Serveurs SPARC M5-32 et SPARC M6-32

Guide de sécurité

Référence: E49761-02
Juillet 2014

Table des matières

• • • Chapitre 1

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).

Ce chapitre fournit des recommandations en matière de sécurité pour les serveurs SPARC M5-32 et SPARC M6-32.

Il inclut les sections suivantes :

Restrictions d'accès

- 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 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 remplacement. 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 RFID sans fil peuvent simplifier davantage le suivi des ressources. Pour plus d'informations, reportez-vous au livre blanc *How to Track Your Oracle Sun System Assets by Using RFID* disponible à l'adresse suivante :

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, 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 SSD, à cause de leur méthode de gestion de l'accès aux données.

• • • Chapitre 2

Présentation de la sécurité logicielle

La sécurité du matériel passe en grande partie par les logiciels. Ce chapitre fournit des recommandations en matière de sécurité logicielle pour les serveurs SPARC M5-32 et SPARC M6-32.

Il inclut les sections suivantes :

▼ Protection contre les accès non autorisés (SE 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.
  Le document Oracle Solaris contenant les recommandations en matière de sécurité adaptées à votre version du SE est disponible 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 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
2. 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 par rapport à 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 M5-32 et SPARC M6-32* à l'adresse suivante :
http://www.oracle.com/goto/M6-32/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 expliquent comment limiter l'accès à l'invite OpenBoot.

- “Implémentation de la protection par mot de passe (OpenBoot)” à la page 8
- “Vérification des échecs de connexion (OpenBoot)” à la page 8
- “Création d'un message relatif à l'alimentation (OpenBoot)” à la page 9

Informations connexes

- Pour plus d'informations sur la configuration des variables de sécurité OpenBoot, 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

▼ Implémentation de la protection par mot de passe (OpenBoot)

- 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 telle que l'initialisation. Lorsqu'il est défini sur **command**, aucun mot de passe n'est nécessaire pour les commandes **boot** ni **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.

```
ok password
ok setenv security-mode command
ok password
```

▼ Vérification des échecs de connexion (OpenBoot)

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 **security-#badlogins** en saisissant la commande suivante.

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

▼ Création d'un message relatif à l'alimentation (OpenBoot)

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

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

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. 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 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 requiert davantage de procédures d'administration, mais les données de votre système sont mieux protégées.

- Pour le SE 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 réseau*.

  http://www.oracle.com/goto/Solaris10/docs
- Pour le SE Oracle Solaris 11, reportez-vous au manuel *Sécurisation du réseau dans Oracle Solaris 11.1*.

  http://www.oracle.com/goto/Solaris11/docs