# Netra Modular System 安全指南

文件號碼： E68388-01
2015 年 8 月

**文件號碼：** E68388-01



**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


安全簡介 ..... 7
- 基本安全原則 ..... 7
- 進階安全考量 ..... 7
- 安全功能 ..... 8
  - 網路流量隔離 ..... 8
  - Oracle ILOM 的安全管理 ..... 9

規劃安全環境 ..... 11
- 預設網路 ..... 11
- 使用者帳號 ..... 12
- 預設安全設定值 ..... 12

保護硬體的安全 ..... 13
- 存取限制 ..... 13
- 序號 ..... 13
- 硬碟 ..... 14

保護軟體的安全 ..... 15
- ▼ 防止未經授權的存取 (Oracle Linux) ..... 15
- ▼ 防止未經授權的存取 (Oracle ILOM) ..... 15
- ▼ 防止未經授權的存取 (Oracle VM Server With Oracle Linux) ..... 15
- Oracle Hardware Management Pack 安全性 ..... 16

尋找相關安全指南 ..... 17
- 安全指南 ..... 17

# 安全簡介

Oracle Netra Modular System 為事先接線的預先整合平台，在資料中心內可完全虛擬化以減少成本和建置時間。模組化系統內含您指定的硬體，並在工廠組裝完成，然後才會交貨給您。

這些主題描述模組化系統的安全概念和功能：


- 「基本安全原則」[7]
- 「進階安全考量」[7]
- 「安全功能」[8]


## 基本安全原則

對於所有模組化系統軟體和硬體，請遵循這些基本安全原則：

- 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，或共用金鑰) 來識別。認證可確保硬體或軟體的使用者身分。預設會使用本機使用者和密碼來進行認證作業。也可以使用共用金鑰的認證方式。
- 資料記錄與稽核 – 資料記錄與稽核會在系統上維護使用者的活動記錄。模組化系統軟體和硬體功能讓管理員能夠監督登入活動以及維護硬體資產：
  - 使用者登入活動會透過系統記錄來進行監督。系統管理員和服務帳戶具有指令的存取權，若使用不當，可能會造成危害或資料損失。
  - 硬體資產通常透過序號來進行追蹤。所有介面卡、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。

## 進階安全考量

除了基本安全原則之外，模組化系統同時提供深度的容錯能力和防禦。模組化系統提供一組整合良好的安全功能，以滿足重要的安全需求和考量。以下小節描述這些原則：

- 重要任務工作負載的容錯能力 – 模組化系統可以防止內部使用者或外部人員採取之意外和惡意動作所造成的損害，或將此損害降至最低程度。考量重要任務工作負載

來挑選硬體和軟體平台的組織均可獲得如此的保證。下列措施屬於 Oracle Maximum Availability Architecture 最佳措施的一部分，可增加容錯能力：

- 確認使用的元件在設計、製造與測試的過程中均已評估為能夠共同運作並支援安全建置架構。模組化系統支援安全隔離、存取控制、服務品質以及安全管理等功能。
- 減少其組成產品既有的攻擊面，可協助將機器的整體暴露程度降至最低。
- 使用開放並經過核可的協定作為配套措施，以及使用支援傳統安全目標 (包括強式認證、存取控制、機密性、完整性與可用性) 的 API，來保護機器的作業和管理介面。
- 確認軟體和硬體所包含的功能可以維持服務的可用性，甚至發生故障也可提供服務。攻擊者嘗試停用系統中的一或多個個別元件時，這些功能就可以派上用場。

- 深度防禦以保護作業環境 – 模組化系統搭載多種獨立且相互強化的安全控制功能，為工作負載和資料建立安全的作業環境。模組化系統支援的深度防禦原則如下：
  - 提供強式的保護配套措施，以保護傳輸中、使用中以及非使用中資訊的安全。伺服器和網路層均提供安全控制。每一層的獨特安全控制都可以與其他層整合，以建立強化的分層安全架構。
  - 支援使用良好定義且開放的標準、協定及介面。模組化系統可以整合至現有的安全原則、架構、措施以及標準。

# 安全功能

模組化系統的硬體與軟體均經過強化。Oracle 也針對 NTP 和 SSH 之類的服務提供建議的安全配置。此外，模組化系統的架構還針對核心元件提供安全功能。這些安全功能是最常被組織用來建置分層安全策略的功能。這些功能分為下列幾個類別：


- 「網路流量隔離」[8]
- 「Oracle ILOM 的安全管理」[9]


## 網路流量隔離

如果您要合併 IT 基礎架構、實作共用服務架構以及提供安全的多用戶服務，請考慮隔離各個網路流量。模組化系統可根據需求，提供實作隔離政策和策略的彈性。

在實體網路層中，用戶端的存取會與裝置管理及裝置間的通訊隔離。用戶端和管理網路流量會被隔離在不同的網路中。用戶端存取是透過備援的 10 Gbps 乙太網路提供，確保使用者能夠可靠地高速存取系統上執行的服務。管理存取是透過實體獨立的 1 Gbps 乙太網路提供。這樣便可以在作業和管理之間提供獨立的網路環境。

組織可以透過設定虛擬區域網路 (VLAN)，進一步區隔用戶端存取乙太網路的網路流量。VLAN 會根據其需求來區隔網路流量。Oracle 建議 VLAN 使用加密的協定，以確保通訊的機密性和完整性。

# Oracle ILOM 的安全管理

安全控制和安全功能的結合是適當保護個別應用程式和服務安全的必要措施。若要獲得全方位的管理功能，以維持建置的服務和系統的安全性，這二者同樣重要。模組化系統運用 Oracle ILOM 的安全管理功能。

Oracle ILOM 是內嵌在模組化系統之運算節點中的 SP。Oracle ILOM 用於執行頻外管理活動，如下：

- 提供安全存取，以執行資料庫與儲存體伺服器的安全 Lights Out Management。存取包括受到 SSL 保護的 Web 型存取、使用安全 Shell 的指令行存取，以及 IPMI v2.0 和 SNMPv3 協定。
- 使用以角色為基礎的存取控制模型，以達到區隔工作的需求。個別使用者會被指派給只能執行有限功能的特定角色。
- 提供所有登入和配置變更的稽核記錄。每一筆稽核記錄項目都會列出使用者執行的動作和時戳。稽核記錄可以讓組織偵測未經授權的活動或變更作業，並反向追查進行這些動作的特定使用者。

如需有關 Oracle ILOM 安全性的詳細資訊，請參閱「*Oracle ILOM* 安全指南」，網址為：http://www.oracle.com/goto/ILOM/docs。

# 規劃安全環境

安全準則必須在 Netra Modular System 送達之前先行備妥。系統安裝之後，請定期複查並調整安全準則，使安全準則隨著組織的安全需求保持在最新狀態。

這些主題提供安裝 Netra Modular System 的安全準則：

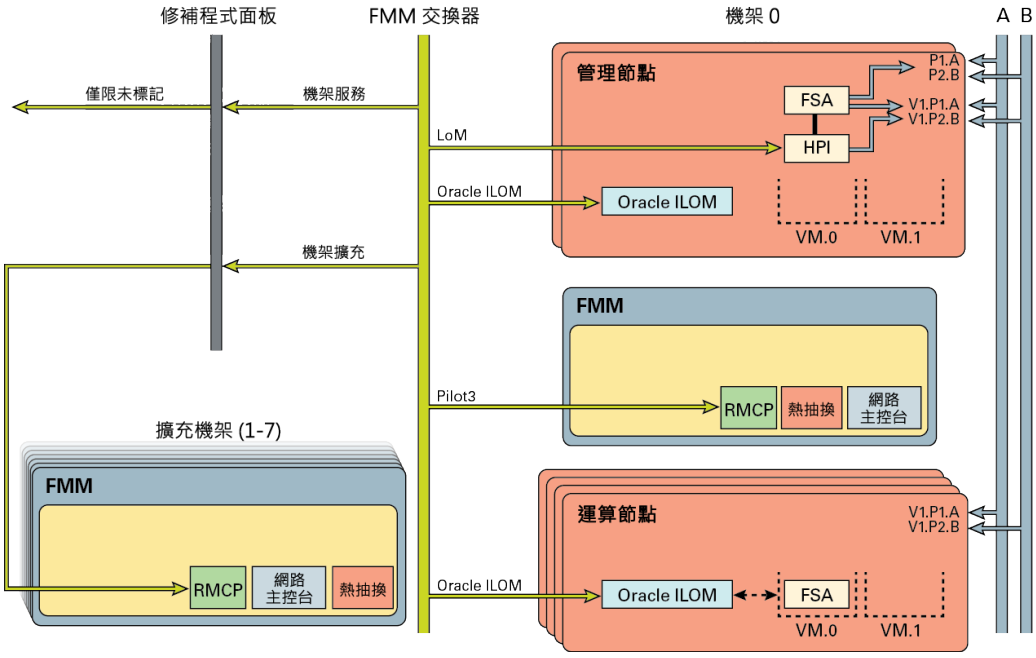
- 「預設網路」[11]
- 「使用者帳號」[12]
- 「預設安全設定值」[12]

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。

## 預設網路

下圖和描述說明 Netra Modular System 的預設網路。

- 系統/遙測網路 (淺綠色網路) 包括管理節點的 LoM 連接埠 (透過 FMM 交換器，位於 VLAN 4090 上)。
- 遙測 ILOM 網路 (位於使用 FMM 的內部 VLAN 4094) 包括運算節點 Oracle ILOM 和透過 FMM 交換器的網路節點 Oracle ILOM。
- 配線架將 Telemetry 網路延伸至機架 1 到 7。多機架配置支援相同子網路和具有不同機架 ID 的 VLAN
- VLAN(1) 透過適當的認證方式，提供其他服務給遙測網路。
- 資料網路 (A &B) 提供對 FSA 節點的頻內存取。
- HA 應用程式可以透過模組化系統公開的介面 (JMX、C- API 等等) 來管理機架。




# 使用者帳號

此表格列出模組化系統元件的預設使用者和密碼。安裝 Netra Modular System 後，請變更所有預設的密碼。

| 元件 | 使用者名稱和密碼 |
|---|---|
| 乙太網路交換器 | `root/changeme`<br>注意 - 保護 `admin` 使用者的 `enable mode password` 和 `secret` 值。 |
| 管理和運算節點 | `root/changeme` |

# 預設安全設定值

模組化系統在安裝時會附有多種預設的安全設定。如果可能且可行的話，請設定安全預設設定。請參閱您使用之版本的 Oracle ILOM 預設設定，網址為：`http://www.oracle.com/goto/ILOM/docs`。

# 保護硬體的安全

您的安全架構是建立在實體隔離和存取控制的基礎上。確實將實體系統安置在安全的環境中，可保護系統免於未經授權的存取。同樣地，記錄所有序號有助於避免硬體元件遭到未經授權的使用。

下列小節提供模組化系統的一般硬體安全準則。


- 「存取限制」[13]
- 「序號」[13]
- 「硬碟」[14]


## 存取限制

- 將系統及相關設備安置在上鎖且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，否則請將機架門隨時保持上鎖。將門上鎖也可以有效限制熱插式或熱抽換式裝置的使用。
- 將所有備用替換零件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。
- 定期檢查機架鎖和備用機櫃鎖是否確實上鎖且未受損，以避免 (或察覺) 鎖被人破壞或不小心未將門上鎖的情況。
- 將機櫃鑰匙放置在限制人員進出的安全位置。
- 限制使用 USB 主控台。系統控制器、PDU 及網路交換器等裝置都具有 USB 連線。實際取用元件是較為安全的存取方法，因為比較不易受到網路攻擊。
- 將主控台連線外部 KVM 以啟用遠端主控台存取。KVM 裝置通常支援雙因素認證、集中式存取控制及稽核功能。如需有關 KVM 之安全準則和最佳措施的詳細資訊，請參閱 KVM 裝置提供的文件。

## 序號

請在收到元件時仔細記錄所有序號並列入資產，以避免硬體元件遭到未經授權的使用。在安裝或使用任何元件之前，請將元件序號與收到元件時所記錄的序號加以比對，以確認其真偽。請遵循下列措施來保護硬體：

- 記錄所有硬體的序號。
- 為所有重要的電腦硬體項目 (例如，替換零件) 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。
- 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。

無線電頻率識別 (RFID) 讀取器可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。

# 硬碟

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妥善處理。

- 請參閱貴單位的資料保護政策，以判斷最適當的硬碟處理方式。
- 如有需要，請利用 Oracle 的 Customer Data and Device Retention 服務。

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

# 保護軟體的安全

大部分的硬體安全會透過軟體方式來實作。下列小節提供 Netra Modular System 的一般軟體安全準則。


- 「防止未經授權的存取 (Oracle Linux)」[15]
- 「防止未經授權的存取 (Oracle ILOM)」[15]
- 「防止未經授權的存取 (Oracle VM Server With Oracle Linux)」[15]
- 「Oracle Hardware Management Pack 安全性」[16]


## ▼ 防止未經授權的存取 (Oracle Linux)

- 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、使用安全性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。

## ▼ 防止未經授權的存取 (Oracle ILOM)

- 使用 Oracle ILOM 指令可以限制對 Oracle ILOM 韌體的存取、變更出廠設定密碼、限制使用 root 超級使用者帳號，並保護 SP 的專用網路。

  請參閱您所使用之版本的「*Oracle ILOM* 安全指南」，網址為：http://www.oracle.com/goto/ILOM/docs。

## ▼ 防止未經授權的存取 (Oracle VM Server With Oracle Linux)

- 使用 Oracle Linux 指令可以限制對 Oracle VM Server 軟體的存取、使用安全性功能以及保護應用程式。

  請參閱 *Oracle VM Security Guide for Release 3.3*，網址為：http://docs.oracle.com/cd/E50245_01/E50254/html/index.html。

# Oracle Hardware Management Pack 安全性

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，可用來管理您的系統。

- 硬體管理代理程式 SNMP 外掛程式 – SNMP 是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 系統，而不需要連線兩個管理點：主機和 Oracle ILOM。這項功能可以讓您使用單一 IP 位址 (主機 IP 位址) 監視多個系統。

  SNMP 外掛程式是在 Oracle 系統的主機作業系統中執行。SNMP 外掛程式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 Oracle Linux，模組會新增到 `net-snmp` 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。
- 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」，網址為：`http://www.oracle.com/goto/OHMP/docs`。

# 尋找相關安全指南

## 安全指南

這些主題描述保護相關產品安全的政策和程序：

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux Security Guide for Release 6*，網址為 http://docs.oracle.com/cd/E37670_01/E36387/html/index.html
- *Oracle ILOM* 安全指南，網址為 http://www.oracle.com/goto/ILOM/docs
- *Oracle VM Security Guide for Release 3.3*，網址為 http://docs.oracle.com/cd/E50245_01/E50254/html/index.html
- *Oracle Hardware Management Pack (HMP)* 安全指南，網址為 http://www.oracle.com/goto/OHMP/docs