Guide de sécurité des serveurs SPARC M8 et SPARC M7

Référence: E55218-02
Septembre 2017

Référence: E55218-02

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.

Référence: E55218-02

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, le fait d'enregistrer tous les numéros de série permet d'empêcher l'utilisation de composants matériels non autorisés.

Les sections qui suivent fournissent des directives générales de sécurité matérielle concernant les serveurs

Restrictions d'accès

- Installez les serveurs et les équipements connexes dans un local interdit d'accès et fermé 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. Le verrouillage des portes permet également de restreindre l'accès aux périphériques enfichables ou échangeables à chaud.
- Stockez toute les pièces de rechange 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 pièces de rechange afin de vous assurer qu'ils ne sont pas abîmés ou que les portes n'ont pas été laissées déverrouillées par inadvertance.
- Conservez les clés de l'armoire dans un endroit sécurisé 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

Empêchez l'utilisation de composants matériels non autorisés en enregistrant soigneusement tous les numéros de série lors de la réception des composants et de leur prise en compte dans le stock. Avant d'installer ou d'utiliser un composant, veillez à vérifier son authenticité en comparant son numéro de série à celui enregistré lors de sa réception. Pour la sécurité du matériel, respectez la procédure suivante :

- Conservez un enregistrement des numéros de série de tous les équipements.
- Apposez une marque de sécurité sur tous les éléments importants du matériel informatique, notamment 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 (disques durs et disques durs électroniques) sont souvent utilisées pour stocker des informations sensibles. Pour protéger ces informations contre toute divulgation non autorisée, nettoyez les unités de disque dur avant de les réutiliser, de les mettre hors service ou de les mettre 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 reporter à leur stratégie de protection des données afin d'identifier la méthode la plus adaptée pour nettoyer les unités de disque dur.
- ******* SENTENCE TO BE DELETED - QUERY 293031 *********

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 qui suivent fournissent des directives générales concernant la sécurité logicielle des serveurs.

Protection contre les accès non autorisés (Oracle Solaris)

- **Utilisez les commandes d'Oracle Solaris pour limiter l'accès au logiciel Oracle Solaris, sécuriser le système d'exploitation, 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)

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

   Vous trouverez le *Guide de sécurité Oracle ILOM* à l'adresse suivante :

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

2. **Si possible, utilisez les commandes Oracle ILOM spécifiques à la plate-forme pour sécuriser les domaines individuels en créant des comptes utilisateur dont les rôles s'appliquent à un domaine physique spécifique.**

   Lorsque vous attribuez des rôles utilisateur à un domaine physique, les capacités accordées pour ce domaine reflètent celles des rôles utilisateur attribués pour la plate-forme, mais elles sont restreintes aux commandes exécutées sur le composant concerné.

   Remarque - Seuls les rôles utilisateur d'administrateur (a), de console (c) et de réinitialisation (r) peuvent être attribués à des domaines physiques individuels.

   Obtenez le *Guide d'administration des serveurs SPARC M8 et SPARC M7* à l'adresse suivante :

   `http://docs.oracle.com/cd/E55211_01/`

▼ 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.**

  Vous trouverez le *Guide de sécurité Oracle VM for SPARC* à l'adresse suivante : `http://www.oracle.com/goto/vm-sparc/docs`.

Restriction d'accès (OBP)

Les rubriques suivantes expliquent comment limiter l'accès à l'invite OBP.

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 peut comprendre de un à huit caractères. Si vous entrez plus de huit caractères, seuls les huit premiers sont retenus. Tous les caractères imprimables sont acceptés. Les caractères de contrôle sont rejetés.

Remarque - Si vous n'entrez aucun caractère pour le mot de passe, la sécurité est désactivée et le paramètre `security-mode` est traité comme s'il avait la valeur `none`. Toutefois, ce paramètre n'est pas modifié.

▼ Activation du mode de sécurité

1. **Affectez au paramètre `security-mode` la valeur `full` ou `command`.**

Lorsque ce paramètre est défini sur `full`, un mot de passe est requis pour toutes les actions, y compris pour les opérations normales comme `boot`. Lorsqu'il est défini sur `command`, aucun mot de passe n'est requis 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 sécurisé.**

Après avoir paramétré le mode de sécurité comme indiqué plus haut, vous avez le choix entre deux méthodes pour afficher l'invite correspondante.

- **Utiliser 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 noms `logout` et `login`.

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

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

Cette commande réinitialise le système. Lorsque le système redémarre, OpenBoot affiche l'invite du mode de sécurité. Pour revenir à l'invite de commande (ou quitter le mode de sécurité), utilisez les noms `logout` et `login` puis entrez le mot de passe comme indiqué précédemment.

Désactivation du mode de sécurité

1. **Affectez au paramètre `security-mode` la valeur `none`.**

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

2. **Définissez un mot de passe de longueur nulle en appuyant sur Entrée après les deux invites de saisie du mot de passe.**

Vérification des échecs de connexion (OBP)

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.**

   ```
   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 entrant :**

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

Définition d'une bannière à afficher au démarrage

Une bannière ne permet pas de contrôle de prévention ou de détection, mais elle peut être utile pour :

- Signaler le propriétaire
- Informer les utilisateurs de l'usage toléré du serveur
- Indiquer que la consultation ou la modification des paramètres OpenBoot est réservée 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 de la bannière peut comprendre 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 pour empêcher toute modification non autorisée. Seul le superutilisateur ou un utilisateur authentifié et autorisé peut 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 à l'adresse suivante :

http://docs.oracle.com/cd/E55211_01/

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 l'O/S 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*.

  Voir http://www.oracle.com/goto/solaris10/docs
- Pour le système d'exploitation Oracle Solaris 11, reportez-vous au manuel *Sécurisation du réseau dans Oracle Solaris* .

  Voir http://www.oracle.com/goto/solaris11/docs