Guide de sécurité d'Oracle® VM Server for SPARC 3.0

Référence : E37590
Décembre 2012

ORACLE

130416@25097

Table des matières

Préface

Le *Guide de sécurité d'Oracle VM Server for SPARC 3.0* fournit des informations indiquant comment installer, configurer et utiliser le logiciel Oracle VM Server for SPARC 3.0 en toute sécurité.

Documentation connexe

Le tableau suivant présente la documentation disponible pour la version Oracle VM Server for SPARC 3.0 et la documentation connexe.

TABLEAU P–1 Documentation connexe

Application	Titre
Logiciel Oracle VM Server for SPARC 3.0	*Guide d'administration d'Oracle VM Server for SPARC 3.0* *Guide de sécurité d'Oracle VM Server for SPARC 3.0* *Oracle VM Server for SPARC 3.0 Reference Manual* *Notes de version d'Oracle VM Server for SPARC 3.0*
Pages de manuel `drd`(1M) et `vntsd`(1M) d'Oracle VM Server for SPARC 3.0	Manuels de référence du SE Oracle Solaris : ■ Documentation Oracle Solaris 10 ■ Documentation Oracle Solaris 11
SE Oracle Solaris : installation et configuration	Guides relatifs à l'installation et la configuration du SE Oracle Solaris : ■ Documentation Oracle Solaris 10 ■ Documentation Oracle Solaris 11
Sécurité d'Oracle VM Server for SPARC et du SE Oracle Solaris	Livre blanc d'Oracle VM Server for SPARC et guides de sécurité du SE Oracle Solaris : ■ *Secure Deployment of Oracle VM Server for SPARC* (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`) ■ *Oracle Solaris 10 Security Guidelines* ■ *Oracle Solaris 11 Security Guidelines*

Vous trouverez des documents relatifs à votre serveur, votre logiciel ou au SE Oracle Solaris à l'adresse `http://www.oracle.com/technetwork/indexes/documentation/index.html`. Utilisez la zone de recherche pour rechercher les documents et les informations dont vous avez besoin.

Vous pouvez accéder au forum de discussion Oracle VM Server for SPARC à l'adresse `http://forums.oracle.com/forums/forum.jspa?forumID=1047`.

Accéder au support Oracle

Les clients d'Oracle peuvent accéder à un 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 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–2 Conventions typographiques

Type de caractères	Description	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez le fichier `.login`. Utilisez `ls -a` pour dresser la liste des fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie stockée localement. N'enregistrez *pas* le fichier . **Remarque :** certains éléments mis en évidence apparaissent en caractères gras.

Invites de shell dans les exemples de commande

Le tableau suivant présente les invites système UNIX et les invites du superutilisateur pour les shells inclus dans le SE Oracle Solaris. Dans les exemples de commandes, l'invite de shell indique si la commande doit être exécutée par un utilisateur standard ou un utilisateur doté des privilèges nécessaires.

TABLEAU P–3 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour un superutilisateur	`#`
Shell C	`machine_name%`
Shell C pour un superutilisateur	`machine_name#`

◆ ◆ ◆ CHAPITRE 1

Présentation de la sécurité d'Oracle VM Server for SPARC

Ce chapitre décrit les fonctions de sécurité suivantes utilisées par le logiciel Oracle VM Server for SPARC

Fonctions de sécurité utilisées par Oracle VM Server for SPARC

Le logiciel Oracle VM Server for SPARC est un produit de virtualisation qui permet l'exécution de plusieurs machines virtuelles (VM) Oracle Solaris sur un même système physique, chaque machine virtuelle étant équipée de son propre système d'exploitation Oracle Solaris 10 ou Oracle Solaris 11. Chaque machine virtuelle est également désignée par le terme *domaine logique*. Les domaines sont des instances indépendantes pouvant exécuter différentes versions du SE Oracle Solaris, ainsi que différents logiciels d'application. Par exemple, des révisions de packages différentes peuvent être installées sur chacun des domaines, des services différents peuvent y être activés et les comptes système peuvent avoir des mots de passe différents. Pour plus d'informations sur la sécurité d'Oracle Solaris, reportez-vous aux manuels *Oracle Solaris 10 Security Guidelines* et *Oracle Solaris 11 Security Guidelines* .

La commande `ldm` doit être exécutée sur le domaine de contrôle pour configurer le domaine logique et récupérer les informations sur l'état. Pour assurer la sécurité des domaines exécutés sur le système, il est crucial de restreindre l'accès au domaine de contrôle et à la commande `ldm`. Pour restreindre l'accès aux données de configuration des domaines, utilisez les fonctions de sécurité d'Oracle VM Server for SPARC telles que la fonction de contrôle d'accès basé sur les rôles (RBAC) d'Oracle Solaris pour les consoles et les autorisations `solaris.ldoms`. Reportez-vous à la section "Profils contenus dans Logical Domains Manager" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

Le logiciel Oracle VM Server for SPARC utilise les fonctions de sécurité suivantes

- Les fonctions de sécurité disponibles dans les SE Oracle Solaris 10 et Oracle Solaris 11 sont également disponibles dans les domaines qui exécutent le logiciel Oracle VM Server for SPARC. Reportez-vous aux manuels *Oracle Solaris 10 Security Guidelines* et *Oracle Solaris 11 Security Guidelines* .
- Les fonctions de sécurité du SE Oracle Solaris peuvent être appliquées au logiciel Oracle VM Server for SPARC. Pour des informations exhaustives sur la sécurité d'Oracle VM Server for SPARC, reportez-vous au document *Secure Deployment of Oracle VM Server for SPARC*.
- Les SE Oracle Solaris 10 et Oracle Solaris 11 incluent les correctifs de sécurité disponibles pour votre système. Vous pouvez obtenir les correctifs du SE Oracle Solaris 10 sous forme de patchs de sécurité ou de mises à jour. Vous pouvez obtenir les correctifs du SE Oracle Solaris 11 sous forme de SRU (Support Repository Updates, mises à jour du référentiel support).
- Pour restreindre l'accès aux commandes d'administration d'Oracle VM Server for SPARC et aux consoles des domaines, ainsi que pour activer la fonction d'audit d'Oracle VM Server for SPARC, reportez-vous au Chapitre 3, “Sécurité d’Oracle VM Server for SPARC” du manuel *Guide d’administration d’Oracle VM Server for SPARC 3.0*.

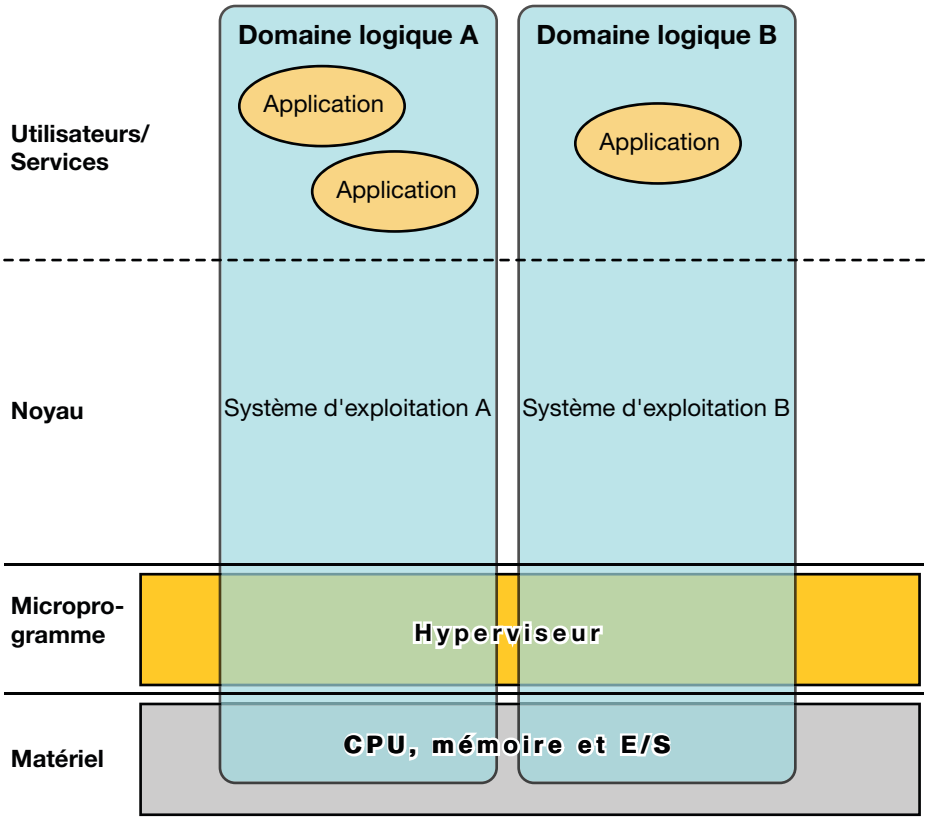
Présentation du produit Oracle VM Server for SPARC

Oracle VM Server for SPARC offre des capacités de visualisation de classe entreprise très efficaces pour les serveurs SPARC de série T d'Oracle. Grâce au logiciel Oracle VM Server for SPARC, vous pouvez créer jusqu'à 128 serveurs virtuels, appelés domaines logiques, sur un seul et même système. Ce type de configuration permet de bénéficier de la puissance d'exécution offerte par les serveurs SPARC de série T et le SE Oracle Solaris.

Un *domaine logique* est une machine virtuelle contenant un regroupement logique discret de ressources. Un domaine logique a son propre système d'exploitation et sa propre identité dans un système informatique unique. Chaque domaine logique peut être créé, supprimé, reconfiguré et réinitialisé individuellement, sans avoir à exécuter un cycle d'alimentation du serveur. Il est possible d'exécuter diverses applications dans des domaines logiques différents et de préserver leur indépendance en vue d'optimiser les performances et d'assurer leur sécurité.

Pour plus d'informations sur l'utilisation du logiciel Oracle VM Server for SPARC, reportez-vous aux manuels *Guide d’administration d’Oracle VM Server for SPARC 3.0* et *Oracle VM Server for SPARC 3.0 Reference Manual* . Pour plus d'informations sur la configuration matérielle et logicielle requise, reportez-vous au manuel *Notes de version d’Oracle VM Server for SPARC 3.0*.

FIGURE 1–1 Hyperviseur prenant en charge deux domaines logiques



Le logiciel Oracle VM Server for SPARC utilise les composants suivants pour assurer la virtualisation du système

- **Hyperviseur.** L'hyperviseur est une petite couche de microprogramme qui fournit une architecture de virtualisation stable dans laquelle un système d'exploitation peut être installé. Les serveurs Sun d'Oracle utilisant cet hyperviseur fournissent des fonctions matérielles renforçant le contrôle de l'hyperviseur sur les activités du système d'exploitation sur un domaine logique.

  Le nombre de domaines et les fonctions de chaque domaine pris en charge par un hyperviseur SPARC particulier sont des caractéristiques qui dépendent du serveur. L'hyperviseur peut allouer des sous-ensembles des ressources de CPU, de mémoire et d'E/S du serveur à un domaine logique donné. Cette allocation permet la prise en charge simultanée de plusieurs systèmes d'exploitation, chacun dans son propre domaine logique. Les ressources peuvent être réorganisées entre des domaines logiques distincts avec un niveau de précision quelconque. Il est par exemple possible d'assigner des CPU à un domaine logique avec une précision de l'ordre du thread de CPU.

Le processeur de service (SP), également appelé *contrôleur système* (SC) surveille et exécute la machine physique, mais ne gère pas les domaines logiques. Les domaines logiques sont gérés par Logical Domains Manager.

- **Domaine de contrôle.** Logical Domains Manager s'exécute dans ce domaine, vous permettant ainsi de créer et de gérer d'autres domaines logiques et d'allouer des ressources virtuelles à d'autres domaines. Vous ne pouvez avoir qu'un seul domaine de contrôle par serveur. Le domaine de contrôle est le premier domaine créé lorsque vous installez le logiciel Oracle VM Server for SPARC. Le domaine de contrôle est nommé `primary`.
- **Domaine de service.** Un domaine de service fournit à d'autres domaines des services de périphériques virtuels tel qu'un commutateur virtuel, un concentrateur de consoles virtuelles et un serveur de disque virtuel. N'importe quel domaine peut être configuré en tant que domaine de service.
- **Domaine d'E/S.** Un domaine d'E/S dispose d'un accès direct à des périphériques d'E/S physiques tels qu'une carte réseau dans un contrôleur PCI EXPRESS (PCIe). Un domaine d'E/S peut posséder un complexe racine PCIe ou il peut posséder un emplacement PCIe ou un périphérique PCIe intégré à l'aide de la fonction d'E/S directes (DIO). Reportez-vous à la section "Assignation des périphériques d'extrémité PCIe" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

  Un domaine d'E/S peut partager des périphériques d'E/S physiques avec d'autres domaines sous la forme de périphériques virtuels lorsque le domaine d'E/S est également utilisé en tant que domaine de service.
- **Domaine racine.** Un domaine racine dispose d'un complexe racine PCIe qui lui est assigné. Ce domaine possède la topologie Fabric PCIe et fournit tous les services associés à la Fabric, notamment le traitement des erreurs Fabric. Un domaine racine est également un domaine d'E/S, car il possède et a un accès direct aux périphériques d'E/S.

  Le nombre de domaines racine que vous pouvez avoir dépend de l'architecture de votre plate-forme. Par exemple, si vous utilisez un serveur Sun SPARC Enterprise T5440 d'Oracle, vous pouvez avoir jusqu'à quatre domaines racine.
- **Domaine invité.** Un domaine invité est un domaine non E/S qui consomme des services de périphériques virtuels fournis par un ou plusieurs domaines de service. Un domaine invité ne dispose d'aucun périphérique d'E/S physique. Il dispose uniquement de périphériques d'E/S virtuels tels que des disques virtuels et des interfaces réseau virtuelles.

Bien souvent, un système Oracle VM Server for SPARC ne comporte qu'un domaine de contrôle fournissant les services assurés par les domaines d'E/S et les domaines de service. Pour améliorer la redondance et la capacité de fonctionnement de la plate-forme, envisagez de configurer plus d'un domaine d'E/S sur votre système Oracle VM Server for SPARC.

Application de principes de sécurité généraux à Oracle VM Server for SPARC

Les domaines invités peuvent être configurés de différentes manières pour fournir des niveaux variables d'isolement des domaines invités, de partage du matériel et de connectivité des domaines. Ces facteurs contribuent à la sécurité de la configuration globale d'Oracle VM Server for SPARC, à laquelle vous pouvez appliquer certains des principes de sécurité généraux suivants :

- **Minimisez la surface d'attaque.**
  - Minimisez les erreurs de configuration involontaires en créant des lignes directrices opérationnelles vous permettant d'évaluer périodiquement la sécurité du système. Reportez-vous à la section “Counter Measure #1: Operational Guidelines” du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Planifiez avec soin l'architecture de l'environnement virtuel pour maximiser l'isolement des domaines. Reportez-vous aux contre-mesures décrites à la section “Threat #2: Errors in the Architecture of the Virtual Environment” du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Planifiez avec soin les ressources à affecter et décidez si elles doivent être partagées. Reportez-vous aux sections “Counter Measure #7: Carefully Assigning Hardware Resources” et “Counter Measure #8: Careful Assignment of Shared Resources” du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Assurez-vous que les domaines logiques sont à l'abri des manipulations en appliquant la contre-mesure décrite aux sections “Threat #4: Manipulation of the Execution Environment” et “Counter Measure #28: Securing the Guest OS” du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Exposez *uniquement* un domaine invité au réseau en cas de besoin. Vous pouvez utiliser des commutateurs virtuels pour restreindre la connectivité réseau d'un domaine invité aux réseaux appropriés *uniquement*.
  - Effectuez les opérations requises pour réduire la surface d'attaque dans Oracle Solaris 10 et Oracle Solaris 11, telles que décrites dans les manuels *Oracle Solaris 10 Security Guidelines* et *Oracle Solaris 11 Security Guidelines* .
  - Protégez le coeur de l'hyperviseur comme décrit dans les sections “Counter Measure #15: Validating Firmware and Software Signatures” et “Counter Measure #16: Validating Kernel Modules” du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Protégez le domaine de contrôle contre les attaques par déni de service. Reportez-vous à la section “Counter Measure #17: Console Access” du document *Secure Deployment of Oracle VM Server for SPARC*.

- Assurez-vous que Logical Domains Manager ne peut pas être exécuté par des utilisateurs non autorisés. Reportez-vous à la section “Threat #8: Unauthorized Use of Configuration Utilities” du document *Secure Deployment of Oracle VM Server for SPARC*.
- Assurez-vous que le domaine de service n'est pas accessible à des utilisateurs ou des processus non autorisés. Reportez-vous à la section “Threat #9: Manipulation of a Service Domain” du document *Secure Deployment of Oracle VM Server for SPARC*.
- Protégez un domaine d'E/S ou un domaine de service contre les attaques par déni de service. Reportez-vous à la section “Threat #10: Denial-of-Service of IO Domain or Service Domain” du document *Secure Deployment of Oracle VM Server for SPARC*.
- Assurez-vous qu'un domaine d'E/S n'est pas accessible à des utilisateurs ou des processus non autorisés. Reportez-vous à la section “Threat #11: Manipulation of an IO Domain” du document *Secure Deployment of Oracle VM Server for SPARC*.
- Désactivez les services non indispensables du gestionnaire de domaines. Logical Domains Manager fournit des services réseau pour l'accès aux domaines, ainsi que pour leur surveillance et leur migration. Désactivez les services réseau suivants lorsque vous ne les utilisez pas :
  - Service de migration sur le port TCP `8101`

    Pour désactiver ce service, reportez-vous à la description des propriétés `ldmd/incoming_migration_enabled` et `ldmd/outgoing_migration_enabled` dans la page de manuel `ldmd(1M)`.
  - La prise en charge XMPP (Extensible Messaging and Presence Protocol) sur le port TCP `6482`

    Pour désactiver ce service, reportez-vous à la section “Transport XML” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
  - Protocole SNMP (Simple Network Management Protocol) sur le port UDP `161`

    Déterminez si vous souhaitez utiliser la base MIB (Base d'informations de gestion) d'Oracle VM Server for SPARC pour observer les domaines. Cette fonction nécessite que le service SNMP soit activé. En fonction de votre choix, effectuez l'une des opérations suivantes :
    - **Activez le service SNMP afin d'utiliser la base MIB d'Oracle VM Server for SPARC.** Installez la base MIB d'Oracle VM Server for SPARC en toute sécurité. Reportez-vous à la section “Procédure d'installation du package logiciel Oracle VM Server for SPARC MIB” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0* et à la section “Gestion de la sécurité” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
    - **Désactivez le service SNMP.** Pour désactiver ce service, reportez-vous à la section “Procédure de suppression du package logiciel Oracle VM Server for SPARC MIB” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
  - Service de découverte sur l'adresse de multidiffusion `239.129.9.27` et le port `64535`

Il est *impossible* de désactiver ce service pendant que le démon de Logical Domains Manager, `ldmd`, est en cours d'exécution. Au lieu de cela, utilisez la fonction IP Filter d'Oracle Solaris pour bloquer l'accès à ce service, ce qui réduit la surface d'attaque de Logical Domains Manager. Le blocage de l'accès empêche l'utilisation non autorisée de l'utilitaire, ce qui permet de lutter efficacement contre les attaques par déni de service et les autres tentatives d'utilisation abusive de ces services réseau. Reportez-vous au Chapitre 20, "IP Filter in Oracle Solaris (Overview)" du manuel *Oracle Solaris Administration: IP Services* et à la section "Using IP Filter Rule Sets" du manuel *Oracle Solaris Administration: IP Services*.

Reportez-vous également aux sections "Counter Measure #14: Securing the ILOM" et "Counter Measure #20: Hardening LDoms Manager" du document *Secure Deployment of Oracle VM Server for SPARC*.

- **Accordez le privilège minimal nécessaire pour effectuer une opération.**
  - Isolez les systèmes en *classes de sécurité*, lesquelles correspondent à des groupes formés de systèmes invités individuels partageant les mêmes exigences en matière de sécurité et les mêmes privilèges. En assignant uniquement des domaines invités de la même classe de sécurité à une plate-forme matérielle donnée, vous créez une violation de l'isolement qui empêche les domaines de passer dans une autre classe de sécurité. Reportez-vous à la section "Counter Measure #2: Carefully Assigning Guests to Hardware Platforms" du document *Secure Deployment of Oracle VM Server for SPARC*.
  - Utilisez RBAC pour restreindre l'aptitude à gérer des domaines à l'aide de la commande `ldm`. *Seuls* les utilisateurs chargés d'administrer des domaines doivent être habilités à utiliser cette commande. Assignez un rôle utilisant le profil de droits LDoms Management (Gestion de domaines logiques) aux utilisateurs qui ont besoin d'accéder à l'ensemble des sous-commandes de `ldm`. Assignez un rôle utilisant le profil de droits LDoms Review (Vérification de domaines logiques) aux utilisateurs qui ont uniquement besoin d'accéder aux sous-commandes liées aux listes de `ldm`. Reportez-vous à la section "Utilisation des profils de droits et des rôles" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
  - Utilisez RBAC pour restreindre l'accès aux consoles des *seuls* domaines auxquels vous, en tant qu'administrateur d'Oracle VM Server for SPARC, devez accéder. N'autorisez *pas* l'accès général à tous les domaines. Reportez-vous à la section "Utilisation des profils de droits et des rôles" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
- **Surveillez l'activité du système.**

  Activez l'audit d'Oracle VM Server for SPARC. Reportez-vous à la section "Activation et utilisation de l'audit" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

Pour des recommandations sur le déploiement sécurisé du logiciel Oracle VM Server for SPARC, reportez-vous à la section “Recommended Deployment Options” in *Secure Deployment of Oracle VM Server for SPARC*.

◆ ◆ ◆ CHAPITRE 2

Installation et configuration sécurisées d'Oracle VM Server for SPARC

Ce chapitre décrit les considérations relatives à la sécurité liées à l'installation et la configuration d'Oracle VM Server for SPARC.

Installation

Le logiciel Oracle VM Server for SPARC est automatiquement installé de manière sécurisée en tant que package Oracle Solaris 10 ou Oracle Solaris 11. A l'issue de l'installation, vous devez disposer des privilèges d'administrateur pour configurer les domaines à l'aide des fonctions de contrôle d'accès basé sur les rôles (RBAC), d'audit et d'autorisation. Ces fonctionnalités ne sont pas activées par défaut.

Configuration postinstallation

Effectuez les tâches suivantes après avoir installé le logiciel Oracle VM Server for SPARC pour maximiser l'utilisation sécurisée

- Configurez le domaine de contrôle avec les services d'E/S virtuelles requis, tels que le commutateur virtuel, le serveur de disque virtuel et les services de concentrateur de consoles virtuelles. Reportez-vous au Chapitre 4, “Configuration des services et du domaine de contrôle” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.
- Configurez des domaines invités. Reportez-vous au Chapitre 5, “Configuration des domaines invités” du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

  Vous pouvez utiliser un commutateur virtuel pour configurer les domaines invités par le biais d'un réseau administratif et d'un réseau de production. Dans ce cas, un commutateur virtuel est créé en utilisant l'interface du réseau de production en tant que périphérique réseau du commutateur virtuel. Reportez-vous à la section “Counter Measure #13: Dedicated Management Network” du document *Secure Deployment of Oracle VM Server for SPARC*.

La sécurité d'un domaine invité est compromise lorsque l'un de ses disques virtuels est compromis. Assurez-vous donc que les disques virtuels (système de stockage rattaché au réseau, fichiers image de disque enregistrés localement ou disques physiques) sont stockés à un emplacement sécurisé.

Le démon `vntsd` est désactivé par défaut. Lorsque ce démon est activé, tout utilisateur connecté au domaine de contrôle est autorisé à se connecter à la console d'un domaine invité. Afin d'éviter ce type d'accès, assurez-vous que le démon `vntsd` est désactivé ou utilisez RBAC pour limiter l'accès à la console aux utilisateurs autorisés *uniquement*.

- Le processeur de service (SP) est, par défaut, configuré de manière sécurisée. Pour plus d'informations sur l'utilisation du logiciel Integrated Lights Out Management (ILOM) pour gérer le SP, reportez-vous à la documentation de votre plate-forme disponible à l'adresse `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

◆ ◆ ◆ CHAPITRE 3

Fonctions de sécurité d'Oracle VM Server for SPARC

Ce chapitre offre une présentation générale des fonctions de sécurité utilisées par le logiciel Oracle VM Server for SPARC.

Pour plus d'informations sur l'authentification, le contrôle d'accès et l'audit, reportez-vous au Chapitre 3, “Sécurité d’Oracle VM Server for SPARC” du manuel *Guide d’administration d’Oracle VM Server for SPARC 3.0*.

Modèle de sécurité

Le logiciel Oracle VM Server for SPARC s'appuie sur le modèle de sécurité et les fonctions intégrés dans le SE Oracle Solaris. Pour plus d'informations sur les directives de sécurité du SE Oracle Solaris, reportez-vous aux manuels *Oracle Solaris 11 Security Guidelines* et *Oracle Solaris 10 Security Guidelines* .

Configuration et utilisation de l'authentification

Comme dans une installation de base d'Oracle Solaris, tout utilisateur qui dispose d'un compte peut se connecter à un domaine logique, y compris le domaine de contrôle. Le logiciel Oracle VM Server for SPARC ne crée aucun compte utilisateur. Reportez-vous à la section “Installation de Logical Domains Manager” du manuel *Guide d’administration d’Oracle VM Server for SPARC 3.0*. Pour plus d'informations sur les méthodes de sécurisation des utilisateurs d'Oracle Solaris, reportez-vous à la section “Securing Users” du manuel *Oracle Solaris 11 Security Guidelines*.

Pour pouvoir utiliser Logical Domains Manager afin d'effectuer des activités de gestion du domaine de contrôle, un utilisateur doit posséder des privilèges spéciaux de lecture et d'écriture des données de configuration. Reportez-vous à la section “Profils contenus dans Logical Domains Manager” du manuel *Guide d’administration d’Oracle VM Server for SPARC 3.0* et à la section “Utilisation des profils de droits et des rôles” du manuel *Guide d’administration d’Oracle VM Server for SPARC 3.0*.

Configuration et utilisation de RBAC

La fonctionnalité RBAC (role-based access control, contrôle d'accès basé sur les rôles) du SE Oracle Solaris permet de gérer les autorisations et les profils de droits, et d'affecter des rôles aux comptes utilisateur. Pour plus d'informations sur RBAC, reportez-vous au Chapitre 9, "Using Role-Based Access Control (Tasks)" du manuel *System Administration Guide: Security Services*.

L'installation de Logical Domains Manager ajoute les autorisations et profils de droits nécessaires dans les fichiers locaux. Reportez-vous à la section "Utilisation des profils de droits et des rôles" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

Pour configurer les utilisateurs, les autorisations, les profils de droits et les rôles dans un service de noms, reportez-vous au *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Configuration et utilisation de l'audit

Vous devez administrer et auditer une instance d'Oracle Solaris dans un domaine invité de la même façon que vous géreriez un SE Oracle Solaris s'exécutant sur un système à nu. Vous pouvez personnaliser la fonction d'audit du SE Oracle Solaris pour auditer uniquement les fonctions et les services système importants pour votre environnement. Pour Oracle VM Server for SPARC, assurez-vous que la classe des logiciels de virtualisation est soumise à un audit. Vous pouvez effectuer d'autres tâches liées à l'audit. Reportez-vous à la section "Using the Audit Service" du manuel *Oracle Solaris 11 Security Guidelines* et à la section "How to Audit Significant Events in Addition to Login/Logout" du manuel *Oracle Solaris 11 Security Guidelines*.

Logical Domains Manager crée des événements d'audit et les transmet au sous-système d'audit d'Oracle Solaris en vue de les stocker et de les soumettre à un examen ultérieur. L'historique est conservé dans un journal consignant ce qui a été fait, à quel moment et par qui, ainsi que les éléments affectés. Notez que vous *ne pouvez pas* consulter les informations d'audit des domaines d'un système à partir du domaine de contrôle de celui-ci.

Par conséquent, pour chaque domaine du système, vous pouvez activer et désactiver la fonction d'audit selon la version du SE Oracle Solaris exécutée sur votre système en procédant de la manière suivante :

- **SE Oracle Solaris 10.** Utilisez les commandes `bsmconv` et `bsmunconv`. Reportez-vous aux pages de manuel `bsmconv(1M)` et `bsmunconv(1M)`, ainsi qu'à la version Oracle Solaris 10 du *System Administration Guide: Security Services*.
- **SE Oracle Solaris 11.** Utilisez la commande `audit`. Reportez-vous à la page de manuel `audit(1M)` et à la version Oracle Solaris 11 du manuel *Administration d'Oracle Solaris Services de sécurité*.

Pour plus d'informations, reportez-vous à la section "Activation et utilisation de l'audit" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

Configuration et utilisation d'autres fonctions de sécurité

Oracle VM Server for SPARC sécurise l'utilisation de certaines fonctionnalités de virtualisation. Lorsque le démon `vntsd` est activé, il est configuré par défaut de la manière la plus sûre possible. Il accepte uniquement les connexions à partir du domaine de contrôle et *non* celles transitant par le biais du réseau. Si nécessaire, vous pouvez configurer une option moins sécurisée pour permettre les connexions via le réseau. Reportez-vous à la description de la propriété `vntsd/listen_addr` dans la page de manuel `vntsd`(1M).

Faites très attention lorsque vous configurez le démon `vntsd` de manière à ce qu'il accepte les connexions réseau. Il est préférable d'autoriser uniquement les connexions à partir du domaine de contrôle ou de désactiver le démon `vntsd` pour une sécurité optimale. Reportez-vous à la section "Application de principes de sécurité généraux à Oracle VM Server for SPARC" à la page 13.

La fonction de migration de domaine d'Oracle VM Server for SPARC applique des mesures de sécurité. Logical Domains Manager sur la machine source accepte les demandes de migration d'un domaine et établit une connexion réseau sécurisée avec Logical Domains Manager s'exécutant sur la machine cible. La migration se produit une fois la connexion établie. Ces connexions sécurisées sont créées à l'aide de fonctionnalités d'authentification et de chiffrement. Reportez-vous à la section "Sécurité pour les opérations de migration" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

En particulier, l'opération de migration de domaine utilise par défaut le protocole SSL (Secure Sockets Layer) pour chiffrer toutes les données envoyées et reçues par le biais du réseau. Vous pouvez améliorer les performances de migration en affectant des unités cryptographiques aux domaines de contrôle sur les systèmes prenant en charge ces unités.

Lorsque la migration de domaine n'est pas nécessaire, vous pouvez désactiver la fonction de migration afin d'empêcher que le processus `ldmd` n'écoute sur le port de migration.

Si vous avez recours à la migration de domaine, assurez-vous que le démon `ldmd` est configuré de manière à exiger l'authentification par mot de passe pendant la migration. Il s'agit du comportement par défaut.

◆ ◆ ◆ CHAPITRE 4

Considérations relatives à la sécurité pour les développeurs

Ce chapitre fournit des informations utiles aux développeurs produisant des applications pour le logiciel Oracle VM Server for SPARC.

Interface XML d'Oracle VM Server for SPARC

Vous pouvez créer des programmes externes disposant d'une interface avec le logiciel Oracle VM Server for SPARC au moyen du mécanisme de communication XML (Extensible Markup Language), lequel utilise le protocole XMPP (Extensible Messaging and Presence Protocol).

Des personnes malveillantes étant susceptibles de tenter d'exploiter ce protocole réseau pour accéder à un système, il est recommandé de désactiver le protocole XMPP. Pour plus d'informations sur la désactivation du protocole XMPP, reportez-vous à la section "Transport XML" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*. Pour plus d'informations sur les mécanismes de sécurité utilisés par Logical Domains Manager, reportez-vous à la section "Serveur XMPP" du manuel *Guide d'administration d'Oracle VM Server for SPARC 3.0*.

Notez que la désactivation de XMPP vous empêche d'utiliser certaines fonctions essentielles d'Oracle VM Server for SPARC telles que la migration de domaine, la reconfiguration dynamique de la mémoire et la commande `ldm init-system`.

◆ ◆ ◆ ANNEXE A

Liste de contrôle pour un déploiement sécurisé

Cette liste de contrôle récapitule les opérations que vous pouvez effectuer pour renforcer la sécurité de votre environnement Oracle VM Server for SPARC. Les descriptions détaillées sont fournies dans d'autres documents, tels que les suivants :

- *Guide d'administration d'Oracle VM Server for SPARC 3.0*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*
- *Déploiement sécurisé d'Oracle VM Server for SPARC*

Liste de contrôle de sécurité d'Oracle VM Server for SPARC

- ❒ Effectuez les opérations de renforcement de la sécurité d'Oracle Solaris dans vos domaines invités comme vous le feriez dans un environnement non virtualisé.
- ❒ Utilisez les profils de droits LDoms Management (Gestion de domaines logiques) et LDoms Review (Vérification de domaines logiques) pour accorder les privilèges appropriés aux utilisateurs.
- ❒ Utilisez le contrôle d'accès basé sur les rôles (RBAC) pour restreindre l'accès aux consoles des *seuls* domaines auxquels vous, en tant qu'administrateur d'Oracle VM Server for SPARC, devez accéder.
- ❒ Activez la fonction d'audit du SE Oracle Solaris pour Oracle VM Server for SPARC.
- ❒ Désactivez les services non indispensables du gestionnaire de domaines.
- ❒ Déployez uniquement des systèmes invités de la même classe de sécurité sur une plate-forme physique donnée.
- ❒ Assurez-vous qu'il n'existe aucune connexion réseau entre l'administration de l'environnement d'exécution et les domaines invités.
- ❒ Affectez uniquement les ressources nécessaires aux systèmes invités.