Oracle MiniCluster S7-2 安全指南

文件號碼： **E78275-02**
2016 年 10 月

文件號碼： E78275-02

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

本文件使用方式

- **簡介** – 提供規劃、設定以及維護 Oracle MiniCluster S7-2 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/minicluster-s7-2/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 MiniCluster S7-2 系統之安全環境的相關資訊。

本節涵蓋下列主題：

最低必要安全工作

MiniCluster 是一個工程系統，在出廠時即預設為高度安全系統，並提供下列安全特性：

- 預先配置所有虛擬機器 (VM) 的完全自動化安全控制。
- 預設會啟用加密，確保非使用中和傳輸中的資料安全。
- VM 會自動設定具有主機式防火牆的強化及最小化 OS。
- 存取控制需要以角色為基礎，並設定最低權限。
- 所有 VM 都會使用加密 ZFS 儲存體。
- 具有集中化金鑰管理設備，使用 PKCS#11 並支援 FIPS。
- 系統包含具有集中化稽核記錄的全面性稽核原則。
- 系統和所有 VM 都是設定成 PCI-DSS、CIS 等效或 DISA-STIG 安全設定檔。注意 – 最後一個設定檔目前在複查中。只在非生產環境中以實驗性質使用 DISA-STIG 設定檔。
- 具有方便檢視的規範儀表板可支援易於執行的規範基準。

在 MiniCluster 安裝之後，安全管理員立即會有兩個必要工作：

- 變更 Oracle ILOM root 密碼。請參閱「變更預設 Oracle ILOM `root` 密碼」[25]

此外，請複查本指南中的安全資訊，瞭解和確認 MiniCluster 安全功能。

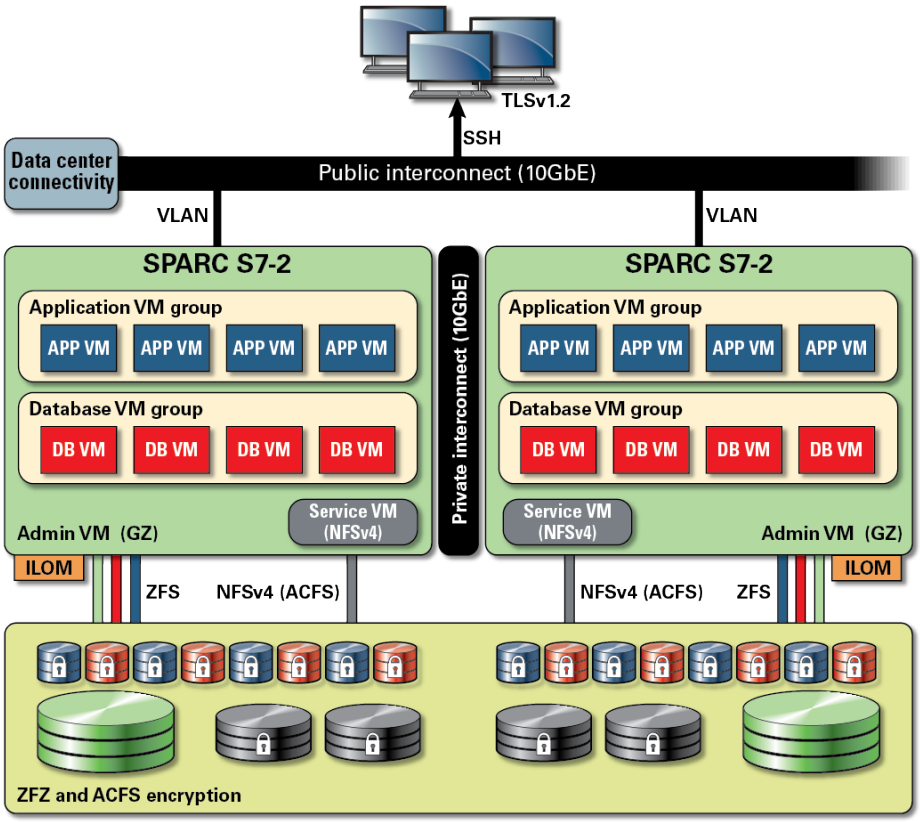
核心安全原則

MiniCluster 是進行應用程式和資料庫合併的安全雲端基礎架構平台，而且最適合提供以專用運算基礎架構即服務 (IaaS) 為基礎的雲端服務。它本身具有多用途工程系統，可合併 Oracle SPARC S7 處理器的運算功能、SPARC Solaris 的具效率虛擬化功能、與專用儲存體整合的 Oracle 資料庫的最佳化資料庫效能。此外還採用了 10 GbE 網路，讓用戶端存取在 MiniCluster 上執行的服務。最後，另一個 10 GbE 網路可提供管道，允許 SPARC S7 伺服器和代管應用程式上虛擬機器環境之間進行所有互通。

SPARC S7 處理器具備永遠開啟的硬體輔助加密功能，可協助 MiniCluster 代管實體利用非使用中、使用中和傳輸中高效能資料保護來保護其資訊。處理器也具備 Silicon Secured Memory 功能，可偵測和防止與記憶體資料毀損和記憶體擷取相關的攻擊，進而確保應用程式資料的完整性。

MiniCluster 預設會預先設定超過 250 個立即可用的安全控制，而停用非絕對必要的服務、連接埠和協定，並設定公開的服務僅接受信任連線，以減少系統的受攻擊面。

系統支援各種組態和部署選項。此圖說明可合併 Oracle 資料庫和應用程式工作負載的一般部署。



安全虛擬機器

有許多層次均提供 MiniCluster 運算節點內的安全。它開始於運算節點的安全驗證式開機，這是以隔離虛擬機器執行的強化和最小化 OS，可防止未授權的使用者和系統存取工作負載和資料。Oracle Solaris Zones 技術是用來當作 MiniCluster 中的虛擬機器，可代管隔離運算環境，並有效且有效率地將相同作業系統上執行的不同應用程式放在封閉測試環境中，保護它們不受其他虛擬機器中發生的非故意或惡意活動的影響。儘管是在相同的核心上執行，但是每個 Solaris 區域都有其專屬識別，以及資源、名稱空間和程序隔離。基本上，Solaris 區域會以 CPU 和記憶體覆蓋區小於「類型 1」Hypervisor 上執行的傳統虛擬機器，提供具有嚴格隔離和彈性資源控制的內建虛擬化。每個虛擬機器都會設定一個安全設定檔，以定義在安裝程序期間自動套用的一組全面性安全控制和原則。使用 ZFS 集區和資料集允許進一步調整儲存體，並將儲存體隔離成較小的虛擬機器單位，且可以有它們專屬的安全原則。

存取控制

為了保護應用程式資料、工作負載，以及用於執行的基礎架構，MiniCluster 提供給使用者和管理員許多全面性且具彈性的存取控制功能。MiniCluster 利用 Oracle Solaris 提供各種存取控制方法，來存取系統服務的使用者和應用程式。雖然傳統的使用者名稱和密碼組仍受廣泛使用，但是使用 Oracle Solaris 可插式認證模組 (PAM) 架構，可以輕鬆地整合更嚴密的認證方法，允許使用 LDAP、Kerberos 和公開金鑰認證。MiniCluster 運算環境的建置基礎為全面性以角色為基礎的存取控制 (RBAC) 設備，允許組織根據需求彈性地委派使用者和管理存取權。除了擁有功能強大的超級使用者，Oracle Solaris 中的 RBAC 功能還會啟用權責區分，並支援管理角色、授權、細微權限，以及統一用來將權限指派給使用者和管理員的權限設定檔。RBAC 與其他核心 Oracle Solaris 服務整合，包括 Oracle Solaris 服務管理設備 (SMF) 和虛擬機器，提供一致的架構來支援所有作業系統層次的存取控制需求。MiniCluster 利用 Oracle Solaris 的 RBAC 功能作為其存取控制架構的基礎，允許組織透過集中式授權單位管理、控制與稽核作業系統和虛擬化管理存取。所有重要作業都是使用多人授權工作流程所支援的權責區分原則來執行。系統需要兩位以上的人員核准每個安全機密作業。這些功能可以統一地用來高度確保使用者的識別以及重要業務運作的處理。

MiniCluster 系統中的所有裝置都可以透過下列方式限制服務的網路存取權：使用架構方法 (例如，網路隔離)，或使用封包篩選和 (或) 存取控制清單來限制實體與虛擬裝置之間的通訊，以及系統公開的服務。MiniCluster 不啟用任何網路服務來接受內送網路流量，只有安全 Shell (SSH) 除外，藉以部署預設保護態勢。其他已啟用的網路服務會在 Oracle Solaris 作業系統 (虛擬機器或區域) 中內部監聽要求。這確保所有網路服務會預設為停用，或所有網路服務都設為僅監聽本機系統通訊。組織可以根據需求自由地自訂此組態。MiniCluster 會使用 Oracle Solaris IP 篩選功能，預先配置網路和傳輸層 (狀態性) 封包篩選。IP 篩選提供各種主機式的網路功能，包括狀態性封包篩選、網路位址轉譯和連接埠位址轉譯。

資料保護

MiniCluster 中的 SPARC S7 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。

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 MiniCluster 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、

表格空間加密等作業，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。MiniCluster 支援使用 IPSec (IP 安全) 和 IKE (網際網路金鑰交換)，保護公用和專用網路上 VM 特定和 VM 之間通訊流的機密性和完整性。

在 MiniCluster 上，ZFS 資料集加密利用集中式 Oracle Solaris PKCS#11 金鑰存放區安全地保護包裝金鑰。若使用 Oracle Solaris PKCS#11 金鑰存放區，則會為所有加密作業自動使用 SPARC 硬體輔助加密加速功能。這可讓 Oracle 顯著提升 ZFS 資料集加密、Oracle 資料庫通透資料加密 (TDE)、表格空間加密、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)，以及重做記錄檔 (使用 Oracle Active Data Guard) 等相關加密與解密作業的效能。資料庫虛擬機器可以使用共用公事包方法，方法是利用 Oracle Solaris PKCS#11 金鑰存放區或在 ACFS 共用儲存體上建立目錄，以跨虛擬機器上的資料庫共用公事包。在每個運算節點上使用共用的集中式金鑰存放區，可讓系統在以 Oracle Grid 基礎架構為基礎的叢集化資料庫架構中更妥善地管理、維護和輪替 Oracle TDE 的金鑰，因為金鑰會在叢集的每個節點上同步化。MiniCluster 也可以安全地刪除虛擬機器和相關 ZFS 資料集，方法是在該 ZFS 資料集 (檔案系統/ZVOL) 層次實行加密原則和金鑰管理，以透過毀損金鑰來確保刪除的進行。

稽核和規範

MiniCluster 使用 Oracle Solaris 稽核子系統來收集、儲存以及處理稽核事件資訊。每個虛擬機器 (非全域區域) 都會產生每個 MiniCluster (全域區域) 稽核存放區本機儲存的稽核記錄。此方式可確保個別虛擬機器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 稽核功能會監督虛擬機器中的所有管理動作、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。設定為使用虛擬機器時，每個虛擬機器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。全域區域也會利用原生的 Oracle Solaris 稽核功能，來記錄虛擬化事件和 MiniCluster 管理相關的動作和事件。

MiniCluster 提供多個工具來評量和報告虛擬機器中的 Oracle Solaris 執行時期環境規範。規範公用程式是根據安全內容自動化協定 (Security Content Automation Protocol，SCAP) 實行。MiniCluster 支援兩種安全規範基準設定檔：

- **預設安全設定檔** – CIS 等效設定檔 (根據 Center of Internet Security 基準)，這較符合法規 (例如 HIPAA、FISMA、SOX 等) 所設定的安全規範需求。
- **PCI-DSS 設定檔** – 支付卡產業資料安全標準
- **DISA STIG 設定檔** – 國防資訊系統局 - 安全防護技術實施指南標準。此設定檔的建置基礎為「預設安全設定檔」，並導入其他 75 個安全控制、FIPS-140-2 加密且支援設定 S 密碼。注意 – 此設定檔目前在複查中。只在非生產環境中以實驗性質使用此設定檔。

MiniCluster 管理員可以依需求執行規範基準，以及確認環境的規範和異常。這些分析工具會將安全控制對應到產業標準所檢驗的規範需求。相關的規範報告則可以節省大量稽核時間和成本。

自 MiniCluster v.1.1.18 起，系統即包含下列稽核功能：

- **稽核者角色** – 若針對 MCMU 使用者指定此角色，使用者可以在 MCMU BUI 中存取稽核者的複查頁面。此使用者無法檢視或執行任何其他的 MiniCluster 管理工作。
- **稽核者複查頁面** – 為特殊的 MCMU BUI 頁面，只有具備 auditor 角色的使用者可以進行檢視。此頁面提供稽核集區狀態的存取權，並可根據每個區域產生所有使用者活動的稽核記錄。請參閱「產生稽核報表」[36]。

瞭解安全組態

下列主題描述 MiniCluster 安全控制：

內建安全設定檔

使用 MCMU BUI 或 CLI 執行 MiniCluster 初始化。在初始化期間，MCMU 需要安裝者選擇其中一個安全設定檔：

- **預設安全設定檔** – 滿足 Center for Internet Security (CIS) 和 Security Technical Implementation Guidelines (STIG) 評量所設定基準的可比較和對等需求。
- **PCI-DSS 設定檔** – 符合支付卡產業資料安全標準委員會 (Payment Card Industry Security Standards Council) 所定義的支付卡產業資料安全標準 (Payment Card Industry Data Security Standard，PCI DSS) 標準。
- **DISA STIG 設定檔** – 國防資訊系統局 - 安全防護技術實施指南標準。此設定檔的建置基礎為「預設安全設定檔」，並導入其他 75 個安全控制、FIPS-140-2 加密且支援設定 eeprom 密碼。注意 – 此設定檔目前在複查中。只在非生產環境中以實驗性質使用此設定檔。

根據選取的原則，MCMU 可使用 250 個以上的安全控制來設定全域區域和非全域區域。

在初始化之後，建立虛擬機器時，MCMU 需要為每個虛擬機器選取一個安全設定檔。根據安全需求，您可以在虛擬機器上混合使用安全設定檔。

▼ 確認 VM 安全設定檔 (CLI)

使用此程序即可確認或識別，針對區域和虛擬機器所設定的安全設定檔。

注意 - 您必須使用具有 `root` 角色的使用者帳號存取系統，才能執行此程序。

注意 - 若要識別指派給全域區域的安全設定檔，請在 MCMU BUI 中檢視 [System Setting] (系統設定) -> [User Input Summary] (使用者輸入摘要)。安全設定檔會顯示在頁面底端。

---

1. **以 `mcinstall` 登入全域區域。**
   如需如何存取系統的指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

2. **使用 `root` 角色。**
   範例：

   ```
   # su root
   ```

3. **決定有問題之 VM 的記錄檔名稱。**
   在此範例中，每個 VM 會有各自的記錄檔：

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **檢視驗證記錄檔。**
   檢視記錄檔的最後幾行。如果顯示 `(PCI-DSS)`，則 VM 的安全設定檔是 PCI-DSS。如果未列出任何設定檔，則 VM 的安全設定檔是「CIS 等效」。

   - 使用 PCI-DSS 設定檔之 VM 的最後 22 行範例：

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured

     (PCI-DSS) Checking audit configuration (user audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (non-attributable audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (audit_binfile plugin):
     Passed/Configured

     (PCI-DSS) Checking audit flags on root and tadmin roles:
     Passed/Configured

     Check if tenant-key exists in keystore:
     ```

```
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- 使用「CIS 等效」設定檔之 VM 的最後 22 行範例：

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

保護資料

下列主題描述 MiniCluster 資料保護技術：

使用 ZFS 資料集加密的資料保護

在 MiniCluster 中，會使用 ZFS 資料集加密自動設定非使用中資料保護。加密設定方式如下：

- 加密虛擬機器中所有的 ZFS 資料集，包括 root 和 swap 檔案系統。
- 加密全域區域中所有的 ZFS 資料集，但 root 和 swap 檔案系統除外。

您可以檢視加密金鑰來確認加密組態。請參閱「檢視 ZFS 資料集加密金鑰 (BUI)」[19]。

▼ 檢視 ZFS 資料集加密金鑰 (BUI)

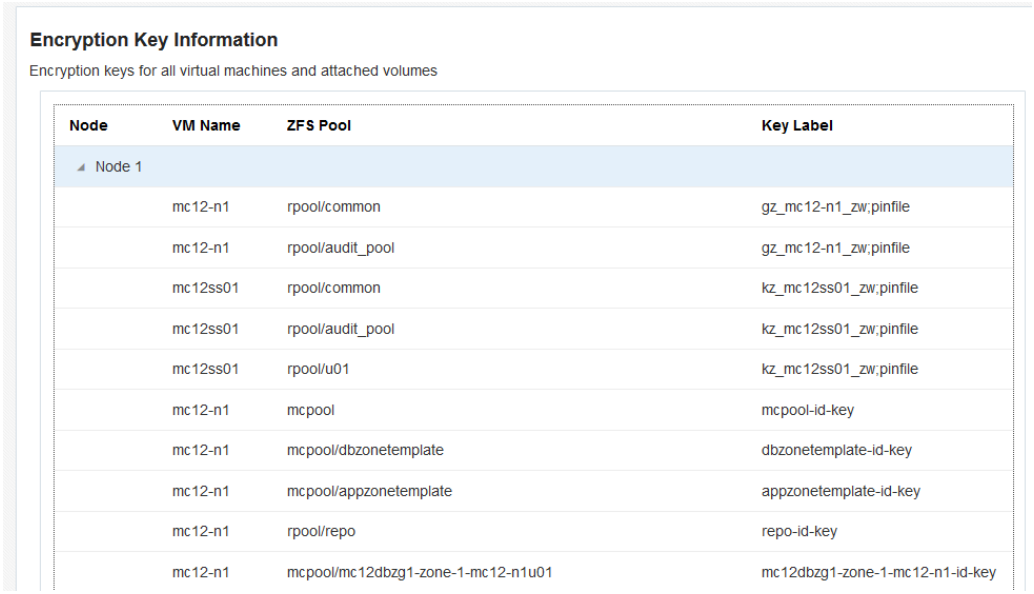
使用此程序，即可檢視加密金鑰詳細資訊。

1. **存取 MCMU BUI。**

   如需如何存取 MCMU BUI 的詳細資訊，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

2. **在導覽面板中，選取 [System Settings] (系統設定值) -> [Security] (安全)。**

按一下節點，以顯示詳細資訊。



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

安全 Shell 服務

MiniCluster 需要使用 SSH 網路協定讓您可以安全地登入 MiniCluster 運算節點 (全域區域) 和虛擬機器實例 (非全域區域)。

使用者第一次使用 SSH 登入時，系統會自動產生使用者新的 SSH 金鑰組。

▼ 變更 SSH 金鑰 (BUI)

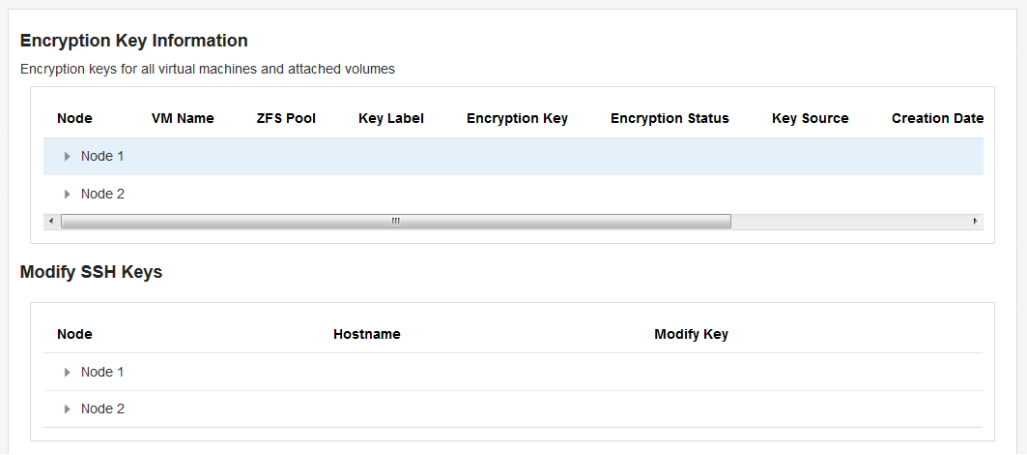
使用此程序，即可使用下列其中一個組態來變更區域或 VM 的 SSH 金鑰：

- 插入新的金鑰以授權無密碼 SSH – 需要您輸入 VM 使用者名稱、VM 機器名稱和 RSA 公開金鑰。
- 自動產生 VM 的新金鑰

注意 - 若要使用 MCMU CLI 執行此程序，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

---

1. **存取 MCMU BUI。**
2. **在導覽面板中，選取 [System Settings] (系統設定值) -> [Security] (安全)。**



3. **在 [Modify SSH Keys] (修改 SSH 金鑰) 面板中，按一下節點以展開顯示。**

4. **針對您計畫變更的 VM，按一下 [Select] (選取)。**
5. **從下拉功能表中選取選項，然後按 [Next] (下一步)。**
   選項如下：
   - 插入新的金鑰以授權無密碼 SSH

- 自動產生機器的新金鑰

6. **按 [Next] (下一步)。**

7. **如果您已選擇授權無密碼 SSH，請輸入此資訊，然後按 [Next] (下一步)：**

   - 機器的使用者名稱
   - 機器的主機名稱
   - 機器的 RSA 公開金鑰

8. **按一下 [Setup SSH] (設定 SSH)。**
   即會套用變更。

使用 IPsec 的安全通訊

建議使用 IPsec (IP 安全) 和 IKE (網際網路金鑰交換)，保護網路上區域之間的 IP 通訊，和 NFS 流量的機密性和完整性。建議使用 IPsec，因為它支援網路層對等認證、資料來源認證、資料機密性、資料完整性和重播保護。在 Oracle MiniCluster 平台上使用時，IPsec 和 IKE 可以自動利用硬體輔助的加密加速，進而將在此網路通道上使用加密法保護機密資訊流的效能影響降到最低。

▼ 設定 IPsec 和 IKE

必須先定義通訊對等之間所使用的特定主機名稱和 (或) IP 位址，才能設定 IPsec。

此程序中的範例，使用 IP 位址 10.1.1.1 和 10.1.1.2，指定單一用戶所操作的兩個 Solaris 非全域區域。這兩個位址之間的通訊，將會使用 IPsec 進行保護。此範例是從與 IP 位址 10.1.1.1 相關聯的非全域區域來進行。

使用下列步驟，即可在指定的 (虛擬機器) 非全域區域配對之間，設定與使用 IPsec 和 IKE：

1. **定義 IPsec 安全原則。**
   定義將在通訊區域配對之間強制執行的安全原則。

   在此範例中，將會加密 10.1.1.1 與 10.1.1.2 之間的所有網路通訊：

   ```
   {laddr 10.1.1.1 raddr 10.1.1.2}
   ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
   ```

2. **將原則儲存在 `/etc/inet/ipsecinit.conf` 檔案中。**

3. **確認 IPsec 原則的語法正確。**

   範例：

   ```
   # ipsecconf –c –f ipsecinit.conf
   ```

4. **設定網際網路金鑰交換 (IKE) 服務。**

   依照 `/etc/inet/ike/config` 檔案中的主機和演算法設定值設定服務。

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5

   auth_alg sha256 encr_alg aes } }
   ```

5. **設定預先共用金鑰。**

   必須先與兩個對等節點共用金鑰資料，讓它們彼此認證，才能啟用 IPsec。

   Oracle Solaris IKE 實作支援各種金鑰類型，包括預先共用金鑰和憑證。為求簡化，此範例使用 /`etc/inet/secret/ike.preshared` 檔案中所儲存的預先共用金鑰。不過，尋求使用更安全認證形式的組織也應該這麼做。

   編輯 /etc/inet/secret/ike.preshared 檔案，並輸入預先共用金鑰資訊。例如：

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **在兩個對等上啟用 IPsec 和 IKE 服務。**

   必須先在兩個通訊對等上啟用服務，才能進行加密通訊。

   範例：

   ```
   # svcadm enable svc:/network/ipsec/policy:default
   # svcadm enable svc:/network/ipsec/ike:default
   ```

控制存取

這些主題涵蓋 MiniCluster 中可用的存取控制功能：

▼ 變更預設 Oracle ILOM `root` 密碼

系統出貨時在兩個節點上都會指定 Oracle ILOM root 帳號的預設密碼。以便使用可預測的初始存取帳號來執行安裝程序。在安裝之後，請立即變更預設密碼，確保最佳安全性。

1. **以 `root` 身分，登入節點 1 上的 Oracle ILOM。**

   使用 `ssh` 指令連線至 Oracle ILOM。

   若要取得 Oracle ILOM 的主機名稱，請在公用程式 BUI 中，選取 [System Settings] (系統設定值) -> [System Information] (系統資訊)。主機名稱會列在 ILOM 欄下。

   語法：

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

   輸入預設 Oracle ILOM root 密碼：welcome1

2. **變更 Oracle ILOM `root` 密碼。**

   ```
   -> set /SP/users/root password
   ```

```
Enter new password: *********
Enter new password again: ***********
```

3. **重複步驟，變更節點 2 上的 Oracle ILOM `root` 密碼。**

4. **使用新的密碼更新 Oracle Engineered Systems Hardware Manager。**
   請參閱「「Update Component Passwords」 in *Oracle MiniCluster S7-2 Administration Guide*」。

▼ 設定 EEPROM 密碼

每個 MiniCluster 節點都具有 EEPROM (有時稱為 OpenBoot PROM)，這是一種低層級韌體，其中含有可加速系統開機的一些組態參數和驅動程式。EEPROM 密碼功能預設為停用。

在安全環境中，使用此程序可啟用密碼功能並設定密碼。密碼會自動啟用並套用至兩個節點。

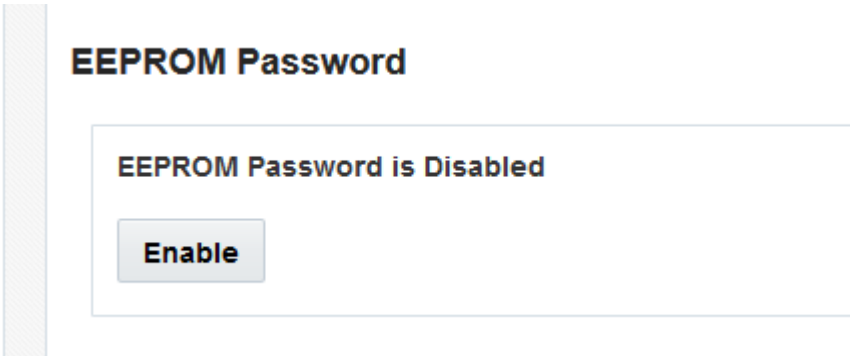
此程序會取代兩種設定密碼的舊方法：在 OpenBoot `ok` 提示或在 Oracle Solaris 透過 `eeprom` 指令。

注意 - 請務必記住密碼。如果忘記密碼，您必須聯絡支援服務才能再次讓您的系統可開機。

注意 - 此程序描述如何使用 MCMU BUI 來設定密碼。或者，您也可以使用 `mcmu security -e` 指令。

1. **以主要管理員身分 (例如 `mcinstall`) 登入 MCMU。**

2. **在導覽面板中，選取 [System Settings] (系統設定值) -> [Security] (安全)**



3. **執行下列其中一個動作：**

   - 啟用並設定密碼 – 按一下 [Enable] (啟用)，輸入兩次密碼後，再按一下 [Set Password] (設定密碼)。
   - 停用此功能 – 依序按一下 [Disable] (停用) 與 [Confirm] (確認)。
   - 變更現有的密碼 – 按一下 [Change Password] (變更密碼)，輸入兩次新密碼，再按一下 [Update] (更新)。

使用者啟動設定

在安裝 MiniCluster 期間，安裝程序需要您建立和註冊名稱為 `mcinstall` 的第一位 MCMU 使用者。系統將會收集使用者的相關資訊，包括電子郵件地址和電話號碼。`mcinstall` 使用者是第一個主要管理員帳號。在第一個 `mcinstall` 登入時，公用程式需要 `mcinstall` 根據與安全設定檔相關聯的 Oracle Solaris 密碼原則來建立新的密碼。

在註冊 `mcinstall` 使用者期間，您需要指定擔任 MCMU supervisor 的人員。supervisor 只能透過名稱和電子郵件地址進行識別。supervisor 不是 MCMU 使用者，因此沒有登入證明資料。

supervisor 和 mcinstall 使用者均與真實的人員名稱和有效的電子郵件地址相關聯。

啟動設定新的 MCMU 使用者時，每個使用者帳號都會被指派主要管理員或次要管理員的角色 (請參閱「以角色為基礎的存取控制 」[28])。啟用新的帳號之前，`mcinstall` 使用者和 supervisor 都必須透過他們在電子郵件中收到的 URL 來核准新的使用者帳號 (請參閱「MCMU 使用者核准程序」[27])。第一次登入時，會強制使用者設定符合 MCMU 密碼原則的密碼。請參閱「使用者認證和密碼原則」[30]。

MCMU 使用者核准程序

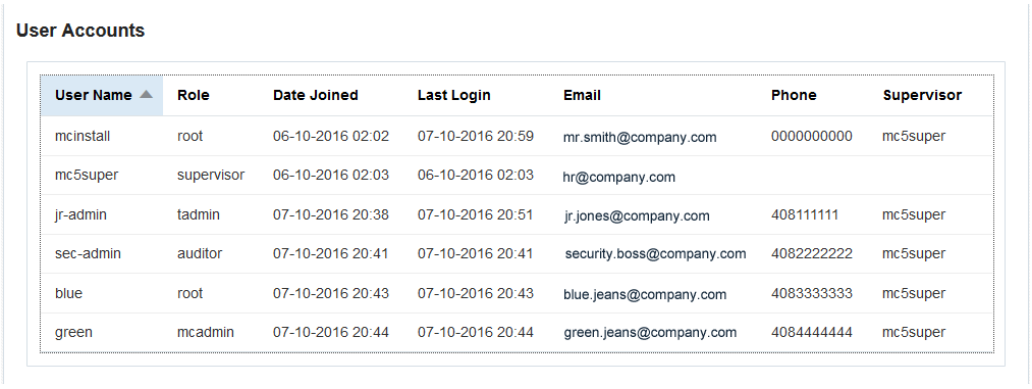
所有 MCMU 使用者帳號都需要 MCMU supervisor 和主要管理員兩人的核准。程序的運作方式如下：

1. 預期使用者 (或代表他們的 MCMU 管理員) 會存取 MCMU 註冊頁面，並提供這些必要詳細資訊：
   - MCMU 使用者名稱
   - 電子郵件地址
   - 全名
   - 電話號碼

- MCMU 角色

2. MCMU 會將一封要求核准或拒絕的電子郵件傳送給 MCMU supervisor 和主要管理員。電子郵件包括 MCMU 核准/拒絕功能的 URL，並包括唯一金鑰 ID。
3. supervisor 和主要管理員都核准帳號時，會啟用使用者帳號，而且 MCMU 會將確認帳號啟動的電子郵件傳送給新的使用者。使用者會接收到可透過 MCMU BUI 或 CLI 存取的 MCMU 帳號。使用者也會接收到 Oracle Solaris 使用者帳號。如果使用者存在於公司 LDAP 中，而且 MiniCluster 設定成 LDAP 用戶端，則使用者只能使用 LDAP 作為 Oracle Solaris 帳號。

所有註冊的使用者都會儲存在 MCMU 儲存區域中。MCMU 管理員可以透過檢視 MCMU [System Settings] (系統設定值) -> [User Accounts] (使用者帳號) 來確認使用者 (包括其角色和 supervisor)。範例：



User Accounts

User Name	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	408111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

本節中的後續主題描述如何執行這些工作。

以角色為基礎的存取控制

MiniCluster 中沒有 `root` 使用者。而是使用 root 角色，並且指派給註冊為主要管理員的 MCMU 使用者。

當您建立 MCMU 使用者時，會將下列其中一個角色指派給使用者：

- **主要管理員 (`root` 角色)** – `root` 角色會定義 MiniCluster 系統 (包括所有其運算節點、網路、資料庫和儲存體) 主要管理員的權限。具有 `root` 角色的使用者，可以執行所有安裝以及沒有任何限制的所有重要管理作業。主要管理員可以委派作業，以及核准新增和刪除使用者，包括新的主要和次要管理員。使用者必須使用其專屬證明資料進行登入。所有執行的動作和作業都是根據使用者 ID (而非角色 ID) 進行記錄和稽核。

- **次要管理員 (**`mcadmin` **角色)** – 此角色定義 MiniCluster 網域和非全域區域的次要管理員權限。此角色預設僅啟用 MCMU 的唯讀存取權。所有執行的動作和作業都是根據使用者 ID (而非角色 ID) 進行記錄和稽核。
- **用戶管理員 (**`tadmin` **角色)** – 此角色定義 MiniCluster VM 管理員的權限。此角色定義支援應用程式安裝和部署日常管理作業的 VM 管理員的權限。所有動作都是根據使用者 ID (而非角色 ID) 進行稽核。
- **稽核者 (**`auditor` **角色)** – 具備此角色的使用者僅具有 MCMU BUI [Audit Review] (稽核複查) 頁面的存取權，他們可以在此檢視稽核集區狀態及產生使用者活動報告。只有具備此角色的使用者可以存取 [Audit Review] (稽核複查) 頁面。稽核者無法存取 MCMU ([Audit] (稽核) 頁面除外)，也不能登入核心區域或 VM。

使用者帳號

MiniCluster 包括此表格中所列的使用者帳號。

使用者	密碼	角色	描述
`mcinstall`	密碼是在安裝期間所設定。它可以透過 MCMU 進行重設和變更。	`root`	安裝程式會要求您建立 `mcinstall` 作為 MCMU 主要管理員與建立密碼。此帳號會是 MCMU 的主要管理員。 此使用者帳號用於下列活動： ■ 執行 `installmc`，以在安裝期間執行系統初始化。 ■ 使用 MCMU BUI 和 `mcmu` CLI 來管理系統 (包括 VM)。 ■ 在應用程式 VM 上以及全域區域和核心區域中使用 `root` 角色 (`su` 到 root) 代表 superuser 權限。
MCMU supervisor – 在安裝期間決定的帳號名稱	N/A	N/A	在 MiniCluster 軟體中，supervisor 使用者只是使用者名稱和電子郵件地址。它不是登入證明資料。您可以使用此帳號提供 MCMU 使用者核准程序中的第二層。 每次建立新的 MCMU 使用者時，此使用者都會接收到電子郵件。supervisor 和主要管理員必須核准新的使用者，才會啟用使用者帳號。 您可以使用此帳號，將「主要管理員」以外的人員指派為 supervisor，以提供 MCMU 使用者核准程序中的第二層。
(選擇性) 用戶管理員 – 在使用者註冊期間決定的帳號名稱	初始登入時決定。	`tadmin`	此使用者只能在 VM 上執行所有安裝後的活動。 此使用者無法存取全域或核心區域，且不能執行 MCMU BUI 或 CLI。
(選擇性) 次要管理員 – 在使用者註冊期間決定的帳號名稱	初始登入時決定。	`mcadmin`	MCMU 使用者建立並指派為次要使用者後，即具有非全域區域的唯讀存取權。
`oracle`	密碼與 `mcinstall` 密碼相同。	`root`	此使用者帳號用於下列活動：

使用者	密碼	角色	描述
			■ 作為資料庫 VM 的初始登入帳號，透過此帳號，您可以使用資料庫、資料以及其他帳號 (依需要) 來設定資料庫 VM。 ■ 在資料庫 VM 上使用 root 角色 (`su` 到 root) 代表 superuser 權限。

第一次登入時使用的預設 MCMU 密碼是 `welcome1`。輸入 `welcome1` 之後，公用程式會強制使用者建立符合密碼原則的新密碼。請參閱「使用者認證和密碼原則」[30]。

所有 MCMU 使用者執行的所有動作都是根據使用者 ID 進行記錄。如需稽核報表的相關資訊，請參閱「稽核和規範報告」[35]。

注意 - MCMU 使用者帳號不會用於系統的例行使用，例如使用應用程式和資料庫。這些使用者帳號是透過 Oracle Solaris、應用程式、VM 上的資料庫以及網站的名稱服務進行管理。

使用者認證和密碼原則

MiniCluster 中啟動設定的所有使用者，都會被指派具有安全設定檔所強制執行的嚴格密碼原則和密碼加密的角色。

預設安全原則會建立這些 MCMU 密碼需求：

- 最少必須包含 14 個字元
- 最少必須有一個數值字元
- 最少必須有一個大寫英文字元
- 最少必須與前一個密碼有三個字元不同
- 不得符合前十個密碼

所有使用者都只會使用使用者的專屬密碼登入其 Oracle Solaris 帳號。

▼ 確認 Oracle Solaris 使用者角色

1. **登入 MiniCluster 全域區域，並使用 root 角色。**
   如需進一步詳細資訊，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

2. **確認可用角色清單。**

   ```
   # logins -r
   ```

3. **確認進行認證所需的使用者角色和密碼：**

   ```
   # grep root /etc/user_attr
   root::::audit_flags=lo\:no;type=role;roleauth=user
   ```

```
mcinstall::::auths=solaris.system.maintenance;roles=root
```

安全地刪除 VM

只有 MCMU 主要管理員才能刪除 VM 和 VM 群組。刪除 VM 元件時，會自動刪除對應的金鑰，並將電子郵件傳送給主要管理員。

若要確認此功能，請在刪除 VM 元件之前，以主要管理員身分登入 MCMU BUI，並檢視加密金鑰 ([System Settings] (系統設定值) -> [Security] (安全))。刪除 VM 元件，並重新檢視金鑰。不再顯示所刪除元件的 VM 和相關聯金鑰標籤。

▼ 確認主機式防火牆規則

所有運算環境 (包括全域區域、核心區域和非全域區域) 都會自動設定 IPFilter 防火牆。不需要手動作業。

若要確認 IPFilters 使用中，請執行下列步驟。

1. **以 `mcinstall` 登入節點 1 上的全域區域，並使用 `root` 角色。**
   如需 Oracle ILOM 登入指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **檢查 IPFilter 組態。**
   確定 `/etc/ipf/ipf.conf` 檔案中的規則符合下列畫面輸出。

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
```

```
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. **確認 IPF 服務已上線。**

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **確定不需要變更防火牆規則，即可存取資料庫和應用程式。**

▼ 確認驗證式開機環境

Oracle Solaris Verified Boot 是一個防止惡意軟體的整合性功能，可減少惡意元件或意外修改重要啟動與核心元件所導致的風險。這項功能會檢查韌體、開機系統和核心的原廠簽署加密簽章。

MiniCluster 全域區域預設便已設定 Oracle Solaris Verified Boot。如果您要確認系統是否已設定驗證式開機，請執行下列步驟。

1. **登入其中一個節點上的 Oracle ILOM。**
   如需 Oracle ILOM 登入指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

2. **檢查 Oracle ILOM 中的驗證式開機組態。**
   確定 `boot_policy` 設為 `warning`。

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **檢查驗證式開機原則設定。**

   確定 `module_policy` 設為 `enforce`。

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **啟動主機主控台以存取全域區域。**

   以 `mcinstall` 進行登入。

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

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **檢查全域區域中，是否有系統是以驗證式開機組態啟動的證據。**

   檢查 `messages` 檔案中是否有 `NOTICE: Verified boot enabled; policy=warning` 字串。

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

▼ 限制存取共用儲存體

MiniCluster 的儲存體陣列混合使用了 SSD 和 HDD。HDD 可設定為將共用儲存體提供給 VM。

MiniCluster 包括共用儲存體隔離功能 – 可讓共用儲存體的隔離機制僅套用至全域或核心區域的切換功能。這有助於將安全和啟用規範的 VM 群組環境隔離，避免與全域和核心區域共用檔案。這確保 VM 群組不再連接至 NFS 掛載並停用 NFS 服務。

為了確保高度安全的環境，請不要啟用共用儲存體供資料庫 VM 和應用程式 VM 使用。如果啟用共用儲存體，檔案系統必須以唯讀方式供 VM 存取。如需如何啟用或停用共用儲存體的指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」，網址為：`http://docs.oracle.com/cd/E69469_01`。

`/sharedstore` 目錄是共用儲存體的掛載點：

- **請務必根據安全需求，依照下列建議來設定共用儲存體：**
  - 確定資料庫 VM 和應用程式 VM 無法使用共用儲存體，或共用儲存體是唯讀的。
  - 在生產環境部署中，請確保無法透過公用網路存取或用戶端存取直接存取兩個核心區域。必須終止來自公用網路或用戶端存取的所有直接存取和共用儲存體服務的使用。如果虛擬機器需要透過 NFS 存取 `/sharedstore` 檔案系統，請確保其會透過 IPSEc/IKE 通道進行存取。

稽核和規範報告

以下主題描述 MiniCluster 中可用的稽核和規範報告功能：

▼ 確認稽核原則

稽核原則是在選取規範設定檔 (預設 CIS 等效或 PCI-DSS) 時，於安裝全域區域和非全域區域期間設定。

若要確認已啟用稽核原則，請執行下列步驟。

1. **以 `mcinstall` 身分登入全域區域，並使用 `root` 角色。**
   如需 Oracle ILOM 登入指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **確認稽核服務已上線。**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **確認稽核外掛程式已作用。**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **確認作用中稽核原則。**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **確認已擷取 `cusa` 稽核原則的所有角色。**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ 複查稽核記錄

1. **以 `mcinstall` 身分登入全域區域，並使用 `root` 角色。**
   如需 Oracle ILOM 登入指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **如所示使用 `auditreduce` 指令。**
   這是檢視稽核記錄的語法：

   `auditreduce -z` *vm_name audit_file_name* `| praudit -s`

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

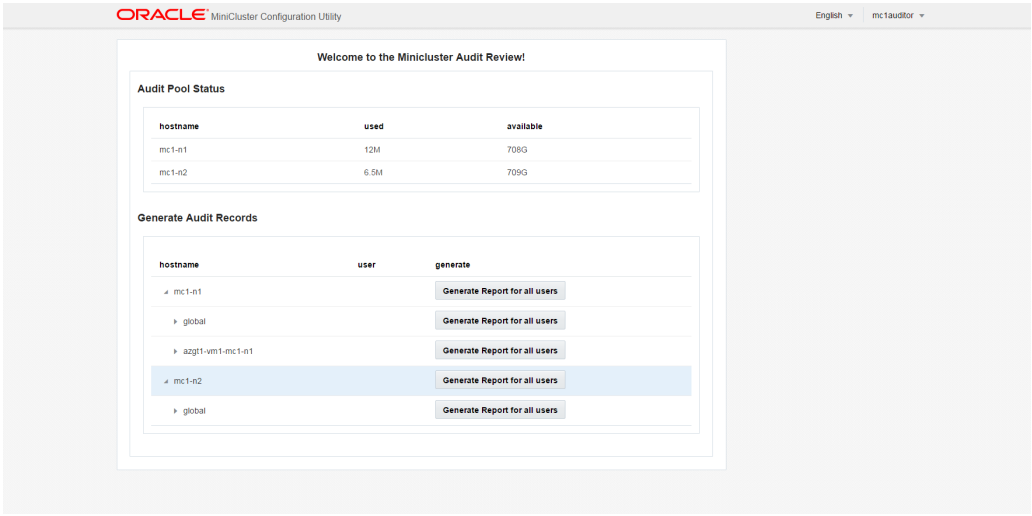
▼ 產生稽核報表

使用此程序可產生節點或個別 VM 及全域區域的稽核報表。

1. **以指派為 [Auditor] (稽核者) 角色的使用者身分登入 MCMU。**
   如需有關 MCMU 使用者與角色，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」，網址為：`http://docs.oracle.com/cd/E69469_01`。

2. **在導覽面板中，選取 [System Settings] (系統設定值) -> [Security] (安全)。**
   即會顯示 [Audit Review] (稽核複查) 頁面。

   注意 - 只有指派為 [Auditor] (稽核者) 角色的 MCMU 使用者可顯示此頁面。

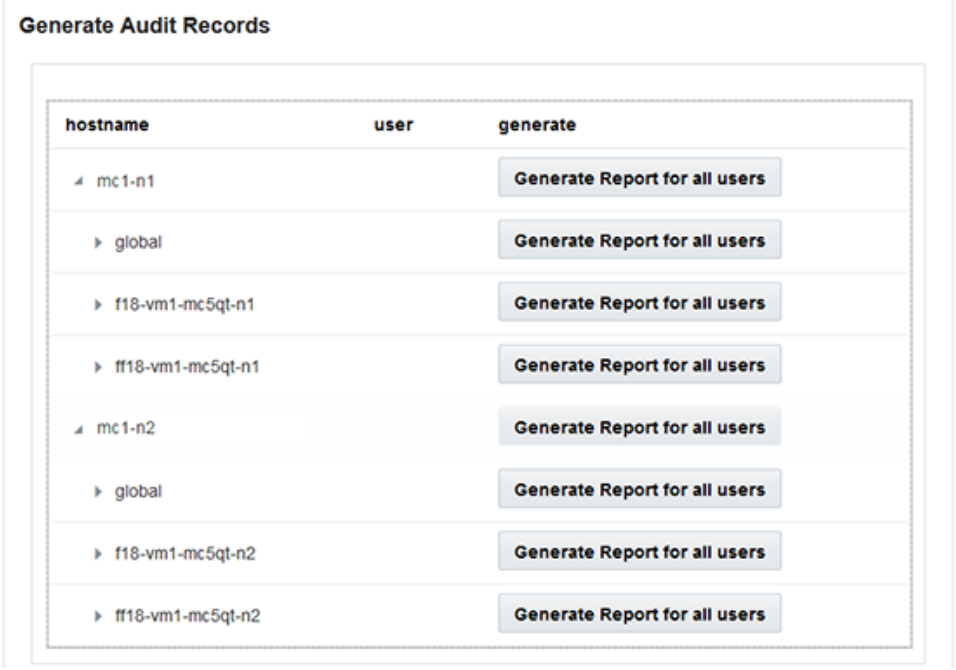


3. **查看「稽核集區狀態」小節。**
   本節列出每個節點上 [used] (已使用) 和 [available] (可使用) 的稽核集區空間大小。

4. **若要產生整個節點的報表，請按一下其中一個節點的 [Generate] (產生) 按鈕，並前往步驟 6**
   或者，您可以產生特定 VM 或區域的報表。請參閱步驟 5

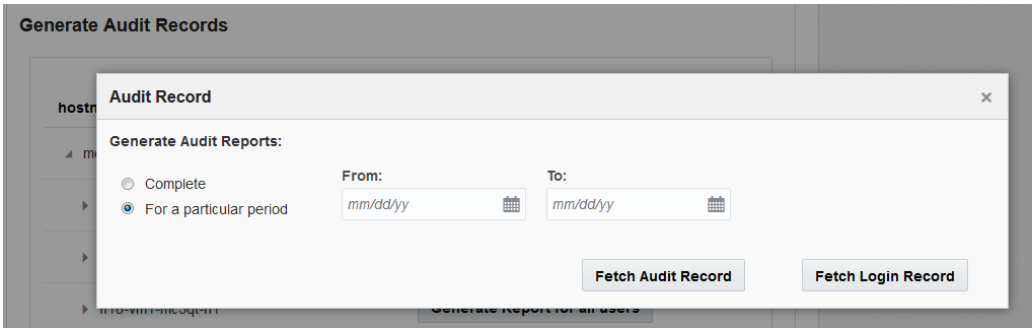
5. **若要產生特定 VM 或全域區域的報表，請執行下列步驟。**

a. 按一下節點旁的三角形即可展開檢視。



b. 針對 VM 或全域區域，請按一下 **[Generate Report for all users] (產生所有使用者的報表)**。

6. 在 **[Audit Record] (稽核記錄)** 對話方塊中，設定稽核記錄參數。



您可以使用以下選項：

- **Complete** (完整) – 如果您要報表包含所有稽核記錄，請選取此選項。
- **For a particular period** (針對特定期間) – 如果您要指定特定的期間，請選取此選項並輸入開始與結束日期。

7. **按一下其中一個擷取按鈕。**
   您可以使用以下選項：
   - **Fetch Audit Record** (擷取稽核記錄) – 產生完整的稽核記錄。
   - **Fetch Login Record** (擷取登入記錄) – 產生使用者活動，例如登入、登出和使用者動作。
8. **按一下 [Click Here] (按一下此處) 按鈕，然後選取 [Download XML File] (下載 XML 檔案)。**
   XML 檔案可匯入至 Oracle Audit Vault 之類的稽核分析應用程式。
9. **按一下 [Close] (關閉)。**

▼ (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。「*Oracle ILOM Security Guide*」的「Unsupported Features When FIPS Mode Is Enabled」小節涵蓋這些功能的清單。

另請參閱「符合 FIPS-140-2 等級 1 規範」[40]。

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，否則將會遺失這些組態變更。

1. **在管理網路上，登入 Oracle ILOM。**
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
```

符合 FIPS-140-2 等級 1 規範

Oracle Solaris 對於 MiniCluster 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)」[39]。

此表格列出 MiniCluster 上 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

金鑰或 CSP	憑證編號	
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」中名為「在 *Oracle Solaris 11.2* 使用啟用 *FIPS 140* 的系統」的文件，網址為：`http://docs.oracle.com/cd/E36784_01`。

評估安全規範

以下主題描述 MiniCluster 安全基準功能：

安全規範基準

安裝系統時，會選取安全設定檔 (PCI-DSS、CIS 等效和 DISA-STiG)，而且系統會自動設定成符合該安全設定檔。為了確保系統根據安全設定檔來繼續作業，MCMU 提供方法來執行安全基準以及存取基準報告。您可以使用 MCMU BUI 和 CLI 來管理基準。

執行安全基準的優點如下：

- 可讓您評估和評量資料庫和應用程式 VM 的目前安全狀態。
- 安全規範測試會根據安裝期間所設定的安全等級來支援 PCI-DSS、CIS 等效標準 (預設) 以及 DISA-STiG。
- 安全規範測試會在系統啟動時自動執行，而且可以依需求或排定的間隔執行。
- 只有 MCMU 主要管理員才能從 MCMU BUI 輕鬆地存取規範評分和報告。
- 規範報告提供補救建議。

注意 - DISA-STIG 設定檔目前在複查中。只在非生產環境中以實驗性質使用此設定檔。

▼ 排定安全規範基準 (BUI)

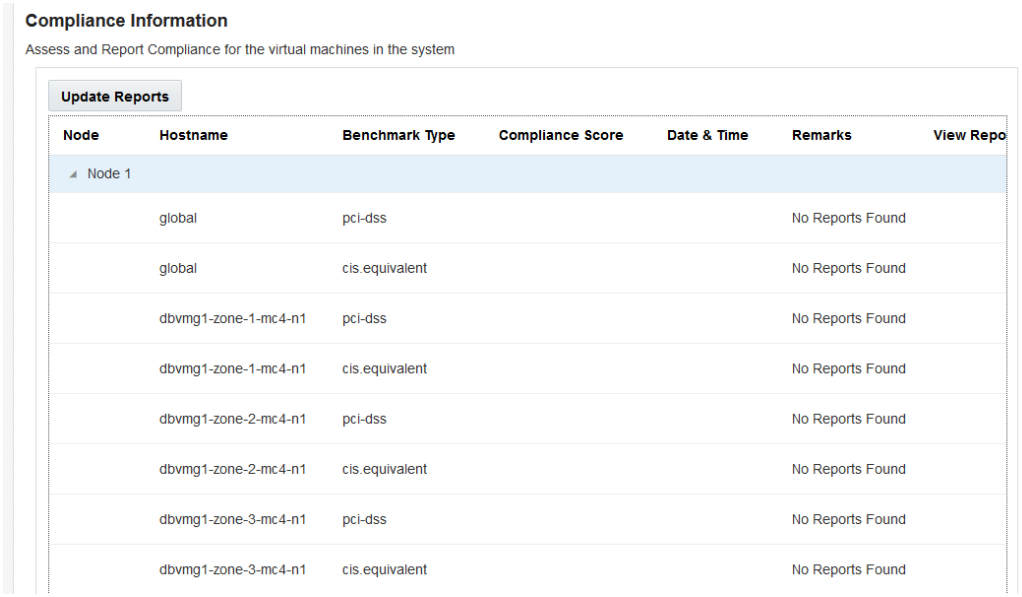
使用此程序，即可使用 MCMU BUI 排定安全基準。若要改用 MCMU CLI，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」以取得指示。

1. **以主要管理員身分登入 MCMU BUI。**
   如需指示，請參閱「*Oracle MiniCluster S7-2 Administration Guide*」。

2. **在首頁中，往下捲動到 [Compliance Information] (規範資訊) 面板。**

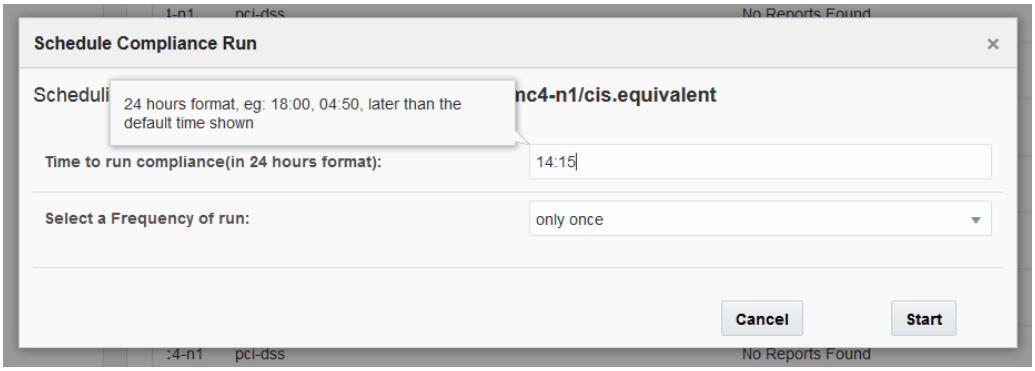
3. **按一下節點，以展開其詳細資訊。**

   每個區域和 VM 都是使用安全設定檔 (CIS 等效或 PCI-DSS) 所設定。當您排定基準時，請選取對應至元件安全設定檔的基準。



4. **捲動到右側，然後按一下其中一個 VM 的 [Schedule] (排定) 按鈕。**

   即會顯示 [Schedule Compliance Run] (排定規範執行) 頁面。



5. **指定時間和頻率，然後按一下 [Start] (啟動)。**
在排定的時間執行安全規範測試之後，請檢視報告。請參閱「檢視基準報告 (BUI)」[45]。

▼ 檢視基準報告 (BUI)

這些是可接受的規範結果：

	CIS 等效	PCI-DSS
全域區域	大約 88%	大約 88%
VM	大約 90%	大約 93%

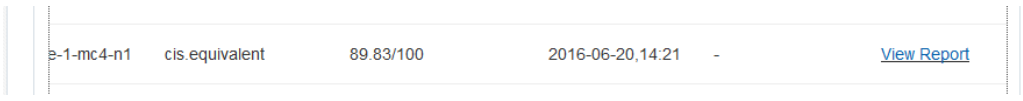
這些是已知的規範測試失敗，是因為 Oracle Solaris 問題所造成：

- 套裝軟體完整性 (核心作業系統、rad-python)
- GDM
- 路由常駐程式
- SSH 回送位址 – 減輕無法修正問題。
- 命名服務無法辨識 DNS
- LDAP 用戶端

這些是已知的規範測試失敗，是因為 MiniCluster 客戶必要組態問題所造成：

- NFS 用戶端服務 – 選取需要的可用服務。
- 設定 eeprom 密碼 – 選擇性設定

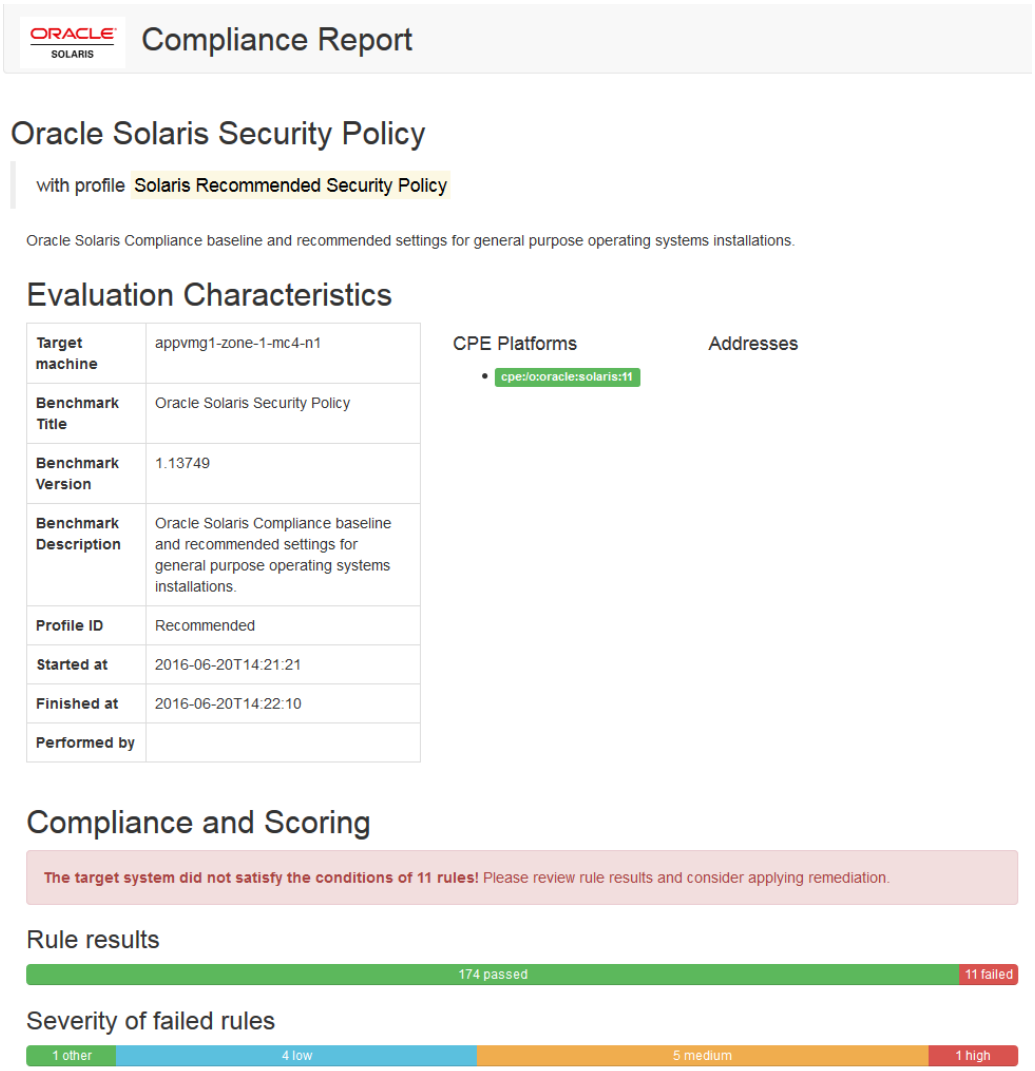
1. **登入 MCMU BUI。**
2. **在首頁中，往下捲動到 [Compliance Information] (規範資訊) 面板。**
3. **按一下 [Update Reports] (更新報告)。**
更新程序需要一分鐘或大約一分鐘的時間才能完成。
4. **展開節點，顯示以及識別規範報告。**



5. **捲動到右側，然後按一下 [View Report] (檢視報告)。**

即會顯示基準報告。

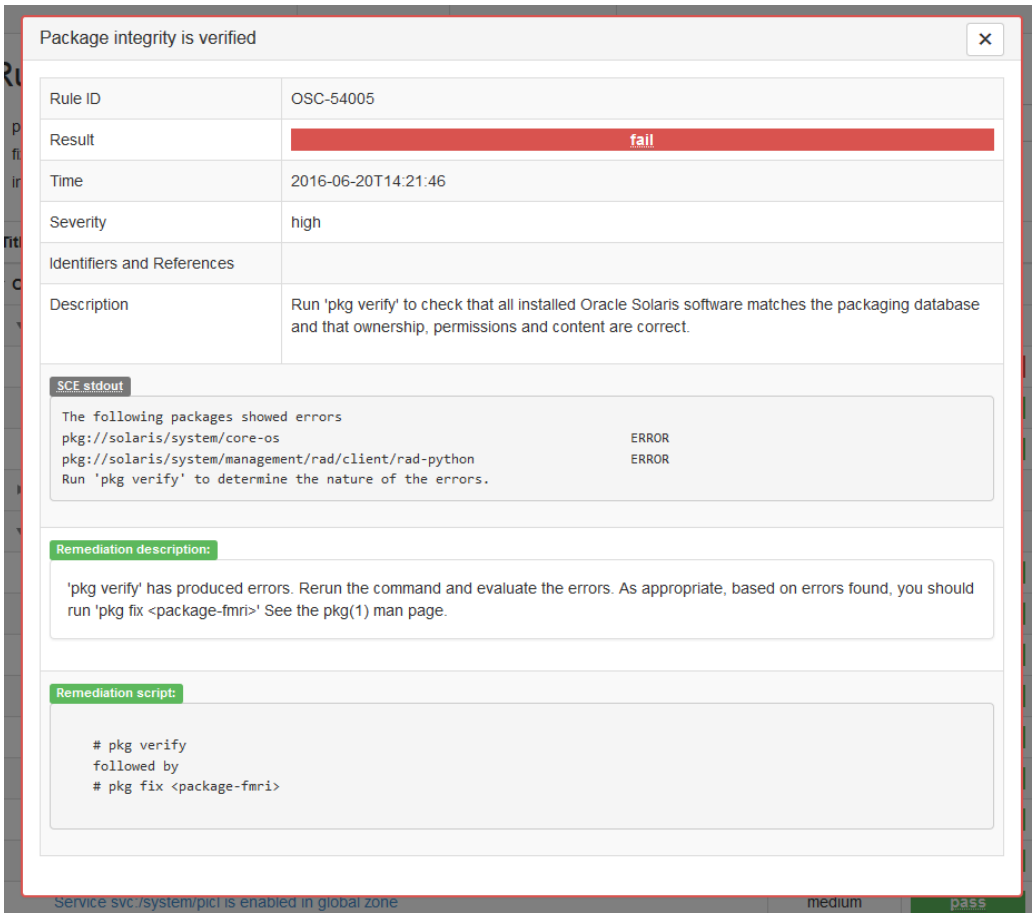
在 [Rule Overview] (規則簡介) 下，您可以選取要根據其結果顯示的測試類型。您也可以在 [Search] (搜尋) 欄位中指定搜尋字串。



6. **根據報告，您可以確認安全控制、規範評分、異常和補救程序。**

7. **按一下測試名稱，以取得詳細資訊和建議補救資訊。**

注意 - 按一下報告底端的 [Show all Result Details] (顯示所有結果詳細資訊)，即可顯示所有測試的詳細資訊。



瞭解 SPARC S7-2 伺服器安全控制

下列主題描述硬體和 OpenBoot 環境的安全控制。

瞭解硬體安全

您的安全架構必須建立在實體隔離和存取控制的基礎上。確實將實體伺服器安裝在安全的環境中，可保護實體伺服器免於未經授權的存取。同樣地，記錄所有序號有助於避免硬體遭到竊取、轉售或承擔供應鏈風險，也就是盜版或偽造的元件流入組織供應鏈的情況。

下列小節提供 MiniCluster 的一般硬體安全準則。

使用限制

- 將伺服器及相關設備安裝在上鎖且限制人員進出的房間內。
- 如果設備安裝在有門可以上鎖的機架內，除非必須維護或操作機架內的元件，否則請將機架門隨時保持上鎖。將門上鎖也可以有效限制熱插式或熱抽換式裝置的使用。
- 將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，以察覺並避免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。
- 限制存取 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。實際取用元件是較為安全的存取方法，因為比較不易受到網路攻擊。

- 將主控台連線外部 KVM 以啟用遠端主控台存取。KVM 裝置通常支援雙因素認證、集中式存取控制及稽核功能。如需有關 KVM 之安全準則和最佳措施的詳細資訊，請參閱 KVM 裝置提供的文件。

序號

- 記錄所有硬體的序號。
- 為所有重要的電腦硬體項目 (例如替換零件) 加上安全標誌。使用特殊的紫外線筆或浮水印標籤來加註安全標誌。
- 將硬體啟動金鑰與授權文件存放在安全的位置。發生系統緊急狀況時，系統管理人員必須能輕易地存取此位置。書面文件可能會是擁有權的唯一證明。

無線電頻率識別 (RFID) 讀取器可進一步簡化資產的追蹤。您可以從下列網址取得「如何使用 *RFID* 追蹤您的 *Oracle Sun* 系統資產」Oracle 白皮書：

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

硬碟

硬碟經常用來儲存機密資訊。如果要防止此資訊受到未經授權的存取，硬碟在重新使用、退役或丟棄之前必須先經妥善處理。

- 您可以使用磁碟清除工具 (例如 Oracle Solaris `format` (1M) 指令) 來徹底清除磁碟機上的所有資料。
- 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

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

限制存取 OpenBoot

下列主題描述如何在 OpenBoot 提示下限制存取。

如需如何設定 OpenBoot 密碼的指示，請參閱「設定 EEPROM 密碼」[26]。

- 「進入 OpenBoot 提示」[51]
- 「查看失敗的登入」[51]
- 「提供開啟電源系統資訊」[51]

如需設定 OpenBoot 安全變數的相關資訊，請參閱 OpenBoot 文件，網址如下：

http://www.oracle.com/goto/openboot/docs

▼ 進入 OpenBoot 提示

此程序描述如何到達 MiniCluster 運算節點上的 OpenBoot 提示，以設定安全控制。

您必須關閉系統，才能到達 OpenBoot 提示。遵循完全關閉 VM 的適當程序 (如「*Oracle MiniCluster S7-2 Administration Guide*」中所述)。

1. **登入節點上的 Oracle ILOM，並發出此指令。**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

以 `mcinstall` 使用者身分登入主機主控台，並 `su` 成為 `root`。

2. **關閉所有 VM 之後，請以 root 角色中止全域區域。**

```
# init 0
.
.
.
{0} ok
```

▼ 查看失敗的登入

1. **請依照下列範例，使用 `security-#badlogins` 參數判斷是否有失敗的 OpenBoot 環境存取嘗試。**

```
{0} ok printenv security-#badlogins
```

如果此指令傳回任何大於 Ø 的值，則代表記錄了失敗的 OpenBoot 環境存取嘗試。

2. **鍵入此指令即可重設參數。**

```
{0} ok setenv security-#badlogins 0
```

▼ 提供開啟電源系統資訊

儘管這並不是直接的預防或偵測控制措施，您仍可基於下列原因來運用系統資訊：

- 傳達擁有權。

- 對使用者顯示伺服器的合理使用警告。
- 說明僅限獲得授權的人員，才能夠存取或修改 OpenBoot 參數。

- **請使用下列指令來啟用自訂警告訊息。**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

系統資訊訊息長度上限為 68 個字元。可以使用所有可列印的字元。

索引

O

P

R

S

V

Z