

**Guide de sécurité d'Oracle® Hardware  
Management Pack pour Oracle Solaris  
11.3**

**ORACLE®**

Référence: E76539-02  
Mars 2017



**Référence: E76539-02**

Copyright © 2015, 2017, Oracle et/ou ses affiliés. Tous droits réservés.

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 stipulation 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 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, sauf mention contraire stipulée dans un contrat entre vous et Oracle. 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, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

**Accessibilité de la documentation**

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

**Accès aux services de support Oracle**

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.



# Table des matières

---

<b>Présentation de la sécurité du produit et des applications</b> .....	7
A propos d'Oracle Hardware Management Pack pour Oracle Solaris .....	7
Principes de sécurité élémentaires .....	8
Récapitulatif de la sécurité d'Oracle Hardware Management Pack .....	9
<b>Sécurisation d'Oracle Hardware Management Pack</b> .....	11
Interface d'interconnexion entre l'hôte et ILOM .....	11
Prise en charge de l'utilisation d'IPMI avec TLS (Transport Layer Security) .....	12
Suppression de l'ancien fichier contenant les informations d'identification et de connexion .....	12
Choix des paramètres de sécurité SNMP .....	13
<b>Installation ou désinstallation de composants d'Oracle Hardware Management Pack</b> .....	15
Installation de composants .....	15
Désinstallation de composants .....	15



# Présentation de la sécurité du produit et des applications

---

Cette section offre une vue d'ensemble du produit Oracle Hardware Management Pack (HMP) pour Oracle Solaris ainsi que des principes généraux de sécurité de l'application.

Cette section aborde les sujets suivants :

- ["A propos d'Oracle Hardware Management Pack pour Oracle Solaris" à la page 7](#)
- ["Principes de sécurité élémentaires" à la page 8](#)
- ["Récapitulatif de la sécurité d'Oracle Hardware Management Pack" à la page 9](#)

## A propos d'Oracle Hardware Management Pack pour Oracle Solaris

Oracle Hardware Management Pack pour Oracle Solaris est disponible 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) 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. Pour plus d'informations sur l'agent de gestion du matériel, reportez-vous au [Guide de l'utilisateur des agents de gestion des serveurs Oracle® pour Oracle Solaris 11.3](#).

Vous pouvez tirer parti des outils de ligne de commande (CLI) pour configurer les serveurs Oracle. Une liste d'outils est fournie dans le *Guide de l'utilisateur des outils de la CLI Oracle® pour Oracle Solaris 11.3*.

Reportez-vous à la documentation d'Oracle Hardware Management Pack pour Oracle Solaris pour plus d'informations sur ses fonctionnalités et son utilisation.

- Bibliothèque de documentation d'Oracle Hardware Management Pack pour Oracle Solaris à l'adresse : <http://www.oracle.com/goto/ohmp/solarisdocs>
- Pour des informations d'ordre général sur Oracle ILOM, reportez-vous à la page Web : <http://www.oracle.com/goto/ilom/docs>

## 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 par exemple en place 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 tous les modules, cartes et cartes mères.

## 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 dont l'exécution exige le niveau d'accès root.*  
Avec ce niveau d'accès, il est possible de modifier la configuration du matériel et de supprimer des données.



# Sécurisation d'Oracle Hardware Management Pack

---

Dans le cas d'Oracle Solaris, les composants d'Oracle Hardware Management Pack les plus fréquemment utilisés sont préinstallés. Des paramètres supplémentaires peuvent être nécessaires pour assurer la sécurité du programme.

- ["Interface d'interconnexion entre l'hôte et ILOM" à la page 11](#)
- ["Prise en charge de l'utilisation d'IPMI avec TLS \(Transport Layer Security\)" à la page 12](#)
- ["Suppression de l'ancien fichier contenant les informations d'identification et de connexion" à la page 12](#)
- ["Choix des paramètres de sécurité SNMP" à la page 13](#)

## Interface d'interconnexion entre l'hôte et ILOM

L'interface d'interconnexion entre l'hôte et ILOM permet aux clients du système d'exploitation de l'hôte de 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. Cette connexion est activée par défaut dans le système d'exploitation Oracle Solaris.

La connexion à Oracle ILOM par le biais de l'interconnexion entre l'hôte et ILOM 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 entre l'hôte et ILOM. 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.

Oracle recommande que votre réseau prenne en charge RFC 3927 et la possibilité de disposer d'adresses IPv4 lien-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 via l'interconnexion entre l'hôte et ILOM reste privé.

C'est la raison pour laquelle Oracle recommande de créer des mots de passe uniques pour chaque utilisateur sur chaque processeur de service Oracle ILOM, de manière à ce qu'un mot de passe compromis ne puisse pas être utilisé sur d'autres systèmes Oracle ILOM.

Pour plus d'informations, reportez-vous au [Guide d'installation d'Oracle® Hardware Management Pack pour Oracle Solaris 11.3](#).

## Prise en charge de l'utilisation d'IPMI avec TLS (Transport Layer Security)

Dans les versions d'Oracle Hardware Management Pack pour Oracle Solaris antérieures à Oracle Solaris 11.3 SRU 18, le chiffrement IPMI du réseau était géré à l'aide du protocole LANPLUS. S'y ajoute désormais la prise en charge d'IPMI avec le protocole TLS si ce protocole est pris en charge par l'environnement Oracle ILOM cible. Pour utiliser IPMI sur TLS, il faut une cible Oracle ILOM de version 3.2.8.1 ou ultérieure. Vous pouvez vérifier cette prise en charge en vous connectant à la cible Oracle ILOM à l'aide de l'interface Web et en consultant le paramètre TLS Sessions sous Administration > Management Access > IPMI.

Si la prise en charge d'IPMI sur TLS n'est pas disponible dans la cible Oracle ILOM, le protocole utilisé sera LANPLUS (s'il est activé).

---

**Remarque** - Bien que la communication chiffrée pour IPMI sur TLS soit prise en charge dans Oracle Hardware Management Pack pour Oracle Solaris 11.3 SRU 18, la vérification des certificats n'est pas disponible pour l'instant. La vérification complète des certificats devrait être prise en charge dans une prochaine version d'Oracle Hardware Management Pack pour Oracle Solaris 11.3.

---

## Suppression de l'ancien fichier contenant les informations d'identification et de connexion

Dans les versions d'Oracle Hardware Management Pack for Oracle Solaris antérieures à Oracle Solaris 11.3, l'outil `ilomconfig` vous permettait de stocker un nom d'utilisateur et un mot de passe dans un fichier chiffré pouvant uniquement être lu par l'utilisateur root. Si ce fichier était détecté lors de l'utilisation des outils `ilomconfig`, `fwupdate` ou `ubiosconfig` pour accéder à Oracle ILOM, les informations d'identification et de connexion mises en cache étaient utilisées. La

fonctionnalité relative au fichier contenant les informations d'identification et de connexion n'est pas prise en charge avec Oracle Hardware Management Pack for Oracle Solaris 11.3.

Si vous avez procédé à une mise à niveau depuis une version antérieure d'Oracle Solaris vers Oracle Solaris 11.3 et que vous avez déjà créé un fichier contenant les informations d'identification et de connexion, utilisez la commande `ilomconfig delete credential` pour supprimer ce fichier.

Reportez-vous au [Guide de l'utilisateur des outils de la CLI Oracle® pour Oracle Solaris 11.3](#) pour obtenir des instructions sur la manière d'appeler des commandes qui accèdent à un processeur de service.

## Choix des paramètres de sécurité SNMP

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 le système d'exploitation Oracle Solaris, un module est ajouté à l'agent de gestion Solaris.

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. Les paramètres SNMP peuvent inclure :

- SNMPv1/v2c. Cette version 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.
- SNMPv3. Cette version 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. Pour obtenir des instructions sur la configuration de `net-snmp` pour SNMPv3, reportez-vous à la documentation d'Oracle Solaris.

En outre, Oracle recommande d'isoler l'ensemble du trafic SNMP dans un réseau de gestion sécurisé distinct.

---

**Remarque** - La fonctionnalité SNMP est désactivée par défaut et doit être activée et configurée par l'utilisateur conformément aux instructions du [Guide de l'utilisateur des agents de gestion des serveurs Oracle® pour Oracle Solaris 11.3](#).

---



# Installation ou désinstallation de composants d'Oracle Hardware Management Pack

---

Cette section aborde les sujets suivants :

- "Installation de composants" à la page 15
- "Désinstallation de composants" à la page 15

## Installation de composants

Oracle Hardware Management Pack pour Oracle Solaris consiste en un ensemble d'outils préinstallés. D'autres packages constitutifs d'Oracle Hardware Management Pack qui ne sont pas préinstallés peuvent être installés à l'aide d'Oracle Solaris Image Packaging System (IPS).

Seul un administrateur disposant des privilèges root est habilité à installer les packages Oracle Hardware Management Pack.

- Bibliothèque de documentation d'Oracle Hardware Management Pack pour Oracle Solaris : <http://www.oracle.com/goto/ohmp/solarisdocs>

## Désinstallation de composants

Les packages Oracle Hardware Management Pack pour Oracle Solaris peuvent être désinstallés à l'aide de la commande `pkg uninstall` d'Oracle Solaris.

---

**Remarque** - Lors de la désinstallation des packages, si vous avez précédemment enregistré un fichier cache d'informations d'identification de l'hôte à l'aide de la commande `ilomconfig` d'Oracle Hardware Management Pack pour faciliter l'accès à Oracle ILOM via l'interconnexion entre l'hôte et ILOM, le fichier n'est pas supprimé. Dans ce cas, avant d'installer les packages Oracle Hardware Management Pack, exécutez la commande `ilomconfig delete credential` pour supprimer ce fichier.

---

- Bibliothèque de documentation d'Oracle Hardware Management Pack pour Oracle Solaris à l'adresse : <http://www.oracle.com/goto/ohmp/solarisdocs>