

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

安全指南

发行版 6.0

**E62080-01**

**2015 年 3 月**

---

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

**E62080-01**

版权所有 © 2015, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，则适用以下注意事项：

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.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应依照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

---

# 目录

---

前言 .....	5
目标读者 .....	5
文档可访问性 .....	5
印刷约定 .....	5
命令中的 shell 提示符示例 .....	5
<b>1. 概述 .....</b>	<b>7</b>
1.1. 产品概述 .....	7
1.2. 一般安全原则 .....	8
1.2.1. 保持软件为最新 .....	8
1.2.2. 限制关键服务的网络访问权限 .....	8
1.2.3. 遵循最小特权原则 .....	8
1.2.4. 监视系统活动 .....	8
1.2.5. 及时了解最新安全信息 .....	9
<b>2. 安全安装 .....</b>	<b>11</b>
2.1. 了解环境 .....	11
2.1.1. 需要保护哪些资源? .....	11
2.1.2. 要避免资源被哪些用户访问? .....	11
2.1.3. 如果对战略资源的保护失败, 将发生什么情况? .....	12
2.2. 建议的部署拓扑结构 .....	12
2.2.1. 安装 SAM-Remote .....	13
2.2.2. 安装管理器 GUI .....	13
2.2.3. 安装后配置 .....	13
<b>3. 安全功能 .....</b>	<b>15</b>
3.1. 安全模型 .....	15
3.1.1. 验证 .....	15
3.1.2. 访问控制 .....	15
<b>4. 开发者的安全注意事项 .....</b>	<b>17</b>
<b>A. 安全部署核对表 .....</b>	<b>19</b>



# 前言

---

《Oracle Hierarchical Storage Manager and StorageTek QFS Software 安全指南》包括有关 Oracle Hierarchical Storage Manager 和 QFS 产品的信息并介绍了应用程序的一般安全原则。

## 目标读者

本指南的目标读者是要使用 Oracle Hierarchical Storage Manager and StorageTek QFS Software 的安全功能以及要安全可靠地安装和配置 Oracle Hierarchical Storage Manager and StorageTek QFS Software 的所有人。

## 文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站：<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>。

### 获得 Oracle 支持

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>；如果您听力受损，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>。

## 印刷约定

下表介绍了本书中使用的印刷约定。

字样	含义	示例
<i>AaBbCc123</i>	命令名称和计算机屏幕输出	使用 <code>ls -a</code> 列出所有文件。
<b>AaBbCc123</b>	用户键入的内容，与计算机屏幕输出的显示不同	<code>machine_name% su</code>  <code>Password:</code>
<i>aabbcc123</i>	要使用实名或值替换的命令行占位符	删除文件的命令为 <code>rm filename</code> 。
<i>AaBbCc123</i>	要强调的新术语和术语	高速缓存是指存储在本地的副本。  请勿保存该文件。  注意：有些强调的项目在联机时以粗体显示。
《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。

Shell	提示符
Bashshell、Kornshell 和 BourneShell	\$
Bashshell、Kornshell 和 BourneShell 超级用户	#
Cshell	machine_name%
Cshell 超级用户	machine_name#

本章概述了 Oracle Hierarchical Storage Manager and StorageTek QFS Software 产品并介绍了应用程序的一般安全原则。

### 1.1. 产品概述

Oracle Hierarchical Storage Manager and StorageTek QFS Software 是一个共享文件系统，带有一个分层存储管理器。该产品包含以下主要组件：

#### **StorageTek QFS 软件包**

包括高性能 QFS 文件系统，可配置为独立文件系统或共享文件系统。配置为独立模式时，QFS 配置在单个系统上且没有共享客户机。QFS 使用标准 VFS vnode 操作与 Oracle Solaris 和 Linux 操作系统连接。

QFS 安装软件包包括 SUNWqfsr 和 SUNWqfsu。这两个软件包不包含 Oracle Hierarchical Storage Manager (HSM) 组件。

在没有任何共享客户机的情况下独立配置 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 时，除了与磁盘的 FC 连接，还有客户机与元数据服务器 (metadata server, MDS) 之间的 TCP/IP 连接。

#### **Oracle HSM 软件包**

包括 QFS 文件系统以及运行 Oracle HSM 所需的代码。Oracle HSM 安装软件包包括 SUNWsamfsr 和 SUNWsamfsu。如果不需要分层存储管理，可仅安装 StorageTek QFS 软件包。

#### **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。StorageTek 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 QFS 软件包或 SAM-QFS 软件包安装 SAM-Remote，但您必须单独启用和配置 SAM-Remote。有关 SAM-Remote 的更多信息，请参见 *Oracle Hierarchical Storage Manager and StorageTek QFS Software* 软件发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

#### **管理器图形用户界面**

管理器图形用户界面 (Graphical User Interface, GUI) fsmgr 在 MDS 上运行，可通过 Web 浏览器远程访问。通过端口 6789 (<https://hostname:6789>) 进行访问。

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。有关安装和配置管理器 GUI 的信息，请参见 *Oracle Hierarchical*

*Storage Manager and StorageTek QFS Software* 发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

## 1.2. 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。

### 1.2.1. 保持软件为最新

使运行的 Oracle HSM 版本保持最新。可以在 Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>) 找到软件的最新版本进行下载。

### 1.2.2. 限制关键服务的网络访问权限

Oracle HSM 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 SAM-Remote
- tcp/6789 是 HTTP 端口，用于浏览器连接 fsmgr
- tcp/5012 用于 sam-rpcd

---

注：

对于 MDS 双向客户机通信，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。

---

### 1.2.3. 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。管理器 GUI 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。从命令行执行管理任务需要 root 用户权限。

有关使用管理器 GUI 的更多信息，请参见 *Oracle Hierarchical Storage Manager and StorageTek QFS Software* 发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

### 1.2.4. 监视系统活动

监视系统活动以确定 Oracle HSM 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/\*

### 1.2.5. 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, 请访问 <http://www.us-cert.gov>。有关特定于 SAM-QFS 的信息, 请访问 [https://communities.oracle.com/portal/server.pt/community/sam\\_qfs\\_storage\\_archive\\_manager\\_and\\_sun\\_qfs/401](https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401)。及时解决最新安全问题的主要方式是运行最新版本的 Oracle HSM 软件。



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。

## 2.1. 了解环境

要更好地了解安全需求，必须回答以下问题：

### 2.1.1. 需要保护哪些资源？

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 Oracle HSM 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 Oracle HSM 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 Oracle HSM 方式）存在安全风险，因为这样做会绕过正常的 Oracle HSM 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。

#### Oracle HSM 磁带

单独访问磁带（通常位于磁带库中，关闭 Oracle HSM 文件系统时会在其中写入文件数据）存在安全风险。

#### Oracle HSM 转储磁带

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。

#### Oracle HSM 元数据服务器 (metadata server, MDS)

Oracle HSM 客户机需要通过 TCP/IP 访问 MDS。但是，请确保阻止外部 WAN 访问客户机。

#### 配置文件和设置

必须阻止管理员之外的人员访问 Oracle HSM 配置设置。通常，Oracle HSM 会在您使用管理器 GUI 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。

### 2.1.2. 要避免资源被哪些用户访问？

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。

### 2.1.3. 如果对战略资源的保护失败，将发生什么情况？

保护战略资源失败可能源于非正常访问（在没有正常 Oracle HSM 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。

## 2.2. 建议的部署拓扑结构

本节介绍了如何安全地安装和配置基础结构组件。有关安装 Oracle HSM 的信息，请参见 *Oracle Hierarchical Storage Manager* 发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

安装和配置 Oracle HSM 时请注意以下几点：

#### 独立的元数据网络

要将 Oracle HSM 客户机连接到 MDS 服务器，请提供一个独立的 TCP/IP 网络以及未连接到任何 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 Oracle HSM 端口的通信。请参见第 1.2.2 节“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 Oracle HSM 磁盘的任何服务器访问这些磁盘。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

通常可通过 TCP/IP（更典型的是 HTTP）访问 SAN RAID 磁盘执行管理操作。您必须将对 SAN RAID 磁盘的管理访问权限仅限于可信域中的系统，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 Oracle HSM 软件包

首先，仅安装所需的软件包。例如，如果不需要分层存储管理，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 Oracle HSM 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。仅配置需要访问所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。

### Oracle HSM 磁带安全

防止从 Oracle HSM 外部对 Oracle HSM 磁带进行访问，或将此类访问权限限定于管理员。使用 FC 区域划分可将磁带机的访问权限仅限于 MDS（或者如果已配置了备份 MDS，则仅限于潜在的 MDS）。要配置为使用分布式 I/O 的 Solaris 客户机需要访问磁带机。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 Oracle HSM 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 Oracle HSM 数据备份。像对 Oracle HSM 磁带所建议的那样，限制转储磁带的访问权限。

## 2.2.1. 安装 SAM-Remote

有关安全地安装 SAM-Remote 软件的信息，请参见 *Oracle Hierarchical Storage Manager and StorageTek QFS Software* 发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

## 2.2.2. 安装管理器 GUI

有关安全地安装管理器 GUI 的信息，请参见 *Oracle Hierarchical Storage Manager and StorageTek QFS Software* 发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

## 2.2.3. 安装后配置

安装任意 Oracle HSM 软件包之后，执行附录 A, [安全部署核对表](#) 中的安全核对表



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。

## 3.1. 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。

### 3.1.1. 验证

Oracle HSM 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。使用管理器 GUI 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。

### 3.1.2. 访问控制

Oracle HSM 中的访问控制分为两个部分：

- 管理访问控制—控制可以对 Oracle HSM 执行管理操作的人员。这些控制基于通过管理器 GUI 分配给用户的角色。对于命令行操作，控制基于 root 用户权限。有关管理器 GUI 的更多信息，请参见 *Oracle Hierarchical Storage Manager and StorageTek QFS Software* 软件发行版 6.0 客户文档库，网址为：<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>
- 文件/目录访问控制—Oracle HSM 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 Oracle HSM 文档。





---

---

## 开发者的安全注意事项

通常，开发者不会直接与 Oracle HSM 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 *intro\_libsam(3)* 和 *intro\_libsamrpc(3)* 手册页。

---

---

# 附录 A

---

## 安全部署核对表

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。

1. 对已分配有任何 Oracle HSM 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：
  - 管理器 GUI 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。
2. 如果对管理器 GUI 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。请勿对管理器 GUI 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其他帐户。
3. 在 WAN 边界路由器上安装端口过滤，以便防止在 [第 1.2 节“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。
4. 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。
5. 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 Oracle HSM 数据遭到非正常访问或破坏。
6. Oracle HSM 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 Oracle HSM 文档。
7. 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 Oracle HSM 磁带和磁盘那样保护备份。

---