Sun Server X3-2L (先前名稱為 Sun Fire X4270 M3)

安全指南

文件號碼： E36127-02
2013 年 9 月

目錄

• • • 第 1 章

Sun Server X3-2L 安全指南

本文件提供一般性的安全指導方針，協助您保護 Oracle Sun Server X3-2L、其網路介面及其連接的網路交換器。

注意

Sun Server X3-2L 先前名稱為 Sun Fire X4270 M3 伺服器。先前的名稱可能仍會顯示在軟體中。新產品名稱並不代表系統功能有任何變更。

本章涵蓋下列各節：

系統簡介

Sun Server X3-2L 是企業級的兩機架單元 (2U) 伺服器，支援一或兩顆處理器、十六支 DDR3 DIMM (每顆處理器八支)、六個 PCIe Gen3 插槽，以及八、十二或二十四顆 SAS/SATA 儲存磁碟。伺服器包含一個內建 Oracle Integrated Lights Out Manager (Oracle ILOM) 服務處理器 (SP)。Oracle System Assistant 伺服器設定工具也會內嵌在預先安裝的 USB 快閃磁碟機上，作為伺服器配置的一部分。

安全性原則

有四項安全性原則：存取、認證、授權及資料記錄。

- **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。
  - 參考軟體隨附的文件，啟用軟體提供的安全功能。

  - 在上鎖並限制人員進出的房間內安裝伺服器及相關設備。
  - 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。
  - 限制使用連接器或連接埠，因為它們可以提供比 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會提供連接器及連接埠。
  - 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**

  認證是指確認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**

  授權是指對工作人員使用硬體或軟體所設的限制。
  - 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**

  資料記錄是指用來監視登入活動及硬體資產維護的軟體及硬體功能。
  - 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功能強大的指令。
  - 保留所有硬體的序號記錄。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。
  - 在所有重要的電腦硬體元件 (如 FRU) 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。

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，請遵守下列安全指導方針。

- 第 6 頁的 「Oracle System Assistant 安全性」
- 第 7 頁的 「Oracle ILOM 安全性」
- 第 8 頁的 「Oracle Hardware Management Pack 安全性」

Oracle System Assistant 安全性

Oracle System Assistant 是已預先安裝的工具，可以幫助您從本機或遠端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 *Sun Server X3-2L Administration Guide*，網址：

http://www.oracle.com/pls/topic/lookup?ctx=SunServerX3-2L

下列資訊可以協助您瞭解 Oracle System Assistant 的相關安全問題。

- **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。它是建立在可開機的 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，就可以存取 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。建議限制對伺服器實體的接觸使用，並謹慎指定 Oracle ILOM 使用者的管理員及主控台權限。

- 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。

建議您將相同的磁碟保護方法應用到 Oracle System Assistant 儲存裝置，並包括定期的病毒掃描及完整性檢查。

- Oracle System Assistant 可以停用

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 表示主機作業系統將無法再存取 USB 儲存裝置。此外，也將無法啟動 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。建議您設定密碼保護 BIOS Setup，讓只有獲得授權的使用者才能重新啟用 Oracle System Assistant。如需取得如何停用及重新啟用 Oracle System Assistant 的資訊，請參閱 *Sun Server X3-2L Administration Guide*。

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 管理韌體來主動保護、管理及監視系統元件，這個韌體已預先安裝至 Sun Server X3-2L、其他 Oracle x86 型伺服器以及部分的 Oracle SPARC 型伺服器中。

讓服務處理器 (SP) 使用專用網路，與一般網路分開。Oracle ILOM 可以讓系統管理員控制和監視伺服器。視授予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。因此，若要維持最可靠和最安全的 Oracle ILOM 環境，伺服器的專用網路管理連接埠或邊頻帶管理連接埠必須一律連線到內部信任的網路或專用的安全管理/專用網路。

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**)。除了變更預設管理員帳號的密碼之外，您必須為每個新 Oracle ILOM 使用者建立使用唯一密碼的新使用者帳號，並指派其授權等級。

請參閱 Oracle ILOM 文件，深入瞭解如何設定密碼、管理使用者以及套用安全保護功能 (包括「安全 Shell (SSH)」、「安全通訊端層 (SSL)」以及 RADIUS 驗證)。如需 Oracle ILOM 特定的安全指示，請參閱 *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide* (Oracle ILOM 3.1 文件庫中的一部分)。您可以在下列位置找到 Oracle ILOM 3.1 文件：

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Oracle Hardware Management Pack 安全性

您的伺服器以及許多其他 x86 型伺服器與部分 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 位址) 監視多個伺服器和伺服器模組。SNMP 外掛程式是在 Oracle 伺服器的作業系統中執行。

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 Microsoft Windows 作業系統使用。

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 特定的安全指示，請參閱 *Oracle Hardware Management Pack (HMP) Security Guide* (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/pls/topic/lookup?ctx=ohmp

規劃安全的環境

安裝及設定伺服器和相關設備時，請參考下列資訊。

- 第 8 頁的 「Oracle 作業系統指示」
- 第 9 頁的 「網路連接埠及交換器」
- 第 9 頁的 「VLAN 安全性」
- 第 9 頁的 「Infiniband 安全性」
- 第 9 頁的 「硬體實體安全」
- 第 10 頁的 「軟體安全」

Oracle 作業系統指示

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 作業系統的安全文件。若要取得 Oracle 作業系統的安全文件，請前往 Oracle 作業系統文件庫：

- Oracle Solaris 10 1/13 - http://www.oracle.com/goto/Solaris10/docs
- Oracle Solaris 11.1 - http://www.oracle.com/goto/Solaris11/docs
- Oracle Linux - http://www.oracle.com/technetwork/documentation/ol-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、Windows 以及 VMware ESXi) 作業系統的相關資訊，請參閱廠商的說明文件。

網路連接埠及交換器

不同的交換器會提供不同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。

- 使用驗證、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。

- 定義 VLAN，讓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。

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。
- 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。

硬體實體安全

實體硬體的保護方式相當簡單：限制對硬體的存取，並記錄序號。

- **限制存取**
  - 在上鎖並限制人員進出的房間內安裝伺服器及相關設備。
  - 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。設備維護完畢之後，請將門鎖上。

  - 限制使用 USB 連線，因為它們可以提供比 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) 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**
  - 在所有重要的電腦硬體元件 (如 FRU) 上加註安全標誌。使用特殊的紫外線筆或浮水印標籤來加註安全標誌。
  - 保留所有硬體的序號記錄。
  - 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。書面文件可能會是擁有權的唯一證明。

軟體安全

大部分的硬體安全性會透過軟體方式來實作。

- 安裝新系統時，請變更所有預設的密碼。大部分設備類型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。
- 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。
- 將預設管理員帳號 (root) 限制為只有一位管理員使用者能取得。您必須為每個新使用者建立新的 Oracle ILOM 帳號。請務必為每個 Oracle ILOM 使用者帳號指派唯一的密碼和適當等級的授權權限 (操作員、管理員等)。
- 讓服務處理器使用專用的網路，與一般網路分開。
- 保護 USB 連線存取。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，它們可以提供比 SSH 連線更強大的存取功能。
- 參考軟體隨附的文件，啟用軟體提供的安全功能。
- 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。

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。

- 第 10 頁的 「硬體電源控制」
- 第 10 頁的 「資產追蹤」
- 第 11 頁的 「軟體和韌體的更新」
- 第 11 頁的 「網路存取」
- 第 11 頁的 「資料保護」
- 第 12 頁的 「記錄維護」

硬體電源控制

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版的韌體中嵌入序號。您可以透過區域網路連線看到這些序號。

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

請讓您伺服器設備的軟體與韌體版本維持在最新狀態。

- 請定期檢查更新。
- 務必安裝最新的軟體或韌體版本。
- 安裝任何必要的軟體安全修補程式。
- 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。

網路存取

請依照下列指示，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。
- 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。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。
- 使用 LDAP 存取系統時，請遵循 LDAP 安全措施。請參閱 *Oracle ILOM Security Guide*，網址：http://www.oracle.com/goto/ILOM/docs
- 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。

資料保護

請依照下列指示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。

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。
- 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。