Oracle® ILOM 安全指南韌體發行版本 3.0、3.1 及 3.2

文件號碼： E40362-04
2015 年 10 月

文件號碼： E40362-04

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** — 提供關於 Oracle ILOM 安全工作準則的 Web 和 CLI 資訊。請將本指南與 Oracle ILOM 文件庫中的其他指南一起搭配使用。
- **對象** — 具備系統硬體管理經驗之技術人員、系統管理員及授權的 Oracle 服務提供者。
- **必備知識** — 具備配置和管理 Oracle 伺服器的經驗。

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/goto/ilom/docs。

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

每一 Oracle ILOM 韌體發行版本的安全功能

請使用下表識別每一韌體發行版本中所提供的 Oracle ILOM 安全功能。

韌體版本適用性	安全功能	如需詳細資訊，請參閱：
全部	認證與授權	■ 「保護 Oracle ILOM 使用者存取」[21]
全部	專用的安全管理連線	■ 「保護實體管理連線」[13] ■ 「維護安全管理連線」[47]
全部	加密的預先配置網路連接埠	■ 「預先配置的服務與網路連接埠」[17]
全部	IPMI 2.0 安全管理	■ 「配置 IPMI 管理存取以獲得最高安全性」[43]
全部	安全 Shell 金鑰加密配置	■ 「使用伺服器端金鑰加密 SSH 連線」[40] ■ 「將 SSH 金鑰附加到使用者帳戶以執行自動化 CLI 認證」[41]
全部	SNMP 3.0 安全管理	■ 「配置 SNMP 管理存取以獲得最高安全性」[42]
全部	SSL 協定與憑證	■ 「將自訂 SSL 憑證與私密金鑰上傳至 Oracle ILOM」[34] ■ 「使用 OpenSSL 取得 SSL 憑證與私密金鑰」[33] ■ 「啟用最安全的 SSL 與 TLS 加密特性」[35]
全部	遠端主控台加密與安全協定	■ 「安全地使用遠端 KVMS」[50]
3.0.4 和更新版本	KVMS 主機鎖定配置	■ 「結束 KVMS 階段作業時鎖定主機存取」[29]
3.0.4 和更新版本	階段作業逾時配置	■ 「設定非作用中 Web 階段作業的逾時間隔」[37] ■ 「設定非作用中 CLI 階段作業的逾時間隔」[39]
3.0.12 和更新版本	本機主機連結已認證的階段作業	■ 「偏好的已認證主機連結存取」[48]
3.0.8 和更新版本	登入標題配置	「使用登入標題保護系統存取 (3.0.8 及更新版本)」[31]
3.0.8 至 3.1.2	WS-Management 安全存取	■ 「配置 WS-Management 存取以獲得最高安全性」[46]
3.1.0 和更新版本	個別的稽核日誌	■ 「監督稽核事件以找出未經授權的存取」[55]
3.1.0 和更新版本	實體安全存在性檢查	■ 「重設 `root` 帳戶預設密碼的實體安全存在性」[53]
3.2.4 和更新版本	IPMI 1.5 的可配置特性	■ 「配置 IPMI 管理存取以獲得最高安全性」[43]
3.2.4 和更新版本	TLS 協定版本 1.1 和 1.2	■ 「啟用最安全的 SSL 與 TLS 加密特性」[35]
3.2.4 和更新版本	KVMS 階段作業數目	■ 「限制 Remote System Console Plus 的可檢視 KVMS 階段作業 (3.2.4 或更新版本)」[30]
3.2.4 和更新版本	符合 FIPS 規範的加密支援	■ 「在建置時選擇是否要配置 FIPS 模式」[14] ■ 「FIPS 模式啟用時不支援的功能」[16] ■ 「建置後保護使用者存取的考量」[52]

韌體版本適用性	安全功能	如需詳細資訊，請參閱：
3.2.5 和更新版本	SSH 伺服器狀況和弱加密	■ 「管理 SSH 伺服器狀況和弱加密 (3.2.5 及更新版本) 」[38]
3.2.5 和更新版本	本機使用者帳戶的密碼制定原則	■ 「設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)」[26]

其他安全資訊

如需保護 Oracle ILOM 的其他相關資訊，請參閱本指南下列各節：

- 「Oracle ILOM 安全最佳措施檢查清單」
- 「Oracle ILOM 的建置安全最佳措施 」
- 「Oracle ILOM 建置後的安全最佳措施」

Oracle ILOM 安全最佳措施檢查清單

Oracle Integrated Lights Out Manager (ILOM) 是預先安裝在所有 Oracle 伺服器和多數傳統 Sun 伺服器上的服務處理器 (SP)。系統管理員可使用 Oracle ILOM 的使用者介面來執行遠端伺服器管理工作和即時的伺服器狀況監督作業。

為確保您的環境實行 Oracle ILOM 最佳安全措施，系統管理員應參考下列檢查清單中建議的安全工作：

- 「伺服器建置的安全檢查清單」[11]
- 「伺服器建置後的安全檢查清單」[12]

相關資訊

- 「Oracle ILOM 的建置安全最佳措施 」
- 「Oracle ILOM 建置後的安全最佳措施」
- 每一 Oracle ILOM 韌體發行版本的安全功能[9]

伺服器建置的安全檢查清單

計畫建置新伺服器時，為判斷哪些是最佳的 Oracle ILOM 安全措施，系統管理員應參考下列表 1,「檢查清單 - 在伺服器建置時配置 Oracle ILOM 安全 」中建議的安全工作清單。

表 1　檢查清單 - 在伺服器建置時配置 Oracle ILOM 安全

✓	安全工作	適用的韌體版本	如需詳細資訊，請參閱：
	建立 Oracle ILOM 的安全專用管理連線。	所有韌體版本	■ 「保護實體管理連線」[13]
	在建置時或建置後 (或都不需要) 決定是否需要符合 FIPS 140-2 安全規範。	韌體版本 3.2.4 和更新版本	■ 「在建置時選擇是否要配置 FIPS 模式」[14] ■ 「FIPS 模式啟用時不支援的功能」[16]
	設定所有本機使用者的密碼制定原則	韌體版本 3.2.5 和更新版本	■ 「設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)」[26]
	修改為預先配置之管理員 `root` 帳戶提供的預設密碼。	所有韌體版本	■ 「避免建立共用的使用者帳戶」[22] ■ 「第一次登入時修改 `root` 帳戶的預設密碼」[27]

✓	安全工作	適用的韌體版本	如需詳細資訊，請參閱：
	決定您的目標環境是否適用預先配置的 Oracle ILOM 服務及其開啟的網路連接埠。	所有韌體版本	■ 「保護服務與開啟的網路連接埠」[17]
	配置 Oracle ILOM 的使用者存取。	所有韌體版本	■ 「保護 Oracle ILOM 使用者存取」[21] ■ 「建立具有以角色為基礎之權限的本機使用者帳戶」[28]
	決定結束遠端 KVMS 階段作業時，是否應鎖定主機作業系統的存取。	韌體版本 3.0.4 和更新版本	■ 「結束 KVMS 階段作業時鎖定主機存取」[29]
	決定是否限制其他 SP 使用者檢視從 SP 啟動的遠端 KVMS 階段作業。	韌體版本 3.2.4 和更新版本	■ 「限制 Remote System Console Plus 的可檢視 KVMS 階段作業 (3.2.4 或更新版本)」[30]
	決定要在使用者登入時或於使用者登入後立即顯示標題訊息。	韌體版本 3.0.8 和更新版本	■ 「使用登入標題保護系統存取 (3.0.8 及更新版本)」[31]
	確定已為所有 Oracle ILOM 使用者介面設定最高安全性特性。	所有韌體版本	■ 「配置 Oracle ILOM 介面以獲得最高安全性」[32]

伺服器建置後的安全檢查清單

為判斷哪些是最適合在您環境中現有伺服器上維護的 Oracle ILOM 安全措施，系統管理員應參考下列表 2,「檢查清單 - 在伺服器建置後維護 Oracle ILOM 安全 」中建議的安全工作清單。

表 2　檢查清單 - 在伺服器建置後維護 Oracle ILOM 安全

✓	安全工作	適用的韌體版本	如需詳細資訊，請參閱：
	維護 Oracle ILOM 的安全管理連線	所有韌體版本	■ 「避免未經認證的主機 KCS 裝置存取」[47] ■ 「偏好的已認證主機連結存取」[48] ■ 「對安全通道使用 IPMI 2.0 加密」[49]
	確定已從 Oracle ILOM 安全地啟動遠端 KVMS 和序列文字式階段作業。	所有韌體版本	■ 「KVMS 遠端通訊與加密」[50] ■ 「保護遠端 KVMS 共用存取」[51] ■ 「保護主機序列主控台共用存取」[51]
	維護和追蹤 Oracle ILOM 的使用者存取。	所有韌體版本	■ 「建置後保護使用者存取的考量」[52]
	為預先配置的 Admin `root` 帳戶重設遺失密碼所需的安全動作。	韌體版本 3.1 和更新版本	■ 「重設 `root` 帳戶預設密碼的實體安全存在性」[53]
	在伺服器建置後，如必須修改 Oracle ILOM 中的 FIPS 140-2 合規模式時，必須執行的安全動作。	韌體版本 3.2.4 和更新版本	■ 「在建置後修改 FIPS 模式」[56] ■ 「FIPS 模式啟用時不支援的功能」[16]
	確認伺服器上的軟體和韌體是最新版本。	所有韌體發行版本	■ 「更新至最新的軟體與韌體」[57]

Oracle ILOM 的建置安全最佳措施

使用下列主題決定建置伺服器時要實行的最佳 Oracle ILOM 安全措施。

- 「保護實體管理連線」[13]
- 「在建置時選擇是否要配置 FIPS 模式」[14]
- 「保護服務與開啟的網路連接埠」[17]
- 「保護 Oracle ILOM 使用者存取」[21]
- 「配置 Oracle ILOM 介面以獲得最高安全性」[32]

相關資訊

- 「Oracle ILOM 安全最佳措施檢查清單」
- 「Oracle ILOM 建置後的安全最佳措施」
- 每一 Oracle ILOM 韌體發行版本的安全功能[9]

保護實體管理連線

Oracle ILOM 是一個頻外 (OOB) 管理工具，使用專用的管理通道來維護及監督 Oracle 伺服器。與具備頻內管理工具的伺服器不同，Oracle 伺服器內建遠端管理能力，可讓系統管理員透過服務處理器上的個別專用網路連線安全地存取 Oracle ILOM。雖然 Oracle ILOM 的管理功能提供系統管理員監督與管理 Oracle 伺服器的特定能力，但 Oracle ILOM 並不是針對作為一般用途的運算引擎，或是從不安全、不信任的網路連線進行存取所設計。

無論您是否透過本機序列埠、專用網路管理連接埠或標準資料網路連接埠建立 Oracle ILOM 實體管理連線，伺服器或機架監督模組 (CMM) 上的這個實體連接埠都必須一律連線至內部信任的網路，或專用的安全管理或專用網路。如需建立 Oracle ILOM 實體管理連線時的進一步準則，請參閱下表。

對 Oracle ILOM 的實體連接埠管理連線	支援的 Oracle 硬體	管理連線安全準則
專用連線	■ 伺服器 (連接埠：NET MGT)	讓服務處理器 (SP) 使用專用的內部網路，與一般資料網路流量分開。 如需建立 Oracle ILOM 專用網路管理連線的進一步詳細資訊，請參閱：

對 Oracle ILOM 的實體連接埠管理連線	支援的 Oracle 硬體	管理連線安全準則
	■ CMM (連接埠：NET MGT)	■ *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* 中的 "Dedicated Network Management Connection"
本機連線	■ 伺服器 (連接埠：SER MGT) ■ CMM (連接埠：SER MGT)	使用本機序列管理連線，從實體伺服器或 CMM 直接存取 Oracle ILOM。 如需建立 Oracle ILOM 本機序列管理連線的進一步詳細資訊，請參閱： ■ *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* 中的 "Local Serial Network Management Connection to Oracle ILOM"
邊頻帶連線	伺服器 (連接埠：NET0, NET1, NET2, NET3)	在必要時使用共用的乙太網路資料網路來存取服務處理器 SP，以簡化纜線管理和網路配置，避免兩個不同網路連線的需求。 如需建立 Oracle ILOM 邊頻帶管理連線的進一步詳細資訊，請參閱： ■ *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* 中的 "Sideband Management Connection" 注意 - 大部分的 Oracle 伺服器都支援邊頻帶管理。

注意 - 為了防範安全攻擊，**絕不應將 Oracle ILOM SP 連線至公用網路**，例如網際網路。您應該將 Oracle ILOM SP 管理流量限制在個別的管理網路上，並只對系統管理員授予存取權。

在建置時選擇是否要配置 FIPS 模式

自 Oracle ILOM 韌體發行版本 3.2.4 起，Oracle ILOM CLI 與 Web 介面提供符合美國聯邦資訊處理標準 (Federal Information Processing Standards, FIPS) 等級 1 規範的可配置模式。啟用此模式時，Oracle 會使用符合 FIPS 140-2 安全標準規範的加密演算法來保護系統機密資料或重要資料。

系統管理員在建置韌體為 3.2.4 或更新版本的伺服器時，應先決定是否要配置 FIPS 模式，然後再配置其他的 Oracle ILOM 特性。依預設，Oracle ILOM 出廠時的 FIPS 合規模式為停用。變更 FIPS 合規模式將使所有配置資料重設為原廠預設值。

如果要在建置時 (在配置 Oracle ILOM 特性之前) 啟用 FIPS 合規模式，請參閱「在建置時啟用 FIPS 模式」[15]。若已在 Oracle ILOM 中設定使用者定義的配置特性，而需要修改 FIPS 特性，請參閱「建置後修改 FIPS 模式的動作」[55]。

▼ 在建置時啟用 FIPS 模式

注意 - Oracle ILOM 中的 FIPS 合規模式以「State (狀況)」和「Status (狀態)」特性表示。「State (狀況)」特性代表 Oracle ILOM 中配置的模式，「Status (狀態)」特性代表 Oracle ILOM 中的作業模式。當 FIPS「State (狀況)」特性變更後，直到下次 Oracle ILOM 重新開機時變更才會影響作業模式 (FIPS「Status (狀態)」特性)。

開始之前

- FIPS「State (狀況)」與「Status (狀態)」特性出廠時預設為停用。
- 啟用 FIPS 時 (已配置且作業中)，將不支援 Oracle ILOM 中的某些功能。如需 FIPS 啟用時不支援的功能清單，請參閱表 3,「啟用 FIPS 模式時 Oracle ILOM 中不支援的功能」。
- 修改 FIPS「State (狀況)」特性需使用 Admin (a) 角色。
- 自韌體 3.2.4 和更新版本起，Oracle LOM 中已提供符合 FIPS 規範的可配置特性。在韌體發行版本 3.2.4 之前，Oracle ILOM 未提供符合 FIPS 規範的可配置特性。
- 修改 Oracle ILOM 中的 FIPS 模式「State (狀況)」與「Status (狀態)」特性後，所有使用者定義的配置設定值會重設為原廠預設值。

1. 在 Oracle ILOM Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「FIPS」。

2. 在「FIPS」頁面中，執行下列動作：

   a. 選取 FIPS「State (狀況)」核取方塊以啟用配置的 FIPS 特性。

   b. 按一下「Save (儲存)」套用變更。

   如需其他配置詳細資訊，請按一下 FIPS 網頁上的「`More details`.... (其他詳細資訊....)」連結。

3. 如果要變更 Oracle ILOM 中的 FIPS 作業模式狀態，請執行下列步驟將 Oracle ILOM 重新開機。

   a. 在 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Maintenance (維護)」→「SP Reset (SP 重設)」。

   b. 在「SP Reset (SP 重設)」頁面中，按一下「SP Reset (SP 重設)」按鈕。

   Oracle ILOM 重新開機後，會發生下列情況：

   - 系統上會套用最後配置的 FIPS「State (狀況)」(已啟用)。
   - 先前在 Oracle ILOM 中配置的所有使用者定義配置設定值，都會重設為原廠預設值。

- 系統會更新 FIPS「Status (狀態)」特性，以反映 Oracle ILOM 中目前啟用的作業狀況。

  如需 FIPS「Status (狀態)」訊息的完整清單與描述，請按一下 FIPS 頁面上的「`More details` (其他詳細資訊)」連結。
- Web 介面的上方區域會顯示一個 FIPS 盾牌圖示。
- 所有不支援的 FIPS 功能都會停用或自 CLI 與 Web 介面移除。

  如需不支援的 FIPS 功能完整清單與描述，請按一下 FIPS 頁面上的「`More details` (其他詳細資訊)」連結。

相關資訊

- 「FIPS 模式啟用時不支援的功能」[16]
- 「建置後修改 FIPS 模式的動作」[55]
- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* 中的 "Configure FIPS Mode Properties"。

FIPS 模式啟用時不支援的功能

在 Oracle ILOM 中啟用 FIPS 規範後，將不支援下列 Oracle ILOM 中不符合 FIPS 140-2 規範的功能。

表 3　啟用 FIPS 模式時 Oracle ILOM 中不支援的功能

不支援的 FIPS 模式功能	描述
IPMI 1.5	當 FIPS 模式在系統上啟用並執行時，會從 Oracle ILOM CLI 與 Web 介面移除 IPMI 1.5 配置特性。Oracle ILOM 中會自動啟用 IPMI 2.0 服務。IPMI 2.0 同時支援 FIPS 相容與不相容模式。
Oracle ILOM System Remote Console 的韌體相容性	Oracle ILOM 中的 FIPS 模式使舊的 Oracle ILOM System Remote Console 韌體版本無法相容於新的 Oracle ILOM System Remote Console 韌體版本。 例如，Oracle ILOM System Remote Console 用戶端韌體版本 3.2.4 可向下相容 Oracle ILOM System Remote Console 韌體版本 3.2.3 和更舊版本。不過，Oracle ILOM System Remote Console 用戶端韌體版本 3.2.2 和更舊版本無法向前相容 Oracle ILOM System Remote Console 韌體版本 3.2.4 及更新版本。 注意 - 此韌體相容性限制不適用於 Oracle ILOM Remote System Console Plus。Oracle ILOM Remote System Console Plus 是在較新的服務處理器系統 (例如 SPARC T5 及更新的系統和 (或) Oracle Server x4-4、x4-8 及更新的系統) 上提供。Oracle ILOM Remote System Console 則是在較舊的服務處理器系統 (例如 SPARC T3、T4 和 Sun Server x4-2/2L/2B 及較舊的系統) 上提供。
輕量型目錄存取協定 (LDAP)	當 FIPS 模式在系統上啟用並執行時，會自動從 Oracle ILOM CLI 與 Web 介面移除 Oracle ILOM 中的 LDAP 配置特性。 注意 - FIPS 相容模式及不相容模式均支援下列遠端認證服務：Active Directory 與 LDAP/SSL。
遠端認證撥入使用者服務 (Remote	當 FIPS 模式在系統上啟用並執行時，會自動從 Oracle ILOM CLI 與 Web 介面移除 Oracle ILOM 中的 RADIUS 配置特性。

不支援的 FIPS 模式功能	描述
Authentication Dial-In User Service, RADIUS)	注意 - FIPS 相容模式及不相容模式均支援下列遠端認證服務：Active Directory 與 LDAP/SSL。
簡單網路管理協定 (SNMP) DES 與 MD5	當 FIPS 模式在系統上啟用並執行時，Oracle ILOM CLI 或 Web 介面將不支援 DES 私密協定與 MD5 認證協定的 SNMP 配置特性。

保護服務與開啟的網路連接埠

為確保在 Oracle ILOM 中正確配置服務及其個別的網路連接埠，請參閱下列主題：

- 「預先配置的服務與網路連接埠」[17]
- 「管理不想要的服務與開啟的連接埠」[18]
- 「配置服務與網路連接埠」[19]

預先配置的服務與網路連接埠

Oracle ILOM 已預先配置大部分會預設啟用的服務。這樣可簡單且直接地建置 Oracle ILOM。不過，伺服器上每個開啟的服務網路連接埠都代表惡意使用者的潛在連接點。因此，一定要瞭解初始 Oracle ILOM 設定和其目的，選擇已建置系統實際需要的服務。為求最佳安全，請僅啟用必要的 Oracle ILOM 服務。

下表列出 Oracle ILOM 預設啟用的服務。

表 4　　預設啟用的服務與連接埠

服務	連接埠
HTTP 重導至 HTTPS	80
HTTPS	443
IPMI	623
Oracle ILOM Remote Console 的遠端 KVMS	5120、5121、5122、5123、5555、5556、7578、7579
Oracle ILOM Remote Console Plus 的遠端 KVMS	5120、5555
服務標記	6481
SNMP	161
Single Sign-on	11626
SSH	22

下表顯示 Oracle ILOM 預設停用的服務。

表 5 預設停用的服務與連接埠

服務	連接埠
HTTP	80

管理不想要的服務與開啟的連接埠

所有的 Oracle ILOM 服務都可以選擇性地予以停用，以將那些服務個別開啟的網路連接埠關閉。雖然預設會啟用大部分的服務，但是您可以停用一些功能或變更預設設定，讓 Oracle ILOM 環境更為安全。您可以停用任何 Oracle ILOM 服務，但會失去功能。一般是只啟用建置環境中絕對必要的服務。失去功能和啟用較少網路服務的安全優點，這兩者之間必須加以取捨。

下表描述啟用或停用每個服務的影響。

表 6 服務停用時

服務	描述	啟用/停用的結果
HTTP	存取 Oracle ILOM Web 介面的非加密協定	啟用此服務可提供較加密的 HTTP (HTTPS) 更快的效能。不過，使用此協定會使得機密資訊未經加密就透過網際網路傳送。
HTTPS	存取 Oracle ILOM Web 介面的加密協定	啟用此服務時，可提供 Web 瀏覽器與 Oracle ILOM 之間的安全通訊。然而，由於 Oracle ILOM 上需要有開啟的網路連接埠，所以會增加攻擊漏洞 (例如「阻斷服務」)。
Servicetag	用來識別伺服器以及協助進行服務要求的 Oracle 尋找協定	停用此服務時，Oracle Enterprise Manager Ops Center 即無法尋找 Oracle ILOM，也無法與其他 Oracle 自動服務解決方案整合。 必須從 Oracle ILOM CLI 才能配置 Servicetag 狀態。例如，如果要修改 servicetag 狀態特性，請輸入： `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	標準管理協定	停用此服務時，可能會使 Oracle Enterprise Manager Ops Center 及部分協力廠商軟體的 Oracle 管理連接器無法管理系統。
SNMP	可監督 Oracle ILOM 狀況及監督收到之設陷通知的標準管理協定	停用此服務時，可能會使 Oracle Enterprise Manager Ops Center 及部分協力廠商軟體的 Oracle 管理連接器無法管理系統。
KVMS	提供遠端鍵盤、視訊、滑鼠和儲存裝置的一組協定	停用此服務時，會讓主機主控台和遠端儲存裝置功能無法使用，使其無法使用 Oracle ILOM Remote Syetem Console (或 Oracle ILOM Remote System Console Plus) 和 CLI Storage Redirection 應用程式。
SSH	用於存取遠端 Shell 的安全協定	停用此服務時，會禁止透過網路進行命令行存取，並可能使 Oracle Enterprise Manager Ops Center 無法尋找 Oracle ILOM。
SSO	單一登入功能，可減少使用者必須輸入使用者名稱和密碼的次數	停用此服務時，無須重新輸入密碼即可啟動 KVMS，並且允許無須重新輸入密碼即可從機架監督模組 (CMM) 向下展開至 Blade SP。

如需啟用和停用個別網路服務的相關資訊，請參閱下列主題：「配置服務與網路連接埠」[19]。

配置服務與網路連接埠

如需如何在 Oracle ILOM 中配置管理服務及其個別網路連接埠的指示，請參閱下列程序。

您可使用 Oracle ILOM 命令行介面 (CLI) 或 Web 介面來停用或啟用服務及其個別的網路連接埠。本節中的程序提供所有 Oracle ILOM 韌體發行版本的 Web 介面操作指示。如需 CLI 指示或關於配置特性的其他詳細資訊，請參閱每個程序後之「相關資訊」一節中列出的適當文件。

▼ 修改協定管理服務狀態與連接埠

開始之前

- 請根據下列表格，判斷 Oracle ILOM 中的哪些協定服務和網路連接埠預設為啟用或停用。
  - 表 4,「預設啟用的服務與連接埠」 預設啟用的服務與連接埠
  - 表 5,「預設停用的服務與連接埠」 預設停用的服務與連接埠
- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改協定服務的「狀況 (State)」特性。

請依照下列步驟修改網路服務的「State (狀況)」特性。

1. 在 Oracle ILOM Web 介面中，瀏覽至「Management Access (管理存取)」服務。例如，在：

   - 3.0.x Web 介面中，按一下「Configuration (配置)」→「System Management Access (系統管理存取)」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」。

2. 按一下下表中適當的「Management Access (管理存取)」→ 服務頁籤。

Management Access (管理存取) →	描述
Web Server (Web 伺服器)	使用「Web Server (Web 伺服器)」頁面可管理 HTTP 與 HTTPS 協定管理存取的服務狀況和連接埠指派。
IPMI	使用「IPMI」頁面可管理 IPMI 協定管理存取的服務狀況和連接埠特性。
SNMP	使用「SNMP」頁面可管理 SNMP 管理存取的服務狀況和連接埠特性。
SSH	使用「SSH」頁面可管理安全 Shell 管理存取的服務狀況特性。

3. 在「Management Access (管理存取)」→ 服務頁面上修改「State (狀況)」特性，然後按一下「Save (儲存)」套用變更。
請注意，停用協定服務的「State (狀況)」特性會使個別的協定服務網路連接埠被關閉，導致協定服務無法和 Oracle ILOM 搭配使用。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Management Services and Network Default Properties"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Management Services and Network Default Properties"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Configuring Network Settings"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Configuring Network Settings"

▼ 修改 KVMS 服務狀況與連接埠

開始之前
- Oracle ILOM 中的 KVMS 服務「State (狀況)」特性預設為啟用。如需與 KVMS 服務相關聯之開啟的網路連接埠清單，請參閱表 4,「預設啟用的服務與連接埠」。
- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改 KVMS「State (狀況)」特性。

1. 瀏覽至 Oracle ILOM Web 介面中的「KVMS」頁籤。
例如，在：

   - 3.0.x Web 介面中，按一下「Remote Control (遠端控制)」→「KVMS」。
   - 3.1 和更新版本的 Web 介面中，按一下「Remote Control (遠端控制)」→「KVMS」。

2. 在「KVMS」頁籤中修改 KVMS「State (狀況)」特性，然後按一下「Save (儲存)」套用變更。
請注意，停用「State (狀況)」特性會使個別之開啟的 KVMS 服務網路連接埠被關閉，而導致下列項目無法使用：a) 遠端主機主控台、b) Oracle ILOM Remote Console 與 Oracle ILOM Remote Storage CLI；或 Oracle ILOM Remote Console Plus。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Configure Local Client KVMS Settings"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Configure Local Client KVMS Settings"
- *Oracle ILOM 3.0 Remote Redirection Console - Web and CLI Guide* 中的 "Initial Setup Tasks"

▼ 修改 Single Sign-On 服務狀況與連接埠

開始之前
- Single Sign-On (SSO) 服務「State (狀況)」特性和個別的網路連接埠 (1126) 在 Oracle ILOM 中預設為啟用。
- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改 SSO 服務「State (狀況)」特性。

1. 在 Oracle ILOM Web 介面中，瀏覽至「User Account (使用者帳戶)」頁籤。
   例如，在：
   - 3.0.x Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「User Account (使用者帳戶)」。
2. 在「User Account (使用者帳戶)」頁面中修改 SSO「State (狀況)」特性，然後按一下「Save (儲存)」套用變更。
   請注意，在 Oracle ILOM 中停用 SSO「State (狀況)」特性會導致：a) 將開啟的 SSO 網路連接埠關閉；b) 啟動 KVMS 主控台時提示使用者重新輸入密碼；c) 讓 CMM 使用者不需重新輸入密碼即可瀏覽至刀鋒伺服器 SP。

   相關資訊
   - *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Single Sign-On Service"
   - *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Single Sign-On Service"
   - *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Configure Single Sign-On"
   - *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Configure Single Sign-On"

保護 Oracle ILOM 使用者存取

若要保護 Oracle ILOM 中的使用者存取，請參閱下列主題：

- 「避免建立共用的使用者帳戶」[22]
- 「以角色為基礎的權限指派」[22]
- 「管理使用者帳戶與密碼的安全準則」[23]
- 「遠端認證服務與安全性設定檔」[24]

- 「配置使用者存取以獲得最高安全性」[25]

避免建立共用的使用者帳戶

避免建立共用的帳戶以維護安全環境。共用帳戶是共用指定之使用者帳戶密碼的使用者帳戶。處理使用者帳戶最理想的方法是為能夠存取 Oracle ILOM 的每位使用者建立唯一的密碼，而不要建立共用帳戶。確定每個使用者帳戶與密碼組合都只有一位使用者知道。

注意 - Oracle ILOM 最多支援 10 個本機使用者帳戶。如果您需要讓更多使用者存取 Oracle ILOM，可以使用中央資料庫來配置目錄服務 (例如 LDAP 或 Active Directory)，以支援更多的帳戶。如需詳細資訊，請參閱「遠端認證服務與安全性設定檔」[24]。

在建立具有唯一密碼的個別使用者帳戶後，系統管理員應確定已指派唯一密碼給預先配置的管理員 `root` 帳戶。否則，如果沒有唯一密碼，預先配置的管理員 `root` 帳戶就會被視為共用帳戶。為確保未經授權的使用者無法使用預先配置的管理員 `root` 帳戶，您必須修改密碼或從 Oracle ILOM 移除預先配置的 `root` 帳戶。如需預先配置之管理員 `root` 帳戶的進一步詳細資訊，請參閱「第一次登入時修改 `root` 帳戶的預設密碼」[27]。

如需建立具有唯一密碼之安全帳戶的進一步準則，請參閱「管理使用者帳戶與密碼的安全準則」[23]。

如需使用者帳戶配置資訊，請參閱「配置使用者存取以獲得最高安全性」[25]。

以角色為基礎的權限指派

所有 Oracle ILOM 使用者帳戶都會被指派一組以角色為基礎的權限。這些以角色為基礎的權限提供對 Oracle ILOM 內各種功能的存取。您可以配置使用者帳戶，讓使用者可以監督系統，但不能進行任何配置變更。或者，您可以允許使用者修改大部分的配置選項，但不包括建立及修改使用者帳戶。也可以限制誰可以控制伺服器功能，誰可以存取遠端主控台。請務必瞭解權限等級，並將它們適當地指派給組織中的使用者。

下表定義可指派給個別的 Oracle ILOM 使用者帳戶的權限清單。

表 7　使用者帳戶權限描述

角色	描述
`Admin` (a)	讓使用者可以變更所有 Oracle ILOM 配置選項，但不含由其他權限明確授權的配置選項 (例如使用者管理)。
`User Management` (u)	讓使用者可以新增和移除使用者、變更使用者密碼，以及配置認證服務。具備此角色的使用者可以建立第二個具備所有權限的使用者帳戶，因此，此角色具備所有使用者角色最高等級的權限。

角色	描述
Console (c)	讓使用者可以遠端存取主機主控台。此遠端主控台存取可能會允許使用者存取 BIOS 或 OpenBoot PROM (OBP)，讓使用者可以將開機行為變更為存取系統的一種方式。
Reset and Host Control (r)	讓使用者可以控制主機功能，以及重設 Oracle ILOM。
Read-only (o)	讓使用者具備 Oracle ILOM 使用者介面的唯讀存取權。所有使用者都具備此存取權，讓使用者有權讀取日誌和環境資訊，以及檢視配置設定。

如需建立本機使用者帳戶和指派以角色為基礎之權限的詳細資訊，請參閱「建立具有以角色為基礎之權限的本機使用者帳戶」[28]。

管理使用者帳戶與密碼的安全準則

管理 Oracle ILOM 使用者帳戶與密碼時，請考量下列安全準則：

- 「使用者帳戶管理準則」[23]
- 「密碼管理準則」[24]

使用者帳戶管理準則

使用者帳戶管理準則	描述
絕對不要共用使用者帳戶	應一律為每個 Oracle ILOM 使用者建立個別的帳戶。 Oracle ILOM 支援最多 10 個本機使用者帳戶。如果您是管理大型網站並且需要 10 個以上的使用者帳戶，則應考慮使用第三方使用者認證服務，例如 LDAP 或 Active Directory。 如需關於透過外部認證服務在 Oracle ILOM 中實作使用者認證的詳細資訊，請參閱「遠端認證服務與安全性設定檔」[24]。
為本機使用者帳戶選擇符合原則的名稱	為本機 Oracle ILOM 使用者帳戶選擇使用者名稱時，使用者名稱必須： ■ 名稱長度為 4 到 16 個字元 (第一個字元必須是字母)。 ■ 是您整個組織中唯一的名稱 ■ 不包含空格、句號 (.) 或冒號 (:)
為本機使用者帳戶選擇符合原則的密碼	為本機 Oracle ILOM 使用者帳戶選擇密碼時，密碼必須： ■ 一律使用強式密碼，密碼長度最多為 16 個字元 ■ 混合使用小寫與大寫字元及一或兩個特殊字元，以建立更安全的複雜密碼 ■ 不包含空格、句號 (.) 或冒號 (:) ■ 符合公司的密碼管理原則 如需 Oracle ILOM 中之密碼管理的進一步詳細資訊，請參閱「管理使用者帳戶與密碼的安全準則」[23]。
依據工作角色限制使用者帳戶權限 (最低權限原則)	為求良好的安全措施，最低權限狀態原則會將可執行工作所需的最低權限授予使用者。過度授予職責、角色等 (特別是在組織的週期早期階段)，可能會導致系統遭到濫用。請定期複查使用者權限，以決定權限與每個使用者目前工作職責的相關性。

使用者帳戶管理準則	描述
	Oracle ILOM 提供控制每位使用者之使用者權限的能力。因此，請根據工作角色，將適當的使用者角色權限指派給每個使用者帳戶。 如需如何建立具有以角色為基礎之權限的使用者帳戶詳細資訊，請參閱：「建立具有以角色為基礎之權限的本機使用者帳戶」[28]。

密碼管理準則

密碼管理準則	描述
在第一次登入之後立即變更預設 `root` 密碼 (`changeme`)	為了能夠執行第一次登入並存取 Oracle ILOM，系統提供一個本機管理員 `root` 帳戶。為了建立安全環境，您必須在第一次登入 Oracle ILOM 之後變更提供的管理員密碼 (`changeme`)。 取得對管理員 `root` 帳戶的未授權存取，會讓使用者無限制地存取所有 Oracle ILOM 功能。因此，指定安全的密碼非常重要。
定期變更所有 Oracle ILOM 帳戶密碼	為避免惡意活動，並確保密碼仍符合目前的密碼制定原則，您應該定期變更所有 Oracle ILOM 密碼。
強制執行建立更安全之複雜密碼的通用措施	強制執行下列通用措施以建立更安全的複雜密碼： ■ 請勿建立長度短於 16 個字元的密碼。 ■ 請勿建立包含使用者名稱、員工姓名或家族成員姓名的密碼。 ■ 請勿選擇容易猜測的密碼。 ■ 請勿建立包含連續數字字串的密碼，例如 12345。 ■ 請勿建立包含透過簡單的網路搜尋即可找到之文字或字串的密碼。 ■ 請勿允許使用者在多個系統中重複使用相同的密碼。 ■ 請勿允許使用者重複使用舊密碼。 ■ 為了得到最高的安全性，應使用下列語法以隨時遮罩 CLI 中輸入的新密碼： **`set [`***SP*|*CMM*`]/users/root password=`**[*do not type password, press Enter*] - 或- **`set [`***SP*|*CMM*`]/users/newuser password=`**[*do not type password, press Enter*] CLI 將會提示輸入新的密碼值，並遮罩密碼以防檢視。
設定本機使用者的密碼制定原則限制 (3.2.5 版和更新版本的韌體可以使用)	對所有本機使用者帳戶強制實施密碼制定原則。如需詳細資訊，請參閱「設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)」[26]。
洽詢您的 IT 安全人員以瞭解密碼管理原則	請洽詢您的 IT 安全人員以確定符合貴公司的密碼管理要求與原則。

遠端認證服務與安全性設定檔

Oracle ILOM 可以配置成使用外部集中使用者存放區，而不需要在每個 Oracle ILOM 執行處理上配置本機使用者。這可增加便利性，可以集中建立和修改使用者證明資料，並可讓使用者存取多個不同系統。

選擇和配置認證服務之前，請瞭解這些服務的運作方式，以及每個服務的配置方式。除了認證之外，每個支援的服務還可以配置授權規則，以定義如何指派指定之遠端使用者的 Oracle ILOM 使用者權限。確認已指派正確的使用者角色或權限。

下表描述 Oracle ILOM 支援的使用者認證服務。

表 8 遠端認證服務與安全性設定檔

服務名稱	安全性設定檔	資訊
Active Directory	高	■ 此服務預設是安全的。 ■ 使用嚴格憑證模式時，需要有憑證伺服器，但是可增加額外的一層安全。
輕量型目錄存取協定/安全通訊端層 (LDAP/SSL)	高	■ 此服務預設是安全的。 ■ 使用嚴格憑證模式時，需要有憑證伺服器，但是可增加額外的一層安全。
傳統 LDAP	低	■ 在沒有可疑惡意使用者的專用安全網路上，可使用此服務。
遠端認證撥入使用者服務 (RADIUS)	低	■ 在沒有可疑惡意使用者的專用安全網路上，可使用此服務。

具有高安全性設定檔的服務可以用於極為安全的環境，因為它們是透過憑證和其他形式的高度加密來保護通道，以保護其本身的安全。預設會停用具有低安全性設定檔的服務。請只在您瞭解並接受這個低安全性等級的限制時，才啟用這些低安全性設定檔。

如需遠端認證服務配置詳細資訊，請參閱下方適當的 Oracle ILOM 文件：

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Setting Up and Maintaining User Accounts"
- Oracle ILOM 3.1 *Configuration and Maintenance Guide* 中的 "Setting Up and Maintaining User Accounts"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Managing User Accounts"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Managing User Accounts"

配置使用者存取以獲得最高安全性

如需如何有效配置 Oracle ILOM 之使用者存取以獲得最高安全性的相關資訊，請參閱下列主題。

- 「設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)」[26]
- 「第一次登入時修改 root 帳戶的預設密碼」[27]
- 「建立具有以角色為基礎之權限的本機使用者帳戶」[28]
- 「結束 KVMS 階段作業時鎖定主機存取」[29]
- 「限制 Remote System Console Plus 的可檢視 KVMS 階段作業 (3.2.4 或更新版本)」[30]
- 「使用登入標題保護系統存取 (3.0.8 及更新版本)」[31]

您可以使用命令行介面 (CLI) 或 Web 介面來配置 Oracle ILOM 中的使用者存取特性。本節中的程序提供所有 Oracle ILOM 韌體發行版本的 Web 介面操作指示。如需 CLI 指示或關於配置特性的其他詳細資訊，請參閱每個程序後之「相關資訊」一節中列出的適當文件。

▼ 設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)

Oracle ILOM 從韌體發行版本 3.2.5 起，會對所有本機使用者帳戶強制實施密碼制定原則。密碼制定原則內含預設的一組密碼制定原則限制。系統管理員可以選擇使用預設的特性，或是加以修改以符合需要的密碼制定原則。

注意 - 密碼制定原則特性的修改應在建立本機使用者帳戶之前完成。如果在配置本機使用者帳戶之後修改了「密碼制定原則」特性，則 Oracle ILOM 將會自動：1) 移除所有本機使用者帳戶的配置，接著 2) 回復系統初始提供的預設 root 帳戶。

開始之前

- 配置「密碼制定原則」特性需要使用 Admin (a) 角色。
- 「密碼制定原則」只會套用到本機使用者帳戶。對於遠端使用者認證服務帳戶 (例如 LDAP 或 Active Directory) 則無影響。
- 儲存對密碼制定原則特性的變更時，將會發生下面幾件事：
  - 所有本機使用者帳戶配置都將從 Oracle ILOM 刪除。
  - 回復系統出廠時的預設本機使用者帳戶 (root)。
  - 在 root 第一次登入時，系統會提示 root 使用者變更 root 帳戶密碼。

依照 Web 介面操作指示，設定所有本機使用者的「密碼制定原則」：

注意 - 如需「CLI 密碼制定原則」指示，請按一下此程序的「Related Information (相關資訊)」段落中所列的 Oracle ILOM Administration Guide 參考資料。

---

1. 若要在 Oracle ILOM 中檢視目前的「密碼制定原則」限制，請按一下「ILOM Administration (ILOM 管理)」>「User Management (使用者管理)」>「Password Policy (密碼制定原則)」。
2. 若要修改「密碼制定原則」限制，請按一下「Password Policy (密碼制定原則)」頁面上的「More Details... (其他詳細資訊...)」連結，以取得進一步的指示。
3. 若要儲存變更，請按一下「Save (儲存)」。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*中的「Modify Password Policy Restrictions for Local Users」

▼ 第一次登入時修改 root 帳戶的預設密碼

為了能夠執行第一次登入並存取 Oracle ILOM，系統提供了一個預先配置的管理員 root 帳戶及預設密碼 (changme)。為避免 Oracle ILOM 遭受未經授權的存取，第一次登入時必須變更隨預先配置之 root 帳戶提供的預設密碼 (changeme)。否則，預先配置的 root 帳戶與預設密碼 (changeme) 將成為共用帳戶，任何使用者都能獲得管理員存取權。

請使用下列 Web 介面操作指示來修改隨預先配置的管理員 root 帳戶提供的預設密碼 (changeme)。

注意 - 如果您沒有預先配置之 root 帳戶的存取權，但需要存取 Oracle ILOM 管理員功能，請洽詢您的系統管理員以取得具備管理員權限的使用者帳戶。

開始之前

- 再次確認「管理使用者帳戶與密碼的安全準則」[23]。

  注意 - 為 root 帳戶指派一個強式安全密碼十分重要，如此可避免 Oracle ILOM 功能遭受未經授權的存取。強式密碼的組合應包含大小寫字元和至少一個特殊字元 (如 % 或 $)。

- 需具備 User Management (u) 角色才能修改 Oracle ILOM 中的本機使用者帳戶密碼。

1. 瀏覽至 Oracle ILOM Web 介面中的「User Account (使用者帳戶)」頁面。

   例如，在：

   - 3.0.x Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。
   - 3.1 和更新版本的 Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。

2. 在「User Account (使用者帳戶)」頁面中，針對 **root** 帳戶按一下「Edit (編輯)」。

   「Edit: User Root (編輯：使用者 Root)」對話方塊即會出現。

3. 在「Edit: User Root (編輯：使用者 Root)」對話方塊中執行下列動作：

   - 在「New Password (新密碼)」文字方塊中輸入唯一密碼，然後在「Confirm New Password (確認新密碼)」文字方塊中再次輸入相同密碼。
   - 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Configuring a Local User Account"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Configuring a Local User Account"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Modify a User Account"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Modify a User Account"
- 「重設 root 帳戶預設密碼的實體安全存在性」[53]

▼ 建立具有以角色為基礎之權限的本機使用者帳戶

開始之前

Oracle ILOM 支援在單一 SP 或機架監督模組 (CMM) 中建立和儲存最多 10 個本機使用者帳戶。Oracle ILOM 使用者會被指派一組權限，使他們能夠依據其配置之帳戶所具備的權限來使用功能。

注意 - 此外，系統管理員也可將 Oracle ILOM 配置為透過遠端認證服務支援其他使用者帳戶。使用遠端認證服務配置時，登入、密碼和權限是從外部使用者存放區所衍生。如需詳細資訊，請參閱「遠端認證服務與安全性設定檔」[24]。

如需有關配置以角色為基礎之存取權限的本機使用者帳戶 的 Web 介面操作指示，請參閱下列指示。

開始之前

- 再次確認「管理使用者帳戶與密碼的安全準則」[23]。
- 再次確認表 7,「使用者帳戶權限描述」中 Oracle ILOM 支援的 Web 瀏覽器。
- 在 Oracle ILOM 中，需具備 User Management (u) 角色才能建立具有權限的本機使用者帳戶。

1. 瀏覽至 Oracle ILOM Web 介面中的「User Account (使用者帳戶)」頁面。

   例如，在：

   - 3.0.x Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。
   - 3.1 和更新版本的 Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。

2. 在「User Account (使用者帳戶)」頁面中，按一下「Add (新增)」。

   「Add User (新增使用者)」對話方塊即會出現。

3. 在「Add User (新增使用者)」對話方塊中，執行下列動作：

   a. 在「User Name (使用者名稱)」文字方塊中，指定使用者名稱。

   b. 在「Roles (角色)」下拉式清單中，選取適當的使用者角色設定檔 (管理員、操作員或進階)。

   c. 在「New Password (新密碼)」文字方塊中輸入唯一密碼，然後在「Confirm New Password (確認新密碼)」文字方塊中再次輸入相同密碼。

   d. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Create User Account and Assign User Role"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Create User Account and Assign User Role"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Add User Account and Assign Roles"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Add User Account and Assign Roles"

▼ 結束 KVMS 階段作業時鎖定主機存取

因為使用「遠端 KVMS」時，會將主機主控台視為共用的網路資源，所以如果某使用者登入主機作業系統並關閉 Oracle ILOM Remote System Console、Remote System Console Plus 或 CLI Storage Redirection 應用程式，而未登出主機作業系統，則使用「遠端 KVMS」連線至相同主控台的第二位使用者就可以使用先前認證過的作業系統階段作業。因此，Oracle ILOM 提供只要「遠端 KVMS」階段作業中斷連線就會自動鎖定主機作業系統的功能。為求最高安全性，請在 Oracle ILOM 中啟用或配置此功能。

如果要在終止 KVMS 階段作業之後鎖定遠端主機桌面，請參閱下列 Web 介面操作指示。如需如何啟用主機鎖定功能的相關資訊，請參閱 *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*。

開始之前

- 在 Oracle ILOM 中，需具備 Console (c) 角色才能修改主機鎖定模式特性。
- 需有韌體 3.0.4 或更新版本才能在 Oracle ILOM 中使用主機鎖定模式功能。
- 主機鎖定模式功能預設為停用。

1. 在 Oracle ILOM Web 介面中，瀏覽至「KVMS」頁面。
   例如，在：

- 3.0.x Web 介面中，按一下「Remote Console (遠端主控台)」→「KVMS」。
- 3.1 和更新版本的 Web 介面中，按一下「Remote Console (遠端主控台)」→「KVMS」。

2. 在「KVMS」頁面的「Host Lock Settings (主機鎖定設定值)」區段中，執行下列動作：
   - 指定鎖定模式 (「Windows」、「Custom (自訂)」或「Disabled (停用)」)。
   - 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Lock Host Desktop"
- *Oracle ILOM 3.1 Configuration and Maintenance* 中的 "Lock Host Desktop"
- *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide* 中的 "KVMS Lock"

▼ 限制 Remote System Console Plus 的可檢視 KVMS 階段作業 (3.2.4 或更新版本)

自韌體發行版本 3.2.4 起，主要的 Remote System Console Plus 使用者可透過將「Maximum Client Session Count (最大用戶端階段作業數目)」限制為一個階段作業檢視器，以避免 SP 上其他已登入的階段作業使用者檢視視訊重新導向階段作業期間所輸入的機密資料。Oracle ILOM Remote System Console Plus 的「Maximum Client Session Count (最大用戶端階段作業數目)」特性預設為四個階段作業檢視器。

如果要修改 Oracle ILOM Remote System Console Plus 的「Maximum Client Session Count (最大用戶端階段作業數目)」特性，請參閱下列 Web 介面操作指示。

開始之前
- Oracle ILOM Remote System Console Plus 自韌體發行版本 3.2.4 或更新版本起，提供了 KVMS「Maximum Client Session Count (最大用戶端階段作業數目)」特性。

注意 - 在支援 Oracle ILOM Remote Console 的系統上無法配置 KVMS「Maximum Client Session Count (最大用戶端階段作業數目)」特性。

- 只有新發行的 SP 系統 (自韌體發行版本 3.2.1 起) 才提供 Oracle ILOM Remote System Console Plus。
- 在 Oracle ILOM 中，需具備 Console (c) 角色才能修改 KVMS「Maximum Client Session Count (最大用戶端階段作業數目)」特性。

- 在重設 Oracle ILOM 中的「Maximum Client Session Count (最大用戶端階段作業數目)」後，SP 上所有作用中的 Oracle ILOM Remote System Console Plus 視訊階段作業將會終止。
- 在 Oracle ILOM 的「Redirection (重導)」頁面中，預設每個 SP 最多可以啟動四個 Remote System Console Plus 視訊重導階段作業。

1. 在 Oracle ILOM Web 介面中，按一下「Remote Console (遠端主控台)」→「KVMS」以瀏覽至「KVMS」頁面。
2. 在「KVMS」頁面中，修改「Maximum Client Session Count (最大用戶端階段作業數目)」特性 (可接受的值為：*4* (預設值)|*1*|*2*|*3*)。
3. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Remote Device Redirection Properties"

▼ 使用登入標題保護系統存取 (3.0.8 及更新版本)

自韌體發行版本 3.0.8 起，Oracle ILOM 可讓系統管理員在所有使用者登入 Oracle ILOM CLI 與 Web 介面時顯示標題訊息。使用登入標題有助防止遠端裝置未經授權存取系統，並告知經過授權且合法之使用者其合理使用系統的義務。

您實行的標題訊息應遵循資訊安全原則撰寫。如需關於撰寫之訊息的進一步準則，請洽詢您的網站管理員或安全人員。

如果要在登入或後續的登入時向所有使用者顯示標題訊息，請參閱下方的 Web 介面操作指示。

開始之前
- 需具備 Admin (a) 角色才能建立標題訊息。
- 自 Oracle ILOM 韌體發行版本 3.0.8 和更新版本起，已可配置標題訊息。
- 管理員可配置標題訊息，使其顯示在「Login (登入)」頁面，或在使用者登入 Oracle ILOM 之後立即以對話方塊顯示。

1. 在 Oracle ILOM Web 介面中，瀏覽至「Banner Message (標題訊息)」頁面。

   例如，在：

   - 3.0.x Web 介面中，按一下「System Information (系統資訊)」→「Banner Messages (標題訊息)」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「Banner Messages (標題訊息)」。

2. 在「Banner Message (標題訊息)」頁面中，按一下*More Details... (*其他詳細資訊*...)* 連結以判斷如何配置標題訊息。
   如需 CLI 指示，請參閱此程序的「Related Information (相關資訊)」段落中所列適用的 *Oracle ILOM Administration Guide*。

3. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*中的「Management of Banner Messages at Log-In」
- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Management of Banner Messages"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Banner Message Configuration Properties"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Display Banner Message"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Display Banner Message"

配置 Oracle ILOM 介面以獲得最高安全性

如果要配置 Oracle ILOM 介面以獲得最高安全性，請參閱下列主題：

- 「配置 Web 介面以獲得最高安全性」[32]
- 「配置 CLI 以獲得最高安全性」[38]
- 「配置 SNMP 管理存取以獲得最高安全性」[42]
- 「配置 IPMI 管理存取以獲得最高安全性」[43]
- 「配置 WS-Management 存取以獲得最高安全性」[46]

配置 Web 介面以獲得最高安全性

如需如何有效配置 Oracle ILOM Web 介面以獲得最高安全性的關資訊，請參閱下列主題。

注意 - 如果要在 Oracle ILOM 中配置 Web 管理介面特性，可以使用命令行介面 (CLI) 或 Web 介面。本節中的程序提供所有 Oracle ILOM 韌體發行版本的 Web 介面操作指示。如需 CLI 指示或關於配置特性的其他詳細資訊，請參閱每個程序後之「相關資訊」一節中列出的適當文件。

- 「使用信任的 SSL 憑證和私密金鑰提高安全性」[33]

- 「啟用最安全的 SSL 與 TLS 加密特性」[35]
- 「設定非作用中 Web 階段作業的逾時間隔」[37]

使用信任的 SSL 憑證和私密金鑰提高安全性

安全通訊端層 (SSL) 憑證是用來加密透過網路的通訊，確保伺服器或用戶端的真實性。Oracle ILOM 包括自行設計的 SSL 憑證，讓 HTTP over SSL 協定預設可立即使用，無須再上傳憑證。第一次連線至 Oracle ILOM Web 介面時，系統會通知使用者正在使用自行簽署的憑證，並要求使用者接受使用它。使用提供的憑證，完整加密 Web 瀏覽器與 Oracle ILOM 之間的所有通訊。

不過，也可以建立和上傳信任的憑證來提升安全性。信任憑證表示該憑證是由信任的憑證授權機構所授予。使用來自已知憑證授權機構的信任憑證，確保 Oracle ILOM Web 伺服器的真實性。使用不信任的 (自行簽署) 憑證，會有受到攔截式 (MITM) 攻擊的可能性。

如果要取得和上傳暫時的自行簽署憑證或憑證授權機構簽署的憑證，請參閱下列程序。

- 「使用 OpenSSL 取得 SSL 憑證與私密金鑰」[33]
- 「將自訂 SSL 憑證與私密金鑰上傳至 Oracle ILOM」[34]

▼ 使用 OpenSSL 取得 SSL 憑證與私密金鑰

本程序概述如何使用 OpenSSL 工具程式建立 SSL 憑證和私密金鑰。

注意 - Oracle ILOM 不會要求您使用 OpenSSL 產生 SSL 憑證。本程序中使用的 OpenSSL 僅為示範用途。還有其他工具可產生 SSL 憑證。

要使用暫時自行簽署憑證或憑證授權機構簽署的憑證，應由網站管理員或安全人員決定。若您確實需要取得 SSL 憑證 (暫時自行簽署憑證或憑證授權機構簽署的憑證)，您可以依照下列的範例 OpenSSL 命令行指示進行。

注意 - 如需產生 SSL 憑證的進一步 OpenSSL 指示，應參考隨 OpenSSL 工具程式提供的使用者文件。

---

1. 建立網路共用目錄或本機目錄以儲存憑證和私密金鑰。
2. 如果要使用 OpenSSL 工具程式產生新的 RSA 私密金鑰，請輸入：

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   其中，*<foo>* 是私密金鑰的名稱。

注意 - 此私密金鑰是以 PEM 格式儲存的 2048 位元 RSA 金鑰，因此可以 ASCII 文字形式讀取。

---

3. 如果要使用 OpenSSL 工具程式產生憑證簽署要求 (CSR)，請輸入：
   `openssl req -new -key <foo>.key -out <foo>.csr`
   其中，*<foo>* 是憑證簽署要求的名稱。

   注意 - 在 CSR 產生過程中，系統會提示您輸入幾項資訊。

   <foo>`.csr` 檔案現在應該會顯示在您目前的工作目錄中。

4. 如果要產生 SSL 憑證，請執行下列其中一項動作：

   - 產生暫時自我簽署憑證 (有效期限 365 天)。
     自我簽署的 SSL 憑證是從 `server.key` 私密金鑰和 `server.csr` 檔案所產生。
     使用 OpenSSL 工具組時，請輸入：
     `openssl x509 -req -days 365 -in <foo>.csr`
     `-signkey <foo>.key -out <foo>.cert`
     其中，*<foo>* 是指派給私密金鑰 (`.key`) 或憑證 (`.cert`) 的名稱。

     注意 - 此暫時憑證在用戶端瀏覽器中將產生錯誤，主因是簽署憑證機構不明或未受信任。如果無法接受此錯誤，應要求憑證授權機構核發簽署的憑證給您。

   - 從憑證授權機構提供者取得正式簽署的憑證。
     將您的憑證簽署要求 (*<foo>*`.csr`) 提交給 SSL 憑證授權機構提供者。大多數的憑證授權機構提供者會要求您剪下並貼上 Web 應用程式畫面中的 CSR 輸出。通常最多需要 7 個工作天才能收到您的簽署憑證。

5. 將新的 SSL 憑證和私密金鑰上傳至 Oracle ILOM。
   請參閱下列指示：「將自訂 SSL 憑證與私密金鑰上傳至 Oracle ILOM」[34]。

▼ 將自訂 SSL 憑證與私密金鑰上傳至 Oracle ILOM

開始之前

- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改 Web 伺服器特性。
- 取得新的 (暫時自我簽署憑證或憑證授權機構簽署的憑證) HTTPS 憑證和私密金鑰。
  如需使用 OpenSSL 工具程式的指示，請參閱「使用 OpenSSL 取得 SSL 憑證與私密金鑰」[33]。
- 請確定您可以透過網路或本機檔案系統存取新的 HTTPS 憑證和私密金鑰。

1. 在 Oracle ILOM Web 介面中，瀏覽至「SSL Certificate (SSL 憑證)」頁面。
   例如，在：

- 3.0.x Web 介面中，按一下「Configuration (配置)」→「System Management Access (系統管理存取)」→「SSL Certificate (SSL 憑證)」。
- 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「SSL Certificate (SSL 憑證)」。

2. 在 SSL 伺服器頁面中，執行下列動作：

   a. 按一下「Load Certificate (載入憑證)」按鈕以上傳在「File Transfer Method (檔案傳輸方法)」特性中指定的「Custom Certificate (自訂憑證)」檔案。

   b. 按一下「Load Custom Private Key (載入自訂私密金鑰)」按鈕以上傳在「File Transfer Method (檔案傳輸方法)」特性中指定的「Custom Private Key (自訂私密金鑰)」檔案。

   c. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "SSL Certificate and Private Key Configuration Properties"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "SSL Certificate and Private Key Configuration Properties"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Upload SSL Certificate"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Upload SSL Certificate"

▼ 啟用最安全的 SSL 與 TLS 加密特性

Oracle ILOM 支援具有最安全加密的安全通訊端層加密 (SSLv3、TLS v1.0、v1.1及 v1.2)。不過，在某些情況下，您可能需要啟用 SSLv2 或弱加密以支援使用較舊的 Web 瀏覽器。

使用此程序可設定 Oracle ILOM 中的 SSL 和 TLS 特性，以符合您的安全原則需求。

注意 - 自韌體發行版本 3.1.0 起，已支援 SSL 與 TLSv1.0。自韌體發行版本 3.2.4 起，Oracle ILOM 中已支援 TLS v1.1 與 v1.2。

開始之前

- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改 Web 伺服器特性。
- Oracle ILOM 中 TLS 特性的預設設定會根據伺服器上目前安裝的韌體版本而定。

韌體	TLS 預設值
3.1.x、3.2.1.x、3.2.2.x 及 3.2.3.x	啟用 TLS v1.0
3.2.4 和更新版本	啟用 TLS v1.0、v1.1 和 v1.2

- 對於早於 3.2.4 的 Oracle ILOM 韌體版本，預設會啟用 SSLv3 特性。

注意 - 由於 SSLv3 中發現安全漏洞，在提供修正之前，您應停用 SSLv3。如需詳細資訊，請參閱 Oracle：MOS SSLv3 Vulnerability Article。

- 對於 Oracle ILOM 韌體發行版本 3.2.4.x 和更新版本，預設的 SSLv3 設定會根據伺服器型號及安裝的 3.2.4.x 韌體版本而定。

伺服器型號	韌體	SSLv3 預設值
SPARC T3、T4、 T5、M5、M6	3.2.4.1	停用 SSLv 3
X4-2	3.2.4.20 (x4-2)	啟用 SSLv3
X4-2L X4-2B	3.2.4.22 (x4-2L) 3.2.24.24 (X4-2B)	如需進一步的詳細資訊，請參閱 MOS SSLv3 Vulnerability Article。
X4-4 X4-8	3.2.4.18	啟用 SSLv3 如需進一步的詳細資訊，請參閱 MOS SSLv3 Vulnerability Article。
X5-2 X5-2L	3.2.4.10 (x5-2) 3.2.4.12 (x5-2L)	停用 SSLv3

- 預設會停用 Oracle ILOM 中的 SSLv2 和弱加密特性

如果要檢視或修改 Oracle ILOM 中的 SSL 或 TLS Web 伺服器安全特性，請參閱下列 Web 介面操作指示。

1. 在 Oracle ILOM Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「Web Server (Web 伺服器)」。
2. 在「Web Server (Web 伺服器)」頁面中，檢視或修改 SSL、TLS 或弱加密的 Web 安全特性。
3. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Web Server Configuration Properties"

- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Web Server Configuration Properties"

▼ 設定非作用中 Web 階段作業的逾時間隔

Oracle ILOM Web 階段作業逾時間隔可為忘記登出的 Web 存取使用者提供安全性。Web 階段作業逾時間隔可決定自動登出非作用中 HTTP 或 HTTPS Web 階段作業之前的分鐘數。此功能可降低未授權使用者使用已建立的 Oracle ILOM 已認證 Web 階段作業來尋找自動作業電腦的風險。

如果要檢視或修改為 HTTP 與 HTTPS 階段作業設定的 Web 階段作業逾時間隔，請參閱下列 Web 介面操作指示。

開始之前

- 為 HTTP 與 HTTPS 連線設定的預設 Web 階段作業逾時間隔為 15 分鐘。

注意 - 若降低階段作業逾時值，使用者可能需要更頻繁地重新輸入使用者名稱和密碼 (在階段作業到期時)。不過，降低階段作業逾時值可縮短自動作業之已認證 Web 階段作業保持作用中的時間長度。

- 需具備 Admin (a) 角色才能修改 Web 伺服器特性
- 只有在執行韌體發行版本 3.0.4 或更新版本的伺服器 SP 上，才能在 Oracle ILOM 中配置 HTTP 與 HTTPS 階段作業逾時間隔特性。

1. 瀏覽至「Web Server (Web 伺服器)」頁面。

   例如，在：

   - 3.0.x Web 介面中，按一下「Configuration (配置)」→「System Management Access (系統管理存取)」→「Web Server (Web 伺服器)」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「Web Server (Web 伺服器)」。

2. 在「Web Server (Web 伺服器)」頁面中，執行下列動作：

   a. 瀏覽至「HTTP」或「HTTP Session Timeout (HTTP 階段作業逾時)」特性。

   b. 輸入一個介於 1-720 分鐘之間的數字，以指定自動登出非作用中 Web 階段作業之前的分鐘數。

   c. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Web Server Configuration Properties"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Web Server Configuration Properties"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Set Session Time-Out"

配置 CLI 以獲得最高安全性

如需如何有效配置 Oracle ILOM 命令行介面 (CLI) 以獲得最高安全性的資訊，請參考下列主題。

- 「管理 SSH 伺服器狀況和弱加密 (3.2.5 及更新版本) 」[38]
- 「設定非作用中 CLI 階段作業的逾時間隔」[39]
- 「使用伺服器端金鑰加密 SSH 連線」[40]
- 「將 SSH 金鑰附加到使用者帳戶以執行自動化 CLI 認證」[41]

如果要在 Oracle ILOM 中配置 CLI 管理特性，可以使用命令行介面 (CLI) 或 Web 介面。本節中的程序提供所有 Oracle ILOM 韌體發行版本的 Web 介面操作指示。如需 CLI 指示或關於配置特性的其他詳細資訊，請參閱每個程序後之「相關資訊」一節中列出的適當文件。

▼ 管理 SSH 伺服器狀況和弱加密 (3.2.5 及更新版本)

從韌體發行版本 3.2.5 開始，可以在 Oracle ILOM CLI 和 Web 介面中配置「SSH 伺服器狀況」特性和「弱加密」特性。為了得到最高的安全性，會啟用「SSH 伺服器狀況」特性並停用「弱加密」特性。若要修改這些 SSH 管理存取特性，請參閱下列的 Web 介面操作指示。

1. 在 Oracle ILOM Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「SSH Server (SSH 伺服器)」。
2. 在「SSH Server (SSH 伺服器)」頁面中，按一下 *More Details... (*其他詳細資訊*...)* 連結以取得進一步的指示。
3. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Management of SSH Server State and Weak Ciphers"

▼ 設定非作用中 CLI 階段作業的逾時間隔

Oracle ILOM CLI (透過安全 Shell (SSH) 協定連線至 Oracle ILOM 或使用序列連線存取) 支援用於關閉非作用中 CLI 階段作業的可配置階段作業逾時間隔。配置時，此功能可降低未授權使用者使用 Oracle ILOM 的已認證 CLI 階段作業來尋找自動作業電腦的風險。

為達最高安全性，您應在共用主控台上使用 Oracle ILOM CLI 的任何環境中配置 CLI 階段作業逾時間隔。理想狀況下，您應將 CLI 階段作業逾時間隔設為等於或小於 15 分鐘。

如果要檢視或修改為非作用中 Oracle ILOM CLI 階段作業設定的逾時間隔特性，請參閱下列 Web 介面操作指示。

開始之前
- 需具備 Admin (a) 角色才能修改 CLI 特性。
- 為 SSH 連線設定 CLI 階段作業逾時間隔預設為停用，並且設為 0 (零) 分鐘。

注意 - 當 CLI 逾時間隔設為 0 (零) 時，無論階段作業閒置多久，Oracle ILOM 都不會關閉非作用中的 CLI 階段作業。

- 只有在執行韌體發行版本 3.0.4 或更新版本的伺服器 SP 上，才能在 Oracle ILOM 中配置 CLI 階段作業逾時間隔特性。

1. 在 Oracle ILOM Web 介面中，瀏覽至「CLI」頁面。
   例如，在：
   - 3.0.x Web 介面中，按一下「Configuration (配置)」→「System Management Access (系統管理存取)」→「CLI」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「CLI」。
2. 在「CLI」頁面中，執行下列動作以設定 CLI 階段作業逾時間隔。
   a. 選取「Enable (啟用)」核取方塊。
   b. 輸入一個介於 1-1440 分鐘之間的數字，以指定自動登出非作用中命令行階段作業之前的分鐘數。
   c. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "CLI Session Time-Out Configuration Properties"

- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "CLI Session Time-Out Configuration Properties"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Set a CLI Session Time-Out"

▼ 使用伺服器端金鑰加密 SSH 連線

Oracle ILOM 提供安全 Shell (SSH) 伺服器功能，允許遠端用戶端透過命令行介面安全地連線和管理 Oracle ILOM。SSH 協定使用伺服器端金鑰來加密管理通道，以及保護所有通訊的安全。SSH 用戶端也使用這些金鑰來確認 SSH 伺服器的真實性。

Oracle ILOM 會在第一次啟動原廠預設值系統時產生一組唯一的 SSH 金鑰。如果需要新的伺服器端金鑰，Oracle ILOM 支援手動產生額外的 SSH 伺服器端金鑰。

如果要檢視或手動產生 SSH 伺服器端加密金鑰，請參閱下列 Web 介面操作指示。

開始之前

- 需具備 Admin (a) 才能修改 SSH 伺服器特性。

1. 在 Oracle ILOM Web 介面中，瀏覽至「SSH Server (SSH 伺服器)」頁面。
   例如，在：
   - 3.0.x Web 介面中，按一下「System Management (系統管理)」→「SSH Server (SSH 伺服器)」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「SSH Server (SSH 伺服器)」。
2. 在「SSH Server (SSH 伺服器)」頁面中，再次確認產生的「RSA Key (RSA 金鑰)」與「DSA Key (DSA 金鑰)」資訊，或執行下列動作：
   a. 按一下「Generate RSA Key (產生 RSA 金鑰)」以產生新的金鑰。
   b. 按一下「Generate DSA Key (產生 DSA 金鑰)」以產生新的金鑰。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "SSH Server Configuration Properties"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "SSH Server Configuration Properties"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Generate a New SSH Key"

- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Generate a New SSH Key"

▼ 將 SSH 金鑰附加到使用者帳戶以執行自動化 CLI 認證

自訂之產生的 SSH 金鑰組 (DSA 或 RSA) 可用於個別的使用者帳戶，而公用金鑰會上傳至 Oracle ILOM。在使用不需手動介入即可執行，且未包含內嵌純文字密碼的命令檔時，很有幫助。使用者可撰寫會自動或定期透過網路型 SSH 連線從遠端系統執行服務處理器命令的命令檔。

若要上傳產生的公用 SSH 金鑰並將其附加至 Oracle ILOM 帳戶，請參閱下列 Web 介面操作指示。

開始之前

- 使用 SSH 連線工具 (如 ssh-keygen) 產生私密和公用 SSH 金鑰，然後將產生的 SSH 金鑰檔案儲存在遠端 SSH 系統上。
- 需具備 User Management (u) 角色才能將 SSH 公用金鑰附加至其他使用者帳戶。
- 需具備 Read Only (o) 角色才能將 SSH 公用金鑰附加至您自己的使用者帳戶。

1. 瀏覽至 Oracle ILOM Web 介面中的「User Account (使用者帳戶)」頁面。
例如，在：

   - 3.0.x Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。

   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「User Management (使用者管理)」→「User Accounts (使用者帳戶)」。

2. 在「使用者帳戶 (User Account)」頁面中，執行下列動作：

   a. 向下捲動至「SSH Keys (SSH 金鑰)」區段，然後按一下「Add (新增)」。

   b. 從「User (使用者)」清單中選取一個使用者帳戶。

   c. 從清單中選取一個傳輸方法，然後指定上傳公用 SSH 金鑰所需的傳輸方法特性。

3. 按一下「Load (載入)」以上傳公用 SSH 金鑰並附加到選取的使用者帳戶。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "CLI Authentication Using Local SSH Key"
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "CLI Authentication Using Local SSH Key"

- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Managing User Accounts"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Managing User Accounts"

配置 SNMP 管理存取以獲得最高安全性

SNMP 是用來監督或管理系統的標準協定。Oracle ILOM 提供用於監督與管理的 SNMP 解決方案，但是必須先加以配置才能使用。請務必先瞭解各種 SNMP 使用者可配置選項的安全事項，再配置此服務。如需進一步的詳細資訊，請參閱下列資訊：

- 「使用 SNMPv3 加密與使用者認證」[42]
- 「支援可配置物件的 Sun SNMP MIB」[43]

▼ 使用 SNMPv3 加密與使用者認證

SNMPv1 和 SNMPv2c 未提供加密，而且使用認證形式的社群字串。社群字串是透過網路以純文字形式傳送，通常在一群個人之間共用，而非個人使用者專用。相反的，SNMPv3 使用加密來提供安全通道，以及個別使用者名稱和密碼。SNMPv3 使用者密碼是本機密碼，因此可以安全地儲存在管理工作站上。

Oracle ILOM 支援 SNMPv1、SNMPv2c 以及 SNMPv3，並且可以個別啟用或停用。此外，還可以啟用或停用 "sets"，提供其他安全層。這個可配置的選項決定 SNMP 服務是否允許設定可配置的 SNMP MIB 特性。停用 sets，可有效率地只將 SNMP 服務用於監視。

預設會停用 SNMPv1 和 SNMPv2c。預設會啟用 SNMPv3，但是需要先建立一或多位 SNMP 使用者，才能使用。沒有預先配置的 SNMPv3 使用者。

如果要在 Oracle ILOM 中配置 SNMP 管理，請參閱下列 Web 介面操作指示。

開始之前

- 為求最高 SNMP 安全性，請只使用 SNMPv1 和 SNMPv2c 進行監督，而且啟用這些較不安全的協定時，請不要啟用 "sets"。
- 只有 SNMPv3 管理應啟用 SNMP sets。「SNMP Set」特性預設為停用。
- SNMPv3 sets 需要配置 SNMPv3 使用者帳戶。不會提供預先配置的 SNMPv3 使用者帳戶。
- SNMP 服務「State (狀況)」特性預設為啟用。
- 需具備 Admin role (a) 權限才能修改 SNMP 特性。
- 需具備 User management (u) 權限才能新增或修改 SNMPv3 使用者帳戶。

1. 在 Oracle ILOM Web 介面中，瀏覽至「SNMP」頁面。

例如：

- 3.0.x Web 介面中，按一下「System Management Access (系統管理存取)」→「SNMP」。
- 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「SNMP」。

2. 在「SNMP」頁面中，檢視或修改 SNMP 特性，然後按一下「Save (儲存)」套用變更。
如需進一步指示，請參閱此程序之「相關資訊」一節中列出的文件。對於執行韌體發行版本 3.2 或更新版本的使用者，按一下「SNMP」頁面中的「`More details` (其他詳細資訊)」連結可取得其他相關資訊。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Configuring SNMP Settings"
- *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)* 中的 "Configuring SNMP Settings"
- *Oracle ILOM 3.1 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference* 中的 "Configuring SNMP Settings"
- *Oracle ILOM 3.0 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference* 中的 "Configuring SNMP Settings"

支援可配置物件的 Sun SNMP MIB

支援可配置的物件且適用 "sets" 的 Oracle Sun MIB 如下：

- `SUN-HW-CTRL-MIB` – 此 MIB 是用來配置硬體原則 (例如電源管理原則)。
- `SUN-ILOM-CONTROL-MIB` – 此 MIB 是用來配置 Oracle ILOM 功能 (例如，建立使用者以及配置服務)。

注意 - 以下為可以設定 MIB 物件的情況：1) MIB 物件支援修改；2) MIB 物件的 `MAX-ACCESS` 元素設為 `read-write`；以及 3) 嘗試執行 set 的使用者有執行作業的授權。

配置 IPMI 管理存取以獲得最高安全性

如需如何有效配置 Oracle ILOM IPMI 管理存取以獲得最高安全性的資訊，請參閱下列主題。

- 「使用 IPMI v2.0 以使用增強的認證和封包加密」[44]

- 「IPMI 安全準則與最佳措施」[45]
- 「IPMI 2.0 認證加密法支援」[45]

▼ 使用 IPMI v2.0 以使用增強的認證和封包加密

雖然 Oracle ILOM 支援 IPMI v1.5 與 v2.0 來進行遠端管理，但是系統管理員應一律使用 IPMI v2.0 -I lanplus 介面以安全地管理 Oracle 伺服器。IPMI 2.0 版的 -I lanplus 介面提供增強的認證與資料整合檢查。

自韌體發行版本 3.2.4 起，Oracle ILOM 提供可配置的特性以啟用或停用 IPMI v1.5 階段作業。為獲得高安全性，IPMI v1.5 特性預設為停用。當 IPMI v1.5 特性停用時，會禁止 (封鎖) Oracle ILOM 的所有 IPMI v1.5 階段作業連線。

請參閱下列程序以檢視或修改 IPMI 特性服務「State (狀況)」，或是自韌體發行版本 3.2.4 起提供的可配置 IPMI v1.5 特性。

開始之前

- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能修改 IPMI 特性。
- IPMI 服務「State (狀況)」特性預設為啟用。使用之前，Oracle ILOM 中的使用者帳戶必須設定適當、以角色為基礎的權限 (管理員、操作員) 才能執行 IPMI 管理功能。
- 對於執行 Oracle ILOM 韌體 3.2.4 或更新版本的 SP，可支援 IPMI v2.0 管理階段作業，但預設不支援 IPMI v1.5 管理階段作業。在 Oracle ILOM 中可配置 IPMI v1.5 特性。

注意 - 當 Oracle ILOM 中停用 IPMI v1.5 階段作業時，IPMItool 的使用者必須使用 IPMI 2.0 -I lanplus 選項。

- 對於執行 Oracle ILOM 韌體發行版本 3.2.3 或更舊版本的 SP，Oracle ILOM 可支援 IPMI v2.0 與 v1.5 管理階段作業。在 Oracle ILOM 中無法配置 IPMI v1.5 特性。

注意 - IPMI v1.5 階段作業不支援增強的認證與封包加密。如需增強的認證與 IPMI 封包加密，您必須使用 IPMI v2.0。

---

1. 在 Oracle ILOM Web 介面中，瀏覽至「IPMI」頁面。

   例如，在：

   - 3.0 Web 介面中，按一下「Configuration (配置)」→「System Management Access (系統管理存取)」→「IPMI」。
   - 3.1 和更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「IPMI」。

2. 在「IPMI」頁面中，檢視或配置適當的 IPMI 特性，然後按一下「Save (儲存)」套用變更。

   如需其他 IPMI 配置指示，請參閱下方的「相關資訊」一節中列出的適當文件。

相關資訊

- *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)* 中的 "Server Management Using IPMI"
- *Oracle ILOM 3.1 SNMP, IPMI, CIM, WS-MAN Protocol Management Reference* 中的 "Server Management Using IPMI"
- *Oracle ILOM 3.0 SNMP, IPMI, CIM, WS-MAN Protocol Management Reference* 中的 "Server Management Using IPMI"
- 「IPMI 安全準則與最佳措施」[45]
- 「IPMI 2.0 認證加密法支援」[45]

IPMI 安全準則與最佳措施

為確保建立的 IPMI 系統管理階段作業安全且不易受到網路攻擊，系統管理員應該：

- 勿使用 IPMI 1.5 版 (`-I lan` IPMItool 介面) 來建立 IPMI 遠端管理階段作業。使用命令行公用程式 (例如 IPMItool (`-I lanplus` IPMItool 介面)) 時，應明確使用 IPMI 2.0 版。
- 定期變更您的 IPMI 密碼。確定 Oracle ILOM 使用者帳戶的生命週期受到適當的管理。

  如需進一步的詳細資訊，請參閱「保護 Oracle ILOM 使用者存取」[21]。
- 限制來自外部的網路存取。使用專用的乙太網路管理通道與 Oracle ILOM 通訊。

  如需進一步的詳細資訊，請參閱「保護實體管理連線」[13]。
- 與您的 IT 安全人員合作，針對伺服器管理與 IPMI 安全建立一組最佳措施與原則。

IPMI 2.0 認證加密法支援

IPMI 2.0 版中的認證、機密及完整性檢查是透過加密方法套件來支援。依據 IPMI 2.0 規格中的描述，這些加密方法套件是使用 RMCP+ 認證金鑰交換協定。

Oracle ILOM 支援下列加密方法套件金鑰演算法，在從屬端與伺服器之間建立安全的 IPMI 2.0 階段作業。

- Cipher Suite 2 – Cipher Suite 2 使用認證與完整性演算法。
- Cipher Suite 3 – Cipher Suite 3 使用認證、機密及完整性三種演算法。

注意 - 為確保所有 IPMI 2.0 流量都會被加密，Oracle ILOM 並未實作對 IPMI 2.0 Cipher Type 0 (未加密作業模式) 的支援。

配置 WS-Management 存取以獲得最高安全性

對於韌體發行版本 3.0.8 到韌體發行版本 3.1.2，Oracle ILOM 提供標準的 Web 服務介面來監督伺服器的狀況，以及使用稱為 Ws-Management (Ws-Man) 的協定提供產品目錄資訊。

Oracle ILOM Ws-Man 介面也允許主機的對等控制，以及自行重設 Oracle ILOM SP。Ws-Man 是一種利用 HTTP(S) 協定的簡單物件存取通訊協定 (SOAP) 型的協定。Oracle ILOM Ws-Man 介面可以搭配 HTTP 或 HTTPS 傳輸使用。如果使用 HTTPS，將會使用 SSL 憑證來加密通道。如需使用 SSL 憑證的安全優點，以及自行簽署與信任的憑證間之差異的詳細資訊，請參閱「使用信任的 SSL 憑證和私密金鑰提高安全性」[33]。

只有在使用 SSL 憑證時，才會使用此 Web 服務介面。為達最高安全性，請使用 HTTPS 作為傳輸機制。如需配置 Web 伺服器特性的詳細資訊，請參閱「配置 Web 介面以獲得最高安全性」[32]。

Oracle ILOM 建置後的安全最佳措施

請使用下列主題決定伺服器建置後應實行的最佳 Oracle ILOM 安全措施。

相關資訊

- 「Oracle ILOM 的建置安全最佳措施 」
- 「Oracle ILOM 安全最佳措施檢查清單」

維護安全管理連線

為維護與 Oracle ILOM 的安全管理連線，請考量下列資訊。

避免未經認證的主機 KCS 裝置存取

Oracle 伺服器支援主機與 Oracle ILOM (稱為 Keyboard Controller Style (KCS) 介面) 之間的標準低速連線。這個支援的 KCS 介面與 Intelligent Platform Management Interface (IPMI) 2.0 版規格完全相容，且同樣地無法停用。

KCS 裝置存取可能是從主機配置 Oracle ILOM 最便利的方式，但這種存取類型也可能產生安全風險，因為任何作業系統使用者都具備對實體 KCS 裝置的核心或驅動程式存取權，則不需要認證就可以修改 Oracle ILOM 設定。一般只有 `root` 或管理員使用者才

能存取 KCS 裝置。不過，可以配置大部分作業系統，以提供對 KCS 裝置的較高存取權。

例如，具有 KCS 存取權的作業系統使用者可以執行下列作業：

- 新增或建立 Oracle ILOM 使用者。
- 變更使用者密碼。
- 以 ILOM 管理員身分存取 Oracle ILOM CLI。
- 存取日誌和硬體資訊。

在 Linux 或 Oracle Solaris 上，此裝置一般稱為 `/dev/kcs0` 或 `/dev/bmc`，而在 Microsoft Windows 上，則稱為 `ipmidrv.sys` 或 `imbdrv.sys`。必須使用屬於主機作業系統的適當存取控制機制謹慎地控制對此裝置 (亦稱為 Baseboard Management Controller (BMC) 驅動程式或 IPMI 驅動程式) 的存取。

您也可以考慮使用 Oracle ILOM 連結介面作為使用主機 IPMI KCS 裝置來配置 Oracle ILOM 設定值的替代方式。如需進一步的詳細資訊，請參閱「偏好的已認證主機連結存取」[48]。

如需如何控制或保護硬體裝置 (如 KCS 裝置) 存取的其他資訊，請參閱隨主機作業系統提供的文件。

偏好的已認證主機連結存取

KCS 介面的較快速替代方式是，主機作業系統上的用戶端可以透過內部高速連結與 Oracle ILOM 進行通訊。連結主要透過內部 Ethernet-over-USB 連線並執行 IP 堆疊予以實作。Oracle ILOM 會有一個內部且無法路由的 IP 位址，供主機上的用戶端用來與 Oracle ILOM 連線。

與 KCS 介面不同 (依賴對硬體裝置的受保護存取權)，所有作業系統使用者預設都可以使用 LAN 連結。因此，透過 LAN 連結連線至 Oracle ILOM 時需要認證，就像連線是透過網路的 Oracle ILOM 管理連接埠一樣。

此外，主機還可以透過 LAN 連結使用管理網路上公開的所有服務或協定。使用主機上的 Web 瀏覽器可以存取 Oracle ILOM Web 介面，或使用安全 Shell 用戶端連線至 Oracle ILOM 命令行介面。無論如何都必須提供有效的使用者名稱和密碼，才能使用 LAN 連結。

預設會停用 LAN 連結。停用時，主機作業系統看不到乙太網路裝置，且通道不存在。Oracle Hardware Management Pack 可協助啟動設定和配置 LAN 連結。

如需透過安全的專用主機連結連線管理 Oracle ILOM 的相關資訊，請參閱下列其中一項資源：

- 對於韌體發行版本 3.2 或更新版本，請參閱 *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2x)* 中的 "Dedicated Interconnect SP Management Connection"

- 對於韌體發行版本 3.1.x，請參閱 *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Dedicated Interconnect SP Management Connection"
- 對於韌體發行版本 3.0.12 到 3.0.16，請參閱 *Oracle ILOM 3.0 Web Procedures Guide* 中的 "Configuring Local Host Interconnect"

對安全通道使用 IPMI 2.0 加密

Intelligent Platform Management Interface (IPMI) 2.0 版支援稱為 Remote Management and Control Protocol+ (RMCP+) 的加密網路協定。此協定使用對稱式金鑰型查問回應機制來加密通道。此機制可確保不會以未加密方式透過網路傳送機密資料，且需要使用者密碼才能加密和解密流量。為確保所有 IPMI 2.0 流量都會被加密，Oracle ILOM 並未實作任何對 IPMI 2.0 密碼類型 0 (未加密) 作業模式的支援。

如果是 IPMItool，請使用 `-I lanplus` 旗標指出必須建立加密的 RMCP+ 階段作業。

如需詳細資訊，請參閱 `ipmitool` 文件。

注意 - 自韌體發行版本 3.2.4起 ，Oracle ILOM 提供 IPMI 1.5 的可配置特性。IPMI 1.5 特性預設為停用。如需詳細資訊，請參閱「使用 IPMI v2.0 以使用增強的認證和封包加密」[44]。

針對遠端管理使用安全協定

Oracle ILOM 支援許多不同的遠端管理協定。在部分情況下，同時支援相同協定的加密和未加密版本。基於安全理由，應一律使用最安全的協定 (可能的話)。如需支援的加密和未加密協定清單，請參閱下表。

表 9　　支援的安全協定

類別	安全/已加密	未加密
Web 瀏覽器存取	HTTPS	HTTP
命令行存取	SSH	不支援
IPMI 存取	IPMI v2.0	IPMI v1.5
協定存取	SNMPv3	SNMPv1/v2c

建立安全的信任網路管理連線

具備 Oracle ILOM 的所有 Oracle 伺服器，都具有用來透過網路連線至 Oracle ILOM 的專用管理連接埠。使用專用管理連接埠，可提供專用且安全的網路以進行管理。部分系統也支援邊頻帶管理，允許在標準伺服器資料連接埠上存取主機和 Oracle ILOM。使用邊頻帶管理，不需要兩個不同的網路連線，因此可簡化纜線管理和網路配置。不過，它

也表示如果專用或邊頻帶管理連接埠不是連線至信任的網路，Oracle ILOM 流量可能會透過不信任的網路進行傳送。

若要維持最可靠和最安全的 Oracle ILOM 環境，一定要將伺服器的專用網路管理連接埠或邊頻帶管理連接埠連線到內部信任的網路或專用的安全管理/專用網路。

建立安全的本機序列管理連線

您可以透過伺服器的實體序列管理連接埠，從本機使用終端機伺服器或簡易型終端機連線至 Oracle ILOM。如果終端機裝置同時連線至內部或專用網路，請避免將該裝置連接至本機序列管理連接埠，以維護 Oracle ILOM 本機管理連線的安全。

安全地使用遠端 KVMS

Oracle ILOM 可以將主機伺服器的鍵盤、視訊和滑鼠遠端重導至遠端用戶端，以及掛載遠端儲存裝置。這些功能統稱為「遠端 KVMS」。「遠端 KVMS」可讓您透過在用戶端機器上執行稱為 Oracle ILOM Remote Console、Remote Console Plus 及 CLI Storage Redirection 的 Java 應用程式，查看伺服器上主機作業系統的圖形主控台。

為確保可以從 Oracle ILOM 安全地啟動遠端 KVMS 和序列文字式階段作業，請考慮下列事項：

- 「KVMS 遠端通訊與加密」[50]
- 「保護遠端 KVMS 共用存取」[51]
- 「保護主機序列主控台共用存取」[51]

KVMS 遠端通訊與加密

Oracle ILOM Remote System Console、Remote System Console Plus 及 CLI Storage Redirection 應用程式使用一系列的網路協定，以遠端方式與 Oracle ILOM 進行通訊。使用這些 Java 應用程式，您可以控制主機鍵盤和滑鼠，以及在遠端伺服器上掛載本機儲存裝置 (例如 CD 或 DVD 光碟機)。

下表詳述透過網路傳輸「遠端 KVMS」資訊的方式。

表 10　KVMS 功能與加密

KVMS 功能	加密或未加密	描述
滑鼠重導	加密	滑鼠座標會透過網路安全地傳送至 Oracle ILOM。
鍵盤重導	加密	您在用戶端機器上鍵入的任何字元，都會使用加密協定傳輸至 Oracle ILOM。

KVMS 功能	加密或未加密	描述
視訊重導	加密	使用加密協定，在 Java 用戶端與 Oracle ILOM 之間傳輸視訊資料。
儲存裝置重導	未加密	讀取和寫入儲存裝置的資料會不經過加密，透過網路傳輸至 Oracle ILOM。

如需遠端 KVMS 啟用的網路連接埠清單，請參閱表 4,「預設啟用的服務與連接埠」。

保護遠端 KVMS 共用存取

「遠端 KVMS」視訊主控台會重導您在查看連線至該伺服器的實體監視器時所看到的畫面。有多個 Oracle ILOM 的 KVMS 階段作業遠端用戶端時，因為單一伺服器一般只有一個視訊輸出，所以每個階段作業都會顯示完全相同的視訊。

同樣地，連接至相同機器的其他 KVMS 使用者也可以看到您在畫面上從「遠端 KVMS」階段作業鍵入的任何項目。最重要的是，如果某使用者在 Oracle ILOM Remote Console、Remote Console Plus 或 CLI Storage Redirection 應用程式中，以授權的使用者身分登入主機作業系統，則所有其他 KVMS 使用者將可以共用這個已認證的階段作業。因此，請務必瞭解共用連線允許的「遠端 KVMS」功能。

為保護終止遠端 KVMS 重導階段作業後閒置的已認證作業系統階段作業，您應該：

- 將 Oracle ILOM 配置為在終止遠端 KVMS 重導階段作業時自動鎖定主機作業系統。
  如需指示，請參閱「結束 KVMS 階段作業時鎖定主機存取」[29]。
- 設定主機作業系統中自動關閉自動作業之已認證使用者階段的逾時間隔。
  如需指示，請參閱主機作業系統的使用者文件。

如果您是 Oracle ILOM Remote System Console Plus 使用者，而且需限制從 Oracle ILOM 啟動的可檢視 KVMS 階段作業數目，請參閱「限制 Remote System Console Plus 的可檢視 KVMS 階段作業 (3.2.4 或更新版本)」[30]。

保護主機序列主控台共用存取

使用文字式序列主控台，也可以使用大部分作業系統的主機主控台。在 Oracle ILOM CLI 的命令行中執行 `start /HOST/console` 命令，即可使用此主控台。與圖形主控台類似，所有 Oracle ILOM 使用者只能使用一個序列主控台。因此，會將它視為共用資源。如果某位使用者從序列主控台登入主機作業系統，然後終止主控台重導，但未登出，則序列主控台的第二位使用者就可以存取先前認證過的作業系統階段作業。

終止主控台重導階段作業時，Oracle ILOM 會將「資料傳送要求 (DTR)」訊號傳送至主機作業系統。收到這個訊號時，許多作業系統會自動登出使用者。不過，並非所有作業系統都支援此功能：

- Oracle Linux 5 預設即支援且啟用 DTR 訊號。
- Oracle Linux 6 支援 DTR，但是必須手動加以啟用。
- Oracle Solaris 不支援 DTR 訊號。若要降低安全風險，使用者可以在主機作業系統中配置階段作業逾時。

如需保護終止主機序列重導階段作業後閒置之已認證作業系統階段作業的準則，請參閱下列資源：

- 判斷主機作業系統是否支援 DTR 訊號功能，如果支援，請確定此功能預設為啟用。

  如需 DTR 訊號的詳細資訊，請參閱主機作業系統的使用者文件。
- 在主機作業系統中配置階段作業逾時間隔。

  如需如何在主機作業系統中設定階段作業逾時間隔的資訊，請參閱您主機作業系統的使用者文件。
- 實行安全原則以確保使用者絕不會讓遠端序列主機主控台自動作業。不使用遠端主機主控台階段作業時，使用者應隨時登出所有階段作業。

建置後保護使用者存取的考量

為確保可維護安全的使用者存取，請考慮下列事項：

- 「強制密碼管理」[52]
- 「重設 root 帳戶預設密碼的實體安全存在性」[53]
- 「監督稽核事件以找出未經授權的存取」[55]

強制密碼管理

定期變更所有 Oracle ILOM 密碼。這可避免惡意活動，並確保密碼仍符合目前的密碼制定原則。

一般而言，使用者可以變更自己的密碼，但具有使用者管理權限的系統管理員可修改和其他使用者帳戶相關聯的密碼。

如果要變更與 Oracle ILOM 使用者帳戶相關聯的密碼，請參閱下列 Web 介面操作指示。

注意 - 如需 CLI 指示或關於使用者管理配置特性的其他詳細資訊，請參閱下列程序中顯示之「相關資訊」一節中列出的文件。

▼ 修改本機使用者帳戶密碼

開始之前

- 再次確認「管理使用者帳戶與密碼的安全準則」[23]。
- 需具備 User Management (u) 角色才能修改與其他使用者帳戶相關聯的密碼或權限。
- Operator (o) 角色可讓使用者修改自己帳戶的密碼。

1. 瀏覽至 Oracle ILOM Web 介面中的「User Account (使用者帳戶)」頁面。

   例如，在：

   - 3.0.x Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。
   - 3.1 和更新版本的 Web 介面中，按一下「User Management (使用者管理)」→「User Account (使用者帳戶)」。

2. 在「User Account (使用者帳戶)」頁面中，針對要修改的帳戶按一下「Edit (編輯)」。

   隨即顯示「Edit: User Name (編輯：使用者名稱)」對話方塊。

3. 在「Edit: User Name (編輯：使用者名稱)」對話方塊中，執行下列動作：

   - 在「New Password (新密碼)」文字方塊中輸入唯一密碼，然後在「Confirm New Password (確認新密碼)」文字方塊中再次輸入相同密碼。
   - 按一下「Save (儲存)」套用變更。

相關資訊

- 「設定所有本機使用者的密碼制定原則限制 (3.2.5 及更新版本)」[26]
- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Configuring a Local User Account"
- Oracle ILOM 3.1 *Configuration and Maintenance Guide* 中的 "Configuring a Local User Account"
- *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide* 中的 "Modify a User Account"
- *Oracle ILOM 3.0 Daily Management - Web Procedures Guide* 中的 "Modify a User Account"

重設 `root` 帳戶預設密碼的實體安全存在性

萬一遺失 Oracle ILOM 的 `root` 使用者密碼，可以加以重設。若要重設 `root` 密碼，請透過序列埠連線至 Oracle ILOM。在大多數情況下，連線至 Oracle ILOM 序列埠時需要對

系統進行實際存取，序列主控台才能連線至終端機伺服器。終端機伺服器會有效率地授予實體序列埠的網路存取權。

為了避免在使用終端機伺服器時透過網路重設 `root` 密碼，會對大部分的伺服器進行實際存在性檢查功能。這需要按伺服器上的按鈕，以提供對伺服器的實際存取。為求最高安全性，請確定只要 Oracle ILOM 序列埠連線至終端機伺服器時，就啟用存在性檢查功能。

如果要檢視或修改實體存在性檢查功能，請參閱下列 Web 介面操作指示。

注意 - 如需 CLI 指示或關於 `root` 帳戶特性的其他詳細資訊，請參閱下列程序中顯示之「相關資訊」一節列出的文件。

▼ 設定實體存在性檢查

開始之前

- Oracle ILOM 中的「Physical Presence Check (實體存在性檢查)」預設為啟用。
- 需要韌體發行版本 3.1 或更新版本，才能在 Oracle ILOM 中使用「Physical Presence Check (實體存在性檢查)」模式。

1. 在 Oracle ILOM Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Identification (識別)」。
2. 在「Identification (識別)」頁面中，瀏覽至「Physical Presence Check (實體存在性檢查)」特性，然後執行下列其中一項動作：

   - 選取「Physical Presence (實體存在性)」核取方塊以啟用。啟用時，必須按下實體系統上的「Locator (定位器)」按鈕，才能還原預設的 Oracle ILOM 密碼。
     或
   - 清除「Physical Presence (實體存在性)」核取方塊以停用。停用時，不需按下實體系統上的「Locator (定位器)」按鈕也可重設預設的 Oracle ILOM 管理員 root 密碼。

3. 按一下「Save (儲存)」套用變更。

相關資訊

- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Device Identification Configuration Properties"。
- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Device Identification Configuration Properties"
- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Password Recovery for `root` Account"。

- *Oracle ILOM 3.1 Configuration and Maintenance Guide* 中的 "Password Recovery for `root` Account"

監督稽核事件以找出未經授權的存取

Oracle ILOM 稽核日誌會記錄所有登入和配置變更。每個稽核日誌項目都會記下與事件相關聯的使用者和時戳。稽核事件是很有用的工具，可用於追蹤變更，以及判斷是否有對 Oracle ILOM 的未獲授權變更和未獲授權存取。

如果要檢視 Oracle ILOM 稽核日誌中的事件，請參閱下列 Web 介面操作指示。

注意 - 如需 CLI 指示或關於稽核日誌的其他詳細資訊，請參閱下列程序之「相關資訊」一節中列出的文件。

▼ 檢視稽核日誌

開始之前

- 自韌體發行版本 3.1 起，Oracle ILOM 提供稽核日誌。在韌體發行版本 3.1 之前，稽核事件是擷取到 Oracle ILOM 事件日誌中。
- 在 Oracle ILOM 中，需具備 Admin (a) 角色權限才能清除稽核日誌中的項目。

1. 在 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Logs (日誌)」→「Audit (稽核)」。
2. 在「Audit log (稽核日誌)」頁面中，使用控制項篩選日誌項目，或清除日誌中的事件。

   對於執行韌體發行版本 3.2. 或更新版本的使用者，按一下「Audit (稽核)」頁面上的「`More details` (其他詳細資訊)」連結可取得額外資訊。

相關資訊

- *Oracle ILOM User's Guide for System Monitoring and Diagnostics (Firmware 3.2.x)* 中的 "Managing Oracle ILOM Log Entries"
- *Oracle ILOM 3.1 User Guide* 中的 "Managing Oracle ILOM Log Entries"

建置後修改 FIPS 模式的動作

自韌體發行版本 3.2.4 起，Oracle ILOM 提供符合 FIPS 等級 1 規範的可配置特性。此特性出廠時預設為停用。修改 Oracle ILOM 中的 FIPS 規範作業狀態後，會將所有使用

者定義的配置特性重設為出廠預設值。為避免遺失 Oracle ILOM 中使用者定義的配置設定值，應先修改 FIPS 規範再配置任何其他的 Oracle ILOM 設定。如果必須在 Oracle ILOM 配置建置後修改 FIPS 規範，請參閱下列指示以避免遺失使用者定義的設定值。

注意 - Oracle 使用符合 FIPS 140-2 安全標準規範的加密演算法來保護系統機密資料或重要資料。

▼ 在建置後修改 FIPS 模式

在 Oracle ILOM 中執行韌體更新或指定使用者定義的配置特性後，如果必須修改 FIPS 模式作業狀況，請使用此程序。

注意 - Oracle ILOM 中的 FIPS 合規模式以「State (狀況)」和「Status (狀態)」特性表示。「State (狀況)」特性代表 Oracle ILOM 中配置的模式，「Status (狀態)」特性代表 Oracle ILOM 中的作業模式。當 FIPS「State (狀況)」特性變更後，直到下次 Oracle ILOM 重新開機時變更才會影響作業模式 (FIPS「Status (狀態)」特性)。

開始之前

- 自韌體 3.2.4 或更新版本起，Oracle ILOM 中已提供符合 FIPS 等級 1 規範的可配置特性。在韌體發行版本 3.2.4 之前，Oracle ILOM 未提供符合 FIPS 等級 1 規範的可配置特性。
- 啟用 FIPS 時 (已配置且作業中)，將不支援 Oracle ILOM 中的某些功能。如需 FIPS 啟用時不支援的功能清單，請參閱「FIPS 模式啟用時不支援的功能」[16]。
- 需具備 Admin (a) 角色才能執行此程序。

1. 在 Oracle ILOM Web 介面中，備份 Oracle ILOM 配置。

   例如：

   a. 按一下「ILOM Administration (ILOM 管理)」→「Configuration Management (配置管理)」→「Backup/Restore (備份/回復)」。

   b. 在「Backup/Restore (備份/回復)」頁面中，按一下「More details... (其他詳細資訊...)」連結以取得進一步指示。

注意 - 為簡化韌體更新後重新連線至 Oracle ILOM 的程序，您應啟用「Preserve the Configuration (保留配置)」的韌體更新選項。

注意 - 如果您在執行步驟 1 之前執行步驟 2，則必須編輯 XML 備份配置檔並移除 FIPS 設定。否則，會導致伺服器上之備份 Oracle ILOM XML 檔案和 FIPS 模式狀況的配置不一致，系統不允許發生這種情況。

---

2. 如果需要更新韌體，請執行下列步驟：

   a. 按一下「ILOM Administration (ILOM 管理)」→「Maintenance (維護)」→「Firmware Update (韌體更新)」。

   b. 在「Firmware Update (韌體更新)」頁面中，按一下「More details... (其他詳細資訊...)」連結以取得進一步的指示。

3. 依下列方式修改 Oracle ILOM 中的 FIPS 合規模式：

   a. 按一下「ILOM Administration (ILOM 管理)」→「Management Access (管理存取)」→「FIPS」。

   b. 在「FIPS」頁面中，按一下「**More details** (其他詳細資訊)」連結以取得如何執行下列作業的指示：

      - 修改 FIPS「State (狀況)」配置。
      - 重設 SP 以更新系統上的 FIPS 作業狀態。

4. 依下列方式回復備份的 Oracle ILOM 配置：

   a. 按一下「ILOM Administration (ILOM 管理)」→「Configuration Management (配置管理)」→「Backup/Restore (備份/回復)」。

   b. 在「Backup/Restore (備份/回復)」頁面中，按一下「**More details** (其他詳細資訊)」連結以取得進一步指示。

相關資訊

- 「在建置時選擇是否要配置 FIPS 模式」[14]
- 「FIPS 模式啟用時不支援的功能」[16]
- *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)* 中的 "Configure FIPS Mode Properties"

更新至最新的軟體與韌體

請讓您伺服器的軟體與韌體版本維持在最新狀態。

- 定期檢查 My Oracle Support 上發佈的更新。
- 一律安裝您伺服器可用的最新版軟體或韌體，以修正錯誤及使用增強功能。
- 針對所有已安裝的軟體，安裝所有必要的安全修補程式。

如果要更新您伺服器上的 Oracle ILOM 韌體，請參閱下列指示。

▼ 更新 Oracle ILOM 韌體

開始之前

- 在 Oracle ILOM 中，需具備 Admin (a) 角色才能更新 Oracle ILOM 韌體。
- 將排定的韌體更新通知所有 Oracle ILOM 使用者，並要求他們關閉所有用戶端階段作業直到完成韌體更新為止。
- 完成韌體更新程序需要幾分鐘的時間，在這段期間內不應執行其他的 Oracle ILOM 工作。

1. 從 My Oracle Support (MOS) 網站下載您伺服器可用的最新軟體更新。

   如有必要，請參閱隨您的伺服器提供的文件，以獲得從 MOS 取得軟體更新的指示。

   注意 - 您的伺服器可用的最新 Oracle ILOM 韌體版本包含在 MOS 上針對您伺服器所發佈的最新軟體修補程式中。

   ---

2. 將韌體影像存放在本機或網路共用磁碟機。

3. 在 Web 介面中，瀏覽至「Firmware Update (韌體更新)」頁面。

   例如：

   - 在 3.0.x Web 介面中，按一下「Maintenance (維護)」→「Firmware (韌體)」。
   - 在 3.1 或更新版本的 Web 介面中，按一下「ILOM Administration (ILOM 管理)」→「Maintenance (維護)」→「Firmware Upgrade (韌體升級)」。

4. 在「Firmware Upgrade (韌體升級)」頁面中，按一下「Firmware Upgrade (韌體升級)」模式，然後依照提示進行。

   對於執行 Oracle ILOM 韌體 3.2 或更新版本的使用者，按一下「Firmware Upgrade (韌體升級)」頁面上的「`More details` (其他詳細資訊)」連結。