

# **Oracle® Hierarchical Storage Manager and StorageTek QFS Software**

Guida per la sicurezza

Release 6.0

**E62076-01**

**Marzo 2015**

---

## Oracle® Hierarchical Storage Manager and StorageTek QFS Software

Guida per la sicurezza

### E62076-01

copyright © 2015, Oracle e/o relative consociate. Tutti i diritti riservati.

Il software e la relativa documentazione vengono distribuiti sulla base di specifiche condizioni di licenza che prevedono restrizioni relative all'uso e alla divulgazione e sono inoltre protetti dalle leggi vigenti sulla proprietà intellettuale. Ad eccezione di quanto espressamente consentito dal contratto di licenza o dalle disposizioni di legge, nessuna parte può essere utilizzata, copiata, riprodotta, tradotta, diffusa, modificata, concessa in licenza, trasmessa, distribuita, presentata, eseguita, pubblicata o visualizzata in alcuna forma o con alcun mezzo. La decodificazione, il disassemblaggio o la decompilazione del software sono vietati, salvo che per garantire l'interoperabilità nei casi espressamente previsti dalla legge.

Le informazioni contenute nella presente documentazione potranno essere soggette a modifiche senza preavviso. Non si garantisce che la presente documentazione sia priva di errori. Qualora l'utente riscontrasse dei problemi, è pregato di segnalarli per iscritto a Oracle.

Qualora il software o la relativa documentazione vengano forniti al Governo degli Stati Uniti o a chiunque li abbia in licenza per conto del Governo degli Stati Uniti, sarà applicabile la clausola riportata di seguito.

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.

Il presente software o hardware è stato sviluppato per un uso generico in varie applicazioni di gestione delle informazioni. Non è stato sviluppato né concepito per l'uso in campi intrinsecamente pericolosi, incluse le applicazioni che implicano un rischio di lesioni personali. Qualora il software o l'hardware venga utilizzato per impieghi pericolosi, è responsabilità dell'utente adottare tutte le necessarie misure di emergenza, backup e di altro tipo per garantirne la massima sicurezza di utilizzo. Oracle Corporation e le sue consociate declinano ogni responsabilità per eventuali danni causati dall'uso del software o dell'hardware per impieghi pericolosi.

Oracle e Java sono marchi registrati di Oracle e/o delle relative consociate. Altri nomi possono essere marchi dei rispettivi proprietari.

Intel e Intel Xeon sono marchi o marchi registrati di Intel Corporation. Tutti i marchi SPARC sono utilizzati in base alla relativa licenza e sono marchi o marchi registrati di SPARC International, Inc. AMD, Opteron, il logo AMD e il logo AMD Opteron sono marchi o marchi registrati di Advanced Micro Devices. UNIX è un marchio registrato di The Open Group.

Il software o l'hardware e la documentazione possono includere informazioni su contenuti, prodotti e servizi di terze parti o collegamenti agli stessi. Oracle Corporation e le sue consociate declinano ogni responsabilità ed escludono espressamente qualsiasi tipo di garanzia relativa a contenuti, prodotti e servizi di terze parti se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle. Oracle Corporation e le sue consociate non potranno quindi essere ritenute responsabili per qualsiasi perdita, costo o danno causato dall'accesso a contenuti, prodotti o servizi di terze parti o dall'utilizzo degli stessi se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle.

---

# Indice

---

<b>Prefazione</b> .....	5
Destinatari .....	5
Accesso facilitato alla documentazione .....	5
Convenzioni tipografiche .....	5
Prompt delle shell in esempi di comandi .....	6
<b>1. Panoramica</b> .....	7
1.1. Panoramica del prodotto .....	7
1.2. Principi di sicurezza generali .....	8
1.2.1. Mantenere aggiornato il software .....	8
1.2.2. Limitare accesso di rete a servizi fondamentali .....	8
1.2.3. Seguire il principio dei privilegi minimi .....	8
1.2.4. Monitoraggio dell'attività di sistema .....	9
1.2.5. Restare aggiornati per quanto riguarda le informazioni di sicurezza più recenti .....	9
<b>2. Installazione sicura</b> .....	11
2.1. Informazioni sull'ambiente .....	11
2.1.1. Quali risorse è necessario proteggere? .....	11
2.1.2. Da chi è necessario proteggere le risorse? .....	12
2.1.3. Cosa accade se la protezione delle risorse strategiche fallisce? .....	12
2.2. Topologie di distribuzione raccomandate .....	12
2.2.1. Installazione di SAM-Remote .....	13
2.2.2. Installazione della GUI di Manager .....	13
2.2.3. Configurazione post-installazione .....	14
<b>3. Funzioni di sicurezza</b> .....	15
3.1. Modello di sicurezza .....	15
3.1.1. Autenticazione .....	15
3.1.2. Controllo degli accessi .....	15
<b>4. Considerazioni di sicurezza per gli sviluppatori</b> .....	17
<b>A. Lista di controllo per la distribuzione sicura</b> .....	19



# Prefazione

---

Nella Guida per la sicurezza Oracle Hierarchical Storage Manager and StorageTek QFS Software vengono fornite informazioni sul prodotto Oracle Hierarchical Storage Manager and QFS e vengono descritti i principi generali di sicurezza delle applicazioni.

## Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'uso delle funzioni di sicurezza nonché nell'installazione e configurazione sicure di Oracle Hierarchical Storage Manager and StorageTek QFS Software.

## Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program su <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Accesso a Oracle Support

I clienti Oracle che hanno acquistato il servizio di supporto, hanno accesso al supporto elettronico mediante My Oracle Support. Per informazioni, visitare <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per i non utenti.

## Convenzioni tipografiche

Nella seguente tabella vengono descritte le convenzioni tipografiche utilizzate in questo manuale.

Carattere tipografico	Descrizione	Esempio
<i>AaBbCc123</i>	Nomi di comandi e output del computer sullo schermo	<i>Utilizzare ls -a per elencare tutti i file.</i>
<b>AaBbCc123</b>	Input che l'utente immette quando viene visualizzato l'output del computer sullo schermo	<i>nome_computer% su</i> <i>Password:</i>
<i>aabbcc123</i>	Segnaposto da sostituire con il nome o il valore reale.	Il comando per la rimozione di un file è <i>rm nome file</i> .
<i>AaBbCc123</i>	Titoli di manuali, termini citati per la prima volta, termini particolarmente importanti nel contesto	Vedere il Capitolo 6 del <i>Manuale utente</i> .  La <i>cache</i> è una copia memorizzata localmente.  Questo file non deve essere modificato.

Carattere tipografico	Descrizione	Esempio
		Nota: alcuni elementi evidenziati vengono visualizzati in grassetto online.

## Prompt delle shell in esempi di comandi

Nella tabella seguente sono riportati i prompt di sistema UNIX e superutente predefiniti per le shell incluse nel sistema operativo Oracle Solaris. Il prompt di sistema predefinito visualizzato negli esempi di comandi varia in base alla release di Oracle Solaris.

Shell	Prompt
Bash shell, Korn shell e Bourne shell	\$
Bash shell, Korn shell e Bourne shell per utente privilegiato	#
Cshell	nome_computer%
Cshell per utente privilegiato	nome_computer#

---

## Panoramica

In questo capitolo viene fornita una panoramica del prodotto Oracle Hierarchical Storage Manager and StorageTek QFS Software e vengono descritti i principi generali di sicurezza delle applicazioni.

### 1.1. Panoramica del prodotto

Oracle Hierarchical Storage Manager and StorageTek QFS Software è un file system condiviso con funzionalità di gestione archivio memorizzazione gerarchica. Il prodotto è composto dai seguenti componenti principali:

#### **Pacchetto StorageTek QFS**

Include il file system QFS a elevate prestazioni che può essere configurato in modalità standalone o condivisa. Quando viene utilizzata la configurazione standalone, QFS viene configurato su un singolo sistema e non con client condivisi. QFS utilizza operazioni vnode VFS standard per interfacciarsi con i sistemi operativi Oracle Solaris e Linux.

I pacchetti di installazione QFS sono SUNWqfsr e SUNWqfsu. In questi pacchetti non è incluso il componente Oracle Hierarchical Storage Manager (HSM).

La configurazione di QFS in modalità standalone senza client condivisi è la più sicura. In questa configurazione non vengono eseguiti daemon e non sono disponibili connessioni remote diverse da quelle da Fibre Channel (FC) a disco. La configurazione di QFS in modalità condivisa include connessioni FC a disco e una connessione TCP/IP tra il client e il server di metadati (MDS).

#### **Pacchetto Oracle HSM**

Include il file system QFS e il codice necessario per eseguire Oracle HSM. I pacchetti di installazione di Oracle HSM sono SUNWsamfsr e SUNWsamfsu. Se non è necessaria la gestione della memorizzazione gerarchica, installare *solo* il pacchetto StorageTek QFS.

#### **SAM-Remote**

Consente di accedere alle librerie a nastro remote e alle unità mediante connessioni WAN (Wide Area Network) TCP/IP. StorageTek SAM-Remote fornisce una forma di ripristino di emergenza tramite individuazione remota di risorse nastro. È possibile installare SAM-Remote con i pacchetti QFS o SAM-QFS, ma è necessario attivare e configurare SAM-Remote separatamente. Per ulteriori informazioni su SAM-Remote, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

### **Interfaccia utente grafica di Manager**

L'interfaccia grafica utente (GUI) di Manager, fsmgr, viene eseguita su MDS ed è possibile accedervi in remoto tramite un browser Web. L'accesso è consentito mediante la porta 6789 ([https:// hostname:6789](https://hostname:6789)).

Per utilizzare fsmgr, è necessario eseguire il login come utente valido su MDS e aggiungere determinati ruoli all'account utente. Per informazioni sull'installazione e sulla configurazione della GUI di Manager, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

## **1.2. Principi di sicurezza generali**

Le seguenti sezioni descrivono i principi fondamentali necessari per utilizzare in maniera sicura qualsiasi applicazione.

### **1.2.1. Mantenere aggiornato il software**

Tenere aggiornata la versione di Oracle HSM in esecuzione. È possibile trovare versioni correnti del software da scaricare sul sito Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>).

### **1.2.2. Limitare accesso di rete a servizi fondamentali**

Oracle HSM utilizza le seguenti porte TCP/IP:

- tcp/7105 è utilizzata per il traffico di metadati tra il client e MDS
- tcp/1000 è utilizzata per SAM-Remote
- tcp/6789 è la porta HTTP utilizzata da un browser per eseguire la connessione a fsmgr
- tcp/5012 è utilizzato per sam-rpcd

---

**Nota:**

Per il traffico client bidirezionale MDS, prendere in considerazione l'impostazione di una rete separata senza interconnessione con la WAN esterna. Questa configurazione impedisce l'esposizione a rischi esterni e garantisce inoltre che il traffico esterno non limiti le prestazioni MDS.

---

### **1.2.3. Seguire il principio dei privilegi minimi**

Fornire all'utente o all'amministratore i privilegi minimi necessari per portare a termine le attività da eseguire. Nella GUI di Manager sono disponibili diversi ruoli da assegnare agli utenti. Questi ruoli garantiscono privilegi di diverso tipo e quantità. L'esecuzione di attività di amministrazione dalla riga di comando richiede un'autorizzazione root.

Per ulteriori informazioni sull'uso della GUI di Manager, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation*



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

### 1.2.4. Monitoraggio dell'attività di sistema

Monitorare l'attività del sistema per stabilire la corretta esecuzione di Oracle HSM e la presenza di attività anomale. Verificare i seguenti file di log:

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

### 1.2.5. Restare aggiornati per quanto riguarda le informazioni di sicurezza più recenti

È possibile accedere a diverse fonti di informazioni di sicurezza. Per avvisi e informazioni sulla sicurezza relativi a un'ampia varietà di prodotti software, vedere <http://www.us-cert.gov>. Per informazioni specifiche su SAM-QFS, vedere [https://communities.oracle.com/portal/server.pt/community/sam\\_qfs\\_storage\\_archive\\_manager\\_and\\_sun\\_qfs/401](https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401). Il modo migliore per essere sempre aggiornati sulle questioni relative alla sicurezza è quello di utilizzare la versione più aggiornata del software Oracle HSM.



---

## Installazione sicura

---

In questo capitolo viene presentato il processo di pianificazione di un'installazione sicura e sono descritte alcune topologie di distribuzione raccomandate per i sistemi.

### 2.1. Informazioni sull'ambiente

Per comprendere meglio le esigenze di sicurezza, è necessario rispondere alle domande riportate di seguito.

#### 2.1.1. Quali risorse è necessario proteggere?

È possibile proteggere tutte le risorse presenti nell'ambiente di produzione. Considerare il tipo di risorse che si desidera proteggere quando si stabilisce il livello di sicurezza da fornire.

Quando si utilizza Oracle HSM, proteggere le seguenti risorse:

##### **Disco metadati e dati principali**

Queste risorse disco vengono utilizzate per generare il file system Oracle HSM. Sono solitamente collegate tramite Fibre Channel (FC). Un accesso indipendente a questi dischi (non tramite Oracle HSM) presenta rischi per la sicurezza poiché solitamente vengono ignorate le autorizzazioni per file e directory Oracle HSM. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue lettura o scrittura dei dischi FC, o da un sistema interno che può accidentalmente fornire accesso non root a file dispositivo raw.

##### **Nastri Oracle HSM**

L'accesso indipendente ai nastri, solitamente in una libreria a nastro, in cui i dati del file sono scritti durante la fase di disinstallazione da un file system Oracle HSM, è un rischio per la sicurezza.

##### **Nastri dump Oracle HSM**

Dump file system creati da samfsdump che contengono dati e metadati. Questi dati e metadati dovrebbero essere protetti dall'accesso eseguito da utenti diversi dall'amministratore di sistema nel corso di un dump di routine o di attività di ripristino.

##### **Server di metadati (MDS) Oracle HSM**

I client Oracle HSM richiedono l'accesso TCP/IP a MDS. Tuttavia, è necessario garantire che i client siano protetti da accesso WAN esterno.

##### **File e impostazioni di configurazione**

Le impostazioni di configurazione Oracle HSM devono essere protette dall'accesso non di tipo amministratore. In generale, queste impostazioni sono protette automaticamente da

Oracle HSM quando si utilizza la GUI di Manager. Tenere presente che rendere i file di configurazione modificabili da parte di utenti senza diritti di amministrazione costituisce un rischio per la sicurezza.

### 2.1.2. Da chi è necessario proteggere le risorse?

In generale, le risorse descritte nella sezione precedente devono essere protette da tutti gli accessi non root e non di amministratore su un sistema configurato, o da un sistema esterno non autorizzato con accesso a queste risorse mediante fabric WAN o FC.

### 2.1.3. Cosa accade se la protezione delle risorse strategiche fallisce?

Gli errori nella protezione delle risorse strategiche possono comprendere accesso non appropriato (accesso ai dati non conforme alle autorizzazioni dei file POSIX Oracle HSM ordinarie) e danneggiamento dei dati (scrittura su disco o nastro non conforme alle autorizzazioni ordinarie).

## 2.2. Topologie di distribuzione raccomandate

In questa sezione viene descritto come installare e configurare in modo sicuro un componente infrastruttura. Per informazioni sull'installazione di Oracle HSM, consultare *Oracle Hierarchical Storage Manager Release 6.0 Customer Documentation Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>.

Considerare i seguenti punti quando si installa e configura Oracle HSM:

#### **Rete di metadati distinta**

Per connettere client Oracle HSM a server MDS, fornire una rete TCP/IP distinta e un hardware switch non connesso a una rete WAN. Poiché il traffico dei metadati è implementato mediante TCP/IP, un attacco esterno ai danni di questo traffico è teoricamente possibile. Configurando una rete di metadati separata è possibile ridurre i rischi e ottenere prestazioni migliori. È possibile ottenere prestazioni migliorate fornendo un percorso dati garantito ai metadati. Se non è possibile ottenere una rete di metadati separata, bloccare il traffico alle porte Oracle HSM dalla rete WAN esterna e da qualsiasi host non attendibile sulla rete. Consultare la sezione [Sezione 1.2.2, «Limitare accesso di rete a servizi fondamentali» \[8\]](#).

#### **Suddivisione in zone FC**

Utilizzare la suddivisione in zone FC per impedire l'accesso ai dischi Oracle HSM da qualsiasi server che non necessita di accesso ai dischi. È preferibile utilizzare un Fibre Channel switch separato per eseguire il collegamento fisico solo ai server che necessitano di accesso.

#### **Proteggere l'accesso alla configurazione dei dischi SAN**

In genere è possibile accedere ai dischi RAID SAN per scopi di amministrazione mediante TCP/IP o più specificatamente mediante HTTP. È necessario proteggere i dischi dagli accessi esterni limitando l'accesso per scopi amministrativi ai dischi RAID SAN ai

soli sistemi con un dominio attendibile. Inoltre, modificare la password predefinita negli array del disco.

### **Installare il pacchetto Oracle HSM**

Installare innanzitutto solo i pacchetti richiesti. Ad esempio, se non è necessaria la gestione della memorizzazione gerarchica, installare solo i pacchetti QFS. I proprietari e le autorizzazioni di file e directory Oracle HSM predefiniti non devono essere modificati dopo l'installazione senza aver preso in esame le implicazioni di tali modifiche a carico della sicurezza.

### **Accesso client**

Se si desidera configurare client condivisi, stabilire quali client devono avere accesso ai file system nel file hosts. Consultare la pagina `manhosts.fs(4)`. Configurare solo gli host che necessitano di accesso allo specifico file system configurato.

### **Impostare la protezione avanzata del server metadati Oracle Solaris**

Per informazioni sulla protezione avanzata del sistema operativo Oracle Solaris, consultare "Oracle Solaris 10 Security Guidelines" e "Oracle Solaris 11 Security Guidelines". Come precauzioni minime, scegliere una buona password root, installare una versione aggiornata del sistema operativo Oracle Solaris e mantenere aggiornate le patch, specialmente quelle di sicurezza.

### **Impostare la protezione avanzata dei client Linux**

Verificare la documentazione di Linux per informazioni sull'impostazione della protezione avanzata dei client Linux. Come precauzioni minime, scegliere una buona password root, installare una versione aggiornata del sistema operativo Linux e mantenere aggiornate le patch, specialmente quelle di sicurezza.

### **Sicurezza dei nastri Oracle HSM**

Evitare l'accesso esterno ai nastri Oracle HSM dall'esterno di Oracle HSM oppure limitare tale accesso solo agli amministratori. Utilizzare la suddivisione in zone FC per limitare l'accesso alle unità nastro solo a MDS (o a MDS potenziale se è configurato un MDS di backup). I client Solaris configurati per l'utilizzo dell'I/O distribuito necessiteranno dell'accesso alle unità nastro. Inoltre, limitare l'accesso al file dispositivo a nastro consentendo solo le autorizzazioni root. Accessi non autorizzati ai nastri Oracle HSM possono compromettere o distruggere i dati dell'utente.

### **Backup**

Impostare ed eseguire backup di dati Oracle HSM mediante i comandi `samfsdump` o `qfsdump`. Limitare l'accesso ai nastri dump come raccomandato per i nastri Oracle HSM.

## **2.2.1. Installazione di SAM-Remote**

Per informazioni sull'installazione sicura del software SAM-Remote, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

## **2.2.2. Installazione della GUI di Manager**

Per informazioni sull'installazione sicura della GUI Manager, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation*

*Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

### **2.2.3. Configurazione post-installazione**

Dopo aver installato i pacchetti Oracle HSM, consultare la lista di controllo di sicurezza in [Appendice A, \*Lista di controllo per la distribuzione sicura\* \[19\]](#)

---

## Funzioni di sicurezza

Per evitare potenziali rischi di sicurezza, è necessario che i clienti con file system condiviso prestino attenzione ai seguenti elementi:

- Diffusione di dati di file system in violazione dei criteri
- Perdita di dati
- Modifiche non rilevate ai dati

È possibile minimizzare questi rischi per la sicurezza eseguendo una corretta configurazione e consultando la lista di controllo in seguito all'installazione in [Appendice A, Lista di controllo per la distribuzione sicura \[19\]](#).

### 3.1. Modello di sicurezza

Le funzioni di sicurezza fondamentali per la protezione dai rischi sono:

- Autenticazione – Consente di garantire che solo gli utenti autorizzati abbiano accesso al sistema e ai dati.
- Autorizzazione – Controllo dell'accesso a dati e privilegi di sistema. Questa funzione consente di creare l'autenticazione, così da garantire che gli utenti dispongano unicamente dell'accesso appropriato.
- Audit – Consente agli amministratori di rilevare tentativi di violazione del meccanismo di autenticazione o violazioni del controllo degli accessi.

#### 3.1.1. Autenticazione

Oracle HSM utilizza l'autenticazione dell'utente basata su host per controllare quali utenti possono eseguire attività di amministrazione. L'amministrazione mediante la GUI di Manager è controllata principalmente da ruoli assegnati a vari utenti. L'amministrazione mediante la riga di comando è limitata all'utente root.

#### 3.1.2. Controllo degli accessi

Il controllo degli accessi in Oracle HSM è suddiviso in due parti:

- Controllo degli accessi amministrativi – Consente di controllare gli utenti che possono eseguire attività amministrative per Oracle HSM. I controlli sono basati su ruoli assegnati a utenti mediante la GUI di Manager. Per le operazioni della riga di comando, i controlli

sono basati su autorizzazioni root. Per ulteriori informazioni sulla GUI di Manager, consultare *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library* all'indirizzo: <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

- Controllo degli accessi file/directory – Oracle HSM consente di implementare un file system conforme a POSIX con un ampio set di controlli degli accessi. Per ulteriori informazioni consultare la documentazione di Oracle HSM.



---

## Considerazioni di sicurezza per gli sviluppatori

---

Gli sviluppatori generalmente non utilizzano direttamente Oracle HSM. Due eccezioni sono riscontrabili nell'API *libsam* e nell'API *libsamrpc*. Questi due API forniscono la stessa funzionalità. *libsam* è solo per un computer locale, mentre *libsamrpc* consente la comunicazione con MDS mediante *rpc(3)* per l'implementazione delle azioni richieste. L'autenticazione di richieste eseguite da uno dei due metodi è basata su UID e GID del processo chiamante. Le autorizzazioni sono le stesse utilizzate dalle richieste eseguite mediante la riga di comando. Assicurarsi di avere a disposizione uno spazio UID e GID comune per MDS e sistemi client.

Per ulteriori informazioni, consultare le pagine man *intro\_libsam(3)* e *intro\_libsamrpc(3)*.



---

# Appendice A

---

## Lista di controllo per la distribuzione sicura

La lista di controllo di sicurezza include linee guida per proteggere il database.

1. Impostare password sicure per l'account root e per tutti gli altri account ai quali sono assegnati ruoli Oracle HSM. Questa linea guida include:
  - Qualsiasi account con ruoli amministrativi assegnati dalla GUI di Manager.
  - ID utente *acsss*, *acsdb* e *acssa* (se utilizzati).
  - Qualsiasi account amministrativo array di dischi.
2. Se si utilizza l'utente predefinito *samadmin* con la GUI di Manager, sostituire immediatamente la password predefinita installata con una più sicura. Non utilizzare account root con la GUI Manager, assegnare piuttosto ruoli ad altri account utente quando necessario. Proteggere anche altri account con password sicure.
3. Installare il filtro applicato alle porte su edge router WAN per evitare il traffico sulle porte elencate in [Sezione 1.2, «Principi di sicurezza generali» \[8\]](#) da MDS o client, tranne quando necessario per Sun SAM-Remote.
4. Separare i dischi FC e i nastri fisicamente o attraverso la suddivisione in zone FC, così da rendere i dischi accessibili solo da MDS e client e i nastri da MDS e MDS potenziali. In questo modo si previene la perdita di dati provocata dalla sovrascrittura accidentale di nastri o dischi.
5. Verificare */dev* per garantire che i file dispositivo disco e nastro non siano accessibili a utenti diversi da quelli root. In questo modo si previene l'accesso non appropriato o la distruzione dei dati Oracle HSM.
6. Oracle HSM è un file system POSIX e fornisce un ampio set di autorizzazioni per directory/file, incluse le liste di controllo dell'accesso (ACL, Access Control List). Utilizzarli quando necessario per proteggere i dati utente nel file system. Per ulteriori informazioni, consultare la documentazione di Oracle HSM.
7. Impostare un set di dump di backup appropriato basato sui criteri locali. I backup sono fondamentali per la sicurezza e forniscono una soluzione per il ripristino dei dati accidentalmente smarriti o violati. Il backup dovrebbe includere alcuni criteri durante il trasporto in un'altra posizione. Il livello di protezione dei backup deve essere uguale a quello previsto per i dischi e i nastri Oracle HSM.

