# Guide de sécurité du serveur Oracle® Server X6-2L

**Référence: E73723-01**
Avril 2016

**Référence: E73723-01**

Copyright © 2016, 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

**Sécurité de base** ..... 7
Accès ..... 7
Authentification ..... 8
Autorisation ..... 8
Comptabilisation et audit ..... 9

**Utilisation des outils de configuration et de gestion du serveur de façon sécurisée** ..... 11
Sécurité d'Oracle ILOM ..... 11
Sécurité d'Oracle Hardware Management Pack ..... 12

**Planification d'un environnement sécurisé** ..... 15
Protection par mot de passe ..... 15
Recommandations concernant la sécurité du système d'exploitation ..... 16
Commutateurs et ports réseau ..... 16
Sécurité d'un VLAN ..... 17
Sécurité InfiniBand ..... 18

**Gestion d'un environnement sécurisé** ..... 19
Contrôle de l'alimentation ..... 19
Suivi des ressources ..... 19
Mises à jour des microprogrammes et des logiciels ..... 20
Sécurité du réseau ..... 20
Protection et sécurité des données ..... 22
Gestion des journaux ..... 22

# Sécurité de base

Ce document fournit des instructions générales en matière de sécurité afin de vous aider à protéger votre serveur Oracle, les interfaces réseau du serveur et les commutateurs réseau connectés.

Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

Nous vous recommandons de respecter certaines principes de sécurité de base lorsque vous utilisez un matériel ou un logiciel. Cette section présente les quatre principes de sécurité de base :


- "Accès" à la page 7
- "Authentification" à la page 8
- "Autorisation" à la page 8
- "Comptabilisation et audit" à la page 9


## Accès

L'accès peut désigner l'accès physique au matériel mais aussi l'accès physique ou virtuel aux logiciels.

- Mettez en place des contrôles physiques et logiciels pour protéger votre matériel ou vos données contre les intrusions.
- Modifiez tous les mots de passe par défaut lorsque vous installez un nouveau système. La plupart des types d'équipement utilisent des mots de passe par défaut (comme `changeme`) courants et facilitent l'accès non autorisé.
- Reportez-vous à la documentation qui accompagne votre logiciel pour activer les fonctionnalités de sécurité disponibles pour celui-ci.
- Installez les serveurs et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est dotée d'un verrou.
- Si le matériel est installé dans un rack dont la porte est équipée d'un verrou, maintenez-la verrouillée et ne l'ouvrez que pour effectuer la maintenance des composants du rack.

- Limitez l'accès aux ports et consoles USB. Les périphériques tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau sont équipés de connexions USB, lesquelles peuvent fournir un accès direct au système. L'accès physique constitue une méthode d'accès aux composants plus sécurisée dans la mesure où il ne risque aucune attaque réseau.
- Limitez la possibilité de redémarrer le système via le réseau.
- Restreignez l'accès aux périphériques enfichables ou échangeables à chaud, essentiellement parce qu'ils peuvent être facilement retirés.
- Installez les unités remplaçables sur site (FRU) et les unités remplaçables par l'utilisateur (CRU) de remplacement dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.

# Authentification

L'authentification désigne la façon dont l'utilisateur est identifié ; il s'agit généralement d'informations confidentielles telles qu'un nom d'utilisateur et un mot de passe. L'authentification garantit que les utilisateurs du matériel ou des logiciels sont bien ceux qu'ils prétendent être.

- Configurez des fonctions d'authentification, comme un système de mots de passe dans les systèmes d'exploitation de votre plate-forme, afin d'éviter toute usurpation d'identité.
- Veillez à ce que les employés utilisent correctement leur badge pour pénétrer dans la salle informatique.
- Pour les comptes utilisateur, établissez des listes de contrôle d'accès lorsque cette mesure est pertinente. Définissez des délais d'expiration pour les sessions prolongées, ainsi que des niveaux de privilèges pour les utilisateurs.

# Autorisation

L'autorisation permet aux administrateurs de contrôler les tâches et les privilèges qu'un utilisateur peut exécuter ou utiliser. Le personnel peut uniquement effectuer les tâches et utiliser les privilèges qui lui ont été assignés. L'autorisation désigne les restrictions s'appliquant aux employés quant à l'utilisation du matériel ou des logiciels.

- Autorisez uniquement les employés à utiliser le matériel et les logiciels pour lesquels ils ont été formés et certifiés.
- Mettez 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 et audit

La comptabilisation et l'audit désignent la création d'un enregistrement des activités d'un utilisateur sur le système. Les serveurs Oracle sont dotés de fonctions matérielles et logicielles permettant aux administrateurs de surveiller les connexions et de tenir à jour les inventaires de matériel.

- Surveillez les connexions des utilisateurs par le biais de journaux système. Surveillez étroitement les comptes d'administrateur système et de maintenance, lesquels ont accès à des commandes puissantes qui, en cas de mauvaise utilisation, peuvent provoquer une perte de données. Les accès et les commandes doivent être soigneusement contrôlés via les journaux système.
- Enregistrez les numéros de série de l'ensemble de votre matériel. Assurez le suivi des ressources système à l'aide des numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur les cartes, modules et cartes mères, et peuvent être utilisés à des fins d'inventaire.
- Pour détecter les composants et en effectuer le suivi, apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les FRU et les CRU. Utilisez des stylos à ultraviolet ou des étiquettes en relief.
- Conservez les clés d'activation et les licences matérielles dans un emplacement sécurisé auquel l'administrateur système peut facilement accéder, particulièrement en cas d'urgence. Les documents imprimés peuvent être votre seule preuve de propriété.

# Utilisation des outils de configuration et de gestion du serveur de façon sécurisée

Respectez les consignes de sécurité décrites dans les sections suivantes lorsque vous configurez et gérez un serveur à l'aide d'outils logiciels et de microprogrammes.


- "Sécurité d'Oracle ILOM" à la page 11
- "Sécurité d'Oracle Hardware Management Pack" à la page 12


Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

## Sécurité d'Oracle ILOM

Vous pouvez sécuriser, gérer et surveiller de manière active les composants du système à l'aide du microprogramme de gestion Oracle Integrated Lights Out Manager (ILOM) préinstallé sur les serveurs x86 d'Oracle et sur certains serveurs SPARC. Selon le niveau d'autorisation accordé, ces fonctions peuvent inclure la capacité de mettre le serveur hors tension, de créer des comptes utilisateur, de monter des périphériques de stockage distants et ainsi de suite.

- **Utilisez un réseau interne sécurisé.**

  Que vous établissiez une connexion de gestion physique à Oracle ILOM via le port série local, le port de gestion réseau dédié, le port de gestion sideband ou le port réseau de données standard, il est essentiel que ce port physique sur le serveur soit toujours connecté à un réseau interne de confiance, à un réseau de gestion sécurisé dédié ou à un réseau privé.

  Ne connectez jamais le processeur de services (SP) Oracle ILOM à un réseau public tel qu'Internet. Il est recommandé de conserver le trafic de gestion du processeur de service Oracle ILOM sur un réseau de gestion distinct et d'en donner l'accès uniquement aux administrateurs système.

- **Limitez l'utilisateur du compte Administrateur par défaut.**

  Limitez l'utilisation du compte Administrateur par défaut (`root`) à l'utilisateur connecté initialement à Oracle ILOM. Ce compte Administrateur par défaut ne sert qu'à faciliter l'installation initiale du serveur. Pour assurer la sécurité optimale de l'environnement, vous devez remplacer le mot de passe par défaut du compte Administrateur, `changeme`, lors de

la configuration initiale du système. Si une personne non autorisée parvient à se connecter au compte Administrateur par défaut, elle dispose d'un accès illimité à toutes les fonctions d'Oracle ILOM. De plus, créez de nouveaux comptes utilisateur avec des mots de passe uniques et des niveaux d'autorisation (rôles utilisateur) pour tous les nouveaux utilisateurs d'Oracle ILOM.

- **Tenez compte des risques potentiels lorsque vous connectez le port série à un serveur terminal.**

  Les périphériques terminaux ne fournissent pas toujours les niveaux adéquats d'authentification utilisateur ou d'autorisation nécessaires à la protection du réseau contre les utilisateurs malveillants. Pour protéger votre système contre les intrusions réseau indésirables, n'établissez pas de connexion série (port série) à Oracle ILOM via tout type de périphérique de redirection réseau, tel qu'un serveur terminal, sauf si le serveur dispose de contrôles d'accès suffisants.

  De plus, certaines fonctions d'Oracle ILOM, telles que la réinitialisation du mot de passe et le menu de préinitialisation, sont uniquement disponibles lors de l'utilisation du port série physique. La connexion du port série à un réseau utilisant un serveur terminal non authentifié élimine la nécessité d'accès physique et réduit le niveau de sécurité associé à ces fonctions.

- **L'accès au menu de préinitialisation nécessite l'accès physique au serveur.**

  Le menu de préinitialisation d'Oracle ILOM est un utilitaire puissant permettant de rétablir les valeurs par défaut d'Oracle ILOM et de flasher le microprogramme si Oracle ILOM ne répond plus. Après la réinitialisation d'Oracle ILOM, l'utilisateur doit appuyer sur un bouton du serveur (le bouton par défaut) ou saisir un mot de passe. La propriété Présence physique d'Oracle ILOM contrôle ce comportement (`check_physical_presence= true`). Afin d'assurer un niveau de sécurité optimal lors de l'accès au menu de préinitialisation, ne modifiez pas le réglage par défaut (`true`) afin que l'accès au menu de préinitialisation nécessite toujours l'accès physique au serveur.

- **Reportez-vous à la documentation d'Oracle ILOM.**

  Reportez-vous à la documentation d'Oracle ILOM pour en savoir plus sur la configuration des mots de passe, la gestion des utilisateurs et l'application des fonctions de sécurité, notamment l'authentification SSH (Secure Shell), SSL (Secure Socket Layer) et RADIUS. Pour connaître les consignes de sécurité spécifiques d'Oracle ILOM, reportez-vous au *Guide de sécurité d'Oracle ILOM*, disponible dans la bibliothèque de documentation Oracle ILOM. Vous trouverez la documentation relative à Oracle ILOM à l'adresse suivante :

  http://www.oracle.com/goto/ilom/docs

# Sécurité d'Oracle Hardware Management Pack

Oracle Hardware Management Pack est disponible pour votre serveur et pour de nombreux autres serveurs x86 Oracle ainsi que certains serveurs Oracle SPARC. Ce pack se compose de deux éléments : un agent de surveillance SNMP et un ensemble d'outils d'interface de ligne de commande (outils CLI) multiplateformes pour la gestion du serveur. Vous pouvez tirer parti

des outils de ligne de commande (CLI) pour configurer les serveurs Oracle. Les outils CLI sont compatibles avec Oracle Solaris, Oracle Linux, Oracle VM, d'autres versions de Linux et les systèmes d'exploitation Microsoft Windows.

- **Utilisez les plug-ins SNMP de l'agent de gestion du matériel.**

  Le protocole standard SNMP permet de surveiller ou de gérer un système. Avec les plug-ins SNMP de l'agent de gestion du matériel, vous pouvez surveiller les serveurs Oracle de votre centre de données par le biais de SNMP sans avoir à vous connecter aux deux points de gestion que sont l'hôte et Oracle ILOM. Cette fonctionnalité permet d'utiliser une seule adresse IP (celle de l'hôte) pour surveiller plusieurs serveurs.

  Les plug-ins SNMP s'exécutent sur le système d'exploitation hôte des serveurs Oracle. Le module plug-in SNMP étend l'agent SNMP natif dans le système d'exploitation hôte de manière à offrir des fonctions Oracle MIB supplémentaires. Oracle Hardware Management Pack ne contient pas d'agent SNMP. Pour Linux, un module est ajouté à l'agent net-snmp. Pour Oracle Solaris, un module est ajouté à l'agent de gestion Oracle Solaris. Pour Microsoft Windows, le plug-in étend le service SNMP natif. Tous les paramètres de sécurité liés à 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 versions SNMPv1 et SNMPv2c n'offrent pas de chiffrement et procèdent à l'authentification à l'aide de chaînes de communauté. En revanche, SNMPv3 est plus sécurisé et est la version que nous vous recommandons d'utiliser car elle met en oeuvre le chiffrement pour fournir un canal sécurisé, ainsi que des noms et mots de passe utilisateur individuels.

- **Reportez-vous à la documentation d'Oracle Hardware Management Pack.**

  Pour plus d'informations sur ces fonctions, reportez-vous à la documentation relative à Oracle Hardware Management Pack. Pour connaître les consignes de sécurité propres à Oracle Hardware Management Pack, reportez-vous au *Oracle Hardware Management Pack (HMP) Security Guide*, disponible dans la bibliothèque de documentation d'Oracle Hardware Management Pack. Vous trouverez la documentation d'Oracle Hardware Management Pack à l'adresse suivante :

  `http://www.oracle.com/goto/ohmp/docs`

# Planification d'un environnement sécurisé

Des instructions en matière de sécurité doivent être mises en place avant la livraison du système. Après la livraison du système, les instructions de sécurité doivent être contrôlées et adaptées de façon régulière afin de rester conforme avec les exigences de votre société en matière de sécurité.

Utilisez les informations de cette section avant et pendant l'installation et la configuration d'un serveur et des équipements associés.


- "Protection par mot de passe" à la page 15
- "Recommandations concernant la sécurité du système d'exploitation" à la page 16
- "Commutateurs et ports réseau" à la page 16
- "Sécurité d'un VLAN" à la page 17
- "Sécurité InfiniBand" à la page 18


Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

## Protection par mot de passe

Les mots de passe représentent un aspect important de la sécurité : des mots de passe trop faibles peuvent entraîner des accès non autorisés aux ressources de la société. La mise en place de pratiques recommandées pour la gestion des mots de passe permet de garantir que les utilisateurs respectent un ensemble de directives pour la création et la protection de leurs mots de passe. Les composants habituels d'une stratégie de mot de passe doivent définir les éléments suivants :

- Longueur et niveau de sécurité du mot de passe
- Durée du mot de passe
- Pratiques courantes en matière de mot de passe

Mettez en place les pratiques standard suivantes afin de créer des mots de passe complexes :

- N'utilisez pas de mot de passe contenant le nom de l'utilisateur, le nom de l'employé ou les noms des membres de sa famille.

- N'utilisez pas de mots de passe trop faciles à deviner.
- N'utilisez pas de suite de chiffres consécutifs telle que 12345.
- N'utilisez pas de mots de passe contenant un mot ou une chaîne facile à deviner grâce à une simple recherche sur Internet.
- N'autorisez pas les utilisateurs à réutiliser le même mot de passe sur plusieurs systèmes.
- N'autorisez pas les utilisateurs à réutiliser des mots de passe déjà utilisés.

Modifiez régulièrement vos mots de passe. Cela permet de réduire les risques d'activité malveillante et garantit la conformité des mots de passe aux stratégies en vigueur.

# Recommandations concernant la sécurité du système d'exploitation

Reportez-vous à la documentation relative à votre système d'exploitation Oracle pour plus d'informations sur les points suivants :

- Utilisation des fonctions de sécurité lors de la configuration des systèmes.
- Fonctionnement sécurisé lors de l'ajout d'applications et d'utilisateurs à un système.
- Protection des applications réseau.

Vous trouverez la documentation relative à la sécurité des systèmes d'exploitation Oracle pris en charge dans la bibliothèque sur les systèmes d'exploitation. Pour trouver la documentation relative à la sécurité d'un système d'exploitation Oracle donné, accédez à la bibliothèque correspondante :

| Système d'exploitation | Lien |
|---|---|
| Oracle Solaris | http://www.oracle.com/technetwork/documentation/solaris-11-192991.html |
| Oracle Linux | http://www.oracle.com/technetwork/documentation/ol-1-1861776.html |
| Oracle VM | http://www.oracle.com/technetwork/documentation/vm-096300.html |

Pour obtenir des informations sur les systèmes d'exploitation d'éditeurs tiers tels que Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows et VMware ESXi, reportez-vous à la documentation des éditeurs concernés.

# Commutateurs et ports réseau

Les commutateurs réseau proposent différents niveaux de fonctions de sécurité de port. Reportez-vous à la documentation du commutateur concerné pour savoir comment effectuer les opérations suivantes :

- Utilisez les fonctions d'authentification, d'autorisation et de comptabilisation pour l'accès local et à distance à un commutateur.
- Modifiez chaque mot de passe sur des commutateurs réseau susceptibles de comprendre plusieurs comptes utilisateur et mots de passe par défaut.
- Gérez les commutateurs out-of-band (séparés du trafic de données). Si la gestion out-of-band n'est pas réalisable, il convient de dédier un numéro de réseau local virtuel (VLAN) distinct à la gestion in-band.
- Utilisez la fonctionnalité de mise en miroir des ports du commutateur réseau pour l'accès au système de détection des intrusions (IDS).
- Conservez un fichier de configuration de commutateur hors ligne et réservez-en l'accès aux administrateurs autorisés. Le fichier de configuration doit contenir des commentaires descriptifs pour chaque paramètre.
- Implémenter la sécurité des ports pour limiter l'accès en fonction d'une adresse MAC. Désactivez la jonction automatique sur tous les ports.
- Utilisez ces fonctions si elles sont disponibles sur votre commutateur :
  - **MAC Locking** – Implique l'association d'une adresse MAC (Media Access Control) d'un ou de plusieurs périphériques connectés à un port physique sur un commutateur. Si vous verrouillez un port de commutateur avec une adresse MAC particulière, les superutilisateurs ne peuvent pas créer de portes dérobées dans votre réseau avec des points d'accès non autorisés.
  - **MAC Lockout** – Empêche une adresse MAC spécifiée de se connecter à un commutateur.
  - **MAC Learning** – Utilise les informations sur les connexions directes de chaque port de commutateur de manière à ce que le commutateur réseau puisse configurer la sécurité en fonction des connexions en cours.

# Sécurité d'un VLAN

Si vous configurez un réseau local virtuel (VLAN), sachez que les VLAN partagent de la bande passante sur un réseau et nécessitent des mesures de sécurité supplémentaires. Pour renforcer la sécurité, vous pouvez appliquer les mesures suivantes :

- Séparez les clusters de systèmes sensibles du reste du réseau lorsque vous utilisez des VLAN. Vous réduisez ainsi le risque de voir des utilisateurs accéder à des informations sur ces clients et serveurs.
- Affectez un numéro VLAN natif unique aux ports de jonction.
- Limitez les VLAN pouvant être transférés via une jonction à ceux pour qui cela est strictement nécessaire.
- Si possible, désactivez le protocole VTP (VLAN Trunking Protocol). Autrement, définissez les paramètres suivants pour ce protocole : domaine de gestion, mot de passe et nettoyage. Définissez ensuite VTP sur le mode transparent.
- Dans la mesure du possible, utilisez des configurations de VLAN statiques.

- Désactivez les ports de commutateur inutilisés et attribuez-leur un numéro VLAN non utilisé.

# Sécurité InfiniBand

Pour renforcer la sécurité lorsque vous utilisez InfinBand, vous pouvez appliquer les mesures suivantes :

- Les hôtes Infiniband doivent rester sécurisés. La sécurité globale d'un Fabric InfiniBand équivaut à celle de l'hôte InfiniBand le moins sécurisé.
- Notez que le partitionnement ne protège pas un Fabric InfiniBand. Le partitionnement offre uniquement l'isolation du trafic InfiniBand entre les machines virtuelles d'un hôte.

# Gestion d'un environnement sécurisé

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

Utilisez les informations présentées dans ces sections pour maintenir un environnement sécurisé.


- "Contrôle de l'alimentation" à la page 19
- "Suivi des ressources" à la page 19
- "Mises à jour des microprogrammes et des logiciels" à la page 20
- "Sécurité du réseau" à la page 20
- "Protection et sécurité des données" à la page 22
- "Gestion des journaux" à la page 22


Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

## Contrôle de l'alimentation

Certains systèmes Oracle peuvent être mis sous tension et hors tension à l'aide de logiciels. Les unités de distribution de courant (PDU) de certaines armoires système peuvent être activées et désactivées à distance. Généralement, l'autorisation relative à ces commandes est définie au cours de la configuration du système et réservée aux administrateurs système et au personnel de maintenance.

Pour plus d'informations, reportez-vous à la documentation relative à votre système ou votre armoire.

## Suivi des ressources

Assurez le suivi de l'inventaire à l'aide des numéros de série. Les numéros de série Oracle sont intégrés dans le microprogramme des cartes d'option et des cartes mères système. Ces numéros de série peuvent être lus par le biais de connexions au réseau local (LAN).

Vous pouvez également utiliser des lecteurs d'identification par radiofréquence (RFID) pour simplifier davantage le suivi des ressources. Le livre blanc d'Oracle intitulé *How to Track Your Oracle Sun System Assets by Using RFID* est disponible à l'adresse suivante :

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

# Mises à jour des microprogrammes et des logiciels

Les améliorations de sécurité sont intégrées via de nouvelles versions du logiciel et des patchs. La gestion efficace et proactive des patchs est une partie essentielle de la sécurité du système. Afin d'optimiser la sécurité de votre système, mettez celui-ci à jour avec les dernières versions de logiciels et tous les patchs de sécurité nécessaires.

- Vérifiez régulièrement l'existence de mises à jour logicielles et de patchs de sécurité.
- Installez toujours la dernière version officielle du logiciel ou microprogramme sur votre équipement.
- Le cas échéant, installez les patches de sécurité nécessaires pour votre logiciel.
- N'oubliez pas que les périphériques comme les commutateurs réseau contiennent également un microprogramme et peuvent nécessiter des patchs et des mises à jour spécifiques.

Vous pouvez trouver des mises à jour logicielles et des patchs de sécurité sur la page Web My Oracle Support à l'adresse :

https://support.oracle.com

# Sécurité du réseau

Une fois que les réseaux sont configurés selon des principes de sécurité, vous devez assurer un contrôle et une maintenance réguliers.

Respectez les consignes suivantes pour garantir la sécurité des accès locaux et distants aux système :

- Limitez la configuration à distance à des adresses IP spécifiques à l'aide de SSH plutôt que Telnet. En effet, Telnet transmet les noms d'utilisateur et mots de passe en texte clair, si bien que toute personne présente sur le segment de réseau local (LAN) peut éventuellement voir les informations d'identification. Définissez un mot de passe renforcé pour SSH.
- Utilisez la version 3 du protocole SNMP (Simple Network Management Protocol) pour garantir des transmissions sécurisées. Les versions plus anciennes de SNMP ne sont pas sécurisées et transmettent les données d'authentification sous forme de texte non chiffré.

SNMPv3 met en oeuvre le chiffrement pour fournir un canal sécurisé, ainsi que des noms et mots de passe utilisateur individuels.

- Si SNMPv1 ou SNMPv2 est nécessaire, remplacez la chaîne de communauté SNMP par défaut par une chaîne de communauté fiable. Dans certains produits, la chaîne de communauté SNMP par défaut est PUBLIC. Des personnes malveillantes peuvent interroger une communauté afin de dessiner un plan très complet du réseau et, éventuellement, modifier des valeurs de la base d'informations de gestion (MIB).
- Si le contrôleur système emploie une interface de navigateur, veillez à toujours vous en déconnecter après utilisation.
- Activez les services réseau nécessaires et configurez-les de manière sécurisée. Désactivez les services réseau non indispensables, tels que TCP (Transmission Control Protocol) ou HTTP (Hypertext Transfer Protocol).
- Appliquez les mesures de sécurité LDAP lorsque vous utilisez le protocole LDAP pour accéder au système.
- Créez un message d'accueil qui s'affiche lors de la connexion afin d'informer l'utilisateur que tout accès non autorisé est interdit. Vous pouvez également informer les utilisateurs de toute stratégie ou règle importante. Un message d'accueil permet par exemple d'avertir les utilisateurs de restrictions d'accès particulières à un système spécifique ou de leur rappeler les stratégies définies en matière de mots de passe et leur utilisation appropriée.
- Utilisez les listes de contrôle d'accès appropriées pour appliquer des restrictions.
- Définissez des délais d'expiration pour les sessions prolongées, ainsi que des niveaux de privilèges.
- Utilisez les fonctions d'authentification, d'autorisation et de comptabilité pour l'accès local et à distance à un commutateur.
- Utilisez ces services dans les environnements hautement sécurisés dans la mesure où ils sont validés par des certificats et d'autres formes de chiffrement fort en vue de protéger le canal :
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- Activez ces services sur des réseaux sécurisés privés où il ne risque pas d'y avoir des utilisateurs potentiellement malveillants :
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- Utilisez la fonctionnalité de mise en miroir des ports du commutateur pour l'accès au système de détection des intrusions (IDS).
- Implémentez la sécurité des ports pour limiter l'accès en fonction d'une adresse MAC. Désactivez la jonction automatique sur tous les ports.

Pour plus d'informations sur la sécurité réseau, reportez-vous au *Guide de sécurité d'Oracle ILOM*, qui figure dans la bibliothèque de documentation Oracle ILOM. Vous trouverez la documentation relative à Oracle ILOM à l'adresse suivante :

http://www.oracle.com/goto/ilom/docs

# Protection et sécurité des données

Respectez les consignes suivantes pour optimiser la protection et la sécurité des données:

- Sauvegardez les données importantes à l'aide de périphériques tels que des disques durs externes ou des unités de stockage USB. Stockez les données sauvegardées dans un second emplacement sécurisé, hors site.
- Sécurisez les informations confidentielles stockées sur les disques durs à l'aide d'un logiciel de chiffrement des données.
- Lors du retrait d'un ancien disque dur, détruisez-le physiquement ou effacez complètement les données qu'il contient. Il est encore possible de récupérer des données d'un disque après la suppression de fichiers ou le reformatage du disque. Les opérations de suppression des fichiers ou de reformatage d'un disque ont uniquement pour effet de supprimer les tables d'adresses sur le disque. Effacez complètement les données d'un disque à l'aide d'un logiciel de nettoyage de disque.
- Les unités de disque dur servent généralement à stocker des informations sensibles. Pour protéger ces informations d'une divulgation non autorisée, les unités de disque dur doivent être nettoyées avant d'être réutilisées, mises hors service ou mises au rebut.
  - Utilisez des outils d'effacement de disque tels que la commande Oracle Solaris `format (1M)` pour supprimer l'intégralité des données contenues dans l'unité de disque. Le cas échéant, vous pouvez également utiliser des outils physiques de démagnétisation.
  - Dans certains cas, les informations contenues dans les unités de disque dur sont si sensibles que la meilleure méthode de nettoyage consiste à détruire physiquement ces unités en les pulvérisant ou en les incinérant.
  - Les entreprises sont fortement incitées à appliquer leurs stratégies de protection des données afin d'identifier la méthode la plus adaptée pour nettoyer les unités de disque dur.

**Attention -** Les logiciels d'effacement de disque peuvent échouer à supprimer certaines données sur les unités de disque dur modernes, notamment les disques durs électroniques (SSD), à cause de leur méthode de gestion de l'accès aux données.

# Gestion des journaux

Contrôlez et assurez à intervalles réguliers la maintenance des fichiers journaux. Sécurisez les fichiers journaux en suivant les méthodes ci-dessous :

- Activez la journalisation et envoyez les journaux système à un hôte de journal sécurisé dédié.
- Configurez la journalisation de manière à inclure des informations horaires exactes, à l'aide du protocole NTP et d'horodatages.

- Effectuez des analyses planifiées régulière des fichiers journaux des périphériques réseau afin de détecter toute activité ou accès inhabituels sur le réseau.
- Consultez les journaux afin de rechercher d'éventuels incidents et archivez-les conformément à la stratégie de sécurité.
- Retirez régulièrement les fichiers journaux lorsque leur taille devient excessive. Conservez des copies des fichiers retirés pour pouvoir vous y reporter à l'avenir ou en vue d'une analyse statistique.