

StorageTek Storage Archive Manager
and StorageTek QFS Software Security Guide
Release 5.4
E51255-01

August 2014

E51255-01

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Typographic Conventions	v
Shell Prompts in Command Examples	vi
 1 Overview	
Product Overview	1-1
General Security Principles	1-2
Keep Software Up To Date	1-2
Restrict Network Access to Critical Services	1-2
Follow the Principle of Least Privilege	1-2
Monitor System Activity	1-2
Keep Up To Date on Latest Security Information	1-3
 2 Secure Installation	
Understand Your Environment	2-1
Which resources need to be protected?	2-1
From whom are the resources being protected?	2-2
What will happen if the protections on strategic resources fail?	2-2
Recommended Deployment Topologies	2-2
Installing StorageTek SAM-Remote	2-3
Installing SAM-QFS Manager	2-3
Post-Installation Configuration	2-3
 3 Security Features	
The Security Model	3-1
Authentication	3-1
Access Control	3-1
 4 Security Considerations for Developers	
 A Secure Deployment Checklist	

Preface

Oracle's StorageTek Storage Archive Manager and StorageTek QFS software Security Guide includes information about the Storage Archive Manager and QFS (SAM-QFS) product and explains the general principles of application security.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of SAM-QFS.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

Typeface	Meaning	Example
AaBbCc123	Names of commands and on screen computer output	Use <code>ls -a</code> to list all files.
AaBbCc123	user input that you type when accompanied by screen computer output	machine_name% su Password:
<i>aabbcc123</i>	Placeholder, replace with a real name or value	The command to remove a file is <i>rm filename</i> .

Typeface	Meaning	Example
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do not save the file. Note some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

Shell	Prompt
Bashshell, Kornshell, and Bournesshell	\$
Bashshell, Kornshell, and Bournesshell for superuser	#
Cshell	machine_name%
Cshell for superuser	machine_name#

Overview

This chapter provides an overview of the StorageTek QFS and Storage Archive Manager (SAM-QFS) product and explains the general principles of application security.

Product Overview

SAM-QFS is a shared file system with a hierarchical storage manager. SAM-QFS consists of the following major components:

StorageTek QFS package

Includes the high-performance QFS file system that can be configured either standalone or shared. When configured as standalone, QFS is configured on a single system and not with shared clients. QFS uses standard VFS vnode operations to interface with the Oracle Solaris and Linux operating systems.

The QFS installation packages are SUNWqfsr and SUNWqfsu. These packages do not include the hierarchical storage archive manager (SAM) component.

Configuring QFS standalone with no shared clients has the smallest security exposure. This configuration does not run daemons and does not have any remote connections other than Fibre Channel (FC) to disk. Configuring QFS shared includes FC connections to disk and a TCP/IP connection between clients and the metadata server (MDS).

SAM-QFS package

Includes the QFS file system and the code that is required to run SAM. The SAM-QFS installation packages are SUNWsamfsr and SUNWsamfsu. If SAM is not required, install *only* the Sun QFS package.

StorageTek SAM-Remote

Permits access to remote tape libraries and drives by means of TCP/IP wide area network (WAN) connections. StorageTek SAM-Remote provides a form of disaster recovery by remotely locating tape facilities. You can install SAM-Remote with either the QFS or SAM-QFS packages, but you must enable and configure SAM-Remote separately. For more information about SAM-Remote, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

SAM-QFS tools package

Installs tools and man pages in the /opt/SUNWsamfs/tools directory. None of these tools have special privileges, but they all require root access to use. The installation package is SUNWsamtp.

SAM-QFS Manager

The SAM-QFS Manager, fsmgr, runs on the MDS and is accessed remotely through a web browser. Access is granted through port 6789 (<https://hostname:6789>).

To use fsmgr, you must log in as a valid user on the MDS and add certain roles to the user account. For information about installing and configuring the SAM-QFS Manager, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

General Security Principles

The following sections describe the fundamental principles that are required to use any application securely.

Keep Software Up To Date

Stay current with the version of SAM-QFS that you run. You can find current versions of the software for download at the Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>).

Restrict Network Access to Critical Services

SAM-QFS uses the following TCP/IP ports:

- tcp/7105 is used for metadata traffic between the client and the MDS
- tcp/1000 is used for SAM-Remote
- tcp/6789 is the HTTP port that is used for a browser to contact to fsmgr
- tcp/5012 is used for sam-rpcd

Note: For MDS bidirectional client traffic, consider setting up a separate network that is not interconnected to the outside WAN. This configuration prevents exposure from outside threats and also ensures that outside traffic does not limit MDS performance.

Follow the Principle of Least Privilege

Grant the user or administrator the least privilege that is required to accomplish the task to be performed. The SAM-QFS Manager has various roles that can be granted to users. These roles grant varying types and amounts of privilege. Performing SAM-QFS administration tasks from the command line requires root permission.

For more information about using the SAM-QFS Manager, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Monitor System Activity

Monitor system activity to determine how well SAM-QFS is operating and whether it is logging any unusual activity. Check the following log files:

- /var/adm/messages

- /var/opt/SUNWsamfs/sam-log
- /var/opt/SUNWsamfs/archiver.log, see /etc/opt/SUNWsamfs/archiver.cmd
- /var/opt/SUNWsamfs/recycler.log, see /etc/opt/SUNWsamfs/recycler.cmd
- /var/opt/SUNWsamfs/releaser.log, see /etc/opt/SUNWsamfs/releaser.cmd
- /var/opt/SUNWsamfs/stager.log, see /etc/opt/SUNWsamfs/stager.cmd
- /var/opt/SUNWsamfs/trace/*

Keep Up To Date on Latest Security Information

You can access several sources of security information. For security information and alerts for a large variety of software products, see <http://www.us-cert.gov>. For information specific to SAM-QFS, see https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401. The primary way to keep up to date on security matters is to run the most current version of the SAM-QFS software.

Secure Installation

This chapter outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Understand Your Environment

To better understand security needs, the following questions must be asked:

Which resources need to be protected?

You can protect many of the resources in the production environment. Consider the type of resources that you want to protect when determining the level of security to provide.

When using SAM-QFS, protect the following resources:

Metadata and primary data disk

These disk resources are used to build SAM-QFS file systems. They are typically Fibre Channel (FC) connected. Independent access to these disks (not by means of SAM-QFS) presents a security risk because normal SAM-QFS file and directory permissions are bypassed. This type of external access might be from a rogue system that reads or writes the FC disks, or from an internal system that accidentally provides non-root access to raw device files.

SAM tapes

Independent access to tapes, typically in a tape library, where file data is written when staged off a SAM file system is a security risk.

SAM-QFS dump tapes

File system dumps that are created from samfsdump contain data and metadata. This data and metadata should be protected from access other than by the system administrator during a routine dump or restore activity.

SAM-QFS metadata server (MDS)

SAM-QFS clients require TCP/IP access to the MDS. However, ensure that the clients are protected from external WAN access.

Configuration files and settings

SAM-QFS configuration settings must be protected from non-administrator access. In general, these settings are protected automatically by SAM-QFS when you use the SAM-QFS Manager. Note that making the configuration files writable to non-administrative users presents a security risk.

From whom are the resources being protected?

In general, the resources described in the previous section must be protected from all non-root or non-administrator access on a configured system, or from a rogue external system that can access these resources by means of the WAN or FC fabric.

What will happen if the protections on strategic resources fail?

Protection failures against strategic resources can range from inappropriate access (access to data outside of normal SAM-QFS POSIX file permissions) to data corruption (writing to disk or tape outside of normal permissions).

Recommended Deployment Topologies

This section describes how to install and configure an infrastructure component securely.

For information about installing SAM-QFS, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Consider the following points when installing and configuring SAM-QFS:

Separate metadata network

To connect SAM-QFS clients to the MDS servers, provide a separate TCP/IP network and switch hardware that is not connected to any WAN. Because the metadata traffic is implemented by using TCP/IP, an external attack on this traffic is theoretically possible. Configuring a separate metadata network mitigates this risk and also provides enhanced performance. The improved performance is achieved by providing a guaranteed data path to the metadata. If a separate metadata network is infeasible, at least deny traffic to the SAM-QFS ports from the external WAN and any untrusted hosts on the network. See "[Restrict Network Access to Critical Services](#)" on page 1-2.

FC zoning

Use FC zoning to deny access to the SAM-QFS disks from any server that does not require access to the disks. Preferably, use a separate FC switch to physically connect only to the servers that require access.

Safeguard SAN disks configuration access

SAN RAID disks can usually be accessed for administrative purposes by means of TCP/IP or more typically HTTP. You must protect the disks from external access by limiting the administrative access to SAN RAID disks to systems only within a trusted domain. Also, change the default password on the disk arrays.

Install the SAM-QFS package

First, install only those packages that you require. For example, if you do not plan to run SAM, install only the QFS packages. The default SAM-QFS file and directory permissions and owners should not be changed after installation without considering the security implications of such changes.

Client access

If you plan to configure shared clients, determine which clients must have access to the file system in the hosts file. See the `hosts.fs(4)` man page. Configure only those hosts that require access to the particular file system being configured.

Harden Oracle Solaris metadata server

For information about hardening the Oracle Solaris OS, see the Oracle Solaris 10 Security Guidelines and the Oracle Solaris 11 Security Guidelines. At a minimum, choose a good root password, install an up-to-date version of the Oracle Solaris OS, and keep current on patches, particularly security patches.

Harden Linux clients

Check the Linux documentation about how to harden Linux clients. At a minimum, choose a good root password, install an up-to-date version of the Linux operating system, and keep current on patches, particularly security patches.

SAM-QFS tape security

Prevent external access to SAM tapes from outside of SAM, or limit such access to administrators only. Use FC zoning to limit the access to tape drives to only the MDS (or potential MDS if a backup MDS is configured). Solaris clients that will be configured to use distributed I/O will need access to tape drives. Also, limit tape device file access by granting root only permissions. Unauthorized access to SAM tapes can compromise or destroy user data.

Backups

Set up and perform backups of SAM-QFS data by using the `samfsdump` or `qfstdump` command. Limit access to dump tapes as is recommended for SAM tapes.

Installing StorageTek SAM-Remote

For information about securely installing the StorageTek SAM-Remote software, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Installing SAM-QFS Manager

For information about securely installing the SAM-QFS Manager, *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Post-Installation Configuration

After installing any of the SAM-QFS packages, go through the security checklist in [Appendix A, "Secure Deployment Checklist."](#)

Security Features

To avoid potential security threats, customers operating a shared file system must be concerned about:

- Disclosure of file system data in violation of policy
- Loss of data
- Undetected modification of data

These security threats can be minimized by proper configuration and by following the post-installation checklist in [Appendix A, "Secure Deployment Checklist."](#)

The Security Model

The critical security features that provide protections against security threats are:

- Authentication – Ensures that only authorized individuals are granted access to the system and data.
- Authorization – Access control to system privileges and data. This feature builds on authentication to ensure that individuals get only appropriate access.
- Audit – Enables administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.

Authentication

SAM-QFS uses host-based user authentication to control who can perform administration tasks. Administration using the SAM-QFS Manager is mainly controlled by roles which are assigned to various users. Administration using the command line is limited to the root user.

Access Control

Access control in SAM-QFS is divided into two parts:

- Administrative access control – Controls who can take administrative actions for SAM-QFS. The controls are based on roles that are assigned to users through SAM-QFS Manager. For command-line operations, controls are based on root permissions. For more information about SAM-QFS Manager, see the *StorageTek Storage Archive Manager and StorageTek QFS Software Release 5.4 Customer Documentation Library* at:
<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

- File/directory access control – SAM-QFS implements a POSIX compliant file system that has a rich set of access controls. See the SAM-QFS documentation for more details.

Security Considerations for Developers

Developers generally do not interface directly with SAM-QFS. The two exceptions are the `libsam` API and the `libsamrpc` API. These two APIs provide the same functionality. `libsam` is for a local machine only, while `libsamrpc` communicates to the MDS through `rpc(3)` to implement the requested actions. Authentication of requests made by either method is based on the UID and GID of the calling process. They have the same permissions as the requests made through the command line. Make sure you have a common UID and GID space for MDS and the client systems.

For more information, see the `intro_libsam(3)` and `intro_libsamrpc(3)` man pages.

Secure Deployment Checklist

This security checklist includes guidelines that help secure your database.

1. Set strong passwords for root and any other accounts that have any SAM-QFS roles assigned to them. This guideline includes:
 - Any accounts that are given administrative roles by the SAM-QFS Manager.
 - `acsss`, `acsdb`, and `acssa` User IDs (if being used).
 - Any disk array administrative accounts.
2. If using the default user `samadmin` with the SAM-QFS Manager, change the password right away from the default installed password to a strong password. Do not use root with the SAM-QFS Manager, but rather assign roles as needed to other user accounts. Protect other accounts also with strong passwords.
3. Install port filtering on WAN edge routers to prevent traffic on ports listed in "[General Security Principles](#)" on page 1-2 from coming in to the MDS or clients, except as needed for SAM-Remote.
4. Segregate FC disks and tapes either physically or through FC zoning so that disks are accessible only from the MDS and clients, and tapes are accessible only from the MDS and potential MDS. This security practice helps prevent loss-of-data accidents as a result of accidental overwriting of tape or disk.
5. Check `/dev` to ensure that tape and disk device files are not accessible to users other than root. This practice prevents SAM-QFS data from being accessed inappropriately or destroyed.
6. SAM-QFS is a POSIX file system, and provides a rich set of file/directory permissions including Access Control Lists (ACLs). Use them as needed to protect user data on the file system. For more information, see the SAM-QFS documentation.
7. Set up an appropriate set of backup dumps based on local policy. Backups are part of security and provide a way of restoring data lost either accidentally, or through some breach. Your backup should include some policy while being transported to an offsite location. Backups need to be protected to the same degree as SAM-QFS tapes and disk.

