

Guide de sécurité d'Oracle Hardware Management Pack

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Table des matières

Présentation	5
Présentation du produit	5
A propos de ce guide de sécurité	6
Principes de sécurité élémentaires	6
Récapitulatif de la sécurité d'Oracle Hardware Management Pack	7
Considérations préalables à l'installation d'Oracle Hardware Management Pack	9
Composants d'Oracle Hardware Management Pack	9
Paramètres de sécurité du plug-in SNMP basés sur l'agent	10
Choix de la version du protocole SNMP de l'agent SNMP	10
Installation d'Oracle Hardware Management Pack	11
Exécution du programme d'installation d'Oracle Hardware Management Pack	11
Choix de l'activation de l'interconnexion LAN	11
Choix de l'enregistrement des informations d'identification et de connexion dans un fichier	12
Opérations postérieures à l'installation d'Oracle Hardware Management Pack	15
Désinstallation d'Oracle Hardware Management Pack	15

Présentation

Cette section offre une vue d'ensemble du produit Oracle Hardware Management Pack (HMP), contient des informations relatives à la sécurité et explique les principes généraux de sécurité des applications.

Les sujets abordés sont les suivants :

- [“Présentation du produit” à la page 5](#)
- [“A propos de ce guide de sécurité” à la page 6](#)
- [“Principes de sécurité élémentaires” à la page 6](#)
- [“Récapitulatif de la sécurité d'Oracle Hardware Management Pack” à la page 7](#)

Présentation du produit

Oracle Hardware Management Pack est disponible pour votre serveur, pour de nombreux serveurs x86 et pour certains serveurs SPARC. Oracle Hardware Management Pack est formé de deux composants : un agent de surveillance SNMP et un ensemble d'outils d'interface de ligne de commande (outils CLI) multiplates-formes pour la gestion de vos serveurs.

Avec les plug-ins SNMP de l'agent de gestion du matériel, vous pouvez utiliser SNMP pour surveiller les serveurs Oracle et les modules serveur de votre centre de données sans avoir à vous connecter aux deux points de gestion que sont l'hôte et Oracle ILOM. Cette fonction permet d'utiliser une seule adresse IP (celle de l'hôte) pour surveiller plusieurs serveurs et modules serveur.

Les plug-ins SNMP de l'agent de gestion du matériel s'exécutent sur le système d'exploitation hôte des serveurs Oracle. Les plug-ins SNMP utilisent les bibliothèques d'accès au stockage du matériel Oracle pour communiquer avec le processeur de service. Les informations relatives à l'état actuel du serveur sont automatiquement extraites par l'agent de gestion du matériel.

Vous pouvez utiliser les outils CLI de serveur Oracle pour configurer les serveurs Oracle. Les outils CLI sont compatibles avec les systèmes d'exploitation Oracle Solaris, Oracle Linux, Oracle VM, Windows, ainsi que d'autres versions de Linux. Le tableau suivant décrit les tâches que vous pouvez effectuer à l'aide des outils CLI.

Tâches de gestion du système à partir du SE hôte	Outil CLI
Configuration des paramètres du BIOS, de l'ordre d'initialisation des périphériques et de certains paramètres du processeur de service.	ubiosconfig biosconfig
Mise à jour d'Oracle ILOM et du BIOS.	fwupdate
Interrogation, mise à jour et validation des versions des microprogrammes sur les périphériques de stockage SAS pris en charge, contrôleurs de stockage SAS intégrés, extensions de stockage SAS et unités de stockage.	
Restauration, définition et affichage des paramètres de configuration d'Oracle ILOM, ainsi qu'affichage et définition des propriétés d'Oracle ILOM associées à la gestion du réseau, à la configuration de l'horloge et à la gestion des utilisateurs.	ilomconfig
Affichage et création des volumes RAID sur les unités de stockage connectées aux contrôleurs RAID, notamment les baies de stockage.	raidconfig
Surveillance de l'intégrité du système.	hwmgmt

A propos de ce guide de sécurité

Ce document formule des recommandations générales en matière de sécurité pour Oracle Hardware Management Pack. Il a pour objet de vous aider à assurer la sécurité de votre logiciel lorsque vous l'utilisez avec d'autres produits matériels Oracle tels que des commutateurs réseau et des cartes d'interface réseau.

Les sujets abordés sont les suivants :

- [“Présentation” à la page 5](#)
- [“Considérations préalables à l'installation d'Oracle Hardware Management Pack” à la page 9](#)
- [“Installation d'Oracle Hardware Management Pack” à la page 11](#)
- [“Opérations postérieures à l'installation d'Oracle Hardware Management Pack” à la page 15](#)

Principes de sécurité élémentaires

Il existe quatre principes de sécurité élémentaires : l'accès, l'authentification, l'autorisation et la comptabilisation.

- **Accès**
Mettez en place des contrôles physiques et logiciels pour protéger votre matériel ou vos données contre les intrusions.
 - Pour le matériel, les limites d'accès correspondent généralement à des limites d'accès physiques.
 - Pour les logiciels, l'accès est limité à l'aide de moyens physiques et virtuels.

- Seul le processus de mise à jour Oracle permet de modifier les microprogrammes.
- **Authentification**
Configurez toutes les fonctions d'authentification, telles qu'un système de mots de passe, dans les systèmes d'exploitation de votre plate-forme, afin d'éviter toute usurpation d'identité.
L'authentification fournit divers degrés de sécurité grâce à des mesures telles que les badges et les mots de passe. Veillez par exemple à ce que les employés utilisent correctement leur badge pour pénétrer dans la salle informatique.
- **Autorisation**
L'autorisation permet au personnel de la société d'utiliser uniquement le matériel et les logiciels pour lesquels ils ont été formés et certifiés.
Mettez en place par exemple un système d'autorisations en lecture, écriture et exécution pour contrôler l'accès des utilisateurs aux commandes, à l'espace disque, aux périphériques et aux applications.
- **Comptabilisation**
Le personnel informatique du client peut tirer parti des fonctions logicielles et matérielles Oracle pour surveiller les connexions et tenir à jour les inventaires de matériel.
 - Surveillez les connexions des utilisateurs par le biais de journaux système. Organisez en particulier un suivi des comptes d'administrateur système et de maintenance, lesquels ont accès à des commandes puissantes, par le biais de journaux système.
 - Archivez régulièrement les fichiers journaux lorsque leur taille devient excessive, conformément à la stratégie de l'entreprise cliente. Les journaux sont généralement conservés pendant une longue période, c'est pourquoi il est essentiel d'assurer leur maintenance.
 - Effectuez le suivi et dressez l'inventaire des ressources système à l'aide de numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur l'ensemble des cartes, modules et cartes mères, et peuvent être utilisés à des fins d'inventaire.

Récapitulatif de la sécurité d'Oracle Hardware Management Pack

Tenez compte des considérations relatives à la sécurité suivantes lorsque vous configurez des outils de gestion système :

- *Les produits de gestion système permettent d'obtenir un environnement root amorçable.*
Grâce à un environnement root amorçable, il est possible d'accéder à Oracle ILOM, à Oracle System Assistant et aux disques durs.

- *Les produits de gestion système comprennent des outils puissants pouvant uniquement être exécutés à l'aide de privilèges d'administrateur ou de privilèges root.*

Avec ce niveau d'accès, il est possible de modifier la configuration du matériel et de supprimer des données.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Considérations préalables à l'installation d'Oracle Hardware Management Pack

Pendant l'installation et la configuration initiales, servez-vous des fonctions de sécurité logicielles Oracle pour contrôler le matériel et assurer le suivi des ressources système.

Les sujets abordés sont les suivants :

- “Composants d'Oracle Hardware Management Pack” à la page 9
- “Paramètres de sécurité du plug-in SNMP basés sur l'agent” à la page 10
- “Choix de la version du protocole SNMP de l'agent SNMP” à la page 10

Composants d'Oracle Hardware Management Pack

Oracle Hardware Management Pack contient un ensemble d'outils de ligne de commande destinés à la gestion du matériel et permettant de configurer RAID, BIOS et ILOM ainsi que de mettre à jour les microprogrammes. Il contient également un plug-in SNMP permettant d'assurer la surveillance. De plus, Oracle Hardware Management Pack contient un démon ou service qui communique avec Oracle ILOM par le biais d'un canal interne en vue de partager des informations d'inventaire et d'intégrité relatives au serveur.

Ces outils et plug-ins sont installés sur le système d'exploitation de l'hôte, si bien que vous pouvez directement effectuer des tâches de gestion système à partir de l'hôte. Bien qu'Oracle Hardware Management Pack offre des fonctionnalités utiles de gestion des serveurs Oracle, ce logiciel est entièrement facultatif.

Reportez-vous au guide de l'utilisateur d'Oracle Hardware Management Pack pour en savoir plus sur les fonctions d'Oracle Hardware Management Pack et décider si vous souhaitez l'utiliser et l'installer.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)
- Pour des informations d'ordre général sur Oracle ILOM, reportez-vous à la page Web :
<http://www.oracle.com/pls/topic/lookup?ctx=ilom31>

Paramètres de sécurité du plug-in SNMP basés sur l'agent

Oracle Hardware Management Pack contient un module plug-in SNMP qui étend l'agent SNMP natif dans le système d'exploitation hôte de manière à offrir des fonctions Oracle MIB supplémentaires. Notez bien qu'Oracle Hardware Management Pack ne contient aucun agent SNMP. Pour Linux, un module est ajouté à l'agent net-snmp agent, lequel doit être préalablement installé. Pour Solaris, un module est ajouté à l'agent Solaris Management. Pour Windows, le plug-in étend le service SNMP natif.

De même, tous les paramètres de sécurité liés à SNMP du plug-in SNMP d'Oracle Hardware Management Pack sont déterminés par les paramètres de l'agent ou service SNMP natif, et non par le plug-in. Reportez-vous à la documentation de net-snmp ou du service SNMP de Windows pour connaître la procédure de configuration sécurisée de SNMP.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Choix de la version du protocole SNMP de l'agent SNMP

Le protocole standard SNMP permet de surveiller ou de gérer un système. SNMPv1/v2c n'offre pas de chiffrement et procède à l'authentification à l'aide de chaînes de communauté. Ces chaînes de communauté, envoyées sous forme de texte clair sur le réseau, sont généralement partagées par un groupe d'utilisateurs, et non réservées à un seul utilisateur. En revanche, SNMPv3 met en oeuvre le chiffrement pour fournir un canal sécurisé et utilise des noms et des mots de passe d'utilisateurs individuels. Les mots de passe utilisateur SNMPv3 étant localisés, ils peuvent être stockés de manière sécurisée sur les stations de gestion.

Oracle recommande l'usage de SNMPv3, si ce protocole est pris en charge par l'agent SNMP natif. Reportez-vous à la documentation de net-snmp ou du service SNMP de Windows pour connaître la procédure de configuration de SNMPv3.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Installation d'Oracle Hardware Management Pack

Les sujets abordés sont les suivants :

- “Exécution du programme d'installation d'Oracle Hardware Management Pack” à la page 11
- “Choix de l'activation de l'interconnexion LAN” à la page 11
- “Choix de l'enregistrement des informations d'identification et de connexion dans un fichier” à la page 12

Exécution du programme d'installation d'Oracle Hardware Management Pack

Oracle Hardware Management Pack est formé d'un ensemble de packages d'installation natifs pouvant être installés à l'aide des outils d'installation natifs d'un système d'exploitation, tel que RPM par exemple. Il est également possible d'effectuer l'installation à l'aide d'un programme d'installation de type assistant. En plus d'ajouter les packages natifs, le programme d'installation permet de configurer Oracle Hardware Management Pack pour son utilisation future.

Etant donné qu'il doit installer des packages natifs, le programme d'installation d'Oracle Hardware Management Pack doit être exécuté en tant qu'utilisateur root ou en tant qu'administrateur.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Choix de l'activation de l'interconnexion LAN

Pour tirer parti d'une alternative plus rapide que l'interface KCS, les clients résidant sur le système d'exploitation hôte peuvent communiquer avec Oracle ILOM par le biais d'une interconnexion haut débit interne. Cette interconnexion est implémentée par une connexion USB Ethernet interne qui exécute une pile IP. Des adresses IP non routables internes sont attribuées à Oracle ILOM et à l'hôte pour la communication par le biais de ce canal.

La connexion à Oracle ILOM par le biais d'une interconnexion LAN impose une authentification, comme si la connexion s'effectuait sur le réseau au port de gestion d'Oracle ILOM. Tous les services ou protocoles exposés sur le réseau de gestion sont accessibles par le

biais de l'interconnexion LAN à l'hôte. Il est par exemple possible d'accéder à l'interface Web d'Oracle ILOM dans un navigateur sur l'hôte ou à l'interface de ligne de commande d'Oracle ILOM dans un client SSH (Secure Shell, shell sécurisé). Dans tous les cas de figure, il faut fournir un nom et un mot de passe utilisateur valides lors de l'interconnexion LAN.

Le programme d'installation d'Oracle Hardware Management Pack propose une option permettant d'activer l'interconnexion LAN. Oracle recommande d'activer l'interconnexion LAN uniquement si l'instruction de gestion de réseau prend en charge RFC 3927 et la possibilité de disposer d'adresses IPv4 link-local. De même, il faut veiller à ce que le système d'exploitation ne fasse pas office de pont ou de routeur. Ceci afin de garantir que le trafic de gestion entre l'hôte et Oracle ILOM reste privé.

- [Bibliothèque de documentation d'Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Choix de l'enregistrement des informations d'identification et de connexion dans un fichier

Les outils `ilomconfig` et `fwupdate` inclus dans Oracle Hardware Management Pack permettent la connexion à Oracle ILOM par le biais de l'interconnexion LAN haut débit. Le recours à l'interconnexion LAN au lieu de l'interface KCS, plus lente, accélère de façon sensible les performances d'opérations essentielles telles que les mises à jour des microprogrammes Oracle ILOM.

L'interconnexion LAN nécessitant une authentification, chaque appel de ces outils nécessite une authentification auprès d'Oracle ILOM. Pour plus de confort, il est possible de mettre les informations d'identification et de connexion en cache dans un fichier, afin que les outils puissent les utiliser de manière automatique. Cette mesure évite d'avoir à incorporer des mots de passe en texte clair dans des scripts utilisant les outils d'Oracle Hardware Management Pack.

L'outil `ilomconfig` tool permet de stocker le nom d'utilisateur et le mot de passe dans un fichier chiffré pouvant uniquement être lu par l'utilisateur root. Si un tel fichier est détecté lors d'un accès à Oracle ILOM à l'aide d'`ilomconfig` ou de `fwupdate`, les informations d'identification et de connexion mises en cache sont utilisées. Sinon, il est possible de saisir le nom d'utilisateur et le mot de passe dans la ligne de commande à chaque utilisation de l'outil.

L'algorithme de chiffrement utilisé est propre à chaque système. Toutefois, si la clé est découverte, le fichier risque d'être déchiffré et de révéler le nom d'utilisateur et le mot de passe. C'est la raison pour laquelle Oracle recommande de créer un mot de passe unique sur chaque système Oracle ILOM, de manière à ce qu'un mot de passe compromis ne puisse pas être utilisé sur d'autres systèmes Oracle ILOM.

Reportez-vous au guide de l'utilisateur de Sun Server Hardware Management Pack pour connaître la procédure d'enregistrement d'informations d'identification et de connexion dans un fichier.

- Bibliothèque de documentation d'Oracle Hardware Management Pack
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Opérations postérieures à l'installation d'Oracle Hardware Management Pack

Les sujets abordés sont les suivants :

- “Désinstallation d'Oracle Hardware Management Pack” à la page 15

Désinstallation d'Oracle Hardware Management Pack

Il est possible de désinstaller les packages d'Oracle Hardware Management Pack à l'aide d'outils natifs de gestion des packages, tels que RPM, ou à l'aide du programme de désinstallation de type assistant fourni avec Oracle Hardware Management Pack. Lorsque les packages sont désinstallés à l'aide des outils natifs, le fichier chiffré contenant le nom d'utilisateur et le mot de passe mis en cache servant à l'interconnexion LAN n'est pas supprimé. Il faut le supprimer manuellement.

En revanche, le programme de désinstallation de type assistant supprime le fichier contenant les informations d'identification et de connexion. C'est la raison pour laquelle Oracle recommande de désinstaller Oracle Hardware Management Pack à l'aide du programme de désinstallation de type assistant.

- Bibliothèque de documentation d'Oracle Hardware Management Pack
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

