Oracle® VM Server for SPARC 3.3 安全指南

文件號碼： E64654
2015 年 10 月

文件號碼： E64654

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

使用本文件

- **簡介** – 包含安全地使用 Oracle VM Server for SPARC 3.3 軟體的相關資訊。
- **對象** – 管理虛擬化 SPARC 伺服器安全的系統管理員
- **必備知識** – 這些伺服器的系統管理員必須具備 UNIX® 系統和 Oracle Solaris 作業系統 (Oracle Solaris OS) 的使用知識

產品文件庫

本產品與相關產品的文件與資源可在下列網址取得：http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html。

意見

如果您對本文件有任何意見，歡迎您至以下網址提供意見：http://www.oracle.com/goto/docfeedback。

♦ ♦ ♦ 第 1 章

1 Oracle VM Server for SPARC 安全簡介

本文中提供的安全建議數量可能讓您覺得 Oracle VM Server for SPARC 安裝的安全性不足，但是實際上一般的 Oracle VM Server for SPARC 安裝就足以防禦未經授權的使用。不過即使被入侵的可能性不高，我們仍面臨些許的受攻擊面和某種程度的風險。就像您可能會選擇在標準防盜裝置 (如門鎖) 之外增設防盜鈴來為居家安全提供多一道防護一樣，額外的網路安全措施亦有助於降低發生未預期問題的機會，或是協助將可能的損害降至最低。

本章涵蓋下列 Oracle VM Server for SPARC 安全主題：

Oracle VM Server for SPARC 使用的安全功能

Oracle VM Server for SPARC 軟體是一種虛擬化產品，可允許多部 Oracle Solaris 虛擬機器 (VM) 在單一實體系統上執行，並各自安裝專屬的 Oracle Solaris 10 或 Oracle Solaris 11 作業系統。每個 VM 亦稱為邏輯網域。網域是獨立的執行處理，並可執行不同版本的 Oracle Solaris 作業系統和不同的應用程式軟體。例如，網域可以安裝不同的套裝軟體修訂版本、啟用不同的服務以及具備密碼不同的系統帳戶。如需 Oracle Solaris 安全的相關資訊，請參閱*Oracle Solaris 10 Security Guidelines* 與*Oracle Solaris 11 Security Guidelines* 。

`ldm` 指令會呼叫邏輯網域管理程式，它必須在控制網域上執行才能設定網域和擷取狀態資訊。限制控制網域的存取權和 `ldm` 指令的使用，對系統上執行之網域的安全性極為重要。若要限制網域配置資料的存取權，請使用 Oracle VM Server for SPARC 安全功能，例如主控台的 Oracle Solaris 權限和 `solaris.ldoms` 授權。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「Logical Domains Manager Profile Contents」。

Oracle VM Server for SPARC 軟體會使用下列安全功能：

- 能夠在 Oracle Solaris 10 作業系統和 Oracle Solaris 11 作業系統中使用的安全功能也可以在執行 Oracle VM Server for SPARC 軟體的網域上使用。請參閱*Oracle Solaris 10 Security Guidelines* 與*Oracle Solaris 11 Security Guidelines* 。
- Oracle Solaris 作業系統安全功能可套用至 Oracle VM Server for SPARC 軟體。如需確保 Oracle VM Server for SPARC 安全的完整資訊，請參閱第 14 頁的「虛擬化環境的安全」與第 15 頁的「攻擊防禦」。
- Oracle Solaris 10 作業系統與 Oracle Solaris 11 作業系統包含您的系統可以使用的安全性修正。取得 Oracle Solaris 10 作業系統修正作為安全修補程式或更新。取得 Oracle Solaris 11 作業系統修正作為 Support Repository Update (SRU)。
- 如需如何限制 Oracle VM Server for SPARC 管理指令和網域主控台之存取權的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的第 2 章「Oracle VM Server for SPARC Security」。

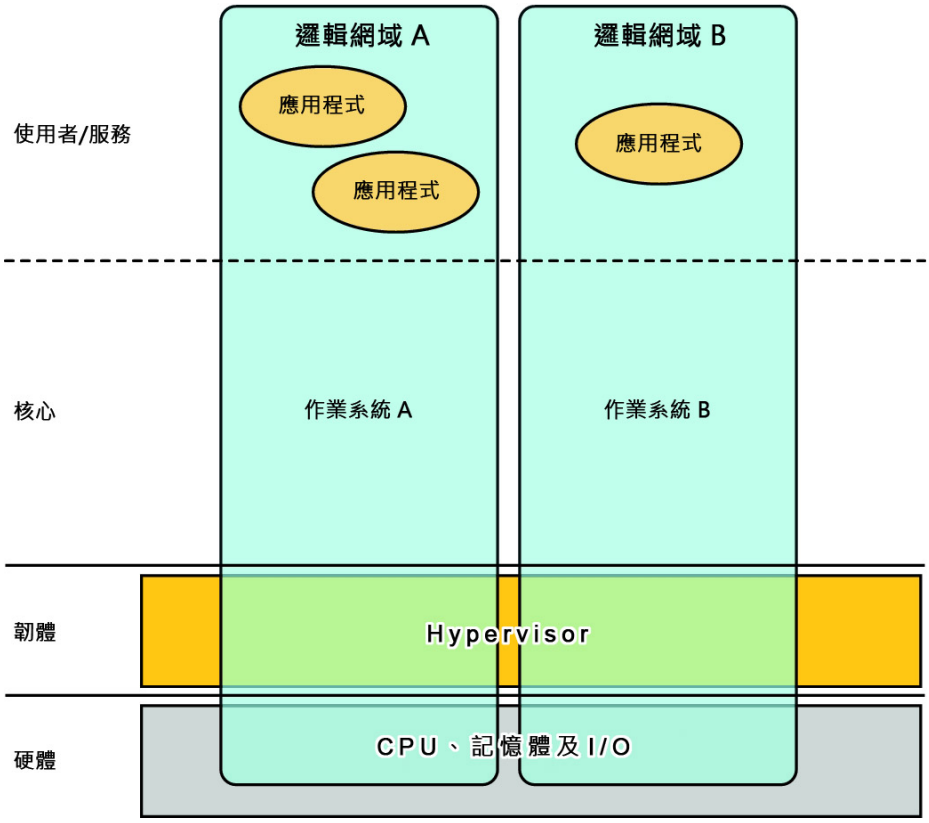
Oracle VM Server for SPARC 產品簡介

Oracle VM Server for SPARC 為 Oracle 的 SPARC T-Series 伺服器、SPARC M5 伺服器及 Fujitsu M10 伺服器提供高效率的企業級虛擬化功能。使用 Oracle VM Server for SPARC 軟體可讓您在單一系統上建立許多虛擬伺服器 (稱為邏輯網域)。此種配置可讓您使用這些 SPARC 伺服器和 Oracle Solaris 作業系統提供大規模的繫線。

邏輯網域是包含不同的資源邏輯群組的虛擬機器。邏輯網域在單一電腦系統內有自己的作業系統和識別。每一邏輯網域都可單獨建立、銷毀、重新設定和重新啟動，不需要重新開啟伺服器電源。您可以在不同的邏輯網域中執行各種應用程式軟體，並使它們保持獨立以確保效能和安全性。

如需使用 Oracle VM Server for SPARC 軟體的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 及*Oracle VM Server for SPARC 3.3 Reference Manual* 。如需必要之硬體和軟體的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Installation Guide* 。

圖 1-1 支援兩個邏輯網域的 Hypervisor



Oracle VM Server for SPARC 軟體使用下列元件提供系統虛擬化功能：

- **Hypervisor。**Hypervisor 是小型韌體層，主要提供穩定的虛擬機器架構來安裝作業系統。使用 Hypervisor 的 Oracle Sun 伺服器會提供硬體功能來支援 Hypervisor 控制邏輯網域中作業系統活動的能力。

  特定 SPARC Hypervisor 所支援的網域數目和每個網域的功能都視伺服器而定。Hypervisor 可將伺服器的 CPU、記憶體和 I/O 資源子集配置給指定的邏輯網域。此配置可同時支援多種作業系統，而每種作業系統各位於自身的邏輯網域中。資源在個別的邏輯網域之間可以進行任意的資料重新排列。例如可以將 CPU 資源以小單位的 CPU 繫線指派給邏輯網域。

  服務處理器 (SP，亦稱為系統控制器 (SC)) 會監視和執行實體機器。邏輯網域管理程式 (而非 SP) 會管理邏輯網域本身。
- **控制網域。**邏輯網域管理程式會在此網域中執行，可讓您建立和管理其他邏輯網域，以及將虛擬資源配置到其他網域。每一部伺服器只能有一個控制網域。控制網域是

您安裝 Oracle VM Server for SPARC 軟體時建立的第一個網域。控制網域的名稱是 `primary`。

- **服務網域。**服務網域會提供虛擬裝置服務 (例如，虛擬交換器、虛擬主控台集中器、虛擬磁碟伺服器) 給其他網域。所有網域都可設定為服務網域。
- **I/O 網域。**I/O 網域可以直接存取實體 I/O 裝置 (例如 PCI EXPRESS (PCIe) 控制器中的網路卡)。I/O 網域可擁有 PCIe 根聯合體 (Root Complex)，或可透過使用直接 I/O (DIO) 功能擁有 PCIe 插槽或內建 PCIe 裝置。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「Creating an I/O Domain by Assigning PCIe Endpoint Devices」。

  當 I/O 網域也作為服務網域使用時，便能夠以虛擬裝置的形式和其他網域共用實體 I/O 裝置。
- **根網域。**根網域會有一個已指派的 PCIe 根聯合體。此網域擁有該根聯合體的 PCIe 結構，並可提供所有結構相關的服務，例如結構錯誤處理。根網域也是一個 I/O 網域，因其可以直接存取實體 I/O 裝置。

  您可以擁有的根網域數目取決於您的平台架構。例如，如果您使用 Oracle 的 SPARC T4-4 伺服器，則最多可擁有四個根網域。
- **來賓網域。**來賓網域是非 I/O 網域，可使用一或多個服務網域提供的虛擬裝置服務。來賓網域沒有任何實體 I/O 裝置。它只有一個虛擬 I/O 裝置，例如虛擬磁碟和虛擬網路介面。

Oracle VM Server for SPARC 系統通常只有一個控制網域，它會提供 I/O 網域和服務網域執行的服務。為改善備援和平台可服務性，請考慮在您的 Oracle VM Server for SPARC 系統中設定一個以上的 I/O 網域。

在 Oracle VM Server for SPARC 套用一般安全原則

以不同方式設定來賓網域即可在來賓網域隔離、硬體共用和網域連線方面提供不同的等級。這些因素會構成整個 Oracle VM Server for SPARC 配置的安全等級。如需安全地建置 Oracle VM Server for SPARC 軟體的相關建議，請參閱第 14 頁的「虛擬化環境的安全」與第 15 頁的「攻擊防禦」。

您可以從下列選擇要套用的部分一般安全原則：

- **儘可能減少受攻擊面。**
  - 制訂可讓您定期評估系統安全的作業準則，儘可能減少意外的配置錯誤。請參閱第 17 頁的「對策：建立作業準則」。
  - 謹慎規劃虛擬環境的架構，以實行最大限度的網域隔離。請參閱第 18 頁的「威脅：虛擬環境架構中的錯誤」所描述的對策。
  - 謹慎規劃要指派的資源和是否要共用這些資源。請參閱第 20 頁的「對策：謹慎地指派硬體資源」與第 21 頁的「對策：謹慎地指派共用資源」。
  - 套用第 21 頁的「威脅：操控執行環境」與第 32 頁的「對策：保護來賓網域作業系統」中描述的對策，確保邏輯網域不會遭到操控。
    - 第 22 頁的「對策：保護互動式存取路徑」。

    - 第 22 頁的「對策：Oracle Solaris 作業系統最小安裝」。
    - 第 22 頁的「對策：強化 Oracle Solaris 作業系統」。
    - 第 27 頁的「對策：強化邏輯網域管理程式」。
    - 第 22 頁的「對策：使用角色區隔與應用程式隔離」描述指派功能角色給各網域的重要性，以及確保控制網域執行的軟體可提供代管來賓網域所需之基礎架構的重要性。您應該在來賓網域上執行可由其他系統執行的應用程式 (來賓網域專為此目的所設計)。
    - 第 23 頁的「對策：設定專用的管理網路」描述更進階的網路配置，該種配置會將擁有 SP 的伺服器連接至專用的管理網路，以杜絕透過網路存取 SP 的情形發生。
- 請只在必要時才向網路公開來賓網域。您可以使用虛擬交換器，將來賓網域的網路限制為只能連接到適當的網路。
- 請遵循*Oracle Solaris 10 Security Guidelines* 與*Oracle Solaris 11 Security Guidelines* 中的步驟，儘可能減少 Oracle Solaris 10 與 Oracle Solaris 11 的受攻擊面。
- 依照第 25 頁的「對策：驗證韌體和軟體簽章」與第 25 頁的「對策：驗證核心模組」描述的方式保護 Hypervisor 的核心。
- 保護控制網域免於阻斷攻擊。請參閱第 26 頁的「對策：保護主控台存取權」。
- 確認未經授權的使用者無法執行邏輯網域管理程式。請參閱第 26 頁的「威脅：未經授權使用配置公用程式」。
- 確認未經授權的使用者或處理作業無法存取服務網域。請參閱第 28 頁的「威脅：操控服務網域」。
- 保護 I/O 網域或服務網域免於拒絕服務攻擊。請參閱第 30 頁的「威脅：發生 I/O 網域或服務網域的拒絕服務攻擊」。
- 確認未經授權的使用者或處理作業無法存取 I/O 網域。請參閱第 31 頁的「威脅：操控 I/O 網域」。
- 停用不必要的網域管理程式服務。邏輯網域管理程式提供網域存取、監視和移轉的網路服務。請參閱第 27 頁的「對策：強化邏輯網域管理程式」與第 24 頁的「對策：保護 ILOM」。
- **提供執行作業所需的最小權限。**
    - 將系統分隔成不同的安全類別，安全類別是共用相同安全需求和權限的個別來賓系統群組。透過只將單一安全類別的來賓網域指派給單一硬體平台，您可以建立隔離屏障，避免網域擁有不同的安全類別。請參閱第 18 頁的「對策：謹慎地指派來賓至硬體平台」。
    - 使用權限來限制以 `ldm` 指令管理網域的能力。只有必須管理網域的使用者才可以具備此能力。將使用「LDoms 管理」權限設定檔的角色指派給需要使用所有 `ldm` 子指令的使用者。將使用「LDoms 複查」權限設定檔的角色指派給只需使用與清單相關之 `ldm` 子指令的使用者。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「Using Rights Profiles and Roles」。
    - 使用權限來限制只有身為 Oracle VM Server for SPARC 管理員的您可以存取您所管理之網域的主控台。請勿在所有網域開放一般存取。請參閱*Oracle VM*

Server for SPARC 3.3 Administration Guide 中的「Controlling Access to a Domain Console by Using Rights」。

虛擬化環境的安全

為有效保護您的 Oracle VM Server for SPARC 虛擬化環境，請保護作業系統和每個網域中執行的每個服務。為減少破壞攻擊的影響，請將服務建置到不同的網域以分隔服務。

Oracle VM Server for SPARC 環境使用 Hypervisor 來虛擬化邏輯網域的 CPU、記憶體和 I/O 資源。每個網域都是獨立的虛擬化伺服器，必須一一防禦以避免可能的攻擊。

虛擬化環境可透過硬體資源共用的方式，將數台伺服器合併為單一伺服器。在 Oracle VM Server for SPARC 中，CPU 和記憶體資源是以獨佔方式配置到每個網域，因此可避免過多的 CPU 使用量或濫用記憶體配置的情形。磁碟和網路資源通常由服務網域提供給多個來賓網域。

在評估安全時，請一律假設您的環境有攻擊者可利用的弱點。例如，攻擊者可能會利用 Hypervisor 中的弱點來控制整個系統，包括其來賓網域。因此，請一律建置多個系統，儘可能降低因破壞而造成損害的風險。

執行環境

執行環境具有下列元件：

- Hypervisor – 可虛擬化硬體的平台特定韌體，主要依賴建置於 CPU 的硬體支援。
- **控制網域** – 設定 Hypervisor 和執行邏輯網域管理程式的特殊網域，負責管理邏輯網域。
- **I/O 網域或根網域** – 擁有部分或所有平台可用之 I/O 裝置並和其他網域共用的網域。
- **服務網域** – 提供服務給其他網域的網域。服務網域可以提供其他網域的主控台存取權，或是提供虛擬磁碟。提供虛擬磁碟存取權給其他網域的服務網域也是 I/O 網域。

如需這些元件的相關資訊，請參閱圖 1-1,「支援兩個邏輯網域的 Hypervisor」"和更詳細的元件描述。

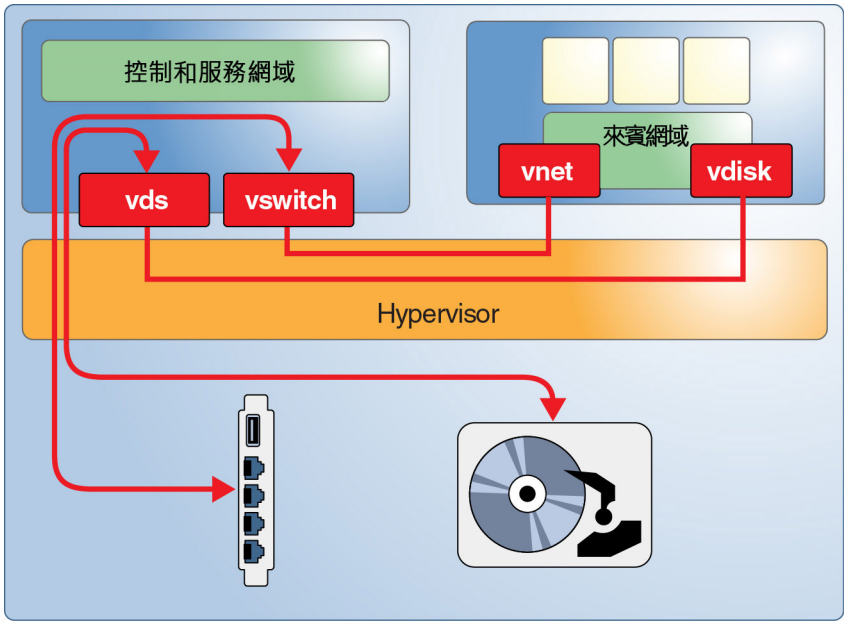
您可以設定第二個 I/O 網域，以改善備援 I/O 配置的可服務性。您也可以使用第二個 I/O 網域來隔離硬體以避免遭到安全攻擊。如需配置選項的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 。

保護執行環境

Oracle VM Server for SPARC 在執行環境中有數個攻擊目標。圖 1-2,「Oracle VM Server for SPARC 環境範例」"顯示簡單的 Oracle VM Server for SPARC 配置，其中的

控制網域會提供網路和磁碟服務給來賓網域。這些服務由控制網域中執行的常駐程式和核心模組實作。邏輯網域管理程式會指派每個服務的邏輯網域通道 (LDC)，並指派一個用戶端以簡化它們之間的點對點通訊。攻擊者可能會利用任一元件中的錯誤來破壞來賓網域的隔離機制。例如，攻擊者可能會在服務網域中執行任意程式碼，或可能中斷平台上的正常作業。

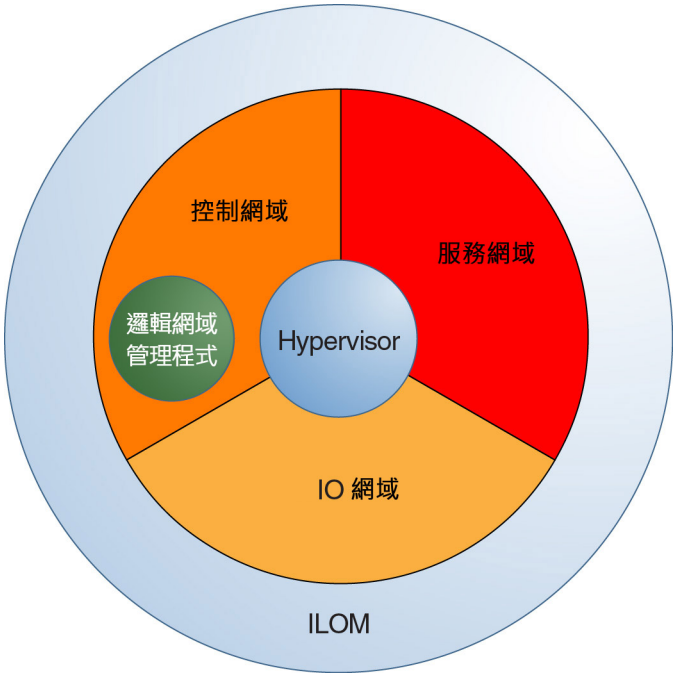
圖 1-2 Oracle VM Server for SPARC 環境範例



攻擊防禦

下圖顯示組成 Oracle VM Server for SPARC「執行環境」的虛擬化元件。這些元件不會嚴格地分隔。最簡單的配置是將這些功能全部合併於單一網域中。控制網域也可作為其他網域的 I/O 網域和服務網域。

圖 1-3 執行環境的元件



假設有攻擊者嘗試破壞系統隔離機制，然後操控執行環境的 Hypervisor 或其他元件來入侵來賓網域。您必須保護每個來賓網域，就像是保護任何獨立伺服器一樣。

本章的其餘部分說明威脅的可能性以及各種因應措施。每個攻擊都會嘗試破壞和去除在單一平台上執行之不同網域的隔離機制。以下小節描述 Oracle VM Server for SPARC 系統各個部分會受到的威脅：

- 第 17 頁的「作業環境」
- 第 21 頁的「執行環境」
- 第 23 頁的「ILOM」
- 第 24 頁的「Hypervisor」
- 第 25 頁的「控制網域」
- 第 26 頁的「邏輯網域管理程式」
- 第 30 頁的「I/O 網域」
- 第 28 頁的「服務網域」
- 第 31 頁的「來賓網域」

作業環境

作業環境包含 IT 組織的實體系統和其元件、資料中心架構、管理員及成員。安全漏洞可能會發生在作業環境的任一環節。

虛擬化在實際硬體和執行實際執行服務的來賓網域之間設定了軟體層。因此，您必須謹慎地規劃和設定虛擬系統，並小心人為錯誤。此外，還需留意攻擊者嘗試利用「社交工程」取得作業環境的存取權。

以下小節描述可以在作業環境層級反制的不同威脅。

威脅：無意的不當配置

虛擬化環境的主要安全考量是維持伺服器的隔離性，而這會透過分隔網路區段、分離管理存取權及將伺服器建置到安全類別 (即擁有相同安全需求和權限的網域群組) 的方法來達成。

請謹慎地設定虛擬資源，以避免發生部分下列錯誤：

- 在實際執行來賓網域和執行環境之間建立不必要的通訊通道
- 建立不必要的網路區段存取權
- 在不同的安全類別之間建立非計畫性的連線
- 非計畫性地將來賓網域移轉到錯誤的安全類別
- 配置的硬體不足，導致意外的資源超載
- 將磁碟或 I/O 裝置指派給錯誤的網域

對策：建立作業準則

開始之前，請謹慎地定義您的 Oracle VM Server for SPARC 環境作業準則。這些準則描述以下要執行的工作和執行方法：

- 管理環境中所有元件的修補程式
- 啟用定義完整、可追蹤及安全的變更實作
- 定期檢查記錄檔
- 監視環境的完整性與可用性

定期執行檢查，以確保這些準則適時合宜，並確認日常作業遵循這些準則。

除這些準則外，您還可以採取幾項更具技術性的措施以降低非計畫性動作的風險。請參閱第 26 頁的「邏輯網域管理程式」。

威脅：虛擬環境架構中的錯誤

將實體系統移到虛擬化環境時，通常可透過重複使用原始的 LUN 將儲存裝置配置維持原狀。但網路配置必須符合虛擬化環境，最終的架構可能與實體系統上使用的架構有相當程度的落差。

您必須考量如何維持不同安全類別的隔離機制和其需求。此外，也必須考量平台的共用硬體和共用元件，例如網路交換器與 SAN 交換器。

為保護您的環境安全，請確認您已確實維持來賓網域的隔離機制和安全類別。設計架構時，請考量可能的錯誤和攻擊，並建構安全防線。完善的設計有助於控制可能的安全問題，並能夠簡化架構和節省成本。

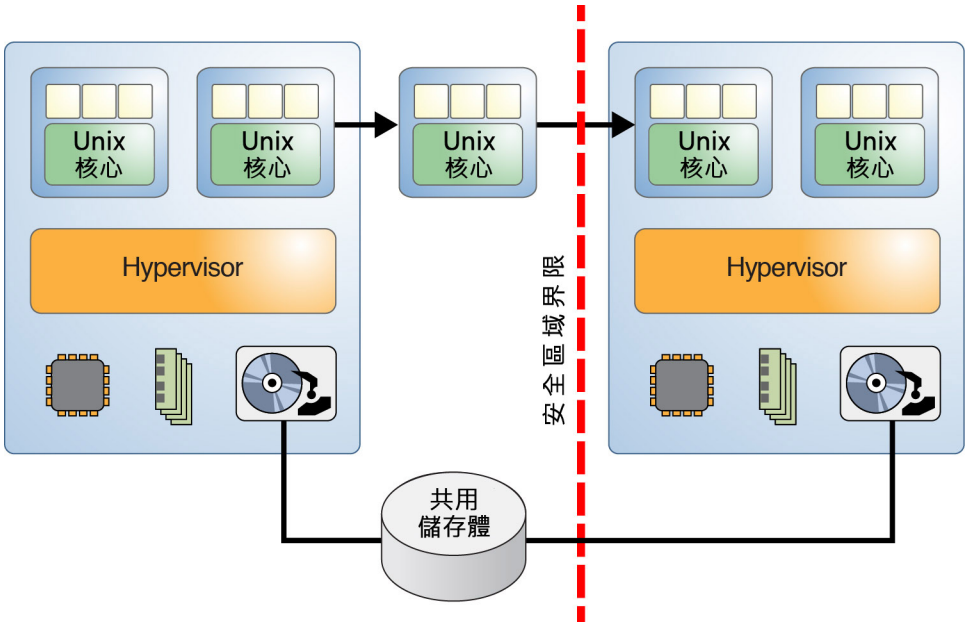
對策：謹慎地指派來賓至硬體平台

使用安全類別 (有相同安全需求和權限的網域群組) 隔離網域。將相同安全類別的來賓網域指派給特定硬體平台之後，即使隔離機制遭受破壞，也能防止攻擊擴及其他安全類別。

對策：規劃 Oracle VM Server for SPARC 網域移轉

如下圖所示，如果來賓網域不當移轉至指派了不同安全類別的平台，則即時網域移轉功能有可能會破壞隔離機制。因此，請謹慎地規劃來賓網域移轉，以確保其無法跨安全類別界限移轉。

圖 1-4 跨安全界限的網域移轉



為儘可能減少或去除移轉作業造成的安全漏洞，您必須在每個來源機器和目標機器組之間以頻外方式手動交換和安裝 `ldmd` 產生的主機憑證。如需如何設定 SSL 憑證的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「Configuring SSL Certificates for Migration」。

對策：正確設定虛擬連線

未確實記錄所有虛擬網路連線可能會導致網域取得錯誤的網路區段存取權。例如，這類存取可能會繞過防火牆或安全類別。

為降低實作錯誤的風險，請謹慎規劃和記錄您環境中的所有虛擬和實體連線。最佳化網域連線計畫以簡化連線和提高管理性。清楚記錄您的計畫，並在實際執行前確認計畫實作的正確性。即使在您的虛擬環境實際運作後，也應定期確認計畫的實作情況。

對策：使用 VLAN 標記

您可以使用 VLAN 標記來將數個乙太網路區段合併為單一實體網路。此功能也適用於虛擬交換器。為降低實作虛擬交換器的軟體錯誤風險，請為每個實體 NIC 和 VLAN 設定一

個虛擬交換器。為進一步防止乙太網路驅動程式發生錯誤，請勿使用已標記的 VLAN。不過，這類錯誤的可能性極低，因為這類的已標記 VLAN 是已知的漏洞。使用 Oracle VM Server for SPARC 軟體之 Oracle Sun SPARC T-Series 平台的入侵測試尚未顯示此漏洞。

對策：使用虛擬安全設備

安全設備 (例如封包篩選器和防火牆) 是隔離的器具，負責保護安全類別的隔離機制。這些設備與任何其他的來賓網域面臨著相同的威脅，因此使用這些設備並無法完全保證隔離不會受到破壞。因此，在您決定虛擬化此服務時，請謹慎考量所有風險和安全層面。

威脅：共用資源的副作用

在虛擬化環境中共用資源可能會導致拒絕服務 (DoS) 攻擊，這類攻擊會超載某項資源，直到該資源對其他元件 (例如其他網域) 造成負面影響為止。

在 Oracle VM Server for SPARC 環境中，只有部分資源可能會受到 DoS 攻擊的影響。CPU 和記憶體資源是以獨佔方式指派給每個來賓網域，因此可避免大多數的 DoS 攻擊。即使是以獨佔方式指派這些資源也可能對來賓網域造成下面的影響：

- 使得在區塊之間共用並指派給兩個來賓網域的快取區域震盪
- 超載記憶體頻寬

有別於 CPU 和記憶體資源，磁碟和網路服務通常會在來賓網域之間共用。這些服務由一或多個服務網域提供給來賓網域。請謹慎考量如何將這些資源指派和分配給來賓網域。請注意，允許最大效能和資源使用量的所有配置同時也能將副作用的風險降至最低。

評估：共用資源的副作用

無論是以獨佔方式指派給網域或是在網域之間共用，網路連結都可能遭到飽和攻擊或磁碟可能會超載。這類攻擊會影響攻擊期間的服務可用性。攻擊的目標不會受到破壞，也不會遺失任何資料。您可輕鬆地將此威脅的影響降至最低，但請記得這只限於 Oracle VM Server for SPARC 上的網路和磁碟資源。

對策：謹慎地指派硬體資源

請確認您只將必要的硬體資源指派給來賓網域。若不再需要某項未使用的資源 (例如只有安裝時需要的網路連接埠或 DVD 光碟機)，請務必將它取消指派。依循此作法，即可儘可能減少攻擊者可能的進入點數目。

對策：謹慎地指派共用資源

共用的硬體資源 (例如實體網路連接埠) 是 DoS 攻擊的可能目標。為了將 DoS 攻擊的影響侷限於單一來賓網域群組，請謹慎地判斷哪些來賓網域應共用哪些硬體資源。

例如，可依照相同的可用性和安全需求來分組共用硬體資源的來賓網域。除了分組外，您還可採取不同的資源控制。

您必須考量如何共用磁碟和網路資源。您可以透過專用的實體存取路徑或專用的虛擬磁碟服務來分隔磁碟存取以減少問題。

摘要：共用資源的副作用

本節中的所有對策都需要您瞭解您的建置和其安全意涵的技術細節。謹慎地規劃、清楚地記錄，並且儘可能維持簡單的架構。確認您瞭解虛擬化硬體的意涵，以便做好安全地建置 Oracle VM Server for SPARC 軟體的準備。

邏輯網域較不會受到共用 CPU 和記憶體的影響，因為它實際上很少共用。即使如此，最好還是採取資源控制，例如來賓網域內的 Solaris 資源管理。使用這些控制可防禦虛擬或非虛擬化環境的不當應用程式行為。

執行環境

圖 1-3,「執行環境的元件」"顯示執行環境的元件。每個元件提供的特定服務會共同組成執行實際執行來賓網域的整個平台。為了系統的完整性，正確設定元件是非常重要的。

所有執行環境元件都是攻擊者的可能目標。本節描述可能影響執行環境中每個元件的威脅。某些威脅與對策可能適用於一個以上的元件。

威脅：操控執行環境

透過操控執行環境，您有數種方式可以取得控制權。例如，您可以在 ILOM 中安裝操控韌體，以查看 I/O 網域內的所有來賓網域 I/O。這類攻擊可以存取和變更系統的配置。取得 Oracle VM Server for SPARC 控制網域控制權的攻擊者可任意重新設定系統，而取得 I/O 網域控制權的攻擊者則可變更連接的儲存裝置，例如啟動磁碟。

評估：操控執行環境

成功入侵執行環境中的 ILOM 或任何網域的攻擊者可以讀取和操控該網域所有的資料。攻擊者可以經由網路取得或因虛擬化堆疊錯誤而取得此存取權。發動這類攻擊並不容易，因為通常無法直接攻擊 ILOM 和網域。

讓執行環境免於遭到操控的對策是一種標準安全措施，因此應在所有系統上實作這些對策。標準安全措施可為執行環境提供額外的保護層，進一步降低受入侵和操控的風險。

對策：保護互動式存取路徑

確認您只針對系統上執行的應用程式建立必要的帳戶。

使用金鑰型認證或強式密碼，確保管理所需的帳戶均受到保護。這些金鑰或密碼不可在不同的網域間共用。另外，請考慮在採取某些動作時實作雙因素認證或「雙人管理規則 (Two-Person Rule)」。

請勿在 `root` 之類的帳戶使用匿名登入，以便確保您可對系統上執行的指令進行完整的追蹤和歸責。請針對個別管理員授予使用權限，讓他們只能存取允許執行的功能。請確認管理網路存取權一律使用像是 SSH 的加密，且管理員的工作站設定為高度安全系統。

對策：Oracle Solaris 作業系統最小安裝

系統上安裝的任何軟體都可能受到危害，因此請確認您只安裝必要的軟體，以儘可能降低受破壞的機會。

對策：強化 Oracle Solaris 作業系統

除了安裝最基本的 Oracle Solaris 作業系統之外，請設定套裝軟體以強化軟體對攻擊的防禦能力。首先，執行受限網路服務以有效停用 SSH 以外的所有網路服務。此原則是 Oracle Solaris 11 系統上的預設行為。如需如何保護 Oracle Solaris 作業系統的相關資訊，請參閱*Oracle Solaris 10 Security Guidelines* 與*Oracle Solaris 11 Security Guidelines* 。

對策：使用角色區隔與應用程式隔離

實際執行應用程式會連線至其他系統，因此必然較容易受到外部攻擊。請勿將實際執行應用程式建置到屬於執行環境的網域中。請確認您只將它們建置到沒有進一步權限的來賓網域。

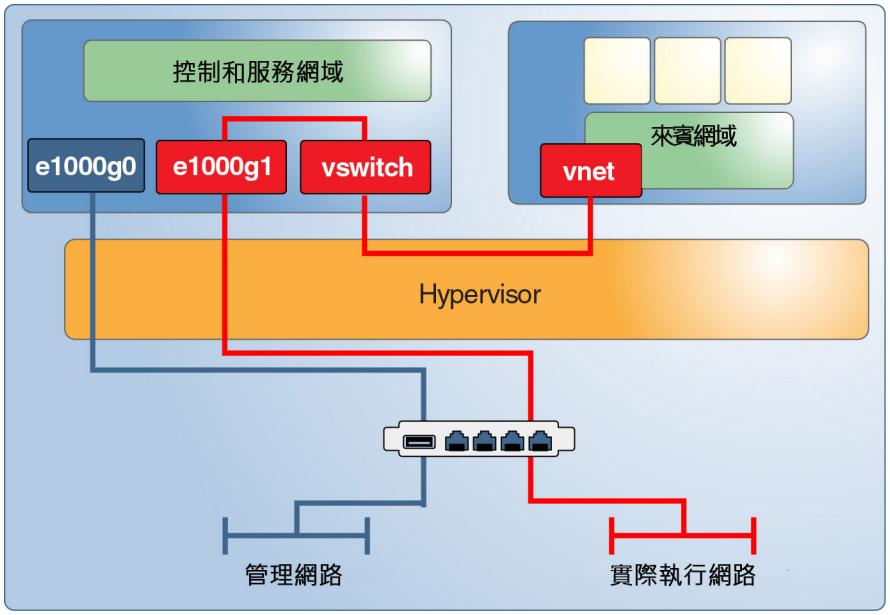
執行環境應只提供這些來賓網域必要的基礎架構。區隔執行環境與實際執行應用程式可讓您劃分管理權限。實際執行來賓網域管理員不需要執行環境的存取權，而執行環境管理員則不需要實際執行來賓網域的存取權。如果可以，請指派不同的執行環境 (例如控制網域和 I/O 網域) 角色給不同的網域。如果這些網域中的任一個網域受到危害，此類型的配置可減少您的損失。

您也可以將角色區隔延伸至您用來連線不同伺服器的網路環境。

對策：設定專用的管理網路

將配備有服務處理器 (SP) 的所有伺服器連線至專用的管理網路。也建議您在執行環境的網域中使用此配置。如果完全是網路環境，請在其專用的網路上代管這些網域。請勿將執行環境網域直接連線至指派給實際執行網域的網路。雖然您可透過 ILOM SP 提供的單一主控台連線來執行所有管理工作，但這種配置會導致管理過於複雜而無法實行。透過區隔實際執行網路與管理網路，您也可以同時防禦竊聽與操控攻擊。此類型的區隔也可排除攻擊者經由共用網路，從來賓網域對執行環境發動攻擊的可能性。

圖 1-5　　專用的管理網路



ILOM

目前所有的 Oracle SPARC 系統均包含內建的系統控制器 (ILOM)，其具有下列功能：

- 管理基本環境控制，例如風扇速度和機架電源
- 啟用韌體升級
- 提供控制網域的系統主控台

您可以透過序列連線存取 ILOM，或是使用 SSH、HTTP、HTTPS、SNMP 或 IPMI 透過網路連接埠存取 ILOM。Fujitsu M10 伺服器使用 XSCF (而非 ILOM) 執行相同的功能。

威脅：完全的系統拒絕服務攻擊

取得 ILOM 控制權的攻擊者可能會危害系統的許多層面，其中包括：

- 使所有執行中的來賓網域失去功能
- 安裝操控韌體以取得至少一個來賓網域的存取權

擁有此控制器裝置的任何系統都會發生這些狀況。虛擬化環境中的損失可能會遠大於實體環境，因為同一系統機器中即包含許多網域。

同樣地，取得控制網域或 I/O 網域控制權的攻擊者可以關閉對應的 I/O 服務，進而輕易地停用所有相依的來賓網域。

評估：完全的系統拒絕服務攻擊

ILOM 通常連線至管理網路，因此您也可以使用 IPMI 搭配 BMC 存取模組以便從控制網域存取 ILOM。因此，這兩種連線類型都應有完善的保護，並且應與一般的實際執行網路隔離。

同樣地，攻擊者可以透過網路或利用虛擬化堆疊錯誤來破壞服務，接著封鎖來賓 I/O 或將系統關閉。雖然損害有限 (因為資料不會遺失或受到危害)，但損害可能會影響大量的來賓網域。因此，請確認您已對此潛在威脅做好防禦，以限制可能發生的損害。

對策：保護 ILOM

ILOM 是用於控制重要功能的系統服務處理器，這些重要功能包括機架電源、Oracle VM Server for SPARC 啟動配置及控制網域的主控台存取權。下列是保護 ILOM 的措施：

- 將 ILOM 的網路連接埠放在與管理網路不同 (且在執行環境的網域中使用) 的網路區段。
- 停用非作業所需的所有服務，例如 HTTP、IPMI、SNMP、HTTPS 及 SSH。
- 設定只會授予必要權限的專用和個人管理員帳戶。為將管理員採取的動作有效歸責，請務必建立個人管理員帳戶。此類型的存取權對主控台存取、韌體升級和管理啟動配置而言格外重要。

Hypervisor

Hypervisor 是實作和控制實際硬體之虛擬化的韌體層。Hypervisor 包含下列元件：

- 實際的 Hypervisor，在韌體中實作並受系統 CPU 支援。
- 在控制網域中執行以設定 Hypervisor 的核心模組。
- 在 I/O 網域和服務網域中執行以提供虛擬化 I/O 的核心模組與常駐程式，以及透過邏輯網域通道 (LDC) 通訊的核心模組。

- 在來賓網域中執行以存取虛擬化 I/O 裝置的核心模組和裝置驅動程式，以及透過 LDC 通訊的核心模組。

威脅：破壞隔離機制

攻擊者可能會入侵 Hypervisor 提供的隔離執行階段環境，以劫持來賓網域或整個系統。此威脅可能會對系統造成最嚴重的損害。

評估：破壞隔離機制

模組化系統設計的特色是只要授予不同的權限等級給來賓網域、Hypervisor 和控制網域，就可以改善隔離機制。每個功能模組都會在獨立且可設定的核心模組、裝置驅動程式或常駐程式中實作。此模組需要全新的 API 和簡單的通訊協定，以降低整體的錯誤風險。

即使錯誤造成的破壞機率微乎其微，但這潛在的危害卻可能導致攻擊者控制整個系統。

對策：驗證韌體和軟體簽章

即使您可以直接透過 Oracle 網站下載系統韌體和作業系統修補程式，這些修補程式還是有可能被竄改。在安裝軟體之前，請確認您已驗證套裝軟體的 MD5 總和檢驗。所有可下載軟體的總和檢驗均是由 Oracle 發行。

對策：驗證核心模組

Oracle VM Server for SPARC 使用數個驅動程式和核心模組來實作整個虛擬化系統。隨 Oracle Solaris 作業系統發行的所有核心模組和多數二進位檔均含有數位簽章。使用 `elfsign` 公用程式可檢查每個核心模組和驅動程式的數位簽章。您可以使用 Oracle Solaris 11 `pkg verify` 指令來檢查 Oracle Solaris 二進位檔的完整性。請參閱 `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`。

首先，您必須建立 `elfsign` 公用程式的完整性。使用基本稽核和報告工具 (BART) 可自動化數位簽章驗證程序。Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`) 描述如何合併 BART 與 Solaris Fingerprint Database，以自動執行相同的完整性檢查。雖然已不再提供指紋資料庫，但您還是可以運用此文件中描述的概念以同樣的方法使用 `elfsign` 與 BART。

控制網域

控制網域 (通常具備 I/O 網域和服務網域角色) 必須受到妥善的保護，因為它能夠修改 Hypervisor 的配置，而此配置控制了所有連接的硬體資源。

威脅：控制網域拒絕服務攻擊

關閉控制網域會導致配置工具拒絕服務。因為只有變更配置時才需要使用控制網域，如果來賓網域是透過其他服務網域存取其網路和磁碟資源，則來賓網域就不會受到影響。

評估：控制網域拒絕服務攻擊

透過網路攻擊控制網域，就如同是攻擊任何受到妥善保護的 Oracle Solaris 作業系統執行處理。控制網域受到關閉或類似之拒絕服務攻擊的損害相對較低。不過，如果控制網域同時作為這些來賓網域的服務網域，來賓網域就會受到影響。

對策：保護主控台存取權

避免在執行環境網域中設定管理網路存取權。如此一來，您必須在控制網域使用 ILOM 主控台服務才能執行所有管理工作。但您仍然可以使用控制網域中執行的 `vntsd` 服務來對所有其他網域進行主控台存取。

請謹慎使用此選項。雖然此方法可降低經由管理網路受攻擊的風險，但一次只有一位管理員可以存取主控台。

如需安全地設定 `vntsd` 的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「How to Enable the Virtual Network Terminal Server Daemon」。

邏輯網域管理程式

邏輯網域管理程式在控制網域中執行，並可用於設定 Hypervisor 以及建立和設定所有網域和其硬體資源。請記錄和監視邏輯網域管理程式的使用狀況。

威脅：未經授權使用配置公用程式

攻擊者可能會控制管理員的使用者 ID，或來自不同群組的管理員可能會在未經授權的情況下存取其他系統。

評估：未經授權使用配置公用程式

透過實作妥善維護的識別管理，確認管理員沒有不必要的系統存取權。另外，請實作嚴格細分的存取控制和其他措施，例如雙人管理規則。

對策：實施雙人管理規則

請考慮為邏輯網域管理程式實作雙人管理規則並使用權限實作其他管理工具。Enforcing a Two Man Rule Using Solaris 10 RBAC (`https://blogs.oracle.com/gbrunett/entry/enforcing_a_two_man_rule`)。此規則可保護系統免於社交工程攻擊、管理帳戶盜用和人為錯誤。

對策：針對邏輯網域管理程式使用權限

透過使用 `ldm` 指令的權限，您可以實作細分的存取控制並維持完整的回溯性。如需設定權限的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 。使用權限有助於避免人為錯誤，因為並非所有管理員都可使用 `ldm` 指令的所有功能。

對策：強化邏輯網域管理程式

停用不必要的網域管理程式服務。邏輯網域管理程式提供網域存取、監視和移轉的網路服務。停用網路服務有助於減少邏輯網域管理程式正常運作時的受攻擊面。此方法可防禦拒絕服務攻擊和其他濫用這些網路服務的嘗試。

注意 - 停用網域管理程式服務有助於減少受攻擊面，但這樣做對特定配置所造成的副作用卻是無法預知的。

在下列任一網路服務未使用時將其停用：

- TCP 連接埠 `8101` 上的移轉服務

  若要停用此服務，請參閱 `ldmd`(1M) 線上手冊中的 `ldmd/incoming_migration_enabled` 與 `ldmd/outgoing_migration_enabled` 特性。
- TCP 連接埠 `6482` 上的 Extensible Messaging and Presence Protocol (XMPP) 支援

  如需如何停用此服務的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「XML Transport」。

  停用 XMPP 會使得部分管理工具和關鍵的 Oracle VM Server for SPARC 功能無法運作。請參閱第 35 頁的「Oracle VM Server for SPARC XML 介面」。
- UDP 連接埠 `161` 上的簡易網路管理協定 (SNMP)

  決定是否要使用 Oracle VM Server for SPARC 管理資訊庫 (MIB) 來監視網域。此功能需要啟用 SNMP 服務。依據您的選擇執行下列其中一項動作：

  - **啟用 SNMP 服務以使用 Oracle VM Server for SPARC MIB。**安全地安裝 Oracle VM Server for SPARC MIB。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「How to Install the Oracle VM Server for SPARC MIB Software Package」及*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「Managing Security」。

- **停用 SNMP 服務。**如需如何停用此服務的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「How to Remove the Oracle VM Server for SPARC MIB Software Package」。
- 多點傳送位址 `239.129.9.27` 與連接埠 `64535` 上的尋找服務

注意 - 請注意，`ldmd` 常駐程式也會使用此尋找機制來偵測自動指派 MAC 位址時所發生的衝突。若您停用尋找服務，MAC 位址衝突偵測功能將無法運作，而自動 MAC 位址配置也將因此無法正確運作。

您不能在邏輯網域管理程式常駐程式 (`ldmd`) 執行時停用此服務。請使用 Oracle Solaris 的 IP 篩選功能封鎖此服務的存取，以儘可能減少邏輯網域管理程式的受攻擊面。封鎖存取可防止公用程式遭到未經授權的使用，如此可有效防禦拒絕服務攻擊和其他濫用這些網路服務的嘗試。請參閱*Oracle Solaris Administration: IP Services* 中的第 20 章「IP Filter in Oracle Solaris (Overview)」與*Oracle Solaris Administration: IP Services* 中的「Using IP Filter Rule Sets」。

另請參閱第 24 頁的「對策：保護 ILOM」。

服務網域

服務網域會將某些虛擬服務提供給系統上的來賓網域。服務可能包含虛擬交換器、虛擬磁碟或虛擬主控台服務。

圖 1-6,「服務網域範例」"顯示提供主控台服務的範例服務網域。控制網域通常會代管主控台服務，因此也是服務網域。執行環境網域通常將控制網域、I/O 網域及服務網域的功能合併在一或兩個網域中。

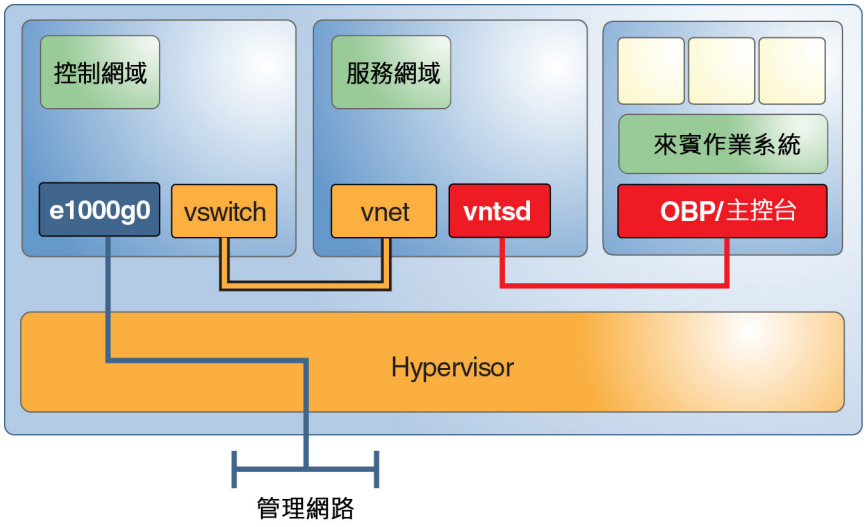
威脅：操控服務網域

取得服務網域控制權的攻擊者可以竄改資料，或是監聽透過提供的服務所進行的任何通訊。這類控制權可能包含來賓網域的主控台存取權、網路服務的存取權或磁碟服務的存取權。

評估：操控服務網域

雖然攻擊策略與控制網域上的攻擊策略相同，但可能造成的損失卻較少，因為攻擊者無法修改系統配置。最終的損失可能包括服務網域提供的資料被竊或被竄改，但並不是竄改任何資料來源。視服務性質而定，攻擊者可能需要交換核心模組。

圖 1-6 服務網域範例



對策：細分服務網域

可以的話，請讓每個服務網域只提供一個服務給其用戶端。如果服務網域受到入侵，此配置可確保只有一個服務會受到危害。不過，請務必權衡此配置類型的重要性和額外的複雜性。請注意，強烈建議您增加備援的 I/O 網域。

對策：隔離服務網域與來賓網域

您可以將 Oracle Solaris 10 和 Oracle Solaris 11 服務網域與來賓網域隔離。下列解決方案是以慣用的實作順序顯示：

- 確認服務網域與來賓網域未共用相同的網路連接埠。此外，請勿在服務網域上探索任何虛擬交換器介面。若為 Oracle Solaris 11 服務網域，請勿在用於虛擬交換器的實體連接埠上探索任何 VNIC。
- 如果您必須在 Oracle Solaris 10 作業系統和 Oracle Solaris 11 作業系統使用相同的網路連接埠，請將 I/O 網域流量配置於來賓網域未使用的 VLAN 中。
- 如果您無法實作上述任一解決方案，請勿在 Oracle Solaris 10 作業系統中探索虛擬交換器和在 Oracle Solaris 11 作業系統中套用 IP 篩選。

對策：限制虛擬主控台存取權

確認只將個別虛擬主控台的存取權指派給必須存取那些虛擬主控台的使用者。此配置可確保沒有任何一位管理員可以存取所有主控台，以防止被盜用的帳戶存取不是指派給它的主控台。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「How to Create Default Services」。

I/O 網域

可直接存取實體 I/O 裝置 (例如網路連接埠或磁碟) 的任何網域都是 I/O 網域。如需設定 I/O 網域的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的第 5 章「Configuring I/O Domains」。

如果某個 I/O 網域提供 I/O 服務給來賓網域以提供硬體的網域存取權，則它也可能是服務網域。

威脅：發生 I/O 網域或服務網域的拒絕服務攻擊

攔阻 I/O 網域之 I/O 服務的攻擊者會設法讓所有相依的來賓網域一起被攔阻。透過讓後端網路或磁碟基礎架構超載或是在網域造成錯誤，就能成功發動 DoS 攻擊。任一種攻擊都可能使網域停止回應或癱瘓。同樣地，中斷服務網域之服務的攻擊者也會讓相依於這些服務的所有來賓網域立即停止回應。如果來賓網域停止回應，它將會在 I/O 服務恢復時繼續作業。

評估：發生 I/O 網域或服務網域的拒絕服務攻擊

DoS 攻擊通常經由網路發動。能成功發動這類攻擊是因為網路連接埠已開啟以進行通訊，因此而可能由於網路流量過大而導致癱瘓。由於服務中斷，便使得相依的來賓網域遭到攔阻。磁碟資源上的類似攻擊可能是由 SAN 基礎架構或 I/O 網域攻擊所造成，而唯一的損失就是會暫時中斷所有相依的來賓網域。DoS 攻擊的影響可能很嚴重，但資料不會受到危害或遺失，系統配置也不會變更。

對策：仔細設定 I/O 網域

設定多個 I/O 網域可減少單一網域失敗或受危害的影響。您可以將個別的 PCIe 插槽指派給來賓網域，或提供它 I/O 網域的功能。若擁有 PCIe 匯流排的根網域損毀，就會重設該匯流排，這會導致已被指派個別插槽的網域後續發生損毀。此功能無法完全排除必須有兩個根網域 (各擁有獨立的 PCIe 匯流排) 的需求。

對策：設定備援的硬體和根網域

高可用性也有助於強化安全性，因為可確保服務足以抵擋拒絕服務攻擊。Oracle VM Server for SPARC 實作高可用性方法，例如在備援的 I/O 網域中使用備援磁碟和網路資源。此配置選項可允許輪流升級 I/O 網域，並保護因為 DoS 攻擊導致 I/O 網域失敗的影響。隨著 SR-IOV 的出現，來賓網域可直接存取個別的 I/O 裝置。不過，無法使用 SR-IOV 時，請考慮建立備援的 I/O 網域。請參閱第 29 頁的「對策：細分服務網域」。

威脅：操控 I/O 網域

I/O 網域可直接存取後端裝置 (通常為磁碟)，以將其虛擬化並提供給來賓網域。順利入侵的攻擊者會取得這些裝置的完整存取權，且可以在來賓網域的啟動磁碟上讀取機密資料或操控軟體。

評估：操控 I/O 網域

I/O 網域攻擊就像是在服務網域或控制網域上發動成功攻擊一樣。I/O 網域是攻擊者覬覦的目標，因為可藉此存取大量的磁碟裝置。因此，在處理虛擬化磁碟上執行之來賓網域的機密資料時，請考慮如何防禦此威脅。

對策：保護虛擬磁碟

當 I/O 網域受到入侵時，攻擊者會取得來賓網域之虛擬磁碟的完整存取權。

請採取下列動作以保護虛擬磁碟的內容：

- **加密虛擬磁碟內容。**在 Oracle Solaris 10 系統上，您可以使用可加密自身資料的應用程式，例如 `pgp`/`gpg` 或 Oracle 11g 加密表格空間。在 Oracle Solaris 11 系統上，您可以使用 ZFS 加密資料集來為檔案系統中儲存的所有資料提供通透的加密。
- **經由數個虛擬磁碟將資料散佈至不同的 I/O 網域。**來賓網域可在從兩個 I/O 網域取得的數個虛擬磁碟間分段建立等量 (RAID 1/RAID 5) 磁碟區。如果其中一個 I/O 網域受到危害，攻擊者將難以利用可取得的資料部分。

來賓網域

來賓網域不是執行環境的一部分，卻是最可能遭受攻擊的目標，因為它們會連線至網路。入侵虛擬化系統的攻擊者可以在執行環境上發動攻擊。

對策：保護來賓網域作業系統

來賓網域上的作業系統通常是阻擋任何攻擊的第一道防線。除了源自資料中心的攻擊外，攻擊者在嘗試破壞來賓網域的隔離機制和操控整個環境之前，必須先入侵與外部連線的來賓網域。因此，您必須強化來賓網域的作業系統。

為進一步強化作業系統，您可以在 Solaris Zone 中建置您的應用程式，以在應用程式的網路服務與來賓網域作業系統之間建立額外的隔離層。成功在服務上發動的攻擊只會危害此區域而不會連累底層的作業系統，如此可防止攻擊者將控制權延伸到該區域所擁有之資源以外的部分。因此，最終破壞來賓隔離機制的困難度將會提高。如需保護來賓作業系統的相關資訊，請參閱*Oracle Solaris 10 Security Guidelines* 與*Oracle Solaris 11 Security Guidelines* 。

♦ ♦ ♦ 第 2 章

2 安全的 Oracle VM Server for SPARC 安裝與配置

本章描述與安裝和設定 Oracle VM Server for SPARC 軟體相關的安全考量。

安裝

Oracle VM Server for SPARC 軟體會以安全的方式自動安裝為 Oracle Solaris 11 套裝軟體。在安裝完成後，您必須具備管理員權限才能設定網域的權限和授權功能。這些功能預設為停用狀態。

安裝後配置

安裝 Oracle VM Server for SPARC 軟體之後，請執行下列工作來以最安全的方式使用軟體：

- 以必要的虛擬 I/O 服務 (如虛擬交換器、虛擬磁碟伺服器和虛擬主控台集中器服務) 設定控制網域。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的第 3 章「Setting Up Services and the Control Domain」。
- 設定來賓網域。請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的第 4 章「Setting Up Guest Domains」。

  您可以透過管理網路和實際執行網路使用虛擬交換器設定來賓網域。在此情況下，虛擬交換器是透過以實際執行網路介面作為虛擬交換器網路裝置的方式建立的。請參閱第 23 頁的「對策：設定專用的管理網路」。

  當來賓網域的任一虛擬磁碟有安全性問題時，來賓網域也會有安全性問題。因此，請確定虛擬磁碟 (連接網路的儲存裝置、在本機儲存的磁碟影像檔案或實體磁碟) 存放在安全的位置。

  `vntsd` 常駐程式預設為停用狀態。當此常駐程式啟用時，登入控制網域的所有使用者都能夠連線至來賓網域的主控台。若要避免此類型的存取，請確定 `vntsd` 常駐程式是停用狀態，或是將使用者權限限制為只有經認可的使用者可以連線至主控台。
- 服務處理器 (SP) 預設會以安全的方式設定。如需使用 Integrated Lights Out Management (ILOM) 軟體管理 SP 的相關資訊，請參閱您的平台適用的文件，網址

為：http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html。

♦ ♦ ♦ 第 3 章

3 開發人員的安全考量

本章提供開發 Oracle VM Server for SPARC 軟體之應用程式的開發人員資訊。

Oracle VM Server for SPARC XML 介面

您可以透過可延伸標記語言 (XML) 通訊機制來建立與 Oracle VM Server for SPARC 軟體互動的外部程式。XML 使用 Extensible Messaging and Presence Protocol (XMPP)。

攻擊者可能會嘗試利用此網路協定存取系統，因此請考慮停用 XMPP。如需停用 XMPP 的相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「XML Transport」。如需邏輯網域管理程式使用的安全機制相關資訊，請參閱*Oracle VM Server for SPARC 3.3 Administration Guide* 中的「XMPP Server」。

停用 XMPP 會使得 Oracle VM 管理程式 或 Ops Center 無法管理系統，也會使您無法使用部分關鍵的 Oracle VM Server for SPARC 功能，如下列指令：

- `ldm migrate-domain`
- `ldm init-system`
- `ldm remove-core -g`
- `ldm add-memory`
- `ldm set-memory`
- `ldm remove-memory`
- `ldm grow-socket`
- `ldm shrink-socket`
- `ldm set-socket`
- `ldm list-socket`

♦ ♦ ♦ 附錄 A

安全建置檢查清單

本檢查清單摘要強化 Oracle VM Server for SPARC 環境可採取的步驟。您可以在其他文件中找到詳細資訊，例如：

- *Oracle VM Server for SPARC 3.3 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Oracle VM Server for SPARC 安全檢查清單

- 在來賓網域中執行與在非虛擬化環境中一樣的 Oracle Solaris 作業系統強化步驟。
- 使用「LDoms 管理」與「LDoms 複查」權限設定檔，將適當的權限委派給使用者。
- 使用權限來限制網域主控台的存取權，限定只有您 (Oracle VM Server for SPARC 的管理員) 可以存取。
- 停用不必要的網域管理程式服務。
- 只將相同安全類別的來賓網域建置到實體平台。
- 確定執行環境的管理網路與來賓網域的管理網路之間未連線。
- 只將必要的資源指派給來賓網域。