

**Oracle® Hierarchical Storage Manager and
StorageTek QFS Software**

安全指南

版本 6.0

E62081-01

2015 年 3 月

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
安全指南

E62081-01

版權 © 2015, Oracle 和 (或) 其關係公司。保留一切權利。

本軟體與相關說明文件是依據含有用途及保密限制事項的授權合約所提供，且受智慧財產法的保護。除了授權合約中或法律明文允許的部分外，不得以任何形式或方法使用、複製、重製、翻譯、廣播、修改、授權、傳送、散佈、展示、演出、出版或陳列本軟體的任何部分。除非依法需要取得互通性操作 (interoperability)，否則嚴禁對本軟體進行還原工程 (reverse engineering)、反向組譯 (disassembly) 或解編 (decompilation)。

本文件中的資訊如有變更恕不另行通知，且不保證沒有任何錯誤。如果您發現任何問題，請來函告知。

如果本軟體或相關說明文件是提供給美國政府或代表美國政府授權使用本軟體者，則適用下列條例：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本軟體或硬體是針對各類資訊管理應用程式的一般使用所開發。不適用任何原本就具危險性的應用上，包含會造成人身傷害風險的應用。如果您將本軟體或硬體應用於危險用途，則應採取適當的防範措施，包括保全、備份、儲備和其他措施以確保使用安全。Oracle Corporation 和其關係公司聲明對將本軟體或硬體應用於危險用途所造成之損害概不負任何責任。

Oracle 和 Java 是 Oracle 和 (或) 其關係公司的註冊商標。其他名稱為各商標持有人所擁有之商標。

Intel 和 Intel Xeon 是 Intel Corporation 的商標或註冊商標。所有 SPARC 商標的使用皆經過授權，且是 SPARC International, Inc. 的商標或註冊商標。AMD、Opteron、AMD 標誌與 AMD Opteron 標誌是 Advanced Micro Devices 的商標或註冊商標。UNIX 是 The Open Group 的註冊商標。

本軟體或硬體與說明文件可能提供有關第三方內容、產品和服務的存取途徑與資訊。除非您與 Oracle 之間的適用合約另有規定，否則 Oracle Corporation 和其關係公司明文聲明對第三方網站所提供的內容、產品與服務不做保證，且不負任何責任。除非您與 Oracle 之間的適用合約另有規定，否則 Oracle Corporation 和其關係公司對於您存取或使用第三方的內容、產品或服務所引起的任何損失、費用或損害亦不負任何責任。

內容

序言	5
對象	5
文件輔助功能	5
排版慣例	5
指令中的 Shell 提示符號範例	5
1. 概覽	7
1.1. 產品概覽	7
1.2. 一般安全原則	8
1.2.1. 持續更新軟體	8
1.2.2. 限制重要服務的網路存取	8
1.2.3. 遵循最低權限的原則	8
1.2.4. 監督系統活動	8
1.2.5. 持續更新最新的安全資訊	9
2. 安全安裝	11
2.1. 瞭解您的環境	11
2.1.1. 需要保護哪些資源？	11
2.1.2. 必須保護資源避免哪些人存取？	11
2.1.3. 如果策略資源的保護失敗會發生什麼事？	12
2.2. 建議的建置拓樸	12
2.2.1. 安裝 SAM-Remote	13
2.2.2. 安裝 Manager GUI	13
2.2.3. 後續安裝配置	13
3. 安全功能	15
3.1. 安全模型	15
3.1.1. 認證	15
3.1.2. 存取控制	15
4. 開發人員的安全考量	17
A. 安全建置檢查清單	19

前言

「Oracle Hierarchical Storage Manager and StorageTek QFS Software 安全指南」包含 Oracle Hierarchical Storage Manager 和 QFS 產品的相關資訊，並說明應用程式安全性的一般原則。

對象

本指南適用於使用 Oracle Hierarchical Storage Manager and StorageTek QFS Software 安全功能、安全安裝及配置的相關人員。

文件輔助功能

如需有關 Oracle 對於輔助功能的承諾資訊，請瀏覽 Oracle Accessibility Program 網站，網址為 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>。

取用 Oracle 支援

已購買支援的 Oracle 客戶可以透過 My Oracle Support 使用電子支援。如需資訊，請瀏覽 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>；如果您在聽力上需要特殊服務，請瀏覽 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>。

排版慣例

下表描述本書所使用的排版慣例。

字體	意義	範例
<i>AaBbCc123</i>	指令的名稱及電腦的螢幕輸出	使用 <code>ls -a</code> 列出所有檔案。
AaBbCc123	您所鍵入的使用者輸入會與電腦螢幕輸出一起顯示	<code>machine_name% su</code> <i>Password:</i>
<i>aabbcc123</i>	預留位置，用實際名稱或值取代	移除檔案的指令是 <code>rm filename</code> 。
<i>AaBbCc123</i>	書名、新的字彙或術語、要強調的詞	閱讀使用者指南中的第 6 章。 快取是本機儲存的複本。 請勿儲存檔案。 注意，某些強調項目在線上會以粗體顯示。

指令中的 Shell 提示符號範例

下表顯示 Oracle Solaris 作業系統中所含與 shell 有關的預設 UNIX 系統提示及超級使用者提示。請注意，指令範例中顯示的預設系統提示符號會視 Oracle Solaris 發行版本而有所不同。

Shell	提示符號
Bashshell、Kornshell 及 BourneShell	\$
超級使用者的 Bashshell、Kornshell 及 BourneShell	#
Cshell	machine_name%
超級使用者的 Cshell	machine_name#

本章提供 Oracle Hierarchical Storage Manager and StorageTek QFS Software 產品的概覽，以及說明應用程式安全性的一般原則。

1.1. 產品概覽

Oracle Hierarchical Storage Manager and StorageTek QFS Software 是一個具有階層式儲存管理程式的共用檔案系統。產品由下列主要元件組成：

StorageTek QFS 套裝軟體

包括高效能的 QFS 檔案系統，可以以獨立或共用方式配置。以獨立方式配置時，會在單一系統上配置 QFS，不可與共用用戶端搭配使用。QFS 使用標準 VFS vnode 作業作為與 Oracle Solaris 和 Linux 作業系統的介面。

QFS 安裝套裝軟體為 SUNWqfsr 和 SUNWqfsu。這些套裝軟體不包括 Oracle Hierarchical Storage Manager (HSM) 元件。

獨立設定 QFS 不搭配共用用戶端使用，具有最低的安全風險。此配置不會執行常駐程式，也沒有「光纖通道 (FC)」以外的任何遠端連線至磁碟。配置 QFS 共用包括 FC 連線至磁碟，以及用戶端和描述資料伺服器 (MDS) 之間的 TCP/IP 連線。

Oracle HSM 套裝軟體

包括 QFS 檔案系統和執行 Oracle HSM 所需的程式碼。Oracle HSM 安裝套裝軟體為 SUNWsamfsr 和 SUNWsamfsu。如果您不需要階層式儲存管理，請只安裝 StorageTek QFS 套裝軟體。

SAM-Remote

允許透過 TCP/IP 廣域網路 (WAN) 連線的方式存取遠端磁帶櫃和磁碟機。StorageTek SAM-Remote 提供一種遠端定位磁帶設備來進行災難復原的方式。您可以安裝 SAM-Remote 和 QFS 或 SAM-QFS 套裝軟體，但必須分別啟用與配置 SAM-Remote。如需 SAM-Remote 的詳細資訊，請參閱 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

管理程式圖形化使用者介面

管理程式圖形化使用者介面 (GUI) fsmgr 會在 MDS 上執行，可透過 Web 瀏覽器遠端存取。透過連接埠 6789 (https://hostname:6789) 可授予存取權。

若要使用 fsmgr，您必須以 MDS 上的有效使用者身分登入，並新增特定角色至該使用者帳號。如需安裝與設定 Manager GUI 的相關資訊，請參閱 *Oracle*

Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2. 一般安全原則

下列各節描述安全地使用任何應用程式所需的基本原則。

1.2.1. 持續更新軟體

讓您執行的 Oracle HSM 保持在最新的版本。您可以在 Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>) 找到最新版本的軟體以進行下載。

1.2.2. 限制重要服務的網路存取

Oracle HSM 使用下列 TCP/IP 連接埠：

- tcp/7105 用於用戶端和 MDS 之間的描述資料流量
- tcp/1000 用於 SAM-Remote
- tcp/6789 是瀏覽器用來連線至 fsmgr 的 HTTP 連接埠
- tcp/5012 用於 sam-rpcd

注意:

對於 MDS 雙向用戶端流量，請考慮設定不會連線至外界 WAN 的獨立網路。此配置可避免暴露在外界威脅中，同時可確保外界流量不會限制 MDS 效能。

1.2.3. 遵循最低權限的原則

授予使用者或管理員完成執行工作所需的最低權限。Manager GUI 管理程式有數種角色可授予使用者。這些角色可授予不同類型和不同數量的權限。從指令行執行管理工作需要 root 權限。

如需使用 Manager GUI 的詳細資訊，請參閱 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2.4. 監督系統活動

監督系統活動以判斷 Oracle HSM 運作的情形，以及是否有任何不尋常活動的記錄。請檢查下列記錄檔：

- /var/adm/messages
- /var/opt/SUNWsamfs/sam-log
- /var/opt/SUNWsamfs/archiver.log，查看 /etc/opt/SUNWsamfs/archiver.cmd
- /var/opt/SUNWsamfs/recycler.log，查看 /etc/opt/SUNWsamfs/recycler.cmd

- /var/opt/SUNWsamfs/releaser.log，查看 /etc/opt/SUNWsamfs/releaser.cmd
- /var/opt/SUNWsamfs/stager.log，查看 /etc/opt/SUNWsamfs/stager.cmd
- /var/opt/SUNWsamfs/trace/*

1.2.5. 持續更新最新的安全資訊

您可以存取數個安全資訊來源。如需各種軟體產品的安全資訊和警示，請參閱 <http://www.us-cert.gov>。如需 SAM-QFS 的特定資訊，請參閱 https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401。持續保持安全的主要方法就是執行最新版本的 Oracle HSM 軟體。

本章概述安全安裝的計畫程序，以及描述數種建議的系統建置拓樸。

2.1. 瞭解您的環境

為了更進一步瞭解安全需求，請考量下列問題：

2.1.1. 需要保護哪些資源？

您可以保護實際執行環境中的許多資源。請考量您想要保護的資源類型，然後決定提供的安全性層級。

使用 Oracle HSM 時，請保護下列資源：

中繼資料和主要資料磁碟

這些磁碟資源是用來建立 Oracle HSM 檔案系統。它們通常使用「光纖通道 (FC)」連線。獨立存取這些磁碟 (未透過 Oracle HSM 的方式) 會帶來安全風險，因為這樣會略過 Oracle HSM 的檔案和目錄權限。這類外部存取可能是來自讀取或寫入 FC 磁碟的有問題系統，或是來自對原始裝置檔案意外提供非 root 存取的內部系統。

Oracle HSM 磁帶

獨立存取磁帶會有安全風險，這通常會發生在離開 Oracle HSM 檔案系統時寫入檔案資料的磁帶櫃中。

Oracle HSM 傾印磁帶

從 samfsdump 建立的檔案系統傾印包含資料和描述資料。這類資料和描述資料應受到保護，避免在例行傾印或復原活動時被系統管理員以外的人存取。

Oracle HSM 描述資料伺服器 (MDS)

Oracle HSM 用戶端要求 TCP/IP 存取 MDS。不過，請確定用戶端受到保護，讓外部 WAN 無法存取。

配置檔和設定值

Oracle HSM 配置設定必須受到保護，不受到非管理員存取。一般而言，當您使用 Manager GUI 時，Oracle HSM 會自動保護這些設定值。注意，若配置檔可供非管理使用者寫入會帶來安全風險。

2.1.2. 必須保護資源避免哪些人存取？

一般而言，前節所述的資源必須受到保護，不受配置的系統上的所有非 root 或非管理員存取，或有問題的外部系統透過 WAN 或 FC 光纖的方法來存取這些資源。

2.1.3. 如果策略資源的保護失敗會發生什麼事？

策略資源的保護失敗，可能會導致不適當的存取 (正常 Oracle HSM POSIX 檔案權限以外的存取資料)，甚至導致資料損毀 (正常權限以外的寫入磁碟或磁帶)。

2.2. 建議的建置拓樸

本節描述如何安全地安裝與設定基礎架構元件。如需安裝 Oracle HSM 的相關資訊，請參閱 *Oracle Hierarchical Storage Manager Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

安裝與設定 Oracle HSM 時，請考量下列各點：

區隔描述資料網路

若要將 Oracle HSM 用戶端連線至 MDS 伺服器，請提供沒有連線至任何 WAN 的其他 TCP/IP 網路和交換器硬體。因為描述資料流量是使用 TCP/IP 來實行，理論上外部有可能會攻擊此流量。配置不同的描述資料網路可降低此風險，同時可提供更好的效能。藉由提供描述資料保證的資料路徑，達成效能上的改進。如果區隔描述資料網路不可行，請至少拒絕來自外部 WAN 以及網路上任何不信任主機的 Oracle HSM 連接埠的流量。請參閱節 1.2.2, 「限制重要服務的網路存取」。

FC 分區

使用 FC 分區來限制任何不需要存取 Oracle HSM 磁碟的伺服器對這些磁碟的存取。最好使用不同的 FC 交換器，僅實體連線到需要存取的伺服器。

保護 SAN 磁碟配置存取

SAN RAID 磁碟通常會透過 TCP/IP 或 HTTP 的方式存取以進行管理。您必須限制只有信任網域中的系統才能對 SAN RAID 磁碟進行管理存取，保護磁碟不受外部存取。同時，變更磁碟陣列上的預設密碼。

安裝 Oracle HSM 套裝軟體

首先，僅安裝您需要的套裝軟體。例如，如果您不要使用階層式儲存管理，請只安裝 QFS 套裝軟體。如果未曾考量變更預設 Oracle HSM 檔案和目錄權限及擁有者所帶來的安全影響，就不應變更這些項目。

用戶端存取

如果您計畫配置共用用戶端，請決定哪些用戶端必須擁有 hosts 檔案中的檔案系統存取權。請參閱 hosts.fs(4) 線上手冊。僅配置需要存取要配置之特定檔案系統的主機。

強化 Oracle Solaris 描述資料伺服器

如需強化 Oracle Solaris 作業系統的相關資訊，請參閱「Oracle Solaris 10 安全性準則」和「Oracle Solaris 11 安全性準則」。至少，選擇一個較好的 root 密碼、安裝最新版本的 Oracle Solaris 作業系統，並持續安裝最新的修補程式 (特別是安全修補程式)。

強化 Linux 用戶端

查看有關如何強化 Linux 用戶端的相關 Linux 文件。至少，選擇一個較好的 root 密碼、安裝最新版本的 Linux 作業系統，並持續安裝最新的修補程式 (特別是安全修補程式)。

Oracle HSM 磁帶安全性

避免來自 Oracle HSM 以外的外部存取 Oracle HSM 磁帶，或限制只有管理員才能進行這類存取。利用 FC 分區，限制只有 MDS 或可能的 MDS (如有設定備份 MDS) 才能存取磁帶機。配置使用分散式 I/O 的 Solaris 用戶端，將需要磁帶機的存取權限。同時，僅授予 root 權限，限制磁帶裝置檔案存取。對 Oracle HSM 磁帶的未授權存取可能會影響或損毀使用者資料。

備份

使用 `samfsdump` 或 `qfsdump` 指令，設定並執行 Oracle HSM 資料的備份。對於 Oracle HSM 磁帶，建議限制對傾印磁帶的存取。

2.2.1. 安裝 SAM-Remote

如需安全安裝 SAM-Remote 軟體的相關資訊，請參閱 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>。

2.2.2. 安裝 Manager GUI

如需安全地安裝 Manager GUI 的相關資訊，*Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

2.2.3. 後續安裝配置

安裝任何 Oracle HSM 套裝軟體之後，請檢查附錄 A, [安全建置檢查清單](#) 中安全檢查清單內的項目

若要避免潛在安全威脅，運作共用檔案系統的客戶必須注意下列事項：

- 違反原則的檔案系統資料揭露
- 資料遺失
- 未偵測到的資料修改

藉由正確地配置和遵循[附錄 A, 安全建置檢查清單](#)中的後續安裝檢查清單，即可使這些安全威脅降至最低。

3.1. 安全模型

提供保護防止安全威脅的重要安全功能有：

- 認證 – 確保只有經過授權的個人才能授權存取系統和資料。
- 授權 – 對系統權限和資料的存取控制。此功能建立在認證上，以確保個人只能得到適當的存取權。
- 稽核 – 可讓管理員偵測對認證機制漏洞的嘗試，以及存取控制漏洞的嘗試或成功嘗試。

3.1.1. 認證

Oracle HSM 使用以主機為基礎的使用者認證，控制能夠執行管理工作的人員。使用 Manager GUI 進行的管理主要由指派給各種使用者的角色控制。只有 root 使用者才能使用指令行管理。

3.1.2. 存取控制

Oracle HSM 中的存取控制分為兩個部分：

- 管理存取控制 – 控制誰能夠進行 Oracle HSM 的管理動作。控制是根據透過 Manager GUI 指派給使用者的角色。對於指令行作業，控制是根據 root 權限。如需 Manager GUI 的詳細資訊，請參閱 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* 客戶文件庫，網址為：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>
- 檔案/目錄存取控制 – Oracle HSM 實行 POSIX 相容的檔案系統，可提供一套豐富的存取控制。請參閱 Oracle HSM 文件瞭解詳細資訊。

開發人員的安全考量

開發人員通常不會直接使用 Oracle HSM 介面。但有兩個例外，分別是 *libsam* API 和 *libsamrpc* API。這兩個 API 提供相同的功能。*libsam* 僅適用於本機，而 *libsamrpc* 則可透過 *rpc(3)* 與 MDS 通訊實行要求的動作。兩種方法所做的要求是根據呼叫程序的 UID 和 GID 來進行認證。它們和透過指令行所做的要求具有相同的權限。請確定您的 MDS 和用戶端系統具有共用的 UID 和 GID 空間。

如需詳細資訊，請參閱 *intro_libsam(3)* 和 *intro_libsamrpc(3)* 線上手冊。

安全建置檢查清單

此安全檢查清單包含可協助您保護資料庫安全的準則。

1. 為 root 及被指派任何 Oracle HSM 角色的任何其他帳號設定更安全的密碼。此準則包括：
 - 由 Manager GUI 授予管理角色的任何帳號。
 - *acsss*、*acsdb* 以及 *acssa* 使用者 ID (如有使用的話)。
 - 任何磁碟陣列管理帳號。
2. 如果在 Manager GUI 使用預設使用者 *samadmin*，請立即將預設的安裝密碼變更為更安全的密碼。請勿在 Manager GUI 使用 root，請視需要將角色指派給其他使用者帳號。並使用更安全的密碼保護其他帳號。
3. 在 WAN 邊緣路由器安裝連接埠篩選，防止節 1.2, 「一般安全原則」所列之連接埠上的流量輸入 MDS 或用戶端 (SAM-Remote 所需流量除外)。
4. 透過實體或 FC 分區方式隔離 FC 磁碟和磁帶，使這些磁碟只能從 MDS 或用戶端存取，磁帶只能從 MDS 和 MDS 存取。此安全應用有助於避免意外覆寫磁帶或磁碟，造成資料遺失意外的發生。
5. 檢查 */dev* 以確保磁帶和磁碟裝置檔案不會被 root 以外的使用者存取。這樣可避免 Oracle HSM 資料受到不適當的存取或毀損。
6. Oracle HSM 是一種 POSIX 檔案系統，提供一套豐富的檔案/目錄權限，包括「存取控制清單 (ACL)」。視需要使用這些權限，保護檔案系統上的使用者資料。如需詳細資訊，請參閱 Oracle HSM 文件。
7. 根據本機原則，設定一組適當的備份傾印。備份是安全性的一部分，提供一個在意外或漏洞造成資料遺失時復原資料的方法。您的備份在傳輸到異地位置時，應包括某些原則。備份應該受到和 Oracle HSM 磁帶與磁碟相同程度的保護。
