

Sicherheitshandbuch zu Oracle® Hardware Management Pack



Teilenr.: E39915-02
Oktober 2015

Teilenr.: E39915-02

Copyright © 2014, 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, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

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, dann 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 in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die Dokumentation können Zugriffsmöglichkeiten auf oder Informationen über Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Barrierefreie Dokumentation

Informationen zu Oracles Verpflichtung zur Barrierefreiheit erhalten Sie über die Website zum Oracle Accessibility Program <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Zugriff auf Oracle-Support

Oracle-Kunden mit einem gültigen Oracle Supportvertrag haben Zugriff auf elektronischen Support über My Oracle Support. Weitere Informationen erhalten Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>, falls Sie eine Hörbehinderung haben.

Inhalt

Überblick	7
Produktüberblick	7
Informationen zu diesem Sicherheitshandbuch	8
Sicherheitsgrundsätze	8
Sicherheitsübersicht zu Oracle Hardware Management Pack	9
 Oracle Hardware Management Pack - Vor der Installation	 11
Komponenten von Oracle Hardware Management Pack	11
Sicherheitseinstellungen des SNMP-Plug-ins basierend auf Agent	12
Wählen einer SNMP-Protokollversion für den SNMP-Agent	12
 Oracle Hardware Management Pack - Installation	 13
Ausführen des Installationsprogramms für Oracle Hardware Management Pack	13
Aktivieren von Host-to-ILOM-Interconnect	13
Speichern von Zugangsdaten in einer Datei	14
 Oracle Hardware Management Pack - Nach der Installation	 17
Deinstallation von Oracle Hardware Management Pack	17

Überblick

Dieser Abschnitt enthält einen Überblick über das Oracle Hardware Management Pack-(HMP-)Produkt, einschließlich Informationen zu dem Sicherheitshandbuch. Außerdem werden die allgemeinen Grundlagen der Anwendungssicherheit erläutert.

Folgende Themen werden behandelt:

- [„Produktüberblick“ \[7\]](#)
- [„Informationen zu diesem Sicherheitshandbuch“ \[8\]](#)
- [„Sicherheitsgrundsätze“ \[8\]](#)
- [„Sicherheitsübersicht zu Oracle Hardware Management Pack“ \[9\]](#)

Produktüberblick

Oracle Hardware Management Pack ist für viele x86-basierte Server und einige SPARC-basierte Server verfügbar. Oracle Hardware Management Pack besteht aus zwei Komponenten: einem SNMP-Überwachungs-Agent sowie einer Gruppe von betriebssystemübergreifenden Befehlszeilentools für die Serververwaltung.

In Verbindung mit den SNMP-Plug-ins von Hardware Management Agent können Sie SNMP zur Überwachung von Oracle-Servern und -Servermodulen in Ihrem Rechenzentrum einsetzen, ohne dass Verbindungen mit zwei Verwaltungspunkten (Host und Oracle ILOM) erforderlich sind. Durch diese Funktion kann eine einzelne IP-Adresse (IP des Hosts) zur Überwachung von mehreren Servern und Servermodulen verwendet werden.

SNMP-Plug-ins von Hardware Management Agent werden auf dem Hostbetriebssystem von Oracle-Servern ausgeführt. Die SNMP-Plug-ins kommunizieren über die Oracle Hardware Storage Access Librarys mit dem Serviceprozessor. Informationen zum aktuellen Status des Servers werden automatisch vom Hardware Management Agent abgerufen. Weitere Informationen zum Hardware Management Agent finden Sie in *Oracle Server Management Agents - Benutzerhandbuch*.

Zur Konfiguration von Oracle-Servern können Sie die Befehlszeilentools der Oracle-Server verwenden. Die CLI-Tools sind kompatibel mit Oracle Solaris, Oracle Linux, Oracle VM, weiteren Linux-Distributionen und den Windows-Betriebssystemen. Eine Liste der Tools finden Sie in *Oracle Server CLI Tools User's Guide*.

In der Oracle Hardware Management Pack for Oracle Solaris-Dokumentation finden Sie weitere Informationen zu Funktionen und Verwendung.

- Oracle Hardware Management Pack-Dokumentationsbibliothek unter: <http://www.oracle.com/goto/ohmp/docs>
- Allgemeine Oracle ILOM-Informationen finden Sie unter: <http://www.oracle.com/goto/ilom/docs>

Informationen zu diesem Sicherheitshandbuch

Dieses Dokument enthält allgemeine Sicherheitsrichtlinien für Oracle Hardware Management Pack. Dieses Handbuch soll Sie bei der Gewährleistung der Sicherheit unterstützen, wenn Sie die Software mit anderen Oracle-Hardwareprodukten wie Netzwerk-Switches und Netzwerkkarten verwenden.

Folgende Themen werden behandelt:

- [Oracle Hardware Management Pack - Vor der Installation \[11\]](#)
- [Oracle Hardware Management Pack - Installation \[13\]](#)
- [Oracle Hardware Management Pack - Nach der Installation \[17\]](#)

Sicherheitsgrundsätze

Es gibt vier Sicherheitsgrundsätze: Zugang, Authentifizierung, Autorisierung und Überwachung.

- **Zugang**

Schützen Sie Ihre Hardware und Ihre Daten durch physische und virtuelle Steuerungsmechanismen vor unerlaubten Zugriffen.

- Bei Hardware sind Zugangsbeschränkungen normalerweise physische Zugangsbeschränkungen.
- Bei Software sollten Sie sowohl den physischen als auch den virtuellen Zugang beschränken.
- Firmware kann nur über den Oracle-Updateprozess geändert werden.

- **Authentifizierung**

Richten Sie alle Funktionen zur Authentifizierung ein, wie ein Passwortsystem in den Betriebssystemen Ihrer Plattform, sodass festgestellt werden kann, ob es sich bei einem Benutzer wirklich um diesen Benutzer handelt.

Die Authentifizierung bietet unterschiedliche Sicherheitsniveaus durch verschiedene Maßnahmen, wie Ausweise und Kennwörter. Beispiel: Stellen Sie sicher, dass das Personal beim Betreten eines Computerraums Mitarbeiterausweise trägt.

- **Autorisierung**

Durch die Autorisierung können Mitarbeiter nur mit der Hardware und Software arbeiten, für die sie geschult wurden.

Beispiel: Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu kontrollieren.

- **Überwachung**

IT-Personal von Kunden kann die Hardware- und Softwarefunktionen von Oracle zur Überwachung von Anmeldevorgängen und zur Wartung der Hardware verwenden.

- Überwachen Sie die Anmeldung von Benutzern anhand von Systemlogs. Verfolgen Sie insbesondere Systemadministrator- und Serviceaccounts über Systemlogs, da vor allem diese Accounts Zugriff auf leistungsstarke Befehle gewähren.
- Stufen Sie Logdateien regelmäßig als veraltet ein, wenn diese gemäß der Unternehmensrichtlinie des Kunden eine bestimmte Größe überschreiten. Logs werden normalerweise für einen langen Zeitraum beibehalten und müssen daher unbedingt gepflegt werden.
- Verfolgen Sie Systemressourcen für Bestandszwecke anhand von Komponentenseriennummern. Oracle-Teilenummern sind auf allen Karten, Modulen und Hauptplatinen elektronisch gespeichert.

Sicherheitsübersicht zu Oracle Hardware Management Pack

Die folgenden wichtigen Sicherheitspunkte müssen bei der Konfiguration aller Systemverwaltungstools berücksichtigt werden:

- *Systemverwaltungsprodukte können dazu verwendet werden, eine bootfähige Root-Umgebung zu erhalten.*

Mit einer bootfähigen Root-Umgebung können Sie Zugriff zu Oracle ILOM, Oracle System Assistant und zu Festplatten erhalten.

- *Systemverwaltungsprodukte enthalten leistungsstarke Tools, für deren Ausführung Administrator- oder Root-Berechtigungen erforderlich sind.*

Mit dieser Berechtigungsstufe ist es möglich, die Hardwarekonfiguration zu ändern und Daten zu löschen.

Oracle Hardware Management Pack - Vor der Installation

Verwenden Sie bei der Erstinstallation und -konfiguration Oracle-Softwaresicherheitsfunktionen, um die Hardware zu steuern und Systemressourcen zu verfolgen.

Folgende Themen werden behandelt:

- „Komponenten von Oracle Hardware Management Pack“ [11]
- „Sicherheitseinstellungen des SNMP-Plug-ins basierend auf Agent“ [12]
- „Wählen einer SNMP-Protokollversion für den SNMP-Agent“ [12]

Komponenten von Oracle Hardware Management Pack

Oracle Hardware Management Pack umfasst eine Sammlung aus Befehlszeilentools für die Hardwareverwaltung zur Konfiguration von RAID, BIOS und Oracle ILOM und zur Aktualisierung der Firmware. Es enthält außerdem ein SNMP-Plug-in zur Überwachung. Oracle Hardware Management Pack enthält darüber hinaus einen Daemon oder Service, der über einen internen Kanal mit Oracle ILOM kommuniziert, um Bestands- und Integritätsinformationen zum Server weiterzugeben.

Diese Tools und Plug-ins werden auf dem Hostbetriebssystem installiert, sodass Sie Systemverwaltungsaufgaben direkt über den Host ausführen können. Oracle Hardware Management Pack enthält zwar nützliche Funktionen für die Verwaltung eines Oracle-Servers, ist aber optional.

Weitere Informationen zu den Funktionen von Oracle Hardware Management Pack finden Sie in den folgenden Dokumentationsbibliotheken:

- Dokumentations-Library für Oracle Hardware Management Pack (<http://www.oracle.com/goto/ohmp/docs>)
- Oracle ILOM-Dokumentationsbibliothek (<http://www.oracle.com/goto/ilom/docs>)

Sicherheitseinstellungen des SNMP-Plug-ins basierend auf Agent

Oracle Hardware Management Pack umfasst ein SNMP-Plug-in-Modul, mit dem der native SNMP-Agent im Hostbetriebssystem um zusätzliche Oracle MIB-Funktionen erweitert wird. Es wird besonders darauf hingewiesen, dass Oracle Hardware Management Pack selbst keinen SNMP-Agent enthält. Bei Linux wird dem net-snmp-Agent, der zunächst installiert werden muss, ein Modul hinzugefügt. Bei Solaris wird dem Solaris Management Agent ein Modul hinzugefügt. Bei Windows wird der native SNMP-Service durch das Plug-in erweitert.

Ebenso werden alle SNMP-bezogenen Sicherheitseinstellungen für das SNMP-Plug-in von Oracle Hardware Management Pack durch die Einstellungen des nativen SNMP-Agents oder Service und nicht durch das Plug-in bestimmt. Anweisungen zum sicheren Konfigurieren von SNMP finden Sie in der Dokumentation für net-snmp oder für den Windows-SNMP-Service. Außerdem wird auf die Anweisungen in *Oracle Server Management Agents - Benutzerhandbuch* unter dem folgenden Link verwiesen:

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

Wählen einer SNMP-Protokollversion für den SNMP-Agent

SNMP ist ein Standardprotokoll, das zur Systemüberwachung oder -verwaltung verwendet wird. SNMPv1/v2c bietet keine Verschlüsselung und führt die Authentifizierung anhand von Communityzeichenfolgen durch. Communityzeichenfolgen werden über das Netzwerk in Klartext übertragen und üblicherweise von einer Gruppe gemeinsam und nicht von einem einzelnen Benutzer privat genutzt. Bei SNMPv3 hingegen wird durch die Verschlüsselung ein sicherer Kanal bereitgestellt, und es werden Benutzernamen und Kennwörter verwendet. SNMPv3-Benutzerkennwörter sind lokalisiert, sodass sie sicher auf Verwaltungsstationen gespeichert werden können.

Oracle empfiehlt die Verwendung von SNMPv3, wenn dies vom nativen SNMP-Agent unterstützt wird. Anweisungen zum Konfigurieren von SNMPv3 finden Sie in der Dokumentation für net-snmp (Oracle Solaris und Linux) oder für den Windows-SNMP-Dienst.

Oracle Hardware Management Pack - Installation

Folgende Themen werden behandelt:

- „Ausführen des Installationsprogramms für Oracle Hardware Management Pack“ [13]
- „Aktivieren von Host-to-ILOM-Interconnect“ [13]
- „Speichern von Zugangsdaten in einer Datei“ [14]

Ausführen des Installationsprogramms für Oracle Hardware Management Pack

Oracle Hardware Management Pack besteht aus einer Reihe von nativen Installationspackages, die mit den nativen Installationstools für ein Betriebssystem, wie RPM, installiert werden können. Darüber hinaus kann ein assistentenbasiertes Installationsprogramm bei der Installation behilflich sein. Mit dem Installationsprogramm werden die nativen Packages hinzugefügt und die Verwendung von Oracle Hardware Management Pack konfiguriert.

Da das Installationsprogramm für Oracle Hardware Management Pack native Packages installieren muss, müssen Sie es als Root oder Administrator ausführen. Weitere Informationen finden Sie in *Oracle Hardware Management Pack - Installationshandbuch* unter dem folgenden Link:

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

Aktivieren von Host-to-ILOM-Interconnect

Eine schnellere Alternative zur KCS-Schnittstelle ist die interne High-Speed Interconnect-Verbindung, über die Clients auf dem Hostbetriebssystem mit Oracle ILOM kommunizieren können. In Oracle Hardware Management Pack wird diese Funktion als Host-to-ILOM-Interconnect bezeichnet. In der Oracle ILOM-Schnittstelle wird diese Funktion als Local Host Interconnect bezeichnet. Dieses Interconnect wird durch eine interne Ethernet-USB-Verbindung

implementiert, und es wird ein IP-Stack ausgeführt. Oracle ILOM und der Host erhalten interne, nicht weiterleitbare IP-Adressen für die Kommunikation über diesen Kanal.

Für die Verbindung mit Oracle ILOM über das Host-to-ILOM-Interconnect (Local Host Interconnect) ist, genau wie für eine Netzwerkverbindung mit dem Oracle ILOM-Verwaltungsport, eine Authentifizierung erforderlich. Alle im Verwaltungsnetzwerk bekannten Services und Protokolle stehen dem Host über das Host-to-ILOM-Interconnect zur Verfügung. Beispiel: Sie können die Oracle ILOM-Webbenutzeroberfläche aufrufen, indem Sie einen Webbrowser auf dem Host verwenden oder mithilfe eines Secure Shell-Clients eine Verbindung mit der Oracle ILOM-Befehlszeilenschnittstelle aufbauen. In allen Fällen sind ein gültiger Benutzername und ein gültiges Passwort für das Host-to-ILOM-Interconnect erforderlich.

Das Installationsprogramm für Oracle Hardware Management Pack enthält eine Option zum Aktivieren von Host-to-ILOM-Interconnect. Oracle empfiehlt die Aktivierung von Host-to-ILOM-Interconnect nur, wenn die Netzwerkanweisung RFC 3927 sowie die Fähigkeit für Link-Local-IPv4-Adressen unterstützt. Sie sollten außerdem sicherstellen, dass das Betriebssystem nicht als Bridge oder Router verwendet wird. Dadurch wird sichergestellt, dass der Verwaltungsverkehr zwischen dem Host und Oracle ILOM privat bleibt. Weitere Informationen finden Sie in *Oracle Hardware Management Pack - Installationshandbuch* unter dem folgenden Link:

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

Speichern von Zugangsdaten in einer Datei

Ab Oracle Hardware Management Pack 2.3.3 wurde diese Funktion deaktiviert.

Die Tools `ilomconfig` und `fwupdate`, die Bestandteil von Oracle Hardware Management Pack for Oracle Solaris sind, können mit dem Hochgeschwindigkeits-Host-to-ILOM-Interconnect Verbindung zu Oracle ILOM herstellen. Da für das Host-to-ILOM-Interconnect eine Authentifizierung erforderlich ist, müssen Sie sich bei jedem Aufruf dieser Tools bei Oracle ILOM authentifizieren. Um dies zu erleichtern, können Sie die Zugangsdaten in einer Datei cachen, damit sie automatisch von den Tools verwendet werden können. So müssen Sie keine Klartext-Passwörter in Skripte einbetten, die die Oracle Hardware Management Pack-Tools verwenden.

Mit dem Tool `ilomconfig` können Sie den Benutzernamen und das Passwort in einer verschlüsselten Datei speichern, die auf Root-Ebene schreibgeschützt ist. Wenn Sie mit `ilomconfig` oder `fwupdate` auf Oracle ILOM zugreifen und diese Datei ermittelt wird, werden die gecachten Zugangsdaten verwendet. Alternativ dazu können Sie den Benutzernamen und das Passwort bei jedem Aufruf des Tools in der Befehlszeile angeben.

Der verwendete Verschlüsselungsalgorithmus ist in jedem System eindeutig. Wenn der Schlüssel ermittelt wird, könnte die Datei allerdings entschlüsselt werden und den

Benutzernamen und das Passwort freigeben. Oracle empfiehlt daher die Erstellung eines eindeutigen Passwortes in jedem Oracle ILOM, sodass ein gefährdetes Passwort nicht für andere Oracle ILOM-Systeme verwendet werden kann.

Anweisungen zur Speicherung von Zugangsdaten in einer Datei finden Sie in *Oracle CLI Tools for Oracle Solaris User's Guide* unter dem folgenden Link.

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

Oracle Hardware Management Pack - Nach der Installation

Folgende Themen werden behandelt:

- „Deinstallation von Oracle Hardware Management Pack“ [17]

Deinstallation von Oracle Hardware Management Pack

Die Oracle Hardware Management Pack-Packages können mit nativen Packagetools, wie RPM, oder mit dem assistentenbasierten Deinstallationsprogramm aus dem Lieferumfang von Oracle Hardware Management Pack deinstalliert werden. Bei der nativen Packagemethode für das Entfernen von Packages wird die Datei nicht gelöscht, wenn Sie vorher eine Cachedatei mit Hostzugangsdaten mit Oracle Hardware Management Pack gespeichert haben, um den Zugriff auf Oracle ILOM mit Host-to-ILOM-Interconnect zu vereinfachen. Führen Sie in diesem Fall vor der Deinstallation der Oracle Hardware Management Pack Packages den Befehl `ilomconfig delete credential` aus, um diese Datei zu löschen.

Beim assistentenbasierten Deinstallationsprogramm wird die Zugangsdatendatei entfernt. Daher wird empfohlen, Oracle Hardware Management Pack mit dem assistentenbasierten Installationsprogramm zu deinstallieren. Weitere Informationen finden Sie in *Oracle Hardware Management Pack - Installationshandbuch* unter dem folgenden Link:

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

