Oracle® Hierarchical Storage Manager and StorageTek QFS Software

Guia de Segurança

Versão 6.0

E62079-01

Março de 2015

ORACLE®

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
Guia de Segurança

E62079-01

Índice

Prefácio

O Guia de Segurança do Oracle Hierarchical Storage Manager and StorageTek QFS software inclui informações sobre o produto Oracle Hierarchical Storage Manager and QFS e explica os princípios gerais de segurança dos aplicativos.

Público-alvo

Este guia destina-se aos envolvidos no uso de recursos de segurança e na instalação e configuração seguras do Oracle Hierarchical Storage Manager and StorageTek QFS Software.

Acessibilidade da Documentação

Para obter informações sobre o comprometimento da Oracle com a acessibilidade, visite o site do Oracle Accessibility Program em `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acesso ao Suporte Técnico da Oracle
Os clientes da Oracle que adquiriram serviços de suporte têm acesso ao suporte eletrônico por meio do My Oracle Support. Para obter informações, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` se você for portador de deficiência auditiva.

Convenções Tipográficas

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

Face de Tipos	Significado	Exemplo
AaBbCc123	Nomes de comandos e saída do computador na tela	*Use ls -a* para listar todos os arquivos.
AaBbCc123	entrada do usuário que você digita quando acompanhada pela saída do computador na tela	*machine_name%* **su** *Senha:*
aabbcc123	Placeholder, substitua por um nome ou valor real	O comando para remover um arquivo é o *rm filename*.
AaBbCc123	Títulos de livros, novos termos e termos a serem enfatizados	Leia o Capítulo 6 do *Guia do Usuário*. Um *cache* é uma cópia armazenada localmente. Não 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.

Shell	Prompt
Bashshell, Kornshell e Bourneshell	$
Bashshell, Kornshell e Bourneshell para superusuário	#
Cshell	machine_name%
Cshell para superusuário	machine_name#

1

Visão Geral

Este capítulo fornece uma visão geral do produto Oracle Hierarchical Storage Manager and StorageTek QFS Software e explica os princípios gerais de segurança do aplicativo.

1.1. Visão Geral do Produto

O Oracle Hierarchical Storage Manager and StorageTek QFS Software é um sistema de arquivos compartilhado com um HSM (Hierarchical Storage Manager). O produto é formado pelos seguintes componentes principais:

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

Os pacotes de instalação do QFS são SUNWqfsr e SUNWqfsu. Esses pacotes não incluem o componente Oracle Hierarchical Storage Manager (HSM).

A configuração do 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 Oracle HSM
Inclui o sistema de arquivos do QFS e o código que é obrigatório para executar o Oracle HSM. Os pacotes de instalação do Oracle HSM são SUNWsamfsr e SUNWsamfsu. Se você não tiver um gerenciamento de armazenamento hierárquico, *só* instale os pacotes do StorageTek QFS.

SAM-Remote
Permite o acesso às bibliotecas e unidades de fita remotas por meio de conexões de rede remota (WAN) TCP/IP. O StorageTek SAM-Remote fornece um modo de recuperação de acidentes localizando instalações de fita remotamente. É possível instalar o SAM-Remote com pacotes do QFS ou SAM-QFS, mas você deve ativar e configurar o Sun SAM-Remote separadamente. Para obter mais informações sobre o SAM-Remote, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* em: `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`

Interface gráfica de usuário do Manager
A Interface gráfica de usuário (GUI) do Manager, fsmgr, é executada no MDS e acessada remotamente por meio de um web browser. 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 da interfade gráfica de usuário do Manager, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* em: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

1.2. Princípios Gerais de Segurança

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

1.2.1. Manter o Software Atualizado

Esteja familiarizado com a versão do Oracle HSM que você executa. É possível encontrar as versões atuais do software para download no Oracle Software Delivery Cloud (https://edelivery.oracle.com/).

1.2.2. Restringir o Acesso de Rede aos Serviços Fundamentais

O Oracle HSM 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 SAM-Remote
- tcp/6789 é a porta HTTP usada para um navegador entrar em contato com o fsmgr
- tcp/5012 é usada para sam-rpcd

Observação:

Para o tráfego de clientes bidirecional 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.

1.2.3. Seguir o Princípio do Menor Privilégio

Conceda ao usuário ou administrador o menor privilégio exigido para concluir a tarefa a ser executada. A interfade gráfica de usuário do 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 na linha de comandos exige permissão root.

Para obter mais informações sobre como usar a interfade gráfica de usuário do Manager, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release*

6.0 Customer Documentation Library em: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

1.2.4. Monitorar a Atividade do Sistema

Monitore a atividade do sistema para determinar a eficiência da operação do Oracle HSM 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/*

1.2.5. Manter-se Atualizado Sobre as Informações de Segurança Mais Recentes

É possível acessar várias fontes de informações de segurança. Para obter informações de segurança e alertas para uma grande variedade de produtos de software, consulte http://www.us-cert.gov. Para obter informações específicas do SAM-QFS, consulte https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401. A principal maneira de se manter atualizado sobre os problemas de segurança é executar a versão mais recente do software Oracle HSM.

2

Instalação Segura

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

2.1. Noções Básicas Sobre o Seu Ambiente

Para melhor compreender suas necessidades de segurança, as seguintes perguntas devem ser feitas:

2.1.1. Quais recursos precisam ser protegidos?

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 Oracle HSM, proteja os seguinte recursos:

Discos de metadados e de dados principais
Esses recursos de disco são usados para criar sistemas de arquivos do Oracle HSM. Geralmente eles são conectados por FC (Fibre Channel). O acesso independente a esses discos (sem ser por meio do Oracle HSM) apresenta um risco de segurança porque as permissões normais de arquivos e diretórios do Oracle HSM 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 Oracle HSM
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 Oracle HSM representa um risco de segurança.

Fitas de dump do Oracle HSM
Os dumps do sistema de arquivos criados a partir 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.

Servidor de metadados (MDS) do Oracle HSM
Os clientes do Oracle HSM requerem 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 Oracle HSM devem ser protegidas de acessos que não sejam do administrador. Em geral, essas definições são protegidas automaticamente pelo

Oracle HSM quando você usa a interfade gráfica de usuário do Manager. Observe que tornar os arquivos de configuração graváveis para usuários não administrativos apresenta um risco de segurança.

2.1.2. De quem os recursos precisam ser protegidos?

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.

2.1.3. O que acontecerá se as proteções dos recursos estratégicos falharem?

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

2.2. Topologias de Implantação Recomendadas

Esta seção descreve como instalar e configurar um componente de infraestrutura de forma segura. Para obter informações sobre a instalação do Oracle HSM, consulte a *Oracle Hierarchical Storage Manager Release 6.0 Customer Documentation Library*em: `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`

Considere os seguintes pontos ao instalar e configurar o Oracle HSM:

Rede de metadados separada
Para conectar os clientes do Oracle HSM aos servidores do MDS, forneça uma rede TCP/IP separada e troque o hardware que não está conectado a uma 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 às portas do Oracle HSM por meio da WAN externa e de qualquer host não confiável na rede. Consulte Seção 1.2.2, “Restringir o Acesso de Rede aos Serviços Fundamentais” [8].

Zoneamento FC
Use zoneamento FC para negar o acesso aos discos do Oracle HSM de qualquer servidor que não solicite acesso aos 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
Em geral, os discos do SAN RAID 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.

Instalação do pacote do Oracle HSM
Primeiro, instale apenas os pacotes que você precisar. Por exemplo, se você não tiver um gerenciamento de armazenamento hierárquico, só instale os pacotes do QFS. As permissões e proprietários de arquivos e diretórios padrão do Oracle HSM devem ser alteradas após a instalação, sem considerar as implicações de segurança dessas 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 hosts.fs(4). Configure somente os hosts que necessitam de acesso ao sistema de arquivos específico que está sendo configurado.

Proteção do servidor de metadados do Oracle Solaris
Para obter informações sobre como proteger 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.

Proteção de clientes Linux
Verifique a documentação do Linux sobre como proteger 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.

Fita de segurança do Oracle HSM
Impeça o acesso externo às fitas do Oracle HSM ou limite esse acesso somente a 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). Os clientes Solaris que serão configurados para usar E/S distribuída precisarão de acesso às unidades de fita. Além disso, limite o acesso ao arquivo do dispositivo de fita concedendo somente permissões root. O acesso não autorizado às fitas do Oracle HSM pode comprometer ou destruir dados do usuário.

Backups
Configure e execute backups dos dados do Oracle HSM usando o comando samfsdump ou qfsdump. Limite o acesso às fitas de dump conforme recomendado para as fitas do Oracle HSM.

2.2.1. Instalando o SAM-Remote

Para obter informações sobre a instalação segura do software SAM-Remote, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* em: `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`

2.2.2. Instalando a interfade gráfica de usuário do Manager

Para obter informações sobre a instalação segura da interfade gráfica de usuário do Manager, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release*

6.0 Customer Documentation Library em: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

2.2.3. Configuração Pós-Instalação

Após a instalação dos pacotes do Oracle HSM, consulte a lista de verificação de segurança em Apêndice A, *Lista de Verificação para Implantação Segura* [19]

3

Recursos de Segurança

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 para Implantação Segura* [19]

3.1. O 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.
- Auditar – Permite que os administradores detectem tentativas de violações do mecanismo de autenticação ou tentativas de violação, ou violações bem-sucedidas, do controle de acesso.

3.1.1. Autenticação

O Oracle HSM usa a autenticação de usuário com base no host para controlar quem pode executar tarefas de administração. A administração por meio da interfade gráfica de usuário do Manager é controlada principalmente pelas funções que são atribuídas a vários usuários. A administração que usa a linha de comandos é limitada ao usuário root.

3.1.2. Controle de Acesso

O controle de acesso no Oracle HSM divide-se em duas partes:

- Controle de acesso administrativo – Controla quem pode tomar ações administrativas para o Oracle HSM. Os controles são baseados em funções atribuídas a usuários por meio da interfade gráfica de usuário do Manager. Para operações da linha de comandos, os

controles são baseados em permissões root. Para obter mais informações sobre a interfade gráfica de usuário do Manager, consulte a *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* em: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

- Controle de acesso do arquivo/diretório – O Oracle HSM implementa um sistema de arquivos compatível com o POSIX que tem um amplo conjunto de controles de acesso. Consulte a documentação do Oracle HSM para obter mais detalhes.

4

Considerações de Segurança para Desenvolvedores

Em geral, os desenvolvedores não fazem uma interface direta com o Oracle HSM. 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 as páginas man *intro_libsam(3)* e *intro_libsamrpc(3)*.

Apêndice A

Lista de Verificação para Implantação Segura

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

1. Defina senhas fortes para root e para quaisquer outras contas que tenham funções do Oracle HSM atribuídas a elas. Essa diretriz inclui:
   - Quaisquer contas que recebam funções administrativas por meio da interfade gráfica de usuário do Manager.
   - IDs de Usuário *`acsss`*, *`acsdb`* e *`acssa`* (caso estejam sendo usados).
   - Quaisquer contas administrativas da matriz de discos.
2. Caso esteja utilizando o usuário padrão *`samadmin`* com a interfade gráfica de usuário do Manager, altere imediatamente a senha padrão instalada para uma senha forte. Não use root com a interfade gráfica de usuário do Manager; em vez disso, atribua funções conforme o necessário para outras contas de usuário. Proteja também outras contas com senhas fortes.
3. Instale a filtragem de portas nos roteadores edge WAN para impedir que o tráfego nas portas listadas nos Seção 1.2, “Princípios Gerais de Segurança” [8] chegue no MDS ou nos clientes, exceto quando necessário para o SAM-Remote.
4. 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.
5. 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 Oracle HSM sejam acessados de modo inadequado ou destruídos.
6. O Oracle HSM é um sistema de arquivos 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 Oracle HSM.
7. 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 o disco do Oracle HSM.