Guide de sécurité d'Oracle® Hardware Management Pack pour Oracle Solaris 11.2

Référence: E56555-02
Septembre 2015

Référence: E56555-02

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

Présentation de la sécurité du produit et des applications 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

Sécurisation d'Oracle Hardware Management Pack 11
Interface d'interconnexion entre l'hôte et ILOM 11
Choix de l'enregistrement des informations d'identification et de connexion dans un fichier 12
Choix des paramètres de sécurité SNMP 12

Installation ou désinstallation de composants d'Oracle Hardware Management Pack 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*.

Vous pouvez tirer parti des outils de ligne de commande (CLI) pour configurer les serveurs Oracle. Pour obtenir une liste des outils, reportez-vous au *Guide de l'utilisateur des outils de la CLI des serveurs Oracle*.

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 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.

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 paramétrages supplémentaires peuvent être nécessaires pour assurer la sécurité du programme.

- "Interface d'interconnexion entre l'hôte et ILOM" à la page 11
- "Choix de l'enregistrement des informations d'identification et de connexion dans un fichier" à la page 12
- "Choix des paramètres de sécurité SNMP" à la page 12

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 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.

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.

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

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

A partir d'Oracle Solaris 11.2 SRU 14, cette fonctionnalité a été désactivée.

Les outils `ilomconfig` et `fwupdate` inclus dans Oracle Hardware Management Pack pour Oracle Solaris permettent la connexion à Oracle ILOM par le biais de l'interconnexion haut débit entre l'hôte et ILOM. Etant donné que l'interconnexion entre l'hôte et ILOM nécessite 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` 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 des outils CLI pour Oracle Solaris* pour connaître la procédure d'enregistrement des informations d'identification et de connexion dans un fichier.

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

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.

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`