Sun QFS 和 Sun Storage Archive Manager 5.3 安全指南

文件号码 E35999
E35999-01，2012 年 6 月

ORACLE

120817@25097

目录

前言

《Sun QFS 和 Sun Storage Archive Manager 安全指南》包括 Sun QFS 和 Storage Archive Manager (SAM-QFS) 产品的相关信息并介绍了应用程序安全的一般原则。

获取 Oracle 支持

Oracle 客户可通过 My Oracle Support 获取电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info 或 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs（如果听力有障碍）。

印刷约定

下表介绍了本书中的印刷约定。

表 P–1 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 选项。 **注意**：有些强调的项目在联机时以粗体显示。
新词术语强调	新词或术语以及要强调的词	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P–2 shell 提示符

shell	提示符
Bash shell、Korn shell 和 Bourne shell	`$`
Bash shell、Korn shell 和 Bourne shell 超级用户	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

◆ ◆ ◆ 第 1 章

Sun QFS 和 Sun Storage Archive Manager 概述

本章概述了 Sun QFS 和 Storage Archive Manager (SAM-QFS) 产品并介绍了应用程序安全的一般原则。

产品概述

SAM-QFS 是具有分层次存储管理器的共享文件系统。SAM-QFS 由以下主要组件组成：

- **Sun QFS 软件包** – 包括可独立配置或共享配置的高性能 Sun QFS 文件系统。以独立方式配置时，Sun QFS 是在没有共享客户机的情况下在单个系统上进行配置的。Sun QFS 使用标准 VFS vnode 操作与 Oracle Solaris 和 Linux 操作系统连接。

  Sun QFS 安装软件包包括 `SUNWqfsr` 和 `SUNWqfsu`。这两个软件包**不**包含分层次存储归档管理器 (Storage Archive Manager, SAM) 组件。

  在没有任何共享客户机的情况下独立配置 Sun QFS 可将安全风险降至最低。此配置并不运行守护进程，除光纤通道 (Fibre Channel, FC) 与磁盘的连接之外，不存在与磁盘的任何其他远程连接。配置共享 QFS 包括与磁盘的 FC 连接以及客户机与元数据服务器 (metadata server, MDS) 之间的 TCP/IP 连接。

- **SAM-QFS 软件包** – 包括 Sun QFS 文件系统以及运行 SAM 所需的代码。

  SAM-QFS 安装软件包包括 `SUNWsamfsr` 和 `SUNWsamfsu`。如果不需要 SAM，则**仅**安装 Sun QFS 软件包。

- **Sun SAM-Remote** – 允许通过 TCP/IP 广域网 (Wide Area Network, WAN) 连接方式来访问远程磁带库和磁带机。Sun SAM-Remote 提供一种通过远程定位磁带设备来进行灾难恢复的方法。可以使用 Sun QFS 软件包或 SAM-QFS 软件包安装 Sun SAM-Remote，但您必须单独启用和配置 Sun SAM-Remote。有关 Sun SAM-Remote 的更多信息，请参见《Sun Storage Archive Manager 5.3 配置和管理指南》中的第 18 章 “使用 Sun SAM-Remote 软件”。

- **SAM-QFS 工具软件包** – 在 `/opt/SUNWsamfs/tools` 目录下安装工具和手册页。这些工具中没有一个工具具有特殊权限，但这些工具全部都需要具有 root 用户访问权限才能使用。安装软件包为 `SUNWsamtp`。

- **SAM-QFS Manager** – SAM-QFS Manager `fsmgr` 在 MDS 上运行并可以通过 Web 浏览器远程访问。通过端口 6789 (`https://`*hostname*`:6789`) 授予访问权限。

  要使用 `fsmgr`，必须以有效用户身份登录到 MDS 并将某些角色添加到用户帐户中。有关安装和配置 SAM-QFS Manager 的信息，请参见《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》中的第 6 章 “安装和配置 SAM-QFS Manager”。

一般安全原则

以下各节介绍了安全使用任何应用程序所需的基本原则。

保持软件为最新

使运行的 SAM-QFS 的版本保持最新。可以在以下位置找到软件的最新版本来下载：Oracle Software Delivery Cloud (`https://edelivery.oracle.com/`)。

限制关键服务的网络访问权限

SAM-QFS 使用以下 TCP/IP 端口：

- `tcp/7105` 用于客户机与 MDS 之间的元数据通信
- `tcp/1000` 用于 Sun SAM-Remote
- `tcp/6789` 是 HTTPS 端口，用于浏览器联系 `fsmgr`
- `tcp/5012` 用于 `sam-rpcd`

注 – 对于 MDS 客户机通信，请考虑设置未与外部 WAN 互连的独立网络。此配置可防止来自外部威胁的安全风险，还可以确保外部通信不限制 MDS 性能。

遵循最小特权原则

授予用户或管理员完成要执行的任务所需的最小特权。SAM-QFS Manager 具有可为用户授予的各种角色。这些角色可以授予不同类型和数量的特权。从命令行执行 SAM-QFS 管理任务需要 root 用户权限。

有关使用 SAM-QFS Manager 的更多信息，请参见《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》中的第 6 章 “安装和配置 SAM-QFS Manager”。

监视系统活动

监视系统活动以确定 SAM-QFS 的运行情况以及是否正在记录任何异常活动。检查以下日志文件：

- /var/adm/messages
- /var/opt/SUNWsamfs/sam-log
- /var/opt/SUNWsamfs/archiver.log，请参见 /etc/opt/SUNWsamfs/archiver.cmd
- /var/opt/SUNWsamfs/recycler.log，请参见 /etc/opt/SUNWsamfs/recycler.cmd
- /var/opt/SUNWsamfs/releaser.log，请参见 /etc/opt/SUNWsamfs/releaser.cmd
- /var/opt/SUNWsamfs/stager.log，请参见 /etc/opt/SUNWsamfs/stager.cmd
- /var/opt/SUNWsamfs/trace/*

及时了解最新安全信息

可以访问安全信息的多个源。有关各种软件产品的安全信息和警报，请参见 http://www.us-cert.gov。有关 SAM-QFS 的特定信息，请参见 http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss。及时了解最新安全信息的主要方式是运行最新版本的 SAM-QFS 软件。

◆ ◆ ◆ 第 2 章

2 安全安装和配置

本章概述了安全安装的规划过程并介绍了建议的一些系统部署拓扑结构。

安装概述

了解环境

为了更好地了解您的安全需求，可以问自己以下几个问题：

- **我要保护的资源是什么？**

  您可以在生产环境中保护很多资源。确定要提供的安全级别时，请考虑要保护的资源的类型。

  使用 SAM-QFS 时，将保护以下资源：

  - **元数据和主数据磁盘**－这些磁盘资源用于构建 SAM-QFS 文件系统。通常，它们通过光纤通道 (Fibre Channel, FC) 连接。单独访问这些磁盘（不通过 SAM-QFS 方式）存在安全风险，因为这样做会绕过正常的 SAM-QFS 文件和目录权限。此种外部访问类型可能来自读取或写入 FC 磁盘的恶意系统，也可能来自意外提供对原始设备文件的非超级用户访问权限的内部系统。
  - **SAM 磁带**－独立访问磁带（通常位于磁带库中，关闭 SAM 文件系统时会在其中写入文件数据）存在安全风险。
  - **SAM-QFS 转储文件**－通过 `samfsdump` 创建的文件系统转储包含数据和元数据。应加以保护以避免访问这些数据和元数据，系统管理员在例行转储或恢复活动期间访问它们除外。
  - **SAM-QFS 元数据服务器 (Metadata server, MDS)**－SAM-QFS 客户机需要对 MDS 进行 TCP/IP 访问。但是，请确保阻止外部 WAN 访问客户机。

- **配置文件和设置－必须**阻止非管理员访问 SAM-QFS 配置设置。通常，SAM-QFS 会在您使用 SAM-QFS Manager 时自动保护这些设置。请注意，使配置文件对非管理用户可写存在安全风险。

- **要阻止谁访问资源？**

  通常，**必须**阻止已配置系统上的所有非超级用户或非管理员访问上一节中介绍的资源，也必须阻止可以通过 WAN 或 FC 结构访问这些资源的外部恶意系统来访问这些资源。

- **如果对战略资源的保护失败，将发生什么情况？**

  针对战略资源的保护失败可能源于非正常访问（在没有正常 SAM-QFS POSIX 文件权限的情况下访问数据）和数据损坏（在没有正常权限的情况下写入磁盘或磁带）等。

建议的部署拓扑结构

安装 SAM-QFS

本节介绍了如何安全安装和配置基础结构组件。

有关安装 SAM-QFS 的信息，请参见《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》中的第 5 章 “安装 Sun QFS 和 SAM-QFS”。

安装和配置 SAM-QFS 时请考虑以下几点：

- **独立的元数据网络－**要将 SAM-QFS 客户机连接到 MDS 服务器，请提供独立的 TCP/IP 网络和未连接到任何 WAN 的交换机硬件。由于元数据通信是通过使用 TCP/IP 实现的，因此，从理论上讲，可能会存在对此通信的外部攻击。配置独立的元数据网络不仅可以缓解此风险，还可以提高性能。提高性能是通过提供元数据的可靠数据路径来实现的。如果独立的元数据网络不可行，则至少拒绝从外部 WAN 和网络中任何不受信任的主机到 SAM-QFS 端口的通信。请参见第 8 页中的 “限制关键服务的网络访问权限”。

- **FC 区域划分－**使用 FC 区域划分可拒绝不需要访问 SAM-QFS 磁盘的任何服务器访问该磁盘。最好使用独立的 FC 交换机，以便采用物理方式**仅**连接到需要访问磁盘的服务器。

- **保护 SAN 磁盘配置访问权限－**通常，出于管理目的，可以通过 TCP/IP 或 HTTP（更常用）访问 SAN RAID 磁盘。您必须将对 SAN RAID 磁盘的管理访问权限仅限定于可信域中的系统，以阻止对磁盘的外部访问。此外，请更改磁盘阵列的默认密码。

- **安装 SAM-QFS 软件包－**首先，仅安装所需的那些软件包。例如，如果计划不运行 SAM，则**仅**安装 QFS 软件包。

  在不考虑此类更改所带来的安全隐患的情况下，完成安装之后，**不**应更改默认 SAM-QFS 文件和目录的权限以及属主。

- **客户机访问权限** – 如果计划配置共享客户机，请在 `hosts` 文件中确定哪些客户机必须对文件系统具有访问权限。请参见 `hosts.fs`(4) 手册页。**仅**配置需要访问正在配置的特定文件系统的那些主机。
- **强化 Oracle Solaris 元数据服务器** – 有关强化 Oracle Solaris OS 的信息，请参见《Oracle Solaris 10 安全准则》和《Oracle Solaris 11 安全准则》。至少，选择一个较好的 root 用户密码，安装最新版本的 Oracle Solaris OS，并保持修补程序为最新，特别是安全修补程序。
- **强化 Linux 客户机** – 查看 Linux 文档中有关如何强化 Linux 客户机的内容。至少，选择一个较好的 root 用户密码，安装最新版本的 Linux 操作系统，并保持修补程序为最新，特别是安全修补程序。
- **SAM-QFS 磁带安全** – 阻止从 SAM 外部对 SAM 磁带进行外部访问，或将此类访问仅限定于管理员。使用 FC 区域划分可将对磁带机的访问权限仅限定于 MDS（或者如果已配置了备份 MDS，则仅限定于潜在的 MDS）。此外，通过仅为 root 用户授予权限来限制磁带设备文件的访问权限。在未经授权的情况下访问 SAM 磁带可能会危及用户数据安全或破坏用户数据。
- **备份** – 使用 `samfsdump` 或 `qfsdump` 命令设置和执行 SAM-QFS 数据的备份。像对待 SAM 磁带那样，建议限制转储文件的访问权限。

安装 Sun SAM-Remote

有关安全安装 Sun SAM-Remote 软件的信息，请参见《Sun Storage Archive Manager 5.3 配置和管理指南》中的第 18 章 “使用 Sun SAM-Remote 软件”。

安装 SAM-QFS Manager

有关安全安装 SAM-QFS Manager 的信息，请参见《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》中的第 6 章 “安装和配置 SAM-QFS Manager”。

安装后配置

安装所有 SAM-QFS 软件包后，请仔细对照附录 A，安全部署核对表中的安全核对表。

◆ ◆ ◆ 第 3 章

Sun QFS 和 Sun Storage Archive Manager 安全功能

要避免潜在的安全威胁，客户在运行共享文件系统时必须考虑以下事项：

- 违反策略的文件系统数据泄漏
- 数据丢失
- 未检测到的数据修改

通过正确配置以及遵循附录 A，安全部署核对表中的安装后核对表，可最大程度地减少这些安全威胁。

安全模型

针对安全威胁提供保护的关键安全功能包括：

- **验证** – 确保仅为已授权的个人授予对系统和数据的访问权限。
- **授权** – 对系统特权和数据的访问控制。此功能基于验证构建，用于确保个人只获取相应的访问权限。
- **审计** – 允许管理员检测尝试的验证机制违规操作以及尝试的或成功的访问控制违规操作。

验证

SAM-QFS 使用基于主机的用户验证来控制可以执行管理任务的人员。使用 SAM-QFS Manager 的管理主要受已分配给各个用户的角色控制。使用命令行的管理仅限于 root 用户。

访问控制

SAM-QFS 中的访问控制分为以下两个部分：

- **管理访问控制**－控制可以对 SAM-QFS 执行管理操作的人员。这些控制基于通过 SAM-QFS Manager 分配给用户的角色。对于命令行操作，控制基于 root 用户权限。有关 SAM-QFS Manager 的更多信息，请参见《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》中的第 6 章 “安装和配置 SAM-QFS Manager”。
- **文件/目录访问控制**－SAM-QFS 实现符合 POSIX 标准且具有大量访问控制的文件系统。有关更多详细信息，请参见 SAM-QFS 文档。

开发者的安全注意事项

通常，开发者不会直接与 SAM-QFS 接触。两个例外是 `libsam` API 和 `libsamrpc` API。这两个 API 提供相同的功能。`libsam` 仅适用于本地计算机，而 `libsamrpc` 通过 `rpc(3)` 与 MDS 通信来实现请求的操作。验证以任一种方式创建的请求这一过程基于调用过程的 UID 和 GID。这些请求与通过命令行创建的请求具有相同的权限。确保具有可用于 MDS 和客户机系统的通用 UID 和 GID 空间。

有关更多信息，请参见《Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual》中的 `intro_libsam(3)` 和 `intro_libsamrpc(3)`。

◆ ◆ ◆ 附 录 A

安全部署核对表

使用本附录中的核对表安全部署 SAM-QFS 软件。

部署核对表

此安全核对表包括多个指导原则，用于帮助保护数据库安全。

- 对已分配有任何 SAM-QFS 角色的 root 帐户和任何其他帐户设置强密码。此指导原则包括：
  - SAM-QFS Manager 为其提供管理角色的所有帐户。
  - `acsss`、`acsdb` 和 `acssa` 用户 ID（如果正在使用）。
  - 所有磁盘阵列管理帐户。
- 如果对 SAM-QFS Manager 使用默认用户 `samadmin`，请立即将密码从默认安装的密码更改为强密码。请勿对 SAM-QFS Manager 使用 root 用户，而是根据需要将角色分配给其他用户帐户。也请使用强密码保护这些帐户。
- 在 WAN 边界路由器上安装端口过滤，以便防止在第 8 页中的 “一般安全原则”中列出的端口上的通信传入 MDS 或客户机，除非 Sun SAM-Remote 需要这样做。
- 以物理方式或通过 FC 区域划分方式隔离 FC 磁盘和磁带，以便只能从 MDS 和客户机访问磁盘，且只能从 MDS 和潜在 MDS 访问磁带。此安全做法可帮助防止由于意外覆写磁带或磁盘而造成的数据丢失事件。
- 检查 `/dev` 以确保除 root 用户以外其他用户不能访问磁带和磁盘设备文件。此做法可防止 SAM-QFS 数据遭到非正常访问或破坏。
- SAM-QFS 是 POSIX 文件系统，提供大量文件/目录权限，包括访问控制列表 (Access Control List, ACL)。根据需要使用这些权限可保护文件系统中的用户数据。有关更多信息，请参见 SAM-QFS 文档。
- 基于本地策略设置相应的一组备份转储。备份属于安全范畴，用于恢复意外丢失或由于某些违规操作而丢失的数据。您的备份应包括有关传输至异地时的相关策略。应像保护 SAM-QFS 磁带和磁盘那样保护备份。

参考文档

- 《Sun QFS 和 Sun Storage Archive Manager 5.3 安装指南》
- 《Sun QFS 文件系统 5.3 配置和管理指南》
- 《Sun Storage Archive Manager 5.3 配置和管理指南》
- 《Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual》