Oracle® Server X5-2 安全指南

文件號碼： **E58187-01**
2014 年 10 月

文件號碼： E58187-01

目錄

基本安全性

本文件提供一般性的安全準則，協助您保護您的 Oracle 伺服器、伺服器網路介面以及連線的網路交換器。

請洽詢您的 IT 安全人員，以瞭解與系統及特定環境有關的其他安全需求。

使用所有的硬體與軟體時，有幾項您必須遵守的基本安全性原則。本節涵蓋四項基本安全性原則：

存取

存取是指對硬體的實際取用，或是對軟體的實際取用或虛擬存取。

- 透過實際及軟體控制，保護您的硬體及資料避免遭到入侵。
- 安裝新系統時，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存取硬體或軟體。
- 參考軟體隨附的文件，啟用軟體提供的安全功能。
- 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，否則請將機架門保持上鎖狀態。
- 限制存取 USB 連接埠和主控台。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，提供了直接存取系統的途徑。實際取用是存取元件較為安全的方法，因為比較不易受到網路攻擊。
- 限制透過網路重新啟動系統的功能。
- 要特別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) 及客戶可更換單元 (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。

認證

認證是識別使用者的方法，一般藉由機密資訊 (例如使用者名稱和密碼) 來識別。認證可確保硬體或軟體的使用者身分。

- 設定認證功能 (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真實無誤。
- 確認您的工作人員需正確配戴識別證才能進入電腦機房。
- 針對使用者帳號的控管：在適當時使用存取控制清單；對延長的階段作業設定結束時間；針對不同使用者設定不同的權限等級。

授權

授權讓管理員得以控制使用者可執行的工作或可使用的權限。工作人員只能執行指派給他們的工作，以及使用指派給他們的權限。授權是指對工作人員使用硬體及軟體所設的限制。

- 僅允許受過訓練並符合使用資格的工作人員使用相應的硬體及軟體。
- 設定系統的讀取/寫入/執行 (Read/Write/Execute) 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。

資料記錄與稽核

資料記錄與稽核是指維護系統上的使用者活動記錄。Oracle 伺服器具備軟體和硬體功能，讓管理員能夠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。尤其是監視系統管理員及服務帳號，因為這些帳號可以存取指令，倘若使用不當，將危害系統或造成資料遺失。存取權與指令應透過系統記錄謹慎監視。
- 記錄所有硬體的序號。使用元件序號來追蹤系統資產。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。
- 在所有重要的電腦硬體元件 (如 FRU 和 CRU) 上加註安全標誌，以偵測及追蹤元件。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，系統管理員必須能輕易地存取此位置。書面文件可能會是擁有權的唯一證明。

安全使用伺服器配置及管理工具

使用軟體和韌體工具設定及管理伺服器時，請遵守下列各節中的安全準則：

- 「Oracle System Assistant 安全性」[9]
- 「Oracle ILOM 安全性」[10]
- 「Oracle Hardware Management Pack 安全性」[11]

請洽詢您的 IT 安全人員，以瞭解與系統及特定環境有關的其他安全需求。

Oracle System Assistant 安全性

Oracle System Assistant 是已預先安裝的工具，可協助您設定與更新伺服器硬體，以及安裝支援的作業系統。若需如何使用 Oracle System Assistant 的資訊，請參閱「*Oracle X5 Series Servers Administration Guide*」，網址為：

`http://www.oracle.com/goto/x86AdminDiag/docs`

以下資訊描述與 Oracle System Assistant 相關的安全問題。

- **Oracle System Assistant 包含一個可開機的 root 環境。**

  Oracle System Assistant 是一種可以在已預先安裝的內部 USB 快閃磁碟機上執行的應用程式。Oracle System Assistant 建立在可開機的 Linux root 環境最上層。Oracle System Assistant 也提供可以存取其相關 root shell 的功能。可以實際存取系統，或者透過 Oracle ILOM 對系統具有遠端 KVMS (鍵盤、視訊、滑鼠及儲存裝置) 存取權的使用者，可存取 Oracle System Assistant 及 root shell。

  Root 環境可用於變更系統配置與原則，也可以存取其他磁碟上的資料。若要提升安全性，請限制對伺服器實體的接觸使用，並謹慎指派 Oracle ILOM 使用者的管理員及主控台權限。

  Oracle System Assistant shell 的設計，能賦予使用者適當的權限來使用 Oracle Hardware Management Pack CLI 工具，以達到系統管理的目的。這個 shell 的設計並非提供網路服務。為確保最高等級的安全性，網路服務預設為停用且不應啟用。

- **Oracle System Assistant 會掛載一個系統可存取的 USB 儲存裝置。**

  除了作為可開機的環境之外，Oracle System Assistant 也可以 USB 儲存裝置 (快閃磁碟機) 的方式掛載，完成安裝後，主機作業系統就可以存取這個裝置。當您存取工具和驅動程式以執行維護和重新設定作業時，這樣的功能是非常好用的。Oracle System Assistant USB 儲存裝置可以讀取及寫入，所以也可能會受到病毒的攻擊。

為提高安全性，將保護磁碟的相同方法，應用到 Oracle System Assistant 儲存裝置，包括定期的病毒掃描及完整性檢查。

- **Oracle System Assistant 可以加以停用。**

  對設定伺服器、更新及設定韌體，以及安裝主機作業系統而言，Oracle System Assistant 是非常實用的工具。不過，如果您無法接受前述的安全事項，或者不需要這個工具，您可以停用 Oracle System Assistant。停用 Oracle System Assistant 之後，主機作業系統將無法再存取 USB 儲存裝置，使用者也將無法啟動進入 Oracle System Assistant。

  您可以從工具本身或從 BIOS 停用 Oracle System Assistant。停用之後，只能從 BIOS Setup 公用程式重新啟用 Oracle System Assistant。建議您設定密碼來保護 BIOS Setup 公用程式，讓只有獲得授權的使用者才能重新啟用 Oracle System Assistant。

- **請參閱 Oracle System Assistant 文件。**

  如需 Oracle System Assistant 功能的相關資訊，請參閱「*Oracle X5 Series Servers Administration Guide*」，網址為：

  `http://www.oracle.com/goto/x86AdminDiag/docs`

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (ILOM) 管理韌體來主動保護、管理及監視系統元件，這個韌體已內嵌在 Oracle x86 伺服器以及 Oracle SPARC 伺服器上。視授予系統管理員的授權等級而定，這些功能可能包括關閉伺服器、建立使用者帳號、掛載遠端儲存裝置等等。

- **使用安全的內部信任網路。**

  無論您是透過本機序列埠、專用網路管理連接埠或標準資料網路連接埠建立 Oracle ILOM 實體管理連線，伺服器上的這個實體連接埠都必須一律連線至內部信任的網路，或專用的安全管理或專用網路。

  絕對不要將 Oracle ILOM 服務處理器 (SP) 連線至公用網路，例如網際網路。您應該將 Oracle ILOM SP 管理流量限制在個別的管理網路上，並只對系統管理員授予存取權。

- **限制使用預設管理員帳號。**

  限制預設管理員帳號 (`root`) 只能在第一次登入 Oracle ILOM 時使用。此預設管理員帳號的目的只是為了協助您進行初始伺服器安裝。因此，為了確保最安全的環境，您必須在第一次設定系統時變更預設的管理員密碼 (`changeme`)。取得預設管理員帳號的存取權，會讓使用者無限制地存取 Oracle ILOM 的所有功能。除此之外，請為每個新 Oracle ILOM 使用者建立具有唯一密碼的使用者帳號，並指派授權等級 (使用者角色)。

- **仔細思考序列埠連線至終端機伺服器時的風險。**

  終端機裝置不一定都會提供適當的使用者認證或授權等級，而這些認證或授權正是保護網路不會遭到惡意入侵的必要條件。若要保護您的系統不會遭到不想要的網路

入侵，請勿透過任何類型的網路重新導向裝置 (例如終端機伺服器) 來建立對 Oracle ILOM 的序列連線 (序列埠)，除非該伺服器具備足夠的存取控制。

此外，某些 Oracle ILOM 功能只會在使用實體序列埠時提供，例如密碼重設以及 [Preboot menu] (啟動前功能表)。使用未經認證的終端機伺服器將序列埠連線至網路，就不需要實際的存取，因而會降低與這些功能有關的安全。

- **存取 [Preboot menu] (啟動前功能表) 必須實際存取伺服器。**

  Oracle ILOM 的 [Preboot menu] (啟動前功能表) 是強大的公用程式，提供重設 Oracle ILOM 為預設值，以及在 Oracle ILOM 沒有回應時刷新韌體的方法。當 Oracle ILOM 重設完成後，使用者接著必須按下伺服器上的某個按鈕 (預設值) 或輸入密碼。「Oracle ILOM 實際存在性」特性會控制這個行為 (`check_physical_presence=true`)。若要在存取 [Preboot menu] (啟動前功能表) 時有最高的安全性，請勿變更預設設定 (`true`)，如此一來，存取 [Preboot menu] (啟動前功能表) 時就一定要實際存取伺服器。

- **參閱 Oracle ILOM 文件。**

  請參閱 Oracle ILOM 文件以瞭解關於設定密碼、管理使用者以及套用安全保護功能的詳細資訊。如需 Oracle ILOM 特定的安全準則，請參閱「*Oracle ILOM* 安全指南」(Oracle ILOM 文件庫中的一部分)。您可以在下列位置找到 Oracle ILOM 文件：

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

Oracle Hardware Management Pack 安全性

您的伺服器以及許多其他 Oracle x86 伺服器與部分 Oracle 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。

- **使用硬體管理代理程式 SNMP 外掛程式。**

  SNMP 是用來監視或管理系統的標準協定。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，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 位址) 監視多部伺服器。

  SNMP 外掛程式是在 Oracle 伺服器的作業系統中執行。SNMP 外掛程式模組可擴充主機作業系統中的原生 SNMP 代理程式，提供額外的 Oracle MIB 功能。Oracle Hardware Management Pack 本身不含任何 SNMP 代理程式。若為 Linux，模組會新增到 net-snmp 代理程式。若為 Oracle Solaris，模組會新增到 Oracle Solaris Management Agent (Oracle Solaris 管理代理程式)。若為 Microsoft Windows，外掛程式會擴充原生的 SNMP 服務。Oracle Hardware Management Pack 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。

  請注意，SNMPv1 和 SNMPv2c 未提供加密，而且使用社群字串作為認證的形式。SNMPv3 較為安全，並且是建議使用的版本，因為它使用加密來提供安全通道，以及個別使用者名稱和密碼。

- **請參閱 Oracle Hardware Management Pack 文件。**

  如需這些功能的詳細資訊，請參閱 Oracle Hardware Management Pack 文件。如需 Oracle Hardware Management Pack 特定的安全準則，請參閱「*Oracle Hardware Management Pack (HMP)* 安全指南」(Oracle Hardware Management Pack 文件庫中的一部分)。您可以在下列網址找到 Oracle Hardware Management Pack 文件：

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

規劃安全的環境

安全準則必須在系統到達前先行備妥。到達之後，必須定期複查安全準則並加以調整，使安全準則與組織的安全需求保持在最新狀態。

安裝與配置伺服器及相關設備之前和期間，請使用下列各節中的資訊：

- 「密碼保護」[13]
- 「作業系統安全準則」[14]
- 「網路交換器及連接埠」[14]
- 「VLAN 安全性」[15]
- 「Infiniband 安全性」[15]

請洽詢您的 IT 安全人員，以瞭解與系統及特定環境有關的其他安全需求。

密碼保護

密碼是安全的重要層面，因為選擇不當的密碼可能會導致公司資源遭到未經授權的存取。實行密碼管理最佳措施可以確保使用者遵循一組用於建立及保護其密碼的準則。典型的密碼制定原則元件應定義下列事項：

- 密碼長度與強度
- 密碼期限
- 通用密碼措施

強制執行下列標準措施以建立更安全的複雜密碼：

- 請勿建立包含使用者名稱、員工姓名或姓氏的密碼。
- 請勿選擇容易猜測的密碼。
- 請勿建立包含連續數字字串的密碼，例如 12345。
- 請勿建立包含透過簡單的網路搜尋即可找到之文字或字串的密碼。
- 請勿允許使用者在多個系統中重複使用相同的密碼。
- 請勿允許使用者重複使用舊密碼。

定期變更密碼。這有助防止惡意的活動，並確保密碼遵循目前的密碼制定原則。

作業系統安全準則

請參閱 Oracle 作業系統 (OS) 文件，瞭解下列相關資訊：

- 如何在設定系統時使用安全保護功能
- 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

您可以在作業系統的文件庫中，找到支援之 Oracle 作業系統的安全指南文件。若要取得 Oracle 作業系統的安全指南文件，請前往 Oracle 作業系統文件庫：

作業系統	連結
Oracle Solaris 作業系統	http://www.oracle.com/technetwork/documentation/Solaris-11-192991.html
Oracle Linux 作業系統	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

如需關於其他廠商 (例如 Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Microsoft Windows 以及 VMware ESXi) 作業系統的相關資訊，請參閱各個廠商的文件。

網路交換器及連接埠

網路交換器會提供不同等級的連接埠安全性功能。請參閱交換器文件，瞭解如何執行下列各項作業：

- 使用認證、授權以及資料記錄功能，從本機和遠端存取交換器。
- 如果網路交換器預設多個使用者帳號和密碼，請變更網路交換器上的每一組密碼。
- 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虛擬區域網域 (VLAN) 編號。
- 使用網路交換器的連接埠監視功能偵測系統入侵行為 (IDS)。
- 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。
- 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。
- 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**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關聯。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**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，以便網路交換器能夠根據目前的連線設定安全性。

VLAN 安全性

如果您設定虛擬區域網路 (VLAN)，請記住 VLAN 會共用網路頻寬，並且需要其他的安全保護措施。

- 使用 VLAN 時，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。
- 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。
- 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。

Infiniband 安全性

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。

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軟體資產。

請使用下列各節中的資訊來維護安全的環境。

請洽詢您的 IT 安全人員，以瞭解與系統及特定環境有關的其他安全需求。

電源控制

您可以使用軟體開啟或關閉部分 Oracle 系統的電源。部分系統機櫃的電源分配器 (PDU) 可以從遠端啟動和停止。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

可使用序號追蹤庫存。Oracle 會在選項卡及系統主機板的韌體中嵌入序號。您可以透過區域網路 (LAN) 連線看到這些序號。

您也可以使用無線電頻率識別 (RFID) 讀取器，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

軟體和韌體的更新

安全性增強功能會透過新軟體發行版本以及修補程式導入。有效且主動的修補程式管理，是系統安全非常重要的一部分。為能具備最佳的安全措施，請使用較新的軟體發行版本以及所有必要的安全修補程式來更新您的系統。

- 定期檢查軟體更新及安全修補程式。
- 務必安裝最新的軟體或韌體版本。
- 為軟體安裝所有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，因此可能需要修補程式和韌體更新。

您可以在 My Oracle Support 網站上找到軟體更新及安全修補程式，網址為：

http://support.oracle.com

網路安全

依據安全性原則配置網路之後，必須定期複查與維護。

請依照下列準則，保護對系統的本機和遠端存取：

- 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 (LAN) 區段上的每個人都能看到登入證明資料。請為 SSH 設定更安全的密碼。
- 使用「簡易網路管理協定 (SNMP)」版本 3 提供安全傳輸。舊版的 SNMP 不安全而且會在未加密的文字中傳送認證資料。SNMPv3 使用加密來提供安全通道，以及個別的使用者名稱和密碼。
- 如果必須使用 SNMPv1 或 SNMPv2，請將預設的 SNMP 社群字串變更為更安全的社群字串。部分產品已將 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。
- 如果系統控制器是使用瀏覽器介面，使用系統控制器之後請務必登出。
- 停用不必要的網路服務，如「傳輸控制協定 (TCP)」或「超本文傳輸協定 (HTTP)」。啟用需要的網路服務並設定這些服務的安全性。
- 建立登入時會顯示的標題訊息，聲明禁止未經授權的存取。您可以將任何重要的原則或規則通知使用者。標題可以用來警告使用者指定的系統是否有特殊存取限制，或是提醒使用者密碼制定原則以及適當的使用。
- 適時使用存取控制清單來套用限制。
- 對延長的階段作業設定結束時間，並設定不同的權限等級。
- 使用認證、授權以及資料記錄功能，從本機和遠端存取交換器。
- 在極為安全的環境中使用這些服務，因為它們是透過憑證和其他形式的高度加密來保護通道：
  - Active Directory

    - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- 在沒有可疑惡意使用者的專用安全網路上使用這些服務：
    - RADIUS (Remote Authentication Dial In User Service)
    - TACACS+ (Terminal Access Controller Access-Control System)
- 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。

如需網路安全的相關詳細資訊，請參閱「*Oracle ILOM* 安全指南」(Oracle ILOM 文件庫中的一部分)。您可以在下列位置找到 Oracle ILOM 文件：

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

資料保護和安全

請依照下列準則以取得最高的資料保護和安全等級：

- 使用如外接式硬碟或 USB 儲存裝置此類的裝置來備份重要的資料。然後將備份的資料存放在其他不同的安全位置。
- 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。檔案經刪除或磁碟機重新格式化後，仍然可以從磁碟機還原資訊。刪除檔案或重新格式化磁碟機時，只會移除磁碟機上的位址表格。請使用磁碟清除軟體來徹底清除磁碟機上的所有資料。
- 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過處理。
    - 您可以使用磁碟清除工具 (例如 Oracle Solaris `format(1M)`) 指令來徹底清除磁碟機上的所有資料。或者，您也可以使用適當的實體消磁工具來完成此工作。
    - 在某些情況下，硬碟中的資訊具有絕對的機密性，而唯一適當的處理方式是實際破壞硬碟，例如粉碎硬碟或焚化硬碟。
    - 強烈建議組織參考其資料保護政策，以判斷最適當的硬碟處理方式。

注意 - 磁碟清除軟體可能因新式硬碟 (尤其是固態硬碟，即 SSD) 管理資料存取的方式而無法刪除其中的某些資料。

記錄維護

定期檢查及維護您的記錄檔。請使用下列方法保護記錄檔：

- 開啟記錄功能，並將系統記錄傳送至專用的安全記錄主機。
- 使用「網路時間協定 (NTP)」與時戳設定記錄功能，以包含正確的時間資訊。

- 定期執行排定的網路裝置記錄掃描，瞭解是否有異常的網路活動或存取。
- 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。
- 當記錄檔超過合理的大小後，定期汰換記錄檔。保留汰換的檔案，以供日後參考或用於統計分析。