

# **Netra Server X3-2 (先前名稱為 Sun Netra X4270 M3 伺服器)**

安全指南

版權所有 ©2012，Oracle 和 (或) 其關係公司。保留一切權利。

本軟體與相關說明文件是依據含有用途及保密限制事項的授權合約所提供，且受智慧財產法的保護。除了授權合約中或法律明文允許的部份外，不得以任何形式或方法使用、複製、重製、翻譯、廣播、修改、授權、傳送、散佈、展示、演出、出版或陳列本軟體的任何部份。除非依法需要取得互通性操作 (interoperability)，否則嚴禁對本軟體進行還原工程 (reverse engineering)、反向組譯 (disassembly) 或解編 (decompilation)。

本文件中的資訊如有變更恕不另行通知，且不保證沒有任何錯誤。如果您發現任何問題，請來函告知。

如果本軟體或相關說明文件是提供給美國政府或代表美國政府授權使用本軟體者，適用下列條例：

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本軟體或硬體是針對各類資訊管理應用程式的一般使用所開發。不適用任何原本就具危險性的應用上，包含會造成人身傷害風險的應用。如果您將本軟體或硬體應用於危險用途，則應採取適當的防範措施，包括保全、備份、儲備和其他措施以確保使用安全。Oracle Corporation 和其關係公司聲明對將本軟體或硬體應用於危險用途所造成之損害概不負任何責任。

Oracle 和 Java 是 Oracle 和 (或) 其關係公司的註冊商標。其他名稱為各商標持有人所擁有之商標。

Intel 和 Intel Xeon 是 Intel Corporation 的商標或註冊商標。所有 SPARC 商標的使用皆經過授權，且是 SPARC International, Inc. 的商標或註冊商標。AMD、Opteron、AMD 標誌與 AMD Opteron 標誌是 Advanced Micro Devices 的商標或註冊商標。UNIX 是 The Open Group 的註冊商標。

本軟體或硬體與說明文件可能提供第三方內容、產品和服務的存取途徑與資訊。Oracle Corporation 和其關係公司明文聲明對第三方網站所提供的內容、產品與服務不做保證，且不負任何責任。Oracle Corporation 和其關係公司對於您存取或使用第三方的內容、產品或服務所引起的任何損失、費用或損害亦不負任何責任。

# 目錄

---

Netra Server X3-2 安全指南 .....	5
系統簡介 .....	5
安全性原則 .....	5
使用伺服器配置及管理工具 .....	6
規劃安全環境 .....	8
維護安全的環境 .....	10



# Netra Server X3-2 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 Netra Server X3-2 (先前名稱爲 Sun Netra X4270 M3 伺服器)、其網路介面及其連接的網路交換器。

本章涵蓋下列各節：

- 第 5 頁的「系統簡介」
- 第 5 頁的「安全性原則」
- 第 6 頁的「使用伺服器配置及管理工具」
- 第 8 頁的「規劃安全環境」
- 第 10 頁的「維護安全的環境」

## 系統簡介

Netra Server X3-2 是企業級、NEBS 相容的 2U 伺服器，具有兩顆處理器、支援十六支 DDR3 DIMM (每顆處理器八支)、六個 PCIe Gen3 插槽，以及八或六顆 SAS/SATA 儲存磁碟。六磁碟的型號同時提供 DVD 光碟機。

伺服器包含一個內建的 Oracle Integrated Lights Out Manager (Oracle ILOM) 服務處理器 (SP)。名爲 Oracle System Assistant 的伺服器設定工具也會內嵌在預先安裝的 USB 磁碟機上，作爲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存取，或是對軟體的實際或虛擬存取。

  - 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，啓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，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及客戶可更換單元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，並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。

  - 僅允許工作人員使用受過訓練並具備其使用資格的硬體及軟體。
  - 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**

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。

### 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。如需如何使用 Oracle System Assistant 的資訊，請參閱伺服器 Administration Guide，網址：

[http://docs.oracle.com/cd/E27124\\_01](http://docs.oracle.com/cd/E27124_01)

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，請參閱伺服器 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伺服器、其他 Oracle x86 型伺服器以及部分的 Oracle SPARC 型伺服器中。

讓服務處理器使用專用的網路，與一般網路分開。限制使用 root 超級使用者帳號。改為儘可能指派 Oracle ILOM 帳號，例如 ilom-operator 及 ilom-admin。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使用設備。

請參閱 Oracle ILOM 文件，深入瞭解密碼的設定方式、使用者的管理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 文件庫中的一部份)。您可以在下列位置找到 Oracle ILOM 3.1 文件：

[http://docs.oracle.com/cd/E24707\\_01](http://docs.oracle.com/cd/E24707_01)

## 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 文件庫中的一部份)。您可以在下列網址找到 Oracle Hardware Management Pack 文件：

[http://docs.oracle.com/cd/E20451\\_01](http://docs.oracle.com/cd/E20451_01)

## 規劃安全環境

安裝及設定伺服器和相關設備時，請參考下列資訊。

### 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** - [http://docs.oracle.com/cd/E23824\\_01](http://docs.oracle.com/cd/E23824_01)
- **Oracle Linux** - <http://linux.oracle.com/documentation/>
- **Oracle VM** - <http://www.oracle.com/technetwork/documentation/vm-096300.html>

## 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**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。

## 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。

### 硬體電源控制

您可以使用軟體開啓或關閉部分 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。

### 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。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。

## 資料保護

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。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。

- 開啓記錄功能，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，請定期將記錄檔歸檔，然後重設記錄。歸檔的檔案可供您參考或進行統計分析。

