Oracle Hardware Management Pack 安全指南

文件號碼：E39913–01
2013 年 3 月

ORACLE

130322@25097

目錄

簡介

本節提供 Oracle Hardware Management Pack (HMP) 產品的簡介 (包括安全指南資訊)，並說明應用程式安全的一般原則。

內容涵蓋下列主題：

產品簡介

您的伺服器以及許多其他 x86 伺服器與部分 SPARC 伺服器都可以使用 Oracle Hardware Management Pack。Oracle Hardware Management Pack 有兩個重要元件：一個是 SNMP 監視代理程式，另一個是跨作業系統指令行介面工具 (CLI 工具) 系列，可用來管理您的伺服器。

您可以透過硬體管理代理程式 SNMP 外掛程式，使用 SNMP 來監視資料中心的 Oracle 伺服器和伺服器模組，而不需要連線主機和 Oracle ILOM 這兩個管理點。這項功能可以讓您使用單一 IP 位址 (主機 IP) 監視多個伺服器和伺服器模組。

硬體管理代理程式 SNMP 外掛程式是在 Oracle 伺服器的主機作業系統中執行。SNMP 外掛程式使用 Oracle Hardware Storage Access Libraries 與服務處理器溝通。硬體管理代理程式會自動擷取伺服器目前狀態的相關資訊。

您可以使用 Oracle Server CLI 工具來設定 Oracle 伺服器。CLI 工具可搭配 Oracle Solaris、Oracle Linux、Oracle VM、其他 Linux 衍生版本及 Windows 作業系統使用。下表描述可使用 CLI 工具執行的工作。

主機作業系統的系統管理工作	CLI 工具
配置 BIOS 設定、裝置開機順序以及部分服務處理器設定。	`ubiosconfig` `biosconfig`

主機作業系統的系統管理工作	CLI 工具
更新 Oracle ILOM 和 BIOS。	`fwupdate`
在支援的 SAS 儲存裝置、嵌入式 SAS 儲存控制器、SAS 儲存擴充器以及儲存磁碟上查詢、更新與驗證韌體版本。	
復原、設定與檢視 Oracle ILOM 配置設定，以及檢視與設定與網路管理、時鐘配置以及使用者管理相關的 Oracle ILOM 特性。	`ilomconfig`
在連接到 RAID 控制器 (包括儲存陣列) 的儲存磁碟上檢視或建立 RAID 磁碟區。	`raidconfig`
監視系統狀態。	`hwmgmt`

關於此安全指南

本文件提供 Oracle Hardware Management Pack 的一般安全指導方針。本指南旨在協助您確保搭配其他 Oracle 硬體產品 (如網路交換器、網路介面卡等) 使用軟體時的安全性。

內容涵蓋下列主題：

- 第 5 頁的 「簡介」
- 第 9 頁的 「Oracle Hardware Management Pack 預先安裝」
- 第 11 頁的 「Oracle Hardware Management Pack 安裝」
- 第 13 頁的 「Oracle Hardware Management Pack 後續安裝」

基本安全原則

有四項安全性原則：存取、認證、授權及資料記錄。

- 存取

  透過實體及軟體控制，保護您的硬體或資料避免遭到入侵。

  - 若爲硬體，存取限制通常是指實體存取限制。
  - 若爲軟體，存取限制通常是指透過實體和虛擬兩種方式。
  - 韌體只能透過 Oracle 更新程序變更。

- 認證

  設定所有認證功能 (例如平台作業系統中的密碼系統功能) 來確認使用者的身分是否眞實無誤。

  認證會透過識別證與密碼等方法，提供各種等級的安全性。例如，確認工作人員需正確配戴識別證才能進入電腦機房。

- 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。

例如，設定系統的讀取/寫入/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

  客戶 IT 人員可使用 Oracle 軟體和硬體功能，監視登入活動以及維護硬體資產。

  - 使用系統記錄來監視使用者登入。尤其是透過系統記錄追蹤系統管理員及服務帳號，因爲這些帳號可以存取功能強大的指令。
  - 當記錄檔超過合理的大小時，請定期汰換記錄檔，以符合客戶公司原則。記錄通常會保留一段很長的時間，因此請務必善加維護。
  - 使用元件序號來追蹤系統資產，以供庫存管理之用。所有介面卡、模組及主機板都有 Oracle 零件編號的電子記錄。

Oracle Hardware Management Pack 安全摘要

設定所有系統管理工具時要記住的重要安全事項：

- **系統管理產品可用來取得一個可開機的 *root* 環境。**

  使用可開機的 root 環境，您可以存取 Oracle ILOM、Oracle System Assistant 和硬碟。

- **系統管理產品包括許多功能強大的工具，需要管理員或 *root* 權限才能執行。**

  運用此層次的存取，可以變更硬體配置，以及清除資料。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack 預先安裝

在初始安裝及設定期間，請使用 Oracle 軟體安全性功能來控制硬體及追蹤系統資產。

內容涵蓋下列主題：

Oracle Hardware Management Pack 元件

Oracle Hardware Management Pack 包含一組硬體管理指令行工具，可用來設定 RAID、BIOS 和 Oracle ILOM 以及更新韌體。同時包含用來監視的 SNMP 外掛程式。Oracle Hardware Management Pack 還包含一個透過內部通道與 Oracle ILOM 通訊的常駐程式或服務，共用與伺服器相關的資產和狀態資訊。

這些工具和外掛程式會安裝在您的主機作業系統中，因此您可以直接從主機執行系統管理工作。雖然 Oracle Hardware Management Pack 提供許多管理 Oracle 伺服器的有用功能，但它是選擇性安裝的。

請參閱 Sun Server Hardware Management Pack User's Guide，取得有關 Oracle Hardware Management Pack 功能的詳細資訊，這有助於您判斷是否要使用及安裝。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)
- 如需一般性的 Oracle ILOM 資訊，請參閱：`http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

植入代理程式的 SNMP 外掛程式安全性設定

Oracle Hardware Management Pack 包含一個 SNMP 外掛程式模組，可延伸主機作業系統中的原生 SNMP 代理程式，提供額外的 Oracle MIB 功能。請特別注意，Oracle Hardware Management Pack 本身並沒有包含 SNMP 代理程式。若爲 Linux，模組會新增到先前就已經安裝好的 net-snmp 代理程式。若爲 Solaris，模組會新增到 Solaris Management Agent (Solaris 管理代理程式)。若爲 Windows，外掛程式會擴充原生的 SNMP 服務。

同樣地，Oracle Hardware Management Pack SNMP 外掛程式中任何與 SNMP 有關的安全性設定，都是由原生的 SNMP 代理程式或服務的設定來決定，而不是由外掛程式決定。請參閱 net-snmp 或 Windows SNMP 服務的文件，取得如何安全設定 SNMP 的指示。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

選擇 SNMP 代理程式的 SNMP 協定版本

SNMP 是用來監視或管理系統的標準協定。SNMPv1/v2c 未提供加密，而且使用認證形式的社群字串。社群字串是透過網路以純文字形式傳送，通常在一群個人之間共用，而非個人使用者專用。相反的，SNMPv3 使用加密來提供安全通道，並且擁有個別使用者名稱和密碼。SNMPv3 使用者密碼是本機密碼，因此可以安全地儲存在管理工作站上。

Oracle 建議，若原生 SNMP 代理程式支援，請使用 SNMPv3。請參閱 net-snmp 或 Windows SNMP 服務的文件，取得如何設定 SNMPv3 的指示。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack 安裝

內容涵蓋下列主題：

執行 Oracle Hardware Management Pack 安裝程式

Oracle Hardware Management Pack 包含一組原生的安裝套裝軟體，可使用作業系統的原生安裝工具 (例如 RPM) 安裝。此外，也可以使用精靈式的安裝程式來協助進行安裝程序。除了新增原生套裝軟體之外，安裝程式也會協助設定 Oracle Hardware Management Pack 以供使用。

因爲 Oracle Hardware Management Pack 安裝程式必須安裝原生套裝軟體，所以必須以 root 或管理員的身分執行。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

選擇啓用 LAN 連結

KCS 介面的較快速的替代方案是，主機作業系統上的用戶端可以透過內部高速連結與 Oracle ILOM 進行通訊。此連結是透過內部 Ethernet-over-USB 連線並執行 IP 堆疊予以實作。Oracle ILOM 與主機會獲得內部不可路由的 IP 位址以透過此通道通訊。

透過 LAN 連結連線至 Oracle ILOM 時需要認證，就像連線是透過網路的 Oracle ILOM 管理連接埠一樣。主機還可以透過 LAN 連結使用管理網路上公開的所有服務或協定。例如，使用主機上的 Web 瀏覽器可以存取 Oracle ILOM 的 Web 介面，或使用 Secure Shell 用戶端連線至 Oracle ILOM CLI。但無論如何都必須提供有效的使用者名稱和密碼，才能使用 LAN 連結。

Oracle Hardware Management Pack 安裝程式會顯示啓用 LAN 連結的選項。Oracle 建議，只有當網路指示支援 RFC 3927，且具備 link-local IPv4 位址功能時，才啓用 LAN 連結。而且，請務必確定作業系統沒有作爲橋接器或路由器。這可確保主機與 Oracle ILOM 之間的管理流量仍然保持隱私。

- Oracle Hardware Management Pack 文件庫 (http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

選擇將證明資料儲存為檔案

Oracle Hardware Management Pack 中的 ilomconfig 和 fwupdate 工具都可以使用高速的 LAN 連結連線至 Oracle ILOM。使用 LAN 連結取代較慢的 KCS 介面，可以大幅提升重要作業 (例如 Oracle ILOM 韌體更新) 的效能。

因爲 LAN 連結需要認證，所以每次使用這些工具時都必須向 Oracle ILOM 認證。因此，可以將這些證明資料快取儲存成檔案，讓工具可以自動取用。這可以避免在使用 Oracle Hardware Management Pack 工具的命令檔中寫入純文字的密碼。

您可以使用 ilomconfig 工具將使用者名稱與密碼儲存成 root 唯讀的加密檔案。使用 ilomconfig 或 fwupdate 存取 Oracle ILOM 時，如果有偵測到這個檔案，就會使用快取的證明資料。另一個方式是，每次使用工具時，可以在指令行中指定使用者名稱與密碼。

每個系統所使用的加密演算法都是唯一的。不過，如果金鑰被發現，就可以解密檔案並洩漏使用者名稱與密碼。Oracle 建議，爲了安全起見，在每個 Oracle ILOM 上均建立唯一的密碼，如此一來即使密碼遭到洩漏也無法用於其他 Oracle ILOM 系統。

請參閱 Sun Server Hardware Management Pack User's Guide，取得如何將證明資料儲存成檔案的指示。

- Oracle Hardware Management Pack 文件庫 (http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Oracle Hardware Management Pack 後續安裝

內容涵蓋下列主題：

解除安裝 Oracle Hardware Management Pack

Oracle Hardware Management Pack 套裝軟體可以使用原生的套裝軟體工具 (例如 RPM) 解除安裝，或者使用 Oracle Hardware Management Pack 隨附的精靈式解除安裝程式解除安裝。若使用原生套裝軟體的方式移除套裝軟體，將不會刪除儲存快取使用者名稱與密碼以用於 LAN 連結的加密檔案。必須手動刪除這類檔案。

精靈式的解除安裝程式則會移除證明資料檔案。因此，Oracle 建議使用精靈式安裝程式來解除安裝 Oracle Hardware Management Pack。

- Oracle Hardware Management Pack 文件庫 (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)