

Oracle® Hierarchical Storage Manager and StorageTek QFS Software

セキュリティーガイド

Release 6.0

E62077-01

2015 年 3 月

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
セキュリティガイド

E62077-01

Copyright © 2015, 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.

このソフトウェアまた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。このソフトウェアまたはハードウェアは、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。このソフトウェアまた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。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用了ことに起因して損害が発生しても、Oracle Corporation 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 はオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

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。適用されるお客様と Oracle Corporation との間の契約に別段の定めがある場合を除いて、Oracle Corporation 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。適用されるお客様と Oracle Corporation との間の契約に定めがある場合を除いて、Oracle Corporation 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。

目次

| | |
|---|-----------|
| はじめに | 5 |
| 対象読者 | 5 |
| ドキュメントのアクセシビリティ | 5 |
| 表記規則 | 5 |
| コマンドの例におけるシェルプロンプト | 6 |
| 1. 概要 | 7 |
| 1.1. 製品の概要 | 7 |
| 1.2. 一般的なセキュリティの原則 | 8 |
| 1.2.1. ソフトウェアを最新の状態に維持する | 8 |
| 1.2.2. ネットワークアクセスを重要なサービスに制限する | 8 |
| 1.2.3. 最小特権の原則に従う | 9 |
| 1.2.4. システムアクティビティをモニターする | 9 |
| 1.2.5. 最新のセキュリティ情報を維持する | 9 |
| 2. セキュアなインストール | 11 |
| 2.1. 環境の理解 | 11 |
| 2.1.1. 保護する必要があるリソースはどれか。 | 11 |
| 2.1.2. だれからリソースを保護するか。 | 12 |
| 2.1.3. 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。 | 12 |
| 2.2. 推奨される配備トポロジ | 12 |
| 2.2.1. SAM-Remote のインストール | 13 |
| 2.2.2. Manager GUI のインストール | 14 |
| 2.2.3. インストール後の構成 | 14 |
| 3. セキュリティ機能 | 15 |
| 3.1. セキュリティモデル | 15 |
| 3.1.1. 認証 | 15 |

| | |
|----------------------------|----|
| 3.1.2. アクセス制御 | 15 |
| 4. 開発者のためのセキュリティの注意点 | 17 |
| A. セキュアな配備のチェックリスト | 19 |

はじめに

『Oracle Hierarchical Storage Manager and StorageTek QFS Software セキュリティーガイド』には、Oracle Hierarchical Storage Manager and QFS Software 製品に関する情報と、アプリケーションセキュリティの一般原則の説明が記載されています。

対象読者

このガイドは、Oracle Hierarchical Storage Manager and StorageTek QFS Software のセキュリティ機能の使用と、セキュアなインストールおよび構成に関与するユーザーを対象としています。

ドキュメントのアクセシビリティ

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>) を参照してください。

Oracle Support へのアクセス

サポートをご契約のお客様には、My Oracle Support を通して電子支援サービスを提供しています。詳細情報は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>) か、聴覚に障害のあるお客様は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>) を参照してください。

表記規則

次の表に、このマニュアルで使用されている表記規則を示します。

| 書体 | 意味 | 例 |
|------------------|-----------------------------|---|
| <i>AaBbCc123</i> | コマンドの名前、およびコンピュータ画面上の出力 | すべてのファイルの一覧を表示するには、 <i>ls -a</i> を使用します。 |
| AaBbCc123 | 画面のコンピュータ出力を伴う場合に入力するユーザー入力 | <i>machine_name% su</i> <i>Password:</i> |
| <i>aabbcc123</i> | プレースホルダ。実際の名前または値に置き換えます | ファイルを削除するためのコマンドは <i>rm filename</i> です。 |
| <i>AaBbCc123</i> | 書籍のタイトル、新しい用語、および強調された用語。 | 『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに格納されたコピーです。 |

| 書体 | 意味 | 例 |
|----|----|------------------------------------|
| | | ファイルを保存しないでください。 |
| | | 強調される項目の中には、オンラインで太字で表示されるものもあります。 |

コマンドの例におけるシェルプロンプト

次の表は、Oracle Solaris OS に含まれているシェルのデフォルトのUNIXシステムプロンプトおよびスーパーユーザープロンプトを示しています。コマンドの例で表示されるデフォルトのシステムプロンプトが Oracle Solaris リリースによって異なることに注意してください。

| シェル | プロンプト |
|--|---------------|
| Bash シェル、Korn シェル、および Bourne シェル | \$ |
| Bash シェル、Korn シェル、および Bourne シェル (スーパーユーザーの場合) | # |
| C シェル | machine_name% |
| C シェル (スーパーユーザーの場合) | machine_name# |

概要

この章では、Oracle Hierarchical Storage Manager and StorageTek QFS Software 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。

1.1. 製品の概要

Oracle Hierarchical Storage Manager and StorageTek QFS Software は、階層型ストレージマネージャーを備えた共有ファイルシステムです。この製品は、次の主要コンポーネントで構成されます。

StorageTek QFS パッケージ

スタンドアロンまたは共有として構成可能な高パフォーマンス QFS ファイルシステムが含まれます。スタンドアロンとして構成された場合、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。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。

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、Oracle Hierarchical Storage Manager (HSM) コンポーネントは含まれません。

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。

Oracle HSM パッケージ

QFS ファイルシステムと、Oracle HSM を実行するために必要なコードを含めます。Oracle HSM インストールパッケージは SUNWsamfsr および SUNWsamfsu です。階層型ストレージ管理が必要ない場合は、StorageTek QFS パッケージのみをインストールします。

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。StorageTek 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。SAM-Remote は 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、SAM-Remote

は個別に有効にして構成する必要があります。SAM-Remote の詳細は、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリを参照してください

Manager グラフィカルユーザーインタフェース

Manager グラフィカルユーザーインタフェース (GUI) である 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。Manager GUI のインストールおよび構成については、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリを参照してください

1.2. 一般的なセキュリティの原則

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。

1.2.1. ソフトウェアを最新の状態に維持する

実行する Oracle HSM のバージョンは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。

1.2.2. ネットワークアクセスを重要なサービスに制限する

Oracle HSM 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、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 HTTP ポートです
- tcp/5012 は、sam-rpcd に使用されます

注:

MDS クライアントの双方向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ト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。

1.2.3. 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。Manager GUI 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。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。

Manager GUI の使用の詳細は、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリを参照してください

1.2.4. システムアクティビティをモニターする

システムアクティビティをモニターして、Oracle HSM 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アクティビティがロギング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/*

1.2.5. 最新のセキュリティ情報を維持する

セキュリティ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、https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401 を参照してください。最新のセキュリティ情報を維持するための主な方法は、Oracle HSM ソフトウェアの最新のバージョンの実行です。

セキュアなインストール

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。

2.1. 環境の理解

セキュリティーニーズをよりよく理解するには、次の質問を尋ねる必要があります。

2.1.1. 保護する必要があるリソースはどれか。

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。

Oracle HSM 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、Oracle HSM ファイルシステムの作成に使用されます。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 (Oracle HSM を使用せずに) 独立してアクセスすると、通常の Oracle HSM 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。

Oracle HSM テープ

通常は、Oracle HSM ファイルシステムへのステージング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するテープ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。

Oracle HSM ダンプテープ

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。

Oracle HSM メタデータサーバー (MDS)

Oracle HSM 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。

構成ファイルと設定

Oracle HSM 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、Manager GUI を使用している場合、これらの設定は Oracle HSM 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、セキュリティリスクが発生することに注意してください。

2.1.2. だれからリソースを保護するか。

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。

2.1.3. 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 Oracle HSM 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。

2.2. 推奨される配備トポロジ

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。Oracle HSM のインストールについては、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager Release 6.0* お客様向けドキュメントライブラリを参照してください

Oracle HSM 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

Oracle HSM クライアントを MDS サーバーに接続するには、WAN に接続されていない個別の TCP/IP ネットワークおよびスイッチハードウェアを提供します。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 Oracle HSM 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

Oracle HSM 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。

セーフガード SAN ディスク構成アクセス

通常、SAN RAID ディスクには、TCP/IP (より一般的には HTTP) を使用して、管理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

システムだけ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。

Oracle HSM 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、階層型ストレージ管理を行わない場合、QFS パッケージのみをインストールします。デフォルトの Oracle HSM 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 セキュリティガイドライン』および『Oracle Solaris 11 セキュリティガイドライン』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、セキュリティパッチ) を最新の状態に維持してください。

Oracle HSM テープのセキュリティ

Oracle HSM の外部からの Oracle HSM テープへの外部アクセスを防止するか、そ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。分散入出力を使用するように構成される Solaris クライアントは、テープドライブへのアクセスが必要です。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。Oracle HSM 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、Oracle HSM データのバックアップを設定および実行します。Oracle HSM テープに推奨されているのと同様に、ダンプテープへのアクセスを制限します。

2.2.1. SAM-Remote のインストール

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、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリを参照してください

2.2.2. Manager GUI のインストール

Manager GUI のセキュアなインストールについては、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリを参照してください

2.2.3. インストール後の構成

いずれかの Oracle HSM パッケージをインストールしたら、[19 ページの付録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

セキュリティ機能

潜在的なセキュリティ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の脅威は、適切な構成によって、および[19 ページの付録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。

3.1. セキュリティモデル

セキュリティ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。

3.1.1. 認証

Oracle HSM 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。Manager GUI 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。

3.1.2. アクセス制御

Oracle HSM でのアクセス制御は次の 2 つの部分に分かれています。

- 管理アクセスの制御 – だれが Oracle HSM の管理アクションを実行できるかを制御します。これらの制御は、Manager GUI 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。Manager GUI の詳細は、<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs> にある *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0* お客様向けドキュメントライブラリ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 – Oracle HSM 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、Oracle HSM 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の注意点

開発者は通常、Oracle HSM 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、リクエストされたアクションを実装するために *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、*intro_libsam(3)* および *intro_libsamrpc(3)* のマニュアルページを参照してください。

セキュアな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。

1. root や、いずれかの Oracle HSM 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。
 - Manager GUI 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。
2. Manager GUI 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。Manager GUI 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。ほかのアカウントも、強力なパスワードで保護してください。
3. 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。
4. 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。
5. */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、Oracle HSM 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。
6. Oracle HSM 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。詳細については、Oracle HSM ドキュメントを参照してください。
7. 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、Oracle HSM 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。