Oracle SuperCluster M7 系列安全指南

文件號碼： **E69656-01**
2016 年 2 月

目錄

使用本文件

- **簡介** – 提供規劃、設定以及維護 Oracle SuperCluster M7 系列系統之安全環境的相關資訊。
- **對象** – 技術人員、系統管理員和取得授權的服務提供者
- **必備知識** – 具備 UNIX 與資料庫管理的進階經驗。

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/sc-m7/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。

瞭解安全原則

本指南提供規劃、設定以及維護 Oracle SuperCluster M7 系列系統之安全環境的相關資訊。

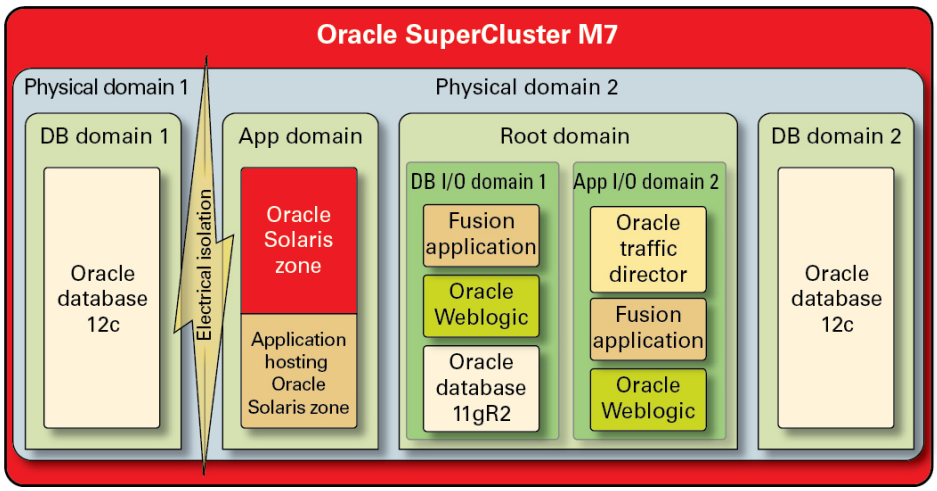
本節涵蓋下列主題：

安全隔離

SuperCluster M7 支援多種隔離策略，雲端提供者可根據其安全及保證需求來選取隔離策略。此彈性可讓雲端提供者針對其業務量身打造客製化、安全的多用戶架構。

SuperCluster M7 支援許多工作負載隔離策略，每種策略都可以設定自己獨有的功能設定。儘管每個實行策略都可以獨立使用，雲端提供者也能夠以混合方式一起使用，讓部署的架構能夠在安全、效能、可用性需求及其他需求之間取得更有效的平衡。

圖 1 使用動態用戶組態進行安全隔離



執行應用程式和資料庫的用戶主機必須與其他工作負載實體隔離的情況下，雲端提供者可以使用實體網域 (亦稱為 PDomain)。由於對組織的重要性、所含之資訊的機密性、規範需求，或甚至只是因為資料庫或應用程式工作負載會完全運用整個實體系統的資源，此部署可能需要專用的實體資源。

對於需要 Hypervisor 調解式隔離的組織，會使用 Oracle VM Server for SPARC 網域 (稱為專用網域) 來建立隔離應用程式和 (或) 資料庫執行處理的虛擬環境。每個專用網域都會建立成為 SuperCluster 安裝的一部分，並且執行自己唯一的 Oracle Solaris 作業系統執行處理。對實體資源的存取會由 SPARC 處理器中內建之硬體輔助的 Hypervisor 來進行調解。

此外，SuperCluster 還可讓您建立利用單一根 I/O 虛擬化 (SR-IOV) 技術的其他網域 (稱為根網域)。根網域擁有一或二個 IB HCA 和 10 GbE NIC。您可以在根網域的頂端，選擇動態建立其他網域 (稱為 I/O 網域)。SuperCluster M7 包含可以用來建立與管理這些網域的瀏覽器工具。

不過，雲端客戶用戶可以利用 Oracle Solaris Zones 技術，在這些網域中建立其他隔離環境。使用區域，便可以將個別應用程式或資料庫執行處理或者是應用程式或資料庫執行處理的群組，部署在一或多個一同在單一作業系統核心頂端執行的虛擬化容器中。此輕量的虛擬化方法是用來在部署的服務周圍建立更安全的邊界。

在 SuperCluster 上架設多個應用程式和資料庫的用戶也可以選擇採用混合式的方法，使用以 Oracle Solaris Zones、I/O 網域及專用網域為基礎的隔離策略組合，建立符合其雲端基礎架構所需之靈活而具有彈性的架構。使用虛擬化選項的主機，SuperCluster 便能

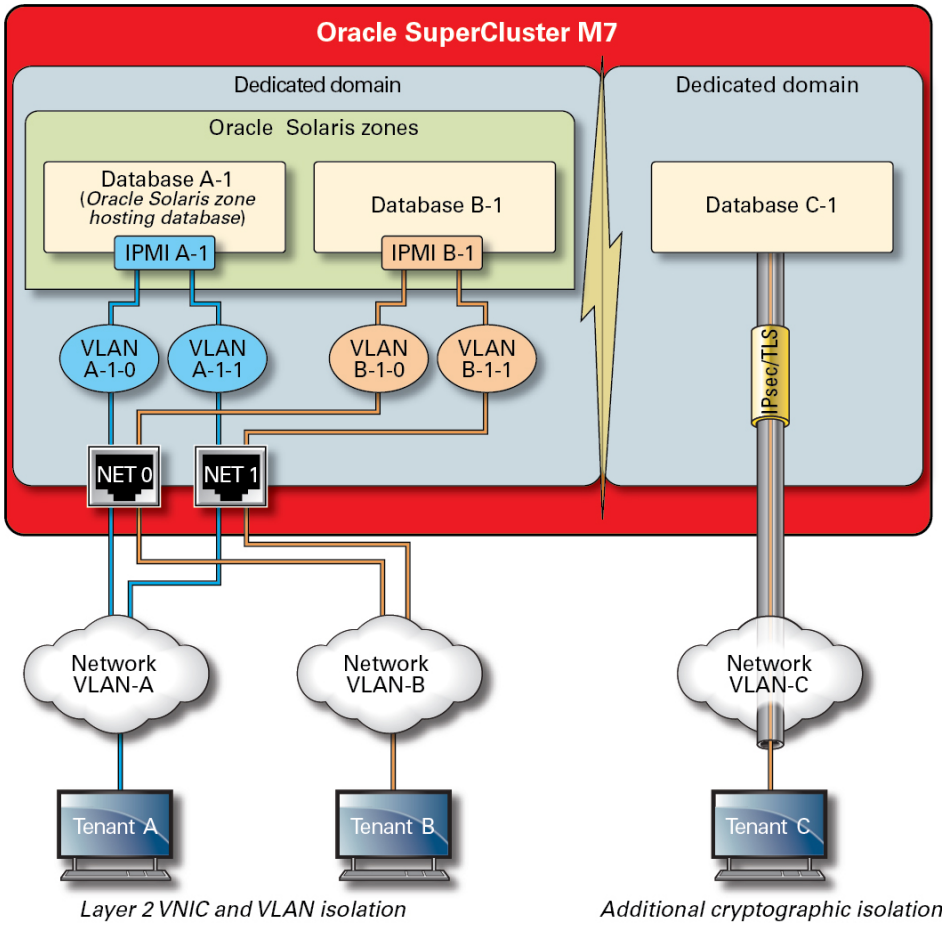
夠在硬體層級安全地隔離雲端代管的用戶，並且提供 Oracle Solaris Zones 以強化安全性，在實際執行環境中實行更進一步地隔離。

確保個別應用程式、資料庫、使用者及處理作業在其主機作業系統上均正確地隔離，是一個好的開始。然而，同等重要的是考量 SuperCluster 中使用的三種主要網路，以及網路隔離功能和保護網路上傳輸之通訊的保護方式：

- 10 GbE 用戶端存取網路
- 專用 IB 服務網路
- 管理網路

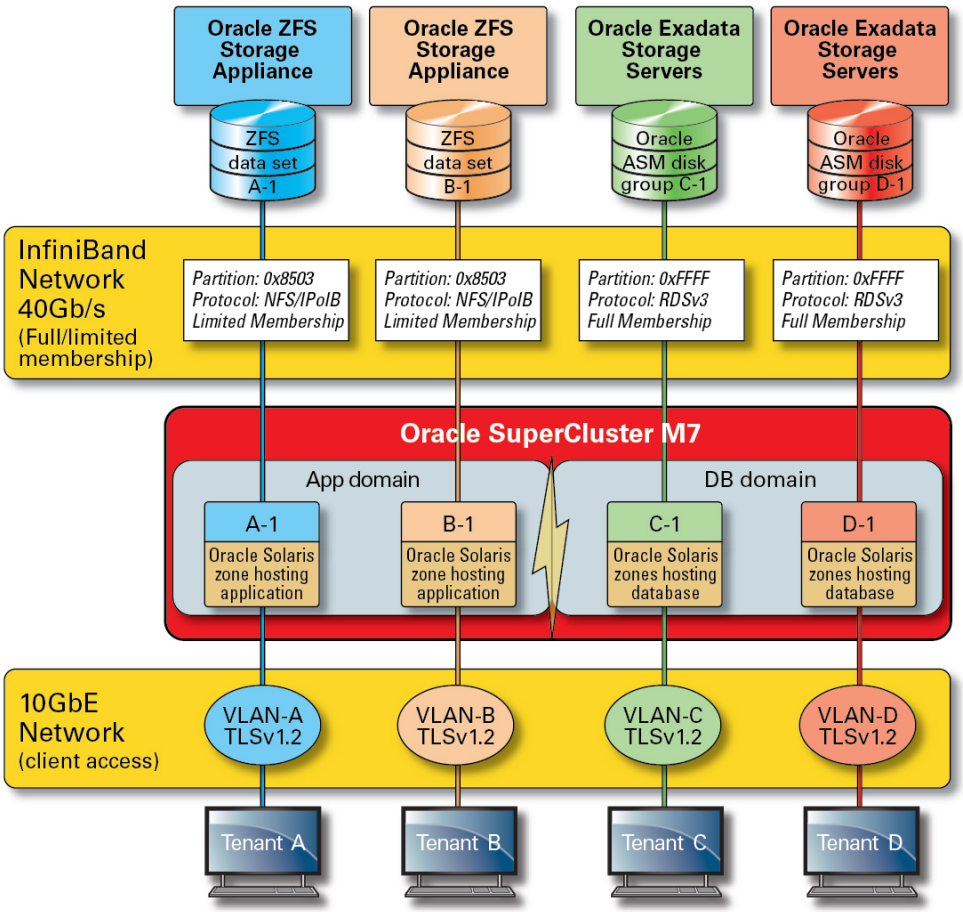
您可以使用多種技術來隔離 SuperCluster 用戶端存取網路上傳輸的網路流量。下圖中顯示將 4 個資料庫執行處理，設定在 3 個不同的虛擬區域網路 (VLAN) 上運作的一種可能組態。藉由將 SuperCluster 的網路介面設定為使用 VLAN，Oracle VM Server for SPARC 專用網域之間以及與 Oracle Solaris Zones 之間的網路流量便可隔離開來。

圖 2 用戶端存取網路上的安全網路隔離



SuperCluster 包含專用的 IB 網路，供資料庫執行處理存取 Exadata 儲存體伺服器和 ZFS 儲存體設備上儲存的資訊，以及執行叢集化和高可用性所需的內部通訊使用。此圖解顯示 SuperCluster M7 上的安全網路隔離。

圖 3 40 Gbs IB 網路上的安全網路隔離



依照預設，SuperCluster IB 網路會在安裝與設定期間分割為 6 個不同的分割區。然而您無法變更預設分割區，在需要將 IB 網路進一步分段的情況時，Oracle 並不支援建立與使用額外的專用分割區。此外，IB 網路支援有限和完整分割區成員身分的概念。有限成員只能與完整成員通訊，而完整成員則可以和分割區上的所有節點通訊。應用程式 I/O 網域和 Oracle Solaris 11 Zones 可以設定為其 IB 分割區上的有限成員，以確保只能與設定為完整成員的 ZFS 儲存體設備通訊，而不會與相同分割區上可能存在的其他有限成員身分節點通訊。

SuperCluster 同時包含專用的管理網路，以便管理與監督其所有核心元件。此策略可將重要的管理和監督功能與用來處理用戶端要求的網路路徑隔離開來。藉由將管理功能隔

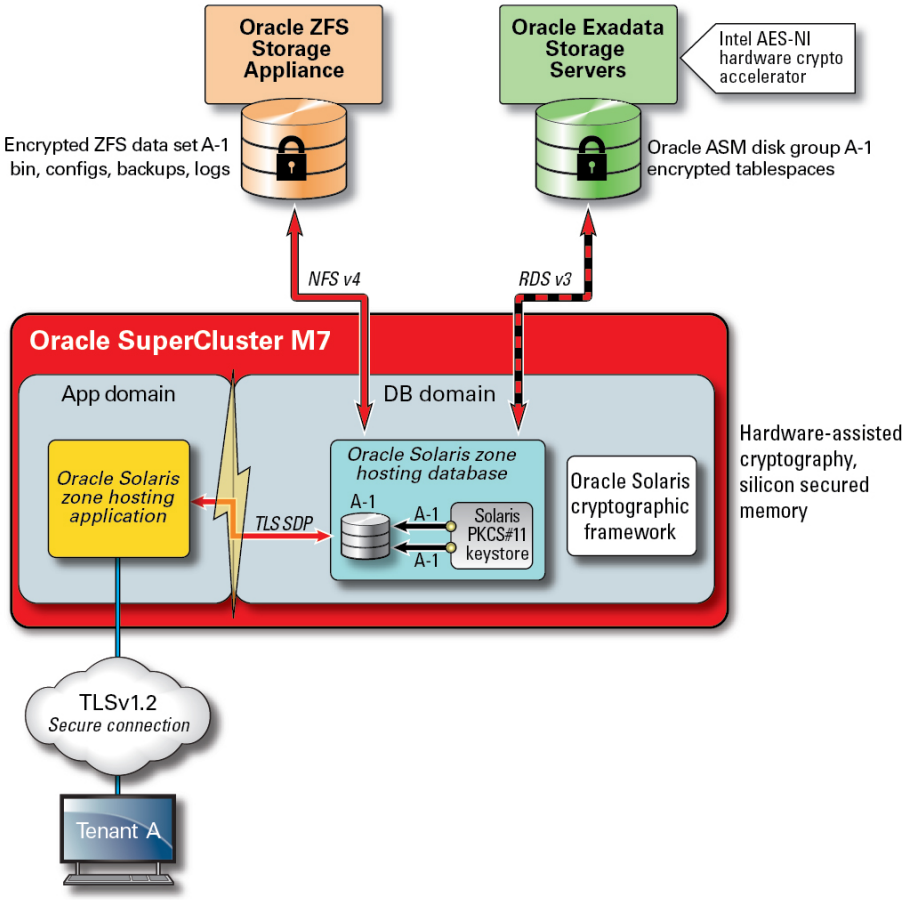
離在此管理網路中，SuperCluster 便可進一步減少暴露在用戶端存取和 IB 網路的網路攻擊面。強烈建議雲端提供者遵循此建議做法，隔離管理、監督以及相關功能，使這些功能只能從管理網路來存取。

資料保護

對於雲端提供者而言，資料保護是其安全策略的核心。為了重視隱私權的重要性和規範需求，考慮採用多用戶架構的組織應認真考慮使用加密來保護進出資料庫的資訊流。全面性地針對資料保護使用加密服務，確保資訊在網路間傳輸以及儲存在磁碟上時的機密性和完整性。

SuperCluster 中的 SPARC M7 處理器有助於安全敏感 IT 環境之資料保護所需的硬體輔助、高效能加密。SPARC M7 處理器同時採用了 Silicon Secured Memory 技術，可確保避免惡意應用程式層次的攻擊，例如記憶體擷取、靜默記憶體損毀、緩衝區溢位以及相關攻擊。

圖 4　藉由硬體輔助加密加速及記憶體入侵保護提供資料保護功能



對於保護多用戶架構而言，資料保護幾乎涵蓋了架構中的每個層面，SuperCluster 及其支援軟體可讓組織符合其安全與合規目標，而不用犧牲效能。SuperCluster 利用設計在其 SPARC M7 處理器中核心內建的加密指令以及 Silicon Secured Memory 功能，提供加速加密作業並確保記憶體入侵保護，而不會影響效能。這些功能可改善加密效能並提供記憶體入侵檢查，還能夠提升整體效能，因為有更多的運算資源能夠專門用來服務用戶工作負載。

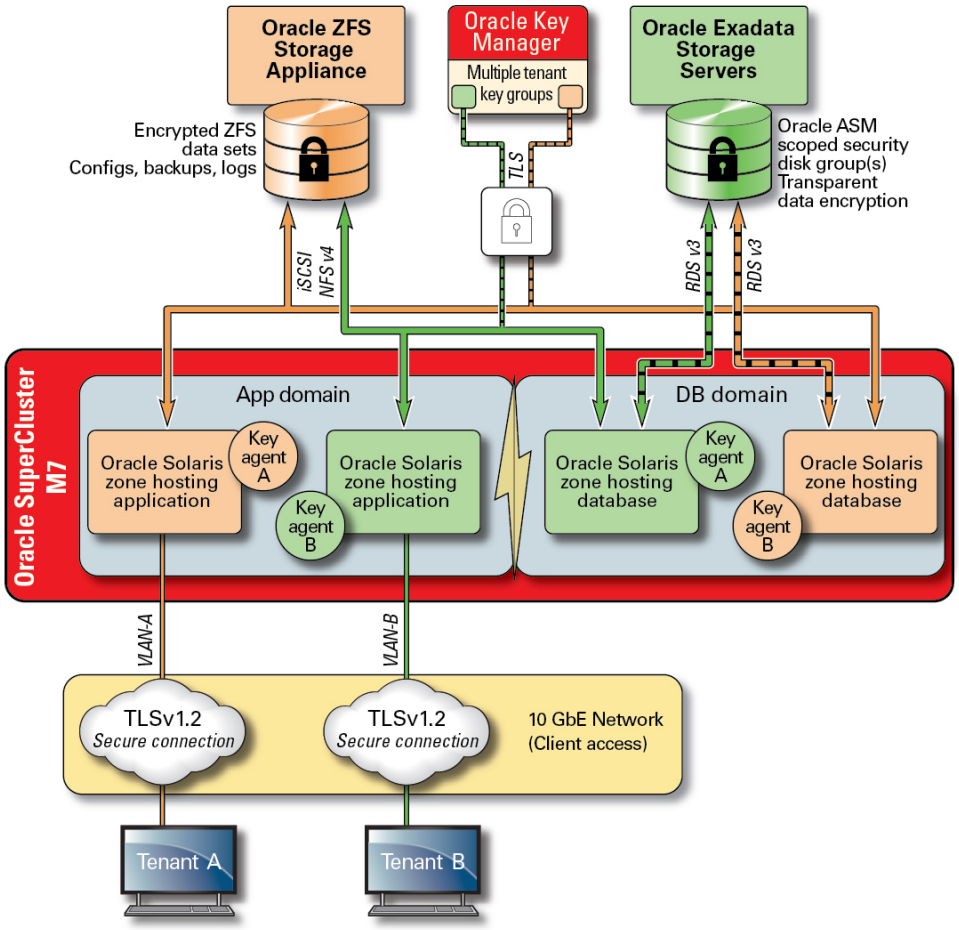
SPARC 處理器提供的硬體輔助加密加速，支援 16 種業界標準的加密演算法。同時，這些演算法支援大多數現代加密需求，包括公用金鑰加密、對稱金鑰加密、亂數產生以及數位簽章和訊息摘要的計算和驗證。此外，在作業系統層次，大多數核心服務均預設啟用加密硬體加速，包括安全 Shell、IPSec/IKE 以及加密 ZFS 資料集。

Oracle 資料庫和 Oracle Fusion Middleware 會自動識別 SuperCluster 所使用的 Oracle Solaris 作業系統和 SPARC 處理器。這可讓資料庫和中介軟體在 TLS、WS-Security、表格空間加密作業等自動使用平台的硬體加密加速功能。同時可讓它們使用 Silicon Secured Memory 功能來確保記憶體保護，並確保應用程式資料的完整性，而無須由一般使用者加以設定。為了保護 IB 網路上用戶特定、區域之間、以 IP 為基礎的通訊流的機密性和完整性，會使用 IPSec (IP 安全) 和 IKE (網際網路金鑰交換)。

加密的任何討論都必須討論加密金鑰的管理方式才會完整。對於組織而言，產生與管理加密金鑰 (特別是大型服務集合) 一向都是大挑戰，在雲端的多用戶環境中，這樣的挑戰更是顯著。在 SuperCluster 上，ZFS 資料集加密和 Oracle 資料庫通透資料加密都可利用 Oracle Solaris PKCS#11 金鑰存放區，安全地保護主要金鑰。若使用 Oracle Solaris PKCS#11 金鑰存放區，則會為任何主要金鑰作業自動使用 SPARC 硬體輔助加密加速功能。這可讓 SuperCluster 顯著提升 ZFS 資料集加密、Oracle 資料庫表格加密、加密資料庫備份 (使用 Oracle Recovery Manager [Oracle RMAN])、加密資料庫匯出 (使用 Oracle 資料庫的資料傾印功能) 以及重做日誌 (使用 Oracle Active Data Guard) 等相關加密與解密作業的效能。

使用共用公事包方法的用戶可以利用 ZFS 儲存體設備，以建立能夠在叢集中所有節點間共用的目錄。使用共用的集中式金鑰存放區可協助用戶更妥善地管理、維護以及輪替叢集化資料庫架構 (例如 Oracle Real Application Clusters (Oracle RAC)) 中的金鑰，因為金鑰將會在叢集中的每個節點上同步化。

圖 5　使用 Oracle Key Manager 透過多用戶金鑰管理的資料保護案例



為瞭解決雲端多用戶環境中多個主機和應用程式之相關金鑰管理的複雜性和問題，可以選擇使用 Oracle Key Manager 作為管理網路中的整合設備。Oracle Key Manager 會集中授權、保護以及管理對 Oracle 資料庫、Oracle Fusion 應用程式、Oracle Solaris 以及 ZFS 儲存體設備所使用之加密金鑰的存取。Oracle Key Manager 同時支援 Oracle 的 StorageTek 加密磁帶機。在 ZFS 資料集 (檔案系統) 層次實行加密原則和金鑰管理，會保證用戶檔案系統可透過毀損金鑰而進行刪除。

Oracle Key Manager 是完整的金鑰管理設備，支援週期金鑰管理作業以及信任金鑰儲存體。設定 Oralce 的額外 Sun Crypto Accelerator 6000 PCIe Card 時，Oracle Key

Manager 提供 FIPS 140-2 等級 3 認證之 AES 256 位元加密金鑰的金鑰儲存體，以及相容 FIPS 186-2 的亂數產生功能。在 SuperCluster 中，所有資料庫和應用程式網域 (包括其全域區域和非全域區域)，都能夠設定為使用 Oracle Key Manager 來管理應用程式、資料庫及加密 ZFS 資料集的相關金鑰。事實上，Oracle Key Manager 能夠支援與個別或多個資料庫執行處理、Oracle RAC、Oracle Active Data Guard、Oracle RMAN 及 Oracle 資料庫的資料傾印功能相關的金鑰管理作業。

最後，由 Oracle Key Manager 強制實施的工作區隔，可讓每位用戶對任何金鑰管理作業都擁有一致的可見性，對其加密金鑰保有完整的控制。有鑑於金鑰對於資訊保護的重要性，用戶實行以角色為基礎的必要層次存取控制與稽核至為重要，可確保金鑰在其有效期間內得到正確的安全保護。

相關資訊

- 「Oracle Key Manager」[112]

存取控制

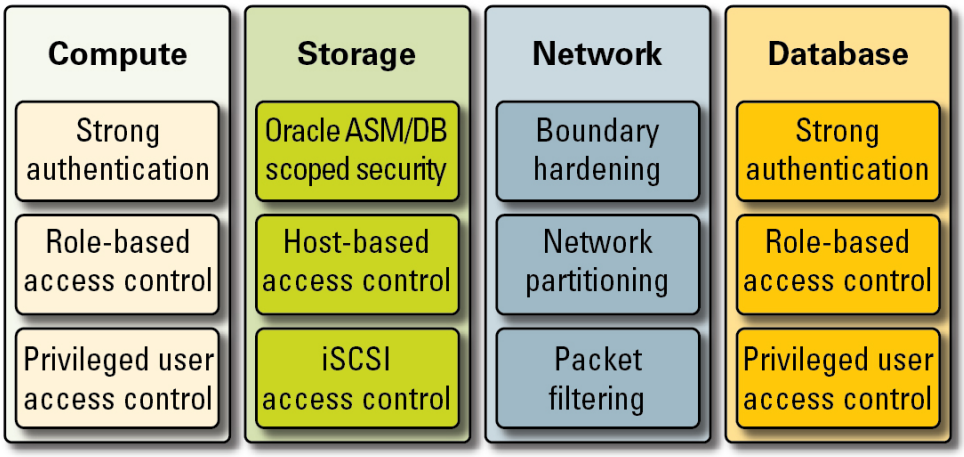
對於採用雲端代管環境策略的組織而言，存取控制是必須解決的最重要挑戰之一。用戶必須對於將資訊儲存在共用基礎架構上具有信心，此共用基礎架構受到保護，且只有授權的主機、服務、個人、群組及角色可以使用。授權的主機、個人和服務必須進一步加以約束，根據最低權限原則，使他們僅具備特定作業所需的權利與權限。

SuperCluster 使用涵蓋堆疊中每一層級的彈性、層層分級的存取控制架構，支援多種角色，包括一般使用者、資料庫管理員及系統管理員。組織可以定義保護各個主機、應用程式及資料庫的原則，保護相關運算、儲存體以及執行這些服務的網路基礎架構。

在虛擬化和作業系統層次，存取控制會從減少暴露在網路上的服務數目開始。這有助於控制對 Oracle VM Server for SPARC 主控台、網域及區域的存取。藉由減少可透過系統存取的進入點數目，存取控制原則的數目也會跟著減少，更易於進行系統的維護。

在 Oracle Solaris 作業系統中，存取控制是利用 POSIX 權限及 Oracle Solaris 以角色為基礎的存取控制 (RBAC) 設備來實行。同樣重要的是保護主機、應用程式、資料庫及 SuperCluster 上執行的相關服務免於網路攻擊的能力。為了達此目的，用戶首先應確認只有核准的網路服務能夠執行與監聽內送網路連線。將網路攻擊面降至最低之後，用戶接著要設定其他服務，使它們只能在核准的網路和介面上監聽內送連線。此一簡單作法有助於確保管理通訊協定 (例如安全 Shell) 不會受到管理網路以外的任何位置存取。

圖 6 點對點存取控制摘要



此外，用戶也可以選擇實行以主機為基礎的防火牆，例如 Oracle Solaris 的 IP 篩選服務。以主機為基礎的防火牆非常實用，因為它們可提供主機更為安全的方式來控制對網路服務的存取。例如，IP 篩選支援有狀態的封包篩選功能，可依據 IP 位址、連接埠、通訊協定、網路介面及流量方向來篩選封包。這些功能對於運作許多網路介面及支援多種內送和外送網路通訊的平台 (例如 SuperCluster) 非常重要。

在 SuperCluster 上，IP 篩選可以設定在 Oracle VM Server for SPARC 網域內部，或是從 Oracle Solaris 區域內運行。這樣就可以在提供資料庫服務的相同作業系統容器中，強制施行網路存取控制原則。在多用戶的情況下，外送網路的活動量可能會很小且能夠輕易分類，如此可以建立原則限制對特定網路介面和目的地的通訊。所有其他流量將會被拒絕並記錄成為「預設拒絕」原則的一部分，以封鎖未經授權的通訊 (包括內送和外送通訊)。

Oracle 一般使用者安全允許用戶將其應用程式和資料庫與其現有的識別管理服務整合，以便支援 Single Sign-on (SSO) 並集中使用者和角色管理。具體而言，Oracle 一般使用者安全有助於集中 (1) 資料庫使用者和管理員的啟動設定和取消啟動設定，(2) 密碼管理和自助密碼重設，以及 (3) 使用全域資料庫角色的授權管理。需要多重因素認證方法 (例如 Kerberos 或 PKI) 的組織，可以利用 Oracle Advanced Security。

Oracle Exadata Storage Server 技術支援一組預先定義的使用者帳號，每個帳號都具備不同的權限。執行 Oracle Exadata Storage Server 管理的管理員必須使用這些預先定義的角色之一來存取系統。另一方面，ZFS 儲存體設備支援建立本機和遠端管理帳號，兩者都能夠支援角色和權限的個別指派。

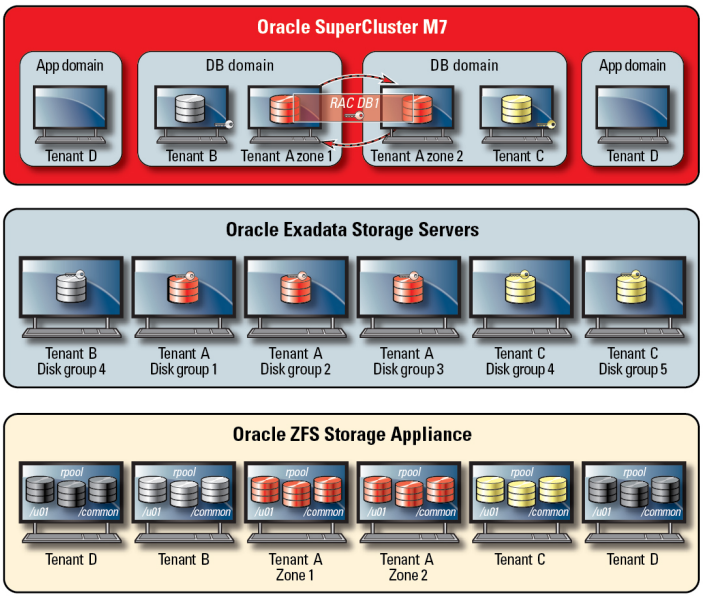
依照預設，資料庫網域可透過 Oracle Automatic Storage Management 設備來存取 SuperCluster 中使用的 Oracle Exadata Storage Server。此設備可讓雲端提供者為

每個用戶建立滿足其容量、效能及可用性需求的不同磁碟群組。在存取控制方面，Oracle Automatic Storage Management 支援三種存取控制模式：開放式安全、Oracle Automatic Storage Management 範圍的安全以及資料庫範圍的安全。

在多用戶情況下，建議使用資料庫範圍的安全，因為它提供最細微層次的存取控制。在此模式中，可以設定只能由單一資料庫存取的磁碟群組。具體而言，這表示資料庫管理員和使用者都被限制為只能存取包含其具有存取權限之資訊的網格磁碟。在資料庫合併的情況下，個別資料庫可能支援不同的組織或用戶，每個用戶都只能夠存取與運用自己的儲存體非常重要。特別是先前所討論到，結合工作負載和資料庫隔離策略的情況下，便能夠有效地區隔用戶對個別資料庫的存取。

資料庫範圍的安全是限制對 Oracle ASM 網格磁碟存取的有效工具。此圖顯示 Oracle ASM 範圍的安全以及 ZFS 安全。在 SuperCluster 平台部署了大量 Oracle 資料庫執行處理的情況下，採用每一用戶的 Oracle ASM 範圍的安全策略會較為合理，因為這樣可以顯著減少必須建立、指派及管理的金鑰數目。此外，因為資料庫範圍的安全需要為每個資料庫建立個別磁碟群組，此方法同時可顯著減少必須在 Exadata Storage Server 上建立個別網格磁碟的數目。

圖 7　每一用戶的 Oracle ASM 範圍的安全



SuperCluster 利用 Oracle Solaris 資料連結保護，可尋找以避免網路上惡意用戶虛擬機器所導致的潛在損害。此整合式 Oracle Solaris 功能提供避免下列基本威脅的保護：IP

和 MAC 位址欺騙以及 L2 框架欺騙 (例如橋接通訊協定資料單元攻擊)。Oracle Solaris 資料連結保護必須個別套用至多用戶環境內的所有 Oracle Solaris 非全域區域。

個別用戶不應該對 Exadata Storage Server 進行管理或主機層次的存取，因此強烈建議限制這類存取。Exadata Storage Server 應設定為防止用戶非全域區域和資料庫 I/O 網路的直接存取，但仍然允許來自 SuperCluster 資料庫網域 (由雲端提供者操作) 的存取。這可確保 Exadata Storage Server 只能從管理網路上的信任位置進行管理。

定義與實行用戶的安全組態之後，服務提供者便可以考慮其他步驟，將用戶特定的全域和非全域區域設定為不可變的唯讀環境。不可變區域會建立一個具有彈性、高完整性的操作環境，用戶可以在其中運行他們自己的服務。不可變區域建立在 Oracle Solaris 固有的安全功能上，可確保在沒有雲端服務提供者介入的情況下，便無法變更部分 (或全部) 作業系統目錄和檔案。強制施行此唯讀態勢有助於防止未經授權的變更，提升為較安全的變更管理程序，以及制止核心和使用者形式的惡意軟體入侵。

監督與合規稽核

在雲端環境中主動進行監督與記錄非常重要，在許多情況下，有助於減輕源自安全漏洞和弱點的攻擊。無論是針對合規報告或未預期事件回應，監督與稽核都是雲端提供者的重要功能，用戶組織必須強制施行良好定義的記錄和稽核原則，以對其代管環境能夠有更深入的瞭解。我們通常會根據受保護環境的風險或重要性，來決定所採用的監督與稽核程度。

SuperCluster 雲端架構使用 Oracle Solaris 稽核子系統來收集、儲存以及處理稽核事件資訊。每個用戶特定的非全域區域都會產生每個 SuperCluster 專用網域 (全域區域) 本機儲存的稽核記錄。此方式可確保個別用戶無法更改其稽核原則、組態或是記錄的資料，因為這是雲端服務提供者負責的事務。Oracle Solaris 稽核功能會監督用戶區域和網域中的所有管理動作、指令呼叫，甚至個別核心層次的系統呼叫。該設備具有高度可設定性，可提供全域、每個區域甚至每個使用者的稽核原則。設定為使用用戶區域時，每個區域的稽核記錄都可以儲存在全域區域中，以保護這些記錄不受到竄改。專用網域和 I/O 網域也會利用原生的 Oracle Solaris 稽核功能，記錄虛擬化事件和網域管理相關的動作和事件。

Exadata Storage Server 和 ZFS 儲存體設備支援登入、硬體以及組態稽核。這可讓組織判斷誰存取了某個裝置及進行了哪些動作。Oracle Solaris 稽核不會直接對一般使用者顯示，而是提供 ZFS 儲存體設備所呈現資訊的相關內容。

同樣地，Exadata Storage Server 稽核是豐富的系統資訊集合，可搭配 Exadata Storage Server 軟體提供的硬體和組態警示資訊一起使用。使用 Oracle Solaris 的 IP 篩選功能，雲端提供者可以選擇性地記錄內送和外送網路通訊，而且此功能也可套用在網域和非全域區域層次。這有助於組織劃分其網路原則以及檢查活動記錄。也可以選擇部署 Oracle Audit Vault and Database Firewall 設備，以便安全地彙總與分析來自各種 Oracle 和非 Oracle 資料庫的稽核資訊，以及來自 Oracle Solaris 的稽核資訊。

透過與 Oracle Enterprise Manager 整合，SuperCluster 能夠支援許多雲端自助服務作業。雲端提供者可以定義資源集區、將集區和配額指派給個別用戶、識別與發佈服務目錄，最終可支援應用程式和資料庫資源的監督與記錄。

相關資訊

- 「合規稽核」[105]
- 「安全監督」[114]

有關 SuperCluster 安全最佳應用的其他資源

如需有關 SuperCluster 安全、架構以及最佳應用的詳細資訊，請參閱下列資源：

- Oracle SuperCluster M7 - Platform Security Principles and Capabilities

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7 - Secure Private Cloud Architecture

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Comprehensive Data Protection on Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Secure Database Consolidation on Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster and PCI Compliance

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - Security Technical Implementation Guide (STIG) Validation and Best Practices

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Developer's Guide to Oracle Solaris 11 Security

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 and PCI Compliance

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 Audit Quick Start

http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html

- Oracle Solaris 11 Security Guidelines

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html

- Oracle Database Security Guide 12c Release 1 (12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

複查預設安全組態

以下主題描述 SuperCluster M7 的預設安全組態。

預設安全設定值

SuperCluster M7 軟體安裝時使用了許多預設的安全設定值。請儘可能使用以下這些預設的安全設定值：

- 密碼原則有基本的密碼複雜度要求。
- 失敗的登入嘗試到達一定次數後，就會導致帳號被鎖定。
- 作業系統中的所有預設系統帳號是鎖定狀態且無法登入。
- 系統設定了使用 `su` 指令的有限能力。
- 停用作業系統核心中非必要的協定和模組。
- 啟動載入器受密碼保護。
- 所有不必要的系統服務均停用，包括 `inetd` (網際網路服務常駐程式)。
- 儲存體單元上設定了軟體防火牆。
- 重要的安全相關組態檔案和可執行檔都設定了有限的檔案權限。
- SSH 監聽連接埠只用於管理網路和專用網路。
- SSH 只能使用 v2 協定。
- 已停用不安全的 SSH 認證機制。
- 已設定特定加密方法。
- 系統中的交換器和網路上的資料流量有所區隔。

預設使用者帳號和密碼

此表格列出 SuperCluster M7 的預設使用者帳號和密碼。如需變更預設密碼的指示，請參閱後續每個元件的章節。

元件	使用者名稱	密碼	使用者帳號和密碼資訊
下列環境中的 Oracle ILOM： ■ SPARC M7 系列伺服器 ■ Exadata Storage Server ■ ZFS Storage Appliance	■ root	welcome1	請參閱 Oracle ILOM 文件集中的「Configuration and Maintenance」，網址為：http://docs.oracle.com/cd/E24707_01/html/E24528
SPARC M7 系列伺服器	■ root ■ oracle ■ grid	welcome1 welcome1 welcome1	請參閱「登入運算伺服器並變更預設密碼」[47]。 另請參閱下列資源： ■ **Oracle Solaris 11** – 請參閱 Oracle Solaris 11 的安全文件，網址為：http://www.oracle.com/goto/Solaris11/docs ■ **Oracle Solaris 10** – 請參閱「*Oracle Solaris Administration: Basic Administration*」，網址為：http://docs.oracle.com/cd/E26505_01
Exadata Storage Server	■ root ■ celladmin ■ cellmonitor	welcome1 welcome welcome	請參閱「變更儲存體伺服器的密碼」[82]。
Oracle ZFS Storage ZS3-ES	■ root	welcome1	請參閱「變更 ZFS 儲存設備 root 密碼」[72]。 另請參閱「*Oracle ZFS Storage Appliance Administration Guide*」中的「Users」小節，網址為：http://www.oracle.com/goto/ZS3-ES/docs
InfiniBand 交換器	■ root ■ nm2user	welcome1 changeme	請參閱「變更 root 和 nm2user 的密碼」[97]。 另請參閱「*Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1*」中的「Controlling the Chassis」，網址為：http://docs.oracle.com/cd/E36265_01
InfiniBand Oracle ILOM	■ ilom-admin ■ ilom-operator	ilom-admin ilom-operator	請參閱「變更 IB 交換器密碼 (Oracle ILOM)」[97]。 另請參閱 InfiniBand 文件，網址為：http://docs.oracle.com/cd/E36265_01
乙太網路管理交換器	■ admin	welcome1	請參閱「變更乙太網路交換器密碼」[103]

元件	使用者名稱	密碼	使用者帳號和密碼資訊
Oracle I/O 網域建立工具	■ admin	welcome1	請參閱「*Oracle I/O Domain Administration Guide*」，網址為：http://www.oracle.com/goto/sc-m7/docs
Oracle Engineered Systems Hardware Manager	■ admin ■ service	welcome1 welcome1	請參閱「*Oracle SuperCluster M7 Series Owner's Guide: Administration*」，網址為：http://www.oracle.com/goto/sc-m7/docs

注意 - 當此元件的 root 或 admin 密碼變更後，也必須在 Oracle Engineered Systems Hardware Manager 中一併加以變更。如需指示，請參閱「*Oracle SuperCluster M7 Series Owner's Guide: Administration*」。另請參閱「Oracle Engineered Systems Hardware Manager 已知的密碼」[29]。

Oracle Engineered Systems Hardware Manager 已知的密碼

Oracle Engineered Systems Hardware Manager 必須使用此表格中的元件帳號和密碼加以設定。

注意 - Oracle Engineered Systems Hardware Manager 不需要知道任一邏輯網域或區域的密碼。

元件	帳號
所有 Oracle ILOM	root
Exadata Storage Server 作業系統	root
ZFS 儲存體控制器作業系統	root
IB 交換器	root
乙太網路管理交換器	admin
PDU	admin

如需 Oracle Engineered Systems Hardware Manager 的詳細資訊，請參閱「Oracle Engineered Systems Hardware Manager」[113] 以及「*Oracle SuperCluster M7 Series Administration Guide*」，網址為：http://www.oracle.com/goto/sc-m7/docs。

保護硬體的安全

以下各節描述保護硬體的安全準則：

使用限制

- 將 Oracle SuperCluster M7 系列系統和相關設備安裝在一個上鎖、限制出入的房間內。
- 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。這麼做可以對可熱插式或可熱抽換裝置、USB 連接埠、網路連接埠和系統主控台限制存取。
- 將備用的現場可更換單元 (FRU) 或客戶可更換單元 (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。
- 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、電源分配器 (PDU) 及網路交換器等裝置都具有 USB 連線。限制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。

序號

- 記錄 SuperCluster M7 系列系統中各元件的序號。
- 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等記錄放在安全的位置。發生系統緊急狀況時，系統管理人員必須能輕易地存取此位置。書面文件可能會是擁有權的唯一證明。
- 安全存放系統隨附的所有資訊文件。

磁碟機

硬碟和固態硬碟經常用來儲存機密資訊。如果要防止此資訊遭到未經授權的存取，磁碟機在重新使用、退役或丟棄之前必須先經過處理。

- 您可以使用磁碟清除工具 (例如 Oracle Solaris `format` (`1M`) 指令) 來徹底清除磁碟機的所有資料。
- 組織應參考其資料保護政策，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。請參閱此文件：`http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

注意 - 磁碟清除軟體可能因新式硬碟管理資料存取的方式而無法刪除其中的某些資料。

OBP

SPARC M7 系列 OBP 預設未使用密碼保護。您可以執行下列動作限制使用 OBP，來加強系統的安全：

- 實作密碼保護。
- 查看失敗的 OBP 登入。
- 提供 OBP 開啟電源系統資訊。

其他硬體資源

「*SPARC M7* 系列伺服器安全指南」中列出的所有安全原則都適用於 SuperCluster 中的 SPARC M7 伺服器。您可在下列網址取得此安全指南：`http://www.oracle.com/goto/M7/docs`

保護 Oracle ILOM 的安全

Oracle ILOM 提供進階的服務處理器硬體和軟體，可用來管理和監督各種 Oracle SuperCluster 元件，包括運算伺服器、儲存體伺服器、ZFS 儲存設備和 IB 交換器。

Oracle ILOM 提供可靠的遠端管理功能，可讓您獨立於作業系統狀態，主動管理和監督底層的伺服器和裝置。

若要在 SuperCluster M7 上完整保護 Oracle ILOM 的安全，您必須將組態設定值分別套用到 Oracle ILOM 所有啟用的元件。下列元件有 Oracle ILOM：

- 運算伺服器
- 儲存體伺服器
- ZFS Storage Appliance
- IB 交換器

執行下列工作保護 Oracle ILOM 的安全：

▼ 登入 Oracle ILOM CLI

1. **在管理網路上，登入 Oracle ILOM。**

   在本範例中，將 *ILOM_SP_ipaddress* 取代為您要存取之元件的 Oracle ILOM IP 位址：

   - 運算伺服器
   - 儲存體伺服器
   - ZFS Storage Appliance

- IB 交換器

組態的 IP 位址會列在由 Oracle 人員提供的「部署摘要」中。

```
% ssh root@ILOM_SP__ipaddress
```

2. **輸入 Oracle ILOM root 密碼。**
   請參閱「預設帳號和密碼 (Oracle ILOM)」[35]。

▼ 判斷 Oracle ILOM 版本

若要運用最新的特色、功能和安全性增強功能，請將 Oracle ILOM 軟體更新為最新支援的版本。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **顯示 Oracle ILOM 版本。**
   在本範例中，Oracle ILOM 軟體版本為 3.2.4.1.b。

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

注意 - 若要在任何 SuperCluster 元件上更新 Oracle ILOM 的版本，請從 My Oracle Support (網址為 https://support.oracle.com) 安裝所提供的最新版 SuperCluster Quarterly Full Stack Download Patch。

注意 - Oracle Engineered Systems (例如 SuperCluster) 能夠使用的 Oracle ILOM 版本和這些版本的更新方式都有所限制。如需進一步的詳細資訊，請聯絡您的 Oracle 服務人員。

▼ (如有需要) 啟用 FIPS-140 相容作業 (Oracle ILOM)

美國聯邦政府的客戶需要使用 FIPS 140 驗證的加密。

Oracle ILOM 預設不會使用 FIPS 140 驗證的加密運作。不過如有需要，可以啟用 FIPS 140 驗證的加密。

若設定 FIPS 140 相容作業，將無法使用某些 Oracle ILOM 特色和功能。這些功能的清單涵蓋在「*Oracle ILOM Security Guide*」中標題為「Unsupported Features When FIPS Mode Is Enabled」的章節中 (請參閱「其他 Oracle ILOM 資源」[46])。

另請參閱「符合 FIPS-140-2 等級 1 規範」[108]。

注意 - 此工作需要您重設 Oracle ILOM。重設會遺失所有使用者設定的設定值。基於這個原因，在對 Oracle ILOM 進行任何其他網站特定的變更之前，您必須先啟用 FIPS 140 相容作業。對於已變更網站特定組態的系統，請備份 Oracle ILOM 組態，以便 Oracle ILOM 重設之後可以進行還原，否則這些組態變更將會遺失。

1. **在管理網路上，登入 Oracle ILOM。**

   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷 Oracle ILOM 是否設定為 FIPS 140 相容作業。**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   Oracle ILOM 中的 FIPS 140 相容模式以 `state` 和 `status` 特性表示。`state` 特性代表 Oracle ILOM 中設定的模式，`status` 特性代表 Oracle ILOM 中的作業模式。當 FIPS `state` 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` 特性。

3. **啟用 FIPS-140 相容作業。**

```
-> set /SP/services/fips state=enabled
```

4. **重新啟動 Oracle ILOM 服務處理器。**

   必須重新啟動 Oracle ILOM SP，此變更才能生效。

```
-> reset /SP
```

預設帳號和密碼 (Oracle ILOM)

帳號	類型	預設密碼	描述
`root`	管理員	`welcome1`	這是針對此元件提供和啟用的預設帳號。此帳號是用來執行初始組態和允許建立其他、非共用的管理帳號。

帳號	類型	預設密碼	描述
			為了安全起見，請變更預設密碼。

預設公開的網路服務 (Oracle ILOM)

此表格列出 Oracle ILOM 公開的預設網路服務。

如需有關這些服務的其他資訊，請參閱「*Oracle ILOM Security Guide*」(「其他 Oracle ILOM 資源」[46])。

服務名稱	協定	連接埠	描述
SSH	TCP	22	由整合的安全 Shell 服務使用，可使用 CLI 對 Oracle ILOM 進行管理存取。
HTTP (BUI)	TCP	80	由整合的 HTTP 服務使用，可使用瀏覽器介面對 Oracle ILOM 進行管理存取。TCP/80 通常用於純文字存取，但是 Oracle ILOM 預設會自動將內送要求重新導向至此服務在 TCP/443 執行的安全版本。
NTP	UDP	123	由整合的網路時間協定 (NTP) 服務使用 (僅限用戶端)，用來將本機系統時鐘同步到一或多個外部時間來源。
SNMP	UDP	161	由整合的 SNMP 服務使用，提供管理介面監督 Oracle ILOM 的狀況和監督收到的設陷通知。
HTTPS (BUI)	TCP	443	由整合的 HTTPS 服務使用，可使用瀏覽器介面透過加密的 (SSL/TLS) 通道對 Oracle ILOM 進行管理存取。
IPMI	TCP	623	由整合的智慧平台管理介面 (IPMI) 服務使用，提供電腦介面供各種監督和管理功能使用。此服務不得停用，因為 Oracle Enterprise Manager Ops Center 使用此服務來收集硬體庫存資料、FRU 描述、硬體感應器資訊以及硬體元件狀態資訊。
遠端 KVMS	TCP	5120 5121 5123 5555 5556 7578 7579	遠端 KVMS 連接埠集體提供一組協定，提供遠端鍵盤、視訊、滑鼠和儲存功能，可與 Oracle Integrated Lights Out Manager 搭配使用。
ServiceTag	TCP	6481	由 Oracle ServiceTag 服務使用。這是一種 Oracle 尋找協定，主要用於識別伺服器及協助進行服務要求。此服務由產品 (像是 Oracle Enterprise Manager Ops Center) 用來尋找 Oracle ILOM 軟體，以及與其他 Oracle 自動服務解決方案整合。
WS-Man over HTTPS	TCP	8888	由整合的 WS-Man 服務使用，提供標準的 Web 服務介面，透過 HTTPS 協定管理 Oracle ILOM。停用此服務時，可防止使用此協定來管理 Oracle ILOM。自 Oracle ILOM 版本 3.2 起不再包含此服務。
WS-Man over HTTP	TCP	8889	此連接埠由整合的 WS-Man 服務使用，提供標準的 Web 服務介面，透過 HTTP 協定管理 Oracle ILOM。停用此服務將可防止使用此協定來管理 Oracle ILOM。自 Oracle ILOM 版本 3.2 起不再包含此服務。

服務名稱	協定	連接埠	描述
Single Sign-On	TCP	11626	此連接埠由整合的 Single Sign-On 功能使用，可減少使用者必須輸入使用者名稱和密碼的次數。停用此服務後，一定要重新輸入密碼才能啟動 KVMS。

強化 Oracle ILOM 安全組態

以下主題描述如何透過各種組態設定值保護 Oracle ILOM。

▼ 停用不需要的服務 (Oracle ILOM)

請停用平台上不是支援操作與管理需求所必要的任何服務。

Oracle ILOM 預設會採用網路預設保護組態 (已經停用非必要的服務)。但是，依據您安全原則與需求的不同，有可能需要停用其他服務。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷 Oracle ILOM 支援的服務清單。**

   ```
   -> show /SP/services
   ```

3. **判斷是否啟用指定的服務。**
   將 *servicename* 取代為步驟 2 中識別的服務名稱。

```
-> show /SP/services/servicename servicestate
```

雖然大多數服務都能辨識和使用 `servicestate` 參數記錄服務為啟用或停用，但是還是有少數服務 (例如 `servicetag`、`ssh`、`sso` 和 `wsman`) 使用稱為 `state` 的參數。無論實際使用的參數為何，若 `servicestate` 或 `state` 參數傳回 `enabled` 值，就代表服務已啟用，如下列範例所示：

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

```
-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **若要停用不需要的服務，請將服務狀態設定為 `disabled`。**

```
-> set /SP/services/http servicestate=disabled
```

5. **判斷是否要停用下列任何服務。**

   根據使用的工具和方法，若不需要或不使用下列其他服務，就可予以停用：

   - **如果是瀏覽器管理介面 (HTTP、HTTPS)，請輸入：**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **如果是鍵盤、視訊、滑鼠服務 (KVMS)，請輸入：**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **如果是 Web 服務管理 (WS-Man over HTTP/HTTPS) - (Oracle ILOM 版本 3.1 和更舊版本)，請輸入：**

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **如果是 Single-Sign On 服務 (SSO)，請輸入：**

     ```
     -> set /SP/services/sso state=disabled
     ```

▼ 設定 HTTP 重新導向至 HTTPS (Oracle ILOM)

Oracle ILOM 預設會設定為將內送 HTTP 要求重新導向至 HTTPS 服務，以確保 Oracle ILOM 和管理員之間的所有瀏覽器通訊都經過加密。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。
2. **確認已啟用安全重新導向。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **若預設值已變更，您可以啟用安全重新導向。**

```
-> set /SP/services/http secureredirect=enabled
```

4. **重複執行步驟 2 來驗證設定。**

停用未核准的協定

請使用下列主題停用未核准的協定：

- 「停用 HTTPS 的 SSLv2 協定」[39]
- 「停用 HTTPS 的 SSLv3 協定」[40]

▼ 停用 HTTPS 的 SSLv2 協定

HTTPS 服務預設會停用 SSLv2 協定。

為了安全起見，請務必要停用 SSLv2。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。
2. **判斷 HTTP 服務是否停用 SSLv2 協定。**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **如果服務已啟用，請停用 SSLv2 協定。**

```
-> set /SP/services/https sslv2=disabled
```

4. **重複執行步驟 2 來驗證設定。**

▼ 停用 HTTPS 的 SSLv3 協定

HTTPS 服務預設會啟用 SSLv3 協定。

為了安全起見，請停用 SSLv3 協定。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷 HTTP 服務是否停用 SSLv3 協定。**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **停用 SSLv3 協定。**

```
-> set /SP/services/https sslv3=disabled
```

4. **重複執行步驟 2 來驗證設定。**

▼ 停用 HTTPS 未核准的 TLS 協定

HTTPS 服務預設會啟用 TLSv1.0、TLSv1.1 和 TLSv1.2 協定。

您可以停用一或多個不符合您安全原則的 TLS 協定版本。

除非必須支援較舊版本的 TLS 協定，否則為了安全起見，請使用 TLSv1.2。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷針對 HTTPS 服務啟用的 TLS 協定版本清單。**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
```

```
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **停用 TLSv1.0。**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **停用 TLSv1.1。**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **重複執行步驟 2 來驗證設定。**

▼ 停用 HTTPS 的 SSL 弱加密和中等強度加密

Oracle ILOM 預設會停用 HTTPS 服務的弱加密和中等強度加密。

1. **在管理網路上，登入 Oracle ILOM。**
請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷是否停用弱加密和中等強度加密。**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **若預設值已變更，您可以停用弱加密和中等強度加密。**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **重複執行步驟 2 來驗證設定。**

▼ 停用未核准的 SNMP 協定 (Oracle ILOM)

預設只會啟用 SNMP 服務的 SNMPv3 協定，此服務用於監督和管理 Oracle ILOM。除非必要，否則請確定將舊版的 SNMP 協定維持停用。

部些 Oracle 和第三方產品可能不支援較新版本的 SNMP 協定。請參閱與這些元件相關的產品文件，以確認是否支援特定的 SNMP 協定版本。請確定已將 Oracle ILOM 設定為支援這些元件所需的協定版本。

注意 - 版本 3 的 SNMP 協定導入以使用者為基礎的安全模型 (USM) 支援。這項功能將傳統的 SNMP 社群字串取代為能夠為其設定特定權限、認證、私密協定以及密碼的實際使用者帳號。Oracle ILOM 預設不會包含任何 USM 帳號。請根據您自己的部署、管理和監督需求，設定 SNMPv3 USM 帳號。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷每個 SNMP 協定的狀態。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **如有需要，請停用 SNMPv1 和 SNMPv2c。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **重複執行步驟 2 來驗證設定。**

▼ 設定 SNMP v1 和 v2c 社群字串 (Oracle ILOM)

此工作只有當啟用 SNMPv1 或 SNMPv2c 且設定使用時才適用。

若要讓 SNMP 正確運作，用戶端和伺服器必須同意用於認證存取的社群字串。因此，變更 SNMP 社群字串後，請確定已經在 Oracle ILOM 和針對使用 SNMP 協定嘗試與 Oracle ILOM 連線的所有元件上設定新的字串。

由於 SNMP 經常會用來監督裝置的狀況，因此請務必將裝置所使用的預設 SNMP 社群字串取代為客戶定義值。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **建立新的 SNMP 社群字串。**
   在本範例中，請取代指令行中的以下項目：

   - *string* – 取代為符合美國國防部有關 SNMP 社群字串組合要求的客戶定義值。

- *access* – 根據這是唯讀或讀寫存取字串，取代為 `ro` 或 `rw`。

```
-> create /SP/services/snmp/communities/string permission=access
```

建立好新的社群字串之後，就必須移除預設的社群字串。

3. **移除預設的 SNMP 社群字串。**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **驗證 SNMP 社群字串。**

```
-> show /SP/services/snmp/communities
```

▼ 取代預設自行簽署的憑證 (Oracle ILOM)

Oracle ILOM 使用自行簽署的憑證，以便立即可使用 SSL 和 TLS 協定。如果可以，請將自行簽署的憑證取代為您環境中核准使用，並且由認可的憑證授權單位簽署的憑證。

Oracle ILOM 支援各種可用來存取數位憑證和私密金鑰的方法，包括 HTTPS、HTTP、SCP、FTP、TFTP 並且會直接將資訊貼入 Web 瀏覽器介面。如需詳細資訊，請參閱「*Oracle ILOM Configuration and Maintenance Guide*」(「其他 Oracle ILOM 資源」[46])。

1. **判斷 Oracle ILOM 是否使用預設自行簽署的憑證。**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **安裝您組織的憑證。**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ 設定瀏覽器管理介面無活動逾時

Oracle ILOM 支援中斷連線並登出超過預先定義分鐘數而無活動之管理階段作業的功能。瀏覽器介面階段作業預設會在 15 分鐘後逾時。

與 HTTPS 和 HTTP 服務相關的階段作業逾時參數需分別設定和管理。務必要設定與每個服務相關的 `sessiontimeout` 參數。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **檢查與 HTTPS 服務有關的無活動逾時參數。**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **設定無活動逾時參數。**
   將 *n* 取代為以分鐘為單位的指定值。

```
-> set /SP/services/https sessiontimeout=n
```

4. **檢查與 HTTP 服務有關的無活動逾時參數。**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **設定無活動逾時參數。**
   將 *n* 取代為以分鐘為單位的指定值。

```
-> set /SP/services/http sessiontimeout=n
```

6. **重複執行步驟 2 和步驟 4 來驗證設定。**

▼ 設定管理介面逾時 (Oracle ILOM CLI)

Oracle ILOM 支援中斷連線並登出超過預先定義分鐘數而無活動之管理 CLI 階段作業的功能。

SSH CLI 預設沒有指定逾時值，因此存取此服務的管理使用者會無限制一直維持登入狀態。

為了安全起見，請將此參數設定為符合與瀏覽器使用者介面相關的值。此值可以是 15 分鐘或其他值。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **檢查與 CLI 有關的無活動逾時參數。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **設定無活動逾時參數。**
   將 *n* 取代為以分鐘為單位的指定值。

```
-> set /SP/cli timeout=n
```

4. **重複執行步驟 2 來驗證設定。**

▼ 設定登入警告標題 (Oracle ILOM)

Oracle ILOM 支援在管理員連線至裝置之前和之後顯示客戶專屬訊息的功能。

Oracle ILOM 連線訊息會在驗證之前顯示，登入訊息則是在驗證之後顯示。

您可以選擇性將 Oracle ILOM 設定為必須接受登入訊息後，才能獲得授權存取 Oracle ILOM 的功能。瀏覽器和指令行存取兩種介面都有實作連線訊息和登入訊息，以及選擇性的接受要求。

Oracle ILOM 支援最多 1,000 個字元的連線訊息和登入訊息。

1. **在管理網路上，登入 Oracle ILOM。**
   請參閱「登入 Oracle ILOM CLI」[33]。

2. **判斷是否設定連線訊息和登入訊息。**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **設定連線訊息或登入訊息。**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **判斷登入訊息接受是否啟用。**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(選擇性) 強制接受登入訊息。**

注意 - 要求登入訊息接受可能會導致使用 SSH 的自動管理程序無法正確運作，因為這些程序可能無法回應或無法設定為回應接受要求。因此，這類連線可能會停止回應或逾時，因為必須先滿足訊息接受要求，Oracle ILOM 才會允許使用 CLI。

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **重複執行步驟 2 和步驟 4 來驗證設定。**

其他 Oracle ILOM 資源

如需有關 Oracle ILOM 管理和安全性程序的詳細資訊，請參閱對應 SuperCluster M7 上執行版本的 Oracle ILOM 文件庫。

- *Oracle ILOM Security Guide Firmware Releases 3.0*、*3.1* 和 *3.2*：

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager 版本 3.2.*x*：

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager 版本 3.1.*x*：

  http://docs.oracle.com/cd/E24707_01
- Oracle Integrated Lights Out Manager 版本 3.0.*x*：

  http://docs.oracle.com/cd/E19860-01

保護運算伺服器的安全

SuperCluster M7 中安裝了一或兩部 SPARC M7 伺服器 (運算伺服器)。每部運算伺服器各分割為兩個硬體分割區 (兩個 PDomain)。每個 PDomian 均包含機架中一半可用的處理器、記憶體和 PCIe 擴充插槽。PDomain 在同一個機架中是以獨立伺服器的形式運行。一組備援的服務處理器模組 (SPM) 負責管理每個分割區。

您必須保護每個 PDomain。

本節提供一系列運算伺服器的安全控制做法。

▼ 登入運算伺服器並變更預設密碼

若要透過 Oracle ILOM 存取單一 PDomain，您必須登入控制該 PDomain 的作用中 SPM。您可以在一個分割區持續正常運作的情況下，開啟另一個分割區的電源、重新啟動該分割區或管理該分割區。

有數種方法可以登入 SuperCluster 運算伺服器。此工作中描述的方法，是在運算伺服器的 SPM 上登入 Oracle ILOM CLI。此方法可讓您存取下列任一種狀態的伺服器：

- 備用電源模式
- 系統電源開啟，但主機未執行
- 作業系統正在啟動
- 完全啟動，且作業系統正在執行

1. **在管理網路上，使用 `ssh` 指令登入。**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **系統出現提示時，請輸入密碼。**
   出廠預設的 `root` 密碼為 `welcome1`。
   若系統提示您變更密碼，請加以變更。
   此時，您就可以在運算伺服器上執行原本在 Oracle ILOM 中執行的任何安全工作。

3. **若您想存取運算伺服器的主機主控台，請啟動主機主控台。**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

注意 - 若主機未執行，您就看不到 PDomain 提示。

注意 - 若要切換回 Oracle ILOM 提示，請輸入跳脫字元 (預設的跳脫字元是 `#.`)。

4. **如有需要，請以超級使用者角色執行操作。**
   使用 `su` 指令切換為已設定 `root` 角色的使用者。

預設帳號和密碼 (運算伺服器)

帳號	預設密碼	描述
`root`	`welcome1`	第一次成功登入後，Oracle ILOM 會要求您立即變更預設密碼。
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ 判斷 SuperCluster 軟體版本

1. **登入其中一部運算伺服器並存取主機主控台。**

請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **輸入這個指令。**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

在輸出中，附加至 `ssc` 的數字代表軟體版本。

若要更新 SuperCluster 軟體的版本，請從 My Oracle Support (網址為 `https://support.oracle.com`) 安裝所提供的最新版 SuperCluster Quarterly Full Stack Download Patch。

注意 - 就 SuperCluster 而言，額外的限制可能限縮能夠使用的軟體版本和這些版本的更新方式。若出現此類情況，請洽詢您的 Oracle 服務人員。

▼ 設定安全 Shell 服務

執行此工作有助於改善在 Oracle SuperCluster 中部署的安全 Shell 安全組態。

`/etc/ssh/sshd_config` 檔案是整個系統的組態檔案，您可以在其中組態安全 Shell 服務的參數。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **編輯 `/etc/ssh/sshd_config` 檔案。**

3. **設定 `ListenAddress` 參數，以確保只會接受來自 SuperCluster 用戶端存取網路的連線。**
   確定 `ListenAddress` IP 位址設為用戶端網路。
   這樣可確保透過管理網路或 IB 網路的元件都無法成功起始安全 Shell 連線。

4. **複查其他 `sshd_config` 參數，依據網站需求加以設定。**
   這些設定值可保護安全 Shell 服務：

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **儲存 `sshd_config` 檔案。**

6. **重新啟動服務。**

   您必須重新啟動服務，才能讓變更生效。

```
# svcadm restart ssh
```

▼ 確認 root 為角色

依照 Oracle Solaris 的預設設定，root 會是角色而非使用者帳號。此外，SuperCluster 組態不允許匿名的 root 使用者登入。正確的作法是在預設 root 角色之前，所有使用者必須先以一般使用者身分登入。所有 SuperCluster 管理作業都必須使用 root 角色來執行。

1. **登入其中一部運算伺服器並存取主機主控台。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **確認 `root` 屬性設為 `type=role`。**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(選擇性) 將 `root` 角色指派給任何一般使用者。**

```
# usermod -R root user_name
```

預設公開的網路服務 (運算伺服器)

此表格列出運算伺服器上公開的預設網路服務。

服務名稱	協定	連接埠	描述
SSH	TCP	22	由整合的安全 Shell 服務使用，以便使用 CLI 對運算伺服器進行管理存取。
HTTP (BUI)	TCP	80	由整合的 HTTP 服務使用，以便使用瀏覽器介面對運算伺服器進行管理存取。
HTTPS (BUI)	TCP	443	由整合的 HTTPS 服務使用，以便使用瀏覽器介面透過加密的 (SSL/TLS) 通道對運算伺服器進行管理存取。
SNMP	UDP	161	由整合的 SNMP 服務使用，以提供管理介面來監督運算伺服器的狀況和監督收到的設陷通知。

強化運算伺服器安全組態

以下主題描述如何安全地設定運算伺服器。

▼ 啟用 intrd 服務

中斷平衡器 (intrd) 服務會監督中斷和 CPU 之間的指派狀況，以確保最佳效能。如需詳細資訊，請參閱 intrd(1M) 線上手冊。

此服務只會在全域區域執行。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟動服務。**

```
# svcadm enable intrd
```

▼ 停用不需要的服務 (運算伺服器)

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **若系統不是 NFS 用戶端或伺服器，請停用 NFS 狀態監督。**
   此服務會與 `lockd(1M)` 互動，為 NFS 上的鎖定服務提供損毀和復原功能。

```
# svcadm disable svc:/network/nfs/status
```

3. **若您並未使用 NFS 或使用的是 NFSv4，請停用 NFS 鎖定管理程式服務。**
   NFS 鎖定管理程式支援 NFSv2 和 NFSv3 之 NFS 檔案的記錄鎖定作業。

```
# svcadm disable svc:/network/nfs/nlockmgr
```

4. **若系統未掛載檔案，您可以停用 NFS 用戶端服務或解除安裝其套裝軟體。**
   只有系統是從 NFS 伺服器掛載檔案時，才需要 NFS 用戶端服務。如需詳細資訊，請參閱 `mount_nfs(1M)` 線上手冊。

```
# svcadm disable svc:/network/nfs/client
```

5. **在非 NFS 檔案伺服器的系統上停用 NFS 伺服器服務。**
   NFS 伺服器服務是透過 NFS 版本 2、3 及 4 來處理用戶端檔案系統要求。若此系統不是 NFS 伺服器，請停用此服務。

```
# svcadm disable svc:/network/nfs/server
```

6. **若您不是為了 DNS SRV 記錄或 LDAP 轉介而使用 FedFS，請停用此服務。**
   聯合檔案系統 (FedFS) 用戶端服務可管理儲存 FedFS 資訊的 LDAP 伺服器預設值和連線資訊。

```
# svcadm disable svc:/network/nfs/fedfs-client
```

7. **停用 `rquota` 服務。**

remote 配額伺服器會傳回透過 NFS 掛載之本機檔案系統的使用者配額。quota(1M) 則利用此結果來顯示遠端檔案系統的使用者配額。rquotad(1M) 常駐程式通常會藉由 inetd(1M) 進行呼叫。此常駐程式會將網路的相關資訊提供給潛在的惡意使用者。

```
# svcadm disable svc:/network/nfs/rquota
```

8. **停用 cbd 服務。**
   cbd 服務可管理 NFS 第 4 版協定的通訊端點。nfs4cbd(1M) 常駐程式會在 NFS 第 4 版用戶端上執行，並為回呼建立監聽器連接埠。

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **若您並未使用 NFSv4，請停用 mapid 服務。**
   NFS 使用者和群組 ID 對應常駐程式服務會在 NFS 第 4 版 owner 和 owner_group 識別屬性之間與本機 UID 和 GID 編號之間進行對應，NFS 第 4 版用戶端與伺服器都會用到這些資訊。

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **停用 ftp 服務。**
    FTP 服務提供未加密的檔案傳輸服務，並使用純文字認證。請使用安全的複製程式 scp(1) 取代 ftp，因為前者提供加密的認證和檔案傳輸。

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **停用遠端磁碟區管理程式服務。**
    卸除式磁碟區管理程式是 HAL 感知的磁碟區管理程式，會自動掛載和卸載卸除式媒體和可熱插式儲存體。使用者可能會匯入惡意程式，或是將機密資料傳送到系統之外。如需詳細資訊，請參閱 rmvolmgr(1M) 線上手冊。
    此服務只會在全域區域執行。

    ```
    # svcadm disable svc:/system/filesystem/rmvolmgr
    ```

12. **停用 smserver 服務。**
    smserver 服務是用來存取卸除式媒體裝置。

    ```
    # svcadm disable rpc/smserver:default
    ```

13. **在 /etc/pam.d 目錄中指定 pam_deny.so.1 作為 r-protocol 服務的認證堆疊模組。**
    預設不會安裝 r-protocols、rlogin(1) 及 rsh(1) 等傳統服務。但這些服務會定義在 /etc/pam.d 中。若從 /etc/pam.d 移除這些服務的定義，您啟用這些傳統服務時，就會使用其他服務 (如 SSH)。

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. 編輯 `/etc/default/keyserv` 檔案以將 `ENABLE_NOBODY_KEYS` 的值變更為 `NO`。

`keyserv` 服務無法使用 `nobody` 使用者金鑰。依照預設，`ENABLE_NOBODY_KEYS` 的值為 `YES`。

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. 新增使用者到 `ftpusers` 檔案以限制 `ftp` 存取。

FTP 檔案傳輸不得開放給所有使用者存取，因此必須要求合格的使用者提供其名稱和密碼。系統使用者通常不能使用 FTP。此檢查可驗證系統帳號包含在 `/etc/ftpd/ftpusers` 檔案中，這些系統帳號就無法使用 FTP。

使用檔案 `/etc/ftpd/ftpusers` 可禁止使用者使用 FTP 服務。至少應包含所有系統使用者，如 `root`、`bin` 及 `adm` 等。

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. 為 FTP 伺服器建立的檔案設定強式預設檔案建立遮罩。

FTP 伺服器不一定會用到使用者的系統檔案建立遮罩。設定 FTP umask 可確保經由 FTP 傳輸的檔案會使用強式檔案建立 umask。

```
# pfedit /etc/proftpd.conf
Umask          027
```

17. 停用對網路拓樸查詢的回應。

停用對 echo 要求的回應很重要。ICMP 要求是以 `ipadm` 指令來管理。

這些設定值可防止散播網路拓樸的資訊。

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

18. 停用重導 ICMP 訊息。

路由器會使用 ICMP 重導訊息來通知主機有更直接的目的地路由。違法的 ICMP 重導訊息可能會導致攔截式攻擊。

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
```

19. **停用 `mesg(1)` 可防止 `talk(1)` 和 `write(1)` 存取遠端終端機。**

```
# mesg -n
```

20. **(選擇性) 複查並停用網路上不需要的服務監聽活動。**
依照預設，`ssh(1)` 是唯一可傳送和接收網路封包的網路服務。

```
# svcadm disable FMRI_of_unneeded_service
```

▼ 啟用嚴格的多址機制

對於作為其他網域閘道的系統 (例如防火牆或 VPN 節點)，必須啟用嚴格的多址機制。`hostmodel` 特性控制多址系統上 IP 封包的傳送與接收運作方式。將嚴格的多址設定設為 `1`，讓其他介面不會再接受封包。預設值為 `0`。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **將嚴格的多址設定設為 `1`。**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

▼ 啟用 ASLR

注意 - 在資料庫網域或資料庫區域中，請勿啟用 ASLR。

Oracle Solaris 會標記許多使用者二進位檔以啟用位址空間配置隨機載入 (ASLR)。ASLR 會隨機配置位址空間關鍵部分的起始位址。此安全防禦機制會讓「返回導向程式設計 (ROP)」攻擊在嘗試入侵軟體漏洞時失敗。區域的處理作業會繼承此隨機配置。由於 ASLR 的使用對所有二進位檔而言可能不是最佳做法，因此可以在區域和二進位檔層次設定 ASLR。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用 ASLR。**

```
# sxadm delcust aslr
```

```
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

▼ 設定 TCP 連線

將每一連接埠、每一 IP 位址的半開放式 TCP 連線數上限設為 4096，將有助於防範 SYN 洪水式阻斷服務攻擊。將佇列的 TCP 內送連線數上限設為大於或等於 1024，將有助於防範某些分散式阻斷服務 (DDoS) 攻擊。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **設定半開放式和佇列的內送 TCP 連線數上限。**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

▼ 設定密碼歷史記錄和密碼原則以符合 PCI 規範

`/etc/default/passwd` 中的 `HISTORY` 參數可防止使用者在 `HISTORY` 值的期限內使用類似的密碼。

如果 `MINWEEKS` 設為 `3` 而 `HISTORY` 設為 `10`，則 10 個月內不能重複使用類似的密碼。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **編輯 `/etc/default/passwd` 檔案並設定密碼參數。**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **編輯 `/etc/default/login` 檔案以包含這些參數。**

```
# pfedit /etc/default/login
```

```
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

▼ 確定使用者本位目錄已設定適當權限

本位目錄必須可供其擁有者寫入和搜尋。其他使用者通常無法修改這些檔案或新增檔案到使用者的本位目錄。為確保此一情況，請在使用者目錄上設定權限。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **在使用者目錄上設定權限。**

```
# chmod 750 /export/home/user_home_directory
```

▼ 啟用 IP 篩選防火牆

IP 篩選是以主機為基礎的防火牆，可提供狀態性封包篩選和網路位址轉譯 (NAT)。封包篩選可提供基本的網路攻擊防護。IP 篩選也包含無狀態的封包篩選，並可建立與管理位址集區。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用 IP 篩選防火牆。**

```
# svcadm svc:/network/ipfilter:default
```

▼ 確定名稱服務僅使用本機檔案

作業系統會使用許多關於主機、`ipnodes`、使用者 (`passwd(4)`、`shadow(4)`、`user_attr(4)`) 及 `groups` 的資訊資料庫。這些項目的資料有許多不同來源。例如，您可以在 `/etc/hosts`、NIS、LDAP、DNS 或多點傳送 DNS 中找到主機名稱和主機位址。若這些項目只使用本機檔案項目，則受限制環境中的系統會更加安全。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **將名稱服務設定為只使用本機檔案。**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

▼ 啟用 Sendmail 與 NTP 服務

sendmail 服務必須執行，否則寄給 `root` 的重要系統郵件將無法遞送。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用 sendmail。**

```
# svcadm enable smtp:sendmail
```

3. **如有需要，請安裝 NTP 服務。**
   安裝 `ntp` 服務的所有系統都必須符合安全和規範要求。

```
# pkg install service/network/ntp
```

4. **將 NTP 服務設定為用戶端並啟用該服務。**
   「網路時間協定」常駐程式必須啟用，並正確設定為用戶端。`/etc/inet/ntp.conf` 檔案必須至少包含一個伺服器定義。該檔案也必須包含 `restrict default ignore` 指令行，以防止用戶端同時作為伺服器。

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

▼ 停用 GSS (除非有使用 Kerberos)

一般安全服務 (`gss`) 是用來管理「一般安全服務應用程式的程式介面 (GSS-API)」安全記號的產生和驗證。`gssd(1M)` 常駐程式是在核心 `rpc` 與 GSS-API 之間運作。

注意 - Kerberos 會用到此服務。若未設定且未使用 Kerberos，請停用 `rpc/gss` 服務。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用 `rpc/gss`。**

```
# svcadm enable rpc/gss
```

3. **設定 `/tmpfs` 的大小限制。**
   `tmpfs` 檔案系統的大小預設為沒有限制。為避免效能影響，您可以限制每個 `tmpfs` 掛載的大小。如需詳細資訊，請參閱 `mount_tmpfs(1M)` 與 `vfstab(4)` 線上手冊。

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **重新啟動運算伺服器。**

```
# reboot
```

▼ 為全球可寫入檔案設定黏著位元

目錄上的黏著位元能防止全球可寫入目錄中的檔案被檔案擁有者以外的任何人或 `root` 角色刪除或移動。這對許多使用者共用的目錄 (例如 `/tmp` 目錄) 而言格外實用。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **在 `/tmp` 和全球可寫入的任一檔案上設定黏著位元。**

```
# chmod 1777 /tmp
```

▼ 保護核心傾印

核心傾印可能包含機密資料。保護的範圍包括檔案權限和記錄日誌核心傾印事件。請參閱 `coreadm(1m)` 與 `chmod(1M)` 線上手冊。

使用 `coreadm` 指令可檢視和設定目前的組態。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **檢視目前的組態。**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **設定核心檔案和保護核心傾印目錄。**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **檢查權限。**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **正確地設定目錄權限。**

```
# chmod 700 /var/share/cores
```

▼ 強制施行不可執行的堆疊

啟用不可執行的堆疊對阻撓某些緩衝區溢位攻擊而言，是一項非常有利的技術。若啟用 Oracle Solaris `nxstack`，處理作業堆疊記憶體區段會標示為不可執行。此擴充功能可防禦會植入並在堆疊上執行惡意程式碼的攻擊。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用 `nxstack`。**

```
# sxadm set model=all nxstack
```

3. **請確認組態。**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

▼ 啟用加密的交換空間

加密交換空間 (ZFS 磁碟區或原始裝置皆可使用)。若系統需要將任何機密資料 (如使用者密碼) 頁面交換到磁碟，加密功能可確保這些資料受到保護。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **編輯 `/etc/vfstab` 檔案並將 `swap` 設為 `encrypted`。**

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **建立並起始 PKCS #11 金鑰存放區。**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **產生對稱式金鑰，並將它儲存在 PKCS #11 金鑰存放區。**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

▼ 啟用稽核

確定稽核記錄會擷取所有管理動作，包括指令和引數。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **設定稽核設備。**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

▼ 在全域區域上啟用資料連結 (詐騙) 保護

Oracle Solaris 資料連結保護可防止惡意的來賓 VM 可能對網路造成的潛在損害。

藉由將虛擬環境的網路流量與主機系統所接收或傳送的較大流量隔離，啟用窺探防護組態，進而改善網路效能。連結保護可防止潛在的惡意來賓 VM 可能對網路造成的損害。此功能可保護系統，不會受到下列基本威脅的危害：

- IP 與 MAC 詐騙
- L2 框架詐騙 (如橋接器協定資料單位 (BPDU) 攻擊)

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **設定連結保護。**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **確認組態。**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **在連結上設定允許的 IP。**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

▼ 在非全域區域上啟用資料連結 (詐騙) 保護

Oracle Solaris 資料連結保護也可以個別套用至 SuperCluster 環境內的所有 Oracle Solaris 非全域區域。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **請使用 `zonecfg(1M)` 指令在特定網路介面上強制執行資料連結保護。**

   確定允許的 IP 位址清單正確且完整。此清單必須包含 Oracle Solaris IPMP 及 Oracle Real Application Clusters 等使用的任何虛擬 IP 位址。另請注意，對 SuperCluster 非全域區域組態所做的變更，要在非全域區域重新啟動後才會生效。

```
# zonecfg -z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

▼ 建立加密的 ZFS 資料集

需要 *data-at-rest* 保護的組織可選擇使用加密的 ZFS 資料集，進一步保護區域部署的應用程式和資訊。為確保每個非全域區域都能在沒有管理員介入的情況下啟動，加密的 ZFS 資料集是設定為存取個別的資料庫或應用程式網域內本機儲存的 ZFS 加密金鑰。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **建立 ZFS 加密金鑰。**

   建立所需金鑰的一個簡易方法，是使用類似下列的指令：

```
# zfs createzfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **建立加密的 ZFS 資料集。**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
zfs_pool_name/zone_name
```

4. **加密 u01 和通用資料集。**

   這個方法也可用來加密 u01 和通用資料集，依據網站特定的需求和原則，使用相同的 (SuperCluster 特定的) 金鑰或每一資料集各使用唯一的金鑰。在此範例中，我們使用步

驟 3 中建立的金鑰來建立通用資料集。請注意，建立這些額外的資料集時，也可以定義額外的 ZFS 組態參數 (如 compression)。

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ (選擇性) 設定存取金鑰存放區的密碼詞組

先前的工作「建立加密的 ZFS 資料集」[63] 中，我們使用本機定義的 (原始) 金鑰檔案，此檔案必須直接儲存在檔案系統中。另一個金鑰儲存技術則利用密碼詞組保護的 PKCS#11 金鑰存放區，稱為 *Sun Software PKCS#11 Softtoken*。若要使用此方法，請執行本工作。

PKCS#11 金鑰存放區必須先手動解除鎖定，才能將金鑰提供給 ZFS 使用。這終究意味著需要管理員介入，才能掛載加密的 ZFS 資料集和啟動非全域區域 (若此區域也使用加密的 ZFS 資料集)。如需其他金鑰儲存策略的詳細資訊，請參閱 `zfs_encrypt(1M)` 線上手冊。

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**
   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **設定存取金鑰存放區所需的 PIN (密碼詞組)。**
   與新的 PKCS#11 金鑰存放區關聯的預設 PIN 為 `changeme`。在本範例的第一個提示中使用此密碼詞組。

   ```
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

3. **定義一個 `${SOFTTOKEN}` 環境變數，以便將金鑰儲存在不同的位置。**
   PKCS#11 Softtoken 使用的金鑰資料預設會儲存在 `/var/user/ ${USERNAME}/pkcs11_softtoken` 目錄。您可以定義 `${SOFTTOKEN}` 環境變數，將金鑰資料儲存在不同的位置。您可以使用此功能，為這個密碼詞組保護的金鑰資料啟用 SuperCluster 特定的存放區。

   ```
   # export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

4. **建立金鑰。**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **建立加密的 ZFS 資料集，參考先前步驟中建立的金鑰。**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

▼ 建立不可變的全域區域

使用不可變特性的防竄改功能，可讓全域區域和非全域區域建立一個具有彈性、高完整性的作業環境，SuperCluster 運算伺服器可以在其中運行其服務。建立在 Oracle Solaris 全域和非全域區域固有的安全功能上，不可變的區域可確保在沒有管理員介入的情況下，就無法變更部分或全部的作業系統目錄和檔案。強制施行此唯讀態勢有助於防止未經授權的變更，提升為更安全的變更管理程序，以及制止核心和使用者形式的惡意軟體入侵。

注意 - 一旦不可變的區域設定後，除非經由「信任的路徑」登入或使用 `reboot -- -w` 以可寫入模式重新啟動系統，否則將無法加以更新。

您應該一再確認應用程式軟體在不可變的環境中可以如預期般運作，而 Oracle 資料庫執行處理與 Oracle RAC 叢集則已通過驗證，可以在 Oracle Solaris 不可變的非全域區域正確執行。

1. **以超級使用者身分登入 Oracle Solaris 全域區域 (專用網域、根網域或 I/O 網域)。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **設定 `file-mac-profile` 特性，以修改 Oracle Solaris 全域組態。**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
zonecfg:global> commit
```

3. **重新啟動 Oracle Solaris 全域區域，使變更生效。從 ILOM 主控台登入網域。**

4. **啟動不可變的全域區域信任路徑主控台。**

   在不可變的全域區域設定後，必須使用下列其中一項中斷序列才能進入主控台登入：

   - **圖形主控台** – F1-A
   - **序列主控台** – <Break> 或替代的中斷序列 (CR~ Ctrl-b)

```
trusted path console login:
```

5. **登入 I/O 網域的全域區域，並以 `root` 角色對系統執行任何特定更新，然後將系統重新開機使其回到唯讀模式。**

```
# reboot
```

▼ 設定不可變的非全域區域

若要將 Oracle Solaris 非全域區域設定為不可變，請執行本工作。

注意 - 除了本工作中識別的不可變的區域組態以外 (固定組態)，Oracle Solaris 11 作業系統還支援其他不可變的區域組態。如需這些選項的詳細資訊，請參閱 `zonecfg(1M)` 線上手冊。但是，唯有固定組態選項經過 SuperCluster 架構組成的測試。

注意 - 一旦啟用 Oracle Solaris 非全域區域的不可變特性後 (如本工作所述)，就無法新增、修改或刪除區域使用者帳號和密碼。不過，您只要部署 LDAP 目錄以包含區域特定的資訊 (如使用者、角色、群組及權限設定檔等) 即可解決此問題。

注意 - 只有預設實作於 Oracle Solaris 非全域區域中的那些 ZFS 資料集，可以使用 Oracle Solaris 不可變的區域功能。其他檔案系統、集區或資料集不受不可變的區域原則約束，但可使用其他方法 (例如使用唯讀的回送掛載) 來控制對這些檔案元素的存取。

---

1. **以超級使用者身分登入其中一部運算伺服器並存取主機主控台。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **確定 Oracle Solaris 非全域區域已關閉。**

   若這個指令傳回值，就表示 Oracle Solaris 非全域區域正在執行，您必須將其關閉。

   注意 - 雖然您可以使用 `zoneadm(1M)` 指令來暫停區域，但請依您組織建立的正常關閉程序進行，以避免服務中斷或資料遺失的可能性。

```
# zoneadm list | grep -w "zone_name"
```

3. **設定 `file-mac-profile` 區域組態特性以調整 Oracle Solaris 非全域區域組態。**

```
# zonecfg -z zone_name set file-mac-profile=fixed-configuration
```

4. **如有需要，請停用非全域區域不可變的組態。**

```
# zonecfg -z zone_name set file-mac-profile=none
```

5. **重新啟動 Oracle Solaris 非全域區域以使變更生效。**

```
# zoneadm -z zone_name boot
```

▼ 啟用安全驗證式開機 (Oracle ILOM CLI)

使用此工作可透過 Oracle ILOM CLI 啟用安全驗證式開機。您也可以使用 Oracle ILOM Web 介面。請參閱「安全驗證式開機 (Oracle ILOM Web 介面)」[68]。

驗證式開機是指先驗證物件模組，再使用數位簽章執行。Oracle Solaris 的保護會讓惡意核心模組無法載入。驗證式開機會在核心模組執行前先行驗證，因此可增加 Oracle Solaris 的安全和穩定性。

啟用後，Oracle Solaris 驗證式開機會先檢查核心模組中的原廠簽署簽章，然後才載入和執行該模組。這項檢查可偵測模組是否不慎被修改或經過惡意修改。您可以設定要採取的動作，若啟用，則可以列出警告訊息並繼續載入和執行模組，或是宣告失敗而不載入且不執行模組。

1. **存取運算伺服器上的 Oracle ILOM。**

   請參閱「登入運算伺服器並變更預設密碼」[47]。

2. **啟用驗證式開機。**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **存取和顯示 Oracle 提供的憑證。**

   預先安裝的驗證式開機憑證檔案 `/etc/certs/ORCLS11SE` 是隨著 Oracle ILOM 所提供。

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **開始載入憑證。**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **複製 `/etc/certs/ORCLS11SE` 檔案的內容並貼到 Oracle ILOM 主控台。**

輸入 Ctrl-z 以儲存並處理資訊。

輸入 Ctrl-c 以結束並捨棄變更。

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. 驗證憑證。

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. 確認 OBP `use-nvram` 參數已設為 `false`。

使用驗證式開機時，OBP `use-nvram` 參數必須設為 `false`。這樣可防止 OBP 被修改為停用驗證式開機功能。預設值為 false。登入 Oracle Solaris 並輸入：

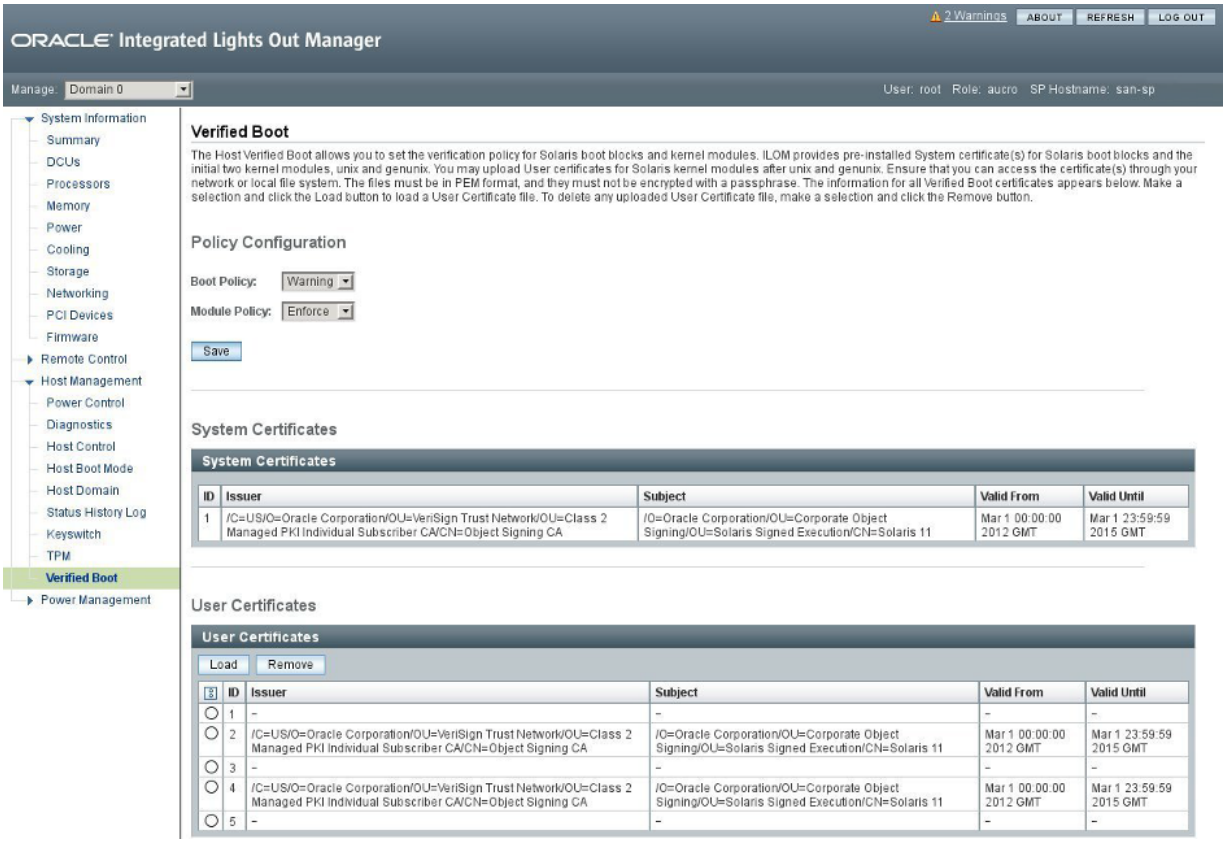
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

安全驗證式開機 (Oracle ILOM Web 介面)

Oracle ILOM Web 介面也提供與 CLI 相同的功能，可支援設定驗證式開機原則變數和管理憑證檔案。瀏覽至 [Host Management] (主機管理) 瀏覽功能表下的 [Verified Boot] (驗證式開機) 連結。

例如：



其他運算伺服器資源

如需 Oracle Solaris 作業系統和 Oracle Solaris Cluster 安全指南，請參閱您的作業系統版本對應的文件庫。文件庫位於：http:/docs.oracle.com/en/operating-systems。

如需 Oracle VM Server for SPARC 安全資訊，請參閱安全指南，網址為 http://docs.oracle.com/cd/E62357_01。

如需運算伺服器硬體的安全資訊，請參閱安全指南，網址為 http://docs.oracle.com/cd/E55211_01。

保護 ZFS 儲存設備的安全

ZFS 儲存設備是 SuperCluster 元件之一，提供各種不同工作負載需求的儲存合併支援，包括商業智慧、資料倉儲、虛擬化、開發與測試，以及資料保護。

ZFS 儲存設備有兩個備援的 ZFS 儲存控制器。您必須要保護這兩個控制器。

以下各節描述 ZFS 儲存設備安全準則與功能：

▼ 登入 ZFS 儲存設備

若要執行本節中的安全工作，您需要透過管理網路登入 ZFS 儲存設備。

本工作描述如何使用 CLI 登入。如需登入 Oracle ILOM Web 介面的指示，請參閱「*Oracle ZFS Storage Appliance Administration Guide*」中的「其他 ZFS 儲存設備資源」[79]。

1. **在您的管理網路，使用 SSH 連線至 ZFS 儲存設備。**
   如果您尚未設定可管理此設備的其他使用者，請使用 `root` 身分登入。

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **如有需要，請利用 CLI 說明。**

`help` 指令提供相關資訊環境的特定說明。如需特定主題的說明，請將該主題指定作為 `help` 的引數。在 help 指令輸入時按 Tab 鍵就會自動顯示提供的主題，或者也可以輸入 `help topics`。

▼ 判斷 ZFS 儲存設備軟體版本

請使用下述程序判斷 ZFS 儲存設備上的軟體版本。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **顯示軟體版本。**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

在本範例中，ZFS 儲存設備軟體的版本是 `2013.06.05.2.10`。

若要更新 ZFS 儲存設備軟體的版本，請從 My Oracle Support (網址為 `https://support.oracle.com`) 安裝所提供的最新版 SuperCluster Quarterly Full Stack Download Patch。

注意 - 就 SuperCluster 而言，額外的限制可能限縮能夠使用的 ZFS 儲存設備軟體版本和這些版本的更新方式。若出現此類情況，請洽詢您的 Oracle 服務人員。

▼ 變更 ZFS 儲存設備 `root` 密碼

ZFS 儲存設備本身並沒有預先設定的預設 `root` 密碼。初始組態 ZFS 儲存設備時，需要透過其內嵌之 Oracle ILOM 的主控台階段作業來執行。此設備的 `root` 密碼就是在進行此初始組態階段作業中加以設定。

當您第一次存取此設備的主控台時，會顯示一個 Shell 介面組態畫面。請驗證此畫面中的資訊並輸入必要的值。ZFS 儲存設備的 `root` 密碼就是在此程序中設定。

注意 - 此設備的 Oracle ILOM 有一個預設的 `root` 帳號和 `welcome1` 密碼。請參閱「保護 Oracle ILOM 的安全」[33]。

有了 `root` 帳號之後，您便可以依本作業中的描述隨時變更密碼。

注意 - 若是變更 Oracle Engineered Systems Hardware Manager 管理之任何 SuperCluster 元件 (例如 AFS 儲存控制器 OS) 的密碼，您必須同時在 Oracle Engineered Systems Hardware Manager 更新該密碼。如需詳細資訊，請參閱「*Oracle SuperCluster M7 Series Administration Guide*」。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **變更 `root` 密碼。**
   在本範例中，會將 *password* 取代為符合美國國防部密碼複雜性原則的密碼。

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

如需初次安裝及組態 ZFS 儲存設備的詳細資訊，請參閱「*Oracle ZFS Storage Appliance Installation Guide*」。請參閱「其他 ZFS 儲存設備資源」[79]。

預設公開的網路服務 (ZFS 儲存設備)

此表格列出 ZFS 儲存設備的公開預設網路服務。

服務	協定	連接埠	描述
SSH	TCP	22	由安全 Shell 服務使用，以便使用 CLI 對 ZFS 儲存設備進行管理存取。
PORTMAP	TCP/UDP	111	由遠端程序呼叫 (RPC) 連接埠對應常駐程式 (亦稱為 `rpcbind` 或 `portmap`) 使用。這項服務是支援 NFS 版本 3 的必備要素。
NTP	UDP	123	由整合的網路時間協定 (NTP) 服務使用 (僅限用戶端)，以便將本機系統時鐘與一或多個外部時間來源同步。
HTTPS (BUI)	TCP	215	由整合的 HTTPS 服務使用，以便使用瀏覽器介面透過加密的 (SSL/TLS) 通道對 ZFS 儲存設備進行管理存取。
遠端複製	TCP	216	由整合的遠端資料複製服務使用。遠端資料複製功能會複製並同步專案，然後通過加密的 (SSL/TLS) 通道在 ZFS 儲存設備之間共用專案。
NFS	TCP/UDP	2049 4045 依版本而定	由網路檔案系統 (NFS) 服務使用。NFS 提供網路檔案共用服務。實際的連接埠數目取決於使用之 NFS 協定的版本。NFS 版本 3 倚賴 RPC 連接埠對應常駐程式 (以上所列)，會動態配置連接埠來提供掛載、狀態、配額以及相關服務。NFS 版本 4 則只倚賴於 TCP/2049。NFS 鎖定服務使用 TCP/4045。
iSCSI / iSNS	TCP	3260	由 iSCSI 服務使用，此服務提供以 IP 為基礎的儲存網路協定來連結資料儲存設備。可以將 ZFS 儲存設備設定為與網路用戶端共用 iSCSI 裝置 (稱為 LUN)。
服務標記	TCP	6481	由 Oracle ServiceTag 服務使用。這是一種 Oracle 尋找協定，主要用於識別伺服器及協助進行服務要求。產品 (例如 Oracle Enterprise Manager Ops Center) 可以

服務	協定	連接埠	描述
			使用此服務來尋找 ZFS 儲存設備軟體，以及與其他 Oracle 自動服務解決方案整合。
NDMP	TCP	10000	由網路資料管理協定 (NDMP) 服務使用，此服務讓 ZFS 儲存設備能夠參與遠端協調備份。

ZFS 儲存設備還支援預設停用的其他各種不同服務，包括 `HTTP`、`FTP`、`SFTP`、`TFTP`、`WebDAV` 等等。安裝後若啟用這些服務，可能會公開其他網路連接埠。

強化 ZFS 儲存設備安全組態

以下主題描述如何強化 ZFS 儲存設備的安全組態：

- 「實作 Oracle ILOM 安全組態強化」[74]
- 「停用不需要的服務 (ZFS 儲存設備)」[74]
- 「停用動態路由」[75]
- 「限制遠端 `root` 使用安全 Shell 存取」[76]
- 「設定管理介面無活動逾時 (HTTPS)」[76]
- 「停用未核准的 SNMP 協定」[77]
- 「設定 SNMP 社群字串」[78]
- 「設定 SNMP 授權網路」[78]

▼ 實作 Oracle ILOM 安全組態強化

ZFS 儲存設備包含內嵌的 Oracle ILOM，此為產品的一部分。就像其他的 Oracle ILOM 實作，您可以實作一些安全相關組態變更，以增強裝置的預設安全組態。

- **執行「保護 Oracle ILOM 的安全」[33]中的程序，以保護 ZFS 儲存設備的 Oracle ILOM 介面。**

▼ 停用不需要的服務 (ZFS 儲存設備)

請停用平台上不是支援操作與管理需求所必要的任何服務。

ZFS 儲存設備預設會採用網路預設保護組態 (已經停用非必要的服務)。但是，依據您安全原則與需求的不同，有可能需要啟用或停用其他服務。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **顯示 ZFS 儲存設備支援的服務清單。**

   ```
   hostname:> configuration services
   ```

3. **判斷是否啟用指定的服務。**
   將 *servicename* 取代為步驟 2 中識別的服務名稱。

   ```
   hostname:> configuration services servicename get <status>
   ```

   服務狀態參數若傳回 `enabled` 值，就代表服務已啟用。例如：

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **將不再需要的服務停用。**
   將服務狀態設為停用。例如：

   ```
   hostname:> configuration services iscsi disable
   ```

▼ 停用動態路由

ZFS 儲存設備預設設定為執行動態路由協定。

將動態路由服務停用之前，請先確定 ZFS 儲存設備可直接連線至它必須通訊的任何網路，或者確定已將它設定為使用靜態路由或預設路由。必須執行此步驟，以確定停用動態路由之後不會發生連線中斷的情況。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **停用動態路由。**

   ```
   hostname:> configuration services dynrouting disable
   ```

3. **若要判斷動態路由是否啟用，請輸入：**

```
hostname:> configuration services dynrouting get <status>
```

▼ 限制遠端 root 使用安全 Shell 存取

ZFS 儲存設備預設設定為允許 root 帳號使用安全 Shell (SSH) 服務進行遠端管理存取。

您可以使用此程序來停用透過 SSH 進行的遠端 root 存取。

進行此組態變更之後，root 帳號就不能再使用 SSH 存取系統。但是，root 帳號可以使用 HTTPS 管理介面來存取本系統。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **停用遠端 root 存取。**

   ```
   hostname:> configuration services ssh set permit_root_login=false
   ```

3. **確認不再允許 root 帳號使用 SSH 存取系統。**

   ```
   hostname:> configuration services ssh get permit_root_login
   ```

4. **如果需要進行 SSH 管理存取，請至少建立一個非 root 帳號。**
   如需相關指示，請參閱 ZFS 儲存設備上執行之版本的「*Oracle ZFS Storage Appliance Administration Guide*」。請參閱「其他 ZFS 儲存設備資源」[79]。

▼ 設定管理介面無活動逾時 (HTTPS)

ZFS 儲存設備支援當管理階段作業在一段預先定義的時間 (以分鐘為單位) 後沒有活動的話，便會將其中斷連線並登出。瀏覽器使用者介面 (HTTPS) 預設會在 15 分鐘後將階段作業視為逾時。

注意 - ZFS 儲存設備的 SSH 指令行介面不提供強制無活動逾時的相等參數。

請使用下述程序將無活動逾時參數設為自訂的值。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **檢視瀏覽器介面目前的無活動逾時參數。**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **設定逾時參數。**
   以分鐘為單位指定 `session_timeout` 的值 (本範例為 10 分鐘)。

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **重複執行步驟 2 以驗證逾時參數。**

▼ 停用未核准的 SNMP 協定

ZFS 儲存設備預設啟用 SNMPv1 和 SNMPv2c。ZFS 儲存設備在所有支援的產品版本均提供 SNMPv1/v2c 支援。從版本 2013.1.2 開始，ZFS 儲存設備也支援 SNMPv3。

注意 - 版本 3 的 SNMP 協定導入以使用者為基礎的安全模型 (USM) 支援。這項功能將傳統的 SNMP 社群字串取代為能夠為其設定特定權限、認證、私密協定以及密碼的實際使用者帳號。ZFS 儲存設備預設並不包括整合之 (唯讀) USM 帳號的使用者名稱或密碼。基於安全理由，請依據部署、管理以及監督需求設定 USM 證明資料和協定。

除非必要，否則請確定將未使用或舊版的 SNMP 協定都停用。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **判斷裝置所使用的 SNMP 協定版本。**

```
hostname:> configuration services snmp get version
version = v2
```

3. **啟用使用 SNMPv3 (若有的話)。**
   SNMPv1/v2c 和 SNMPv3 不可同時使用，因此若啟用 SNMPv3，請將 SNMPv1/v2c 停用。

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **驗證 SNMP 版本。**

```
hostname:> configuration services snmp get version
```

```
version = v3
```

▼ 設定 SNMP 社群字串

只有當 ZFS 儲存設備設定為使用 SNMPv1 或 v2 時，才需要執行此工作。

由於 SNMP 經常用來監督裝置的狀況，因此請務必將裝置使用的預設 SNMP 社群字串變更為客戶定義值。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **變更 SNMP 社群字串。**
   在本範例中，會將 *string* 取代為符合美國國防部對於 SNMP 社群字串組成要求的值。

   ```
   hostname:> configuration services snmp set community=string
   community = value
   ```

3. **驗證 SNMP 社群字串。**

   ```
   hostname:> configuration services snmp get community
   ```

▼ 設定 SNMP 授權網路

只有當 ZFS 儲存設備設定為使用 SNMPv1 或 v2 時，才需要執行此工作。

為了將揭露的系統組態資訊減至最低，請只接受已核准之網路或主機來源的 SNMP 查詢。

1. **登入 ZFS 儲存設備。**
   請參閱「登入 ZFS 儲存設備」[71]。

2. **設定 SNMP 授權網路參數。**

   ```
   hostname:> configuration services snmp set network=127.0.0.1/8
   network = 127.0.0.1/8
   ```

3. **檢查 SNMP 授權網路參數的值。**
   在本範例中，會將網路參數設為 `127.0.0.1/8`，以有效地攔阻所有透過網路的 SNMP 查詢。這個值必須視需要調整，以允許核准的主機和網路。

值若為 `0.0.0.0/0`，代表允許來自任何網路位置的查詢。

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

▼ 限制管理網路存取

除了這些安全強化程序之外，還必須將 ZFS 儲存設備公開的管理介面部署在專用的獨立管理網路上。此步驟可協助讓 ZFS 儲存設備避開未經授權或未預期的管理網路流量。您必須將存取權只授予需要此層次存取的管理員，以嚴格控制對管理網路的存取。

甚至可以進一步設定讓 ZFS 儲存設備啟用或停用特定網路介面的管理存取。您可以使用以下程序實作這項變更。

1. **登入 ZFS 儲存設備。**

   請參閱「登入 ZFS 儲存設備」[71]。

2. **設定管理網路介面。**

   在本範例中，會將 *interface* 值取代為此設定適用之實際網路介面的名稱。

   ```
   hostname:> configuration net interfaces select interface set admin=false
   ```

其他 ZFS 儲存設備資源

如需 ZFS 儲存設備的其他安全準則，請參閱 ZFS 儲存設備上執行之版本的安全指南。請參閱「判斷 ZFS 儲存設備軟體版本」[72]。

這些指南提供產品之安全特性、功能以及組態選項的其他資訊：

- *Oracle ZFS Storage Appliance* 發行安全指南 (版本 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Oracle ZFS Storage Appliance* 發行安全指南 (版本 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Oracle ZFS Storage Appliance* 發行安全指南 (版本 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

保護 Exadata Storage Server 的安全

Exadata Storage Server (儲存體伺服器) 是 SuperCluster 的儲存體建置區塊。每一台儲存體伺服器於出廠時都已預先安裝並整合為 SuperCluster M7 的一部分，包含所有必要的運算、儲存和軟體元件。

注意 - 您只能透過套用核准的方法、修補程式或更新，對組態進行變更。儲存體伺服器軟體無法以任何其他方式改變。

SuperCluster M7 至少要有三台儲存體伺服器。額外的儲存體伺服器可安裝在主要的 SuperCluster 機架或選擇性的擴充機架中。您必須要保護每台儲存體伺服器的安全。

以下主題描述如何保護儲存體伺服器：

▼ 登入儲存體伺服器作業系統

- **在管理網路上，以 `celladmin` 的身分登入其中一台儲存體伺服器。**
  如需預設密碼，請參閱「預設帳號和密碼」[81]。

```
# ssh celladmin@Storage_Server_IP_address
```

預設帳號和密碼

此表格列出儲存體伺服器的預設帳號和密碼。

帳號名稱	類型	預設密碼	描述
root	管理員	welcome1	用來存取儲存體伺服器作業系統，以執行一般管理動作和更新儲存體伺服器軟體。
celladmin	單元管理員	welcome	用來執行儲存體伺服器的設定和組態。此外，平台上的所有儲存體服務都使用此帳號來運作。
cellmonitor	監督	welcome	僅供監督使用。此帳號利用受限制的 Shell，確保儲存體伺服器上的組態和物件不會遭到此帳號修改。

▼ 變更儲存體伺服器的密碼

如需預設帳號和密碼的清單，請參閱「預設帳號和密碼」[81]。

注意 - 若是變更 Oracle Engineered Systems Hardware Manager 管理之任一 SuperCluster 元件 (例如 Exadata Storage Server 作業系統) 的密碼，您必須同時在 Oracle Engineered Systems Hardware Manager 更新該密碼。如需詳細資訊，請參閱「*Oracle SuperCluster M7 Series Administration Guide*」。

---

1. **以 `celladmin` 的身分登入儲存體伺服器。**

   請參閱「登入儲存體伺服器作業系統」[81]。

2. **使用下列其中一種方法變更預設密碼。**

   - **在您登入的伺服器上變更帳號的密碼。**

     ```
     # passwd account_name
     ```

   - **變更所有儲存體伺服器之間使用的帳號密碼。**

     `cell_group` 是一個純文字檔案，列出所有儲存體伺服器的主機名稱 (每一行一部主機)。

     在本範例中，請取代以下的指令行項目：

     - *new_password* – 取代為符合網站原則的新密碼。
     - *account_name* – 取代為 Oracle Linux 帳號的名稱。

     ```
     # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
     ```

▼ 判斷 Exadata Storage Server 軟體版本

1. **登入其中一台儲存體伺服器。**

請參閱「登入儲存體伺服器作業系統」[81]。

2. **輸入這個指令。**

   在本範例中，儲存體伺服器軟體版本為 12.1.2.1.1.150316.2。

```
# imageinfo -ver
12.1.2.1.1.150316.2
```

   若要更新軟體的版本，請從 My Oracle Support (網址為 `https://support.oracle.com`) 安裝所提供的最新版 SuperCluster Quarterly Full Stack Download Patch。

注意 - 就 SuperCluster 而言，額外的限制可能限縮能夠使用的軟體版本和這些版本的更新方式。若出現此類情況，請洽詢您的 Oracle 服務人員。

預設公開的網路服務 (儲存體伺服器)

服務名稱	協定	連接埠	描述
SSH	TCP	22	由整合至儲存體伺服器軟體的安全 Shell 服務使用，可透過 CLI 對系統進行管理存取。 安全 Shell 伺服器預設會設定為只回應管理網路 (NET 0) 和 IB 網路 (BONDIB0) 上的連線要求。

儲存體伺服器也會透過遠端直接記憶體存取 (RDMA) 介面，使用 Reliable Datagram Socket (RDSv3) 協定在 SuperCluster 上與 Oracle 資料庫網域進行通訊。這個點對點通訊不會使用 TCP/IP，而且限制為在 SuperCluster 上的 Oracle 資料庫網域和儲存體伺服器兩者所在的內部 IB 網路分割區。

強化儲存體伺服器安全組態

注意 - 儲存體伺服器產品中包括內嵌的 Oracle ILOM。就像其他的 Oracle ILOM 實作，您可以實作一些安全相關組態變更，以增強裝置的預設安全組態。如需詳細資訊，請參閱「保護 Oracle ILOM 的安全」[33]。

以下主題描述如何強化儲存體伺服器的安全：

- 「安全組態限制」[84]
- 「使用 `host_access_control` 顯示可用的安全組態」[84]

安全組態限制

host_access_control 公用程式是在儲存體伺服器上實作安全組態唯一允許和支援的方法。根據 Oracle Support 注意事項 1068804.1，您不得手動變更這些裝置的組態。而且在使用此工具之前，您必須先從 Oracle SuperCluster Support 取得明確的核准，才能變更其儲存體伺服器的安全組態。若要取得此項核准，請向 Oracle Support 提出服務要求。

自 Exadata 軟體版本 11.2.3.3.0 起的 host_access_control 指令，可用來實作有限的存取權和安全組態設定值：

- 限制遠端 root 存取。
- 限制網路存取特定帳號。
- 實作密碼時效和複雜性原則。
- 實作登入警告標題。
- 定義帳號鎖定和階段作業逾時原則。

▼ 使用 host_access_control 顯示可用的安全組態

若要查看 host_access_control 公用程式提供的功能，請執行下列步驟。

1. **登入儲存體伺服器作業系統。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **(選擇性) 顯示 host_access_control 說明以瞭解詳細資訊。**

```
# /opt/oracle.cellos/host_access_control --help
```

▼ 設定系統啟動載入器密碼

您可以設定儲存體伺服器在管理員嘗試存取啟動載入器 (GRUB) 編輯器或指令介面時，一律要求輸入系統啟動載入器密碼。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **設定系統啟動載入器密碼。**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **驗證設定。**
   若指令傳回類似本範例的值，則表示已安裝啟動載入器密碼。

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

▼ 停用 Oracle ILOM 系統主控台存取

每一台儲存體伺服器都含有內嵌的 Oracle ILOM 以便進行遠端監督和管理。Oracle ILOM 也可在遠端存取儲存體伺服器系統主控台。

若您想要透過 Oracle ILOM 停用儲存體伺服器的存取，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **停用 Oracle ILOM 系統主控台存取。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **驗證設定。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

▼ 限制遠端 root 使用 SSH 存取

預設允許 root 使用者遠端存取每一台儲存體伺服器。

1. **以 celladmin 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **停用遠端 root 透過 SSH 存取。**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **驗證設定。**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

▼ 設定系統帳號鎖定

儲存體伺服器的預設設定，會在連續嘗試五次失敗的驗證後鎖定系統帳號。

若要變更此臨界值，請執行此程序。

1. **以 celladmin 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **變更臨界值。**
   若要符合美國國防部的安全要求，請將值指定為 3。如有必要，請將該值取代為符合您當地網站原則的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **驗證設定。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

▼ 設定密碼複雜性規則

儲存體伺服器預設不會實作任何管控系統帳號密碼複雜性的重要限制。

1. **以 celladmin 的身分登入儲存體伺服器。**

請參閱「登入儲存體伺服器作業系統」[81]。

2. **定義密碼複雜性原則。**
語法：

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

將 *N0,N1,N2,N3,N4* 取代為以逗號分隔的五個值。這五個值一起設定了實際的系統密碼複雜性原則。以下是這些值 (`passwdqc.conf(5)` 線上手冊也會列出)：

- *N0* –用於只包含一種字元類別 (數字、小寫字元、大寫字元和特殊字元) 的密碼。因為簡單的密碼不安全，所以此參數通常會設定為 `disabled`。
- *N1* –用於包含兩種不符合密碼詞組要求之字元類別的密碼。要套用此規則，密碼長度至少必須為 N1 個字元。
- *N2* –用於包含密碼詞組的密碼。要套用此規則，密碼長度至少必須為 N2 個字元，而且必須符合密碼詞組要求。
- *N3* –用於至少包含三種字元類別的密碼。要套用此規則，密碼長度至少必須為 N3 個字元。
- *N4* –用於至少包含四種字元類別的密碼。要套用此規則，密碼長度至少必須為 *N4* 個字元。

若要符合美國國防部的安全要求，請將 *N0,N1,N2,N3,N4* 參數設定為 `disabled,disabled,disabled,disabled,15`。這會確保只接受包含四種字元類別 (大寫、小寫、數字和特殊字元) 的密碼，而且長度至少為 15 個字元。

注意 - 計算字元類別數目時，不會計入密碼開頭的大寫字母和密碼結尾的數字。

例如，若要設定符合美國國防部要求的密碼複雜性，請輸入：

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **驗證此設定目前的狀態。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

▼ 設定密碼歷史記錄原則

儲存體伺服器預設會定義避免使用者重複使用其前十 (10) 組密碼的密碼歷史記錄原則。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢視目前的設定。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **變更密碼歷史記錄。**

   若要符合美國國防部和 PCI-DSS 的安全要求，請將密碼歷史記錄原則指定為 5。這會確保帳號無法重複使用指派給帳號的任何前五組密碼。如有必要，請將該值取代為符合您當地網站原則的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **若要驗證設定，請重複執行步驟 2。**

▼ 設定失敗驗證鎖定延遲

儲存體伺服器預設會實作一項原則：在系統帳號任一次失敗驗證之後，將該帳號鎖定 10 分鐘。

若要變更此臨界值，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**

   請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢視目前的設定。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **變更臨界值。**

   若要符合美國國防部的安全要求，請將值設定為 4 (秒)。如有必要，請將該值取代為符合您當地網站原則的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **若要驗證設定，請重複執行步驟 2。**

▼ 設定密碼時效控制原則

儲存體伺服器支援各種密碼時效控制，包括使用參數控制密碼使用天數上限、密碼變更之間的天數下限，以及預先警告使用者密碼到期的天數。

若要符合美國國防部安全規範和 PCI-DSS 的要求，請使用此表格中的美國國防部值。

原則	Oracle 預設值	美國國防部值
密碼使用期上限	90 天	60 天
密碼使用期下限	1 天	1 天
密碼長度下限	8 個字元	15 個字元
密碼到期警告	7 天	7 天

若要變更以上任何參數，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢視目前的設定值。**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **根據您的網站密碼原則設定這些原則。**

   - **若要變更密碼使用期上限參數，請輸入：**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

   - **若要變更密碼使用期下限參數，請輸入：**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

   - **若要變更密碼長度下限參數，請輸入：**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

   - **若要變更密碼到期警告參數，請輸入：**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **若要驗證設定值，請重複執行步驟 2。**

▼ 設定管理介面無活動逾時 (登入 Shell)

儲存體伺服器支援終止超過預先定義秒數而無活動之管理階段作業的功能。

若要定義系統帳號登入 Shell 的管理介面無活動逾時，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢視目前的設定。**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **定義管理介面無活動逾時。**
   若要符合美國國防部安全規範和 PCI-DSS 的要求，請將值指定為 `900` (秒)。如有必要，請將該值取代為符合您當地網站原則的值。

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **若要驗證設定，請重複執行步驟 2。**

▼ 設定管理介面無活動逾時 (安全 Shell)

儲存體伺服器支援終止超過預先定義秒數而無活動之管理 SSH 階段作業的功能。

若要定義 SSH 階段作業的管理介面無活動逾時，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢視目前的設定。**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

3. **定義 SSH 階段作業的管理介面無活動逾時。**
   若要符合美國國防部的安全要求，請將值指定為 `900` (秒)。如有必要，請將該值取代為符合當地網站原則的值。

```
# /opt/oracle.cellos/host_access_control idle-timeout --client 900
```

4. **若要驗證設定，請重複執行步驟 2。**

▼ 設定登入警告標題 (儲存體伺服器)

儲存體伺服器支援在使用者成功驗證進入系統之前顯示客戶專屬訊息的功能。

若要定義驗證前登入警告標題，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **判斷目前的設定。**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **建立一個包含核准登入警告標題訊息的文字檔。**

4. **定義驗證前登入警告標題。**
   若要符合美國國防部的安全要求，請將 *filename* 取代為包含核准登入警告標題訊息的檔案路徑和名稱。

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **若要驗證設定，請重複執行步驟 2。**

限制遠端網路存取

您可以實作篩選規則集，限制內送的遠端網路存取儲存體伺服器。您也可以定義自訂的規則集來微調網路存取。

請使用下列程序限制遠端存取。

- 「儲存體伺服器管理網路隔離」[91]
- 「限制遠端網路存取」[92]

儲存體伺服器管理網路隔離

儲存體伺服器是部署在專用、隔離的管理網路中。這可協助儲存體伺服器避開未經授權或未預期的網路流量。存取權只能授予需要此存取層次的管理員，以嚴格控制對管理網路的存取。

▼ 限制遠端網路存取

儲存體伺服器上有幾種方式可以讓您限制遠端網路存取。您可以實作由上到下的篩選規則集 (透過定義使用者帳號和來源的存取權)，限制內送網路存取儲存體伺服器。您也可以根據美國國防部和 PCI-DSS 的要求，定義自訂的規則集以允許或拒絕存取。

注意 - 實作非預設原則時請小心，以確保不會中斷系統的存取。當您新增個別規則時，變更會立即生效。

若要實作規則集，請執行此程序。

1. **以 `celladmin` 的身分登入儲存體伺服器。**
   請參閱「登入儲存體伺服器作業系統」[81]。

2. **檢驗作用中的規則集。**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **將目前的規則集匯出成檔案，並另存成備份複本。**
   下列指令會將規則集匯出成 ASCII 文字檔：

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **根據您要用來建立規則集的方法，執行下列一或多個指令設定規則集：**

   - **若要實作可移除內送網路限制的開放規則集，請輸入：**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **若要實作只允許使用 SSH 內送存取的封閉規則集，請輸入：**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **若要修改現有的規則集，請輸入：**
     將目前的規則集匯出成 ASCII 文字檔：

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     使用編輯器編輯此文字檔以設定規則集。

     從文字檔匯入規則集，覆寫現有的規則集：

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

- **分別新增特定規則：**

  此方法根據下列參數包含允許和拒絕存取：

  - **使用者名稱** – 有效值包括關鍵字 `all`，或是一或多個有效的本機帳號使用者名稱。
  - **來源** – 有效值包括關鍵字 `all`，或是描述系統存取來源的個別項目，包括來自主控台、虛擬主控台、Oracle ILOM、IP 位址、網路位址、主機名稱或 DNS 網域。

  在以下範例中，當連線是從 `trustedhost.example.org` 主機起始，或從 `.trusted.domain.com` 網域內的任何主機起始時，授予 `celladmin` 使用者存取儲存體伺服器。

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

其他儲存體伺服器資源

請參閱「Exadata Database Machine Security Guide」，網址為 http://docs.oracle.com/cd/E50790_01/welcome.html。

保護 IB 和乙太網路交換器的安全

SuperCluster 使用的 Oracle Sun Data Center InfiniBand Switch 36 提供高效能、高可擴充的網路基礎，在所有內部元件提供完全備援的機板。

IB 交換器可連接運算伺服器、儲存單元和 ZFS 儲存設備。IB 交換器搭配內嵌的 Oracle ILOM，可提供進階的管理和監督功能。Oracle ILOM 尤其可以監督和控制使用者、硬體、服務、協定和其他組態參數。

SuperCluster M7 至少有兩台 IB 交換器，若安裝其他 IB 交換器，則可以符合更大組態的需求。您必須要保護每台 IB 交換器。

以下主題描述如何保護 SuperCluster M7 中的 IB 交換器：

▼ 登入 IB 交換器

以下工作描述如何登入交換器的 Oracle ILOM 介面，當中可執行主要的管理工作。

- **在管理網路上，以 `ilom-admin` 的身分登入 IB 交換器上的 Oracle ILOM。**
  如需預設密碼，請參閱「預設帳號和密碼 (IB 交換器)」[96]。

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ 判斷 IB 交換器韌體版本

若要運用最新的特色、功能和安全性增強功能，請確保已使用最新支援的韌體版本更新 IB 交換器。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**

   請參閱「登入 IB 交換器」[95]。

2. **顯示韌體版本。**

   在本範例中，IB 交換器韌體的版本為 `2.1.5-1`。

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

若要更新 IB 交換器韌體的版本，請從 My Oracle Support (網址為 `https://support.oracle.com`) 安裝所提供的最新版 SuperCluster Quarterly Full Stack Download Patch。

注意 - 就 SuperCluster M7 而言，額外的限制可能限縮能夠使用的 IB 交換器軟體版本。限制也會指定如何更新韌體。若出現此類情況，請洽詢您的 Oracle 服務人員。

預設帳號和密碼 (IB 交換器)

帳號名稱	類型	預設密碼	描述
`root`	管理員	`welcome1`	用來存取 IB 交換器作業系統。此帳號一般不會加以使用，而會改用 `ilom-admin`、`ilom-operator` 或客戶定義的帳號。
`ilom-admin`	管理員	`ilom-admin`	在內嵌的 Oracle ILOM 軟體上用來執行管理功能、執行軟體更新、設定使用者和服務，以及執行 IB 交換器診斷和結構管理功能。
`ilom-operator`	操作員	`ilom-operator`	僅用於 Oracle ILOM 監督和 IB 結構診斷功能。
`nm2user`	唯讀	`changeme`	此帳號只具備 IB 交換器指令行管理介面的唯讀權限。此帳號通常由 Oracle Enterprise Manager 使用，以便支援交換器硬體和軟體的監督功能。

▼ 變更 root 和 nm2user 的密碼

IB 交換器維護兩個位置的系統帳號。root 和 nm2user 帳號由交換器的底層作業系統設定和公開。這一層不支援新增、移除或變更帳號，但是您必須變更預設密碼。

如需其他帳號和密碼，請參閱「變更 IB 交換器密碼 (Oracle ILOM)」[97]。

IB 交換器沒有定義或強制執行密碼複雜性、時效、歷史記錄或其他規則的功能。您必須確保指派的密碼符合美國國防部的密碼複雜性要求，並且實作程序以確保依照美國國防部的原則更新密碼。

如需有關 IB 交換器帳號管理的詳細資訊，包括如何建立新帳號、指派權限給現有帳號或移除帳號，請參閱「*Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide*」和「*Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*」。請參閱「其他 IB 交換器資源」[103]。

注意 - 若是變更 Oracle Engineered Systems Hardware Manager 管理之任一 SuperCluster 元件 (例如 IB 交換器) 的密碼，您必須同時在 Oracle Engineered Systems Hardware Manager 更新該密碼。如需詳細資訊，請參閱「*Oracle SuperCluster M7 Series Administration Guide*」。

---

1. **以 root 的身分登入 IB 交換器。**

```
# ssh root@IB_Switch_IP_address
```

如需預設密碼，請參閱「預設帳號和密碼 (IB 交換器)」[96]。

2. **變更 root 密碼。**

```
$ passwd root
```

3. **變更 nm2user 密碼。**

```
$ passwd nm2user
```

▼ 變更 IB 交換器密碼 (Oracle ILOM)

IB 交換器維護兩個位置的系統帳號。本節說明如何在 IB 交換器的 Oracle ILOM 介面變更密碼。如需其他帳號和密碼，請參閱「變更 root 和 nm2user 的密碼」[97]。

預設的 IB 交換器帳號和所有客戶定義的帳號都是透過 IB 交換器上內嵌的 Oracle ILOM 管理。

若要檢視帳號和變更密碼，請執行此程序。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
   請參閱「登入 IB 交換器」[95]。
   如需預設密碼，請參閱「預設帳號和密碼 (IB 交換器)」[96]。

2. **在 IB 交換器上檢視設定的 Oracle ILOM 帳號。**

   ```
   -> show /SP/users
   ```

3. **變更 `ilom-admin` 帳號的密碼。**

   ```
   -> set /SP/users/ilom-admin password=password
   ```

IB 交換器網路隔離

IB 交換器的管理介面是部署在專用、隔離的管理網路中。這可讓 IB 交換器避開未經授權或未預期的網路流量。

存取權只能授予需要此存取層次的管理員，以嚴格控制對此管理網路的存取。

預設公開的網路服務 (IB 交換器)

服務名稱	協定	連接埠	描述
SSH	TCP	22	由整合的安全 Shell 服務使用，可使用 CLI 對 IB 交換器進行管理存取。
HTTP (BUI)	TCP	80	由整合的 HTTP 服務使用，可使用瀏覽器介面對 IB 交換器進行管理存取。TCP/80 通常用於純文字存取，但是 IB 交換器預設會自動將內送要求重新導向至此服務在 TCP/443 執行的安全版本。
NTP	UDP	123	由整合的網路時間協定 (NTP) 服務使用 (僅限用戶端)，用來將本機系統時鐘同步到一或多個外部時間來源。
SNMP	UDP	161	由整合的 SNMP 服務使用，提供管理介面監督 IB 交換器的狀況和監督收到的設陷通知。
HTTPS (BUI)	TCP	443	由整合的 HTTPS 服務使用，可使用瀏覽器介面透過加密的 (SSL/TLS) 通道對 IB 交換器進行管理存取。
IPMI	TCP	623	由整合的智慧平台管理介面 (IPMI) 服務使用，提供電腦介面供各種監督和管理功能使用。請不要停用此服務，因為 Oracle Enterprise Manager Ops Center 使用此服務來收集硬體庫存資料、現場可更換單元描述、硬體感應器資訊以及硬體元件狀態資訊。

服務名稱	協定	連接埠	描述
ServiceTag	TCP	6481	由 Oracle ServiceTag 服務使用。這是一種 Oracle 尋找協定，主要用於識別伺服器及協助進行服務要求。此服務由產品 (像是 Oracle Enterprise Manager Ops Center) 用來尋找 IB 交換器軟體，以及與其他 Oracle 自動服務解決方案整合。

強化 IB 交換器組態

以下主題描述如何透過各種組態設定值保護 IB 交換器。

▼ 停用不需要的服務 (IB 交換器)

請停用平台上不是支援操作與管理需求所必要的任何服務。IB 交換器預設會採用網路預設保護組態 (已經停用非必要的服務)。但是，依據客戶安全原則與需求的不同，有可能需要停用其他服務。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
   請參閱「登入 IB 交換器」[95]。

2. **判斷 IB 交換器支援的服務清單。**

   ```
   -> show /SP/services
   ```

3. **判斷是否啟用指定的服務。**
   將 *servicename* 取代為步驟 2 中的服務名稱。

   ```
   -> show /SP/services/servicename servicestate
   ```

   雖然大多數服務都能辨識和使用 `servicestate` 參數記錄服務為啟用或停用，但還是有少數服務 (例如 `servicetag`、`ssh`、`sso` 和 `wsman`) 使用稱為 `state` 的參數。無論實際使用的參數為何，若服務狀態參數傳回 `enabled` 值，就代表服務已啟用，如下列範例所示：

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled


-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **若要停用不再需要的服務，請將服務狀態設定為 `disabled`。**

```
-> set /SP/services/http servicestate=disabled
```

5. **判斷是否要停用下列任何服務。**

   根據使用的工具和方法，若不需要或不使用 HTTP 和 HTTPS 瀏覽器服務，就可以將其停用。輸入：

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

   - 瀏覽器管理介面 (HTTP、HTTPS)：
     -> **set /SP/services/http servicestate=disabled**
     -> **set /SP/services/http secureredirect=disabled**
     -> **set /SP/services/https servicestate=disabled**

▼ 設定 HTTP 重新導向至 HTTPS (IB 交換器)

IB 交換器預設會設定為將內送 HTTP 要求重新導向至 HTTPS 服務，以確保交換器和管理員之間的所有瀏覽器通訊都經過加密。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**

   請參閱「登入 IB 交換器」[95]。

2. **確認已啟用安全重新導向。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **若預設值已變更，您可以啟用安全重新導向。**

```
-> set /SP/services/http secureredirect=enabled
```

▼ 停用未核准的 SNMP 協定 (IB 交換器)

用來監督和管理 IB 交換器的 SNMP 服務預設會啟用 SNMPv1、SNMPv2c 和 SNMPv3。除非必要，否則請確定將舊版的 SNMP 協定維持停用。

注意 - 版本 3 的 SNMP 協定導入以使用者為基礎的安全模型 (USM) 支援。這項功能將傳統的 SNMP 社群字串取代為能夠為其設定特定權限、認證、私密協定以及密碼的實際使用者帳號。IB 交換器預設不會包含任何 USM 帳號。請根據您自己的部署、管理和監督需求，設定 SNMPv3 USM 帳號。

---

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
   請參閱「登入 IB 交換器」[95]。

2. **判斷每個 SNMP 協定的狀態。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **如有需要，請停用 SNMPv1 和 SNMPv2c。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

▼ 設定 SNMP 社群字串 (IB 交換器)

此工作只有當啟用 SNMPv1 或 SNMPv2c 且設定使用時才適用。

由於 SNMP 經常會用來監督裝置的狀況，因此請務必將裝置所使用的預設 SNMP 社群字串取代為客戶定義值。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
   請參閱「登入 IB 交換器」[95]。

2. **建立新的 SNMP 社群字串。**
   在本範例中，請取代指令行中的以下項目：

   - *string* – 取代為符合美國國防部有關 SNMP 社群字串組合要求的客戶定義值。
   - *access* – 根據這是唯讀或讀寫存取字串，取代為 `ro` 或 `rw`。

```
-> create /SP/services/snmp/communities/string permission=access
```

建立好新的社群字串之後，就必須移除預設的社群字串。

3. **移除預設的 SNMP 社群字串。**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **驗證 SNMP 社群字串。**

```
-> show /SP/services/snmp/communities
```

▼ 取代預設自行簽署的憑證 (IB 交換器)

IB 交換器使用自行簽署的憑證，以便立即可使用 HTTPS 協定。最好的作法是，將自行簽署的憑證取代為您環境中核准使用，並且由認可的憑證授權單位簽署的憑證。

IB 交換器支援各種可用來存取 SSL/TLS 憑證和私密金鑰的方法，包括 HTTPS、HTTP、SCP、FTP、TFTP 並且會直接將資訊貼入 Web 瀏覽器介面。如需詳細資訊，請參閱「*Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36 document*」(「其他 IB 交換器資源」[103])。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
請參閱「登入 IB 交換器」[95]。

2. **判斷 IB 交換器是否使用預設自行簽署的憑證。**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **安裝您組織的憑證。**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

▼ 設定管理 CLI 階段作業逾時 (IB 交換器)

IB 交換器支援中斷連線並登出超過預先定義分鐘數而無活動之管理 CLI 階段作業的功能。

CLI 預設會在 15 分鐘後逾時。

1. **以 `ilom-admin` 的身分登入 IB 交換器。**
   請參閱「登入 IB 交換器」[95]。

2. **檢查與 CLI 有關的無活動逾時參數。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **設定無活動逾時參數。**
   將 *n* 取代為以分鐘為單位的指定值。

```
-> set /SP/cli timeout=n
```

其他 IB 交換器資源

如需有關 IB 交換器管理和安全性程序的詳細資訊，請參閱 Sun Datacenter InfiniBand Switch 36 文件庫，網址為 http://docs.oracle.com/cd/E36265_01。

▼ 變更乙太網路交換器密碼

注意 - 若是變更 Oracle Engineered Systems Hardware Manager 管理之任一 SuperCluster 元件 (例如乙太網路交換器) 的密碼，您必須同時在 Oracle Engineered Systems Hardware Manager 更新該密碼。如需詳細資訊，請參閱「*Oracle SuperCluster M7 Series Administration Guide*」。

---

1. **將乙太網路交換器主控台的序列纜線連接到膝上型電腦或類似裝置。**
   預設的序列埠速度為 9600 傳輸速率、8 位元、無同位、1 停止位元且無交握。

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **將交換器設為啟用模式。**

```
sscsw-adm0> enable
```

3. **設定密碼。**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **儲存組態。**

```
sscsw-adm0# copy running-config startup-config
```

5. **結束階段作業。**

```
sscsw-adm0# exit
```

6. **將膝上型電腦與乙太網路交換器中斷連線。**

合規稽核

您可以使用 Oracle Solaris 合規公用程式，來評估和報告系統是否合乎已知的基準要求。

Oracle Solaris `compliance` 指令會對照基準要求，來驗證程式碼、檔案或指令輸出是否符合特定的規範要求。Oracle SuperCluster 目前支援兩種安全規範基準設定檔：

- **建議** – 以 Center of Internet Security 基準為基礎的設定檔。
- **PCI-DSS** – 驗證「支付卡產業資料安全標準 (PCI DSS)」規範要求的設定檔。

這些分析工具會對照合規要求來檢驗安全控制做法，且所產生的合規報告可節省大量稽核時間。此外，合規功能還提供含有每項安全檢查的說明及修正未通過檢查的步驟指南。指南可用於訓練用途和作為未來測試的準則。依照預設，在安裝時會建立每個安全設定檔的指南。SuperCluster Solaris 管理員可以新增或變更基準並建立新指南。

以下主題描述如何執行合規報告，並且描述 FIPS-140 規範：

- 「產生合規評估」[105]
- 「(選擇性) 使用 `cron` 工作執行合規報告」[107]
- 「符合 FIPS-140-2 等級 1 規範」[108]

▼ 產生合規評估

若要執行此工作，您必須受指派 Software Installation 權限設定檔才能在系統新增套裝軟體。您必須受指派管理權限，才能執行大多數的合規指令。

1. **請安裝合規套裝軟體。**

```
# pkg install compliance
```

此訊息表示已安裝此套裝軟體：

```
No updates necessary for this image.
```

如需詳細資訊，請參閱 `pkg(1)` 線上手冊。

注意 - 請在您計畫執行合規測試的每個區域中安裝此套裝軟體。

---

2. **列出可用的基準、設定檔和先前執行的任何評估。**

   此範例中有兩個基準。

   - **`pci-dss`** – 包含一個設定檔，稱為 `Solaris_PCI-DSS`
   - **`solaris`** – 包含兩個設定檔，分別是 `Baseliine` 與 `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **產生合規評估。**

   使用下列語法執行 `compliance` 指令：

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	指定特定的基準。如未指定，此值預設為 `solaris`。
`-p`	指定設定檔。設定檔名稱有大小寫之別。如未指定，此值會預設為第一個設定檔。

   範例：

   - 使用 `Recommended` 設定檔。

```
# compliance assess -b solaris -p Recommended
```

     此指令會在 `/var/share/compliance/assessments` 中建立一個目錄，其中包含三個檔案 (日誌檔、XML 檔案和 HTML 檔案) 的評估。
   - 使用 PCI-DSS 設定檔：

```
# compliance assess -b pci-dss
```

注意 - `pci-dss` 基準只有一個設定檔，因此指令行中不需要設定檔選項 (`-p`)。

4. **確認已建立合規檔案。**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

注意 - 如果您再次執行相同的 `compliance` 指令，這些檔案並不會被取代。在重複使用某個評估目錄之前，您必須先移除這些檔案。

5. **(選擇性) 建立自訂報告。**

您可以重複執行自訂報告。不過，您只能在原始目錄中執行一次評估。

在此範例中，-s 選項是用來選取報告中應顯示何種結果類型。

依照預設，除了 notselected 或 notapplicable 以外，報告中會顯示所有結果類型。結果類型是以逗號區隔清單的形式指定，以顯示預設值以外的結果。在個別的結果類型前面加上 - 可以將它們隱藏，而清單前面加上 = 則可明確指定應包含的結果類型。結果類型包含：pass、fixed、notchecked、notapplicable、notselected、informational、unknown、error 或 fail。

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

此指令會使用 HTML 格式，建立包含失敗和未選取之項目的報告。此報告是根據最近的評估所製作。

6. **檢視完整報告。**

   您可以在文字編輯器中檢視日誌檔、在瀏覽器中檢視 HTML 檔案，或是在 XML 檢視器中檢視 XML 檔案。例如，若要檢視前面步驟的自訂 HTML 報告，請輸入下列瀏覽器項目：

   file:///var/share/compliance/assessments/*filename_timestamp***/report_A.html**

7. **若有任何必須通過的安全性原則失敗，請加以修正。**

   如果修正包括重新啟動系統，請於再次執行評估之前重新啟動系統。

8. **重複進行評估，直到沒有發生任何失敗為止。**

▼ (選擇性) 使用 cron 工作執行合規報告

- **以超級使用者身分使用 crontab -e 指令將適當的項目新增到 crontab 檔案。**

  此清單提供 crontab 項目的範例：

  - 於上午 2:30 執行每日合規評估

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - 於每週日上午 1:15 執行每週合規評估

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - 於每個月 1 號上午 4:00 執行每月評估

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - 於每個月第一個週一上午 3:45 執行評估

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

符合 FIPS-140-2 等級 1 規範

Oracle Solaris 對於 SuperCluster 上代管的加密應用程式，使用符合 FIPS 140-2 等級 1 規範驗證的加密架構。Oracle Solaris 加密架構是 Oracle Solaris 的中央加密存放區，此架構提供兩個符合 FIPS 140 驗證的模組，這些模組都支援使用者空間和核心層次的處理作業。這些程式庫模組提供應用程式的加密、解密、雜湊、簽章產生和驗證、憑證產生和驗證以及訊息認證功能。呼叫這些模組的使用者層次應用程式會以 FIPS 140 模式執行。

除了 Oracle Solaris 加密架構外，隨附於 Oracle Solaris 的 OpenSSL 物件模組符合 FIPS 140-2 等級 1 規範驗證，可支援以安全 Shell 和 TLS 協定為基礎的應用程式加密。雲端服務提供者可選擇開啟用戶主機的 FIPS 140 相容模式。以 FIPS 140 相容模式執行時，Oracle Solaris 與 OpenSSL (兩者都是 FIPS 140-2 提供者) 可強制使用經 FIPS 140 驗證的加密演算法。

另請參閱「(如有需要) 啟用 FIPS-140 相容作業 (Oracle ILOM)」[34]。

此表格列出 SuperCluster M7 中 Oracle Solaris 支援的 FIPS 核准演算法。

金鑰或 CSP	**憑證編號**	
	v1.0	**v1.1**
對稱式金鑰		
AES：ECB、CBC、CFB-128、CCM、GMAC、GCM 及 CTR 模式適用於 128、192 及 256 位元金鑰大小	#2311	#2574
AES：XTS 模式適用於 256 與 512 位元金鑰大小	#2311	#2574
TripleDES：CBC 與 ECB 模式適用於金鑰選項 1	#1458	#1560
非對稱式金鑰		
RSA PKCS#1.5 簽章產生/驗證：1024、2048 位元 (搭配 SHA-1、SHA-256、SHA-384、SHA-512)	#1194	#1321
ECDSA 簽章產生/驗證：P-192、-224、-256、-384、-521；K-163、-233、-283、-409、-571；B-163、-233、-283、-409、-571	#376	#446
安全雜湊標準 (SHS)		
SHA-1、SHA-224、SHA-256、SHA-384、SHA-512	#1425	#1596
(金鑰) 雜湊式訊息認證		
HMAC SHA-1、HMAC SHA-224、HMAC SHA-256、HMAC SHA-384、HMAC SHA-512	#1425	#1596
亂數產生器		
swrand FIPS 186-2 亂數產生器	#1154	#1222
n2rng FIPS 186-2 亂數產生器	#1152	#1226

Oracle Solaris 提供兩種符合 FIPS 140-2 等級 1 規範驗證的加密演算法提供者。

- Oracle Solaris 的「加密架構」功能是 Oracle Solaris 系統的中央加密存放區，此架構提供兩種 FIPS 140 模組。userland 模組為使用者空間執行的應用程式提供加密，

kernel 模組為核心層次的處理作業提供加密。這些程式庫模組提供應用程式的加密、解密、雜湊、簽章產生和驗證、憑證產生和驗證以及訊息認證功能。呼叫這些模組的使用者層次應用程式會以 FIPS 140 模式執行，例如 `passwd` 指令與 IKEv2。核心層次用戶 (例如 Kerberos 與 IPsec) 會使用專屬 API 呼叫核心「加密架構」。

- OpenSSL 物件模組為 SSH 和 Web 應用程式提供加密。OpenSSL 是「安全通訊端層 (SSL)」與「傳輸層安全 (TLS)」協定的開放程式碼工具程式，並提供一個加密程式庫。在 Oracle Solaris 中，SSH 和 Apache Web Server 是 OpenSSL FIPS 140 模組的用戶。Oracle Solaris 在 Oracle Solaris 11.2 中隨附 FIPS 140 版的 OpenSSL，可供所有用戶使用，但 Oracle Solaris 11.1 隨附的版本僅供 Solaris SSH 使用。由於 FIPS 140-2 提供者模組會耗用大量 CPU，因此預設未啟用。若您為管理員，則必須負責以 FIPS 140 模式啟用提供者並設定用戶。

如需在 Oracle Solaris 上啟用 FIPS-140 提供者的詳細資訊，請參閱「保護 Oracle Solaris 11 作業系統安全」標題下名為「*Using a FIPS 140 Enabled System in Oracle Solaris 11.2*」的文件，網址為：`http://docs.oracle.com/cd/E36784_01`。

保護 SuperCluster M7 系列系統的安全

以下主題描述 SuperCluster M7 系列使用期間用於維護系統安全的功能。

管理 SuperCluster 安全

SuperCluster M7 採用許多產品的安全管理功能，這些產品包括 Oracle ILOM、Oracle Enterprise Manager Ops Center、Oracle Enterprise Manager 及 Oracle Identity Management Suite。以下各節有詳細的描述：

Oracle ILOM 的安全管理

Oracle ILOM 是內嵌在許多 SuperCluster M7 元件中的服務處理器。使用 Oracle ILOM 可執行下列頻外管理活動：

- 提供安全存取，以執行 SuperCluster 元件的 Lights Out 管理。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 RBAC 模型，以達到區隔工作的需求。指派個別使用者給只能執行有限功能的特定角色。
- 提供所有登入和組態變更的稽核記錄。每一筆稽核記錄項目都會列出使用者執行的動作和時戳。此功能可讓您偵測未經授權的活動或變更，並反向追查進行這些動作的特定使用者。

如需詳細資訊，請參閱 Oracle Integrated Lights Out Manager 文件，網址為：http://docs.oracle.com/en/hardware/?tab=4

Oracle Identity Management Suite

Oracle Identity Management Suite 可管理整個組織的使用者識別和帳號的點對點生命週期。此套件支援單一登入、Web 型存取控制、Web 服務安全、識別管理、強式認證及識別和存取管理。

Oracle Identity Management 不僅可集中管理 Oracle SuperCluster 上執行的應用程式及服務的識別和存取，也能集中管理所需的相關基礎架構及服務。

如需詳細資訊，請參閱 Oracle Identity Management 文件，網址為：

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager 是一個全面的金鑰管理系統 (KMS)，可簡化管理和監督用於保護靜態資訊之加密金鑰的工作。

Oracle Key Manager 支援企業級的環境，其極具可擴充性和可用性的架構可管理數千個裝置與數百萬個金鑰。此功能可在強化的作業環境上執行、強制執行金鑰管理和監督作業所需的強式存取控制和角色區隔，並選擇性支援 Oracle Sun Crypto Accelerator 6000 PCIe Card (一種符合 FIPS 140-2 評比的硬體安全模組) 中的安全金鑰儲存。

在 SuperCluster 的相關資訊環境中，Oracle Key Manager 可以授權、保護和管理下列機制的加密金鑰存取：Oracle StorageTek 加密磁帶機、使用通透的資料加密方式加密的 Oracle 資料庫和 Oracle Solaris 11 作業系統上提供的加密 ZFS 檔案系統。

如需詳細資訊，請參閱 Oracle Key Manager 文件，網址為：

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager 是 Oracle 服務人員專用的 BUI 機架層次硬體管理工具。如需詳細資訊，請參閱「*Oracle SuperCluster M7 Series Owner's Guide: Administration*」。

Oracle Engineered Systems Hardware Manager 包含兩組認證資訊：

- **SuperCluster M7 元件密碼**

  Oracle Engineered Systems Hardware Manager 可安全儲存所有 SuperCluster M7 硬體的所有原廠帳號密碼。此軟體會使用這些密碼來管理 SuperCluster M7 元件。

  當這些密碼變更時，您必須以新密碼更新 Oracle Engineered Systems Hardware Manager 應用程式。
- **本機認證**

  Oracle Engineered Systems Hardware Manager 有兩個本機使用者帳號。一個是客戶專用帳號，可讓客戶自訂 Oracle Engineered Systems Hardware Manager 以符合環境需求並管理服務帳號。另一個是 Oracle 服務人員專用帳號，可設定、支援和提供 SuperCluster M7 硬體服務。

Oracle Engineered Systems Hardware Manager 提供下列本機管理資源。

- **密碼原則** – 可依據您的公司原則設定應用程式密碼，確保密碼符合公司的標準。

  注意 - 關於密碼原則設定值的資訊，請洽詢您的公司安全人員。

- **憑證** – Oracle Engineered Systems Hardware Manager 使用憑證來保護電腦伺服器與 Oracle Engineered Systems Hardware Manager 伺服器及 BUI 之間的通訊安全。這些憑證是安裝時自動建立的，每個 SuperCluster 執行處理都有唯一的憑證，但可替換為客戶提供的憑證和金鑰。
- **連接埠** – 假如 Oracle Engineered Systems Hardware Manager 使用的網路連接埠和您的公司原則發生衝突，您可以自行進行設定。連接埠 8001 到 8004 (含) 已在使用中。

如需組態指示，請參閱「*Oracle SuperCluster M7 Series Owner's Guide: Administration*」。

Oracle Enterprise Manager

Oracle Enterprise Manager 套件是全面的整合式雲端管理解決方案，主要運用在應用程式、中介軟體、資料庫及實體和虛擬基礎架構的生命週期管理 (使用 Oracle Enterprise Manager Ops Center)。Oracle Enterprise Manager 提供下列管理技術：

- 支援詳細監督、事件通知、修正、變更管理、連續組態、合規管理及應用程式、中介軟體和資料庫的報告功能。
- 可讓您集中維護安全組態設定值和資料庫群組的存取控制與稽核原則。這些功能可以限定只有授權人員才能存取，以確保管理存取權合乎職責劃分、最低權限及歸責的規範要求。
- 支援使用多種方法的強式認證、精密地存取控制和全面性稽核，確保 SuperCluster 環境的管理可以透過安全的方式實行。

如需詳細資訊，請參閱 Oracle Enterprise Manager 文件，網址為：http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html

Oracle Enterprise Manager Ops Center (選擇性)

Oracle Enterprise Manager Ops Center 是一種選擇性技術，可用來管理 Oracle SuperCluster 的部分安全層面。

Oracle Enterprise Manager Ops Center 是 Oracle Enterprise Manager 套件的一部分，它是一種集中式硬體管理解決方案，可為伺服器、作業系統、韌體、虛擬機器、區域、儲存裝置及網路光纖提供單一管理介面。

您可以使用 Oracle Enterprise Manager Ops Center 指派大量實體和虛擬系統的管理存取權、監督管理員活動、偵測錯誤以及設定和管理警示。Oracle Enterprise Manager Ops Center 支援多樣化報告，可讓您對照已知的組態基準、修補程式等級和安全漏洞比較系統差異。

如需詳細資訊，請參閱 Oracle Enterprise Manager Ops Center 文件，網址為：http://docs.oracle.com/cd/E27363_01/index.htm

---

注意 - 舊版的 Oracle Enterprise Manager Ops Center 已裝有 Ops Center 軟體，可直接從 SuperCluster 系統執行。從 Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0) 版本開始，您必須在 SuperCluster 系統以外的系統上安裝和執行 Ops Center。

安全監督

無論是針對合規報告或未預期事件回應，監督與稽核都提供重要功能，讓您對 IT 環境能夠有更深入的瞭解。通常會根據環境的風險或重要性來決定所採用的監督與稽核程度。

SuperCluster M7 系列系統提供在伺服器、網路、資料庫和儲存裝置層級的全面性監督與稽核功能，可確保資訊的提供符合稽核與規範的要求。

以下各節描述工作負載和資料庫監督與稽核：

工作負載監督

Oracle Solaris 作業系統有一套全面性稽核設備，可監督管理動作、指令行的使用，甚至是個別的核心層次系統呼叫。該設備具有高度可設定性，可提供全域、每個區域甚至每個使用者的稽核原則。

當系統設定為使用 Oracle Solaris Zones 時，每個區域的稽核記錄都可儲存在全域區域中，以防止這些記錄被竄改。

Oracle Solaris 稽核可利用系統日誌 (`syslog`) 工具傳送稽核記錄到遠端收集站。許多商業性質的入侵偵測及防禦服務都可使用 Oracle Solaris 稽核記錄作為分析和報告時的額外輸入。

Oracle VM Server for SPARC 利用原生的 Oracle Solaris 稽核功能來記錄虛擬化事件和網域管理相關的動作和事件。

如需詳細資訊，請參閱「Oracle Solaris 安全性指導方針」中的「監視和維護 Oracle Solaris 安全性」小節，網址為：

`http://docs.oracle.com/cd/E26502_01`

資料庫活動的監督與稽核

Oracle 資料庫精密地稽核支援可讓您建立原則，以選擇性判斷產生稽核記錄的時機。此功能可讓您專注在其他資料庫活動上，並能減少通常與稽核活動關聯的超載情況。

Oracle Audit Vault and Database Firewall 能集中管理資料庫稽核設定值，並自動將稽核資料合併到安全的儲存區域。此軟體內建的報告功能可監督多種活動，包括授權的使用者活動和資料庫結構變更。Oracle Audit Vault and Database Firewall 產生的報告可讓您掌握各種應用程式和管理資料庫活動，並提供動作歸責所需的詳細資訊。

Oracle Audit Vault and Database Firewall 可主動偵測和警示可能與未授權的嘗試或濫用系統權限有關的活動。這些警示可包含系統和使用者定義的事件和狀況，例如建立授權的使用者帳號或修改包含機密資訊的表格。

Oracle Audit Vault and Database Firewall Remote Monitor 可提供即時的資料庫安全監督。此功能可查詢資料庫連線狀況以偵測惡意的流量，例如應用程式繞道、未授權的活動、SQL 資料隱碼攻擊和其他威脅等。此軟體使用準確的 SQL 文法，可協助您快速識別可疑的資料庫活動。

如需詳細資訊，請參閱 Oracle Audit Vault and Database Firewall 文件，網址為：http://docs.oracle.com/cd/E37100_01/index.htm

網路監督

依據安全準則設定網路之後，必須定期複查與維護。

請依照下列準則，確保系統本機和遠端存取的安全：

- 複查記錄以找出可能的未預期事件，然後依據您組織的安全原則加以歸檔。
- 定期複查用戶端存取網路，以確保主機和 Oracle ILOM 設定值安全無虞。

如需詳細資訊，請參閱 Oracle Solaris 作業系統的安全指南：

- Oracle Solaris 11 作業系統 – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 作業系統 – http://www.oracle.com/goto/Solaris10/docs

軟體和韌體更新

我們會在 QFSDP 中提供 SuperCluster M7 系列的系統更新。安裝 QFSDP 會同時更新所有元件。此做法會確保所有元件可在經過 Oracle 完整測試的軟體版本組合上繼續執行。

從 My Oracle Support 取得最新的 QFSDP，網址為：http://support.oracle.com

如需支援的軟體和韌體的詳細資訊，請參閱「*Oracle SuperCluster M7 Series Product Notes*」。MOS 注意事項 1605591.1 中提供存取「產品注意事項」的指示。

注意 - 只有在 Oracle Support 的建議下進行被動維護，以隔離方式升級、更新或修補個別的元件。

索引

P

R

S

T

Z