

Guide de sécurité d'Oracle® VM Server for SPARC 3.1



Référence: E40603-01
Août 2013

Copyright © 2007, 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. 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. 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

Utilisation de cette documentation	5
 1 Présentation de la sécurité d'Oracle VM Server for SPARC	 7
Fonctions de sécurité utilisées par Oracle VM Server for SPARC	7
Présentation du produit Oracle VM Server for SPARC	8
Application de principes de sécurité généraux à Oracle VM Server for SPARC	11
Sécurité dans un environnement virtualisé	13
Environnement d'exécution	14
Sécurisation de l'environnement d'exécution	14
Défense contre les attaques	15
Environnement opérationnel	17
Environnement d'exécution	22
ILOM	25
Hyperviseur	26
Domaine de contrôle	28
Logical Domains Manager	28
Domaine de service	31
Domaine d'E/S	33
Domaines invités	35
 2 Installation et configuration sécurisées d'Oracle VM Server for SPARC	 37
Installation	37
Configuration post-installation	37
 3 Considérations relatives à la sécurité pour les développeurs	 39
Interface XML d'Oracle VM Server for SPARC	39
 A Liste de contrôle pour un déploiement sécurisé	 41
Liste de contrôle de sécurité d'Oracle VM Server for SPARC	41

Utilisation de cette documentation

Le *Guide de sécurité d'Oracle VM Server for SPARC 3.1* contient des informations indiquant comment installer, configurer et utiliser le logiciel Oracle VM Server for SPARC 3.1 en toute sécurité.

Bibliothèque de documentation produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse : <http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html>.

Le tableau suivant présente la documentation disponible pour la version Oracle VM Server for SPARC 3.1. Ces documents sont disponibles aux formats HTML et PDF, sauf mention contraire.

TABLEAU P-1 Documentation connexe

Application	Titre
Logiciel Oracle VM Server for SPARC 3.1	“ Oracle VM Server for SPARC 3.1 Administration Guide ”
	“ Oracle VM Server for SPARC 3.1 Security Guide ”
	“ Oracle VM Server for SPARC 3.1 Reference Manual ”
	“ Oracle VM Server for SPARC 3.1 Release Notes ”
Pages de manuel drd(1M) et vntsd(1M) d'Oracle VM Server for SPARC 3.1	Manuels de référence du SE Oracle Solaris :
	<ul style="list-style-type: none">■ Documentation Oracle Solaris 10 (http://www.oracle.com/technetwork/documentation/solaris-10-192992.html)■ Documentation Oracle Solaris 11.1 (http://docs.oracle.com/cd/E26502_01)
SE Oracle Solaris : installation et configuration	Guides relatifs à l'installation et la configuration du SE Oracle Solaris :
	<ul style="list-style-type: none">■ Documentation Oracle Solaris 10 (http://www.oracle.com/technetwork/documentation/solaris-10-192992.html)■ Documentation Oracle Solaris 11.1 (http://docs.oracle.com/cd/E26502_01)
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 :

Application	Titre
	<ul style="list-style-type: none">■ <i>Déploiement sécurisé d'Oracle VM Server for SPARC</i> (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.

Accès aux services de support Oracle

Les clients Oracle 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.

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>.

Commentaires

Faites part de vos commentaires sur cette documentation à l'adresse : <http://www.oracle.com/goto/docfeedback>.

Présentation de la sécurité d'Oracle VM Server for SPARC

Même si le nombre de recommandations relatives à la sécurité dans ce document peut laisser supposer le contraire, l'installation par défaut d'Oracle VM Server for SPARC est déjà bien protégée contre les utilisations non autorisées. Il subsiste toutefois une petite surface d'exposition aux attaques qui engendre un certain risque, mais son exploitation est peu probable. De la même manière que vous pouvez choisir de protéger votre maison en installant un système d'alarme en plus des éléments de dissuasion classiques tels que les verrous, des mesures de sécurité supplémentaires peuvent vous aider à réduire le risque de voir se produire des problèmes imprévus ou à minimiser les dommages potentiels.

Ce chapitre aborde les thèmes liés à la sécurité d'Oracle VM Server for SPARC suivants :

- [“Fonctions de sécurité utilisées par Oracle VM Server for SPARC” à la page 7](#)
- [“Présentation du produit Oracle VM Server for SPARC” à la page 8](#)
- [“Application de principes de sécurité généraux à Oracle VM Server for SPARC” à la page 11](#)
- [“Sécurité dans un environnement virtualisé” à la page 13](#)
- [“Défense contre les attaques” à la page 15](#)

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, Virtual Machine) 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` appelle Logical Domains Manager et doit être exécutée sur le domaine de contrôle pour configurer les domaines 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 les droits Oracle Solaris pour les consoles et les autorisations `solaris.ldoms`. Reportez-vous à la section [“Contenus du profil de droits Logical Domains Manager” du manuel “Guide d'administration d'Oracle VM Server for SPARC 3.1”](#).

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 manière d'assurer la sécurité d'Oracle VM Server for SPARC, reportez-vous aux sections [“Sécurité dans un environnement virtualisé” à la page 13](#) et [“Défense contre les attaques” à la page 15](#).
- 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 patches 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 plus d'informations sur la limitation de l'accès aux commandes d'administration d'Oracle VM Server for SPARC et aux consoles de 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 3.1”](#).

Présentation du produit Oracle VM Server for SPARC

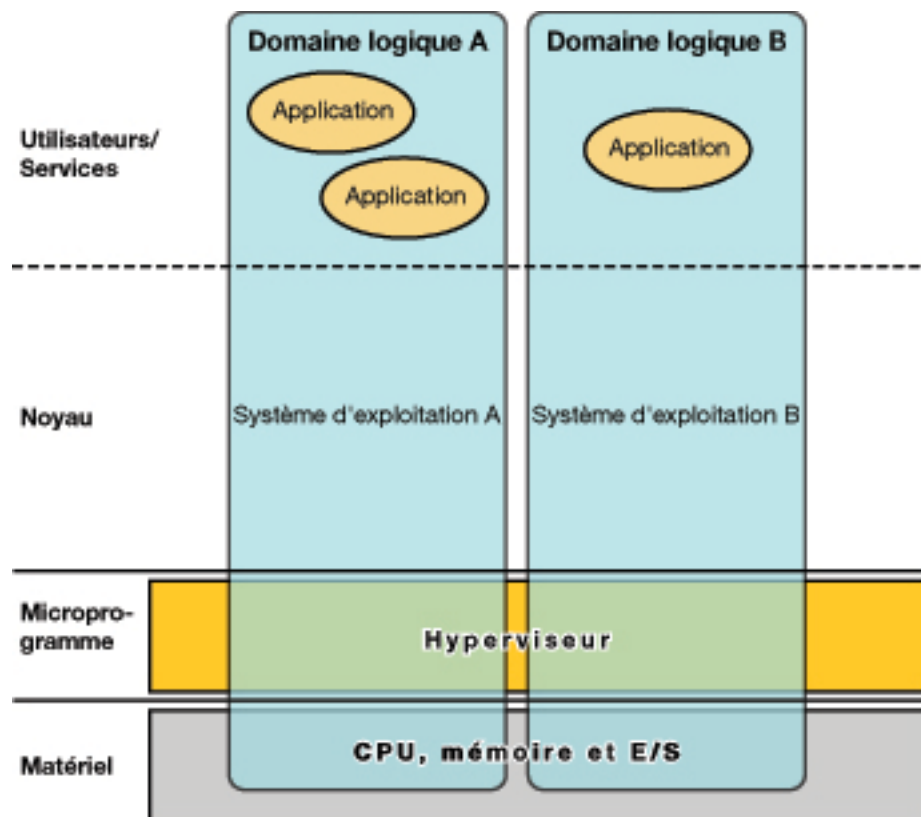
Oracle VM Server for SPARC fournit des fonctions de virtualisation professionnelles performantes pour les serveurs SPARC T-Series ainsi que pour le serveur SPARC M5 d'Oracle et les systèmes Fujitsu M10. Le logiciel Oracle VM Server for SPARC vous permet de créer un grand nombre de serveurs virtuels, 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 et le SE Oracle Solaris.

Un *domaine logique* est une machine virtuelle contenant un regroupement logique de ressources distinct. 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 nécessiter de 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 3.1](#) ” et “ [Oracle VM Server for SPARC 3.1 Reference Manual](#) ”. Pour plus d'informations sur la configuration matérielle et logicielle requise, reportez-vous au manuel “ [Oracle VM Server for SPARC 3.1.1.1, 3.1.1, and 3.1 Release Notes](#) ”.

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. C'est Logical Domains Manager, et non le processeur de service, qui gère les domaines logiques.

- **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. Il ne peut y 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 tels 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). En utilisant la fonction d'E/S directes (DIO), un domaine d'E/S peut posséder un complexe root PCIe ou il peut posséder un emplacement PCIe ou un périphérique PCIe intégré. Reportez-vous à la section [“ Création d'un domaine d'E/S par assignation de périphériques d'extrémité PCIe ” du manuel “ Guide d'administration d'Oracle VM Server for SPARC 3.1 ”](#).

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 root.** Un domaine root dispose d'un complexe root PCIe qui lui est assigné. Ce domaine est propriétaire de la topologie Fabric PCIe du complexe root concerné et fournit tous les services associés au Fabric, notamment le traitement des erreurs Fabric. Un domaine root est également un domaine d'E/S, car il possède et a un accès direct aux périphériques d'E/S.

Le nombre de domaines root que vous pouvez avoir dépend de l'architecture de votre plate-forme. Par exemple, si vous utilisez un serveur SPARC T4-4 d'Oracle, vous pouvez avoir jusqu'à quatre domaines root.

- **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 au niveau de sécurité de la configuration globale d'Oracle VM Server for SPARC. Pour obtenir des recommandations sur le déploiement sécurisé du logiciel Oracle VM Server for SPARC, reportez-vous aux sections [“Sécurité dans un environnement virtualisé” à la page 13](#) et [“Défense contre les attaques” à la page 15](#).

Vous pouvez appliquer certains des principes de sécurité généraux suivants :

- **Minimisez la surface d'exposition aux attaques.**
 - 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 [“Contre-mesure : création d'instructions opérationnelles” à la page 17](#).
 - Planifiez avec soin l'architecture de l'environnement virtuel pour maximiser l'isolement des domaines. Reportez-vous aux contre-mesures décrites à la section [“Menace : erreurs dans l'architecture de l'environnement virtuel” à la page 18](#).
 - Planifiez avec soin les ressources à affecter et décidez si elles doivent être partagées. Reportez-vous aux sections [“Contre-mesure : affectation attentive des ressources matérielles” à la page 21](#) et [“Contre-mesure : affectation attentive des ressources partagées” à la page 21](#).
 - Assurez-vous que les domaines logiques sont protégés contre les manipulations en appliquant les contre-mesures décrites aux sections [“Menace : manipulation de l'environnement d'exécution” à la page 22](#) et [“Contre-mesure : sécurisation du SE du domaine invité” à la page 35](#).
 - [“Contre-mesure : sécurisation des chemins d'accès interactifs” à la page 22](#).
 - [“Contre-mesure : réduction du SE Oracle Solaris” à la page 23](#).
 - [“Contre-mesure : sécurisation du SE Oracle Solaris” à la page 23](#).
 - [“Contre-mesure : sécurisation de Logical Domains Manager” à la page 29](#).
 - La section [“Contre-mesure : recours à la séparation des rôles et à l'isolement des applications” à la page 23](#) décrit l'importance d'attribuer des rôles de fonctionnalité aux différents domaines et de s'assurer que le domaine de contrôle exécute des logiciels fournissant l'infrastructure nécessaire pour héberger des domaines invités. Vous devez exécuter des applications qui peuvent être

exécutées par d'autres systèmes sur des domaines invités, lesquels doivent être conçus pour cet usage.

- La section [“Contre-mesure : configuration d'un réseau de gestion dédié” à la page 24](#) décrit une configuration réseau plus avancée qui relie des serveurs équipés de processeurs de service à un réseau de gestion dédié afin de protéger les processeurs de service contre les accès via le réseau.
- 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'exposition aux attaques 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 cœur de l'hyperviseur comme indiqué dans les sections [“Contre-mesure : validation des signatures des microprogrammes et des logiciels” à la page 27](#) et [“Contre-mesure : validation des modules de noyau” à la page 27](#).
- Protégez le domaine de contrôle contre les attaques par déni de service. Reportez-vous à la section [“Contre-mesure : sécurisation de l'accès à la console” à la page 28](#).
- Faites en sorte que Logical Domains Manager ne puisse pas être exécuté par des utilisateurs non autorisés. Reportez-vous à la section [“Menace : utilisation non autorisée d'utilitaires de configuration” à la page 29](#).
- Faites en sorte que le domaine de service ne soit pas accessible à des utilisateurs ou des processus non autorisés. Reportez-vous à la section [“Menace : manipulation d'un domaine de service” à la page 31](#).
- Protégez un domaine d'E/S ou un domaine de service contre les attaques par déni de service. Reportez-vous à la section [“Menace : survenance d'un déni de service d'un domaine d'E/S ou d'un domaine de service” à la page 33](#).
- 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 [“Menace : manipulation d'un domaine d'E/S” à la page 34](#).
- 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. Reportez-vous aux sections [“Contre-mesure : sécurisation de Logical Domains Manager” à la page 29](#) et [“Contre-mesure : sécurisation d'ILOM” à la page 26](#).
- **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 appartenant à la même classe de sécurité à une plate-forme matérielle donnée, vous créez une barrière d'isolement qui empêche les domaines de passer dans une autre classe de sécurité. Reportez-vous à la section

“Contre-mesure : affectation attentive de domaines invités aux plates-formes matérielles” à la page 18.

- Utilisez les droits 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 LDom 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 LDom 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 3.1](#) ”.
- Utilisez les droits pour restreindre l'accès aux consoles des *seuls* domaines que vous, en tant qu'administrateur d'Oracle VM Server for SPARC, administrez. N'autorisez *pas* l'accès général à tous les domaines. Reportez-vous à la section “ [Contrôle de l'accès à une console de domaine à l'aide de droits utilisateur](#) ” du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.
- **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 3.1](#) ”.

Sécurité dans un environnement virtualisé

Afin d'optimiser la sécurité de votre environnement Oracle VM Server for SPARC virtualisé, sécurisez le système d'exploitation et chaque service s'exécutant dans chaque domaine. Pour réduire les effets d'une violation de la sécurité, séparez les services en les déployant dans des domaines différents.

L'environnement d'Oracle VM Server for SPARC utilise un hyperviseur pour virtualiser la CPU, la mémoire et les ressources d'E/S pour les domaines logiques. Chaque domaine est un serveur virtualisé distinct que vous devez protéger contre d'éventuelles attaques.

Un environnement virtualisé vous permet de consolider plusieurs serveurs en un serveur unique par le biais du partage des ressources matérielles. Dans Oracle VM Server for SPARC, les ressources de CPU et de mémoire sont allouées de manière exclusive à chaque domaine, ce qui empêche les abus de type usage excessif de la CPU ou allocation excessive de mémoire. Les ressources de disque et les ressources réseau sont généralement fournies par les domaines de service à un grand nombre de domaines invités.

Lorsque vous évaluez la sécurité, partez *toujours* du principe que votre environnement présente une défaillance qu'une personne malveillante peut exploiter. Une personne malveillante peut par exemple tirer parti d'une faiblesse de l'hyperviseur pour pirater l'intégralité du système,

domaines invités compris. Par conséquent, vous devez *toujours* déployer les systèmes de manière à réduire les risques de dommages en cas de violation de la sécurité.

Environnement d'exécution

L'environnement d'exécution comprend les éléments suivants :

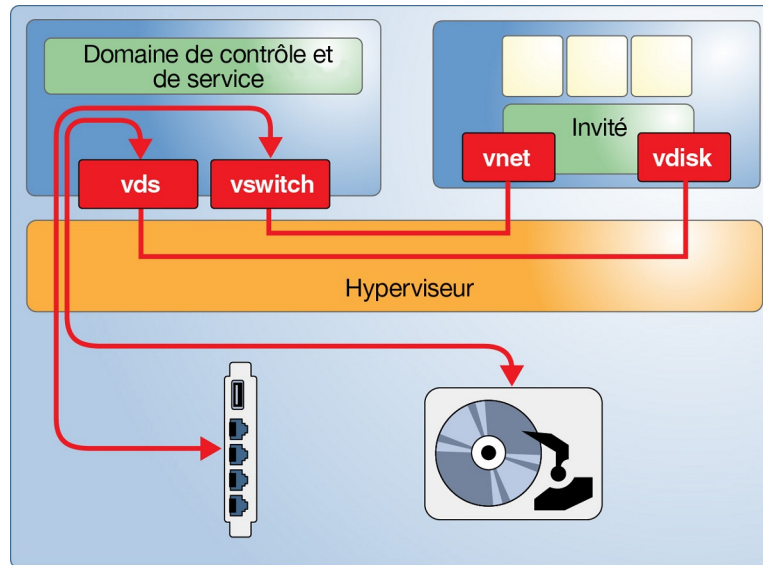
- **Hyperviseur** – Microprogramme propre à la plate-forme qui virtualise le matériel et s'appuie largement sur la prise en charge matérielle intégrée à la CPU.
- **Domaine de contrôle** – Domaine spécialisé qui configure l'hyperviseur et exécute Logical Domains Manager, lequel gère les domaines logiques.
- **Domaine d'E/S ou domaine root** – Domaine qui est propriétaire de certains ou de tous les périphériques d'E/S disponibles de la plate-forme et les partage avec d'autres domaines.
- **Domaine de service** – Domaine qui propose des services à d'autres domaines. Un domaine de service peut permettre l'accès par console à d'autres domaines ou fournir des disques virtuels. Un domaine de service qui fournit un accès à des disques virtuels à d'autres domaines est également un domaine d'E/S.

Pour plus d'informations sur ces composants, reportez-vous à la [Figure 1-1, “Hyperviseur prenant en charge deux domaines logiques”](#) et aux descriptions plus détaillées des composants.

Vous pouvez améliorer la gestion des configurations d'E/S redondantes en configurant un deuxième domaine d'E/S. Vous pouvez également utiliser un deuxième domaine d'E/S pour mettre le matériel à l'abri des violations de sécurité. Pour plus d'informations sur les options de configuration, reportez-vous au manuel “[Guide d'administration d'Oracle VM Server for SPARC 3.1](#)”.

Sécurisation de l'environnement d'exécution

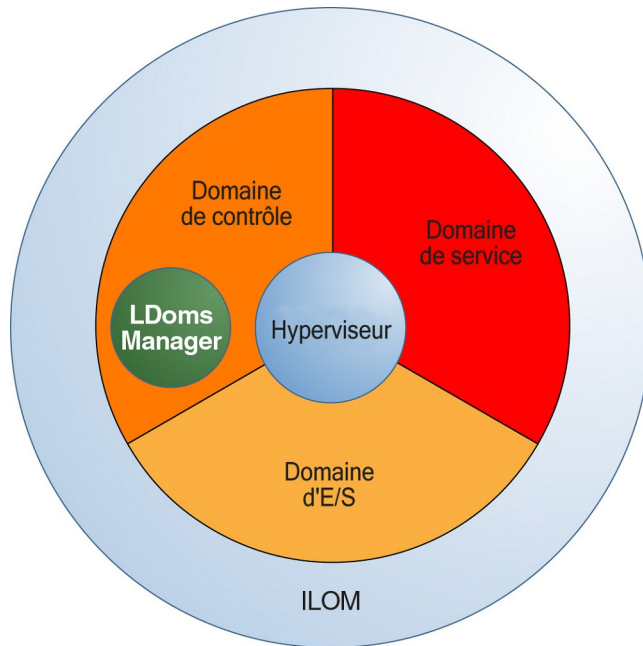
Oracle VM Server for SPARC présente plusieurs cibles d'attaques potentielles dans l'environnement d'exécution. La [Figure 1-2, “Exemple d'environnement Oracle VM Server for SPARC”](#) présente une configuration Oracle VM Server for SPARC simple où le domaine de contrôle fournit des services réseau et de disque à un domaine invité. Ces services sont implémentés au moyen de démons et de modules de noyau qui s'exécutent dans le domaine de contrôle. Logical Domains Manager attribue des canaux de domaine logique (LDC, Logical Domain Channel) pour chaque service et assigne un client pour faciliter la communication point à point entre eux. Une personne malveillante peut exploiter une erreur dans n'importe quel composant pour rompre l'isolement des domaines invités. Par exemple, cette personne peut exécuter un code quelconque dans le domaine de service ou interrompre le fonctionnement normal de la plate-forme.

FIGURE 1-2 Exemple d'environnement Oracle VM Server for SPARC

Défense contre les attaques

La figure suivante représente les composants de virtualisation qui forment l'“environnement d'exécution” Oracle VM Server for SPARC. Ces composants ne sont pas strictement séparés. La configuration la plus simple consiste à combiner toutes ces fonctions dans un domaine unique. Le domaine de contrôle peut également faire office de domaine d'E/S et domaine de service pour d'autres domaines.

FIGURE 1-3 Composants de l'environnement d'exécution



Supposons qu'une personne malveillante tente de rompre l'isolement puis de manipuler l'hyperviseur ou un autre composant de l'environnement d'exécution pour atteindre un domaine invité. Vous devez protéger chaque domaine invité de la même manière que vous le feriez pour n'importe quel serveur autonome.

La suite de ce chapitre présente les menaces possibles et les différentes mesures que vous pouvez prendre pour les contrer. Chacune de ces attaques tente de surmonter ou d'éliminer l'isolement des différents domaines qui s'exécutent sur une plate-forme unique. Les sections suivantes décrivent les menaces qui pèsent sur chaque partie d'un système Oracle VM Server for SPARC :

- “Environnement opérationnel” à la page 17
- “Environnement d'exécution” à la page 22
- “ILOM” à la page 25
- “Hyperviseur” à la page 26
- “Domaine de contrôle” à la page 28
- “Logical Domains Manager” à la page 28
- “Domaine d'E/S” à la page 33
- “Domaine de service” à la page 31
- “Domaines invités” à la page 35

Environnement opérationnel

L'environnement opérationnel comprend les systèmes physiques et leurs composants, les architectes de centre de données, les administrateurs et les membres du département informatique. Une violation de la sécurité peut se produire en n'importe quel point de l'environnement opérationnel.

La virtualisation place une couche logicielle entre le matériel proprement dit et les domaines invités qui exécutent les services de production, ce qui accroît la complexité. Par conséquent, planifiez et configurez avec soin le système virtuel et méfiez-vous des erreurs humaines. Méfiez-vous également des tentatives de personnes malveillantes d'accéder à l'environnement opérationnel par le biais de "l'ingénierie sociale".

Les sections suivantes décrivent les menaces caractéristiques que vous pouvez contrer au niveau de l'environnement opérationnel.

Menace : configuration incorrecte non intentionnelle

En matière de sécurité, la préoccupation principale pour un environnement virtualisé est d'assurer l'isolement du serveur en séparant les segments du réseau, en prévoyant un accès administratif séparé et en répartissant les serveurs dans des classes de sécurité, lesquelles correspondent à des groupes de domaines partageant les mêmes exigences et privilèges de sécurité.

Configurez attentivement les ressources virtuelles afin d'éviter les erreurs suivantes :

- Création de canaux de communication inutiles entre les domaines invités de production et l'environnement d'exécution
- Création d'accès inutiles à des segments du réseau
- Création de connexions non intentionnelles entre des classes de sécurité distinctes
- Migration non intentionnelle d'un domaine invité dans la mauvaise classe de sécurité
- Allocation insuffisante de matériel pouvant entraîner une surcharge inattendue des ressources
- Affectation de disques ou de périphériques d'E/S au mauvais domaine

Contre-mesure : création d'instructions opérationnelles

Avant de commencer, définissez soigneusement les instructions opérationnelles applicables à votre environnement Oracle VM Server for SPARC. Ces instructions décrivent les tâches à effectuer et la manière de les effectuer. Il s'agit des tâches suivantes :

- Gestion des patchs pour tous les composants de l'environnement
- Mise en place d'une procédure d'implémentation des modifications sécurisée, traçable et bien définie
- Vérification des fichiers journaux à intervalles réguliers

- Surveillance de l'intégrité et de la disponibilité de l'environnement

Effectuez régulièrement des contrôles pour vous assurer que ces instructions restent à jour et adaptées, et pour vérifier qu'elles sont suivies au jour le jour.

En plus de ces instructions, vous pouvez prendre plusieurs mesures plus techniques pour réduire le risque d'actions non intentionnelles. Reportez-vous à la section [“Logical Domains Manager” à la page 28.](#)

Menace : erreurs dans l'architecture de l'environnement virtuel

Lorsque vous déplacez un système physique vers un environnement virtualisé, vous pouvez en général conserver la configuration du stockage existante en réutilisant les LUN d'origine. Toutefois, la configuration réseau doit être ajustée par rapport à l'environnement virtualisé et l'architecture résultante peut différer considérablement de l'architecture utilisée sur le système physique.

Vous devez vous poser la question de savoir comment préserver l'isolement des classes de sécurité distinctes et connaître leurs besoins. Vous devez également prendre en compte le matériel partagé de la plate-forme et les composants partagés tels que les commutateurs réseau et SAN.

Pour optimiser la sécurité de votre environnement, assurez-vous de préserver l'isolement des domaines invités et des classes de sécurité. Lors de la conception de l'architecture, anticipez les erreurs possibles et les attaques et mettez en oeuvre des moyens de défense. Une bonne conception permet de limiter les éventuels problèmes de sécurité tout en permettant la gestion de la complexité et des coûts.

Contre-mesure : affectation attentive de domaines invités aux plates-formes matérielles

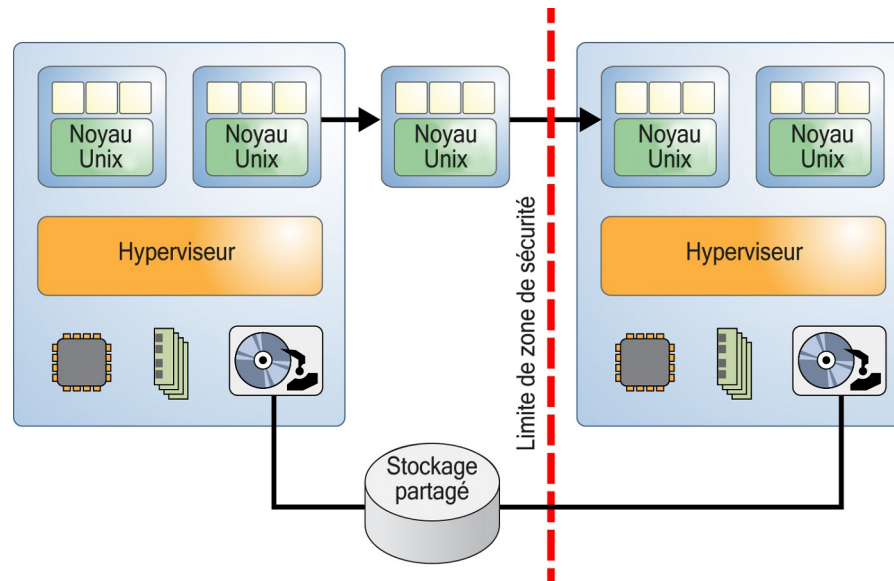
Utilisez des classes de sécurité, c'est-à-dire des groupes de domaines partageant les mêmes exigences et privilèges de sécurité, pour isoler les domaines les uns des autres. En affectant à une plate-forme matérielle donnée des domaines invités appartenant à la même classe de sécurité, vous empêchez qu'une éventuelle violation de l'isolement ne se propage à une autre classe de sécurité.

Contre-mesure : planification d'une migration de domaine Oracle VM Server for SPARC

La fonction de migration de domaine en direct peut rompre l'isolement si un domaine invité est migré par inadvertance vers une plate-forme assignée à une autre classe de sécurité, comme

illustré dans la figure suivante. Planifiez donc avec soin la migration des domaines invités afin de vous assurer qu'aucune migration entre classes de sécurité différentes n'est autorisée.

FIGURE 1-4 Migration de domaine d'une classe de sécurité à une autre



Contre-mesure : configuration correcte des connexions virtuelles

Si vous n'assurez pas le suivi de toutes les connexions réseau virtuelles, il est possible qu'un domaine puisse accéder de manière indue à un segment du réseau. Un tel accès peut par exemple contourner le pare-feu ou une classe de sécurité.

Pour réduire les risques d'erreurs d'implémentation, planifiez et documentez soigneusement toutes les connexions virtuelles et physiques de votre environnement. Optimisez le plan de connexion des domaines pour plus de simplicité et de facilité de gestion. Documentez précisément votre plan et vérifiez l'exactitude de votre implémentation par rapport à votre plan avant le passage en production. Même une fois votre environnement virtuel en production, vérifiez régulièrement l'implémentation par rapport au plan.

Contre-mesure : utilisation du balisage VLAN

Vous pouvez utiliser le balisage VLAN pour consolider plusieurs segments Ethernet sur un même réseau physique. Cette fonctionnalité est également disponible pour les commutateurs

virtuels. Pour limiter les risques liés à des erreurs logicielles dans l'implémentation des commutateurs virtuels, configurez un commutateur virtuel par carte NIC physique et réseau VLAN. De plus, pour vous protéger contre des erreurs dans le pilote Ethernet, évitez d'utiliser des VLAN balisés. Toutefois, la probabilité que de telles erreurs se produisent est faible car la vulnérabilité des VLAN balisés est bien connue. Des tests d'intrusion sur la plate-forme Sun SPARC T-Series d'Oracle avec le logiciel Oracle VM Server for SPARC n'ont pas mis en évidence cette vulnérabilité.

Contre-mesure : utilisation des dispositifs de sécurité virtuels

Les dispositifs de sécurité tels que les filtres de paquets et les pare-feux sont des instruments d'isolement et protègent l'isolement des classes de sécurité. Ces dispositifs sont soumis aux mêmes menaces que tout autre domaine invité, c'est pourquoi leur utilisation ne garantit pas une protection complète contre une violation d'isolement. Par conséquent, évaluez avec soin tous les aspects des risques et de la sécurité avant de prendre la décision de virtualiser un tel service.

Menace : effets secondaires du partage des ressources

Le partage des ressources dans un environnement virtualisé peut conduire à des attaques par déni de service (DoS, denial-of-service), qui surchargent une ressource jusqu'à ce qu'un autre composant tel qu'un autre domaine soit affecté.

Dans un environnement Oracle VM Server for SPARC, seules certaines ressources sont susceptibles d'être affectées par une attaque par déni de service. Les ressources de CPU et de mémoire sont assignées de manière exclusive à chaque domaine invité, ce qui empêche la plupart des attaques par déni de service. Mais même l'assignation exclusive de ces ressources peut ralentir un domaine invité de l'une des manières suivantes :

- Emballement des zones de cache partagées par les strands et assignées à deux domaines invités
- Surcharge de la bande passante de la mémoire

Contrairement aux ressources de CPU et de mémoire, les services de disque et les services réseau sont généralement partagés par les domaines invités. Ces services sont fournis aux domaines invités par un ou plusieurs domaines de service. Étudiez avec soin comment assigner et répartir ces ressources entre les domaines invités. Notez que toute configuration permettant à la fois des performances maximales et une exploitation optimale des ressources réduit les risques d'effets secondaires.

Evaluation : effets secondaires liés aux ressources partagées

Qu'il soit assigné à un domaine de manière exclusive ou partagé par plusieurs domaines, un lien réseau peut être saturé ou un disque peut être surchargé. De telles attaques affectent la disponibilité d'un service pendant toute la durée de l'attaque. Leur cible n'est pas compromise

et aucune donnée n'est perdue. Vous pouvez facilement réduire les effets de cette menace, mais vous devez la garder à l'esprit, même si elle se limite aux ressources réseau et de disque dans Oracle VM Server for SPARC.

Contre-mesure : affectation attentive des ressources matérielles

Assurez-vous que vous affectez uniquement les ressources matérielles requises aux domaines invités. Veillez à annuler l'affectation d'une ressource inutilisée lorsque celle-ci n'est plus nécessaire ; c'est le cas par exemple d'un port réseau ou d'une unité de DVD requis uniquement lors d'une installation. En appliquant cette pratique, vous réduisez le nombre de points d'entrée possibles pour une personne malveillante.

Contre-mesure : affectation attentive des ressources partagées

Les ressources matérielles partagées, telles que les ports réseau physiques, constituent une cible potentielle pour des attaques par déni de service. Pour limiter l'impact d'attaques par déni de service à un seul groupe de domaines invités, déterminez avec soin quels domaines invités partagent quelles ressources matérielles.

Par exemple, vous pouvez regrouper des domaines invités partageant des ressources matérielles en fonction de leur disponibilité ou de leurs exigences en matière de sécurité. Outre le regroupement, vous pouvez appliquer différents types de contrôles des ressources.

Vous devez vous poser la question de savoir comment partager les ressources de disque et les ressources réseau. Vous pouvez limiter les problèmes en séparant l'accès au disque au moyen de chemins d'accès physiques dédiés ou de services de disque virtuel dédiés.

Résumé : effets secondaires liés aux ressources partagées

Toutes les contre-mesures décrites dans cette section exigent que vous maîtrisiez les aspects techniques de votre déploiement et leurs implications en matière de sécurité. Veillez à planifier avec soin, à bien documenter et mettez en place l'architecture la plus simple possible. Assurez-vous de connaître les implications du matériel virtualisé afin de pouvoir vous préparer à déployer le logiciel Oracle VM Server for SPARC en toute sécurité.

Les domaines logiques font preuve de robustesse face aux effets du partage de CPU et de mémoire, car le partage qui se produit effectivement est très limité. Néanmoins, il est préférable d'appliquer des contrôles de ressources tels que la gestion des ressources Solaris dans les domaines invités. L'utilisation de ces contrôles vous protège contre les défauts de comportement des applications, que vous travailliez dans un environnement virtualisé ou non virtualisé.

Environnement d'exécution

La [Figure 1-3, “Composants de l'environnement d'exécution”](#) présente les composants de l'environnement d'exécution. Chaque composant fournit des services donnés qui, ensemble, constituent la plate-forme globale sur laquelle les domaines invités de production peuvent s'exécuter. Une configuration correcte des composants est primordiale pour garantir l'intégrité du système.

Tous les composants de l'environnement d'exécution sont des cibles potentielles pour une personne malveillante. Cette section décrit les menaces qui pèsent sur chaque composant dans l'environnement d'exécution. Certaines menaces et contre-mesures peuvent s'appliquer à plusieurs composants.

Menace : manipulation de l'environnement d'exécution

En manipulant l'environnement d'exécution, il est possible de prendre le contrôle de plusieurs façons. Par exemple, il est possible d'installer des microprogrammes manipulés dans ILOM pour intercepter toutes les entrées/sorties d'un domaine invité à partir d'un domaine d'E/S. Ce type d'attaque peut permettre d'accéder à la configuration du système et de la modifier. Une personne malveillante qui prend le contrôle du domaine de contrôle d'Oracle VM Server for SPARC peut reconfigurer le système comme elle l'entend, et une personne malveillante qui prend le contrôle d'un domaine d'E/S peut apporter des modifications aux dispositifs de stockage connectés, tels que des disques d'initialisation par exemple.

Evaluation : manipulation de l'environnement d'exécution

Une personne malveillante qui parvient à entrer dans ILOM ou dans n'importe quel domaine de l'environnement d'exécution peut lire et manipuler toutes les données mises à la disposition de ce domaine. Un accès de ce type peut s'effectuer par l'intermédiaire du réseau ou par le biais d'une erreur dans la pile de virtualisation. Ce type d'attaque est difficile à mettre en oeuvre car en général, ILOM et les domaines ne peuvent pas être attaqués directement.

La mise en oeuvre de contre-mesures pour éviter une manipulation de l'environnement d'exécution est une pratique de sécurité courante et doit être implémentée sur n'importe quel système. Les pratiques de sécurité courantes constituent une barrière protectrice supplémentaire pour l'environnement d'exécution et réduisent un peu plus les risques d'intrusion et de manipulation.

Contre-mesure : sécurisation des chemins d'accès interactifs

Assurez-vous de ne créer que les comptes *absolument nécessaires* pour les applications qui s'exécutent sur le système.

Assurez-vous que les comptes requis pour l'administration sont sécurisés en recourant à l'authentification basée sur une clé ou à des mots de passe forts. Ces clés ou mots de passe ne doivent pas être partagés par différents domaines. Envisagez également d'implémenter une authentification à deux facteurs ou une "règle des deux personnes" pour l'exécution de certaines actions.

N'utilisez *pas* des connexions anonymes pour les comptes tels que root, afin que toutes les commandes exécutées sur le système puissent être tracées et attribuées à un utilisateur donné. Utilisez plutôt des droits pour accorder à des administrateurs donnés l'accès aux *seules* fonctions qu'ils sont autorisés à effectuer. Assurez-vous que l'accès au réseau d'administration utilise toujours un protocole de chiffrement tel que SSH et que les stations de travail des administrateurs sont traitées comme des systèmes à haute sécurité.

Contre-mesure : réduction du SE Oracle Solaris

L'intégrité de n'importe quel logiciel installé sur un système étant susceptible d'être compromise, vous devez veiller à n'installer que les logiciels *indispensables* pour minimiser les failles de sécurité.

Contre-mesure : sécurisation du SE Oracle Solaris

En plus d'effectuer une installation minimale du SE Oracle Solaris, configurez les packages logiciels de manière à "sécuriser" le logiciel contre les attaques. Exécutez tout d'abord des services réseau limités afin de désactiver tous les services réseau à l'exception de SSH. Cette stratégie est le comportement par défaut sur les systèmes Oracle Solaris 11. Pour plus d'informations sur la sécurisation du SE Oracle Solaris, reportez-vous à la [page de sécurité Solaris \(http://www.oracle.com/us/products/servers-storage/solaris/security/index.html\)](http://www.oracle.com/us/products/servers-storage/solaris/security/index.html).

Contre-mesure : recours à la séparation des rôles et à l'isolement des applications

Les applications de production sont nécessairement connectées à d'autres systèmes et sont, par conséquent, plus exposées aux attaques extérieures. Ne déployez *pas* les applications de production sur un domaine qui fait partie de l'environnement d'exécution. Au contraire, déployez-les *uniquement* sur des domaines invités dépourvus de privilèges particuliers.

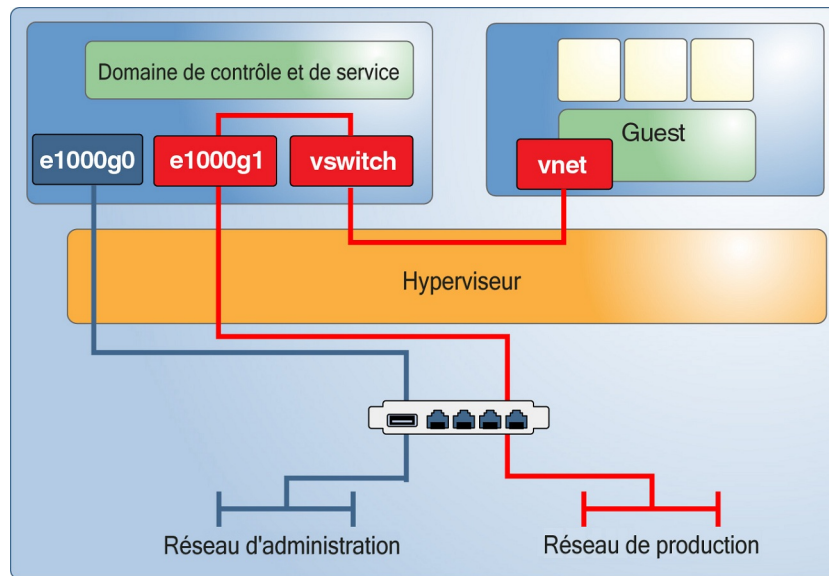
L'environnement d'exécution doit uniquement fournir l'infrastructure nécessaire pour ces domaines invités. En séparant l'environnement d'exécution des applications de production, vous pouvez introduire un certain niveau de précision dans les privilèges d'administration. Un administrateur de domaine invité de production n'a pas besoin d'accéder à l'environnement d'exécution et un administrateur d'environnement d'exécution n'a pas besoin d'accéder aux domaines invités de production. Si possible, affectez les différents rôles de l'environnement d'exécution, tels que le domaine de contrôle et le domaine d'E/S, à des domaines différents. Une configuration de ce type permet de limiter les dommages si l'un des domaines est compromis.

Vous pouvez également étendre la séparation des rôles à l'environnement réseau utilisé pour la connexion des différents serveurs.

Contre-mesure : configuration d'un réseau de gestion dédié

Connectez tous les serveurs équipés de processeurs de service à un réseau de gestion dédié. Cette configuration est également recommandée pour les domaines de l'environnement d'exécution. S'ils sont connectés en réseau, hébergez ces domaines sur leur propre réseau dédié. Ne connectez *pas* directement les domaines de l'environnement d'exécution aux réseaux qui sont affectés aux domaines de production. Bien que vous ayez la possibilité d'effectuer toutes les tâches d'administration en vous connectant à la console unique mise à disposition par le processeur de service d'ILOM, cette configuration rend l'administration suffisamment fastidieuse pour la rendre impraticable. En séparant les réseaux de production et d'administration, vous vous protégez contre les écoutes électroniques et les manipulations. Ce type de séparation élimine également le risque d'une attaque dirigée contre l'environnement d'exécution et menée depuis les domaines invités via le réseau partagé.

FIGURE 1-5 Réseau de gestion dédié



ILOM

Tous les systèmes Oracle SPARC actuels incluent un contrôleur système intégré (ILOM) qui assure les fonctions suivantes :

- Gère les contrôles environnementaux de base tels que la vitesse du ventilateur et l'alimentation du châssis
- Permet les mises à niveau du microprogramme
- Fournit la console système pour le domaine de contrôle

Vous pouvez accéder à ILOM via une connexion série ou utiliser SSH, HTTP, HTTPS, SNMP, ou IPMI pour y accéder par l'intermédiaire d'un port réseau. Les systèmes Fujitsu M10 utilisent XSCF à la place d'ILOM pour assurer des fonctions similaires.

Menace : déni de service du système complet

Une personne malveillante qui parvient à prendre le contrôle d'ILOM peut compromettre le système de multiples façons. Il peut notamment :

- Mettre hors tension tous les invités en cours d'exécution
- Installer un microprogramme manipulé pour accéder à un domaine invité au moins

Ces scénarios concernent tous les systèmes qui disposent de ce type de contrôleur. Dans un environnement virtualisé, les dommages peuvent être beaucoup plus importants que dans un environnement physique car de nombreux domaines qui sont hébergés dans le même boîtier système sont menacés.

De même, une personne malveillante qui parvient à prendre le contrôle du domaine de contrôle ou d'un domaine d'E/S peut aisément désactiver tous les domaines invités dépendants en arrêtant les services d'E/S correspondants.

Evaluation : déni de service du système complet

Alors qu'ILOM est généralement connecté à un réseau administratif, il est également possible d'accéder à ILOM depuis le domaine de contrôle en utilisant l'IPMI avec le module d'accès du BMC. Par conséquent, ces deux types de connexions doivent être bien protégés et isolés des réseaux de production normaux.

De même, une personne malveillante peut violer la sécurité d'un domaine de service à partir du réseau ou par le biais d'une erreur dans la pile de virtualisation, puis bloquer les E/S invitées ou arrêter le système. Bien que les dommages soient limités car les données ne sont ni perdues, ni compromises, ils peuvent affecter un grand nombre de domaines invités. Veillez donc à vous protéger contre cette menace possible pour limiter les dommages potentiels.

Contre-mesure : sécurisation d'ILOM

En tant que processeur de service, ILOM contrôle des fonctions essentielles telles que l'alimentation du châssis, les configurations de démarrage d'Oracle VM Server for SPARC et l'accès par console au domaine de contrôle. Les mesures suivantes vous permettent de sécuriser ILOM :

- Placement du port réseau d'ILOM dans un segment de réseau distinct du réseau administratif, qui est utilisé pour les domaines dans l'environnement d'exécution.
- Désactivation de tous les services qui ne sont pas requis pour le fonctionnement normal, tels que HTTP, IPMI, SNMP, HTTPS et SSH.
- Configuration de comptes administrateur dédiés et personnels qui accordent uniquement les droits requis. Pour permettre une traçabilité maximale des actions effectuées par les administrateurs, assurez-vous de créer des comptes administrateur personnels. Ce type d'accès est particulièrement important pour l'accès à la console, les mises à niveau de microprogrammes et la gestion des configurations de démarrage.

Hyperviseur

L'hyperviseur est la couche du microprogramme qui implémente et contrôle la virtualisation du matériel réel. L'hyperviseur est formé des composants suivants :

- L'hyperviseur réel, qui est implémenté dans le microprogramme et pris en charge par les CPU des systèmes.
- Des modules de noyau qui s'exécutent dans le domaine de contrôle pour configurer l'hyperviseur.
- Des modules de noyau et des démons qui s'exécutent dans les domaines d'E/S et les domaines de service pour fournir des E/S virtualisées, ainsi que des modules de noyau qui communiquent par le biais de canaux de domaines logiques (LDC, Logical Domain Channels).
- Des modules de noyau et des pilotes de périphériques qui s'exécutent dans les domaines invités pour accéder aux périphériques d'E/S virtualisées ainsi que les modules de noyau qui communiquent par le biais de canaux de domaines logiques (LDC).

Menace : rupture de l'isolement

Une personne malveillante peut détourner des domaines invités ou l'ensemble du système en s'introduisant dans l'environnement d'exécution isolé fourni par l'hyperviseur. C'est la menace qui peut entraîner les plus graves dommages sur un système.

Evaluation : rupture de l'isolement

Une conception de système modulaire peut améliorer l'isolement en accordant différents niveaux de privilèges aux domaines invités, à l'hyperviseur et au domaine de contrôle. Chaque module fonctionnel est implémenté dans un module de noyau, un pilote de périphérique ou un démon distinct et configurable. Cette modularité requiert des API nettes et des protocoles de communication simples qui réduisent le risque global d'erreurs.

Même si l'exploitation d'une erreur semble peu probable, l'une des conséquences possibles est la prise de contrôle totale de l'ensemble du système par la personne malveillante.

Contre-mesure : validation des signatures des microprogrammes et des logiciels

Même si vous pouvez télécharger les patches des microprogrammes système et du SE directement à partir d'un site Web d'Oracle, ces patches peuvent avoir été manipulés. Avant d'installer le logiciel, vérifiez les sommes de contrôle MD5 des packages logiciels. Oracle publie les sommes de contrôle de tous les logiciels téléchargeables.

Contre-mesure : validation des modules de noyau

Oracle VM Server for SPARC utilise plusieurs pilotes et modules de noyau pour implémenter le système de virtualisation global. Tous les modules de noyau et la plupart des fichiers binaires distribués avec le SE Oracle Solaris portent une signature numérique. Servez-vous de l'utilitaire `elfsign` pour vérifier la signature numérique de chaque pilote et module de noyau. Vous pouvez utiliser la commande `pkg verify` d'Oracle Solaris 11 pour vérifier l'intégrité d'un fichier binaire Oracle Solaris. Consultez la page Web https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it.

Vous devez commencer par établir l'intégrité de l'utilitaire `elfsign`. Utilisez l'outil de génération de rapports et d'audit de base (BART) pour automatiser le processus de vérification des signatures numériques. Le document [Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System](http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf) (<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf>) indique comment associer BART et la base de données d'empreintes Solaris pour effectuer automatiquement des vérifications d'intégrité similaires. Bien que la base de données d'empreintes ait été abandonnée, les concepts décrits dans ce document peuvent être repris et peuvent servir à utiliser de façon analogue `elfsign` et BART.

Domaine de contrôle

Le domaine de contrôle, qui joue souvent les rôles de domaine d'E/S et de domaine de service, doit être protégé car il peut modifier la configuration de l'hyperviseur, lequel contrôle toutes les ressources matérielles connectées.

Menace : déni de service du domaine de contrôle

L'arrêt du domaine de contrôle peut entraîner un déni de service des outils de configuration. Le domaine de contrôle n'étant indispensable que pour les modifications de configuration, les domaines invités peuvent indifféremment accéder à leurs ressources réseau et leurs ressources de disque par le biais d'autres domaines de service.

Evaluation : déni de service du domaine de contrôle

Attaquer le domaine de contrôle via le réseau équivaut à attaquer n'importe quelle autre instance du SE Oracle Solaris correctement protégée. Les dommages causés par un arrêt ou un déni de service du domaine de contrôle sont relativement faibles. Toutefois, des domaines invités peuvent être affectés si le domaine de contrôle joue également pour eux le rôle de domaine de service.

Contre-mesure : sécurisation de l'accès à la console

Évitez de configurer un accès réseau administratif aux domaines de l'environnement d'exécution. Ce scénario exige d'utiliser le service de console ILOM sur le domaine de contrôle pour effectuer toutes les tâches d'administration. L'accès par console à tous les autres domaines est toujours possible par le biais du service `vntsd` s'exécutant sur le domaine de contrôle.

Réfléchissez bien avant d'implémenter cette solution. Bien qu'elle réduise le risque d'attaques via le réseau administratif, cette solution signifie qu'un seul administrateur peut accéder à la console à la fois.

Pour plus d'informations sur la configuration sécurisée de `vntsd`, reportez-vous à la section [“ Procédure d'activation du démon du serveur de terminal du réseau virtuel ” du manuel “ Guide d'administration d'Oracle VM Server for SPARC 3.1 ”](#).

Logical Domains Manager

Logical Domains Manager s'exécute dans le domaine de contrôle et sert à configurer l'hyperviseur, ainsi qu'à créer et à configurer tous les domaines et les ressources matérielles associées. Assurez-vous que l'utilisation de Logical Domains Manager est consignée et surveillée.

Menace : utilisation non autorisée d'utilitaires de configuration

Une personne malveillante peut prendre le contrôle de l'ID utilisateur d'un administrateur ou un administrateur d'un autre groupe peut accéder de manière illicite à un autre système.

Evaluation : utilisation non autorisée d'utilitaires de configuration

Assurez-vous qu'un administrateur ne dispose pas d'un accès à un système dont il n'a pas besoin en implémentant une gestion des identités efficace. Implémentez également un contrôle d'accès strict et détaillé ainsi que d'autres mesures telles que la règle des deux personnes.

Contre-mesure : application de la règle des deux personnes

Envisagez d'implémenter une règle des deux personnes pour Logical Domains Manager et d'autres outils d'administration par le biais de droits. Reportez-vous au document [Enforcing the Two-Person Rule Via Role-Based Access Control in the Oracle Solaris 10 Operating System](http://www.oracle.com/technetwork/articles/systems-hardware-architecture/twoperson-rule-solaris-277014.pdf) (<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/twoperson-rule-solaris-277014.pdf>). Cette règle protège votre système contre les attaques d'ingénierie sociale, les comptes d'administration non fiables et les erreurs humaines.

Contre-mesure : utilisation de droits pour Logical Domains Manager

En utilisant des droits pour la commande `ldm`, vous pouvez implémenter un contrôle d'accès détaillé et une traçabilité complète. Pour plus d'informations sur la configuration des droits, reportez-vous au manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”. L'utilisation de droits permet de protéger votre système des erreurs humaines car les fonctions de la commande `ldm` ne sont pas toutes accessibles à tous les administrateurs.

Contre-mesure : sécurisation de Logical Domains Manager

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. La désactivation des services réseau réduit la surface d'exposition aux attaques de Logical Domains Manager au minimum requis pour un fonctionnement normal. Ce scénario permet de lutter contre les attaques par déni de service et les autres tentatives d'utilisation abusive de ces services réseau.

Remarque - Bien que la désactivation des services du gestionnaire de domaines permette de réduire la surface d'exposition aux attaques, il n'est pas possible de prévoir les effets secondaires d'une telle désactivation pour une configuration donnée.

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\(1M\)](#).
- **Prise en charge XMPP (Extensible Messaging and Presence Protocol) sur le port TCP 6482**
Pour plus d'informations sur la désactivation de ce service, reportez-vous à la section “ [Transport XML](#) ” du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.

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`. La désactivation de XMPP empêche également Oracle VM Manager ou Ops Center de gérer le système.
- **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 3.1](#) ” et à la section “ [Gestion de la sécurité](#) ” du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.
 - **Désactivez le service SNMP.** Pour plus d'informations sur la désactivation de 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 3.1](#) ”.
- **Service de découverte sur l'adresse de multidiffusion 239.129.9.27 et le port 64535**

Remarque - Notez que ce mécanisme de détection est également utilisé par le démon `ldmd` pour détecter les collisions lors de l'affectation automatique d'adresses MAC. Si vous désactivez le service de repérage, la détection de collision d'adresses MAC ne fonctionnera pas et par conséquent, l'allocation d'adresses MAC ne fonctionnera pas correctement non plus.

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'exposition aux attaques 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 à la section “[Contre-mesure : sécurisation d'ILOM](#)” à la page 26.

Contre-mesure : audit de Logical Domains Manager

Protéger Logical Domains Manager est primordial pour assurer la sécurité de l'ensemble du système. Toutes les modifications apportées à la configuration d'Oracle VM Server for SPARC doivent être consignées afin de permettre le traçage des actions hostiles. Analysez régulièrement les journaux d'audit et copiez-les sur un système distinct pour un archivage sécurisé. Pour plus d'informations, reportez-vous au [Chapitre 3, “ Sécurité d'Oracle VM Server for SPARC ”](#) du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.

Domaine de service

Un domaine de service fournit des services virtuels aux domaines invités sur le système. Les services peuvent inclure un service de commutateur virtuel, de disque virtuel ou de console virtuelle.

La [Figure 1-6, “Exemple de domaine de service”](#) présente un exemple de domaine de service qui propose des services de console. Le domaine de contrôle héberge fréquemment les services de console, ce qui en fait également un domaine de service. Les domaines de l'environnement d'exécution associent souvent des fonctions de domaine de contrôle, de domaine d'E/S et de domaine de service dans un ou deux domaines.

Menace : manipulation d'un domaine de service

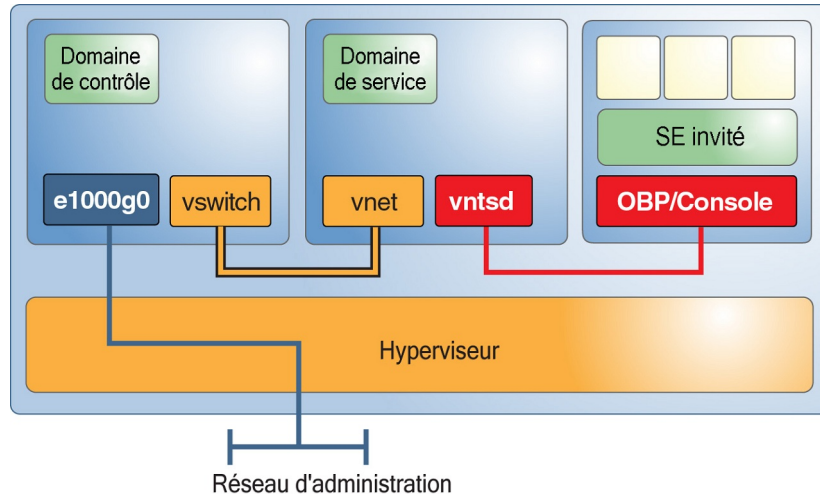
Une personne malveillante qui prend le contrôle d'un domaine de service peut manipuler des données ou écouter toutes les communications qui s'effectuent via les services offerts. Ce contrôle peut comprendre l'accès de la console aux domaines invités, l'accès aux services réseau ou l'accès aux services de disque.

Evaluation : manipulation d'un domaine de service

Bien que les stratégies d'attaque soient les mêmes que pour une attaque dirigée contre un domaine de contrôle, les dommages potentiels sont moindres car la personne malveillante ne peut pas modifier la configuration système. Les dommages possibles sont par exemple le vol ou la manipulation de données offertes par le domaine de service, mais pas la manipulation de

sources de données. Selon le service concerné, une personne malveillante peut être contrainte d'échanger des modules de noyau.

FIGURE 1-6 Exemple de domaine de service



Contre-mesure : séparation des domaines de service de manière granulaire

Dans la mesure du possible, chaque domaine de service ne doit proposer qu'un *seul* service à ses clients. Une telle configuration permet de garantir qu'un seul service est compromis si un domaine de service subit une attaque. Tenez compte toutefois de la complexité accrue du système avant d'opter pour une configuration de ce type. Notez que la présence de domaines d'E/S redondants est fortement recommandée.

Contre-mesure : isolation des domaines de service et des domaines invités

Vous pouvez isoler aussi bien les domaines de service Oracle Solaris 10 que les domaines de service Oracle Solaris 11 des domaines invités. Les solutions suivantes sont présentées dans l'ordre d'implémentation à privilégier :

- Faites en sorte que le domaine de service et le domaine invité ne partagent pas le même port réseau. En outre, ne raccordez pas d'interface de commutateur virtuel à un domaine de service. Pour les domaines de service Oracle Solaris 11, ne raccordez pas de carte VNIC aux ports physiques utilisés pour les commutateurs virtuels.

- Si vous devez utiliser le même port réseau pour les SE Oracle Solaris 10 et Oracle Solaris 11, placez le trafic du domaine d'E/S dans un réseau VLAN qui n'est pas utilisé par des domaines invités.
- Si vous ne pouvez implémenter aucune des solutions précédentes, ne raccordez pas le commutateur virtuel dans le SE Oracle Solaris 10 et appliquez des filtres IP dans le SE Oracle Solaris 11.

Contre-mesure : limitation de l'accès aux consoles virtuelles

Assurez-vous que l'accès aux différentes consoles virtuelles est limité aux *seuls* utilisateurs qui doivent y accéder. Cette configuration garantit qu'aucun administrateur n'a accès à toutes les consoles, ce qui empêche l'accès aux consoles autres que celles assignées à un compte compromis. Reportez-vous à la section “ [Procédure de création des services par défaut](#) ” du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.

Domaine d'E/S

Tout domaine qui a directement accès à un périphérique d'E/S physique tel que des ports ou des disques réseau est un domaine d'E/S. Pour plus d'informations sur la configuration des domaines d'E/S, reportez-vous au [Chapitre 6, “ Configuration des domaines d'E/S ”](#) du manuel “ [Guide d'administration d'Oracle VM Server for SPARC 3.1](#) ”.

Un domaine d'E/S peut également être un domaine de service s'il offre des services d'E/S à des domaines invités, ce qui permet à ces derniers d'accéder au matériel.

Menace : survenance d'un déni de service d'un domaine d'E/S ou d'un domaine de service

Une personne malveillante qui bloque les services d'E/S d'un domaine d'E/S bloque par la même occasion l'ensemble des domaines invités dépendants. Il est possible de lancer une attaque par déni de service réussie en surchargeant l'infrastructure du réseau ou du disque ou en introduisant une erreur dans le domaine. Chacune de ces attaques peut provoquer un blocage ou une erreur grave du domaine. De même, une personne malveillante qui suspend les services d'un domaine de service provoque le blocage immédiat de tout domaine invité qui dépend de ces services. Si le domaine invité se bloque, il se remet à fonctionner lorsque le service d'E/S reprend.

Evaluation : survenance d'un déni de service d'un domaine d'E/S ou d'un domaine de service

Les attaques par déni de service sont fréquemment effectuées par le biais du réseau. Ce type d'attaque peut réussir car les ports réseau sont ouverts à la communication et peuvent être

submergés par le trafic réseau. La perte de service qui en résulte bloque les domaines invités dépendants. Une attaque similaire peut être dirigée contre les ressources de disque par le biais de l'infrastructure SAN ou en attaquant le domaine d'E/S. Le seul dommage qui en résulte est un arrêt temporaire de tous les domaines invités dépendants. Bien que l'impact d'un déni de service sur les tâches puisse être conséquent, les données ne sont ni compromises, ni perdues, et la configuration du système reste intacte.

Contre-mesure : configuration des domaines d'E/S de manière granulaire

La configuration de plusieurs domaines d'E/S permet de réduire l'impact d'une défaillance ou d'une perte de fiabilité d'un domaine. Vous pouvez affecter des emplacements PCIe individuels à un domaine invité pour lui accorder des capacités de domaine d'E/S. Si le domaine root propriétaire du bus PCIe tombe en panne, ce bus est réinitialisé, ce qui entraîne l'arrêt brutal du domaine auquel l'emplacement individuel a été affecté. Cette fonctionnalité n'élimine pas complètement la nécessité de disposer de deux domaines root possédant chacun un bus PCIe distinct.

Contre-mesure : configuration d'un matériel et de domaines root redondants

La haute disponibilité participe également à l'amélioration de la sécurité car elle permet aux services de résister aux attaques par déni de service. Oracle VM Server for SPARC implémente des méthodologies de haute disponibilité telles que l'utilisation de disques et de ressources réseau redondants dans des domaines d'E/S redondants. Cette option de configuration permet des mises à niveau progressives des domaines d'E/S et protège contre l'impact d'une défaillance d'un domaine d'E/S due à une attaque par déni de service. Depuis l'apparition de SR-IOV, les domaines invités sont en mesure d'accéder directement à des périphériques d'E/S individuels. Cependant, si SR-IOV ne peut pas être implémenté, envisagez de créer des domaines d'E/S redondants. Reportez-vous à la section [“Contre-mesure : séparation des domaines de service de manière granulaire”](#) à la page 32.

Menace : manipulation d'un domaine d'E/S

Un domaine d'E/S a directement accès à des périphériques back-end, généralement des disques, qu'il virtualise puis propose aux domaines invités. Après une attaque réussie, une personne malveillante dispose d'un accès total à ces périphériques et peut lire des données sensibles ou manipuler des logiciels sur les disques d'initialisation des domaines invités.

Evaluation : manipulation dans un domaine d'E/S

Une attaque dirigée contre un domaine d'E/S est aussi probable qu'une attaque réussie sur un domaine de service ou le domaine de contrôle. Le domaine d'E/S est une cible particulièrement

prise car il offre potentiellement un accès à un grand nombre de périphériques de disque. Tenez donc compte de cette menace lorsque vous travaillez avec des données sensibles dans un domaine invité s'exécutant sur des disques virtualisés.

Contre-mesure : protection des disques virtuels

Lorsqu'un domaine d'E/S est compromis, la personne malveillante dispose d'un accès total aux disques virtuels du domaine invité.

Protégez le contenu des disques virtuels en effectuant les opérations suivantes :

- **Chiffrement du contenu des disques virtuels.** Sur les systèmes Oracle Solaris 10, vous pouvez utiliser une application capable de chiffrer ses propres données, telle que les tablespaces chiffrés pgp/gpg ou Oracle 11g. Sur les systèmes Oracle Solaris 11, vous pouvez utiliser des ensembles de données chiffrés ZFS pour assurer un chiffrement transparent de toutes les données stockées dans le système de fichiers.
- **Répartition des données sur plusieurs disques virtuels dans plusieurs domaines d'E/S.** Un domaine invité peut créer un volume entrelacé (RAID 1/RAID 5) qui s'étend sur plusieurs disques virtuels obtenus à partir de deux domaines d'E/S. Si l'un de ces domaines d'E/S est compromis, la personne malveillante auteur de l'attaque ne pourra que difficilement utiliser la portion de données disponible.

Domaines invités

Les domaines invités ne font pas partie de l'environnement d'exécution, mais ils sont la cible d'attaque la plus probable car ils sont connectés au réseau. Une personne malveillante qui pénètre dans un système virtualisé peut lancer des attaques contre l'environnement d'exécution.

Contre-mesure : sécurisation du SE du domaine invité

Le système d'exploitation sur le domaine invité est souvent la première ligne de défense contre toute attaque. Sauf s'il s'agit d'une attaque provenant de l'intérieur du centre de données, une personne malveillante doit s'introduire dans un domaine invité qui a des connexions externes avant de tenter de rompre l'isolement du domaine invité et de capturer l'intégralité de l'environnement. Par conséquent, vous devez sécuriser le SE du domaine invité.

Pour sécuriser davantage le SE, vous pouvez déployer votre application dans des zones Solaris Zone, qui isolent un peu plus le service réseau de l'application du système d'exploitation du domaine invité. Une attaque réussie sur le service compromet uniquement la zone concernée, et non le système d'exploitation sous-jacent, ce qui permet d'éviter que la personne malveillante n'étende son contrôle au-delà des ressources affectées à la zone. Il est ainsi plus difficile à la personne malveillante de rompre l'isolement de l'invité. Pour obtenir plus d'informations sur la sécurisation du SE invité, reportez-vous à la [Solaris Page de sécurité \(http://www.oracle.com/us/products/servers-storage/solaris/security/index.html\)](http://www.oracle.com/us/products/servers-storage/solaris/security/index.html).

Installation et configuration sécurisées d'Oracle VM Server for SPARC

Ce chapitre décrit les considérations relatives à la sécurité liées à l'installation et à la configuration du logiciel 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 fonctionnalités de droits, d'audit et d'autorisation. Ces fonctionnalités ne sont pas activées par défaut.

Configuration post-installation

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 3.1](#) ”.
- Configurez des domaines invités. Reportez-vous au [Chapitre 5, “ Configuration des domaines invités ”](#) du manuel “ [Guide d’administration d’Oracle VM Server for SPARC 3.1](#) ”.

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 “[Contre-mesure : configuration d'un réseau de gestion dédié](#)” à la page 24.

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 des droits pour limiter l'accès de connectivité 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>.

Considérations relatives à la sécurité pour les développeurs

Ce chapitre fournit des informations destinées aux développeurs qui produisent des applications pour le logiciel Oracle VM Server for SPARC.

Interface XML d'Oracle VM Server for SPARC

Vous pouvez créer des programmes externes qui interagissent avec le logiciel Oracle VM Server for SPARC à l'aide du mécanisme de communication XML (Extensible Markup Language). XML utilise le protocole XMPP (Extensible Messaging and Presence Protocol).

Une personne malveillante étant susceptible 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 3.1](#) ”. 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 3.1](#) ”.

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`. La désactivation de XMPP empêche également Oracle VM Manager ou Ops Center de gérer le système.



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 3.1 ”](#)
- [“ Oracle Solaris 10 Security Guidelines ”](#)
- [“ Oracle Solaris 11 Security Guidelines ”](#)

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

- Effectuez les opérations de renforcement de la sécurité du SE 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 des droits pour restreindre l'accès aux consoles des domaines auxquels *vous seul*, 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 domaines invités appartenant à la même classe de sécurité sur une plate-forme physique donnée.
- Assurez-vous qu'il n'existe aucune connexion réseau entre le réseau d'administration de l'environnement d'exécution et les domaines invités.
- Affectez uniquement les ressources nécessaires aux domaines invités.

