

Oracle® Hierarchical Storage Manager and StorageTek QFS Software

Sicherheitshandbuch

Release 6.0

E62074-01

März 2015

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
Sicherheitshandbuch

E62074-01

Copyright © 2015, Oracle und/oder verbundene Unternehmen. All rights reserved. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse engineering, Disassemblieren bzw. Dekompilieren dieser Software ist verboten, es sei denn dies ist zur Interoperabilität gesetzlich gestattet.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

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.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden unter Lizenz verwendet und sind Marken oder eingetragene Marken von SPARC International Inc. AMD, Opteron, das AMD-Logo und das AMD-Opteron-Logo sind Marken oder eingetragene Marken von Advanced Micro Devices. UNIX ist eine eingetragene Marke von The Open Group.

Diese Software oder Hardware und die Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab, es sei denn, zwischen Ihnen und Oracle wurde eine andere Vereinbarung getroffen. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden aufgrund Ihres Zugriffs oder Ihrer Nutzung von Inhalten, Produkten oder Serviceleistungen von Dritten, es sei denn, zwischen Ihnen und Oracle wurde eine andere Vereinbarung getroffen.

Inhalt

Vorwort	5
Zielgruppe	5
Hinweise zu barrierefreier Dokumentation	5
Typografische Konventionen	5
Shell-Eingabeaufforderungen in Befehlbeispielen	6
1. Überblick	7
1.1. Produktüberblick	7
1.2. Allgemeine Sicherheitsgrundsätze	8
1.2.1. Software aktualisieren	8
1.2.2. Netzwerkzugriff auf kritische Services beschränken	8
1.2.3. Prinzip der geringsten Berechtigungen beachten	8
1.2.4. Überwachen der Systemaktivität	9
1.2.5. Neueste Sicherheitsinformationen verwenden	9
2. Sichere Installation	11
2.1. Umgebung analysieren	11
2.1.1. Welche Ressourcen müssen geschützt werden?	11
2.1.2. Vor wem müssen die Ressourcen geschützt werden?	12
2.1.3. Folgen des Ausfalls strategischer Ressourcen	12
2.2. Empfohlene Bereitstellungstopologien	12
2.2.1. Installation von SAM-Remote	14
2.2.2. Installation der grafischen Benutzeroberfläche des Managers	14
2.2.3. Konfiguration nach der Installation	14
3. Sicherheitsfunktionen	15
3.1. Sicherheitsmodell	15
3.1.1. Authentifizierung	15
3.1.2. Zugriffskontrolle	15
4. Sicherheitsinformationen für Entwickler	17
A. Checkliste für sichere Bereitstellung	19

Vorwort

"Oracle Hierarchical Storage Manager and StorageTek QFS Software - Sicherheitshandbuch" enthält Informationen zum Oracle Hierarchical Storage Manager- und QFS-Produkt und erläutert die allgemeinen Grundlagen der Anwendungssicherheit.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung von Sicherheitsfunktionen und der sicheren Installation und Konfiguration von Oracle Hierarchical Storage Manager and StorageTek QFS Software beteiligt sind.

Hinweise zu barrierefreier Dokumentation

Weitere Informationen zur barrierefreien Dokumentation finden Sie auf der Oracle Accessibility Program-Webseite unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Kontakt zum Support von Oracle

Oracle-Kunden, die Support abonniert haben, können über My Oracle Support den Onlinesupport nutzen. Weitere Informationen finden Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>, wenn Sie hörbehindert sind.

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

Schriftart	Bedeutung	Beispiel
<i>AaBbCc123</i>	Namen von Befehlen und Bildschirmausgaben	Verwenden Sie <i>ls -a</i> , um alle Dateien aufzuführen.
AaBbCc123	Benutzereingabe, die Sie zusammen mit einer Bildschirmausgabe vornehmen	<i>machine_name% su</i> <i>Password:</i>
<i>aabbcc123</i>	Platzhalter, durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet <i>rm Dateiname</i> .
<i>AaBbCc123</i>	Buchtitel, neue Ausdrücke; hervorgehobene Begriffe	Lesen Sie hierzu Kapitel 6 im <i>Benutzerhandbuch</i> . Ein <i>Cache</i> ist eine lokal gespeicherte Kopie. Diese Datei nicht speichern. Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlbeispielen

Die folgende Tabelle zeigt die UNIX -Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung variiert, abhängig von der Oracle Solaris-Version.

Shell	Eingabeaufforderung
Bashshell, Kornshell und Bournesshell	\$
Bashshell, Kornshell und Bournesshell für Superuser	#
Cshell	machine_name%
Cshell für Superuser	machine_name#

Überblick

Dieses Kapitel enthält einen Überblick über das Oracle Hierarchical Storage Manager and StorageTek QFS Software-Produkt und erläutert die allgemeinen Grundlagen der Anwendungssicherheit.

1.1. Produktüberblick

Oracle Hierarchical Storage Manager and StorageTek QFS Software ist ein gemeinsam verwendetes Dateisystem mit einem hierarchischen Storage Manager. Das Produkt setzt sich aus den folgenden Hauptkomponenten zusammen:

StorageTek QFS-Paket

Umfasst das High-Performance-QFS-Dateisystem, das entweder als eigenständiges oder gemeinsam verwendetes Dateisystem konfiguriert werden kann. Als eigenständige Anwendung ist QFS auf einem Einzelsystem ohne gemeinsam verwendete Clients konfiguriert. QFS verwendet VFS/vnode-Standardvorgänge für die Verbindung mit den Oracle Solaris- und Linux-Betriebssystemen.

Die QFS-Installationspakete sind SUNWqfsr und SUNWqfsu. In diesen Paketen ist die Oracle HSM-Komponente (Hierarchical Storage Manager) nicht enthalten.

Die Konfiguration von QFS als eigenständige Anwendung ohne gemeinsam genutzte Clients bietet die höchste Sicherheit. Bei dieser Konfiguration werden keine Dämonen ausgeführt, und die einzige Remote-Verbindung besteht zwischen FC (Fibre Channel) und der Festplatte. QFS als gemeinsam genutzte Anwendung umfasst FC-Verbindungen zur Festplatte und eine TCP/IP-Verbindung zwischen Clients und dem MDS (Metadatenserver).

Oracle HSM-Paket

Enthält das QFS-Dateisystem und den Code, der zum Ausführen von Oracle HSM erforderlich ist. Die Oracle HSM-Installationspakete heißen SUNWsamfsr und SUNWsamfsu. Falls Sie keine hierarchische Speicherverwaltung wünschen, installieren Sie *nur* das StorageTek QFS-Paket.

SAM-Remote

Gewährt Zugriff auf Remote-Bandbibliotheken und -laufwerke über TCP/IP-WAN-Verbindungen (Wide Area Network). Storage Tek SAM-Remote bietet eine Form von Disaster Recovery durch die Remote-Bereitstellung von Bandfunktionen. Sie können SAM-Remote entweder mit QFS oder SAM-QFS-Paketen installieren, müssen jedoch SAM-Remote separat aktivieren und konfigurieren. Weitere Informationen zu

SAM-Remote finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Manager-GUI

Die grafische Benutzeroberfläche des Managers, fsmgr, wird auf dem MDS ausgeführt und kann remote über einen Webbrowser geöffnet werden. Der Zugriff erfolgt über Port 6789 ([https:// hostname:6789](https://hostname:6789)).

Um fsmgr zu verwenden, müssen Sie sich als gültiger Benutzer beim MDS anmelden und bestimmte Rollen dem Benutzerkonto hinzufügen. Informationen zur Installation und Konfiguration der grafischen Benutzeroberfläche des Managers finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2. Allgemeine Sicherheitsgrundsätze

In den folgenden Abschnitten werden die Grundsätze beschrieben, die für eine sichere Verwendung von Anwendungen unerlässlich sind.

1.2.1. Software aktualisieren

Halten Sie die Oracle HSM-Version, die Sie nutzen, immer aktuell. Sie können aktuelle Versionen der Software aus der Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>) herunterladen.

1.2.2. Netzwerkzugriff auf kritische Services beschränken

Oracle HSM verwendet die folgenden TCP/IP-Ports:

- tcp/7105 wird für den Metadatenverkehr zwischen den Clients und dem MDS verwendet
- tcp/1000 wird für SAM-Remote verwendet
- tcp/6789 ist der HTTP-Port, den ein Browser für die Verbindung mit "fsmgr" verwendet
- tcp/5012 wird für sam-rpcd verwendet

Hinweis:

Für den bidirektionalen MDS-Clientdatenverkehr sollten Sie das Einrichten eines separaten Netzwerks, das nicht mit dem externen WAN verbunden ist, in Betracht ziehen. Durch diese Konfiguration können externe Bedrohungen das System nicht verwundbar machen, außerdem wird die MDS-Leistung durch externen Datenverkehr nicht beeinträchtigt.

1.2.3. Prinzip der geringsten Berechtigungen beachten

Gewähren Sie dem Benutzer oder Administrator die geringsten Berechtigungen, die für das Durchführen der Aufgabe erforderlich sind. Die grafische Benutzeroberfläche des

Managers verfügt über verschiedene Rollen, die Benutzern zugewiesen werden können. Diese Rollen gewähren Berechtigungen, die in Art und Umfang unterschiedlich sind. Für Verwaltungsaufgaben aus der Befehlszeile sind Root-Berechtigungen erforderlich.

Weitere Informationen zur Verwendung der grafischen Benutzeroberfläche des Managers finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2.4. Überwachen der Systemaktivität

Überwachen Sie die Systemaktivität, um festzustellen, wie gut Oracle HSM arbeitet und ob ungewöhnliche Aktivitäten protokolliert werden. Überprüfen Sie die folgenden Protokolldateien:

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

1.2.5. Neueste Sicherheitsinformationen verwenden

Sie können Sicherheitsinformationen aus mehreren Quellen erhalten.

Sicherheitsinformationen und Warnungen für zahlreiche Produkte finden Sie unter <http://www.us-cert.gov>. Für SAM-QFS spezifische Informationen finden Sie unter https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401. Sie bleiben hinsichtlich der Sicherheit vor allem dann auf dem neuesten Stand, wenn Sie die neueste Version der Oracle HSM-Software ausführen.

Sichere Installation

In diesem Kapitel wird der Planungsprozess für eine sichere Installation beschrieben und mehrere empfohlene Bereitstellungstopologien für die Systeme beschrieben.

2.1. Umgebung analysieren

Damit die Sicherheitsanforderungen verständlicher werden, müssen die folgenden Fragen gestellt werden:

2.1.1. Welche Ressourcen müssen geschützt werden?

In der Produktionsumgebung können zahlreiche Ressourcen gesichert werden. Berücksichtigen Sie bei der Bestimmung der Sicherheitsstufe den zu sichernden Ressourcentyp.

Schützen Sie bei der Verwendung von Oracle HSM die folgenden Ressourcen:

Datenträger für Metadaten und Primärdaten

Mit diesen Datenträgerressourcen werden Oracle HSM-Dateisysteme erstellt. Üblicherweise sind sie über FC (Fibre Channel) verbunden. Ein unabhängiger Zugriff auf diese Datenträger (nicht über Oracle HSMS) stellt ein Sicherheitsrisiko dar, weil so die normalen Oracle HSM-Datei- und Verzeichnisberechtigungen umgangen werden. Diese Form des externen Zugriffs kann von einem Rogue-System stammen, das von FC-Festplatten liest oder darauf schreibt, oder von einem internen System, das unbeabsichtigt Non-Root-Zugriff (Zugriff ohne Root-Rechte) auf Raw Device-Dateien gewährt.

Oracle HSM-Bänder

Unabhängiger Zugriff auf Bänder, die sich normalerweise in einer Bandbibliothek befinden, in der Dateidaten geschrieben werden, wenn ein Oracle HSM-Dateisystem ein Sicherheitsrisiko ist.

Oracle HSM-Dumpbänder

Dateisystemdumps, die mit samfsdump erstellt werden, enthalten Daten und Metadaten. Diese Daten und Metadaten sollten während dem routinemäßigen Erstellen eines Speicherabbilds oder eines Wiederherstellungsvorgangs nur Systemadministratoren zugänglich sein.

Oracle HSM-Metadatenserver (MDS)

Oracle HSM-Clients erfordern TCP/IP-Zugriff auf den MDS. Vergewissern Sie sich jedoch, dass die Clients vor dem externen WAN-Zugriff geschützt sind.

Konfigurationsdateien und Einstellungen

Oracle HSM-Konfigurationseinstellungen müssen vor dem Zugriff durch Nicht-Administratoren geschützt werden. Im Allgemeinen werden diese Einstellungen bei Verwendung der grafischen Benutzeroberfläche des Managers automatisch durch Oracle HSM geschützt. Beachten Sie, dass ein Sicherheitsrisiko entsteht, wenn andere Benutzer als der Administrator in Konfigurationsdateien schreiben können.

2.1.2. Vor wem müssen die Ressourcen geschützt werden?

Im Allgemeinen müssen die auf einem konfigurierten System im vorherigen Abschnitt beschriebenen Ressourcen vor sämtlichen Zugriffen geschützt werden. Dazu gehören auch Zugriffe eines externen Rogue-Systems über WAN oder FC-Fabric. Root- sowie Administratorenzugriffe sind davon nicht betroffen.

2.1.3. Folgen des Ausfalls strategischer Ressourcen

Die Ursachen für das Versagen des Schutzes strategischer Ressourcen können von unberechtigten Zugriffen (Datenzugriffe, die den Oracle HSM-POSIX-Dateiberechtigungen nicht entsprechen) bis hin zu Datenbeschädigungen (Schreiben auf Datenträger oder Band außerhalb der normalen Berechtigungen) reichen.

2.2. Empfohlene Bereitstellungstopologien

In diesem Abschnitt wird beschrieben, wie Sie eine Infrastrukturkomponente sicher installieren und konfigurieren. Weitere Informationen zur Installation von Oracle HSM finden Sie in *Oracle Hierarchical Storage Manager Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfss>

Beachten Sie bei der Installation und Konfiguration von Oracle HSM Folgendes:

Separates Metadatenetzwerk

Um Oracle HSM-Clients mit den MDS-Servern zu verbinden, stellen Sie ein separates TCP/IP-Netzwerk und Hardware bereit, die nicht mit einem WAN verbunden ist. Da der Metadatenverkehr über TCP/IP implementiert wird, kann theoretisch ein externer Angriff erfolgen. Die Konfiguration eines separaten Metadatenetzwerks verringert dieses Risiko und sorgt zudem für eine bessere Leistung. Die Leistungsverbesserung ergibt sich durch den garantierten Pfad zu den Metadaten. Wenn kein separates Metadatenetzwerk erstellt werden kann, verweigern Sie wenigstens den Datenverkehr vom externen WAN und von allen nicht vertrauenswürdigen Hosts im Netzwerk zu den Oracle HSM-Ports. Siehe [Abschnitt 1.2.2, „Netzwerkzugriff auf kritische Services beschränken“ \[8\]](#)

FC-Zoning

Mit FC-Zoning können Sie allen Servern, die keinen Zugriff auf die Datenträger benötigen, den Zugriff auf die Oracle HSM-Datenträger verweigern. Verwenden Sie einen separaten FC-Switch, um eine physische Verbindung nur mit den Servern herzustellen, die den Zugriff benötigen.

Zugriff auf SAN-Datenträgerkonfiguration absichern

Auf SAN RAID-Datenträger kann im Allgemeinen zu administrativen Zwecken mit TCP/IP oder eher mit HTTP zugegriffen werden. Sie müssen die Festplatten vor externen Zugriffen schützen, indem Sie den Systemverwaltungszugriff auf SAN RAID-Festplatten auf vertrauenswürdige Domains beschränken. Ändern Sie außerdem das Standardpasswort auf den Festplattenarrays.

Oracle HSM-Paket installieren

Installieren Sie immer nur Pakete, die Sie wirklich benötigen. Falls Sie keine hierarchische Speicherverwaltung wünschen, installieren Sie nur die QFS-Pakete. Die Standardberechtigungen für Oracle HSM-Dateien und Verzeichnisse sowie Eigentümer sollten nach der Installation nicht ohne vorherige gründliche Überlegung der Auswirkungen geändert werden.

Clientzugriff

Wenn Sie gemeinsam verwendete Clients konfigurieren möchten, bestimmen Sie, welche Clients Zugriff auf das Dateisystem in der Datei "hosts" haben müssen. Weitere Informationen finden Sie auf der Manpage hosts.fs(4). Konfigurieren Sie nur diejenigen Hosts, die Zugriff auf das gerade konfigurierte Dateisystem benötigen.

Oracle Solaris-Metadatenserver absichern

Weitere Informationen zum Absichern des Oracle Solaris-Betriebssystems finden Sie in "Oracle Solaris 10 - Sicherheitsbestimmungen" und "Oracle Solaris 11 - Sicherheitsbestimmungen". Mindestanforderungen sind ein sicheres Root-Passwort, die Installation der neuesten Version des Oracle Solaris-Betriebssystems sowie der neuesten Patches (insbesondere Sicherheitspatches).

Linux-Clients absichern

Weitere Informationen zum Absichern von Linux-Clients finden Sie in der Linux-Dokumentation. Mindestanforderungen sind ein sicheres Root-Passwort, die Installation der neuesten Version des Linux-Betriebssystems sowie der neuesten Patches (insbesondere Sicherheitspatches).

Sicherheit von Oracle HSM-Bändern

Verhindern Sie den externen Zugriff auf Oracle HSM-Bänder außerhalb von Oracle HSM, oder beschränken Sie derartige Zugriffe nur auf Administratoren. Gewähren Sie mithilfe von FC-Zoning nur dem MDS (oder dem potenziellen MDS bei konfiguriertem MDS-Backup) Zugriff auf die Bandlaufwerke. Solaris-Clients, die zur Verwendung von verteilter I/O konfiguriert werden, benötigen Zugriff auf Bandlaufwerke. Beschränken Sie ebenfalls den Zugriff auf Bandgerätedateien ausschließlich auf root. Durch den unberechtigten Zugriff auf Oracle HSM-Bänder können Benutzerdaten gefährdet oder gelöscht werden.

Backups

Einrichtung und Backups von Oracle HSM-Daten müssen mit den Befehlen samfsdump oder qfsdump durchgeführt werden. Schränken Sie den Zugriff auf Dumpbänder in dem für Oracle HSM-Bänder empfohlenen Maße ein.

2.2.1. Installation von SAM-Remote

Informationen zur sicheren Installation der SAM-Remote-Software finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

2.2.2. Installation der grafischen Benutzeroberfläche des Managers

Informationen zur sicheren Installation der grafischen Benutzeroberfläche des Managers finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

2.2.3. Konfiguration nach der Installation

Gehen Sie nach der Installation eines der Oracle HSM-Pakete durch die Sicherheitscheckliste in *Anhang A, Checkliste für sichere Bereitstellung* [19]

Sicherheitsfunktionen

Benutzer, die ein Dateisystem gemeinsam nutzen, müssen in folgenden Fällen aufmerksam werden, um Sicherheitslücken zu verhindern:

- Richtlinienverletzung durch Offenlegung von Dateisystemdaten
- Datenverlust
- Nicht erkannte Änderung von Daten

Diese Sicherheitsrisiken können durch ordnungsgemäße Konfiguration und Befolgen der Checkliste nach Abschluss der Installation in [Anhang A, Checkliste für sichere Bereitstellung \[19\]](#) minimiert werden.

3.1. Sicherheitsmodell

Die folgenden kritischen Sicherheitsfunktionen bieten Schutz vor Sicherheitslücken:

- Authentifizierung – Dadurch wird sichergestellt, dass nur berechtigten Personen Zugriff auf System und Daten gewährt wird.
- Autorisierung – Der Zugriff auf Systemberechtigungen und -daten wird kontrolliert. Diese Funktion baut auf der Authentifizierung auf, um zu gewährleisten, dass Benutzer nur den für sie vorgesehenen Zugriff erhalten.
- Prüfung – Ermöglicht Administratoren, versuchte Verletzungen der Authentifizierungsfunktion sowie versuchte oder erfolgreiche Verletzungen der Zugriffskontrolle zu erkennen.

3.1.1. Authentifizierung

Oracle HSM verwendet eine hostbasierte Benutzerauthentifizierung, um zu kontrollieren, wer Verwaltungsaufgaben durchführen darf. Die Verwaltung mithilfe der grafischen Benutzeroberfläche des Managers wird hauptsächlich durch Rollen gesteuert, die verschiedenen Benutzern zugewiesen sind. Die Verwaltung über die Befehlszeile ist dem Root-Benutzer vorbehalten.

3.1.2. Zugriffskontrolle

Die Zugriffskontrolle in Oracle HSM ist in zwei Bereiche unterteilt:

- Verwaltungszugriffskontrolle – Dadurch wird gesteuert, wer Verwaltungsaktionen für Oracle HSM durchführen darf. Die Kontrollen basieren auf Rollen, die Benutzern über die

grafische Benutzeroberfläche des Managers zugewiesen werden. Bei Befehlszeilenaktionen basieren die Kontrollen auf Root-Berechtigungen. Weitere Informationen zur grafischen Benutzeroberfläche des Managers finden Sie in der *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* unter:

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

- Datei-/Verzeichniszugriffskontrolle – Oracle HSM implementiert ein POSIX-kompatibles Dateisystem mit umfangreichen Zugriffskontrollen. Weitere Informationen finden Sie in der Oracle HSM-Dokumentation.

Sicherheitsinformationen für Entwickler

Entwickler haben in der Regel keinen direkten Zugang zu Oracle HSM. Die Ausnahme bilden die APIs *libsam* und *libsamrpc*. Diese beiden APIs bieten dieselbe Funktionalität. *libsam* wird nur für lokale Rechner verwendet, während *libsamrpc* mit dem MDS über *rpc(3)* kommuniziert, um die angeforderten Aktionen zu implementieren. Die Authentifizierung von Anforderungen beider Methoden basiert auf der UID und dem GID des aufrufenden Prozesses. Sie verfügen über dieselben Berechtigungen wie die Anforderungen über die Befehlszeile. Vergewissern Sie sich, dass Sie über einen gemeinsamen UID- und GID-Bereich für den MDS und die Clientsysteme verfügen.

Weitere Informationen finden Sie in den Manpages *intro_libsam(3)* und *intro_libsamrpc(3)*.

Checkliste für sichere Bereitstellung

Diese Sicherheitscheckliste enthält Richtlinien zur Gewährleistung der Sicherheit Ihrer Datenbank.

1. Legen Sie sichere Passwörter für Root und alle anderen Konten fest, denen Oracle HSM-Rollen zugewiesen wurden. Diese Richtlinie umfasst Folgendes:
 - Konten, denen von der grafischen Benutzeroberfläche des Managers Verwaltungsrollen zugewiesen wurden.
 - Benutzer-IDs *acsss*, *acsdb* und *acssa* (sofern verwendet)
 - Alle Verwaltungskonten im Festplattenarray
2. Wenn der Standardbenutzer *samadmin* in Verbindung mit der grafischen Benutzeroberfläche des Managers verwendet wird, ändern Sie das Standardpasswort umgehend in ein sicheres Kennwort. Verwenden Sie Root nicht in Verbindung mit der grafischen Benutzeroberfläche des Managers, sondern weisen Sie Rollen nach Bedarf anderen Benutzerkonten zu. Belegen Sie auch andere Konten mit einem sicheren Passwort.
3. Installieren Sie die Portfilterung auf WAN-Edge-Routern, um zu verhindern, dass Datenverkehr auf den unter [Abschnitt 1.2, „Allgemeine Sicherheitsgrundsätze“ \[8\]](#) aufgeführten Ports zu MDS oder Clients gelangt mit Ausnahme von SAM-Remote.
4. Trennen Sie FC-Festplatten und Bänder entweder physisch oder mithilfe von FC-Zoning, sodass die Festplatten nur auf dem MDS und auf Clients und die Bänder nur auf dem MDS und dem potenziellen MDS verfügbar sind. Durch diese Sicherheitsmaßnahme wird verhindert, dass Zwischenfälle aufgrund von Datenverlust als Folge von unabsichtlichem Überschreiben von Bändern oder Festplatten auftreten.
5. Vergewissern Sie sich, ob unter */dev* nur root und kein anderer Benutzer auf die Band- und Festplattendateien zugreifen kann. Dadurch werden unberechtigte Zugriffe auf und das Löschen von Oracle HSM-Daten verhindert.
6. Bei Oracle HSM handelt es sich um ein POSIX-Dateisystem mit umfangreichen Datei-/Verzeichnisberechtigungen einschließlich Zugriffskontrolllisten (ACL, Access Control List). Verwenden Sie sie bei Bedarf, um Benutzerdaten im Dateisystem zu schützen. Weitere Informationen finden Sie in der Oracle HSM-Dokumentation.
7. Erstellen Sie ausreichend Sicherungskopien gemäß den lokalen Richtlinien. Mithilfe von Sicherungen, die Teil eines Sicherheitskonzepts sind, können Daten, die unabsichtlich oder durch Unbefugte gelöscht wurden, wiederhergestellt werden. Ihre Sicherung sollte richtlinienkonform sein, wenn sie an einem anderen Speicherort abgelegt wird. Sicherungen müssen in demselben Maße wie Oracle HSM-Bänder und -Festplatten geschützt werden.

