Sun QFS 和 Sun Storage Archive Manager 5.3 安全指南

文件號碼：E36000
2012 年 6 月

ORACLE

120817@25097

目錄

前言

Sun QFS 和 Sun Storage Archive Manager 安全指南 包含 Sun QFS 和 Storage Archive Manager (SAM-QFS) 產品的相關資訊，以及應用程式安全性的一般原則。

存取 Oracle Support

Oracle 客戶可透過 My Oracle Support 擁有電子支援的存取權。如需詳細資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info，或如果您有聽力方面的障礙，請造訪 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。

表 P–1 排版慣例

字體	描述	範例
AaBbCc123	指令、檔案和目錄的名稱，以及電腦的螢幕輸出	編輯您的 .login 檔案。 使用 ls -a 列出所有檔案。 machine_name% you have mail.
AaBbCc123	您所鍵入的內容 (相對於電腦的螢幕輸出)	machine_name% **su** Password:
aabbcc123	預留位置：用實際名稱或值取代	移除檔案的指令是 rm *filename* 。
AaBbCc123	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 OS 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，顯示在指令範例中的預設系統提示符號會視 Oracle Solaris 發行版本而有所不同。

表 P–2 Shell 提示

Shell	提示
Bash shell、Korn shell 和 Bourne shell	`$`
適用於超級使用者的 Bash shell、Korn shell 和 Bourne shell	`#`
C shell	`machine_name%`
適用於超級使用者的 C shell	`machine_name#`

◆ ◆ ◆ 第 1 章

1 Sun QFS 和 Sun Storage Archive Manager 概覽

本章提供 Sun QFS 和 Storage Archive Manager (SAM-QFS) 產品的概覽，以及說明應用程式安全性的一般原則。

產品概覽

SAM-QFS 是一個具有階層式儲存管理程式的共用檔案系統。SAM-QFS 由下列主要元件組成：

- **Sun QFS 套裝軟體** – 包括高效能的 Sun 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 Sun QFS，不可以與共用用戶端搭配使用。Sun QFS 使用標準 VFS vnode 作業作爲與 Oracle Solaris 和 Linux 作業系統的介面。

  Sun QFS 安裝套裝軟體爲 `SUNWqfsr` 和 `SUNWqfsu`。這些套裝軟體**不**包括階層式儲存歸檔管理程式 (SAM) 元件。

  獨立配置 Sun 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。
- **SAM-QFS 套裝軟體** – 包括 Sun QFS 檔案系統和執行 SAM 所需的程式碼。

  SAM-QFS 安裝套裝軟體爲 `SUNWsamfsr` 和 `SUNWsamfsu`。若不需要 SAM，請**僅**安裝 Sun QFS 套裝軟體。
- **Sun 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。Sun 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 Sun SAM-Remote 和 Sun QFS 或 SAM-QFS 套裝軟體，但是必須分別啓用與配置 Sun SAM-Remote。如需 Sun SAM-Remote 的進一步相關資訊，請參閱「Sun Storage Archive Manager 5.3 Configuration and Administration Guide」中的第 18 章「Using the Sun SAM-Remote Software」。
- **SAM-QFS 工具套裝軟體** – 在 `/opt/SUNWsamfs/tools` 目錄中安裝工具和線上手冊。這些工具都需要 root 權限才能使用，沒有其他特殊權限。安裝套裝軟體爲 `SUNWsamtp`。

- **SAM-QFS 管理程式** – SAM-QFS 管理程式 `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`) 可授與存取權。

  若要使用 `fsmgr`，您必須以 MDS 上的有效使用者身份登入，並新增特定角色至該使用者帳號。如需安裝與配置 SAM-QFS 管理程式的相關資訊，請參閱 「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」中的第 6 章「Installing and Configuring SAM-QFS Manager」 。

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。

持續更新軟體

讓您執行的 SAM-QFS 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。

限制重要服務的網路存取

SAM-QFS 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 Sun SAM-Remote
- `tcp/6789` 是瀏覽器用來連線至 `fsmgr` 的 HTTPS 連接埠。
- `tcp/5012` 用於 `sam-rpcd`

備註 – 對於 MDS 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。

遵循最低權限的原則

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

如需使用 SAM-QFS 管理程式的進一步相關資訊，請參閱 「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」中的第 6 章「Installing and Configuring SAM-QFS Manager」 。

監視系統活動

監視系統活動以判斷 SAM-QFS 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/*`

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 `http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss`。持續更新安全事項的主要方法是執行最新版本的 SAM-QFS 軟體。

◆ ◆ ◆ 第 2 章

2 保護安裝和組態

本章概述保護安裝的計畫程序，以及描述數種建議的系統建置拓樸。

安裝概覽

瞭解您的環境

爲了更進一步瞭解您的安全需求，請思考下列問題：

- **我要保護哪些資源**？

  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 SAM-QFS 時，請保護下列資源：

  - **描述資料和主要資料磁碟** – 這些磁碟資源是用來建立 SAM-QFS 檔案系統。他們通常使用「光纖通道 (FC)」連線。獨立存取這些磁碟 (不是透過 SAM-QFS 的方式) 會帶來安全風險，因爲這樣會略過一般 SAM-QFS 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。
  - **SAM 磁帶** – 獨立存取磁帶是一種安全風險，這通常發生在離開 SAM 檔案系統時寫入檔案資料的磁帶櫃中。
  - **SAM-QFS 傾印檔** – 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。
  - **SAM-QFS 描述資料伺服器 (MDS)** – SAM-QFS 用戶端需要 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** – SAM-QFS 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「SAM-QFS 管理程式」時，SAM-QFS 會自動保護這些設定值。注意，使配置檔可供非管理使用者寫入會帶來安全風險。

- **我要保護資源不受到哪些人存取**？

  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。

- **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 SAM-QFS POSIX 檔案權限以外的存取資料) 甚至資料損毀 (正常權限以外的寫入磁碟或磁帶)。

建議的建置拓樸

安裝 SAM-QFS

本節描述如何安全地安裝與配置基礎架構元件。

如需安裝 SAM-QFS 的相關資訊，請參閱「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」中的第 5 章「Installing Sun QFS and SAM-QFS」。

安裝與配置 SAM-QFS 時，請考量下列各點：

- **區隔描述資料網路** – 若要將 SAM-QFS 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。因爲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 SAM-QFS 連接埠的流量。請參閱第 8 頁的「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 SAM-QFS 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 SAM-QFS 套裝軟體** – 首先，僅安裝您需要的套裝軟體。例如，如果您沒有計畫要執行 SAM，請**僅**安裝 QFS 套裝軟體。

  未考量變更預設 SAM-QFS 檔案和目錄權限及擁有者的安全影響，就**不**應進行這些項目的變更。
- **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 OS 的相關資訊，請參閱 Oracle Solaris 10 安全性指導方針和 Oracle Solaris 11 安全性指導方針。至少，選擇一個較好的 root 密碼、安裝最新版本的 Oracle Solaris OS，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)。
- **SAM-QFS 磁帶安全性** – 避免來自 SAM 以外的外部存取 SAM 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。同時，僅授與 root 權限，限制磁帶裝置檔案存取。對 SAM 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 SAM-QFS 資料的備份。對於 SAM 磁帶，建議限制對傾印檔的存取。

安裝 Sun SAM-Remote

如需安全地安裝 Sun SAM-Remote 軟體的相關資訊，請參閱 「Sun Storage Archive Manager 5.3 Configuration and Administration Guide」中的第 18 章「Using the Sun SAM-Remote Software」。

安裝 SAM-QFS 管理程式

如需安全地安裝 SAM-QFS 管理程式的相關資訊，請參閱 「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」中的第 6 章「Installing and Configuring SAM-QFS Manager」。

後續安裝配置

安裝任何 SAM-QFS 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。

◆ ◆ ◆ 第 3 章

Sun QFS 和 Sun Storage Archive Manager 安全功能

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。

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。

認證

SAM-QFS 使用以主機爲基礎的使用者認證，控制能夠執行管理工作的人員。使用「SAM-QFS 管理程式」管理主要由指派給不同使用者的角色來控制。只有 root 使用者才能使用指令行管理。

存取控制

SAM-QFS 中的存取控制區分爲兩個部分：

- **管理存取控制** – 控制誰能夠進行 SAM-QFS 的管理動作。控制是根據透過「SAM-QFS 管理程式」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 SAM-QFS 管理程式的進一步相關資訊，請參閱「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」中的第 6 章「Installing and Configuring SAM-QFS Manager」。
- **檔案/目錄存取控制** – SAM-QFS 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 SAM-QFS 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 SAM-QFS 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 通訊以實行要求的動作。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「Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual」中的 `intro_libsam(3)` 和 `intro_libsamrpc(3)`。

◆ ◆ ◆ 附錄 A

安全建置檢查清單

利用附錄中的檢查清單，安全地建置 SAM-QFS 軟體。

建置檢查清單

此安全檢查清單包含可協助您保護資料庫的指導方針。

- 爲 root 及被指派任何 SAM-QFS 角色的任何其他帳號設定更安全的密碼。此指導方針包括：
  - 由「SAM-QFS 管理程式」授與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。
- 如果「SAM-QFS 管理程式」使用預設使用者 `samadmin`，請立即將密碼從預設安裝的密碼變更爲更安全的密碼。請勿在「SAM-QFS 管理程式」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這些帳號。
- 在 WAN 邊緣路由器安裝連接埠篩選，防止第 8 頁的 「一般安全原則」所列之連接埠上的流量輸入 MDS 或用戶端 (Sun SAM-Remote 所需流量的除外)。
- 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。
- 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。此應用可避免 SAM-QFS 資料受到不適當的存取或毀損。
- SAM-QFS 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 SAM-QFS 文件。
- 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。備份應受到和 SAM-QFS 磁帶與磁碟相同程度的保護。

參考資料

- 「Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide」
- 「Sun QFS File System 5.3 Configuration and Administration Guide」
- 「Sun Storage Archive Manager 5.3 Configuration and Administration Guide」
- 「Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual」