Oracle 雙埠 QDR InfiniBand 配接卡 M4 安全指南

文件號碼： E76159-01
2016 年 6 月

文件號碼： E76159-01

說明文件協助工具

如需有關 Oracle 對於協助工具的承諾資訊，請瀏覽 Oracle Accessibility Program 網站，網址為 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

存取 Oracle 支援

已經購買客戶支援的Oracle 客戶可從 My Oracle Support 取得網路支援。如需資訊，請瀏覽 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如您有聽力障礙，請瀏覽 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

目錄

Oracle 雙埠 QDR InfiniBand 配接卡 M4 安全

本文件提供 Oracle 雙埠 QDR InfiniBand 配接卡 M4 的一般安全準則。本指南適用於具有經驗的網路管理員，可提供一般準則及強化安全的特定指示。

本文件涵蓋下列主題：

安全原則

有四項基本安全原則：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

  設定授權功能 (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。
- 授權

  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

  使用 Oracle 軟體和硬體功能，監督登入活動以及維護硬體資產。

  - 使用系統記錄來監督使用者登入。尤其是監督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。
  - 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。

規劃安全的環境

安裝與組態伺服器及相關設備時，請使用下列注意事項。

硬體安全

實體硬體的保護相當簡單：限制對硬體的存取，並記錄序號。

- 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，否則請將機架門保持上鎖狀態。
  - 限制使用 USB 主控台，因為它們的存取能力比 SSH 連線更強。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) 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。
- 記錄序號
  - 為所有重要的電腦硬體項目 (例如，FRU) 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。
  - 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夠方便取用。書面文件可能會是擁有權的唯一證明。

軟體安全

大部分的硬體和軟體安全會透過軟體的方式來實作。

- 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來限制存取。停用所有連接埠的自動中繼功能。
- 讓服務處理器使用專用的網路而不是一般網路。
- 透過廣域網路 (WAN) 或儲存區域網路 (SAN) 可安全地啟動系統。如需使用 WAN Boot 或 iSCSI Boot 進行安全開機的相關資訊，請參閱您 Oracle Solaris 作業系統版本適用的 Oracle Solaris Installation Guide: Network-Based Installations 一書。
- 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。
- 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。

Oracle Solaris 作業系統指導方針

請參閱 Oracle Solaris 安全指導方針文件以取得下列相關資訊：

- 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

  您可以在下列位置找到 Oracle Solaris 安全指導方針文件：http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Oracle Linux 作業系統準則

使用 Oracle Linux 作業系統指令可以限制對軟體的存取，並能強化作業系統、使用安全功能以及保護應用程式。請參閱 Oracle Linux Security Guide for Release 6，網址為：http://docs.oracle.com/cd/E37670_01/E36387/html/index.html。

網路交換器

不同的交換器會提供不同等級的連接埠安全功能。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。
- 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。
- 使用網路交換器的連接埠監督功能偵測系統入侵行為 (IDS)。
- 離線保留一份交換器組態檔，並限制只有授權的管理員才可以使用。組態檔應該包含每一項設定的描述性註解。

- 如果您的交換器提供下列連接埠安全功能，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。

Oracle 韌體安全

請使用超級使用者帳號來設定與更新 OpenBoot PROM (OBP) 或其他 Oracle 韌體。一般使用者帳號僅允許使用者檢視韌體，但無法編輯韌體。Oracle Solaris 作業系統韌體更新處理作業禁止未經授權的韌體修改。

如需設定 OBP 安全變數的相關資訊，請參閱 OpenBoot 4.x Command Reference Manual，網址為：http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM 韌體

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 管理韌體，主動保護、管理及監督系統元件，此韌體已預先安裝在部分 SPARC 伺服器上。

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 認證：http://docs.oracle.com/cd/E37444_01/index.html

VLAN 安全

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。

- 定義虛擬區域網路 (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

Infiniband (IB) 安全是 IB 結構及 IB 結構中執行之 Subnet Manager (SM) 的功能。請將所有 IB 主機都連接至 IB 結構安全。只有連接的 IB 主機安全，IB 結構才會安全。若攻擊者擁有某個主機的 root 存取權，將會瓦解整個 IB 結構的安全。(實體存取在這方面也很重要 - 能夠將自己的主機連線至 IB 交換器的攻擊者，也能夠威脅 IB 結構的安全。)

在虛擬環境中使用 Oracle 雙埠 EDR InfiniBand 配接卡或 Oracle 雙埠 QDR InfiniBand 配接卡 M4 時，請特別注意實體網域的安全性，因為受威脅的實體網域會導致所有虛擬機器暴露在容易受到攻擊的環境中。

如需有關保護 InfiniBand 及支援交換器 (其中同時執行 SM) 的詳細資訊，請參閱適用交換器的 InfiniBand 交換器安全指南：

- 若為 Sun Datacenter InfiniBand Switch 36，請參閱 Sun Datacenter InfiniBand Switch 36 Hardware Security Guide，網址為：http://docs.oracle.com/cd/E36265_01/
- 若為 Sun Network QDR InfiniBand Gateway Switch，請參閱 Sun Network QDR InfiniBand Gateway Switch Hardware Security Guide，網址為：http://docs.oracle.com/cd/E36256_01/
- 若為 IB 交換器和 Oracle Virtual Network InfiniBand 交換器上的 SM，請參閱：http://docs.oracle.com/cd/E38500_01/

使用者帳號

- 如果可以的話，請設定 RADIUS 和 TACACS+ 存取協定：RADIUS (遠端認證撥入使用者服務) 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。
- 限制使用超級使用者帳號 (root)。此帳號具有特殊的權限，如遭誤用，對安全會有不利的影響。請儘可能改用其他權限較低的使用者帳號。此準則適用於主機作業系統 (Solaris、Linux) 及 Oracle ILOM。
- 適時使用存取控制清單。
- 對延長的階段作業設定結束時間。
- 設定權限等級。
- 建立系統公告，提醒使用者禁止未經授權的存取。

系統記錄

- 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。

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組態時所指定，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

可使用序號追蹤資產。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連線查看這些序號。

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

請將伺服器設備的韌體版本及相關主機軟體 (驅動程式、使用者空間工具) 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。
- 為軟體安裝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，因此可能需要修補程式和韌體更新。

如要查看是否有可用的更新和修補程式，請前往：https://support.oracle.com

網路存取

請依照下列準則，保護對系統的本機和遠端存取：

- 依據 MAC 位址實作連接埠安全來限制存取。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) 執行遠端組態。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。
- 使用第 3 版的 SNMP 以提供安全傳輸。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

資料保護

請依照下列準則，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。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。

記錄安全

定期檢查及維護您的記錄檔。

- 複查記錄以找出可能的未預期事件，然後依據安全原則將它們歸檔。
- 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，以供日後參考或進行統計分析。