

Serveurs des séries SPARC et Netra SPARC T5

Guide de sécurité

Copyright © 2013 , 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 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. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. 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

1. Sécurité des serveurs des séries SPARC et Netra SPARC T5	5
Présentation des principes de sécurité	5
Planification d'un environnement sécurisé	6
Sécurité du matériel	6
Sécurité des logiciels	6
Sécurité des microprogrammes	7
Sécurité d'Oracle OpenBoot	7
Microprogramme Oracle ILOM	7
Gestion d'un environnement sécurisé	8
Contrôles du matériel	8
Suivi des ressources	8
Mises à jour des microprogrammes et des logiciels	8
Accès local et à distance	8
Sécurité des données	9
Sécurité du réseau	9

• • • C h a p i t r e 1

Sécurité des serveurs des séries SPARC et Netra SPARC T5

Ce document formule des recommandations générales en matière de sécurité pour les serveurs SPARC T5-1B, T5-2, T5-4, T5-8 et Netra SPARC T5-1B. Il a pour objet de vous aider à assurer la sécurité de ces serveurs lorsque vous les utilisez avec d'autres produits matériels Oracle tels que des commutateurs réseau et des cartes d'interface réseau.

Ce chapitre contient les sections suivantes :

- [“Présentation des principes de sécurité” à la page 5](#)
- [“Planification d'un environnement sécurisé” à la page 6](#)
- [“Gestion d'un environnement sécurisé” à la page 8](#)

Présentation des principes de sécurité

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

- **Accès**

Les contrôles physiques et logiciels protègent 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.
- Les microprogrammes peuvent uniquement être modifiés par le processus de mise à jour Oracle.

- **Authentification**

Les systèmes d'exploitation de toutes les plates-formes fournissent des fonctions d'authentification qui peuvent être configurées de façon à s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être.

L'authentification fournit divers degrés de sécurité grâce à des mesures telles que les badges et les mots de passe.

- **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 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**

Tirez parti des fonctions logicielles et matérielles Oracle pour surveiller les connexions et tenir à jour les inventaires de matériel.

- Les informations de connexion des utilisateurs peuvent être contrôlées via des journaux système. Les comptes d'administrateur système et de maintenance, en particulier, ont accès à des commandes puissantes et doivent être soigneusement contrôlés via les journaux système. Les journaux sont généralement conservés pendant une longue période, de sorte qu'il est essentiel de retirer régulièrement les fichiers journaux lorsqu'ils dépassent une taille raisonnable, conformément à la politique client de la société.
- Les ressources informatiques du client sont généralement suivies 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.

Planification d'un environnement sécurisé

Prenez en compte les remarques suivantes avant et pendant l'installation et la configuration d'un serveur et des équipements connexes.

Sécurité du matériel

Pour sécuriser le matériel physique, il suffit de limiter l'accès au matériel et d'enregistrer les numéros de série.

- **Limiter l'accès**

- Installez les serveurs et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est fermée à clé.
- Si le matériel est installé dans un rack dont la porte est dotée d'un verrou, verrouillez toujours celle-ci jusqu'à ce que vous deviez effectuer la maintenance des composants du rack.
- Limitez l'accès aux consoles USB, qui peuvent offrir un accès plus aisé que les connexions SSH. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau peuvent être équipés de connexions USB.
- Restreignez l'accès aux périphériques enfichables ou échangeables à chaud, parce qu'ils sont facilement retirés.
- Installez les unités remplaçables sur site (FRU) ou les unités remplaçables par l'utilisateur (CRU) de remplacement dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.

- **Enregistrer les numéros de série**

- Enregistrez les numéros de série de l'ensemble de votre matériel.
- Apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les pièces de rechange. 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 en cas d'urgence. Les documents imprimés peuvent être votre seule preuve de propriété.

Sécurité des logiciels

La sécurité du matériel passe en grande partie par des logiciels.

- 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. En outre, les périphériques tels que les commutateurs réseau peuvent avoir plusieurs comptes d'utilisateur par défaut. Assurez-vous de modifier tous les mots de passe de compte.
- Limitez l'utilisation du compte superutilisateur `root`. Utilisez plutôt dans la mesure du possible des profils utilisateur Oracle Integrated Lights Out Manager (Oracle ILOM), tels que `operator` et `administrator`.
- Utilisez un réseau dédié pour les processeurs de service afin de les séparer du réseau général.
- Reportez-vous à la documentation qui accompagne votre logiciel pour activer les fonctionnalités de sécurité disponibles.
- Un serveur peut être initialisé en toute sécurité avec l'initialisation via connexion WAN ou l'initialisation iSCSI.
 - Reportez-vous au manuel *Oracle Solaris Installation Guide: Network-Based Installations* de votre version d'Oracle Solaris 10.
 - Si vous possédez une version Oracle Solaris 11, reportez-vous au manuel *Installing Oracle Solaris 11 Systems* pour des informations d'initialisation WAN et au manuel *System Administration Guide: Basic Administration* pour des informations d'initialisation iSCSI.

Le document *Oracle Solaris Security Guidelines* fournit les informations suivantes :

- Sécurisation d'Oracle Solaris
- Utilisation des fonctions de sécurité Oracle Solaris lorsque vous configurez vos systèmes
- Fonctionnement sécurisé lors de l'ajout d'applications et d'utilisateurs à un système
- Protection des applications réseau

Vous trouverez le document *Oracle Solaris Security Guidelines* de votre version aux pages suivantes :

- <http://www.oracle.com/goto/Solaris11/docs>
- <http://www.oracle.com/goto/Solaris10/docs>

Sécurité des microprogrammes

Les sous-composants du microprogramme du système Oracle ne peuvent être mis à jour qu'ensemble. Le microprogramme du système Oracle utilise un processus contrôlé de mise à jour des microprogrammes pour empêcher les modifications non autorisées des microprogrammes. Seuls le superutilisateur ou un utilisateur authentifié et autorisé peuvent exécuter le processus de mise à jour.

Sécurité d'Oracle OpenBoot

L'accès à l'interface de ligne de commande du microprogramme Oracle OpenBoot peut être protégé par mot de passe à l'aide de variables de sécurité OpenBoot.

Pour plus d'informations sur la configuration des variables de sécurité OBP, reportez-vous au manuel *OpenBoot 4.x Command Reference Manual* à l'adresse suivante :

- <http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfid-17069>

Microprogramme Oracle ILOM

Le microprogramme de gestion système Oracle Integrated Lights Out Manager (Oracle ILOM) est préinstallé sur le serveur, le module serveur, le système modulaire et autre matériel Oracle. Oracle

ILOM vous permet de gérer et de contrôler de manière active les composants installés sur le système. Votre utilisation d'Oracle ILOM a une incidence sur la sécurité de votre système. Pour en savoir plus sur l'utilisation de ce microprogramme lors de la configuration des mots de passe, de la gestion des utilisateurs et de l'application des fonctions de sécurité, y compris l'authentification SSH (Secure Shell), SSL (Secure Socket Layer) et RADIUS, reportez-vous à la documentation d'Oracle ILOM :

- <http://www.oracle.com/goto/ILOM/docs>

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.

Contrôles du matériel

Certains systèmes Oracle peuvent être configurés de sorte à être activés ou désactivés à l'aide de commandes logicielles. En outre, les unités de distribution de courant (PDU) de certaines armoires système peuvent être activées et désactivées à distance à l'aide de commandes logicielles. 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

Les numéros de série Oracle sont incorporés dans le microprogramme situé sur les cartes d'option et les cartes mères système. Ces numéros de série peuvent être lus par le biais de connexions au réseau local à des fins de suivi d'inventaire.

Les lecteurs d'identification par radiofréquence (RFID) peuvent 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

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

Accès local et à distance

Suivez les recommandations ci-dessous pour garantir la sécurité des accès local et à distance à vos systèmes :

- Créez une bannière afin d'indiquer que l'accès non autorisé est interdit.
- Utilisez les listes de contrôle d'accès appropriées.
- 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 (AAA) pour l'accès local et à distance à un commutateur.
- Dans la mesure du possible, utilisez les protocoles de sécurité RADIUS et TACACS+ :
 - RADIUS (Remote Authentication Dial-In User Service) est un protocole client/serveur qui permet de sécuriser les réseaux contre les accès non autorisés.
 - TACACS+ (Terminal Access Controller Access-Control System) est un protocole qui permet à un serveur d'accès à distance de communiquer avec un serveur d'authentification pour déterminer si un utilisateur a accès au réseau.
- 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.
- 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 LAN peut éventuellement voir les informations d'identification. Définissez un mot de passe fiable pour SSH.
- Les versions plus anciennes de SNMP ne sont pas sécurisées et transmettent les données d'authentification sous forme de texte non chiffré. Seule la version 3 de SNMP peut fournir des transmissions sécurisées.
- Certains produits sont livrés avec PUBLIC défini en tant que chaîne de communauté SNMP par défaut. Des personnes malveillantes peuvent interroger une communauté afin de dessiner un plan très complet du réseau et, le cas échéant, modifier des valeurs de la base d'informations de gestion (MIB). Si le service SNMP est nécessaire, remplacez la chaîne de communauté SNMP par défaut par une chaîne de communauté fiable.
- Activez la journalisation et envoyez les journaux à un hôte de journal sécurisé dédié.
- Configurez la journalisation pour inclure des informations horaires exactes, à l'aide du protocole NTP et d'horodatages.
- Consultez les journaux afin de rechercher d'éventuels incidents et archivez-les conformément à la stratégie de sécurité.
- Si le contrôleur système utilise une interface de navigateur, pensez à vous déconnecter après utilisation.

Sécurité des données

Suivez les recommandations ci-dessous pour optimiser la sécurité des données :

- Sauvegardez les données importantes à l'aide de périphériques tels que des disques durs externes, des clés USB ou des cartes mémoire MS. 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. La suppression de tous les fichiers ou le reformatage du disque dur supprime uniquement les tables d'adresses sur le disque ; il est toujours possible de récupérer les informations sur le disque après suppression des fichiers ou le reformatage. Utilisez un logiciel de nettoyage de disque pour effacer complètement toutes les données d'un disque.

Sécurité du réseau

Suivez les directives ci-après pour optimiser la sécurité de votre réseau :

- Dans la plupart des cas, les commutateurs permettent de définir des réseaux locaux virtuels (VLAN). Si vous utilisez votre commutateur pour définir des VLAN, séparez les clusters de systèmes sensibles du reste du réseau. Vous réduisez ainsi le risque de voir des utilisateurs accéder à des informations sur ces clients et serveurs.
- Gérez les commutateurs out-of-band (séparés du trafic de données). Si la gestion out-of-band n'est pas réalisable, dédiez un numéro VLAN distinct à la gestion in-band.
- 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.
- Conservez un fichier de configuration de commutateur hors ligne et en réserver l'accès aux administrateurs autorisés. Le fichier de configuration doit contenir des commentaires descriptifs pour chaque paramètre.
- Dans la mesure du possible, utilisez la configuration de VLAN statique.
- Désactivez les ports de commutateur libres et attribuez-leur un numéro VLAN non utilisé.
- 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). Sinon, définissez les paramètres suivants pour ce protocole : domaine de gestion, mot de passe et nettoyage. Définissez ensuite VTP sur le mode transparent.
- Désactivez les services réseau inutiles, tels que les petits serveurs TCP ou HTTP. Activez les services réseau nécessaires et configurez-les de manière sécurisée.
- Différents commutateurs proposent différents niveaux de fonctions de sécurité de port. Utilisez ces fonctions si elles sont disponibles sur votre commutateur :
 - MAC Locking (verrouillage MAC) : cela implique la liaison 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 (verrouillage MAC) : cette option permet d'empêcher une adresse MAC spécifiée de se connecter à un commutateur.
 - MAC Learning (apprentissage MAC) : utilisez les informations sur les connexions directes de chaque port de commutateur afin que le commutateur puisse configurer la sécurité en fonction des connexions en cours.