SPARC 與 Netra SPARC T5 系列伺服器

安全指南

文件號碼： E40479-01
2013 年 4 月

目錄

1. SPARC 與 Netra SPARC T5 系列伺服器安全 5
瞭解安全原則 5
規劃安全環境 6
硬體安全 6
軟體安全 6
韌體安全 7
Oracle OpenBoot 安全 7
Oracle ILOM 韌體 7
維護安全的環境 7
硬體控制 7
資產追蹤 7
軟體和韌體的更新 8
本機與遠端存取 8
資料安全 8
網路安全 8

• • • 第 1 章

SPARC 與 Netra SPARC T5 系列伺服器安全

本文件提供 SPARC T5-1B、T5-2、T5-4、T5-8 及 Netra SPARC T5-1B 伺服器的一般安全指導方針。當您使用這些伺服器搭配網路交換器與網路介面卡等其他 Oracle 硬體產品時，此指南可協助您確保安全性。

本章涵蓋下列各節：

- 第 5 頁的「瞭解安全原則」
- 第 6 頁的「規劃安全環境」
- 第 7 頁的「維護安全的環境」

瞭解安全原則

有四項基本安全性原則：存取、認證、授權及資料記錄。

- **存取**

  實體與軟體控制可保護您的硬體或資料避免遭受入侵。
  - 若為硬體，存取限制通常是指實體存取限制。
  - 若為軟體，則是透過實體和虛擬方式限制存取。
  - 韌體只能透過 Oracle 更新程序變更。
- **認證**

  所有平台作業系統均提供認證功能，可設定此功能來確認使用者的身分是否真實無誤。

  認證會透過識別證與密碼等方法，提供各種等級的安全性。
- **授權**

  授權僅允許受過訓練並符合使用資格的公司員工使用相應的硬體及軟體。設定系統的「讀取」、「寫入」和「執行」權限，以控制使用者對指令、磁碟空間、裝置及應用程式的存取。
- **資料記錄**

  使用 Oracle 軟體和硬體資料記錄功能，監視登入活動以及維護硬體資產。
  - 可透過系統記錄來監視使用者登入。尤其是「系統管理員」及「服務」帳號，可存取功能強大的指令，故應透過系統記錄謹慎監視。記錄通常會保留一段很長的時間，因此請務必定期汰換記錄檔，以符合客戶公司原則。

- 客戶 IT 資產通常透過序號進行追蹤。所有介面卡、模組及主機板都有 Oracle 零件編號的電子記錄，可用於庫存管理。

規劃安全環境

安裝與配置伺服器及相關設備之前和期間，請使用下列注意事項。

硬體安全

限制對於硬體的存取並記錄序號，即可非常輕易地達到保護實體硬體的效果。

- **限制存取**
  - 將伺服器及相關設備安裝在上鎖並限制人員進出的房間內。
  - 如果設備安裝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，否則請將機架門隨時保持上鎖。
  - 限制使用 USB 主控台，它們可以提供比 SSH 連線更強大的存取功能。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。
  - 要限制使用熱插式或熱抽換式裝置，因為這些裝置非常容易移除。
  - 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。
- **記錄序號**
  - 保留所有硬體的序號記錄。
  - 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輕易地存取此位置。書面文件可能將成為擁有權的唯一證明。

軟體安全

大部分硬體安全性是透過軟體的方式來實作。

- 安裝新系統之後，請變更所有預設的密碼。多數類型的設備都是使用很多人都知道的預設密碼 (例如 changeme)，所以可能會讓他人得以在未經授權的情況下使用設備。此外，例如網路交換器等裝置，預設可有多個使用者帳號。請務必變更所有帳號密碼。
- 限制使用 `root` 超級使用者帳號。儘可能改為使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 使用者設定檔，例如，`operator` 與 `administrator`。
- 讓服務處理器使用專用的網路，與一般網路分開。
- 參考軟體隨附的文件，啟用軟體提供的安全性功能。
- 使用 WAN Boot 或 iSCSI Boot 可安全地啟動伺服器。
  - 若為 Oracle Solaris 10 發行版本，請參閱 *Oracle Solaris Installation Guide: Network-Based Installations* 一書
  - 若為 Oracle Solaris 11 發行版本，請參閱 *Installing Oracle Solaris 11 Systems* 一書瞭解 WAN Boot 資訊，以及 *System Administration Guide: Basic Administration* 一書瞭解 iSCSI Boot 資訊。

Oracle Solaris Security Guidelines 文件提供下列資訊：

- 如何強化 Oracle Solaris
- 如何在設定系統時使用 Oracle Solaris 安全保護功能

- 如何安全地將應用程式及使用者新增至系統
- 如何保護網路應用程式

您目前所使用之版本的 *Oracle Solaris Security Guidelines* 文件網址如下：

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

韌體安全

「Oracle 系統韌體」的所有子元件都只能一起進行升級。「Oracle 系統韌體」使用受控制的韌體更新處理作業，以防止未經授權的韌體修改。只有超級使用者或具備適當授權之認證的使用者才能使用更新處理作業。

Oracle OpenBoot 安全

使用 OpenBoot 安全變數，即可以密碼保護對「Oracle OpenBoot 韌體」指令行介面的存取。

如需設定 OpenBoot 安全變數的相關資訊，請參閱 *OpenBoot 4.x Command Reference Manual*，網址如下：

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM 韌體

Oracle Integrated Lights Out Manager (Oracle ILOM) 是系統管理韌體，已預先安裝在伺服器、伺服器模組、模組化系統以及其他 Oracle 硬體上。Oracle ILOM 可讓您主動管理與監視安裝在系統中的元件。您使用 Oracle ILOM 的方式會影響您系統的安全性。若要深入瞭解如何在進行設定密碼、管理使用者與套用 Secure Shell (SSH)、安全通訊端層 (SSL) 與 RADIUS 認證等安全相關功能時使用此韌體，請參閱 Oracle ILOM 文件：

- http://www.oracle.com/goto/ILOM/docs

維護安全的環境

完成初始安裝及設定後，請使用 Oracle 硬體和軟體安全性功能來繼續控制硬體及追蹤系統資源。

硬體控制

部分 Oracle 系統可設定為透過軟體指令開啟和關閉。此外，部分系統機櫃的電源分配器 (PDU) 也可透過軟體指令從遠端啟動和停止。這些指令的授權通常是在設定系統配置時所指定，而且一般僅限授權給系統管理員和服務人員。請參閱系統或機櫃文件，瞭解詳細資訊。

資產追蹤

Oracle 序號會嵌入在選項卡及系統主機板的韌體中。這些序號可透過區域網路連線讀取，以供追蹤庫存。

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 *How to Track Your Oracle Sun System Assets by Using RFID* 的 Oracle 白皮書：

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

軟體和韌體的更新

- 請定期檢查更新。
- 務必在設備上安裝最新的軟體或韌體版本。
- 安裝軟體任何必要的安全修補程式。
- 請記住，網路交換器這類的裝置也包含韌體，可能需要修補程式和韌體更新。

本機與遠端存取

請依照下列指示，保護對系統的本機和遠端存取：

- 張貼公告，禁止未經授權的存取。
- 適時使用存取控制清單。
- 對延長的階段作業設定結束時間，並設定不同的權限等級。
- 使用驗證、授權以及資料記錄 (AAA) 功能，從本機和遠端存取交換器。
- 儘可能使用 RADIUS 與 TACACS+ 安全協定：
  - RADIUS (Remote Authentication Dial In User Service) 是一種用戶端/伺服器協定，可保護網路免於未經授權的存取。
  - TACACS+ (Terminal Access Controller Access-Control System) 協定可允許遠端存取伺服器與認證伺服器溝通，以決定使用者是否能存取網路。
- 使用交換器的連接埠監視功能偵測系統入侵行為 (IDS)。
- 依據 MAC 位址實作連接埠安全性來限制存取。停用所有連接埠的自動中繼功能。
- 限制只有特定 IP 位址能使用 SSH (而非 Telnet) 執行遠端配置。Telnet 會以文字方式傳送使用者名稱及密碼，可能會讓區域網路區段上的每個人都能看到登入證明資料。為 SSH 設定更安全的密碼。
- 舊版的 SNMP 並不安全，而且會在未加密的文字中傳送認證資料。只有第 3 版的 SNMP 可提供安全傳輸。
- 部分產品出廠時已將 PUBLIC 設為預設的 SNMP 社群字串。攻擊者可以查詢社群來繪製非常完整的網路地圖，並且有可能修改管理資訊庫 (MIB) 值。如果必須使用 SNMP，請將預設的 SNMP 社群字串變更為更安全的社群字串。
- 開啟記錄功能，並將記錄傳送至專用的安全記錄主機。
- 使用 NTP 與時戳設定記錄功能，以包含正確的時間資訊。
- 複查記錄以找出可能的未預期事件，然後依據安全性原則將它們歸檔。
- 如果系統控制器是使用瀏覽器介面，使用之後請務必登出。

資料安全

請依照下列指示，以達到最高的資料安全等級：

- 使用各種裝置 (如外接式硬碟、隨身碟或記憶卡) 來備份重要的資料。將備份的資料儲存至安全的其他不同備份位置。
- 使用資料加密軟體來保護硬碟中的機密資訊。
- 報廢舊硬體時，請務必銷毀磁碟機或徹底清除磁碟機中的資料。刪除所有檔案或重新格式化磁碟機只會移除磁碟機上的位址表 - 刪除檔案或重新格式化磁碟機後，仍然可以從磁碟機還原資訊。(請使用磁碟清除軟體來徹底清除磁碟機上的所有資料。)

網路安全

請依照下列指示，讓您的網路達到最高安全等級：

- 絕大多數的交換器都可讓您定義虛擬區域網路 (VLAN)。如果您使用交換器定義 VLAN，請將重要的系統叢集與網路上的其他叢集分開。這可以降低使用者取得這些用戶端及伺服器資訊的機會。
- 管理頻外 (與資料流量分開) 交換器。如果無法執行頻外管理，請為頻內管理指定專用的 VLAN 編號。
- 保護 Infiniband 主機的安全。只有 Infiniband 主機安全，Infiniband 結構才沒有安全問題。
- 請注意，分割無法保護 Infiniband 結構。分割只會隔離主機上的虛擬機器之間的 Infiniband 流量。
- 離線保留一份交換器配置檔，並限制只有授權的管理員才可以使用。配置檔應該包含每一項設定的描述性註解。
- 如果可以，請使用靜態 VLAN 配置。
- 停用未使用的交換器連接埠，然後指定未使用的 VLAN 編號給它們。
- 將唯一的原生 VLAN 編號指定給主幹連接埠。
- 嚴格限制只有必要的 VLAN 可在主幹上傳輸。
- 如果可以，請停用「VLAN 中繼協定 (VTP)」。否則，請設定 VTP 的下列項目：管理網域、密碼和刪除。然後將 VTP 設定為通透模式。
- 停用不需要的網路服務，例如 TCP 小型伺服器或 HTTP。啟用需要的網路服務並設定這些服務的安全性。
- 不同的交換器將會提供不同的連接埠安全性功能。如果您的交換器提供下列連接埠安全性功能，請多加利用：
  - MAC 位址鎖定：這包括將一或多個連接裝置的媒體存取控制 (MAC) 位址與交換器的實體連接埠連結。如果您將交換器連接埠鎖定至特定的 MAC 位址，超級使用者就無法利用惡意存取點在您的網路中建立後門。
  - MAC 位址閉鎖：這會停用與交換器連線中的指定 MAC 位址。
  - MAC 位址學習：會使用與每一個交換器連接埠的直接連線有關的知識，交換器即可根據目前的連線設定安全性。