

**Guida per la sicurezza di Oracle®
Hardware Management Pack per Oracle
Solaris 11.2**



N. di parte: E56558-02
Settembre 2015

N. di parte: E56558-02

Copyright © 2014, 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.

Accessibilità alla documentazione

Per informazioni sull'impegno di Oracle per l'accessibilità, visitare il sito Oracle Accessibility Program all'indirizzo: <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=dacacc>.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso il portale Oracle My Oracle Support. Per tutte le necessarie informazioni, si prega di visitare il sito <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oppure <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per clienti non utenti.

Indice

Panoramica del prodotto e della sicurezza per l'applicazione	7
Informazioni su Oracle Hardware Management Pack per Oracle Solaris	7
Principi di sicurezza di base	8
Riepilogo della sicurezza di Oracle Hardware Management Pack	9
 Protezione di Oracle Hardware Management Pack	 11
Interfaccia di interconnessione tra host e ILOM	11
Scelta di salvare le credenziali in un file	12
Scelta delle impostazioni di sicurezza SNMP	12
 Installazione o disinstallazione dei componenti di Oracle Hardware Management Pack	 15
Installazione dei componenti	15
Disinstallazione dei componenti	15

Panoramica del prodotto e della sicurezza per l'applicazione

In questa sezione viene fornita una panoramica del prodotto Oracle Hardware Management Pack (HMP) e dei principi generali della sicurezza dell'applicazione.

Vengono trattati gli argomenti seguenti:

- [sezione chiamata «Informazioni su Oracle Hardware Management Pack per Oracle Solaris» \[7\]](#)
- [sezione chiamata «Principi di sicurezza di base» \[8\]](#)
- [sezione chiamata «Riepilogo della sicurezza di Oracle Hardware Management Pack» \[9\]](#)

Informazioni su Oracle Hardware Management Pack per Oracle Solaris

Oracle Hardware Management Pack per Oracle Solaris è disponibile per molti server basati su x86 e per alcuni server basati su SPARC. In Oracle Hardware Management Pack sono disponibili due componenti: un agente di monitoraggio SNMP e una gamma di strumenti CLI (interfaccia della riga di comando) per la gestione dei server.

Grazie ai plugin SNMP di Hardware Management Agent, è possibile utilizzare il protocollo SNMP per monitorare i server Oracle e i moduli server nel centro dati, con il vantaggio di non dover eseguire la connessione a due punti di gestione, l'host e Oracle ILOM. Questa funzionalità consente di utilizzare un singolo indirizzo IP (quello dell'host) per monitorare più server e moduli server.

I plugin SNMP di Hardware Management Agent vengono eseguiti sul sistema operativo host dei server Oracle. I plugin SNMP utilizzano le Oracle Hardware Storage Access Library per comunicare con il processore di servizio. Le informazioni sullo stato corrente del server vengono recuperate automaticamente da Hardware Management Agent. Per ulteriori informazioni su Hardware Management Agent, consultare il manuale *Oracle Server Management Agents User's Guide*.

È possibile utilizzare gli strumenti CLI di Oracle Server per configurare i server Oracle. Per un elenco degli strumenti, consultare il manuale *Oracle Server CLI Tools User's Guide*.

Consultare la documentazione di Oracle Hardware Management Pack per Oracle Solaris per ulteriori informazioni sulle funzionalità e sull'uso.

- Libreria della documentazione di Oracle Hardware Management Pack per Oracle Solaris all'indirizzo <http://www.oracle.com/goto/ohmp/solarisdocs>
- Informazioni di carattere generale su Oracle ILOM sono disponibili a questo indirizzo: <http://www.oracle.com/goto/ilom/docs>

Principi di sicurezza di base

I principi di sicurezza di base sono quattro: accesso, autenticazione, autorizzazione e accounting.

- **Accesso**

Eseguire controlli fisici e del software per proteggere l'hardware o i dati da eventuali intrusioni.

- Per l'hardware, i limiti di accesso sono in genere limiti all'accesso fisico.
- Per il software, i limiti di accesso comprendono in genere sia mezzi fisici che mezzi virtuali.
- Il firmware può essere modificato solo tramite il processo di aggiornamento Oracle.

- **Autenticazione**

Impostare tutte le funzioni di autenticazione, ad esempio un sistema di password, nei sistemi operativi della piattaforma per verificare l'effettiva identità degli utenti.

L'autenticazione fornisce vari livelli di sicurezza tramite misure quali i badge e le password. Ad esempio, assicurarsi che il personale utilizzi in modo corretto i badge dipendente per accedere a una sala computer.

- **Autorizzazione**

L'autorizzazione consente al personale della società di utilizzare l'hardware e il software solo se correttamente formato e qualificato per tale scopo.

Ad esempio, impostare un sistema di autorizzazioni di lettura, scrittura ed esecuzione per controllare l'accesso utente a comandi, spazio su disco, dispositivi e applicazioni.

- **Accounting**

Il personale di IT del cliente può utilizzare le funzioni software e hardware Oracle per monitorare le attività di login e gestire i magazzini hardware.

- Utilizzare i log di sistema per monitorare i login utente. In particolare, utilizzare i log di sistema per monitorare gli account di amministratore di sistema e di servizio poiché tali account dispongono di privilegi per l'accesso a comandi potenti.
- Rimuovere periodicamente i file di log quando superano una determinata dimensione nel rispetto dei criteri in uso nella società del cliente. In genere i log rimangono attivi per lunghi periodi di tempo, pertanto è importante garantirne la gestione.

- Utilizzare i numeri di serie dei componenti per tenere traccia degli asset del sistema a scopo di inventario. I numeri parte Oracle sono elettronicamente registrati su tutte le schede, i moduli e le schede madri.

Riepilogo della sicurezza di Oracle Hardware Management Pack

Di seguito sono riportati degli elementi di sicurezza importanti da tenere presenti durante la configurazione di tutti gli strumenti di gestione del sistema.

- *I prodotti di gestione del sistema possono essere utilizzati per ottenere un ambiente root di boot.*

Un ambiente root di boot consente di accedere a Oracle ILOM, Oracle System Assistant e ai dischi rigidi.

- *I prodotti di gestione del sistema includono potenti strumenti la cui esecuzione richiede privilegi di amministratore o root.*

Questo livello di accesso consente di modificare la configurazione hardware e di eliminare i dati.

Protezione di Oracle Hardware Management Pack

Per Oracle Solaris, i componenti di Oracle Hardware Management Pack utilizzati più di frequente sono già installati. Per garantire la sicurezza, potrebbero essere richiesti task di configurazione aggiuntivi.

- [sezione chiamata «Interfaccia di interconnessione tra host e ILOM» \[11\]](#)
- [sezione chiamata «Scelta di salvare le credenziali in un file» \[12\]](#)
- [sezione chiamata «Scelta delle impostazioni di sicurezza SNMP» \[12\]](#)

Interfaccia di interconnessione tra host e ILOM

L'interfaccia di interconnessione tra host e ILOM consente ai client nel sistema operativo dell'host di comunicare con Oracle ILOM tramite un'interconnessione ad alta velocità interna. Questa interconnessione viene implementata mediante una connessione Ethernet tramite USB interna, in cui è in esecuzione uno stack IP. In Oracle ILOM e nell'host sono disponibili indirizzi IP interni non routable per la comunicazione su questo canale. Questa connessione è abilitata per impostazione predefinita nel sistema operativo di Oracle Solaris.

La connessione a Oracle ILOM mediante l'interconnessione tra host e ILOM richiede un'autenticazione, come se la connessione provenisse dalla rete e fosse diretta a una porta di gestione Oracle ILOM. Tutti i servizi o i protocolli visibili sulla rete di gestione sono disponibili mediante l'interconnessione LAN all'host. Ad esempio, è possibile utilizzare un browser Web sull'host per accedere all'interfaccia Web di Oracle ILOM o utilizzare un client shell sicuro per eseguire la connessione all'interfaccia della riga di comando di Oracle ILOM. In ogni caso, è necessario fornire un nome utente e una password validi per utilizzare l'interconnessione LAN.

Oracle consiglia che la rete supporti RFC 3927 e possa disporre di indirizzi IPv4 con collegamento locale. Inoltre, è necessario prestare attenzione per assicurarsi che il sistema operativo non agisca da bridge o router. Questo consente di assicurare che il traffico di gestione tra l'host e Oracle ILOM nell'interconnessione tra host e ILOM rimanga privato.

- Libreria della documentazione di Oracle Hardware Management Pack per Oracle Solaris:
<http://www.oracle.com/goto/ohmp/solarisdocs>

Scelta di salvare le credenziali in un file

A partire da Oracle Solaris 11.2 SRU 14, questa funzione è stata disabilitata.

Gli strumenti `ilomconfig` e `fwupdate`, che fanno parte di Oracle Hardware Management Pack per Oracle Solaris, possono connettersi a Oracle ILOM tramite l'interconnessione tra host e ILOM ad alta velocità. Poiché l'interconnessione tra host e ILOM richiede l'autenticazione, è necessario eseguire tale operazione in Oracle ILOM per ogni richiamo di questi strumenti. Pertanto è possibile inserire le credenziali nella cache di un file in modo che possano essere utilizzate automaticamente dagli strumenti. Questo impedisce di dover incorporare password non cifrate in script che utilizzano gli strumenti di Oracle Hardware Management Pack.

Lo strumento `ilomconfig` può essere utilizzato per memorizzare il nome utente e la password in un file cifrato di sola lettura root. Se questo file viene rilevato quando si utilizza `ilomconfig` o `fwupdate` per accedere a Oracle ILOM, vengono utilizzate le credenziali inserite nella cache. In alternativa, è possibile specificare il nome utente e la password sulla riga di comando per ogni richiamo dello strumento.

L'algoritmo di cifratura usato è univoco per ogni sistema. Tuttavia, se viene trovata la chiave, è possibile decifrare il file e visualizzare il nome utente e la password.

A tale scopo, Oracle consiglia di creare una password univoca su ciascun Oracle ILOM in modo che non sia possibile utilizzare una password compromessa su altri sistemi Oracle ILOM.

Vedere il documento *Oracle CLI Tools for Oracle Solaris User's Guide* per istruzioni su come salvare le credenziali in un file.

- Libreria della documentazione di Oracle Hardware Management Pack per Oracle Solaris:
<http://www.oracle.com/goto/ohmp/solarisdocs>

Scelta delle impostazioni di sicurezza SNMP

Oracle Hardware Management Pack contiene un modulo del plugin SNMP che estende l'agente SNMP nativo nel sistema operativo host per fornire funzionalità aggiuntive di Oracle MIB. È particolarmente importante tenere presente che Oracle Hardware Management Pack non contiene un agente SNMP. Nel sistema operativo di Oracle Solaris è stato aggiunto un modulo a Solaris Management Agent.

Allo stesso modo, tutte le impostazioni di sicurezza relative a SNMP per il plugin SNMP di Oracle Hardware Management Pack vengono determinate dalle impostazioni dell'agente o servizio SNMP nativo e non dal plugin. Le impostazioni SNMP potrebbero includere quanto segue.

- SNMPv1/v2c. Questa versione non fornisce alcuna cifratura e utilizza stringhe comunità come forma di autenticazione. Le stringhe comunità vengono inviate in testo non cifrato sulla rete e sono solitamente condivise da un gruppo di utenti e non limitate a uno solo.

- **SNMPv3.** Questa versione utilizza la cifratura per fornire un canale sicuro e dispone di singoli nomi utente e password. Le password utente SNMPv3 sono localizzate, in modo da poter essere archiviate in maniera sicura nelle stazioni di gestione.

Oracle consiglia di utilizzare SNMPv3 se supportato dall'agente SNMP nativo. Vedere la documentazione di Oracle Solaris per istruzioni sulla configurazione di net-snmp per SNMPv3.

Installazione o disinstallazione dei componenti di Oracle Hardware Management Pack

Vengono trattati gli argomenti seguenti:

- [sezione chiamata «Installazione dei componenti» \[15\]](#)
- [sezione chiamata «Disinstallazione dei componenti» \[15\]](#)

Installazione dei componenti

Oracle Hardware Management Pack per Oracle Solaris è composto da una serie di strumenti preinstallati. È possibile installare altri pacchetti di componenti di Oracle Hardware Management Pack che non sono preinstallati utilizzando Oracle Solaris Image Packaging System (IPS).

Solo un amministratore con privilegi root può installare i pacchetti di Oracle Hardware Management Pack.

- Libreria della documentazione di Oracle Hardware Management Pack per Oracle Solaris: <http://www.oracle.com/goto/ohmp/solarisdocs>

Disinstallazione dei componenti

È possibile disinstallare i pacchetti di Oracle Hardware Management Pack per Oracle Solaris utilizzando il comando `pkg uninstall` di Oracle Solaris.

Nota - Quando si disinstallano i pacchetti, il file della cache delle credenziali host, salvato in precedenza utilizzando il comando `ilomconfig` di Oracle Hardware Management Pack per facilitare l'accesso a Oracle ILOM tramite l'interconnessione tra host e ILOM, non verrà eliminato. In questo caso, prima di disinstallare i pacchetti di Oracle Hardware Management Pack, eseguire il comando `ilomconfig delete credential` per eliminare questo file.

- Libreria della documentazione di Oracle Hardware Management Pack per Oracle Solaris all'indirizzo <http://www.oracle.com/goto/ohmp/solarisdocs>

