徹底清除磁碟機上的所有資料。
- 組織應參考其資料保護政策，以判斷最適當的硬碟處理方式。
- 如有需要，請利用 Oracle 的 Customer Data and Device Retention 服務

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

瞭解軟體安全

大部分硬體安全性是透過軟體的方式來實作。下列小節提供 SPARC T8-1、T8-2 以及 SPARC T8-4 伺服器的一般軟體安全準則。

- 「防止未經授權的存取 (Oracle Solaris 作業系統)」[9]
- 「防止未經授權的存取 (Oracle ILOM)」[9]
- 「防止未經授權的存取 (Oracle VM Server for SPARC)」[9]
- 「限制存取 (OpenBoot)」[10]
- 「Oracle 系統韌體」[12]
- 「安全的 WAN Boot」[12]

▼ 防止未經授權的存取 (Oracle Solaris 作業系統)

- **使用 Oracle Solaris 作業系統指令可以限制對 Oracle Solaris 軟體的存取，並能強化作業系統、使用安全性功能以及保護應用程式。**

  您可以從下列網址取得您正在使用之版本的 *Oracle Solaris* 安全性準則文件：

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ 防止未經授權的存取 (Oracle ILOM)

- **使用 Oracle ILOM 指令可以限制對 Oracle ILOM 軟體的存取、變更出廠設定密碼、限制使用 root 超級使用者帳號，並保護服務處理器的專用網路。**

  您可以從下列網址取得 *Oracle ILOM* 安全指南：

  `http://www.oracle.com/goto/ilom/docs`

▼ 防止未經授權的存取 (Oracle VM Server for SPARC)

- **使用 Oracle VM for SPARC 指令可以限制對 Oracle VM for SPARC 軟體的存取。**

  您可以從下列網址取得 *Oracle VM for SPARC* 安全指南：

http://www.oracle.com/goto/vm-sparc/docs

限制存取 (OpenBoot)

這些主題描述如何在 OpenBoot 提示符號限制存取。

- 「實作密碼保護」[10]
- 「啟用安全模式」[10]
- 「停用安全模式」[11]
- 「查看失敗的登入」[11]
- 「提供開啟電源系統資訊」[12]

如需設定 OpenBoot 安全變數的相關資訊，請參閱 OpenBoot 文件，網址如下：

http://www.oracle.com/goto/openboot/docs

▼ 實作密碼保護

- **如果您尚未設定密碼，請執行此步驟。**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

密碼可以有 1 到 8 個字元。如果您輸入超過 8 個字元，將只使用前 8 個字元。可以使用所有可列印的字元。不接受控制字元。

注意 - 若將密碼設為零個字元，便會關閉安全模式並將 `security-mode` 參數視為設成 `none`。不過，這不會變更設定。

▼ 啟用安全模式

1. **將 `security-mode` 參數設為 `full` 或 `command`。**

   設為 `full` 時，必須輸入密碼才能執行任何動作 (包括 `boot` 等一般作業)。設為 `command` 時，無須輸入密碼即可執行 `boot` 或 `go` 指令，但執行其他所有指令均必須輸入密碼。基於業務連續性的考量，請依照下列範例將 `security-mode` 參數設為 `command`。

   ```
   {0} ok setenv security-mode command
   {0} ok
   ```

2. **取得安全模式提示符號。**

依上述方式設定安全模式之後，有兩種方法可取得安全模式提示符號。

注意 - 當主機主控台啟動時，會將 HUP 傳送到主控台。如果在 OpenBoot 中設定 `security-mode`，HUP 將會導致登出動作。因此，當主機主控台重新啟動時，使用者需要登入才能看到 OpenBoot OK 提示符號。

- **使用 `logout` 和 `login` 文字。**

```
{0} ok logout
Type boot , go (continue), or login (command mode)
>
> login
Firmware Password: password
Type help for more information
{0} ok
```

若要退出安全模式，請使用 `logout` 和 `login` 的名稱，如範例所示。

- **使用 `reset-all` 文字。**

```
{0} ok reset-all
```

這個字會將系統重設。當系統重新啟動之後，OpenBoot 就會進入安全模式提示符號。若要重新登入指令提示符號 (或登出安全模式)，請使用 `logout` 和 `login` 的名稱，然後輸入密碼，如上所述。

▼ 停用安全模式

1. **將 `security-mode` 參數設為 `none`。**

```
{0} ok setenv security-mode none
```

2. **在這兩個密碼提示符號後面按下 Return 鍵，即可將密碼長度設為零。**

▼ 查看失敗的登入

1. **請依照下列範例，使用 `security-#badlogins` 參數判斷是否有失敗的 OpenBoot 環境存取嘗試。**

```
{0} ok printenv security-#badlogins
```

如果此指令傳回任何大於 Ø 的值，則代表記錄了失敗的 OpenBoot 環境存取嘗試。

2. **鍵入此指令即可重設參數。**

```
{0} ok setenv security-#badlogins 0
```

▼ 提供開啟電源系統資訊

儘管這並不是直接的預防或偵測控制措施，您仍可基於下列原因來運用系統資訊：

- 傳達擁有權。
- 對使用者顯示伺服器的合理使用警告。
- 說明只有獲得授權的人員才能夠存取或修改 OpenBoot 參數。

- **請使用下列指令來啟用自訂警告訊息。**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

系統資訊訊息的長度上限為 68 個字元。可以使用所有可列印的字元。

Oracle 系統韌體

Oracle 系統韌體使用一個受控制的更新處理作業來防止未經授權的修改。只有超級使用者或具備適當授權的認證使用者才能使用更新處理作業。

如需取得最新更新或修補程式之方式的相關資訊，請參閱您伺服器的產品注意事項。

安全的 WAN Boot

WAN Boot 支援多種安全等級。您可以組合 WAN Boot 中支援的安全功能來滿足不同的網路需求。雖然更安全的組態需要更多的管理，但是也會顯著增加系統資料的安全性。

- 若為 Oracle Solaris 10 作業系統，請參閱 *Oracle Solaris Installation Guide: Network-Based Installations* 一書中，關於安全的 WAN Boot 安裝組態資訊。
- 若為 Oracle Solaris 11 作業系統，請參閱 Installing Oracle Solaris 11.3 Systems。