Sun QFS および Sun Storage Archive Manager 5.3 セキュリティーガイド

Part No: E35998
2012 年 6 月

ORACLE

Copyright © 2011, 2012, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

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.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

120817@25097

目次

はじめに

『Sun QFS および Sun Storage Archive Manager セキュリティーガイド』には、Sun QFS および Storage Archive Manager (SAM-QFS) 製品に関する情報が含まれており、アプリケーションのセキュリティーの一般的な原則が説明されています。

Oracle Support へのアクセス

Oracle のお客様は、My Oracle Support から電子サポートにアクセスできます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info にアクセスするか、または聴覚障害をお持ちの場合は http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs にアクセスしてください。

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 P–1　表記上の規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 system%
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	system% **su** password:
AaBbCc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、rm *filename* と入力します。
『 』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。

表 P–1 表記上の規則 (続き)

字体または記号	意味	例
「」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	`sun% grep '^#define \` `XV_VERSION_STRING'`

Oracle Solaris OS に含まれるシェルで使用する、UNIX のデフォルトのシステムプロンプトとスーパーユーザープロンプトを次に示します。コマンド例に示されるデフォルトのシステムプロンプトは、Oracle Solaris のリリースによって異なります。

- C シェル

  ```
  machine_name% command y|n [filename]
  ```

- C シェルのスーパーユーザー

  ```
  machine_name# command y|n [filename]
  ```

- Bash シェル、Korn シェル、および Bourne シェル

  ```
  $ command y|n [filename]
  ```

- Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー

  ```
  # command y|n [filename]
  ```

[ ] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

◆ ◆ ◆ 第 1 章

1 Sun QFS および Sun Storage Archive Manager の概要

この章では、Sun QFS および Storage Archive Manager (SAM-QFS) 製品の概要と、アプリケーションのセキュリティーの一般的な原則について説明します。

製品の概要

SAM-QFS は、階層ストレージ管理プログラムを備えた共有ファイルシステムです。SAM-QFS は、次の主なコンポーネントで構成されています:

- **Sun QFS** パッケージ – スタンドアロンまたは共有として構成できる高性能な Sun QFS ファイルシステムが含まれています。スタンドアロンとして構成された場合、Sun QFS は 1 つのシステム上に構成され、共有クライアントは含まれません。Sun QFS は、標準の VFS vnode 操作を使用して、Oracle Solaris および Linux オペレーティングシステムとのインタフェースの役割を果たします。

  Sun QFS インストールパッケージは `SUNWqfsr` および `SUNWqfsu` です。これらのパッケージには、階層型 Storage Archive Manager (SAM) コンポーネントは含まれません。

  Sun QFS をスタンドアロンとして構成し、共有クライアントが含まれない場合、セキュリティーエクスポージャーは最小限に抑えられます。この構成ではデーモンは実行されず、ファイバチャネル (FC) からディスクへの接続以外のリモート接続も存在しません。QFS を共有として構成した場合は、ディスクへの FC 接続、およびクライアントとメタデータサーバー (MDS) の間の TCP/IP 接続が含まれます。

- **SAM-QFS** パッケージ – Sun QFS ファイルシステムと、SAM を実行するために必要なコードが含まれています。

  SAM-QFS インストールパッケージは `SUNWsamfsr` および `SUNWsamfsu` です。SAM が必要でない場合は、Sun QFS パッケージのみをインストールしてください。

- **Sun SAM-Remote** – TCP/IP 広域ネットワーク (WAN) 接続を使用した、リモートのテープライブラリおよびドライブへのアクセスを許可します。Sun SAM-Remote では、テープ設備をリモートに配置することによる障害回復の 1 つの形式が提供

されます。Sun SAM-Remote は Sun QFS パッケージまたは SAM-QFS パッケージとともにインストールできますが、Sun SAM-Remote は個別に有効にして構成する必要があります。Sun SAM-Remote の詳細は、『Sun Storage Archive Manager 5.3 構成および管理ガイド』の第 18 章「Sun SAM-Remote ソフトウェアの使用」を参照してください。

- **SAM-QFS** ツールパッケージ – ツールとマニュアルページを `/opt/SUNWsamfs/tools` ディレクトリにインストールします。これらのどのツールにも特殊な特権はありませんが、使用するには、すべてのツールに root アクセスが必要です。インストールパッケージは `SUNWsamtp` です。
- **SAM-QFS Manager** – SAM-QFS Manager (`fsmgr`) は MDS 上で実行され、Web ブラウザ経由でリモートからアクセスされます。アクセスは、ポート 6789 経由で付与されます (`https://`*hostname*`:6789`)。

  `fsmgr` を使用するには、MDS 上の有効なユーザーとしてログインし、そのユーザーアカウントに特定の役割を追加する必要があります。SAM-QFS Manager のインストールと構成については、『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』の第 6 章「SAM-QFS Manager のインストールと構成」を参照してください。

一般的なセキュリティーの原則

以降のセクションでは、すべてのアプリケーションをセキュアに使用するために必要な基本原則について説明します。

ソフトウェアを最新の状態に維持する

実行する SAM-QFS のバージョンを最新の状態に維持してください。ソフトウェアの最新バージョンは、Oracle Software Delivery Cloud (`https://edelivery.oracle.com/`) からダウンロードできます。

ネットワークアクセスを重要なサービスに制限する

SAM-QFS では、次の TCP/IP ポートを使用します:

- `tcp/7105` は、クライアントと MDS の間のメタデータトラフィックに使用されます
- `tcp/1000` は、Sun SAM-Remote に使用されます
- `tcp/6789` は、ブラウザが `fsmgr` に接続するために使用される HTTPS ポートです
- `tcp/5012` は、`sam-rpcd` に使用されます

注 – MDS クライアントのトラフィックのために、外部の WAN に相互接続されていない個別のネットワークを設定することを考慮してください。この構成によって、外部の脅威からのエクスポージャーが回避されるだけでなく、MDS のパフォーマンスが外部のトラフィックによって制限されることもなくなります。

最小特権の原則に従う

ユーザーまたは管理者には、実行されるタスクを達成するために必要な最小特権を付与してください。SAM-QFS Manager には、ユーザーに付与できるさまざまな役割があります。これらの役割では、さまざまなタイプと量の特権が付与されます。SAM-QFS の管理タスクをコマンド行から実行するには、root アクセス権が必要です。

SAM-QFS Manager の使用の詳細は、『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』の第 6 章「SAM-QFS Manager のインストールと構成」を参照してください。

システムの動作状態を監視する

システムの動作状態を監視して、SAM-QFS がどれだけ適切に動作しているか、および何らかの異常な操作がログに記録されているかどうかを判断してください。次のログファイルを確認します:

- `/var/adm/messages`
- `/var/opt/SUNWsamfs/sam-log`
- `/var/opt/SUNWsamfs/archiver.log` (`/etc/opt/SUNWsamfs/archiver.cmd` を参照)
- `/var/opt/SUNWsamfs/recycler.log` (`/etc/opt/SUNWsamfs/recycler.cmd` を参照)
- `/var/opt/SUNWsamfs/releaser.log` (`/etc/opt/SUNWsamfs/releaser.cmd` を参照)
- `/var/opt/SUNWsamfs/stager.log` (`/etc/opt/SUNWsamfs/stager.cmd` を参照)
- `/var/opt/SUNWsamfs/trace/*`

最新のセキュリティー情報を維持する

セキュリティー情報の複数のソースにアクセスできます。さまざまなソフトウェア製品のセキュリティー情報や警告については、`http://www.us-cert.gov` を参照してください。SAM-QFS に固有の情報については、`http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss` を参照してください。最新のセキュリティー情報を維持するための主な方法は、SAM-QFS ソフトウェアの最新のバージョンの実行です。

◆ ◆ ◆ 第 2 章

2 セキュアなインストールおよび構成

この章では、セキュアなインストールのための計画プロセスの概要と、システムに推奨されるいくつかの配備トポロジについて説明します。

インストールの概要

環境の理解

セキュリティーのニーズをよりよく理解するために、次の内容を確認してください:

- どのリソースを保護しているか。

  本稼働環境内の多くのリソースを保護できます。提供するセキュリティーのレベルを決定する場合は、保護するリソースの種類を考慮してください。

  SAM-QFS を使用している場合は、次のリソースを保護します:

  - メタデータおよびプライマリデータディスク – これらのディスクリソースは、SAM-QFS ファイルシステムを構築するために使用されます。これらは通常、ファイバチャネル (FC) に接続されています。これらのディスクに (SAM-QFS を使用せずに) 独立してアクセスすると、通常の SAM-QFS ファイルおよびディレクトリアクセス権がバイパスされるため、セキュリティーリスクが発生します。この種類の外部アクセスは、FC ディスクを読み書きする悪意のあるシステムか、または raw デバイスファイルへの root 以外のアクセスを誤って提供している内部システムから来ている可能性があります。
  - **SAM** テープ – テープ (通常は、SAM ファイルシステムへの書き込み時にファイルデータが書き込まれるテープライブラリ内に存在します) への独立したアクセスはセキュリティーリスクになります。

- **SAM-QFS** ダンプファイル – `samfsdump` から作成されるファイルシステムダンプには、データとメタデータが含まれています。このデータとメタデータは、日常のダンプまたは復元操作中にシステム管理者以外からアクセスされないように保護されるべきです。
- **SAM-QFS** メタデータサーバー **(MDS)** – SAM-QFS クライアントには、MDS への TCP/IP アクセスが必要です。ただし、クライアントが外部の WAN アクセスから保護されていることを確認してください。
- 構成ファイルおよび設定 – SAM-QFS の構成設定は、管理者以外のアクセスから保護する必要があります。一般に、SAM-QFS Manager を使用している場合、これらの設定は SAM-QFS によって自動的に保護されます。管理ユーザー以外のユーザーが書き込むことのできる構成ファイルを作成すると、セキュリティーリスクが発生することに注意してください。

- リソースをだれから保護しているか。

  一般に、前のセクションで説明したリソースは、構成されているシステム上の root 以外または管理者以外のすべてのアクセスから、あるいは WAN または FC ファブリックを使用してこれらのリソースにアクセスできる悪意のある外部システムから保護する必要があります。
- 戦略的なリソースに対する保護が失敗したらどうなるか。

  戦略的なリソースに対する保護の失敗には、不適切なアクセス (通常の SAM-QFS POSIX ファイルアクセス権の外部でのデータへのアクセス) から、データ破壊 (通常のアクセス権の外部でのディスクまたはテープへの書き込み) までさまざまな場合があります。

推奨される配備トポロジ

SAM-QFS のインストール

このセクションでは、インフラストラクチャーコンポーネントをセキュアにインストールおよび構成する方法について説明します。

SAM-QFS のインストールについては、『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』の第 5 章「Sun QFS と SAM-QFS のインストール」を参照してください。

SAM-QFS をインストールおよび構成する場合は、次の点を考慮してください:

- 個別のメタデータネットワーク – SAM-QFS クライアントを MDS サーバーに接続するには、どの WAN にも接続されていない個別の TCP/IP ネットワークとスイッチハードウェアを提供してください。メタデータトラフィックは TCP/IP を使用して実装されるため、このトラフィックに対する外部の攻撃が理論的には可能です。個別のメタデータネットワークを構成すると、このリスクが軽減されるだけでなく、パフォーマンスも向上します。このパフォーマンスの向上は、メタデータへの保証されたデータパスを提供することによって達成されます。個別のメタデータネットワークを実現できない場合は、少なくとも、外部の WAN や、ネットワーク上のすべての信頼できないホストから SAM-QFS ポートへのトラフィックを拒否してください。8 ページの「ネットワークアクセスを重要なサービスに制限する」を参照してください。
- **FC** ゾーニング – SAM-QFS ディスクへのアクセスを必要としないすべてのサーバーからこれらのディスクへのアクセスを拒否するには、FC ゾーニングを使用します。できれば、個別の FC スイッチを使用して、アクセスを必要とするサーバーにのみ物理的に接続してください。
- **SAN** ディスク構成へのアクセスの保護 – SAN RAID ディスクには通常、TCP/IP か、またはより一般的には HTTP を使用して管理上の目的でアクセスできます。SAN RAID ディスクへの管理アクセスを信頼できるドメイン内のシステムのみに制限することによって、ディスクを外部アクセスから保護する必要があります。また、ディスクアレイ上のデフォルトのパスワードも変更してください。
- **SAM-QFS** パッケージのインストール – まず、必要なパッケージのみをインストールします。たとえば、SAM を実行することを予定していない場合は、QFS パッケージのみをインストールします。

  デフォルトの SAM-QFS ファイルおよびディレクトリアクセス権や所有者の、インストール後の変更は、このような変更のセキュリティーへの影響を考慮せずに行うべきではありません。
- クライアントアクセス – 共有クライアントを構成することを予定している場合は、`hosts` ファイルで、どのクライアントがファイルシステムにアクセスできる必要があるかを決定してください。`hosts.fs(4)` のマニュアルページを参照してください。構成されている特定のファイルシステムへのアクセスを必要とするホストのみを構成します。
- **Oracle Solaris** メタデータサーバーの強化 – Oracle Solaris OS の強化については、Oracle Solaris 10 のセキュリティーガイドラインおよび Oracle Solaris 11 セキュリティーガイドラインを参照してください。少なくとも、適切な root パスワードを選択し、最新バージョンの Oracle Solaris OS をインストールし、さらにパッチ (特に、セキュリティーパッチ) を最新の状態に維持してください。
- **Linux** クライアントの強化 – Linux クライアントを強化する方法については、Linux のドキュメントを確認してください。少なくとも、適切な root パスワードを選択し、最新バージョンの Linux オペレーティングシステムをインストールし、さらにパッチ (特に、セキュリティーパッチ) を最新の状態に維持してください。

- **SAM-QFS** テープのセキュリティー – SAM の外部から SAM テープへの外部アクセスを防ぐか、またはこのようなアクセスを管理者のみに制限します。テープドライブへのアクセスを MDS (または、バックアップ MDS が構成されている場合は潜在的な MDS) のみに制限するには、FC ゾーニングを使用します。また、root のみのアクセス権を付与することによって、テープデバイスファイルへのアクセスも制限します。SAM テープへの未承認のアクセスによって、ユーザーデータが危険にさらされたり、破棄されたりする場合があります。
- バックアップ – `samfsdump` または `qfsdump` コマンドを使用して、SAM-QFS データのバックアップを設定および実行します。SAM テープに推奨されているのと同様に、ダンプファイルへのアクセスを制限します。

Sun SAM-Remote のインストール

Sun SAM-Remote ソフトウェアのセキュアなインストールについては、『Sun Storage Archive Manager 5.3 構成および管理ガイド』の第 18 章「Sun SAM-Remote ソフトウェアの使用」を参照してください。

SAM-QFS Manager のインストール

SAM-QFS Manager のセキュアなインストールについては、『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』の第 6 章「SAM-QFS Manager のインストールと構成」を参照してください。

インストール後の構成

いずれかの SAM-QFS パッケージをインストールしたら、付録 A「セキュアな配備のチェックリスト」にあるセキュリティーのチェックリストに従ってください。

◆ ◆ ◆ 第 3 章

Sun QFS および Sun Storage Archive Manager のセキュリティー機能

潜在的なセキュリティーの脅威を回避するために、共有ファイルシステムを操作しているお客様は次の点に注意を払う必要があります:

- ポリシーに違反しているファイルシステムデータの公開
- データの損失
- 検出されないデータ変更

これらのセキュリティーの脅威は、適切な構成によって、および付録 A「セキュアな配備のチェックリスト」にあるインストール後のチェックリストに従うことによって最小限に抑えることができます。

セキュリティーモデル

セキュリティーの脅威からの保護を実現するための重要なセキュリティー機能は次のとおりです:

- 認証 – 承認された個人にのみシステムおよびデータへのアクセス権が付与されることを保証します。
- 承認 – システム特権およびデータへのアクセス制御。この機能は、認証に基づいて、個人が適切なアクセスのみを取得することを保証します。
- 監査 – 管理者が認証メカニズムの侵害の試行や、アクセス制御の侵害の試行または成功を検出できるようにします。

認証

SAM-QFS は、ホストベースのユーザー認証を使用して、だれが管理タスクを実行できるかを制御します。SAM-QFS Manager を使用した管理は、主に、さまざまなユーザーに割り当てられた役割によって制御されます。コマンド行を使用した管理は、root ユーザーに制限されます。

アクセス制御

SAM-QFS でのアクセス制御は、次の 2 つの部分に分けられます:

- 管理アクセスの制御 – だれが SAM-QFS の管理操作を実行できるかを制御します。これらの制御は、SAM-QFS Manager を通してユーザーに割り当てられた役割に基づいています。コマンド行の操作の場合、制御は root アクセス権に基づいています。SAM-QFS Manager の詳細は、『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』の第 6 章「SAM-QFS Manager のインストールと構成」を参照してください。
- ファイル/ディレクトリのアクセス制御 – SAM-QFS には、一連の豊富なアクセス制御を備えた POSIX 準拠のファイルシステムが実装されています。詳細は、SAM-QFS のドキュメントを参照してください。

開発者のためのセキュリティーの注意点

開発者は通常、SAM-QFS と直接の接点を持つことはありません。この例外として、`libsam` API と `libsamrpc` API の 2 つがあります。これらの 2 つの API は同じ機能を提供します。`libsam` がローカルマシン専用であるのに対して、`libsamrpc` は、リクエストされた動作を実装するために `rpc(3)` 経由で MDS と通信します。どちらかの方法によって実行されるリクエストの認証は、呼び出し元プロセスの UID と GID に基づいています。これらは、コマンド行から実行されたリクエストと同じアクセス権を持っています。MDS とクライアントシステムに共通の UID および GID スペースがあることを確認してください。

詳細は、『Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual』の `intro_libsam(3)` および `intro_libsamrpc(3)` を参照してください。

◆ ◆ ◆ 付録 A

セキュアな配備のチェックリスト

SAM-QFS ソフトウェアをセキュアに配備するには、この付録のチェックリストを使用します。

配備のチェックリスト

このセキュリティーのチェックリストには、データベースのセキュリティー保護に役立つガイドラインが含まれています。

- root や、いずれかの SAM-QFS の役割が割り当てられているその他のすべてのアカウントには強力なパスワードを設定してください。このガイドラインには次が含まれます:
  - SAM-QFS Manager によって管理役割が与えられているすべてのアカウント。
  - `acsss`、`acsdb`、および `acssa` ユーザー ID (使用されている場合)。
  - すべてのディスクアレイ管理アカウント。
- SAM-QFS Manager でデフォルトユーザー `samadmin` を使用している場合は、パスワードを、インストールされているデフォルトのパスワードから強力なパスワードにただちに変更してください。SAM-QFS Manager では root を使用せず、必要に応じて、ほかのユーザーアカウントに役割を割り当ててください。これらのアカウントも、強力なパスワードで保護してください。
- Sun SAM-Remote に必要な場合を除き、8 ページの「一般的なセキュリティーの原則」に示されているポート上のトラフィックが MDS またはクライアントに転送されないようにするために、WAN エッジルーターにポートフィルタリングをインストールしてください。
- FC ディスクおよびテープを物理的に、または FC ゾーニングで分離することにより、ディスクが MDS とクライアントからしかアクセスできず、テープが MDS と潜在的な MDS からしかアクセスできないようにしてください。このセキュリティー対策は、テープまたはディスクの誤った上書きによって発生するデータ損失を防止するのに役立ちます。

- /dev をチェックして、テープおよびディスクデバイスファイルが root 以外のユーザーからはアクセスできないことを確認してください。この対策によって、SAM-QFS データが誤ってアクセスされたり、破棄されたりすることが防止されます。
- SAM-QFS は POSIX ファイルシステムであり、アクセス制御リスト (ACL) を含む一連の豊富なファイル/ディレクトリアクセス権を提供します。SAM-QFS は、ファイルシステム上のユーザーデータを保護するために必要に応じて使用してください。詳細は、SAM-QFS のドキュメントを参照してください。
- ローカルポリシーに基づいて、適切な一連のバックアップダンプを設定してください。バックアップはセキュリティーの一部であり、誤って、または何からの侵害によって失われたデータを復元するための方法を提供します。バックアップをオフサイトの場所に移送している間、そのバックアップには何らかのポリシーを含めるようにしてください。バックアップは、SAM-QFS テープおよびディスクと同程度に保護する必要があります。

参考資料

- 『Sun QFS および Sun Storage Archive Manager 5.3 インストールガイド』
- 『Sun QFS File System 5.3 構成および管理ガイド』
- 『Sun Storage Archive Manager 5.3 構成および管理ガイド』
- 『Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual』