Guide de sécurité des serveurs des séries SPARC et Netra SPARC S7-2

Référence: E77183-01
Juin 2016

Référence: E77183-01

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

Présentation de la sécurité du matériel

L'isolement physique et le contrôle d'accès constituent la base de votre architecture de sécurité. Un serveur physique installé dans un environnement sécurisé est protégé contre tout accès non autorisé. De même, l'enregistrement de tous les numéros de série protège l'équipement contre les risques de vol, de revente ou au niveau de la chaîne logistique (autrement dit, le risque que des composants de contrefaçon soient intégrés à la chaîne logistique de votre organisation).

Les sections ci-après fournissent des recommandations générales concernant la sécurité matérielle des serveurs SPARC et Netra SPARC S7-2.

Restrictions d'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. La fermeture des portes permet également de restreindre l'accès aux périphériques enfichables ou échangeables à chaud.
- 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.
- Vérifiez régulièrement l'état et l'intégrité des verrous du rack et de l'armoire contenant les disques de rechange afin de vous assurer qu'ils ne sont pas abîmés ou que les portes n'ont pas été laissées déverrouillées.
- Conservez les clés de l'armoire dans un endroit sécurisé et dont l'accès est limité.
- Limitez l'accès aux consoles USB. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau peuvent être équipés de connexions USB. L'accès physique constitue une méthode d'accès à un composant plus sécurisée dans la mesure où il ne risque aucune attaque réseau.

- Connectez la console à un périphérique KVM externe afin d'activer l'accès à la console à distance. Les périphériques KVM prennent souvent en charge une authentification à deux facteurs, un contrôle des accès centralisé et des procédures d'audit. Pour plus d'informations sur les recommandations en matière de sécurité et les bonnes pratiques relatives aux périphériques KVM, reportez-vous à la documentation fournie avec le périphérique KVM.

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.

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 :

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

Unités de disque dur

Les unités de disque dur servent généralement à stocker des informations sensibles. Pour protéger ces informations d'une divulgation non autorisée, nettoyez les unités de disque dur avant de les réutiliser, ou de les mettre hors service ou 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.
- Les entreprises doivent se référer à leurs stratégies de protection des données afin d'identifier la méthode la plus adaptée pour nettoyer les unités de disque dur.
- Si nécessaire, utilisez le service de conservation des périphériques et des données client d'Oracle

  `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Présentation de la sécurité logicielle

La sécurité du matériel passe en grande partie par des logiciels. Les sections ci-après fournissent des recommandations générales concernant la sécurité logicielle des serveurs SPARC et Netra SPARC S7-2.

Protection contre les accès non autorisés (Oracle Solaris)

- **Utilisez les commandes du SE Oracle Solaris pour limiter l'accès au logiciel Oracle Solaris, sécuriser le SE, utiliser des fonctions de sécurité et protéger les applications.**

  Vous trouverez le document *Directives de sécurité d'Oracle Solaris* correspondant à la version que vous utilisez à l'adresse suivante :

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

Protection contre les accès non autorisés (Oracle ILOM)

- **Utilisez les commandes Oracle ILOM pour limiter l'accès utilisateur au logiciel Oracle ILOM, modifier le mot de passe défini en usine, limiter l'utilisation du compte superutilisateur root et sécuriser le réseau privé au niveau du processeur de service.**

Obtenez le *Guide de sécurité d'Oracle ILOM* à l'adresse suivante :

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

▼ Protection contre les accès non autorisés (Oracle VM Server for SPARC)

- **Utilisez les commandes Oracle VM for SPARC pour limiter l'accès au logiciel Oracle VM for SPARC.**

  Obtenez le *Guide de sécurité d'Oracle VM for SPARC* à l'adresse suivante :

  http://www.oracle.com/goto/vm-sparc/docs

Restriction d'accès (OpenBoot)

Les rubriques suivantes décrivent comment limiter l'accès à l'invite OpenBoot.

- "Implémentation de la protection par mot de passe" à la page 10
- "Activation du mode de sécurité" à la page 11
- "Désactivation du mode de sécurité" à la page 12
- "Vérification des échecs de connexion" à la page 12
- "Création d'un message relatif à la mise sous tension" à la page 12

Pour plus d'informations sur la configuration des variables de sécurité OpenBoot, reportez-vous à la documentation OpenBoot à l'adresse suivante :

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

▼ Implémentation de la protection par mot de passe

- **Si vous n'avez pas encore défini de mot de passe, effectuez cette étape.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

Le mot de passe doit comporter entre un et huit caractères. Si vous entrez plus de huit caractères, seuls les huit premiers sont utilisés. Tous les caractères imprimables sont acceptés. Les caractères de contrôle ne sont pas acceptés.

Remarque - La définition d'un mot de passe sur zéro caractère désactive la sécurité et traite le paramètre `security-mode` comme s'il était défini sur `none`. Cependant, le paramètre n'en est pas modifié.

▼ Activation du mode de sécurité

1. **Définissez le paramètre `security-mode` sur `full` ou `command`.**

   Lorsque ce paramètre est défini sur `full`, un mot de passe est requis pour toutes les actions, y compris des opérations normales comme `boot`. Lorsqu'il est défini sur `command`, aucun mot de passe n'est nécessaire pour les commandes `boot` ou `go`, mais toutes les autres commandes nécessitent un mot de passe. Pour assurer la continuité des opérations, définissez le paramètre `security-mode` sur `command`, comme dans l'exemple suivant.

   ```
   {0} ok setenv security-mode command
   {0} ok
   ```

2. **Affichez l'invite du mode de sécurité.**

   Après avoir défini le mode de sécurité comme décrit ci-dessus, vous pouvez afficher l'invite du mode de sécurité de deux façons.

   - **Utilisez les commandes `logout` et `login`.**

     ```
     {0} ok logout
     Type boot, go (continue), or login (command mode)
     >
     > login
     Firmware Password: password
     Type help for more information
     {0} ok
     ```

     Pour quitter le mode de sécurité, utilisez les commandes `logout` et `login`, comme indiqué dans l'exemple.

   - **Utilisez la commande `reset-all`.**

     ```
     {0} ok reset-all
     ```

     Cette commande réinitialise le système. Quand le système est rétabli, OpenBoot affiche l'invite du mode de sécurité. Pour vous reconnecter à l'invite de commande (ou vous déconnecter du mode de sécurité), utilisez les commandes `logout` et `login`, puis entrez le mot de passe, comme décrit ci-dessus.

Désactivation du mode de sécurité

1. **Définissez le paramètre `security-mode` sur `none`.**

   ```
   {0} ok setenv security-mode none
   ```

2. **Définissez le mot de passe sur une longueur égale à zéro en tapant Return après les deux invites de mot de passe.**

Vérification des échecs de connexion

1. **Vous pouvez vérifier si un utilisateur a tenté de se connecter et n'a pas réussi à accéder à l'environnement OpenBoot en utilisant le paramètre `security-#badlogins`, comme dans l'exemple suivant.**

   ```
   {0} ok printenv security-#badlogins
   ```

   Si cette commande renvoie une valeur supérieure à zéro, cela signifie qu'une tentative d'accès à l'environnement OpenBoot a échoué.

2. **Réinitialisez le paramètre en tapant cette commande.**

   ```
   {0} ok setenv security-#badlogins 0
   ```

Création d'un message relatif à la mise sous tension

Bien qu'il ne serve pas de contrôle préventif ou de détection, un message peut être utilisé pour les raisons suivantes :

- Confirmer la propriété.
- Avertir les utilisateurs sur l'utilisation acceptable du serveur.
- Indiquer que l'accès ou les modifications apportées aux paramètres OpenBoot est restreint au personnel autorisé.

- **Utilisez les commandes suivantes pour activer un message d'avertissement personnalisé.**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  Le message peut comporter jusqu'à 68 caractères. Tous les caractères imprimables sont acceptés.

Microprogramme du système Oracle

Le microprogramme du système Oracle utilise un processus contrôlé de mise à jour des microprogrammes pour empêcher toute modification non autorisée. Seuls le superutilisateur ou un utilisateur authentifié et autorisé peuvent exécuter le processus de mise à jour.

Pour plus d'informations sur l'obtention des derniers patches ou mises à jour, reportez-vous aux notes de produit de votre serveur.

Sécurisation de l'initialisation via connexion WAN

L'initialisation via connexion WAN prend en charge différents niveaux de sécurité. Vous pouvez utiliser une combinaison des fonctions de sécurité prises en charge selon les besoins de votre réseau. Une configuration fortement sécurisée est plus lourde à administrer, mais les données de votre système sont mieux protégées.

- Pour le système d'exploitation Oracle Solaris 10, reportez-vous à la section relative à la configuration sécurisée de l'installation de l'initialisation via connexion WAN dans le manuel *Guide d'installation d'Oracle Solaris : installations basées sur réseau*.
- Pour le système d'exploitation Oracle Solaris 11, reportez-vous au manuel *Sécurisation du réseau dans Oracle Solaris 11.3*.

Verified Boot

La fonctionnalité Verified Boot peut être utilisée pour vérifier les blocs d'initialisation du système et les modules de noyau Oracle Solaris avant qu'ils soient chargés sur le système. Utilisez Oracle ILOM pour activer Verified Boot et pour indiquer la manière dont le système doit réagir lorsqu'une vérification échoue. L'activation de Verified Boot peut empêcher l'application de modifications dangereuses sur les blocs d'initialisation du système ou les modules de noyau Oracle Solaris.

Pour plus d'informations sur la configuration des propriétés Verified Boot des systèmes SPARC, reportez-vous au document *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM*.