

Guia de Segurança do Sun QFS and Sun Storage Archive Manager 5.3

Copyright © 2011, 2012, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados e de titularidade da Oracle Corporation. Proibida a reprodução total ou parcial.

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, nos envie uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue / distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

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.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais SPARC são usadas sob licença e são marcas comerciais ou marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, o logotipo da AMD e o logotipo do AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada licenciada por meio do consórcio The Open Group.

Este programa e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros.

Conteúdo

- Prefácio5**
- 1 Visão Geral do Sun QFS and Sun Storage Archive Manager7**
 - Visão Geral do Produto7
 - Princípios Gerais de Segurança8
 - Manter o Software Atualizado8
 - Restringir o Acesso de Rede aos Serviços Fundamentais8
 - Siga o Princípio do Menor Privilégio9
 - Monitorar a Atividade do Sistema9
 - Manter-se Atualizado Sobre as Informações de Segurança Mais Recentes9
- 2 Instalação e Configuração Seguras 11**
 - Visão Geral da Instalação 11
 - Noções Básicas Sobre o Seu Ambiente 11
 - Topologias de Implantação Recomendadas 12
 - Instalação do SAM-QFS 12
 - Instalação do Sun SAM-Remote 14
 - Instalação do Gerenciador do SAM-QFS 14
 - Configuração de Pós-instalação 14
- 3 Recursos de Segurança do Sun QFS and Sun Storage Archive Manager 15**
 - Modelo de Segurança 15
 - Autenticação 15
 - Controle de Acesso 16
 - Considerações de Segurança para os Desenvolvedores 16

A Lista de Verificação de Implantação Segura 17
 Lista de Verificação de Implantação 17
 Referências 18

Prefácio

O *Guia de Segurança do Sun QFS and Sun Storage Archive Manager* inclui informações sobre o produto do Sun QFS and Storage Archive Manager (SAM-QFS) e explica os princípios gerais de segurança do aplicativo.

Acesso ao Suporte Técnico da Oracle

Os clientes da Oracle têm acesso ao suporte técnico eletrônico por meio do My Oracle Support. Para obter informações, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> caso você tenha deficiência auditiva.

Convenções Tipográficas

A tabela a seguir descreve as convenções tipográficas usadas neste livro.

TABELA P-1 Convenções Tipográficas

Fonte	Descrição	Exemplo
AaBbCc123	Os nomes dos comandos, arquivos e diretórios e a saída do computador na tela	Edite seu arquivo .login. Use <code>ls -a</code> para listar todos os arquivos. <code>machine_name%</code> você recebeu e-mail(s).
AaBbCc123	O que você digita, em comparação com a saída de computador na tela	<code>machine_name% su</code> Senha:
<i>aabbcc123</i>	Placeholder: substitua por um nome ou valor real	O comando para remover um arquivo é o <i>nome de arquivo</i> <code>rm</code> .

TABELA P-1 Convenções Tipográficas (Continuação)		
Fonte	Descrição	Exemplo
AaBbCc123	Títulos de livros, novos termos e termos a serem enfatizados	Leia o Capítulo 6 do <i>Guia do Usuário</i> . Um <i>cache</i> é uma cópia armazenada localmente. <i>Não</i> salve o arquivo. Observação: alguns itens enfatizados são exibidos on-line em negrito.

Prompts de Shell nos Exemplos de Comando

A tabela a seguir mostra o prompt do sistema UNIX padrão e o prompt de superusuário para shells incluídos no SO do Oracle Solaris. Observe que o prompt do sistema padrão exibido nos exemplos de comando varia, dependendo da versão do Oracle Solaris.

TABELA P-2 Prompts de Shell	
Shell	Prompt
Shell Bash, shell Korn e shell Bourne	\$
Shell Bash, shell Korn e shell Bourne para superusuário	#
Shell C	machine_name%
Shell C para superusuário	machine_name#

Visão Geral do Sun QFS and Sun Storage Archive Manager

Este capítulo fornece uma visão geral do produto Sun QFS and Storage Archive Manager (SAM-QFS) e explica os princípios gerais de segurança do aplicativo.

Visão Geral do Produto

O SAM-QFS é um sistema de arquivos compartilhados com um gerenciador de armazenamento hierárquico. O SAM-QFS é composto pelos seguintes componentes:

- **Pacote do Sun QFS** – Inclui o sistema de arquivos de alto desempenho do Sun QFS que pode ser configurado como autônomo ou compartilhado. Quando configurado como autônomo, o Sun QFS é configurado em um único sistema e não com clientes compartilhados. O Sun QFS usa operações vnode do VFS para fazer a interface com os sistemas operacionais Oracle Solaris e Linux.

Os pacotes de instalação do Sun QFS são `SUNWqfsr` e `SUNWqfsu`. Esses pacotes *não* incluem o componente SAM (Storage Archive Manager).

A configuração do Sun QFS autônomo sem clientes compartilhados tem a menor exposição de segurança. Esta configuração não executa daemons e não tem conexões remotas diferentes do FC (Fibre Channel) para discos. A configuração compartilhada do QFS inclui conexões de FC com disco e a conexão TCP/IP entre os clientes e o MDS (Metadata Server).

- **Pacote do SAM-QFS** – Inclui o sistema de arquivos do Sun QFS e o código exigido para a execução do SAM.

Os pacotes de instalação do SAM-QFS são `SUNwsamfsr` e `SUNwsamfsu`. Se o SAM não for exigido, instale *somente* o pacote do Sun QFS.

- **Sun SAM-Remote** – Permite o acesso às bibliotecas e unidades de fita remotas por meio de conexões de rede remota (WAN) TCP/IP. O Sun SAM-Remote fornece um modo de recuperação de acidentes localizando instalações de fita remotamente. É possível instalar o Sun SAM-Remote com pacotes Sun QFS ou SAM-QFS, mas você deve ativar e configurar o Sun SAM-Remote separadamente. Para obter mais informações sobre o software Sun

SAM-Remote, consulte o [Capítulo 18, “Using the Sun SAM-Remote Software,” no *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*](#).

- **Pacote de ferramentas do SAM-QFS** – Instala ferramentas e páginas man no diretório /opt/SUNWsamfs/tools. Nenhuma dessas ferramentas tem privilégios especiais, mas todas elas exigem acesso root para serem usadas. O pacote de instalação é SUNWsamtp.
- **Gerenciador do SAM-QFS** – O Gerenciador do SAM-QFS, fsmgr, é executado no MDS e é acessado remotamente por meio de um navegador da Web. O acesso é concedido por meio da porta 6789 (<https://hostname:6789>).

Para usar o fsmgr, você deverá efetuar login como um usuário válido no MDS e adicionar determinadas funções à conta de usuário. Para obter informações sobre a instalação e a configuração do SAM-QFS Manager, consulte o [Capítulo 6, “Installing and Configuring SAM-QFS Manager,” no *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*](#).

Princípios Gerais de Segurança

As seções a seguir descrevem os princípios fundamentais exigidos para usar qualquer aplicativo de modo seguro.

Manter o Software Atualizado

Manter-se atualizado com a versão do SAM-QFS executada. É possível localizar as versões atuais do software para download no [Oracle Software Delivery Cloud \(https://edelivery.oracle.com/\)](https://edelivery.oracle.com/).

Restringir o Acesso de Rede aos Serviços Fundamentais

SAM-QFS usa as seguintes portas TCP/IP:

- tcp/7105 é usada para o tráfego de metadados entre o cliente e o MDS
- tcp/1000 é usada para o Sun SAM-Remote
- tcp/6789 é a porta HTTPS usada para um navegador entrar em contato com o fsmgr
- tcp/5012 é usada para sam-rpcd

Observação – Para o tráfego de clientes do MDS, considere a configuração de uma rede separada que não esteja interconectada com a WAN externa. Essa configuração impede a exposição a ameaças externas e também garante que o tráfego externo não limite o desempenho do MDS.

Siga o Princípio do Menor Privilégio

Conceda ao usuário ou administrador o menor privilégio exigido para concluir a tarefa a ser executada. O SAM-QFS Manager tem várias funções que podem ser concedidas aos usuários. Essas funções concedem tipos e quantidades variáveis de privilégio. A execução de tarefas de administração do SAM-QFS exige permissão root.

Para obter mais informações sobre o uso do SAM-QFS Manager, consulte o [Capítulo 6, “Installing and Configuring SAM-QFS Manager,”](#) no *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Monitorar a Atividade do Sistema

Monitore a atividade do sistema para determinar a eficiência da operação do SAM-QFS e se ela está registrando alguma atividade fora do normal. Verifique os seguintes arquivos de log:

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

Manter-se Atualizado Sobre as Informações de Segurança Mais Recentes

É possível acessar várias fontes de informações de segurança. Para obter informações e alertas de segurança para uma grande variedade de produtos de software, consulte <http://www.us-cert.gov>. Para obter informações específicas para o SAM-QFS, consulte <http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss>. A principal maneira de manter-se atualizado sobre os problemas de segurança é executar a versão mais recente do software SAM-QFS.

Instalação e Configuração Seguras

Este capítulo destaca o processo de planejamento para uma instalação segura e descreve várias topologias de implantação recomendadas para os sistemas.

Visão Geral da Instalação

Noções Básicas Sobre o Seu Ambiente

Para obter noções básicas sobre suas necessidades de segurança, faça a você mesmo as seguintes perguntas:

- **Quais recursos eu estou protegendo?**

É possível proteger vários dos recursos no ambiente de produção. Considere o tipo de recursos que você deseja proteger ao determinar o nível de segurança a ser oferecido.

Ao usar o SAM-QFS, proteja os seguinte recursos:

- **Metadados e o disco de dados principal** – Esses recursos de disco são usados para criar sistemas de arquivos do SAM-QFS. Geralmente eles são conectados por FC (Fibre Channel). O acesso independente a esses discos (sem ser por meio do SAM-QFS) apresenta um risco de segurança porque as permissões de arquivos e diretórios do SAM-QFS são ignoradas. Esse tipo de acesso externo pode ser por meio de um sistema fraudulento que leia ou grave os discos FC ou por meio de um sistema interno que acidentalmente forneça um acesso que não seja root a arquivos do dispositivo não processado.
- **Fitas do SAM** – O acesso independente a fitas, geralmente em uma biblioteca de fitas, em que os dados são gravados quando preparados fora de um sistema de arquivos do SAM representa um risco de segurança.

- **Arquivos de dump do SAM-QFS** – Dumps do sistema de arquivos criados por meio do `samfsdump` contêm dados e metadados. Esses dados e metadados devem ser protegidos de um acesso que não seja o do administrador do sistema durante um dump de rotina ou uma atividade de restauração.
- **Metadata Server (MDS) do SAM-QFS** – os clientes do SAM-QFS exigem acesso TCP/IP ao MDS. No entanto, verifique se os clientes estão protegidos do acesso WAN externo.
- **Arquivos e definições de configuração** – as definições de configuração do SAM-QFS *devem* ser protegidas de acessos que não sejam do administrador. Em geral, essas definições são protegidas automaticamente pelo SAM-QFS quando você usa o SAM-QFS Manager. Observe que tornar os arquivos de configuração graváveis para usuários não-administrativos apresenta um risco de segurança.
- **De quem eu estou protegendo os recursos?**

Em geral, os recursos descritos na seção anterior *devem* ser protegidos de todos os acessos que não sejam root ou administrativos em um sistema configurado ou de um sistema externo fraudulento que possa acessar esses recursos por meio da malha WAN ou FC.
- **O que acontecerá se as proteções em recursos estratégicos falharem?**

Falhas de proteção nos recursos estratégicos podem variar de acesso inadequado (acesso a dados fora das permissões de arquivo POSIX do SAM-QFS normais) a corrupção de dados (gravação em disco ou fita fora das permissões normais).

Topologias de Implantação Recomendadas

Instalação do SAM-QFS

Esta seção descreve como instalar e configurar um componente de infraestrutura de modo seguro.

Para obter informações sobre a instalação do SAM-QFS, consulte o [Capítulo 5, “Installing Sun QFS and SAM-QFS,” no *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*](#).

Considere os seguintes pontos ao instalar e configurar o SAM-QFS:

- **Rede de metadados separada** – Para conectar clientes do SAM-QFS aos servidores MDS, forneça uma rede TCP/IP separada e alterne o hardware que não esteja conectado a nenhuma WAN. Como o tráfego de metadados é implementado usando o TCP/IP, um ataque externo nesse tráfego é teoricamente possível. A configuração de uma rede de metadados separada extingue esse risco e também fornece um desempenho melhor. O melhor desempenho é obtido pelo fornecimento de um caminho de dados garantido para os metadados. Se uma rede de metadados separada for inviável, pelo menos negue o tráfego para as portas do SAM-QFS por meio da WAN externa e de qualquer host não confiável na rede. Consulte [“Restringir o Acesso de Rede aos Serviços Fundamentais” na página 8](#).
- **Zoneamento FC** – Utilize o zoneamento FC para negar acesso aos discos do SAM-QFS a qualquer servidor que não necessite de acesso a esses discos. De preferência, use um switch FC separado para estabelecer conexão física *apenas* com os servidores que necessitam de acesso.
- **Acesso de configuração aos discos de proteção do SAN** – Os discos do SAN RAID geralmente podem ser acessados para fins administrativos por meio de TCP/IP ou, mais frequentemente, por HTTP. Você deve proteger os discos do acesso externo limitando o acesso administrativo aos discos do SAN RAID somente para sistemas que estejam dentro de um domínio confiável. Além disso, altere a senha padrão nas matrizes de disco.
- **Instalar o pacote do SAM-QFS** – Primeiro instale apenas os pacotes que você precisar. Por exemplo, se você não planejar a execução do SAM, instale *somente* os pacotes do QFS. O arquivo do SAM-QFS padrão e as permissões e proprietários do diretório *não* devem ser alterados após a instalação sem considerar as implicações de segurança de tais alterações.
- **Acesso do cliente** – Se você planeja configurar clientes compartilhados, determine quais devem ter acesso ao sistema de arquivos no arquivo `hosts`. Consulte a página man número 4, `hosts.fs()`. Configure *somente* os hosts que necessitam de acesso ao sistema de arquivos específico que está sendo configurado.
- **Blindagem virtual do servidor de metadados do Oracle Solaris** – Para obter informações sobre como blindar virtualmente o SO Oracle Solaris, consulte o *Oracle Solaris 10 Security Guidelines* e o *Oracle Solaris 11 Security Guidelines*. No mínimo, escolha uma boa senha root, instale uma versão atualizada do SO Oracle Solaris, e mantenha-se atualizado sobre os patches, particularmente patches de segurança.
- **Blindagem Virtual de Clientes Linux** – Verifique a documentação do Linux para obter informações sobre como blindar virtualmente clientes Linux. No mínimo, escolha uma boa senha root, instale uma versão atualizada do sistema operacional Linux, e mantenha-se atualizado sobre os patches, particularmente patches de segurança.
- **Segurança de fita do SAM-QFS** – Impeça o acesso externo às fitas do SAM ou limite o acesso somente para administradores. Use o zoneamento FC para limitar as unidades de fita somente para o MDS (ou o possível MDS, caso um MDS de backup seja configurado). Além disso, limite o acesso ao arquivo do dispositivo de fita concedendo somente permissões root. O acesso não autorizado às fitas do SAM pode comprometer ou destruir dados do usuário.

- **Backups** – Configure e execute backups dos dados do SAM-QFS usando o comando `samfsdump` ou `qfsdump`. Limite o acesso aos arquivos de dump conforme recomendado para as fitas do SAM.

Instalação do Sun SAM-Remote

Para obter informações sobre a instalação segura do software Sun SAM-Remote, consulte o [Capítulo 18, “Using the Sun SAM-Remote Software,”](#) no *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*.

Instalação do Gerenciador do SAM-QFS

Para obter informações sobre a instalação segura do SAM-QFS Manager, consulte o [Capítulo 6, “Installing and Configuring SAM-QFS Manager,”](#) no *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Configuração de Pós-instalação

Após a instalação de qualquer um dos pacotes do SAM-QFS, consulte a lista de verificação no [Apêndice A, “Lista de Verificação de Implantação Segura”](#).

Recursos de Segurança do Sun QFS and Sun Storage Archive Manager

Para evitar possíveis ameaças de segurança, os clientes que estiverem operando um sistema de arquivos compartilhado deve se preocupar com o seguinte:

- Divulgação de dados do sistema de arquivos na violação da política
- Perda de dados
- Modificação de dados não detectada

Essas ameaças de segurança podem ser minimizadas pela configuração adequada e seguindo a lista de verificação de pós-instalação no [Apêndice A, “Lista de Verificação de Implantação Segura”](#).

Modelo de Segurança

Os recursos de segurança críticos que fornecem proteção contra ameaças de segurança são:

- **Autenticação** – Permite que apenas indivíduos autorizados recebam acesso ao sistema e aos dados.
- **Autorização** – Controle de acesso a privilégios e dados do sistema. Este recurso é criado na autenticação para garantir que os indivíduos obtenham apenas o acesso adequado.
- **Auditorar** – Permite que os administradores detectem tentativas de violações do mecanismo de autenticação ou tentativas de violação, ou violações bem-sucedidas, do controle de acesso.

Autenticação

O SAM-QFS usa a autenticação de usuário com base no host para controlar quem pode executar tarefas de administração. A administração que usa o SAM-QFS Manager é controlada principalmente pelas funções atribuídas a vários usuários. A administração que usa a linha de comandos é limitada ao usuário root.

Controle de Acesso

O controle de acesso no SAM-QFS é dividido em duas partes:

- **Controle de acesso administrativo** – Controla quem pode tomar ações administrativas para o SAM-QFS. Os controles são baseados em funções atribuídas a usuários por meio do SAM-QFS Manager. Para operações da linha de comandos, os controles são baseados em permissões root. Para obter mais informações sobre o SAM-QFS Manager, consulte o [Capítulo 6, “Installing and Configuring SAM-QFS Manager,” no *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*](#).
- **Controle de acesso do arquivo/diretório** – O SAM-QFS implementa um sistema de arquivos em conformidade com o POSIX que tenha um amplo conjunto de controles de acesso. Consulte a documentação do SAM-QFS para obter mais detalhes.

Considerações de Segurança para os Desenvolvedores

Os desenvolvedores geralmente não se relacionam diretamente com o SAM-QFS. As duas exceções são a API `libsam` e a API `libsamrpc`. Essas duas APIs fornecem a mesma funcionalidade. A `libsam` serve apenas para uma máquina local, enquanto que a `libsamrpc` comunica-se com o MDS através do `rpc(3)` para implementar as ações necessárias. A autenticação de solicitações feitas por qualquer um dos métodos é baseada no UID e no GID do processo de chamadas. Elas têm as mesmas permissões que as solicitações feitas por meio da linha de comandos. É necessário ter um espaço de UID e GID comum para o MDS e os sistemas cliente.

Para obter mais informações, consulte `intro_libsam(3)` e `intro_libsamrpc(3)` no [Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual](#).

Lista de Verificação de Implantação Segura

Use a lista de verificação neste apêndice para implantar o software SAM-QFS de modo seguro.

Lista de Verificação de Implantação

Essa lista de verificação de segurança inclui diretrizes que ajudam a proteger seu banco de dados.

- Defina senhas fortes para root e para quaisquer outras contas que tenham funções do SAM-QFS atribuídas a elas. Essa diretriz inclui:
 - Quaisquer contas que recebam funções administrativas por meio do SAM-QFS Manager.
 - IDs de Usuário `acsss`, `acsdb` e `acssa` (caso estejam sendo usados).
 - Quaisquer contas administrativas da matriz de discos.
- Caso esteja usando o usuário padrão `samadmin` com o SAM-QFS Manager, altere imediatamente a senha instalada padrão para uma senha forte. Não use root com o SAM-QFS Manager; em vez disso, atribua funções conforme o necessário para outras contas de usuário. Proteja também essas contas com senhas fortes.
- Instale a filtragem de portas nos roteadores edge WAN para impedir que o tráfego nas portas listadas nos [“Princípios Gerais de Segurança” na página 8](#) chegue no MDS ou nos clientes, exceto quando necessário para o Sun SAM-Remote.
- Separe os discos e as fitas FC fisicamente ou por meio do zoneamento FC, de modo que os discos sejam acessíveis apenas por meio do MDS e dos clientes, e as fitas por meio do MDS e do possível MDS. Esta prática de segurança ajuda a impedir a perda de dados em decorrência da sobregravação acidental da fita ou do disco.
- Verifique `/dev` para garantir que os arquivos do dispositivo de fita e disco não estão acessíveis para usuários que não sejam root. Esta prática impede que os dados do SAM-QFS sejam acessados de modo inadequado ou destruídos.

- O SAM-QFS é um sistema de arquivos do POSIX e fornece um amplo conjunto de permissões de arquivo/diretório incluindo as ACLs (listas de controle de acesso). Use-as conforme o necessário para proteger dados do usuário no sistema de arquivos. Para obter mais informações, consulte a documentação do SAM-QFS.
- Configure um conjunto adequado de dumps de backup com base na política local. Os backups fazem parte da segurança e fornecem uma maneira de restaurar dados perdidos acidentalmente ou em decorrência de alguma falha. O backup deve incluir alguma política enquanto ele estiver sendo transportado para um local externo. Backups devem ser protegidos da mesma forma que as fitas e os discos do SAM-QFS.

Referências

- *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*
- *Sun QFS File System 5.3 Configuration and Administration Guide*
- *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*
- *Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual*