

Guide d'administration Logical Domains (LDoms) 1.0.1

Sun Microsystems, Inc.
www.sun.com

Référence : 820-3441-10
Septembre 2007, Révision A

Faites-nous part de vos commentaires à l'adresse suivante : <http://www.sun.com/hwdocs/feedback>

Copyright © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, JumpStart, OpenBoot, Sun Fire, Netra, SunSolve, Sun BluePrints, Sun Blade, Sun Ultra, and SunVTS are service marks, trademarks, or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

The Adobe PostScript logo is a trademark of Adobe Systems, Incorporated.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, JumpStart, OpenBoot, Sun Fire, Netra, SunSolve, Sun BluePrints, Sun Blade, Sun Ultra, et SunVTS sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Le logo Adobe PostScript est une marque déposée de Adobe Systems, Incorporated.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont regis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Adobe PostScript

Contenu

Préface xxv

1. Présentation du logiciel Logical Domains 1

Hyperviseur et domaines logiques 1

Logical Domains Manager 3

 Rôles des domaines logiques 4

 Interface de ligne de commande 4

 Entrée/Sortie virtuelle 5

 Réseau virtuel 5

 Stockage virtuel 6

 Consoles virtuelles 6

 Reconfiguration dynamique 6

 Reconfiguration différée 7

 Configurations permanentes 8

2. Sécurité 9

 Considérations relatives à la sécurité 9

 Solaris Security Toolkit et Logical Domains Manager 10

 Sécurisation 11

 Minimisation des domaines logiques 12

Autorisation 13

Audit 13

Conformité 14

3. Installation et activation du logiciel 15

Mise à niveau vers la version 1.0.1 du logiciel LDOMs 15

- ▼ Pour effectuer une mise à niveau vers la version 1.0.1 du logiciel LDOMs 16

Installation du logiciel sur le domaine de contrôle 17

- ▼ Procédure d'installation du SE Solaris 10 18
- ▼ Procédure de mise à niveau du microprogramme système 19
- ▼ Procédure de mise à niveau du microprogramme système sans serveur FTP 20
- ▼ Procédure de mise à niveau inférieur de la version du microprogramme système 21

Téléchargement de Logical Domains Manager et de Solaris Security Toolkit 21

- ▼ Procédure de téléchargement de Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB 21

Installation de Logical Domains Manager et de Solaris Security Toolkit 22

Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l'aide du script d'installation 23

- ▼ Procédure d'installation à l'aide du script `install-ldm` sans aucune option 24
- ▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-d` 27
- ▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-d none` 28
- ▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-p` 29

Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l'aide de JumpStart 29

- ▼ Procédure d'installation d'un serveur JumpStart 30
- ▼ Procédure d'installation à l'aide du logiciel JumpStart 30

Installation manuelle de Logical Domains Manager et de Solaris Security Toolkit 32

- ▼ Procédure d'installation manuelle du logiciel Logical Domains Manager (LDoms) 1.0.1 32
- ▼ (*Facultatif*) Procédure d'installation manuelle du logiciel Solaris Security Toolkit 4.2 33
- ▼ (*Facultatif*) Procédure de sécurisation manuelle du domaine de contrôle 34
- ▼ Procédure de validation de la sécurisation 34
- ▼ Procédure d'annulation de la sécurisation 35

Activation du démon de Logical Domains Manager 35

- ▼ Procédure d'activation du démon de Logical Domains Manager 35

Création des profils et des autorisations et affectation de rôles aux comptes utilisateurs 36

Gestion des autorisations utilisateurs 37

- ▼ Procédure d'attribution d'une autorisation à un utilisateur 37
- ▼ Procédure de suppression de toutes les autorisations attribuées à un utilisateur 37

Gestion des profils utilisateurs 38

- ▼ Procédure d'attribution d'un profil à un utilisateur 38
- ▼ Procédure de suppression de tous les profils attribués à un utilisateur 38

Attribution de rôles aux utilisateurs 38

- ▼ Procédure de création d'un rôle et d'attribution à un utilisateur 39

4. Configuration des services et des domaines logiques 41

Messages des commandes 41

Processeurs Sun UltraSPARC T1 42

Processeurs Sun UltraSPARC T2 42

Création des services par défaut 42

- ▼ Procédure de création des services par défaut : 43

Configuration initiale du domaine de contrôle	44
▼ Procédure de configuration du domaine de contrôle	44
Redémarrage et utilisation des domaines logiques	46
▼ Procédure de redémarrage et d'utilisation des domaines logiques	46
Activation de la mise en réseau du domaine de contrôle/service et des autres domaines	47
▼ Procédure de configuration du commutateur	47
Activation du démon du serveur de terminal réseau virtuel	48
▼ Procédure d'activation du démon du serveur de terminal réseau virtuel	49
Création et lancement d'un domaine hôte	49
▼ Procédure de création et de lancement d'un domaine hôte	50
Installation JumpStart sur un domaine hôte	53

5. Informations et tâches complémentaires 55

Accès à la page de manuel <code>ldm(1M)</code>	56
▼ Procédure d'accès à la page de manuel <code>ldm(1M)</code>	56
Limitations pour la saisie des noms dans l'interface de ligne de commande	56
Noms de fichier (<i>file</i>) et noms de variable (<i>var_name</i>)	56
Noms de serveur de disque virtuel <i>file device</i> et de commutateur virtuel	56
Nom de configuration (<i>config_name</i>)	57
Autres noms	57
Utilisation des sous-commandes <code>ldm list</code>	57
Résultat lisible par une machine	57
▼ Procédure d'affichage de la syntaxe à utiliser pour les sous-commandes <code>ldm</code>	58
Définition des indicateurs	60
Définition des statistiques d'utilisation	61
Exemples des diverses listes	61
▼ Procédure d'affichage des versions des logiciels (<code>-v</code>)	61
▼ Procédure de génération d'une liste courte	62

- ▼ Procédure de génération d'une liste longue (-l) 62
- ▼ Procédure de génération d'une liste étendue (-e) 64
- ▼ Procédure de génération d'une liste lisible et analysable par une machine (-p) 66
- ▼ Procédure d'affichage de l'état d'un domaine 66
- ▼ Procédure de listage d'une variable 66
- ▼ Procédure de listage des liaisons 67
- ▼ Procédure de listage des configurations 68
- ▼ Procédure de listage des périphériques 68
- ▼ Procédure de listage des services 70

Listage des contraintes 70

- ▼ Procédure de listage des contraintes pour un domaine 70
- ▼ Procédure de listage des contraintes au format XML 71
- ▼ Procédure de listage des contraintes dans un format lisible par une machine 72

La commande `ldm stop-domain` peut expirer si le domaine est très chargé 73

Détermination du nom de l'interface réseau Solaris correspondant à un périphérique réseau virtuel 74

- ▼ Procédure permettant de trouver le nom de l'interface réseau du SE Solaris 74

Assignation des adresses Mac automatiquement ou manuellement 75

Plage d'adresses MAC assignées au logiciel Logical Domains 76

Algorithme d'assignation automatique 76

Détection d'adresses MAC dupliquées 77

Adresses MAC libérées 78

Allocation manuelle d'adresses MAC 78

- ▼ Procédure d'allocation manuelle d'une adresse MAC 78

Mappage de CPU et d'adresse mémoire 79

Mappage de CPU 79

- ▼ Procédure de détermination du numéro de CPU 79

Mappage de mémoire	80
▼ Procédure de détermination de l'adresse réelle	80
Exemples de mappage de CPU et de mémoire	80
Configuration du bus Split PCI Express pour utiliser plusieurs domaines logiques	82
▼ Procédure de création d'une configuration Split PCI	83
Activation du mode évitement MMU E/S sur un bus PCI	86
Utilisation des groupes de consoles	86
▼ Procédure de combinaison de plusieurs consoles dans un groupe	87
Déplacement d'un domaine logique d'un serveur à l'autre	88
▼ Procédure de configuration des domaines en vue d'un déplacement	88
▼ Procédure de déplacement du domaine	88
Suppression de domaines logiques	88
▼ Procédure de suppression de tous les domaines logiques hôtes	89
Fonctionnement du SE Solaris avec Logical Domains	90
Arrêt puis remise sous tension d'un serveur	90
▼ Procédure d'enregistrement des configurations de domaine logique actuelles sur le contrôleur système	90
Résultat d'une commande <code>OpenBoot power-off</code>	91
Résultat d'une commande <code>shutdown</code> du SE Solaris	91
Résultat d'une combinaison de touches d'interruption du SE Solaris (L1-A)	91
Résultats de la halte ou du redémarrage du domaine de contrôle	92
Certaines options de la commande <code>format(1M)</code> ne fonctionnent pas avec des disques virtuels	93
Utilisation de LDomS avec ALOM CMT	94
▼ Procédure de réinitialisation de la configuration du domaine logique à celle par défaut ou à une autre	95
Activation et utilisation de l'audit BSM	95
▼ Procédure d'utilisation du script <code>enable-bsm.fin</code>	96
▼ Procédure d'utilisation de la commande <code>bsmconv(1M)</code> du SE Solaris	96

▼ Procédure permettant de vérifier que l’audit BSM est activé	97
▼ Procédure de désactivation de l’audit	97
▼ Procédure d’impression du résultat d’audit	97
▼ Procédure de roulement des journaux d’audit	98
Configuration du commutateur virtuel et du domaine de service pour NAT et routage	98
▼ Procédure de configuration du commutateur virtuel afin de fournir la connectivité externe aux domaines	99
Utilisation de ZFS avec des disques virtuels	99
Création d’un disque virtuel sur un volume ZFS	100
▼ Procédure de création d’un disque virtuel sur un volume ZFS	100
Utilisation de ZFS sur un disque virtuel	101
▼ Procédure d’utilisation de ZFS sur un disque virtuel	101
Utilisation de ZFS sur des disques d’initialisation	103
▼ Procédure d’utilisation de ZFS sur des disques d’initialisation	103
Utilisation des gestionnaires de volume dans un environnement Logical Domains	105
Utilisation de disques virtuels sur des gestionnaires de volume	105
Remarque sur l’utilisation des disques virtuels sur un volume SVM	106
Remarque sur l’utilisation des disques virtuels lorsque VxVM est installé	107
Utilisation de gestionnaires de volume sur des disques virtuels	108
Utilisation de ZFS sur des disques virtuels	108
Utilisation de SVM sur des disques virtuels	108
Utilisation de VxVM sur des disques virtuels	109
Configuration d’IPMP dans un environnement Logical Domains	109
Configuration de périphériques réseau virtuels dans un groupe IPMP au sein d’un domaine logique	109
Configuration et utilisation d’IPMP dans un domaine de service	110
Glossaire	113

Figures

FIGURE 1-1	Hyperviseur prenant en charge deux domaines logiques	2
FIGURE 5-1	Deux réseaux virtuels connectés à des instances de commutateur virtuel distinctes	110
FIGURE 5-2	Connexion des périphériques réseau virtuels à différents domaines de service	110
FIGURE 5-3	Deux interfaces réseau configurées en groupe IPMP	111

Tableaux

TABLEAU 1-1	Rôles d'un domaine logique	4
TABLEAU 2-1	Sous-commandes <code>ldm</code> et autorisations utilisateurs	13
TABLEAU 5-1	Comportement prévu pour la halte ou le redémarrage du domaine de contrôle (<code>primary</code>)	92

Exemples de code

EXEMPLE DE CODE 3-1	Structure du répertoire du logiciel Logical Domains 1.0.1 téléchargé	22
EXEMPLE DE CODE 3-2	Exemple de message dans la configuration sécurisée Solaris pour LDom	25
EXEMPLE DE CODE 3-3	Exemple de message de choix de profil de configuration personnalisé	26
EXEMPLE DE CODE 3-4	Exemple de message indiquant l'exécution correcte du script <code>install-ldm -d</code>	27
EXEMPLE DE CODE 3-5	Exemple de message indiquant l'exécution correcte du script <code>install-ldm -d none</code>	28
EXEMPLE DE CODE 5-1	Utilisation de la syntaxe pour toutes les sous-commandes <code>ldm</code>	58
EXEMPLE DE CODE 5-2	Versions des logiciels installées	61
EXEMPLE DE CODE 5-3	Liste courte pour tous les domaines	62
EXEMPLE DE CODE 5-4	Liste longue pour tous les domaines	62
EXEMPLE DE CODE 5-5	Liste étendue pour tous les domaines	64
EXEMPLE DE CODE 5-6	Liste lisible par une machine	66
EXEMPLE DE CODE 5-7	État d'un domaine	66
EXEMPLE DE CODE 5-8	Listage d'une variable pour un domaine	66
EXEMPLE DE CODE 5-9	Listage des liaisons pour un domaine	67
EXEMPLE DE CODE 5-10	Listage de configurations	68
EXEMPLE DE CODE 5-11	Listage de toutes les ressources du serveur	68
EXEMPLE DE CODE 5-12	Listage des services	70
EXEMPLE DE CODE 5-13	Listage des contraintes pour un domaine	70
EXEMPLE DE CODE 5-14	Contraintes pour un domaine au format XML	71
EXEMPLE DE CODE 5-15	Contraintes pour tous les domaines dans un format lisible par une machine	72

EXEMPLE DE CODE 5-16 Longue liste analysable de configurations de domaines

logiques 81

Préface

Le *Guide d'administration Logical Domains (LDoms) 1.0.1* fournit des procédures et des informations détaillées sur la présentation, la sécurité, l'installation, la configuration, la modification et l'exécution des tâches courantes via le logiciel Logical Domains Manager 1.0.1 sur les serveurs, les lames et les modules serveurs pris en charge. Reportez-vous à la section « Serveurs pris en charge » des *Notes de version Logical Domains (LDoms) 1.0.1* pour obtenir la liste complète des serveurs pris en charge. Ce guide s'adresse aux administrateurs système de ces serveurs maîtrisant les systèmes UNIX® et le système d'exploitation Solaris™ (SE Solaris).

Avant de lire ce document

Si vous ne maîtrisez ni les procédures et commandes UNIX, ni le système d'exploitation Solaris, familiarisez-vous avec les guides de l'utilisateur et de l'administrateur du SE Solaris fournis avec le matériel. Il est également conseillé de suivre une formation en administration système UNIX.

Présentation du guide

Le [chapitre 1](#) présente le logiciel Logical Domains.

Le [chapitre 2](#) décrit le logiciel Solaris™ Security Toolkit et explique comment l'utiliser pour sécuriser le SE Solaris dans les domaines logiques.

Le [chapitre 3](#) fournit des procédures détaillées sur la mise à niveau, l'installation et l'activation du logiciel Logical Domains Manager.

Le [chapitre 4](#) fournit des procédures détaillées sur la configuration des services et des domaines logiques.

Le [chapitre 5](#) fournit des informations et des procédures supplémentaires sur l'exécution des tâches courantes pour gérer les domaines logiques à l'aide du logiciel Logical Domains.

Le [glossaire](#) répertorie les abréviations, acronymes et termes utilisés, avec leur définition spécifique aux logiciels LDoms.

Utilisation des commandes UNIX

Ce document ne contient pas d'informations sur les commandes UNIX de base, ni sur les procédures telles que le démarrage et l'arrêt du système ou la configuration des périphériques. Pour plus d'informations sur ces sujets, consultez les informations suivantes :

- Documentation des logiciels livrés avec votre système
- Documentation du système d'exploitation Solaris™ disponible à l'adresse suivante :

<http://docs.sun.com>

Invites Shell

Shell	Invite
C shell	<i>nom-ordinateur%</i>
C shell superutilisateur	<i>nom-ordinateur#</i>
Bourne shell et Korn shell	\$
Bourne shell et Korn shell superutilisateur	#

Conventions typographiques

Police*	Signification	Exemples
AaBbCc123	Noms des commandes, fichiers et répertoires. Messages apparaissant à l'écran.	Modifiez le fichier <code>.login</code> . Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers. % vous avez du courrier.
AaBbCc123	Ce que l'utilisateur tape par opposition aux messages apparaissant à l'écran.	% su Mot de passe :
<i>AaBbCc123</i>	Titres de guide, nouveaux mots ou termes, mots à mettre en valeur. Remplacez les variables de ligne de commande par les noms ou les valeurs appropriés.	Consultez le chapitre 6 du <i>Guide de l'utilisateur</i> . Il s'agit d'options de <i>classe</i> . Pour supprimer un fichier, entrez rm <i>nomfichier</i> .

*. Les paramètres de votre navigateur peuvent être différents.

Documentation connexe

Le *Guide d'administration Logical Domains (LDoms) 1.0.1* et les *Notes de version* sont disponibles à l'adresse suivante :

<http://docs.sun.com>

Le manuel *Beginners Guide to LDomS: Understanding and Deploying Logical Domains Software* est disponible sur le site Sun BluePrints™, à l'adresse suivante :

<http://www.sun.com/blueprints/0207/820-0832.html>

Des documents relatifs à votre serveur et à votre système d'exploitation Solaris sont disponibles à l'adresse suivante :

<http://www.sun.com/documentation/>

Entrez le nom de votre serveur ou de votre SE Solaris dans le champ Search pour rechercher les documents dont vous avez besoin.

Application	Titre	Numéro de référence	Format	Emplacement
Notes de version LDomS	<i>Notes de version Logical Domains (LDomS) 1.0.1</i>	819-6429-12	HTML PDF	En ligne
Pages de manuel Solaris pour LDomS	Solaris 10 Reference Manual Collection: <ul style="list-style-type: none">• Page de manuel <code>drd</code>(1M)• Page de manuel <code>vntsd</code>(1M)	S/O	HTML PDF	En ligne
Page de manuel LDomS	Page de manuel <code>ldm</code> (1M) <i>Logical Domains (LDomS) 1.0.1 Manager Man Page Guide</i>	S/O 819-7679-10	SGML	Avec le code LDomS En ligne
Notions de base sur le logiciel Logical Domains	<i>Beginners Guide to LDomS: Understanding and Deploying Logical Domains Software</i>	820-0832-20	PDF	En ligne
Administration de LDomS MIB	<i>Guide d'administration Logical Domains (LDomS) MIB 1.0.1</i>	820-2319-10	HTML PDF	En ligne
Notes de version LDomS MIB	<i>Notes de version Logical Domains (LDomS) MIB 1.0.1</i>	820-2320-10	HTML PDF	En ligne
SE Solaris y compris l'installation à l'aide de JumpStart™ et l'utilisation de l'utilitaire SMF (Service Management Facility)	Solaris 10 Collection	S/O	HTML PDF	En ligne
Sécurité	<i>Solaris Security Toolkit 4.2 Administration Guide</i>	819-1402-10	HTML PDF	En ligne
Sécurité	<i>Solaris Security Toolkit 4.2 Reference Manual</i>	819-1503-10	HTML PDF	En ligne

Application	Titre	Numéro de référence	Format	Emplacement
Sécurité	<i>Solaris Security Toolkit 4.2 Release Notes</i>	819-1504-10	HTML PDF	En ligne
Sécurité	<i>Solaris Security Toolkit 4.2 Man Page Guide</i>	819-1505-10	HTML PDF	En ligne
Logiciel Sun Management Center compatible avec les serveurs de Logical Domains Manager 1.0.1 pris en charge	<i>Sun Management Center 3.6 Version 6 Add-On Software Release Notes: For Sun Fire™, Sun Blade™, Netra™, and Sun Ultra™ Systems</i>	820-1041-10	PDF	En ligne
SunVTS™	<i>Guide de l'utilisateur SunVTS 6.3</i>	820-0080	HTML	En ligne
	<i>Guide de l'utilisateur SunVTS 6.4</i>	820-1669	PDF	
ILOM compatible avec Logical Domains Manager 1.0.1 et les serveurs Sun SPARC® Enterprise T5120 et T5220	<i>Integrated Lights Out Management 2.0 (ILOM 2.0) Supplement for Sun SPARC Enterprise T5120 and T5220 Servers</i>	820-2180	HTML PDF	En ligne
ALOM CMT compatible avec Logical Domains Manager 1.0.1 et les serveurs Sun Fire T1000 et T2000	<i>Advanced Lights Out Management (ALOM) CMT v1.3 Guide</i>	819-7981-11	HTML PDF	En ligne
Sun™ Explorer 5.7 Data Collector	<i>Sun Explorer User's Guide</i>	819-6613	HTML PDF	En ligne
Serveurs Sun Fire et Sun SPARC Enterprise Sun Fire T1000	<i>Sun Fire and Sun SPARC Enterprise T1000 Server Administration Guide</i>	819-3249-12	HTML	En ligne
		820-0020-10	PDF	
Serveurs Sun Fire et Sun SPARC Enterprise Sun Fire T2000	<i>Sun Fire and Sun SPARC Enterprise T2000 Server Administration Guide</i>	819-2549-12	HTML	En ligne
		819-7990-10	PDF	
Serveurs Netra T2000	<i>Netra T2000 Server Administration Guide</i>	819-5837-10	PDF	En ligne
Lames Netra CP3060	<i>Netra CP3060 Board Product Notes</i>	819-4966-12	PDF	En ligne

Application	Titre	Numéro de référence	Format	Emplacement
Modules serveur Sun Blade T6300	<i>Sun Blade T6300 Server Module Administration Guide</i>	820-0277-10	PDF	En ligne
	<i>Sun Blade T6300 Server Module Installation Guide</i>	820-0275-10	PDF	En ligne
	<i>Sun Blade T6300 Server Module Product Notes</i>	820-0278-10	PDF	En ligne
Serveurs Sun SPARC Enterprise T5120 et T5220	<i>Sun SPARC Enterprise T5120 and T5220 Servers Product Notes</i>	820-2176	PDF	En ligne
	<i>Sun SPARC Enterprise T5120 and T5220 Servers Installation Guide</i>	820-2178	PDF	En ligne
	<i>Sun SPARC Enterprise T5120 and T5220 Servers Administration Guide</i>	820-2179	PDF	En ligne
Netra Data Plane Software Suite 1.1	<i>Netra Data Plan Software Suite 1.1 User's Guide</i>	820-2374	HTML	En ligne
	<i>Netra Data Plan Software Suite 1.1 Reference Manual</i>	820-2375	HTML	En ligne
	<i>Netra Data Plan Software Suite 1.1 Release Notes</i>	820-2376	PDF	En ligne

Documentation, support et formation

Fonction Sun	URL
Documentation	http://www.sun.com/documentation
Support	http://www.sun.com/support
Formation	http://www.sun.com/training

Sites Web tiers

Sun décline toute responsabilité quant à la disponibilité des sites Web de parties tierces mentionnés dans ce document. Sun n'avalise pas et n'est pas responsable des contenus, des publicités, des produits ou autres matériaux disponibles sur ou par le biais de ces sites ou ressources. Sun ne saurait pas non plus être tenue responsable de toute perte ou dommage, réel(le) ou prétendu(e), causé(e) par l'utilisation desdits contenus, biens ou services disponibles sur ou via ces sites et ressources ou découlant de la confiance accordée auxdits contenus.

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, tous vos commentaires et suggestions sont les bienvenus. Vous pouvez nous faire part de vos commentaires à l'adresse suivante :

<http://www.sun.com/hwdocs/feedback>

Veuillez mentionner le titre et le numéro de référence du document dans votre message :

Guide d'administration Logical Domains (LDoms) 1.0.1, numéro de référence 820-3441-10.

Présentation du logiciel Logical Domains

Ce chapitre présente le logiciel Logical Domains :

- « Hyperviseur et domaines logiques », page 1
- « Logical Domains Manager », page 3

Toutes les fonctionnalités du SE Solaris et tous les patches requis pour utiliser la technologie Logical Domains de Sun se trouvent dans la version Solaris 10 11/06 (au minimum). Toutefois, un microprogramme système et le logiciel Logical Domains Manager sont également requis pour utiliser les domaines logiques. Reportez-vous à la section « Logiciel requis et recommandé » des *Notes de version Logical Domains (LDoms) 1.0.1* pour plus d'informations à ce sujet.

Hyperviseur et domaines logiques

Cette section contient une présentation succincte de l'hyperviseur SPARC et des domaines logiques qu'il prend en charge.

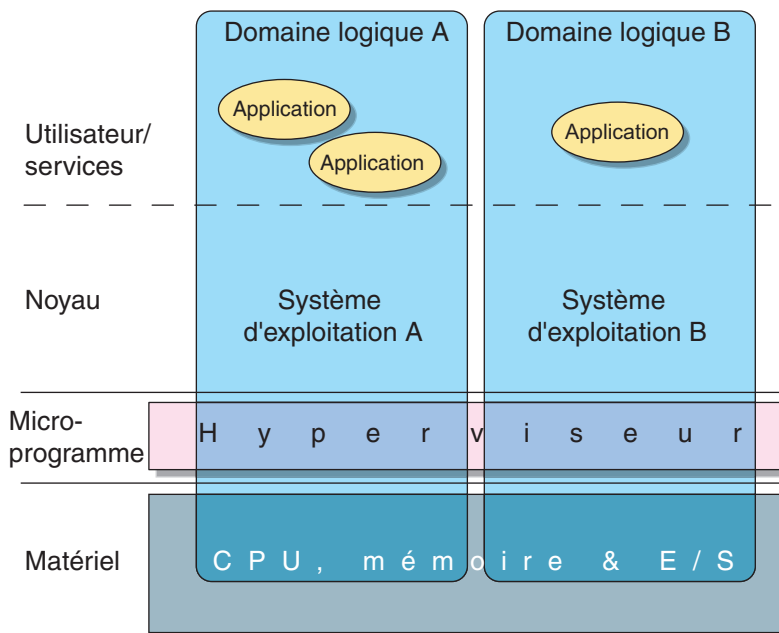
L'hyperviseur SPARC est un microprogramme allégé qui fournit une architecture de virtualisation stable permettant d'assurer l'exécution d'un système d'exploitation. Les serveurs Sun dotés de cet hyperviseur offrent des caractéristiques matérielles pour prendre en charge le contrôle des activités d'un système d'exploitation logique.

Un domaine logique est un regroupement logique discret doté de son propre système d'exploitation, de ses propres ressources et de sa propre identité au sein d'un seul système informatique. Chaque domaine logique peut être créé, supprimé, reconfiguré et redémarré indépendamment, sans interruption du serveur. Vous pouvez exécuter toute une variété de logiciels d'application dans différents domaines logiques indépendants à des fins de sécurité et de performances.

Chaque domaine logique est autorisé à observer et interagir uniquement avec les ressources serveur que l'hyperviseur a rendues disponibles. L'administrateur système détermine l'activité de l'hyperviseur via le domaine de contrôle à l'aide du logiciel Logical Domains Manager. L'hyperviseur applique par conséquent le partitionnement des ressources d'un serveur et fournit des sous-ensembles limités à plusieurs environnements de système d'exploitation. Il s'agit d'un mécanisme fondamental pour créer des domaines logiques. Le schéma suivant indique un hyperviseur prenant en charge deux domaines logiques. Il indique également les couches qui constituent les fonctionnalités des domaines logiques :

- Applications ou utilisateur/services
- Noyau ou systèmes d'exploitation
- Microprogramme ou hyperviseur
- Matériel, y compris CPU, mémoire et E/S

FIGURE 1-1 Hyperviseur prenant en charge deux domaines logiques



Le nombre de fonctionnalités de chaque domaine logique pris en charge par un hyperviseur SPARC dépend de celles du serveur. L'hyperviseur peut attribuer des sous-ensembles de la CPU globale, de la mémoire et des ressources d'E/S d'un serveur à un certain domaine logique. Plusieurs systèmes d'exploitation peuvent ainsi être pris en charge simultanément, chacun se trouvant dans son propre domaine logique. Les ressources peuvent être réorganisées entre les domaines logiques séparés selon une granularité arbitraire. Vous pouvez, par exemple, affecter de la mémoire à un domaine logique avec une granularité de 8 Ko.

Chaque ordinateur virtuel peut être géré en tant qu'ordinateur complètement indépendant, avec ses propres ressources, telles que :

- un noyau, des patchs et des paramètres de réglage ;
- des comptes utilisateurs et administrateurs ;
- des disques ;
- des interfaces réseau, des adresses MAC et des adresses IP.

Chaque ordinateur virtuel peut être arrêté, démarré et redémarré indépendamment, sans interruption du serveur.

Le logiciel hyperviseur est chargé de maintenir une séparation entre les domaines logiques. Il fournit également des LDC (Logical Domain Channels, canaux de domaine logique) afin de permettre aux domaines logiques de communiquer entre eux. Grâce à ces LDC, les domaines peuvent s'échanger des services (mise en réseau ou services de disque, par exemple).

Le contrôle système surveille et exécute l'ordinateur physique, mais ne gère pas les ordinateurs virtuels. C'est le logiciel Logical Domains Manager qui exécute les ordinateurs virtuels.

Logical Domains Manager

Le logiciel Logical Domains Manager permet de créer et de gérer des domaines logiques. Seul un logiciel Logical Domains Manager est autorisé par serveur. Ce logiciel mappe les domaines logiques aux ressources physiques.

Rôles des domaines logiques

La seule différence entre les domaines logiques réside dans les rôles que vous leur attribuez. Les domaines logiques peuvent avoir plusieurs rôles :

TABLEAU 1-1 Rôles d'un domaine logique

Rôle du domaine	Description
Domaine de contrôle	Domaine dans lequel s'exécute le logiciel Logical Domains Manager et qui vous permet de créer et de gérer d'autres domaines logiques et d'allouer des ressources virtuelles à d'autres domaines. Seul un domaine de contrôle est autorisé par serveur. Le premier domaine créé lors de l'installation du logiciel Logical Domains s'appelle <code>primary</code> .
Domaine de service	Domaine qui fournit des services de périphérique virtuel à d'autres domaines, comme un commutateur virtuel, un concentrateur de consoles virtuelles et un serveur de disque virtuel.
Domaine d'E/S	Domaine détenant et ayant un accès direct aux périphériques d'E/S physiques, comme une carte réseau d'un contrôleur PCI-Express. Si le domaine d'E/S est également le domaine de contrôle, il partage alors les périphériques avec d'autres domaines sous forme de périphériques virtuels. Le nombre de domaines d'E/S autorisé dépend de l'architecture de votre plate-forme. Par exemple, si vous disposez d'un processeur Sun UltraSPARC® T1, vous pouvez avoir au maximum deux domaines d'E/S (l'un d'entre eux devant également constituer le domaine de contrôle).
Domaine hôte	Domaine géré par le domaine de contrôle et qui utilise les services des domaines d'E/S et de service.

Si vous disposez déjà d'un système et si un système d'exploitation et d'autres logiciels sont en cours d'exécution sur le serveur, ce domaine constitue votre domaine de contrôle une fois le logiciel Logical Domains Manager installé. Vous pouvez supprimer certaines applications du domaine de contrôle une fois qu'il est installé et répartir la charge des autres applications dans les différents domaines afin d'optimiser l'utilisation du système.

Interface de ligne de commande

Via la CLI (Command-Line Interface, interface de ligne de commande) du logiciel Logical Domains Manager, l'administrateur système peut créer et configurer des domaines logiques.

Pour utiliser cette CLI, le démon de Logical Domains Manager, `ldmd` doit être en cours d'exécution. La CLI est une commande unique, `ldm(1M)`, dotée de plusieurs sous-commandes. La commande `ldm(1M)` et ses sous-commandes sont présentées en détail dans la page de manuel `ldm(1M)` du *Logical Domains (LDDoms) Manager 1.0.1 Man Page Guide*.

Pour exécuter la commande `ldm`, le répertoire `/opt/SUNWldm/bin` doit être présent dans la variable UNIX `$PATH`. Pour accéder à la page de manuel `ldm(1M)`, ajoutez le chemin de répertoire `/opt/SUNWldm/man` à la variable `$MANPATH`. Elles se présentent toutes deux de la manière suivante :

```
$ PATH=$PATH:/opt/SUNWldm/bin; export PATH (for Bourne or K shell)
$ MANPATH=$MANPATH:/opt/SUNWldm/man; export MANPATH
% set PATH=($PATH /opt/SUNWldm/bin) (for C shell)
% set MANPATH=($MANPATH /opt/SUNWldm/man)
```

Entrée/Sortie virtuelle

Dans un environnement de technologie Logical Domains, un administrateur peut placer jusqu'à 32 domaines sur un serveur Sun Fire ou SPARC Enterprise T1000 ou T2000. Bien qu'il soit possible d'affecter des CPU et de la mémoire dédiées à chaque domaine, en raison du nombre limité de bus d'E/S et d'emplacements d'E/S physiques dans ces systèmes, il est impossible de fournir un accès exclusif au disque et aux périphériques réseau à tous les domaines. Même s'il est possible de partager certains périphériques physiques en scindant le bus PCI-Express® (PCI-E) en deux (voir section « [Configuration du bus Split PCI Express pour utiliser plusieurs domaines logiques](#) », page 82), cela reste insuffisant pour fournir à tous les domaines un accès exclusif aux périphériques. L'implémentation d'un modèle d'E/S virtualisé permet de pallier au manque d'accès direct aux périphériques d'E/S physiques.

Les domaines logiques sans accès direct d'E/S sont configurés avec des périphériques d'E/S qui communiquent avec un domaine de service exécutant un service pour exporter l'accès à un périphérique physique ou à ses fonctions. Dans ce modèle client-serveur, les périphériques d'E/S virtuels communiquent soit entre eux, soit par l'intermédiaire d'un service via des canaux de communication interdomaine appelés LDC (Logical Domain Channels, canaux de domaine logique). Dans le logiciel Logical Domains 1.0.1, la fonctionnalité d'E/S virtualisée offre une prise en charge des consoles, du stockage et de la mise en réseau virtuels.

Réseau virtuel

La prise en charge du réseau virtuel s'effectue à l'aide de deux composants : le périphérique réseau virtuel et le périphérique commutateur réseau virtuel. Le périphérique réseau virtuel (`vnet`) émule un périphérique Ethernet et communique

avec d'autres périphériques `vnet` du système à l'aide d'un canal point à point. Le périphérique commutateur virtuel (`vsw`) fonctionne principalement comme un [dé]multiplexeur des paquets entrants et sortants du réseau virtuel. Le périphérique `vsw` s'interface directement avec un adaptateur de réseau physique sur un domaine de service, et envoie et reçoit des paquets au nom d'un réseau virtuel. Ce périphérique `vsw` fonctionne, en outre, comme un simple commutateur de niveau 2 et commute les paquets entre les périphériques `vnet` qui lui sont connectés au sein du système.

Stockage virtuel

L'infrastructure de stockage virtuel permet aux domaines logiques d'accéder au stockage de niveau bloc non affecté directement via un modèle client-serveur. Elle comprend deux composants : un client de disque virtuel (`vdci`) qui effectue l'exportation en tant qu'interface de périphérique bloc, et un service de disque virtuel (`vdss`) qui traite les requêtes disque au nom du client disque virtuel et les soumet au stockage physique résidant sur le domaine de service. Les disques virtuels s'affichent comme des disques standard sur le domaine client, mais toutes les opérations sur disque sont transmises au disque physique via le service de disque virtuel.

Consoles virtuelles

Dans un environnement de technologie Logical Domains, les E/S de console de tous les domaines (à l'exception du domaine `primary`) sont redirigées vers un domaine de service exécutant les services de concentrateur de consoles virtuelles (`vcc`) et du serveur de terminal réseau virtuel (`vntsd`), et non vers le contrôleur système. Le service de concentrateur de consoles virtuelles fonctionne en tant que concentrateur pour tout le trafic de la console du domaine, s'interface avec le démon du serveur de terminal réseau virtuel et fournit l'accès à chaque console via un socket UNIX.

Reconfiguration dynamique

La reconfiguration dynamique (RD) désigne la capacité à ajouter ou supprimer des ressources pendant que le système d'exploitation est en cours d'exécution. Le SE Solaris 10 prend en charge uniquement l'ajout et la suppression de CPU virtuelles (`vcpus`). La reconfiguration dynamique de mémoire et d'entrée/sortie n'est pas prise en charge sous ce système d'exploitation. Pour utiliser la fonction de reconfiguration dynamique dans l'interface de ligne de commande de Logical Domains Manager, le démon de reconfiguration dynamique de Logical Domains, `drd(1M)` doit s'exécuter dans le domaine que vous souhaitez modifier.

Reconfiguration différée

Contrairement aux opérations de reconfiguration dynamique qui s'exécutent immédiatement, les opérations de reconfiguration différées s'exécutent après redémarrage du système d'exploitation (ou après l'arrêt et le démarrage du domaine logique si aucun système d'exploitation n'est en cours d'exécution). Toutes les opérations d'ajout ou de suppression sur les domaines logiques actifs (à l'exception des sous-commandes `add-vcpu`, `set-vcpu` et `remove-vcpu`) sont considérées comme des opérations de reconfiguration différée. La sous-commande `set-vswitch` sur un domaine logique actif est également considérée comme une opération de reconfiguration différée.

Si vous utilisez un processeur Sun UltraSPARC T1, lorsque le logiciel Logical Domains Manager est installé et activé en premier (ou lorsque les paramètres `factory-default` de la configuration sont restaurés), LDoms Manager s'exécute dans le mode de configuration. Dans ce mode, les requêtes de reconfiguration sont acceptées et mises en file d'attente, mais ne sont pas prises en compte. Une nouvelle configuration peut ainsi être générée et stockée sur le contrôleur système, sans affecter pour autant l'état de l'ordinateur en cours d'exécution, et, par conséquent, sans être gênée par des restrictions telles que la reconfiguration différée et le redémarrage des domaines d'E/S.

Dès qu'une reconfiguration différée est en cours pour un domaine logique, les autres requêtes de reconfiguration de ce domaine logique sont différées jusqu'à son redémarrage (ou jusqu'à son arrêt, puis son démarrage). De même, lorsqu'une reconfiguration différée est en cours pour un domaine logique, cela limite considérablement l'exécution des requêtes de reconfiguration pour d'autres domaines logiques ; dans ce cas, elles échouent et un message d'erreur s'affiche.

Même si les tentatives de suppression des périphériques d'E/S virtuels sur un domaine logique actif sont gérées en tant qu'opération de reconfiguration différée, certaines modifications de configuration sont appliquées immédiatement. Cela signifie que le périphérique arrête de fonctionner une fois l'opération associée invoquée via la CLI de Logical Domains Manager.

La sous-commande `remove-reconf` de Logical Domains Manager annule les opérations de reconfiguration différée. Vous pouvez répertorier les opérations de reconfiguration différée à l'aide de la commande `ldm list-domain`. Reportez-vous à la page de manuel `ldm(1M)` ou au *Logical Domains (LDoms) Manager 1.0.1 Man Page Guide* pour en savoir plus sur l'utilisation de la fonction de reconfiguration différée.

Remarque – Vous ne pouvez pas utiliser la commande `ldm remove-reconf` si d'autres commandes `ldm remove-*` ont été émises sur les périphériques d'E/S virtuels. Le cas échéant, la commande `ldm remove-reconf` échoue.

Configurations permanentes

La configuration d'un domaine logique peut être stockée sur le contrôleur système à l'aide des commandes de la CLI de Logical Domains Manager. Vous pouvez ajouter ou supprimer une configuration, indiquer celle à utiliser et toutes les répertorier sur le contrôleur système. (Reportez-vous à la page de manuel `ldm(1M)` ou au *Logical Domains (LDoms) Manager 1.0.1 Man Page Guide*.) La commande ALOM CMT Version 1.3, en outre, vous permet de sélectionner la configuration à initialiser (reportez-vous à la section « [Utilisation de LDoms avec ALOM CMT](#) », page 94).

Sécurité

Ce chapitre décrit le logiciel Solaris Security Toolkit et de quelle manière vous pouvez l'utiliser pour sécuriser le SE Solaris dans vos domaines logiques.

Il couvre les rubriques suivantes :

- « [Considérations relatives à la sécurité](#) », page 9
- « [Solaris Security Toolkit et Logical Domains Manager](#) », page 10

Considérations relatives à la sécurité

Le logiciel Solaris Security Toolkit, couramment appelé kit d'outils JumpStart™ Architecture and Security Scripts (JASS), propose un mécanisme automatisé, extensible et évolutif permettant de construire et de sécuriser des SE Solaris. Solaris Security Toolkit permet de sécuriser les périphériques indispensables à la gestion du serveur, y compris le domaine de contrôle de Logical Domains Manager.

Le logiciel Solaris Security Toolkit 4.2, SUNWjass sécurise le système d'exploitation Solaris sur le domaine de contrôle via l'utilisation du script `install-ldm` de différentes manières :

- En sécurisant automatiquement le domaine de contrôle à l'aide du script `install` (`install-ldm`) et du pilote de contrôle propre à Logical Domains Manager (`ldm_control-secure.driver`).
- En sélectionnant un autre pilote lors de l'utilisation du script `install`.
- En ne sélectionnant aucun pilote lors de l'utilisation du script `install` et en appliquant votre propre sécurisation de Solaris.

Les packages SUNWjass et Logical Domains (LDoms) Manager 1.0.1, SUNWldm sont disponibles sur le site de téléchargement de Sun. Vous pouvez télécharger et installer le logiciel Solaris Security Toolkit 4.2 en même temps que Logical Domains Manager 1.0.1. Solaris Security Toolkit version 4.2 contient tous les patches requis

pour utiliser Solaris Security Toolkit avec le logiciel Logical Domains Manager. Une fois Solaris Security Toolkit 4.2 installé, vous pouvez sécuriser le système. Le [chapitre 3](#) vous indique comment installer et configurer Solaris Security Toolkit et sécuriser le domaine de contrôle.

Les utilisateurs de Logical Domains Manager ont accès aux fonctions de sécurité de Solaris Security Toolkit suivantes :

- *Sécurisation* : fonction permettant de modifier des configurations du SE Solaris afin d'améliorer la sécurité du système à l'aide du logiciel Solaris Security Toolkit version 4.2 et des patchs requis pour utiliser Solaris Security Toolkit avec Logical Domains Manager.
- *Minimisation* : fonction permettant d'installer le nombre minimum de packages du SE Solaris de base afin de prendre en charge LDoms et LDoms Management Information Base (MIB).
- *Autorisation* : fonction permettant de définir des autorisations à l'aide du contrôle RBAC (Role-Based Access Control, contrôle d'accès basé sur les rôles) du SE Solaris adapté au logiciel Logical Domains Manager.
- *Audit* : fonction permettant d'utiliser le BSM (Basic Security module, module de sécurité de base) du SE Solaris adapté au logiciel Logical Domains Manager pour identifier l'origine des modifications de sécurité apportées au système, et déterminer ce qui a été effectué, quand, par qui et ce qui a changé.
- *Conformité* : fonction permettant de déterminer si une configuration du système est conforme à un profil de sécurité prédéfini à l'aide de la fonction d'audit de Solaris Security Toolkit.

Solaris Security Toolkit et Logical Domains Manager

Le [chapitre 3](#) vous indique comment installer le logiciel Solaris Security Toolkit afin de l'utiliser avec Logical Domains Manager. Vous devez installer Solaris Security Toolkit sur le domaine de contrôle ; il s'agit de l'emplacement à partir duquel s'exécute le logiciel Logical Domains Manager. Vous pouvez également installer Solaris Security Toolkit sur les autres domaines logiques. La seule différence réside dans le fait que dans ce cas vous allez utiliser le pilote `ldm_control-secure.driver` pour sécuriser le domaine de contrôle et utiliser un autre pilote (tel que `secure.driver`) pour sécuriser les autres domaines logiques. En effet, le pilote `ldm_control-secure.driver` est propre au domaine de contrôle. `ldm_control-secure.driver` est basé sur le pilote `secure.driver` et a été personnalisé et testé afin d'être utilisé avec le logiciel Logical Domains Manager. Reportez-vous au *Solaris Security Toolkit 4.2 Reference Manual* pour en savoir plus sur le pilote `secure.driver`.

Sécurisation

Solaris Security Toolkit utilise le pilote (`ldm_control-secure.driver`) pour sécuriser le SE Solaris sur le domaine de contrôle ; ce pilote est spécialement adapté à l'exécution de Logical Domains Manager sous ce SE. Le pilote `ldm_control-secure.driver` est similaire au pilote `secure.driver` décrit dans le *Solaris Security Toolkit 4.2 Reference Manual*.

Le pilote `ldm_control-secure.driver` fournit une configuration de base au domaine de contrôle d'un système exécutant le logiciel Logical Domains Manager. Il est conçu pour fournir moins de services système qu'un pilote de domaine standard du SE Solaris, il réserve le domaine de contrôle pour les opérations du logiciel Logical Domains Manager et non pour des opérations d'ordre général.

Le script `install-ldm` installe (si ce n'est pas déjà fait) et active le logiciel Logical Domains Manager.

Vous trouverez ci-après un résumé des principales modifications effectuées par le pilote `secure.driver`.

- L'exécution du serveur Telnet est désactivée. Vous pouvez utiliser le shell sécurisé (`ssh`) à la place. Vous avez toujours la possibilité d'utiliser le client Telnet pour accéder aux consoles virtuelles lancées par le démon du serveur de terminal réseau virtuel Logical Domains (`vntsd`). Par exemple, pour accéder à une console virtuelle en cours d'exécution sur le système local et dont le port d'écoute est TCP 5001, entrez la commande suivante :

```
# telnet localhost 5001
```

Reportez-vous à la section « [Activation du démon de Logical Domains Manager](#) », [page 35](#) pour obtenir des instructions sur l'activation du démon `vntsd`. Il n'est pas activé automatiquement.

- Les scripts `finish` suivants ont été ajoutés. Ils permettent d'installer et de lancer Logical Domains Manager. Vous devez également ajouter certains de ces scripts aux pilotes personnalisés, d'autres en revanche sont facultatifs. Les scripts portent la mention Obligatoire ou Facultatif.
 - `install-ldm.fin` : installe le package `SUNWldm`. (*Obligatoire*)
 - `enable-ldmd.fin` : active le démon de Logical Domains Manager (`ldmd`). (*Obligatoire*)
 - `enable-ssh-root-login.fin` : permet aux superutilisateurs de se connecter directement via le shell sécurisé (`ssh`). (*Facultatif*)
- Les fichiers suivants ont été modifiés. Vous n'êtes pas obligé d'appliquer ces modifications à vos pilotes personnalisés, elles portent la mention « Facultatif ».
 - `/etc/ssh/sshd_config` : l'accès au compte racine est autorisé sur tout le réseau. Ce fichier n'est utilisé dans aucun pilote. (*Facultatif*)

- `/etc/ipf/ipf.conf` : le port UDP 161 (SNMP) est ouvert. (*Facultatif*)
- `/etc/host.allow` : le démon du shell sécurisé (`sshd`) est ouvert sur tout le réseau, pas seulement sur le sous-réseau local. (*Facultatif*)
- Les scripts `finish` suivants sont désactivés (commentés). Vous devez commenter le script `disable-rpc.fin` dans tous vos pilotes personnalisés. Les autres modifications sont facultatives. Les scripts portent la mention Obligatoire ou Facultatif.
 - `enable-ipfilter.fin` : indique que le filtre IP (filtre de paquets réseau) n'est pas activé. (*Facultatif*)
 - `disable-rpc.fin` : indique que le service RPC (Remote Procedure Call, appel de procédure à distance) reste activé. Le service RPC est utilisé par beaucoup d'autres services système, comme NIS (Network Information Service, service d'information réseau) et NFS (Network File System). (*Obligatoire*)
 - `disable-sma.fin` : indique que l'agent SMA (System Management Agent) (NET-SNMP) reste activé. (*Facultatif*)
 - `disable-ssh-root-login.fin` : indique que la connexion `ssh root` ne peut pas être désactivée.
 - `set-term-type.fin` : indique un script hérité inutile. (*Facultatif*)

Minimisation des domaines logiques

Vous pouvez configurer le SE Solaris avec un certain nombre de packages, en fonction de vos besoins. La minimisation permet de réduire au strict minimum le nombre de packages requis pour exécuter les applications souhaitées. Ce processus est important car il permet de réduire le nombre de logiciels susceptibles de présenter des risques et de limiter les tâches relatives à l'application des patches aux logiciels lorsque cela s'avère nécessaire. Le processus de minimisation d'un domaine logique prend en charge le logiciel JumpStart™ pour installer le SE Solaris minimisé avec tous les domaines.

Le logiciel Solaris Security Toolkit fournit un profil JumpStart (`minimal-ldm_control.profile`) pour minimiser le domaine logique pour LDoms, et installer tous les packages du SE Solaris pour prendre en charge LDoms et LDoms MIB. Pour utiliser LDoms MIB sur le domaine de contrôle, vous devez ajouter ce package séparément après avoir installé LDoms et Solaris Security Toolkit. Il n'est pas installé automatiquement avec les autres logiciels. Reportez-vous au *Guide d'administration Logical Domains (LDoms) Management Information Base (MIB) 1.0.1* pour plus d'informations sur l'installation et l'utilisation du logiciel LDoms MIB.

Autorisation

Il existe deux niveaux d'autorisation pour le logiciel Logical Domains Manager :

- Lecture seule : vous pouvez afficher, mais pas modifier la configuration.
- Lecture/Écriture : vous pouvez afficher et modifier la configuration.

Les modifications ne sont pas effectuées sur le SE Solaris, mais sont ajoutées au fichier d'autorisation par le script `postinstall` du package lors de l'installation de Logical Domains Manager. De la même façon, les entrées relatives aux autorisations sont supprimées par le script `preremove` du package.

Le tableau suivant contient la liste des sous-commandes `ldm` ainsi que l'autorisation utilisateur requise pour les exécuter.

TABEAU 2-1 Sous-commandes `ldm` et autorisations utilisateurs

Sous-commande <code>ldm</code> *	Autorisation utilisateur
<code>add-*</code>	<code>solaris.ldoms.write</code>
<code>bind-domain</code>	<code>solaris.ldoms.write</code>
<code>list</code>	<code>solaris.ldoms.read</code>
<code>list-*</code>	<code>solaris.ldoms.read</code>
<code>panic-domain</code>	<code>solaris.ldoms.write</code>
<code>remove-*</code>	<code>solaris.ldoms.write</code>
<code>set-*</code>	<code>solaris.ldoms.write</code>
<code>start-domain</code>	<code>solaris.ldoms.write</code>
<code>stop-domain</code>	<code>solaris.ldoms.write</code>
<code>unbind-domain</code>	<code>solaris.ldoms.write</code>

*. Fait référence à toutes les ressources que vous pouvez ajouter, répertorier, supprimer ou définir.

Audit

L'audit des commandes de CLI de Logical Domains Manager s'effectue via l'audit BSM du SE Solaris. Reportez-vous *System Administration Guide: Security Services* du Solaris 10 pour en savoir plus sur l'utilisation de l'audit BSM.

L'audit BSM n'est pas activé par défaut pour le logiciel Logical Domains Manager ; l'infrastructure est toutefois fournie. Il existe deux façons d'activer ce module :

- En exécutant le script `finish enable-bsm.fin` dans Solaris Security Toolkit.
- En utilisant la commande `bsmconv(1M)` du SE Solaris.

Pour en savoir plus sur l'activation, la vérification, la désactivation, l'impression et la rotation des journaux à l'aide de l'audit BSM via le logiciel Logical Domains Manager, reportez-vous à la section « [Activation et utilisation de l'audit BSM](#) », page 95.

Conformité

Solaris Security Toolkit dispose de ses propres fonctions d'audit. Ce logiciel peut valider automatiquement la sécurisation de tout système exécutant le SE Solaris en le comparant à un profil de sécurité prédéfini. Reportez-vous à la section « Auditing System Security » du *Solaris Security Toolkit 4.2 Administration Guide* pour en savoir plus sur la fonction de conformité.

Installation et activation du logiciel

Ce chapitre décrit comment installer et activer le logiciel Logical Domains Manager 1.0.1 et d'autres logiciels sur un domaine de contrôle, sur les serveurs pris en charge. Reportez-vous à la section « Serveurs pris en charge » des *Notes de version Logical Domains (LDoms) 1.0.1* pour obtenir la liste complète des serveurs pris en charge.

Consultez les informations qui vous intéressent dans ce chapitre en fonction de la plate-forme que vous utilisez. Si vous utilisez le logiciel Logical Domains sous la nouvelle plate-forme Sun UltraSPARC T2, ce logiciel a déjà été préinstallé en usine.

Ce chapitre couvre les rubriques suivantes :

- « [Mise à niveau vers la version 1.0.1 du logiciel LDoms](#) », page 15
- « [Installation du logiciel sur le domaine de contrôle](#) », page 17
- « [Téléchargement de Logical Domains Manager et de Solaris Security Toolkit](#) », page 21
- « [Installation de Logical Domains Manager et de Solaris Security Toolkit](#) », page 22
- « [Activation du démon de Logical Domains Manager](#) », page 35
- « [Création des profils et des autorisations et affectation de rôles aux comptes utilisateurs](#) », page 36

Mise à niveau vers la version 1.0.1 du logiciel LDoms

Les configurations LDoms version 1.0 existantes ne fonctionnent *pas* dans la version 1.0.1 du logiciel. Vous trouverez ci-après une procédure pour migrer les configurations de LDoms version 1.0 lors de la mise à jour vers la version 1.0.1 de ce logiciel.

▼ Pour effectuer une mise à niveau vers la version 1.0.1 du logiciel LDoms

La procédure suivante décrit une méthode pour enregistrer et reconstruire une configuration à l'aide de fichiers de contraintes XML et de l'option `-i` de la commande `ldm start-domain`. Cette méthode ne permet pas de conserver les liaisons, mais uniquement les contraintes utilisées pour les créer. Cela signifie qu'une fois cette procédure effectuée, les domaines disposent des mêmes ressources virtuelles, mais qu'ils ne sont pas forcément associés aux mêmes ressources physiques.

Le processus de base consiste à enregistrer les informations de contraintes de chaque domaine dans un fichier XML, puis de réexécuter ce fichier dans Logical Domains Manager une fois la mise à niveau effectuée, afin de reconstruire la configuration souhaitée. Cette procédure est valable pour les domaines hôtes, mais pas pour le domaine de contrôle. Vous pouvez enregistrer les contraintes du domaine de contrôle (`primary`) dans un fichier XML, mais vous ne pouvez pas le charger ensuite dans la commande `ldm start-domain -i`.

1. Effectuez une mise à jour vers la dernière version du SE Solaris. Pour plus d'informations, reportez-vous à l'étape 2, « [Procédure d'installation du SE Solaris 10](#) », page 18.
2. Créez un fichier de contraintes XML pour chaque domaine.

```
# ldm ls-constraints -x ldom > ldom.xml
```

3. Répertoriez toutes les configurations de domaines logiques enregistrées sur le contrôleur système.

```
# ldm ls-config
```

4. Supprimez toutes les configurations de domaines logiques enregistrées sur le contrôleur système.

```
# ldm rm-config config_name
```

5. Désactivez le démon de Logical Domains Manager (`ldmd`).

```
# svcadm disable ldmd
```

6. Supprimez le package Logical Domains Manager (`SUNWldm`).

```
# pkgrm SUNWldm
```


7. Supprimez le package Solaris Security Toolkit (SUNWjass) si vous utilisez ce logiciel.

```
# pkgrm SUNWjass
```

8. Effectuez une mise à jour instantanée du microprogramme système. Pour connaître la procédure complète, reportez-vous à la section « [Procédure de mise à niveau du microprogramme système](#) », page 19 ou « [Procédure de mise à niveau du microprogramme système sans serveur FTP](#) », page 20.
9. Téléchargez le package du logiciel LDoms 1.0.1.
Reportez-vous à la section « [Procédure de téléchargement de Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB](#) », page 21 pour connaître les procédures de téléchargement et d'installation des logiciels Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB.
10. Reconfigurez le domaine `primary` manuellement. Reportez-vous à la section « [Procédure de configuration du domaine de contrôle](#) », page 44 pour connaître la procédure.
11. Exécutez les commandes suivantes pour chaque fichier XML de domaine hôte créé à l'étape 2.

```
# ldm create -i ldom.xml  
# ldm bind-domain ldom  
# ldm start-domain ldom
```

Installation du logiciel sur le domaine de contrôle

Le domaine de contrôle est le premier domaine créé lors de l'installation du logiciel Logical Domains Manager. Ce domaine porte le nom de `primary` (vous ne pouvez pas modifier ce nom). Les composants principaux suivants sont installés sur le domaine de contrôle.

- Le SE Solaris 10. Ajoutez les patches indiqués dans les *Notes de version Logical Domains (LDoms) 1.0.1*, si nécessaire. Pour plus d'informations, reportez-vous à la section « [Procédure d'installation du SE Solaris 10](#) », page 18.
- La version 6.5 du microprogramme système pour la plate-forme Sun UltraSPARC T1 ou la version 7.0 pour la plate-forme Sun UltraSPARC T2. Pour plus d'informations, reportez-vous à la section « [Procédure de mise à niveau du microprogramme système](#) », page 19.

- Le logiciel Logical Domain Manager 1.0.1. Pour plus d'informations, reportez-vous à la section « [Installation de Logical Domains Manager et de Solaris Security Toolkit](#) », page 22.
- (Facultatif) Le logiciel Solaris Security Toolkit 4.2. Pour plus d'informations, reportez-vous à la section « [Installation de Logical Domains Manager et de Solaris Security Toolkit](#) », page 22.
- (Facultatif) Le package du logiciel Logical Domains (LDoms) Management Information Base (MIB). Reportez-vous au *Guide d'administration Logical Domains (LDoms) Management Information Base (MIB) 1.0.1* pour plus d'informations sur l'installation et l'utilisation du logiciel LDoms MIB.

Le SE Solaris et le microprogramme système doivent être installés sur le serveur avant le logiciel Logical Domains Manager. Une fois le SE Solaris, le microprogramme système et le logiciel Logical Domains Manager installés, le domaine d'origine devient le domaine de contrôle.

▼ Procédure d'installation du SE Solaris 10

Installez le SE Solaris 10 (si ce n'est pas déjà fait). Reportez-vous à la section « Logiciel requis » des *Notes de version Logical Domains (LDoms) 1.0.1* pour connaître le SE Solaris 10 à utiliser pour cette version du logiciel Logical Domains. Reportez-vous au guide d'installation du SE Solaris 10 pour obtenir toutes les instructions sur l'installation de ce système d'exploitation. Vous pouvez adapter l'installation aux besoins du système.

Remarque – Pour les domaines logiques, vous pouvez installer le SE Solaris uniquement sur un disque entier ou dans un fichier exporté en tant que périphérique en mode bloc.

1. **Installez le SE Solaris 10. Si vous utilisez le logiciel Solaris Security Toolkit, vous devez également effectuer l'opération suivante :**
 - a. **Sélectionnez `Entire Distribution` pour effectuer une installation classique ou `SUNWCall` pour effectuer une installation JumpStart.**
 - b. **Sélectionnez les paramètres régionaux `English, C`.**

Remarque – Si vous installez un système d'exploitation avec une langue autre que l'anglais dans un domaine hôte, le terminal de la console doit être affecté des paramètres régionaux requis par le programme d'installation du SE. Par exemple, le programme d'installation du SE Solaris peut nécessiter des codes EUC, et le programme d'installation de Linux des codes Unicode.

2. Si vous installez le SE Solaris 10 11/06, installez également les patches nécessaires. Reportez-vous à la section « Patchs SE Solaris 10 11/06 requis » des *Notes de version Logical Domains (LDoms) 1.0.1* pour obtenir la liste complète des patches requis.

▼ Procédure de mise à niveau du microprogramme système

Le microprogramme système de votre plate-forme est disponible sur le site SunSolve :

<http://sunsolve.sun.com>

Reportez-vous à la section « Patchs du microprogramme système requis » des *Notes de version Logical Domains (LDoms) 1.0.1* pour connaître les microprogrammes système à utiliser sur les serveurs pris en charge.

Cette procédure décrit comment mettre à niveau un microprogramme système à l'aide de la commande `flashupdate(1M)` sur le contrôleur système.

- Si vous n'avez pas accès à un serveur FTP local, reportez-vous à la section « [Procédure de mise à niveau du microprogramme système sans serveur FTP](#) », page 20.
- Pour mettre à jour le microprogramme système à partir du domaine de contrôle, reportez-vous aux notes de version du microprogramme système.

Reportez-vous aux guides d'administration ou aux notes sur le produit des serveurs pris en charge pour en savoir plus sur l'installation et la mise à jour des microprogrammes système de ces serveurs.

1. Arrêtez et mettez hors tension le serveur hôte à partir de l'un des ports de gestion connectés au contrôleur système : série ou réseau.

```
# shutdown -i5 -g0 -y
```

2. Utilisez la commande `flashupdate(1M)` pour mettre à niveau le microprogramme système, en fonction de votre serveur.

```
sc> flashupdate -s IP-address -f path/Sun_System_Firmware-  
x_x_build_mn-server-name.bin  
username: your-userid  
password: your-password
```

Dans cet exemple :

- *IP-address* représente l'adresse IP du serveur FTP.

- *path* représente l'emplacement sur le site SunSolve ou sur votre propre répertoire, à partir duquel vous pouvez obtenir l'image du microprogramme système.
- *x_x_x* représente le numéro de version du microprogramme système.
- *nn* représente le numéro de la build de cette version.
- *server-name* représente le nom du serveur. Par exemple, le *server-name* du serveur Sun Fire T2000 est *Sun_Fire_T2000*.

3. Réinitialisez le contrôleur système.

```
SC> resetsc -y
```

4. Allumez et initialisez le serveur hôte.

```
SC> poweron -c
ok boot disk
```

▼ Procédure de mise à niveau du microprogramme système sans serveur FTP

Si vous n'avez pas accès à un serveur FTP pour charger le microprogramme sur le contrôleur système, vous pouvez utiliser l'utilitaire `sysfwdownload` disponible sur le site SunSolve avec le package de mise à niveau du microprogramme système, à l'adresse suivante :

<http://sunsolve.sun.com>

1. Exécutez les commandes suivantes sous le SE Solaris.

```
# cd firmware_location
# sysfwdownload system_firmware_file
```

2. Arrêtez l'instance du SE Solaris.

```
# shutdown -i5 -g0 -y
```

3. Mettez le contrôleur système hors tension et mettez le microprogramme à niveau sur ce dernier.

```
SC> poweroff -fy
SC> flashupdate -s 127.0.0.1
```

4. Réinitialisez et mettez le contrôleur système sous tension.

```
sc> resetsc -y  
sc> poweron
```

▼ Procédure de mise à niveau inférieur de la version du microprogramme système

Une fois que vous avez mis à niveau le microprogramme système afin de l'utiliser avec le logiciel Logical Domains, vous pouvez le rétrograder vers le microprogramme d'origine, autre que ce logiciel.

- Exécutez la commande `flashupdate(1M)` et indiquez le chemin d'accès au microprogramme d'origine, autre que Logical Domains.

Téléchargement de Logical Domains Manager et de Solaris Security Toolkit

▼ Procédure de téléchargement de Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB

1. Téléchargez le fichier tar (`LDoms_Manager-1_0_1.zip`) contenant le package Logical Domains Manager (`SUNWldm`), le logiciel Solaris Security Toolkit (`SUNWjass`), le script d'installation (`install-lm`) et le package Logical Domains Management Information Base (`SUNWldmib.v`) à partir du site de téléchargement de logiciels de Sun. L'adresse est la suivante :

<http://www.sun.com/ldoms>

2. Dézippez le fichier zip.

```
$ unzip LDoms_Manager-1_0_1.zip
```

La structure du répertoire du logiciel téléchargé est similaire à celle-ci :

EXEMPLE DE CODE 3-1 Structure du répertoire du logiciel Logical Domains 1.0.1 téléchargé

```
LDoms_Manager-1_0_1/  
  Install/  
    install-ldm  
  Legal/  
    Ldoms_1.0.1_Entitlement.txt  
    Ldoms_1.0.1_SLA_Entitlement.txt  
  Product/  
    SUNWjass/  
    SUNWldm.v/  
    SUNWldmib.v  
  README
```

Installation de Logical Domains Manager et de Solaris Security Toolkit

Vous disposez de trois méthodes pour installer les logiciels Logical Domains Manager et Solaris Security Toolkit :

- Vous pouvez utiliser le script d'installation pour installer les packages et les patches. Les logiciels Logical Domains Manager et Solaris Security Toolkit sont alors tous deux installés automatiquement. Pour plus d'informations, reportez-vous à la section « [Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l'aide du script d'installation](#) », page 23.
- Vous pouvez utiliser JumpStart pour installer les packages. Pour plus d'informations, reportez-vous à la section « [Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l'aide de JumpStart](#) », page 30.
- Vous pouvez également installer chaque package manuellement. Pour plus d'informations, reportez-vous à la section « [Installation manuelle de Logical Domains Manager et de Solaris Security Toolkit](#) », page 32.

Remarque – N’oubliez pas que vous devez installer manuellement le package du logiciel LDomS MIB après avoir installé les packages LDomS et Solaris Security Toolkit. Il n’est pas installé automatiquement avec les autres packages. Reportez-vous au *Guide d’administration Logical Domains (LDomS) Management Information Base 1.0.1* pour plus d’informations sur l’installation et l’utilisation du logiciel LDomS MIB.

Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l’aide du script d’installation

Si vous choisissez d’utiliser le script d’installation `install-ldm`, plusieurs options vous sont offertes pour l’exécuter. Ces options sont décrites dans les procédures suivantes.

- **Si vous lancez le script `install-ldm` sans aucune option, il effectue les opérations suivantes automatiquement :**
 - Il vérifie que la version du SE Solaris est bien Solaris 10 11/06.
 - Il vérifie que les sous-répertoires `SUNWldm/` et `SUNWjass/` sont présents.
 - Il vérifie que les packages du pilote Solaris Logical Domains nécessaires, `SUNWldomr` et `SUNWldomu` sont présents.
 - Il vérifie que les packages `SUNWldm` et `SUNWjass` n’ont pas été installés.

Remarque – Si le script détecte une version antérieure de `SUNWjass` au cours de l’installation, vous devez alors la supprimer. Vous n’avez *pas* à annuler les sécurisations précédentes du SE Solaris.

- Il installe le logiciel Logical Domains Manager 1.0.1 (package `SUNWldm`).
- Il installe le logiciel Solaris Security Toolkit 4.2, ainsi que les patches nécessaires (package `SUNWjass`.)
- Il vérifie que tous les packages sont installés.
- Il active le démon de Logical Domains Manager (`ldmd`).
- Il sécurise le SE Solaris sur le domaine de contrôle à l’aide du pilote `ldm_control-secure.driver` du logiciel Solaris Security Toolkit ou de l’un des autres pilotes dont le nom se termine par `-secure.driver` que vous avez sélectionné.

- **Si vous lancez le script `install-ldm` avec l'option `-d`**, vous pouvez alors spécifier un pilote Solaris Security Toolkit autre que celui dont le nom se termine par `-secure.driver`. Le script exécute alors toutes les fonctions répertoriées précédemment et effectue également l'opération suivante :
 - Il sécurise le SE Solaris sur le domaine de contrôle à l'aide du pilote Solaris Security Toolkit personnalisé que vous avez spécifié ; par exemple : `server-secure-myname.driver`.
- **Si vous lancez le script `install-ldm` avec l'option `-d` en spécifiant `none`**, le SE Solaris exécuté sur le domaine de contrôle ne sera *pas* sécurisé à l'aide du logiciel Solaris Security Toolkit. Le script exécute toutes les fonctions répertoriées précédemment à l'exception de la sécurisation. Il est toutefois déconseillé de ne pas effectuer de sécurisation via le logiciel Solaris Security Toolkit, vous devez uniquement le faire si vous avez l'intention de sécuriser le domaine de contrôle à l'aide d'un autre processus.
- **Si vous lancez le script `install-ldm` avec l'option `-p`**, les seules opérations de post-installation effectuées sont l'activation du démon de Logical Domains Manager (`ldmd`) et l'exécution du logiciel Solaris Security Toolkit. Vous pouvez, par exemple, utiliser cette option si les packages `SUNWldm` et `SUNWjass` sont préinstallés sur le serveur. Reportez-vous à la section « [Procédure d'installation à l'aide du script `install-ldm` et de l'option `-p`](#) », page 29.

▼ Procédure d'installation à l'aide du script `install-ldm` sans aucune option

- **Exécutez le script d'installation sans aucune option.**

Le script d'installation se trouve dans le sous-répertoire `Install` du package `SUNWldm`.

```
# Install/install-ldm
```

- a. Si un ou plusieurs packages ont déjà été installés, vous recevez ce message :

```
# Install/install-ldm
ERROR: One or more packages are already installed: SUNWldm SUNWjass.
If packages SUNWldm.v and SUNWjass are factory pre-installed, run
install-ldm -p to perform post-install actions. Otherwise remove the
package(s) and restart install-ldm.
```

Si vous souhaitez effectuer des opérations de post-installation uniquement, passez à la section « [Procédure d'installation à l'aide du script `install-ldm` et de l'option `-p`](#) », page 29.

- b. À la fin du processus, vous recevez des messages semblables à ceux qui suivent.

- Le message de l'exemple de code 3-2 indique l'exécution correcte du script `install-ldm` si vous choisissez le profil de sécurité par défaut suivant :
 - a) Hardened Solaris configuration for LDOMs (recommended)
- Le message de l'exemple de code 3-3 indique l'exécution correcte du script `install-ldm` si vous choisissez le profil de sécurité par défaut suivant :
 - c) Your custom-defined Solaris security configuration profile

Les pilotes qui s'affichent sont ceux dont le nom se termine par `-secure.driver`. Pour indiquer un pilote personnalisé dont le nom ne se termine pas par `-secure.driver`, utilisez l'option `install-ldm -d`. (Reportez-vous à la section « [Procédure d'installation à l'aide du script `install-ldm` et de l'option `-d`](#) », page 27.)

EXEMPLE DE CODE 3-2 Exemple de message dans la configuration sécurisée Solaris pour LDOMs

```
# Install/install-ldm
Welcome to the LDOMs installer.

You are about to install the domain manager package that will enable
you to create, destroy and control other domains on your system. Given
the capabilities of the domain manager, you can now change the security
configuration of this Solaris instance using the Solaris Security
Toolkit.

Select a security profile from this list:

a) Hardened Solaris configuration for LDOMs (recommended)
b) Standard Solaris configuration
c) Your custom-defined Solaris security configuration profile

Enter a, b, or c [a]: a
The changes made by selecting this option can be undone through the
Solaris Security Toolkit's undo feature. This can be done with the
'/opt/SUNWjass/bin/jass-execute -u' command.

Installing LDOMs and Solaris Security Toolkit packages.
pkgadd -n -d "/var/tmp/install/Product/Logical_Domain_Manager" -a pkg_admin
SUNWldm.v
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWldm> was successful.
pkgadd -n -d "/var/tmp/install/Product/Solaris_Security_Toolkit" -a pkg_admin
SUNWjass
Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
```

EXEMPLE DE CODE 3-2 Exemple de message dans la configuration sécurisée Solaris pour LDoms (*suite*)

```
Installation of <SUNWjass> was successful.

Verifying that all packages are fully installed.  OK.
Enabling services: svc:/ldoms/ldmd:default
Running Solaris Security Toolkit 4.2.0 driver ldm_control-secure.driver.
Please wait. . .
/opt/SUNWjass/bin/jass-execute -q -d ldm_control-secure.driver
Executing driver, ldm_control-secure.driver
Solaris Security Toolkit hardening executed successfully; log file
/var/opt/SUNWjass/run/20070208142843/jass-install-log.txt.  It will not
take effect until the next reboot.  Before rebooting, make sure SSH or
the serial line is setup for use after the reboot.
```

EXEMPLE DE CODE 3-3 Exemple de message de choix de profil de configuration personnalisé

```
# Install/install-ldm
Welcome to the LDoms installer.

You are about to install the domain manager package that will enable
you to create, destroy and control other domains on your system. Given
the capabilities of the domain manager, you can now change the security
configuration of this Solaris instance using the Solaris Security
Toolkit.

Select a security profile from this list:

a) Hardened Solaris configuration for LDoms (recommended)
b) Standard Solaris configuration
c) Your custom-defined Solaris security configuration profile

Enter a, b, or c [a]: c
Choose a Solaris Security Toolkit .driver configuration profile from
this list
1) ldm_control-secure.driver
2) secure.driver
3) server-secure.driver
4) suncluster3x-secure.driver
5) sunfire_15k_sc-secure.driver

Enter a number 1 to 5: 2
The driver you selected may not perform all the LDoms-specific
operations specified in the LDoms Administration Guide.
Is this OK (yes/no)? [no] y
The changes made by selecting this option can be undone through the
Solaris Security Toolkit's undo feature. This can be done with the
'/opt/SUNWjass/bin/jass-execute -u' command.

Installing LDoms and Solaris Security Toolkit packages.
```

EXEMPLE DE CODE 3-3 Exemple de message de choix de profil de configuration personnalisé (*suite*)

```
pkgadd -n -d "/var/tmp/install/Product/Logical_Domain_Manager" -a pkg_admin
SUNWldm.v
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWldm> was successful.
pkgadd -n -d "/var/tmp/install/Product/Solaris_Security_Toolkit" -a pkg_admin
SUNWjass
Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWjass> was successful.

Verifying that all packages are fully installed. OK.
Enabling services: svc:/ldoms/ldmd:default
Running Solaris Security Toolkit 4.2.0 driver secure.driver.
Please wait. . .
/opt/SUNWjass/bin/jass-execute -q -d secure.driver
Executing driver, secure.driver
Solaris Security Toolkit hardening executed successfully; log file
/var/opt/SUNWjass/run/20070102142843/jass-install-log.txt. It will not
take effect until the next reboot. Before rebooting, make sure SSH or
the serial line is setup for use after the reboot.
```

▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-d`

- Exécutez le script d'installation avec l'option `-d` pour spécifier un pilote personnalisé Solaris Security Toolkit ; par exemple : `server-secure-myname.driver`.

Le script d'installation se trouve dans le sous-répertoire `Install` du package `SUNWldm`.

```
# Install/install-ldm -d server-secure-myname.driver
```

À la fin du processus, vous recevez des messages semblables à ceux de l'exemple de code 3-4.

EXEMPLE DE CODE 3-4 Exemple de message indiquant l'exécution correcte du script `install-ldm -d`

```
# Install/install-ldm -d server-secure.driver
The driver you selected may not perform all the LDoms-specific
operations specified in the LDoms Administration Guide.
Installing LDoms and Solaris Security Toolkit packages.
```

EXEMPLE DE CODE 3-4 Exemple de message indiquant l'exécution correcte du script `install-ldm -d` (suite)

```
pkgadd -n -d "/var/tmp/install/Product/Logical_Domain_Manager" -a pkg_admin
SUNWldm.v
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWldm> was successful.
pkgadd -n -d "/var/tmp/install/Product/Solaris_Security_Toolkit" -a pkg_admin
SUNWjass
Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWjass> was successful.

Verifying that all packages are fully installed. OK.
Enabling services: svc:/ldoms/ldmd:default
Running Solaris Security Toolkit 4.2.0 driver server-secure-myname.driver.
Please wait. . .
/opt/SUNWjass/bin/jass-execute -q -d server-secure-myname.driver
Executing driver, server-secure-myname.driver
Solaris Security Toolkit hardening executed successfully; log file
/var/opt/SUNWjass/run/20061114143128/jass-install-log.txt. It will not
take effect until the next reboot. Before rebooting, make sure SSH or
the serial line is setup for use after the reboot.
```

▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-d none`

- Exécutez le script d'installation avec l'option `-d none` pour ne *pas* sécuriser le système à l'aide d'un pilote Solaris Security Toolkit.

Le script d'installation se trouve dans le sous-répertoire `Install` du package `SUNWldm`.

```
# Install/install-ldm -d none
```

À la fin du processus, vous recevez des messages semblables à ceux indiqués dans l'exemple de code 3-5.

EXEMPLE DE CODE 3-5 Exemple de message indiquant l'exécution correcte du script `install-ldm -d none`

```
# Install/install-ldm -d none
Installing LDoms and Solaris Security Toolkit packages.
pkgadd -n -d "/var/tmp/install/Product/Logical_Domain_Manager" -a pkg_admin
SUNWldm.v
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
```

EXEMPLE DE CODE 3-5 Exemple de message indiquant l'exécution correcte du script `install-ldm -d none`

```
Installation of <SUNWldm> was successful.
pkgadd -n -d "/var/tmp/install/Product/Solaris_Security_Toolkit" -a pkg_admin
SUNWjass
Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Installation of <SUNWjass> was successful.

Verifying that all packages are fully installed. OK.
Enabling services: svc:/ldoms/ldmd:default
Solaris Security Toolkit was not applied. Bypassing the use of the
Solaris Security Toolkit is not recommended and should only be
performed when alternative hardening steps are to be taken.
```

▼ Procédure d'installation à l'aide du script `install-ldm` et de l'option `-p`

Si les packages `SUNWldm` et `SUNWjass` sont préinstallés sur le serveur, vous pouvez utiliser cette option pour lancer les opérations de post-installation consistant à activer le démon de Logical Domains Manager (`ldmd`) et à exécuter le logiciel Solaris Security Toolkit.

- Exécutez le script d'installation avec l'option `-p` pour effectuer les opérations de post-installation consistant à activer `ldmd` et à exécuter le logiciel Solaris Security Toolkit pour sécuriser le système.

```
# Install/install-ldm -p
Verifying that all packages are fully installed. OK.
Enabling services: svc:/ldoms/ldmd:default
Running Solaris Security Toolkit 4.2.0 driver ldm_control-secure.driver.
Please wait. . .
/opt/SUNWjass/bin/jass-execute -q -d ldm_control-secure.driver
Solaris Security Toolkit hardening executed successfully; log file
var/opt/SUNWjass/run/20070515140944/jass-install-log.txt. It will not
take effect until the next reboot. Before rebooting, make sure SSH or
the serial line is setup for use after the reboot.
```

Installation des logiciels Logical Domains Manager 1.0.1 et Solaris Security Toolkit 4.2 à l'aide de JumpStart

Reportez-vous au manuel *JumpStart Technology: Effective Use in the Solaris Operating Environment* pour obtenir toutes les informations sur l'utilisation de JumpStart.



Attention – Ne vous déconnectez *pas* de la console virtuelle durant une installation réseau.

▼ Procédure d'installation d'un serveur JumpStart

- Si vous avez déjà installé un serveur JumpStart, passez à la section « [Procédure d'installation à l'aide du logiciel JumpStart](#) », [page 31](#) du guide d'administration.
- Si vous n'avez pas encore installé de serveur JumpStart, vous devez le faire.

Reportez-vous au *Solaris 10 11/06 Installation Guide: Custom JumpStart and Advanced Installation* pour obtenir toutes les informations sur cette procédure. Ce guide d'installation est disponible à l'adresse suivante :

<http://docs.sun.com/app/docs/doc/819-6397>

1. **Reportez-vous au chapitre 3 « Preparing Custom JumpStart Installations (Tasks) » du *Solaris 10 11/06 Installation Guide: Custom JumpStart and Advanced Installation*, et effectuez les opérations suivantes.**
 - a. **Consultez la liste des tâches de la section « Task Map: Preparing Custom JumpStart Installations ».**
 - b. **Configurez les systèmes réseau en suivant les procédures de la section « Creating a Profile Server for Network Systems ».**
 - c. **Créez le fichier `rules` en suivant les procédures de la section « Creating the rules File ».**
2. **Validez le fichier `rules` en suivant les procédures de la section « Validating the rules File ».**

Le logiciel Solaris Security Toolkit fournit les profils et les scripts finish. Reportez-vous au document *Solaris Security Toolkit 4.2 Reference Manual* pour plus d'informations sur les profils et les scripts finish.

▼ Procédure d'installation à l'aide du logiciel JumpStart

1. Allez dans le répertoire dans lequel vous avez téléchargé le package Solaris Security Toolkit (SUNWjass).

```
# cd /path-to-download
```

2. Installez le logiciel SUNWjass afin de créer la structure de répertoire JumpStart (jumpstart).

```
# pkgadd -R /jumpstart -d . SUNWjass
```

3. À l'aide de votre éditeur de texte, modifiez le fichier /jumpstart/opt/SUNWjass/Sysidcfg/Solaris_10/sysidcfg en fonction de votre environnement réseau.
4. Copiez le fichier /jumpstart/opt/SUNWjass/Drivers/user.init.SAMPLE dans le fichier /jumpstart/opt/SUNWjass/Drivers/user.init.

```
# cp user.init.SAMPLE user.init
```

5. Modifiez le fichier user.init en fonction des chemins d'accès.
6. Pour installer le package Solaris Security Toolkit (SUNWjass) sur le système cible lors d'une installation JumpStart, placez-le dans le répertoire JASS_PACKAGE_MOUNT défini dans le fichier user.init. Par exemple :

```
# cp -r /path/to/LDoms_Manager-1_0_1/Product/SUNWjass  
/jumpstart/opt/SUNWjass/Packages
```

7. Pour installer le package Solaris Security Toolkit (SUNWldm.v) sur le système cible lors d'une installation JumpStart, placez-le dans le répertoire JASS_PACKAGE_MOUNT défini dans le fichier user.init à partir de la zone de téléchargement. Par exemple :

```
# cp -r /path/to/LDoms_Manager-1_0_1/Product/SUNWldm.v  
/jumpstart/opt/SUNWjass/Packages
```

8. En cas de problème avec un serveur JumpStart multiréseau, modifiez les deux entrées suivantes dans le fichier user.init : JASS_PACKAGE_MOUNT et JASS_PATCH_MOUNT afin d'indiquer le chemin d'accès correct aux répertoires JASS_HOME_DIR/Patches et JASS_HOME_DIR/Packages. Reportez-vous au fichier user.init.SAMPLE pour plus d'informations.

9. Utilisez le pilote de base `ldm_control-secure.driver` pour le domaine de contrôle de Logical Domains Manager.

Reportez-vous au chapitre 4 du *Solaris Security Toolkit 4.2 Reference Manual* pour en savoir plus sur la modification et l'utilisation de ce pilote. `secure.driver` est le pilote principal du logiciel Solaris Security Toolkit, il est l'homologue du pilote `ldm_control-secure.driver`.

10. Une fois les modifications du pilote `ldm_control-secure.driver` effectuées, indiquez une entrée correcte dans le fichier de règles.

- Pour minimiser le domaine de contrôle de LDoms, entrez une ligne `minimal-ldm-control.profile` dans le fichier de règles, semblable à celle-ci :

```
hostname imbulu - Profiles/minimal-ldm_control.profile Drivers/ldm_control-secure-abc.driver
```

Remarque – N'oubliez pas que vous devez installer manuellement le package du logiciel LDoms MIB après avoir installé les packages LDoms et Solaris Security Toolkit. Il n'est pas installé automatiquement avec les autres packages. Reportez-vous au *Guide d'administration Logical Domains (LDoms) Management Information Base 1.0.1* pour plus d'informations sur l'installation et l'utilisation du logiciel LDoms MIB.

- Si vous ne souhaitez pas minimiser le domaine de contrôle de LDoms, entrez une ligne dans le fichier, semblable à celle-ci :

```
hostname imbulu - Profiles/oem.profile Drivers/ldm_control-secure-abc.driver
```

11. En cas d'annulation de la sécurisation lors d'une installation JumpStart, vous devez exécuter la commande SMF pour redémarrer le logiciel Logical Domains Manager.

```
# svcadm enable svc:/ldoms/ldmd:default
```

Installation manuelle de Logical Domains Manager et de Solaris Security Toolkit

Effectuez les procédures décrites dans les sections ci-après pour installer manuellement les logiciels Logical Domains Manager et Solaris Security Toolkit :

- « [Procédure d'installation manuelle du logiciel Logical Domains Manager \(LDoms\) 1.0.1](#) », page 33.
- « (Facultatif) [Procédure d'installation manuelle du logiciel Solaris Security Toolkit 4.2](#) », page 33.

- « (Facultatif) Procédure de sécurisation manuelle du domaine de contrôle », page 34.

▼ Procédure d'installation manuelle du logiciel Logical Domains Manager (LDoms) 1.0.1

Téléchargez le logiciel Logical Domains Manager 1.0.1, le package `SUNWldm` à partir du site de téléchargement de logiciels de Sun. Reportez-vous à la section « [Procédure de téléchargement de Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB](#) », page 21 pour obtenir des instructions spécifiques sur le téléchargement de logiciel.

1. Utilisez la commande `pkgadd(1M)` pour installer le package `SUNWldm.v`. Utilisez l'option `-G` pour installer le package dans la zone globale.

```
# pkgadd -Gd . SUNWldm.v
```

2. Répondez `y` (yes) à toutes les questions qui s'affichent dans les fenêtres interactives.
3. Utilisez la commande `pkginfo(1)` pour vérifier que le package `SUNWldm` du logiciel Logical Domains Manager 1.0.1 est bien installé.
Le message obtenu suite à cette commande (REV) est semblable à celui-ci.

```
# pkginfo -l SUNWldm | grep VERSION
VERSION=1.0.1,REV=2007.08.23.10.20
```

▼ (Facultatif) Procédure d'installation manuelle du logiciel Solaris Security Toolkit 4.2

Si vous souhaitez sécuriser le système, téléchargez et installez le package `SUNWjass`. Les patches nécessaires (122608-03 et 125672-01) sont inclus dans le package `SUNWjass`. Reportez-vous à la section « [Procédure de téléchargement de Logical Domains Manager, Solaris Security Toolkit et Logical Domains MIB](#) », page 21 pour obtenir des instructions spécifiques sur le téléchargement de logiciel.

Reportez-vous au [chapitre 2](#) de ce document pour en savoir plus sur les considérations relatives à la sécurité lors de l'utilisation du logiciel Logical Domains Manager. Vous pouvez obtenir des informations supplémentaires dans la documentation sur Solaris Security Toolkit 4.2, disponible à l'adresse suivante :

<http://docs.sun.com>

1. Utilisez la commande `pkgadd(1M)` pour installer le package `SUNWjass`.

```
# pkgadd -d . SUNWjass
```

2. Utilisez la commande `pkginfo(1)` pour vérifier que le package `SUNWjass` du logiciel Solaris Security Toolkit 4.2 est bien installé.

```
# pkginfo -l SUNWjass | grep VERSION
VERSION: 4.2.0
```

▼ (Facultatif) Procédure de sécurisation manuelle du domaine de contrôle

Effectuez la procédure suivante uniquement si vous avez installé le package Solaris Security Toolkit 4.2.

Remarque – Lorsque vous sécurisez le domaine de contrôle à l’aide du logiciel Solaris Security Toolkit, vous devez désactiver plusieurs services du système et restreindre l’accès réseau. Reportez-vous à la section « [Documentation connexe](#) », [page xix](#) de ce guide pour rechercher des documents sur Solaris Security Toolkit 4.2 et obtenir plus d’informations.

1. Sécurisez le système à l’aide du pilote `ldm_control-secure.driver`.

```
# /opt/SUNWjass/bin/jass-execute -d ldm_control-secure.driver
```

Vous pouvez utiliser d’autres pilotes pour sécuriser le système. Vous pouvez également personnaliser les pilotes et les adapter en fonction des besoins de sécurité de l’environnement. Reportez-vous au *Solaris Security Toolkit 4.2 Reference Manual* pour plus d’informations sur les pilotes et leur personnalisation.

2. Répondez `y` (yes) à toutes les questions qui s’affichent dans les fenêtres interactives.
3. Arrêtez, puis redémarrez le serveur pour appliquer la sécurisation.

```
# /usr/sbin/shutdown -y -g0 -i6
```

▼ Procédure de validation de la sécurisation

- Vérifiez que la sécurisation a bien été effectuée par le pilote de sécurisation de Logical Domains (`ldom_control-secure.driver`).

Si vous voulez vérifier via un autre pilote, remplacez le nom du pilote comme indiqué dans cet exemple de commande :

```
# /opt/SUNWjass/bin/jass-execute -a ldom_control-secure.driver
```

▼ Procédure d'annulation de la sécurisation

1. Annulez les modifications de configuration appliquées par le logiciel Solaris Security Toolkit.

```
# /opt/SUNWjass/bin/jass-execute -u
```

Solaris Security Toolkit vous demande d'indiquer les sécurisations à annuler.

2. Sélectionnez les sécurisations à annuler.
3. Redémarrez le système pour appliquer la configuration non sécurisée.

```
# /usr/sbin/shutdown -y -g0 -i6
```

Remarque – En cas d'annulation d'une sécurisation effectuée lors d'une installation JumpStart, vous devez exécuter les commandes SMF pour redémarrer le logiciel Logical Domains Manager et le démon du serveur de terminal réseau virtuel.

```
# svcadm enable svc:/ldoms/ldmd:default
```

Activation du démon de Logical Domains Manager

Le script d'installation `install-ldm` active automatiquement le démon de Logical Domains Manager (`ldmd`). Si vous avez installé manuellement le logiciel Logical Domains Manager, vous devez activer le démon correspondant, `ldmd`. Ce démon vous permet de créer, de modifier et de contrôler les domaines logiques.

▼ Procédure d'activation du démon de Logical Domains Manager

1. Utilisez la commande `svcadm(1M)` pour activer le démon de Logical Domains Manager `ldmd`.

```
# svcadm enable ldmd
```

2. Utilisez la commande `ldm list` pour vérifier l'exécution de Logical Domains Manager.

Vous recevez un message similaire à celui qui suit, qui correspond à une configuration `factory-default`. Vous pouvez noter que l'état du domaine `primary` est `active`, ce qui signifie que Logical Domains Manager est en cours d'exécution.

```
# /opt/SUNWldm/bin/ldm list
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	---c-	SP	32	3264M	0.3%	19d 9m

Création des profils et des autorisations et affectation de rôles aux comptes utilisateurs

Pour définir des autorisations et des profils et affecter des rôles aux comptes utilisateurs, vous devez utiliser le RBAC (Role-Based Access Control, contrôle d'accès basé sur les rôles) du SE Solaris adapté au logiciel Logical Domains Manager. Reportez-vous au document « Solaris 10 System Administrator Collection » pour en savoir plus sur le RBAC.

Il existe deux niveaux d'autorisation pour le logiciel Logical Domains Manager :

- Lecture seule : vous pouvez afficher, mais pas modifier la configuration.
- Lecture/Écriture : vous pouvez afficher et modifier la configuration.

Les entrées relatives à Logical Domains indiquées ci-après sont ajoutées automatiquement au fichier `/etc/security/auth_attr` du SE Solaris :

- `solaris.ldoms:::LDom administration::`
- `solaris.ldoms.grant:::Delegate LDom configuration::`
- `solaris.ldoms.read:::View LDom configuration::`

■ `solaris.ldoms.write:::Manage LDom configuration::`

Gestion des autorisations utilisateurs

▼ Procédure d'attribution d'une autorisation à un utilisateur

Suivez les étapes suivantes pour attribuer des autorisations aux utilisateurs de Logical Domains Manager dans le fichier `/etc/security/auth_attr`. Le superutilisateur dispose déjà des autorisations `solaris.*`, et dispose par conséquent des autorisations `solaris.ldoms.*`.

1. **Créez un compte utilisateur local pour chaque utilisateur devant utiliser les sous-commandes `ldm(1M)`.**

Remarque – Pour attribuer des autorisations Logical Domains Manager à un utilisateur, vous devez créer un compte local (non LDAP) pour ce dernier. Reportez-vous au document « Solaris 10 System Administrator Collection » pour plus d'informations à ce sujet.

2. **Effectuez l'une des opérations suivantes en fonction des sous-commandes `ldm(1M)` auxquelles vous souhaitez donner accès à l'utilisateur.**

Reportez-vous au [TABLEAU 2-1](#) pour obtenir la liste des commandes `ldm(1M)` et connaître les autorisations utilisateurs correspondantes.

- Attribuez une autorisation en lecture seule à un utilisateur à l'aide de la commande `usermod(1M)`.

```
# usermod -A solaris.ldoms.read username
```

- Attribuez une autorisation en lecture/écriture à un utilisateur à l'aide de la commande `usermod(1M)`.

```
# usermod -A solaris.ldoms.write username
```

▼ Procédure de suppression de toutes les autorisations attribuées à un utilisateur

- Supprimez toutes les autorisations du compte utilisateur local (seule solution possible).

```
# usermod -A `` username
```

Gestion des profils utilisateurs

Le package SUNWldm ajoute deux profils RBAC définis par le système au fichier `/etc/security/prof_attr` afin de permettre aux non-superutilisateurs d'accéder à Logical Domains Manager. Les deux profils spécifiques à LDoms sont les suivants :

- LDoms Review:::Review LDoms configuration:auths=solaris.ldoms.read
- LDoms Management:::Manage LDoms domains:auths=solaris.ldoms.*

Vous pouvez attribuer l'un de ces profils à un compte utilisateur en suivant la procédure décrite ci-après.

▼ Procédure d'attribution d'un profil à un utilisateur

- Attribuez un profil d'administration à un compte utilisateur local, LDoms Management, par exemple.

```
# usermod -P "LDoms Management" username
```

▼ Procédure de suppression de tous les profils attribués à un utilisateur

- Supprimez tous les profils du compte utilisateur local (seule solution possible).

```
# usermod -P `` username
```

Attribution de rôles aux utilisateurs

Cette procédure présente l'avantage d'autoriser uniquement l'utilisateur auquel un rôle spécifique a été attribué à assumer ce rôle. Ainsi, un mot de passe est requis si le rôle nécessite également un mot de passe. Cette procédure garantit donc deux niveaux de sécurité. Si un rôle n'a pas été attribué à un utilisateur, ce dernier ne peut pas assumer ce rôle (en exécutant la commande `su role_name`) même s'il dispose du mot de passe correct.

▼ Procédure de création d'un rôle et d'attribution à un utilisateur

1. Créez un rôle.

```
# roleadd -A solaris.ldoms.read ldm_read
```

2. Attribuez un mot de passe à ce rôle.

```
# passwd ldm_read
```

3. Attribuez ce rôle à un utilisateur ; par exemple, `user_1`.

```
# useradd -R ldm_read user_1
```

4. Attribuez un mot de passe à l'utilisateur (`user_1`).

```
# passwd user_1
```

5. Attribuez l'accès au compte `user_1` uniquement afin qu'il devienne le compte `ldm_read`.

```
# su user_1
```

6. Entrez le mot de passe utilisateur si vous êtes invité à le faire.

7. Vérifiez l'ID utilisateur et l'accès au rôle `ldm_read`.

```
$ id
uid=nn(user_1) gid=nn(<group name>)
$ roles
ldm_read
```

8. Autorisez l'utilisateur à accéder aux sous-commandes `ldm` ayant des autorisations en lecture.

```
# su ldm_read
```

9. Entrez le mot de passe utilisateur si vous êtes invité à le faire.

10. Entrez la commande `id` pour indiquer l'utilisateur.

```
$ id  
uid=nn(ldm_read) gid=nn(<group name>)
```


Configuration des services et des domaines logiques

Ce chapitre décrit les procédures requises pour configurer les services par défaut, le domaine de contrôle et les domaines hôtes :

- « Création des services par défaut », page 42
- « Configuration initiale du domaine de contrôle », page 44
- « Redémarrage et utilisation des domaines logiques », page 46
- « Activation de la mise en réseau du domaine de contrôle/service et des autres domaines », page 47
- « Activation du démon du serveur de terminal réseau virtuel », page 48
- « Création et lancement d'un domaine hôte », page 49
- « Installation JumpStart sur un domaine hôte », page 53

Messages des commandes

En fonction de votre plate-forme, différents messages s'affichent suite aux commandes que vous utilisez pour créer les services par défaut et configurer le domaine de contrôle (`primary`) :

- processeurs Sun UltraSPARC T1 ;
- processeurs Sun UltraSPARC T2.

Processeurs Sun UltraSPARC T1

Si votre serveur est doté d'un processeur Sun UltraSPARC T1, vous recevez le message suivant après l'exécution de la commande setup pour le domaine primary :

```
Notice: the LDom Manager is running in configuration mode. Any
configuration changes made will only take effect after the machine
configuration is downloaded to the system controller and the host
is reset.
```

Processeurs Sun UltraSPARC T2

Première opération : si votre serveur est doté d'un processeur Sun UltraSPARC T2, vous recevez le message suivant après la première opération sur un périphérique quelconque ou suite au lancement d'un service sur le domaine primary :

```
Initiating delayed reconfigure operation on LDom primary. All
configuration changes for other LDom s are disabled until the
LDom reboots, at which time the new configuration for LDom
primary will also take effect.
```

Opérations suivantes jusqu'au redémarrage : si votre serveur est doté d'un processeur Sun UltraSPARC T2, vous recevez le message suivant après chaque opération sur le domaine primary, et ce jusqu'à ce que vous redémarriez :

```
Notice: LDom primary is in the process of a delayed
reconfiguration. Any changes made to this LDom will only take
effect after it reboots.
```

Création des services par défaut

Vous devez au préalable créer les services virtuels par défaut suivants pour pouvoir les utiliser par la suite :

- vdiskserver : virtual disk server, serveur de disque virtuel ;
- vswitch : virtual switch service, service de commutateur virtuel ;
- vconscon : virtual console concentrator service, service de concentrateur de consoles virtuelles.

▼ Procédure de création des services par défaut :

1. **Créez un serveur de disque virtuel (vds) afin de pouvoir importer des disques virtuels dans un domaine logique.**

La commande suivante, par exemple, ajoute un serveur de disque virtuel (primary-vds0) au domaine de contrôle (primary).

```
primary$ ldm add-vds primary-vds0 primary
```

2. **Créez un service de concentrateur de consoles virtuelles (vcc) qui sera utilisé par le démon du serveur de terminal réseau virtuel (vntsd) et en tant que concentrateur pour toutes les consoles du domaine logique.**

La commande suivante, par exemple, ajoute un service de concentrateur de consoles virtuelles (primary-vcc0) avec une plage de numéros de port allant de 5 000 à 5 100 au domaine de contrôle (primary).

```
primary$ ldm add-vcc port-range=5000-5100 primary-vcc0 primary
```

3. **Créez un service de commutateur virtuel (vsw) pour activer la mise en réseau des périphériques réseau virtuels (vnet) dans des domaines logiques. Affectez un adaptateur réseau conforme à la norme GLDv3 au commutateur virtuel si chaque domaine logique doit communiquer vers l'extérieur via le commutateur virtuel.**

La commande suivante, par exemple, ajoute un service de commutateur virtuel (primary-vsw0) sur le pilote de l'adaptateur réseau e1000g0 du domaine de contrôle (primary).

```
primary$ ldm add-vsw net-dev=e1000g0 primary-vsw0 primary
```

Cette commande affecte automatiquement une adresse MAC au commutateur virtuel. Vous pouvez, si vous le souhaitez, indiquer votre propre adresse MAC dans la commande `ldm add-vsw`. Sachez toutefois que dans ce cas vous devez vous assurer que l'adresse MAC indiquée n'entre pas en conflit avec une adresse MAC existante.

Si le commutateur virtuel que vous avez ajouté remplace l'adaptateur physique sous-jacent en tant qu'interface de réseau principale, vous devez lui affecter l'adresse MAC de l'adaptateur physique, afin que le serveur DHCP (Dynamic Host Configuration Protocol) puisse affecter la même adresse IP au domaine. Pour plus d'informations, reportez-vous à la section « [Activation de la mise en réseau du domaine de contrôle/service et des autres domaines](#) », page 47.

```
primary$ ldm add-vsw mac-addr=2:04:4f:fb:9f:0d net-dev=e1000g0 primary-vsw0  
primary
```

4. Vérifiez que les services ont bien été créés à l'aide de la sous-commande `list-services`. Le contenu de votre message doit ressembler à celui-ci :

```
primary$ ldm list-services primary
```

VDS						
NAME	VOLUME	OPTIONS	DEVICE			
primary-vds0						
VCC						
NAME	PORT-RANGE					
primary-vcc0	5000-5100					
VSW						
NAME	MAC	NET-DEV	DEVICE	MODE		
primary-vsw0	02:04:4f:fb:9f:0d	e1000g0	switch@0	prog,promisc		

Configuration initiale du domaine de contrôle

À l'origine, toutes les ressources système sont affectées au domaine de contrôle. Pour pouvoir créer d'autres domaines logiques, vous devez libérer certaines de ces ressources.

Remarque – Les messages signalant que LDoms Manager s'exécute en mode de configuration dans les exemples suivants s'appliquent uniquement aux processeurs Sun UltraSPARC T1.

▼ Procédure de configuration du domaine de contrôle

Remarque – Cette procédure contient des exemples de ressources à configurer pour votre domaine de contrôle. Il s'agit uniquement d'exemples et les valeurs indiquées ne sont pas forcément appropriées à votre domaine de contrôle.

1. Affectez des ressources cryptographiques au domaine de contrôle.

Remarque – Si le domaine de contrôle contient des périphériques cryptographiques, vous ne pouvez pas reconfigurer dynamiquement les CPU. S’il ne contient pas de périphériques cryptographiques, définissez `set-mau` sur 0.

Dans l’exemple suivant, une ressource cryptographique est affectée au domaine de contrôle `primary`. Les autres ressources cryptographiques restent ainsi disponibles pour un domaine hôte.

```
primary$ ldm set-mau 1 primary
```

2. Affectez des CPU virtuelles au domaine de contrôle.

Dans la commande suivante, par exemple, 4 CPU virtuelles sont affectées au domaine de contrôle `primary`. Les autres CPU virtuelles restent ainsi disponibles pour un domaine hôte.

```
primary$ ldm set-vcpu 4 primary
```

3. Affectez de la mémoire au domaine de contrôle.

Dans la commande suivante, par exemple, 1 Go de mémoire est affecté au domaine de contrôle `primary`. La quantité de mémoire restante demeure ainsi disponible pour un domaine hôte.

```
primary$ ldm set-memory 1G primary
```

Remarque – Si vous n’utilisez pas le système de fichiers ZFS pour accéder aux services de disque, 1 Go de mémoire doit suffire. Si vous utilisez ce système de fichiers, vous devez alors affecter un noyau complet de 4 CPU virtuelles et au minimum 4 Go de mémoire. Vous devrez peut-être affecter des noyaux complets supplémentaires en cas de charge d’E/S plus élevée.

4. Ajoutez une configuration d’ordinateur de domaine logique au SC (System Controller, contrôleur système).

La commande suivante, par exemple, ajoute une configuration appelée `initial`.

```
primary$ ldm add-config initial
```

Remarque – Actuellement, 8 configurations au maximum peuvent être enregistrées sur le SC (configuration `factory-default` non comprise).

5. Vérifiez que la configuration est prête à être utilisée au prochain redémarrage.

```
primary$ ldm list-config  
factory-default [current]  
initial [next]
```

Cette sous-commande `list` indique que la configuration `factory-default` est actuellement utilisée et que la configuration `initial` sera utilisée après le redémarrage.

Redémarrage et utilisation des domaines logiques

Vous devez redémarrer le domaine de contrôle/service pour que les modifications apportées prennent effet et que les ressources soient libérées afin d'être utilisées par d'autres domaines logiques.

▼ Procédure de redémarrage et d'utilisation des domaines logiques

- Arrêtez, puis redémarrez le domaine `primary` (il s'agit également du domaine de service cité dans nos exemples).

```
primary# shutdown -y -g0 -i6
```

Remarque – Si vous utilisez la commande indiquée pendant le redémarrage, les modifications apportées prennent alors effet ; le message de la commande `ldm list-config` est identique à celui affiché avant le redémarrage. Une mise hors et sous tension est requise pour que la commande `ldm list-config` mette à jour la configuration affichée.

Activation de la mise en réseau du domaine de contrôle/service et des autres domaines

Par défaut, la mise en réseau du domaine de contrôle/service et des autres domaines du système est désactivée. Pour l'activer, le périphérique commutateur virtuel doit être configuré en tant que périphérique réseau. Le commutateur virtuel peut soit remplacer le périphérique physique sous-jacent (e1000g0 dans cet exemple) en tant qu'interface principale, soit être configuré en tant qu'interface réseau supplémentaire dans le domaine.

Remarque – Vous devez effectuer les différentes étapes de configuration suivantes à partir de la console du domaine ; en effet, ces opérations sont susceptibles d'interrompre momentanément la connexion réseau du domaine.

▼ Procédure de configuration du commutateur

1. Imprimez les informations d'adresses pour toutes les interfaces.

```
primary# ifconfig -a
```

2. Associez le commutateur virtuel. Dans cet exemple, vsw0 est le commutateur virtuel configuré.

```
primary# ifconfig vsw0 plumb
```

3. (Facultatif) Pour obtenir la liste de toutes les instances de commutateurs virtuels présentes dans un domaine, entrez la commande suivante :

```
primary# /usr/sbin/dladm show-link | grep vsw
vsw0                type: non-vlan  mtu: 1500          device: vsw0
```

4. Annulez l'association du périphérique réseau physique affecté au commutateur virtuel (net-dev), e1000g0 dans cet exemple.

```
primary# ifconfig e1000g0 down unplumb
```

5. Pour migrer les propriétés du périphérique réseau physique (e1000g0) vers le périphérique commutateur virtuel (vsw0), entrez l'une des commandes suivantes :

- Si la mise en réseau est configurée via une adresse IP statique, utilisez cette adresse et le masque de réseau e1000g0 pour vsw0.

```
primary# ifconfig vsw0 IP_of_e1000g0 netmask netmask_of_e1000g0 broadcast + up
```

- Si la mise en réseau est configurée via DHCP, activez DHCP pour vsw0.

```
primary# ifconfig vsw0 dhcp start
```

6. Apportez les modifications nécessaires au fichier de configuration afin qu'elles prennent effet.

```
primary# mv /etc/hostname.e1000g0 /etc/hostname.vsw0
primary# mv /etc/dhcp.e1000g0 /etc/dhcp.vsw0
```

Remarque – Le cas échéant, vous pouvez également configurer le commutateur virtuel ainsi que le périphérique réseau physique. Dans ce cas, associez le commutateur virtuel comme indiqué à l'étape 2 et n'annulez pas l'association du périphérique physique (ignorez l'étape 4). Le commutateur virtuel doit ensuite être configuré via une adresse IP statique ou via une adresse IP dynamique à partir d'un serveur DHCP.

Activation du démon du serveur de terminal réseau virtuel

Vous devez activer le démon du serveur de terminal réseau virtuel (vntsd) pour permettre à chaque domaine logique d'accéder à la console virtuelle. Reportez-vous au « Solaris 10 OS Reference Manual » ou à la page de manuel vntsd(1M) pour en savoir plus sur l'utilisation de ce démon.

▼ Procédure d'activation du démon du serveur de terminal réseau virtuel

Remarque – Vérifiez que vous avez bien créé le service par défaut `vconscon` sur le domaine de contrôle avant d'activer `vntsd`. Reportez-vous à la section « [Création des services par défaut](#) », page 42 pour plus d'informations à ce sujet.

1. Utilisez la commande `svcadm(1M)` pour activer le démon du serveur de terminal réseau virtuel `vntsd(1M)`.

```
# svcadm enable vntsd
```

2. Utilisez la commande `svcs(1)` pour vérifier que `vntsd` est activé.

```
# svcs -l vntsd
fmri          svc:/ldoms/vntsd:default
enabled       true
state         online
next_state    none
state_time    Sat Jan 27 03:14:17 2007
logfile       /var/svc/log/ldoms-vntsd:default.log
restarter     svc:/system/svc/restarter:default
contract_id   93
dependency    optional_all/error svc:/milestone/network (online)
dependency    optional_all/none svc:/system/system-log (online)
```

Création et lancement d'un domaine hôte

Le domaine hôte doit exécuter un système d'exploitation comprenant à la fois la plate-forme `sun4v` et les périphériques virtuels présentés par l'hyperviseur. Il s'agit actuellement du SE Solaris 10 11/06 (au minimum). Reportez-vous aux *Notes de version Logical Domains (LDomS) 1.0.1* pour connaître tous les patches nécessaires. Une fois que vous avez créé les services par défaut et réaffecté les ressources à partir du domaine de contrôle, vous pouvez créer et lancer un domaine hôte.

▼ Procédure de création et de lancement d'un domaine hôte

1. Créez un domaine logique.

La commande suivante, par exemple, crée un domaine hôte appelé `ldg1`.

```
primary$ ldm add-domain ldg1
```

2. Ajoutez des CPU au domaine hôte.

Dans la commande suivante, par exemple, 4 CPU virtuelles sont ajoutées au domaine hôte `ldg1`.

```
primary$ ldm add-vcpu 4 ldg1
```

3. Ajoutez de la mémoire au domaine hôte.

Dans la commande suivante, par exemple, 512 Mo de mémoire sont ajoutés au domaine hôte `ldg1`.

```
primary$ ldm add-memory 512m ldg1
```

4. Ajoutez un périphérique réseau virtuel au domaine hôte.

Dans la commande suivante, par exemple, un périphérique réseau virtuel est ajouté au domaine hôte `ldg1`.

```
primary$ ldm add-vnet vnet1 primary-vsw0 ldg1
```

Dans cet exemple :

- `vnet1` représente un nom d'interface unique pour le domaine logique, ce nom est affecté à cette instance de périphérique réseau virtuel pour faire référence aux sous-commandes `set-vnet` ou `remove-vnet` suivantes.
- `primary-vsw0` représente le nom d'un service réseau existant (commutateur virtuel) auquel se connecter.

5. Indiquez le périphérique à être exporté par le serveur de disque virtuel en tant que disque virtuel pour le domaine hôte.

Vous pouvez exporter un disque physique, une tranche de disque, des volumes ou un fichier en tant que périphérique en mode bloc. L'exportation des périphériques loopback (`lofi`) en tant que périphériques en mode bloc n'est pas prise en charge dans cette version du logiciel Logical Domains. Les exemples suivants présentent un disque physique et un fichier.

- **Exemple de disque physique.** Dans le premier exemple, un disque physique avec des données spécifiques est ajouté.

```
primary$ ldm add-vdsdev /dev/dsk/c0t0d0s2 vol1@primary-vds0
```

Dans cet exemple :

- `/dev/dsk/c0t0d0s2` représente le nom du chemin du périphérique physique. Lors de l'ajout d'un périphérique, le nom du chemin doit être associé à son nom.
- `vol1` représente un nom unique que vous devez indiquer pour le périphérique ajouté au serveur de disque virtuel. Le nom du périphérique doit être unique pour cette instance de serveur de disque virtuel, en effet, ce nom est exporté par ce serveur de disque virtuel afin d'être ajouté aux clients. Lors de l'ajout d'un périphérique, son nom doit être associé à celui du chemin du périphérique actuel.
- `primary-vds0` représente le nom du serveur de disque virtuel existant auquel ajouter ce périphérique.
- **Exemple d'un fichier.** Dans le deuxième exemple, un fichier est exporté en tant que périphérique en mode bloc.

```
primary$ ldm add-vdsdev path-to-file/filename vol1@primary-vds0
```

Dans cet exemple :

- `path-to-file/filename` représente le nom du chemin du fichier exporté en tant que périphérique en mode bloc. Lors de l'ajout d'un périphérique, le nom du chemin doit être associé à son nom.
- `vol1` représente un nom unique que vous devez indiquer pour le périphérique ajouté au serveur de disque virtuel. Le nom du périphérique doit être unique pour cette instance de serveur de disque virtuel, en effet, ce nom est exporté par ce serveur de disque virtuel afin d'être ajouté aux clients. Lors de l'ajout d'un périphérique, son nom doit être associé à celui du chemin du périphérique actuel.
- `primary-vds0` représente le nom du serveur de disque virtuel existant auquel ajouter ce périphérique.

6. Ajoutez un disque virtuel au domaine hôte.

Dans l'exemple suivant, un disque virtuel est ajouté au domaine hôte `ldg1`.

```
primary$ ldm add-vdisk vdisk1 vol1@primary-vds0 ldg1
```

Dans cet exemple :

- `vdisk1` représente le nom du disque virtuel.
- `vol1` représente le nom du périphérique serveur de disque virtuel existant auquel se connecter.
- `primary-vds0` représente le nom du serveur de disque virtuel existant auquel se connecter.

Remarque – Les disques virtuels sont des périphériques en mode bloc génériques basés sur plusieurs types de périphériques, volumes ou fichiers physiques. Un disque virtuel n'est pas synonyme de disque SCSI, par conséquent l'ID cible ne figure pas dans son nom. Les disques virtuels d'un domaine logique ont le format suivant : *cNdNsN* ; *cN* représente le contrôleur virtuel, *dN* représente le numéro du disque virtuel et *sN* représente la tranche.

7. Définissez les variables `auto-boot` et `boot-device` pour le domaine hôte.

Dans le premier exemple, la commande définit `auto-boot\?` sur `true` pour le domaine hôte `ldg1`.

```
primary$ ldm set-var auto-boot\?=true ldg1
```

Dans le deuxième exemple, la commande définit `boot-device` sur `vdisk` pour le domaine hôte `ldg1`.

```
primary$ ldm set-var boot-device=vdisk ldg1
```

8. Associez des ressources au domaine hôte `ldg1` et affichez le contenu du domaine pour vous assurer qu'il est bien associé.

```
primary$ ldm bind-domain ldg1
primary$ ldm list-domain ldg1
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg1	bound	-----	5001	4	512M		

9. Pour connaître le port console du domaine hôte, examinez le contenu du message de la sous-commande `list-domain` précédente.

Sous l'en-tête `Cons`, vous voyez que le nom de la console du domaine hôte logique 1 (`ldg1`) est associé au port 5001.

10. Lancez le domaine hôte `ldg1`.

```
primary$ ldm start-domain ldg1
```

11. Connectez-vous à la console d'un domaine hôte. Vous pouvez effectuer cette opération de différentes manières.

- Vous pouvez vous connecter au domaine de contrôle, puis directement au port console de l'hôte local :

```
$ ssh admin@controldom.domain
$ telnet localhost 5001
```

- Vous pouvez également vous connecter à une console hôte sur le réseau, s'il est activé dans le fichier manifeste SMF `vntsd(1M)`. Par exemple :

```
$ telnet host-name 5001
```

Un fichier manifeste SMF (Service Management Facility, utilitaire de gestion de services) est un fichier XML qui décrit un service. Pour plus d'informations sur la création d'un fichier manifeste SMF, reportez-vous au document « Solaris 10 System Administrator Collection ».

Remarque – Pour accéder à un SE autre qu'en anglais dans un domaine hôte via la console, le terminal de la console doit être affecté des paramètres régionaux requis par le SE.

Installation JumpStart sur un domaine hôte

Pour effectuer une installation JumpStart sur un domaine hôte, utilisez une procédure JumpStart normale et modifiez la syntaxe de profil de la manière suivante, afin de passer d'une procédure JumpStart du SE Solaris à une procédure JumpStart spécifique à LDoms, comme indiqué dans les deux exemples suivants.

Profil JumpStart normal

```
filesys c1t1d0s0 free /  
filesys c1t1d0s1 2048 swap  
filesys c1t1d0s5 120 /spare1  
filesys c1t1d0s6 120 /spare2
```

Les noms de périphériques de disque virtuels d'un domaine logique diffèrent de ceux des périphériques de disque physiques : ils ne contiennent pas d'ID cible (`tN`). Au lieu de se présenter dans le format `cNtNdNsN`, les noms de périphériques de disque virtuels se présentent dans le format `cNdNsN`, `cN` représente le contrôleur virtuel, `dN` représente le numéro du disque et `sN` représente la tranche. Modifiez votre profil JumpStart afin d'appliquer cette modification, comme dans l'exemple de profil suivant.

Profil utilisé pour un domaine logique

```
filesys c0d0s0 free /  
filesys c0d0s1 2048 swap  
filesys c0d0s5 120 /spare1  
filesys c0d0s6 120 /spare2
```

Informations et tâches complémentaires

Ce chapitre décrit les concepts et les opérations ci-après, concernant l'utilisation du logiciel Logical Domains :

- « Accès à la page de manuel `ldm(1M)` », page 56
- « Limitations pour la saisie des noms dans l'interface de ligne de commande », page 56
- « Utilisation des sous-commandes `ldm list` », page 57
- « La commande `ldm stop-domain` peut expirer si le domaine est très chargé », page 73
- « Détermination du nom de l'interface réseau Solaris correspondant à un périphérique réseau virtuel », page 74
- « Assignation des adresses Mac automatiquement ou manuellement », page 75
- « Mappage de CPU et d'adresse mémoire », page 79
- « Configuration du bus Split PCI Express pour utiliser plusieurs domaines logiques », page 82
- « Activation du mode évitement MMU E/S sur un bus PCI », page 86
- « Utilisation des groupes de consoles », page 86
- « Déplacement d'un domaine logique d'un serveur à l'autre », page 88
- « Suppression de domaines logiques », page 88
- « Fonctionnement du SE Solaris avec Logical Domains », page 90
- « Utilisation de LDoms avec ALOM CMT », page 94
- « Activation et utilisation de l'audit BSM », page 95
- « Configuration du commutateur virtuel et du domaine de service pour NAT et routage », page 98
- « Utilisation de ZFS avec des disques virtuels », page 99

- « Utilisation des gestionnaires de volume dans un environnement Logical Domains », page 105
- « Configuration d'IPMP dans un environnement Logical Domains », page 109

Accès à la page de manuel `ldm(1M)`

L'interface de ligne de commande (CLI) de Logical Domains Manager est la commande `ldm(1M)`. La page de manuel `ldm(1M)` fait partie du package `SUNWldm` et est installée avec celui-ci. Reportez-vous au *Logical Domains (LDoms) Manager 1.0.1 Man Page Guide* pour le texte complet de la page de manuel `ldm(1M)`.

▼ Procédure d'accès à la page de manuel `ldm(1M)`

- Ajoutez le chemin du répertoire `/opt/SUNWldm/man` à la variable `$MANPATH`.

Limitations pour la saisie des noms dans l'interface de ligne de commande

Les sections suivantes décrivent les limitations relatives à la saisie des noms dans l'interface de ligne de commande de Logical Domains Manager.

Noms de fichier (*file*) et noms de variable (*var_name*)

- Le premier caractère doit être une lettre, un chiffre ou une barre oblique avant (/).
- Les caractères suivants doivent être des lettres, des chiffres ou des signes de ponctuation.

Noms de serveur de disque virtuel *file* | *device* et de commutateur virtuel

- Doivent contenir des lettres, des chiffres ou des signes de ponctuation.

Nom de configuration (*config_name*)

Le nom de configuration d'un domaine logique (*config_name*) que vous assignez à une configuration stockée sur le contrôleur système doit comporter 64 caractères au maximum.

Autres noms

Les autres noms, tels que le nom de domaine logique (*ldom*), le nom de service (*vswitch_name*, *service_name*, *vdpcs_service_name* et *vcc_name*), le nom de réseau virtuel (*if_name*) et le nom de disque virtuel (*disk_name*) doivent respecter le format suivant :

- Le premier caractère doit être une lettre ou un chiffre.
- Les caractères suivants doivent être des lettres, des chiffres ou tout caractère parmi les suivants : `'-_+#.~()'`

Utilisation des sous-commandes `ldm list`

Cette section décrit la syntaxe utilisée par les sous-commandes `ldm`, définit certains termes du résultat, tels que des indicateurs et des statistiques d'utilisation, et donne des exemples de résultat.

Résultat lisible par une machine

Si vous créez des scripts qui utilisent le résultat de la commande `ldm list`, utilisez *toujours* l'option `-p` pour produire le résultat sous une forme lisible par une machine. Consultez la section « [Procédure de génération d'une liste lisible et analysable par une machine \(-p\)](#) », page 66 pour plus d'informations.

▼ Procédure d’affichage de la syntaxe à utiliser pour les sous-commandes `ldm`

- Pour voir l’utilisation de la syntaxe pour toutes les sous-commandes `ldm`, procédez comme suit.

EXEMPLE DE CODE 5-1 Utilisation de la syntaxe pour toutes les sous-commandes `ldm`

```
primary# ldm --help

Usage:
  ldm [--help] command [options] [properties] operands

Command(s) for each resource (aliases in parens):

  bindings
    list-bindings [-e] [-p] [<ldom>...]

  services
    list-bindings [-e] [-p] [<ldom>...]

  constraints
    list-constraints ([-x] | [-e] [-p]) [<ldom>...]

  devices
    list-devices [-a] [-p] [cpu] [mau] [memory] [io]

  domain      ( dom )
    add-domain (-i <file> | mac-addr=<num> <ldom> | <ldom>...)
    remove-domain (-a | <ldom>...)
    list-domain [-e] [-l] [-p] [<ldom>...]
    start-domain start-domain (-a | -i <file> | <ldom>...)
    stop-domain stop-domain [-f] (-a | <ldom>...)
    bind-domain (-i <file> | <ldom>)
    unbind-domain <ldom>
    panic-domain <ldom>

  io
    add-io [bypass=on] <bus> <ldom>
    remove-io <bus> <ldom>

  mau
    add-mau <number> <ldom>
    set-mau <number> <ldom>
    remove-mau <number> <ldom>

  memory      ( mem )
    add-memory <number>[GMK] <ldom>
```

EXEMPLE DE CODE 5-1 Utilisation de la syntaxe pour toutes les sous-commandes ldm (*suite*)

```
set-memory <number>[GMK] <ldom>
remove-memory <number>[GMK] <ldom>

reconf
    remove-reconf <ldom>

spconfig      ( config )
    add-spconfig <config_name>
    set-spconfig <config_name>
    remove-spconfig <config_name>
    list-spconfig

variable      ( var )
    add-variable <var_name>=<value> <ldom>
    set-variable <var_name>=<value> <ldom>
    remove-variable <var_name> <ldom>
    list-variable [<var_name>...] <ldom>

vconscon      ( vcc )
    add-vconscon port-range=<x>-<y> <vcc_name> <ldom>
    set-vconscon port-range=<x>-<y> <vcc_name>
    remove-vconscon [-f] <vcc_name>

vconsole      ( vcons )
    set-vcons [port=[<port-num>]] [group=<group>] [service=<vcc_server>]
<ldom>

vcpu
    add-vcpu <number> <ldom>
    set-vcpu <number> <ldom>
    remove-vcpu <number> <ldom>

vdisk
    add-vdisk [timeout=<seconds>] <disk_name>
<volume_name>@<service_name> <ldom>
    remove-vdisk [-f] <disk_name> <ldom>

vdiskserver   ( vds )
    add-vdiskserver <service_name> <ldom>
    remove-vdiskserver [-f] <service_name>

vdpcc         ( ndpsldcc )
    add-vdpcc <vdpcc_name> <service_name> <ldom>
    remove-vdpcc [-f] <vdpcc_name> <ldom>

vdpcs         ( ndpsldcs )
    add-vdpcs <vdpcs_name> <ldom>
```

EXEMPLE DE CODE 5-1 Utilisation de la syntaxe pour toutes les sous-commandes ldm (suite)

```
remove-vdpcs [-f] <vdpcs_name>

vdiskserverdevice ( vdsdev )
    add-vdiskserverdevice [options=<opts>] <file|device>
<volume_name>@<service_name>
    remove-vdiskserverdevice [-f] <volume_name>@<service_name>

vnet
    add-vnet [mac-addr=<num>] <if_name> <vswitch_name> <ldom>
    set-vnet [mac-addr=<num>] [vswitch=<vswitch_name>] <if_name> <ldom>
    remove-vnet [-f] <if_name> <ldom>

vswitch ( vsw )
    add-vswitch [mac-addr=<num>] [net-dev=<device>] <vswitch_name> <ldom>
    set-vswitch [mac-addr=<num>] [net-dev=<device>] <vswitch_name>
    remove-vswitch [-f] <vswitch_name>
```

Verb aliases:

Alias	Verb
-----	-----
rm	remove
ls	list

Command aliases:

Alias	Command
-----	-----
create	add-domain
destroy	remove-domain
cancel-reconf	remove-reconf
start	start-domain
stop	stop-domain
bind	bind-domain
unbind	unbind-domain
panic	panic-domain

Définition des indicateurs

Les indicateurs suivants peuvent être affichés dans le résultat pour un domaine :

- paramètre substituable
- c domaine de contrôle
- d reconfiguration différée
- n normal

s	démarrage ou stop
t	transition
v	domaine E/S virtuel

Si vous utilisez l’option longue (-l) pour la commande, les indicateurs sont épelés. Sinon, vous voyez la lettre d’abréviation.

Les valeurs des indicateurs dépendent de la position dans la liste. Voici les valeurs qui peuvent apparaître dans chacune des cinq colonnes, de gauche à droite :

Colonne 1	Colonne 2	Colonne 3	Colonne 4	Colonne 5
s ou -	n ou t	d ou -	c ou -	v ou -

Définition des statistiques d’utilisation

Les statistiques d’utilisation par CPU virtuelle (UTIL) sont affichées avec l’option longue (-l) de la commande `ldm list`. Les statistiques sont le pourcentage en temps, depuis le dernier affichage des statistiques, où l’exécution de la CPU virtuelle a été dédiée au système d’exploitation hôte. L’exécution d’une CPU virtuelle est considérée dédiée au système d’exploitation hôte quand elle ne se rapporte pas à l’hyperviseur. Si le système d’exploitation hôte n’attribue pas de CPU virtuelles à l’hyperviseur, l’utilisation des CPU dans le système indique toujours 100%.

Les statistiques d’utilisation signalées pour un domaine logique correspondent à la moyenne d’utilisation des CPU virtuelles sur le domaine.

Exemples des diverses listes

▼ Procédure d’affichage des versions des logiciels (-V)

- Pour voir les versions des logiciels actuellement installées, effectuez l’opération suivante :

EXEMPLE DE CODE 5-2 Versions des logiciels installées

```
primary$ ldm -V

Logical Domain Manager (v 1.0.1)
Hypervisor control protocol v 1.0
```

EXEMPLE DE CODE 5-2 Versions des logiciels installées (*suite*)

System PROM:			
Hypervisor	v. 1.5.2	@(#)Hypervisor	1.5.2 2007/09/25 08:39/015
OpenBoot	v. 4.27.2	@(#)OBP	4.27.2 2007/09/24 16:28

▼ Procédure de génération d’une liste courte

- Pour générer une liste courte pour tous les domaines, procédez comme suit.

EXEMPLE DE CODE 5-3 Liste courte pour tous les domaines

primary\$ ldm list							
NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	-t-cv		4	1G	0.5%	3d 21h 7m
ldg1	active	-t---	5000	8	1G	23%	2m

▼ Procédure de génération d’une liste longue (-l)

- Pour générer une liste longue pour tous les domaines, procédez comme suit.

EXEMPLE DE CODE 5-4 Liste longue pour tous les domaines

primary\$ ldm list -l							
NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	-t-cv		1	768M	0.0%	0s
VCPU							
VID	PID	UTIL	STRAND				
0	0	0.0%	100%				
MEMORY							
RA	PA	SIZE					
0x4000000	0x4000000	768M					
IO							
DEVICE	PSEUDONYM	OPTIONS					
pci@780	bus_a						
pci@7c0	bus_b	bypass=on					
VCC							
NAME	PORT-RANGE						
vcc0	5000-5100						
VSW							
NAME	MAC	NET-DEV	DEVICE	MODE			
vsw0	08:00:20:aa:bb:e0	e1000g0	switch@0	prog,promisc			

EXEMPLE DE CODE 5-4 Liste longue pour tous les domaines *(suite)*

vsw1		08:00:20:aa:bb:e1				routed	
VDS							
NAME		VOLUME		OPTIONS		DEVICE	
vds0		myvol-a		slice		/disk/a	
		myvol-b				/disk/b	
		myvol-c		ro,slice,excl		/disk/c	
vds1		myvol-d				/disk/d	
VDPCS							
NAME							
vdpcs0							
vdpcs1							

NAME		STATE	FLAGS	CONS	VCPU	MEMORY	UTIL UPTIME
ldg1		bound	-----	5000	1	512M	
VCPU							
VID		PID	UTIL		STRAND		
0		1	100%				
MEMORY							
RA		PA		SIZE			
0x4000000		0x34000000		512M			
NETWORK							
NAME		SERVICE			DEVICE		MAC
mynet-b		vsw0@primary			network@0		08:00:20:ab:9a:12
mynet-a		vsw0@primary			network@1		08:00:20:ab:9a:11
DISK							
NAME		VOLUME			DEVICE		SERVER
mydisk-a		myvol-a@vds0			disk@0		primary
mydisk-b		myvol-b@vds0			disk@1		primary
VDPCC							
NAME		SERVICE					
myvdpcc-a		vdpcs0@primary					
myvdpcc-b		vdpcs0@primary					
VCONS							
NAME		SERVICE			PORT		
mygroup		vcc0@primary			5000		

▼ Procédure de génération d'une liste étendue (-e)

- Pour générer une liste étendue pour tous les domaines, procédez comme suit.

EXEMPLE DE CODE 5-5 Liste étendue pour tous les domaines

```
primary$ ldm list -e
NAME                STATE    FLAGS    CONS    VCPU    MEMORY    UTIL    UPTIME
primary             active   -t-cv                1      768M      0.0%    0s

VCPU
  VID    PID    UTIL  STRAND
   0      0    0.0%   100%

MEMORY
  RA                PA                SIZE
0x4000000          0x4000000      768M

IO
  DEVICE                PSEUDONYM          OPTIONS
pci@780                bus_a
pci@7c0                bus_b              bypass=on

VLDC
  NAME
primary

VCC
  NAME                PORT-RANGE
vcc0                  5000-5100

VSW
  NAME                MAC                NET-DEV    DEVICE    MODE
vsw0                 08:00:20:aa:bb:e0  e1000g0    switch@0  prog,promisc
vsw1                 08:00:20:aa:bb:e1

VDS
  NAME                VOLUME                OPTIONS          DEVICE
vds0                 myvol-a              slice            /disk/a
                     myvol-b                                /disk/b
                     myvol-c              ro,slice,excl    /disk/c
vds1                 myvol-d                                /disk/d

VDPCS
  NAME
vdpcs0
vdpcs1

VLDCC
```


EXEMPLE DE CODE 5-5 Liste étendue pour tous les domaines (*suite*)

NAME		SERVICE		DESC			
hvctl		primary@primary		hvctl			
vldcc0		primary@primary		ds			

NAME		STATE	FLAGS	CONS	VCPU	MEMORY	UTIL UPTIME
ldg1		bound	-----	5000	1	512M	
VCPU							
VID		PID	UTIL STRAND				
0		1	100%				
MEMORY							
RA		PA		SIZE			
0x4000000		0x34000000		512M			
VLDCC							
NAME		SERVICE		DESC			
vldcc0		primary@primary		ds			
NETWORK							
NAME		SERVICE		DEVICE		MAC	
mynet-b		vsw0@primary		network@0		08:00:20:ab:9a:12	
mynet-a		vsw0@primary		network@1		08:00:20:ab:9a:11	
DISK							
NAME		VOLUME		DEVICE		SERVER	
mydisk-a		myvol-a@vds0		disk@0		primary	
mydisk-b		myvol-b@vds0		disk@1		primary	
VDPCC							
NAME		SERVICE					
myvdpcc-a		vdpcs0@primary					
myvdpcc-b		vdpcs0@primary					
VCONS							
NAME		SERVICE		PORT			
mygroup		vcc0@primary		5000			

▼ Procédure de génération d'une liste lisible et analysable par une machine (-p)

- Pour générer une liste lisible et analysable par une machine pour tous les domaines, procédez comme suit.

EXEMPLE DE CODE 5-6 Liste lisible par une machine

```
primary$ ldm list -p
VERSION 1.0
DOMAIN|name=primary|state=active|flags=-t-cv|cons=|ncpu=1|mem=805306368|util=
0.0|uptime=0
DOMAIN|name=ldg1|state=bound|flags=-----|cons=5000|ncpu=1|mem=536870912|util=
|uptime=
```

▼ Procédure d'affichage de l'état d'un domaine

- Pour voir l'état d'un domaine (par exemple, du domaine hôte ldg1), procédez comme suit.

EXEMPLE DE CODE 5-7 État d'un domaine

```
primary# ldm list-domain ldg1
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg1	active	-t---	5000	8	1G	0.3%	2m

▼ Procédure de listage d'une variable

- Pour lister une variable (par exemple, boot-device) pour un domaine (par exemple, ldg1), procédez comme suit.

EXEMPLE DE CODE 5-8 Listage d'une variable pour un domaine

```
primary$ ldm list-variable boot-device ldg1
boot-device=/virtual-devices@100/channel-devices@200/disk@0:a
```

▼ Procédure de listage des liaisons

- Pour lister des ressources liées pour un domaine (par exemple, `ldg1`), procédez comme suit.

EXEMPLE DE CODE 5-9 Listage des liaisons pour un domaine

```
primary$ ldm list-bindings ldg1
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg1	bound	-----	5000	1	512M		

VCPU

VID	PID	UTIL	STRAND
0	1		100%

MEMORY

RA	PA	SIZE
0x4000000	0x34000000	512M

NETWORK

NAME	SERVICE	DEVICE	MAC
mynet-b	vsw0@primary	network@0	08:00:20:ab:9a:12
PEER		MAC	
vsw0@primary			08:00:20:aa:bb:e0
mynet-a@ldg1			08:00:20:ab:9a:11
mynet-c@ldg2			08:00:20:ab:9a:22
NAME	SERVICE	DEVICE	MAC
mynet-a	vsw0@primary	network@1	08:00:20:ab:9a:11
PEER		MAC	
vsw0@primary			08:00:20:aa:bb:e0
mynet-b@ldg1			08:00:20:ab:9a:12
mynet-c@ldg2			08:00:20:ab:9a:22

DISK

NAME	VOLUME	DEVICE	SERVER
mydisk-a	myvol-a@vds0	disk@0	primary
mydisk-b	myvol-b@vds0	disk@1	primary

VDPCC

NAME	SERVICE
myvdpcc-a	vdpcs0@primary
myvdpcc-b	vdpcs0@primary

VCONS

NAME	SERVICE	PORT
mygroup	vcc0@primary	5000

▼ Procédure de listage des configurations

- Pour lister des configurations de domaine logique stockées sur le contrôleur système, procédez comme suit.

EXEMPLE DE CODE 5-10 Listage de configurations

```
primary$ ldm list-config  
factory-default [current]  
initial [next]
```

Les libellés à droite du nom de la configuration ont la signification suivante :

- current - configuration actuellement utilisée
- next - configuration utilisée à la prochaine remise sous tension

▼ Procédure de listage des périphériques

- Pour lister toutes les ressources d'un serveur, liées ou dissociées, procédez comme suit.

EXEMPLE DE CODE 5-11 Listage de toutes les ressources du serveur

```
primary$ ldm list-devices -a  
VCPUs  
  PID  %FREE  
  0      0  
  1      0  
  2      0  
  3      0  
  4     100  
  5     100  
  6     100  
  7     100  
  8     100  
  9     100  
 10     100  
 11     100  
 12     100  
 13     100  
 14     100  
 15     100  
 16     100  
 17     100  
 18     100  
 19     100  
 20     100
```

EXEMPLE DE CODE 5-11 Listage de toutes les ressources du serveur *(suite)*

21	100		
22	100		
23	100		
24	100		
25	100		
26	100		
27	100		
28	100		
29	100		
30	100		
31	100		
MAU			
CPUSET		BOUND	
(0, 1, 2, 3)		ldg2	
(4, 5, 6, 7)			
(8, 9, 10, 11)			
(12, 13, 14, 15)			
(16, 17, 18, 19)			
(20, 21, 22, 23)			
(24, 25, 26, 27)			
(28, 29, 30, 31)			
MEMORY			
PA	SIZE	BOUND	
0x0	512K	_sys_	
0x80000	1536K	_sys_	
0x200000	62M	_sys_	
0x4000000	768M	primary	
0x34000000	512M	ldg1	
0x54000000	8M	_sys_	
0x54800000	2G	ldg2	
0xd4800000	29368M		
IO			
DEVICE	PSEUDONYM	BOUND	OPTIONS
pci@780	bus_a	yes	
pci@7c0	bus_b	yes	bypass=on

▼ Procédure de listage des services

- Pour lister les services disponibles, procédez comme suit.

EXEMPLE DE CODE 5-12 Listage des services

```
primary$ ldm list-services
VDS
  NAME          VOLUME          OPTIONS          DEVICE
  primary-vds0
VCC
  NAME          PORT-RANGE
  primary-vcc0   5000-5100
VSW
  NAME          MAC          NET-DEV  DEVICE  MODE
  primary-vsw0  00:14:4f:f9:68:d0  e1000g0  switch@0  prog,promisc
```

Listage des contraintes

Pour Logical Domains Manager, les contraintes sont des ressources que vous souhaitez voir assignées à un domaine particulier. Soit vous obtenez que toutes les ressources demandées soient ajoutées à un domaine, soit vous n'en obtenez aucune, en fonction de leur disponibilité. La sous-commande `list-constraints` liste les ressources que vous avez demandées pour être assignées au domaine.

▼ Procédure de listage des contraintes pour un domaine

- Afin de lister les contraintes pour un domaine (par exemple, `ldg1`), procédez comme suit.

EXEMPLE DE CODE 5-13 Listage des contraintes pour un domaine

```
primary$ ldm list-constraints ldg1
DOMAIN
ldg1

VCPU
  COUNT
  1

MEMORY
  SIZE
  512M

NETWORK
```

EXEMPLE DE CODE 5-13 Listage des contraintes pour un domaine (*suite*)

NAME	SERVICE	DEVICE	MAC
mynet-b	vsw0	network@0	08:00:20:ab:9a:12
mynet-b	vsw0	network@0	08:00:20:ab:9a:12
DISK			
NAME	VOLUME		
mydisk-a	myvol-a@vds0		
mydisk-b	myvol-b@vds0		
VDPCC			
NAME	SERVICE		
myvdpcc-a	vdpcs0@primary		
myvdpcc-b	vdpcs0@primary		
VCONS			
NAME	SERVICE		
mygroup	vcc0		

▼ **Procédure de listage des contraintes au format XML**

- **Pour lister les contraintes au format XML pour un domaine particulier (par exemple, ldg1), procédez comme suit.**

EXEMPLE DE CODE 5-14 Contraintes pour un domaine au format XML

```
primary$ ldm list-constraints -x ldg1
<?xml version="1.0"?>
<LDM_interface version="1.0">
  <data version="2.0">
    <ldom>
      <ldom_info>
        <ldom_name>ldg1</ldom_name>
      </ldom_info>
      <cpu>
        <number>8</number>
      </cpu>
      <memory>
        <size>1G</size>
      </memory>
      <network>
        <vnet_name>vnet0</vnet_name>
        <service_name>primary-vsw0</service_name>
        <mac_address>01:14:4f:fa:0f:55</mac_address>
      </network>
      <disk>
        <vdisk_name>vdisk0</vdisk_name>
```

EXEMPLE DE CODE 5-14 Contraintes pour un domaine au format XML (*suite*)

```
<service_name>primary-vds0</service_name>
<vol_name>vol0</vol_name>
</disk>
<var>
  <name>boot-device</name>
  <value>/virtual-devices@100/channel-devices@200/disk@0:a</value>
</var>
<var>
  <name>nvrarc</name>
  <value>devalias vnet0 /virtual-devices@100/channel-devices@200/
network@0</value>
</var>
<var>
  <name>use-nvrarc?</name>
  <value>true</value>
</var>
</ldom>
</data>
</LDM_interface>
```

▼ Procédure de listage des contraintes dans un format lisible par une machine

- Pour lister les contraintes de tous les domaines dans un format analysable, procédez comme suit.

EXEMPLE DE CODE 5-15 Contraintes pour tous les domaines dans un format lisible par une machine

```
primary$ ldm list-constraints -p
VERSION 1.0
DOMAIN|name=primary
MAC|mac-addr=00:03:ba:d8:b1:46
VCPU|count=4
MEMORY|size=805306368
IO
|dev=pci@780|alias=
|dev=pci@7c0|alias=
VDS|name=primary-vds0
|vol=disk-ldg2|opts=|dev=/ldoms/nv72-ldg2/disk
|vol=vol0|opts=|dev=/ldoms/nv72-ldg1/disk
VCC|name=primary-vcc0|port-range=5000-5100
VSW|name=primary-vsw0|mac-addr=|net-dev=e1000g0|dev=switch@0
DOMAIN|name=ldg1
VCPU|count=8
MEMORY|size=1073741824
VARIABLES
```


EXEMPLE DE CODE 5-15 Contraintes pour tous les domaines dans un format lisible par une machine (*suite*)

```
|boot-device=/virtual-devices@100/channel-devices@200/disk@0:a
|nvramrc=devalias vnet0 /virtual-devices@100/channel-devices@200/network@0
|use-nvramrc?=true
VNET|name=vnet0|dev=network@0|service=primary-vsw0|mac-addr=01:14:4f:fa:0f:55
VDISK|name=vdisk0|vol=vol0@primary-vds0
```



La commande `ldm stop-domain` peut expirer si le domaine est très chargé

Une commande `ldm stop-domain` peut expirer avant l’arrêt complet du domaine. Si cela se produit, Logical Domains Manager renvoie une erreur similaire à la suivante :

```
LDom ldg8 stop notification failed
```

Cependant, le domaine devrait encore pouvoir traiter la requête d’arrêt. Utilisez la commande `ldm list-domain` pour vérifier l’état du domaine. Par exemple :

# <code>ldm list-domain ldg8</code>							
NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg8	active	s----	5000	22	3328M	0.3%	1d 14h 31m

La liste précédente indique que le domaine est actif, mais l’indicateur `s` signale que le domaine est dans le processus d’arrêt. Cela devrait être un état transitoire.

L’exemple suivant indique que le domaine est maintenant arrêté :

# <code>ldm list-domain ldg8</code>							
NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg8	bound	-----	5000	22	3328M		

Détermination du nom de l'interface réseau Solaris correspondant à un périphérique réseau virtuel

Il n'y a pas moyen de déterminer le nom de l'interface réseau du SE Solaris sur un hôte, correspondant à un périphérique virtuel donné, directement à partir du résultat fourni par les commandes `ldm list -*`. Cependant, vous pouvez l'obtenir en combinant le résultat de la commande `ldm list -l` avec les entrées sous `/devices` sur l'hôte SE Solaris.

▼ Procédure permettant de trouver le nom de l'interface réseau du SE Solaris

Dans cet exemple, le domaine hôte `ldg1` contient deux périphériques réseau virtuels, `net-a` et `net-c`, et nous souhaitons trouver le nom de l'interface réseau du SE Solaris dans `ldg1` qui correspond à `net-c`.

1. Utilisez la commande `ldm` pour trouver l'instance de périphérique réseau virtuel `net-c`.

```
# ldm list -l ldg1
...
NETWORK
NAME          SERVICE          DEVICE          MAC
net-a         primary-vsw0@primary  network@0       00:14:4f:f8:91:4f
net-c         primary-vsw0@primary  network@2       00:14:4f:f8:dd:68
...
#
```

L'instance de périphérique réseau virtuel pour `net-c` est `network@2`.

2. Pour trouver l'interface réseau correspondant à `ldg1`, connectez-vous à `ldg1` et trouvez l'entrée pour cette instance sous `/devices`.

```
# uname -n
ldg1
# find /devices/virtual-devices@100 -type c -name network@2\*
/devices/virtual-devices@100/channel-devices@200/network@2:vnet1
#
```

Le nom de l'interface réseau est la partie de l'entrée après les deux-points, en l'occurrence, `vnet1`.

3. Raccordez `vnet1` pour voir son adresse MAC `00:14:4f:f8:dd:68`, comme indiqué dans le résultat de la commande `ldm list -l pour net-c` dans l'étape 1.

```
# ifconfig vnet1
vnet1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 0.0.0.0 netmask 0
    ether 0:14:4f:f8:dd:68
#
```

Assignation des adresses Mac automatiquement ou manuellement

Vous devez disposer de suffisamment d'adresses MAC (Media Access Control, contrôle d'accès aux médias) pour le nombre de domaines logiques, de commutateurs virtuels et de réseaux virtuels que vous allez utiliser. Logical Domains Manager peut assigner automatiquement des adresses MAC à un domaine logique, à un réseau virtuel (`vnet`) et à un commutateur virtuel (`vswitch`), mais vous pouvez aussi les assigner manuellement à partir de votre propre pool d'adresses MAC assignées. Les sous-commandes `ldm` qui définissent les adresses MAC sont `add-domain`, `add-vsw`, `set-vsw`, `add-vnet` et `set-vnet`. Si vous ne spécifiez aucune adresse MAC dans ces sous-commandes, Logical Domains Manager en assigne une automatiquement.

L'avantage lorsque Logical Domains Manager assigne les adresses MAC est qu'il utilise le bloc d'adresses MAC dédiées pour l'utilisation avec les domaines logiques. Par ailleurs, Logical Domains Manager détecte et évite les conflits d'adresses MAC avec d'autres instances de Logical Domains Manager sur le même sous-réseau. Cela vous libère de la gestion manuelle de votre pool d'adresses MAC.

L'assignation d'adresses MAC se produit dès qu'un domaine logique est créé ou qu'un périphérique réseau est configuré dans un domaine. De plus, l'assignation persiste tant que le périphérique, voire le domaine logique lui-même, n'est pas supprimé.

Les sujets suivants sont traités dans cette section :

- « [Plage d'adresses MAC assignées au logiciel Logical Domains](#) », page 76
- « [Algorithme d'assignation automatique](#) », page 76
- « [Détection d'adresses MAC dupliquées](#) », page 77
- « [Adresses MAC libérées](#) », page 78
- « [Allocation manuelle d'adresses MAC](#) », page 78

Plage d'adresses MAC assignées au logiciel Logical Domains

Le bloc de 512 K d'adresses MAC suivant est assigné aux domaines logiques :

00:14:4F:F8:00:00 ~ 00:14:4F:FF:FF:FF

Les 256 K d'adresses inférieures sont utilisées par Logical Domains Manager pour **l'allocation automatique d'adresses MAC**, et vous ne pouvez *pas* demander manuellement une adresse dans cette plage :

00:14:4F:F8:00:00 - 00:14:4F:FB:FF:FF

Vous pouvez utiliser la moitié supérieure de cette plage pour **l'allocation manuelle d'adresses MAC** :

00:14:4F:FC:00:00 - 00:14:4F:FF:FF:FF

Algorithme d'assignation automatique

Lorsque vous ne spécifiez aucune adresse MAC lors de la création d'un domaine logique ou d'un périphérique réseau, Logical Domains Manager alloue et assigne automatiquement une adresse MAC à celui-ci. Pour obtenir cette adresse MAC, Logical Domains Manager essaie de sélectionner une adresse de façon itérative, puis vérifie les conflits potentiels.

Avant de sélectionner une adresse potentielle, Logical Domains Manager regarde d'abord s'il dispose d'une adresse assignée automatiquement et libérée récemment, enregistrée dans une base de données dédiée à cet effet (voir « [Adresses MAC libérées](#) », page 78). Si c'est le cas, Logical Domains Manager sélectionne son adresse candidate à partir de la base de données.

Si aucune adresse libérée récemment n'est disponible, l'adresse MAC est sélectionnée de façon aléatoire dans une plage de 256 K d'adresses réservées à cet effet. L'adresse MAC est sélectionnée de façon aléatoire pour diminuer la probabilité d'une adresse MAC dupliquée, choisie comme candidate.

L'adresse sélectionnée est ensuite vérifiée avec les autres instances de Logical Domains Manager sur les autres systèmes pour éviter l'assignation d'adresses MAC dupliquées. L'algorithme employé est décrit dans la section « [Détection d'adresses MAC dupliquées](#) », page 77. Si l'adresse est déjà assignée, Logical Domains Manager itère : il choisit une autre adresse et vérifie à nouveau les conflits potentiels. Il continue jusqu'à trouver une adresse MAC pas encore allouée ou que le délai de 30 secondes soit écoulé. Lorsque le délai est atteint, la création du périphérique échoue et un message d'erreur similaire au suivant est affiché :

```
Automatic MAC allocation failed. Please set the vnet MAC address manually.
```

Détection d'adresses MAC dupliquées

Pour éviter que la même adresse MAC soit allouée à différents périphériques, Logical Domains Manager procède à une vérification avec les instances de Logical Domains Manager des autres systèmes, en envoyant un message par multidiffusion, via l'interface réseau par défaut du domaine de contrôle, contenant l'adresse qu'il souhaite assigner au périphérique. L'instance Logical Domains Manager essayant d'attribuer l'adresse MAC attend une réponse pendant une seconde. Si cette adresse MAC est déjà assignée à un périphérique sur un autre système LDoms, l'instance Logical Domains Manager de ce système-là renvoie une réponse contenant l'adresse en question. Si l'instance Logical Domains Manager demandeuse reçoit une réponse, elle sait que l'adresse choisie est déjà allouée, et itère pour en choisir une autre.

Par défaut, ces messages multidiffusés sont envoyés uniquement aux gestionnaires du même sous-réseau ; la durée de vie (TTL, time-to-live) par défaut est 1. La durée de vie TTL peut être configurée en utilisant la propriété SMF (Service Management Facilities, utilitaires de gestion de services) `ldmd/hops`.

Chaque Logical Domains Manager est responsable des tâches suivantes :

- Écoute des messages de multidiffusion
- Suivi des adresses MAC assignées dans ses domaines
- Recherche de doublons
- Réponse pour empêcher les doublons

Si Logical Domains Manager est arrêté pour une raison quelconque sur un système, des adresses MAC pourraient être dupliquées tant qu'il ne fonctionne pas.

L'allocation MAC automatique se produit au moment de la création du domaine logique ou du périphérique réseau et persiste tant que celui-ci n'est pas supprimé.

Adresses MAC libérées

Lorsqu'un domaine logique ou un périphérique associé à une adresse MAC automatique est supprimé, cette adresse est enregistrée dans une base de données d'adresses MAC récemment libérées en vue d'un usage ultérieur possible sur ce système. Ces adresses sont enregistrées pour éviter l'épuisement des adresses IP (Internet Protocol) à partir d'un serveur DHCP (Dynamic Host Configuration Protocol). Les serveurs DHCP allouent des adresses IP sur des plages de temps. Ces plages sont souvent configurées pour durer quelques heures ou quelques jours. Si les périphériques réseau sont créés et supprimés à une cadence élevée sans que Logical Domains Manager réutilise automatiquement les adresses MAC allouées, le nombre de ces adresses pourrait bientôt submerger un serveur DHCP configuré de façon standard.

Comme mentionné plus haut, lorsqu'une instance Logical Domains Manager est sollicitée pour obtenir automatiquement une adresse MAC pour un domaine logique ou un périphérique réseau, elle consulte d'abord la base de données des adresses MAC libérées pour voir si une adresse précédemment assignée peut être réutilisée. S'il existe une adresse MAC disponible dans la base de données, l'algorithme de détection d'adresses dupliquées est exécuté. Si l'adresse n'a pas été réattribuée depuis sa libération, elle peut être réutilisée et supprimée de la base de données. Si un conflit est détecté, l'adresse est simplement supprimée de la base de données. Logical Domains Manager essaie alors l'adresse suivante dans la base de données ou, si aucune n'est disponible, choisit de façon aléatoire une nouvelle adresse MAC.

Allocation manuelle d'adresses MAC

La procédure suivante vous indique comment créer manuellement une adresse MAC.

▼ Procédure d'allocation manuelle d'une adresse MAC

1. Convertissez la partie sous-réseau de l'adresse IP de l'hôte physique en format hexadécimal et enregistrez le résultat.

```
# grep $nom_hôte /etc/hosts | awk '{print $1}' | awk -F. '{printf("%x", $4)}'
```

27

2. Déterminez le nombre de domaines présents hormis le domaine de contrôle.

# /opt/SUNWldm/bin/ldm list-domain							
NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	-n-cv	SP	4	768M	0.3%	4h 54m
myldom1	active	-n---	5000	2	512M	1.9%	1h 12m

Il y a un seul domaine hôte et vous devez inclure le domaine que vous voulez créer ; le compte de domaines est donc 2.

3. Insérez l'adresse IP convertie (27) après la chaîne du fournisseur (0x08020ab), suivie de 10 plus le nombre de domaines logiques (2 dans cet exemple), soit 12.

```
0x08020ab and 27 and 12 = 0x08020ab2712 or 8:0:20:ab:27:12
```

Mappage de CPU et d'adresse mémoire

L'architecture de gestion des pannes FMA (Fault Management Architecture) de Solaris signale les erreurs de CPU en termes de numéro de CPU physique et les erreurs de mémoire en termes d'adresse de mémoire physique.

Si vous voulez savoir dans quel domaine logique une erreur s'est produite, avec le numéro de CPU virtuelle ou l'adresse de mémoire réelle correspondant dans le domaine, vous devez effectuer un mappage.

Mappage de CPU

Le domaine et le numéro de CPU virtuelle dans le domaine, correspondant à un numéro de CPU physique donné, peuvent être déterminés à l'aide des procédures suivantes.

▼ Procédure de détermination du numéro de CPU

1. Générez une liste longue analysable pour tous les domaines.

```
primary$ ldm ls -l -p
```

2. Cherchez l'entrée dans les sections VCPU de la liste ayant un champ pid égal au numéro de CPU physique.

- a. Si vous trouvez une telle entrée, la CPU se trouve dans le domaine sous lequel l'entrée est affichée, et le numéro de CPU virtuelle dans le domaine est donné par le champ `vid` de l'entrée.
- b. Si une telle entrée n'existe pas, la CPU ne se trouve dans aucun domaine.

Mappage de mémoire

Le domaine et l'adresse de mémoire réelle dans le domaine, correspondant à une adresse de mémoire physique donnée, peuvent être déterminés de la manière suivante.

▼ Procédure de détermination de l'adresse réelle

1. Générez une liste longue analysable pour tous les domaines.

```
primary$ ldm ls -l -p
```

2. Recherchez dans les sections `MEMORY` de la liste, la ligne où l'adresse physique `PA` appartient à la plage inclusive `pa` à `(pa + taille - 1)` : soit, $pa \leq PA < (pa + \text{taille} - 1)$.

Ici `pa` et `taille` font référence à des valeurs dans les champs correspondants de la ligne.

- a. Si une telle entrée existe, l'adresse physique `PA` appartient au domaine sous lequel l'entrée est affichée, et l'adresse réelle correspondante dans le domaine est donnée par $ra + (PA - pa)$.
- b. Si une telle entrée n'existe pas, l'adresse physique `PA` ne se trouve dans aucun domaine.

Exemples de mappage de CPU et de mémoire

Supposons que vous disposiez d'une configuration de domaine logique comme celle de l'[EXEMPLE DE CODE 5-16](#), et que vous souhaitiez déterminer le domaine et la CPU virtuelle correspondant au numéro de CPU physique 5, ainsi que le domaine et l'adresse réelle correspondant à l'adresse physique 0x7e816000.

En recherchant dans les entrées `VCPU` de la liste celle dont le champ `pid` est égal à 5, vous trouverez l'entrée suivante sous le domaine logique `ldg1` :

Donc, la CPU physique numéro 5 appartient au domaine ldg1 au sein duquel elle porte le numéro de CPU virtuelle 1.

vid=1 pid=5 util=29 strand=100

En parcourant les entrées MEMORY dans la liste, vous découvrez l'entrée suivante sous le domaine ldg2 :

ra=0x8000000 pa=0x78000000 size=1073741824
--

Où $0x78000000 \leq 0x7e816000 \leq (0x78000000 + 1073741824 - 1)$, c'est-à-dire, $pa \leq PA \leq (pa + taille - 1)$.

Donc, l'adresse physique PA appartient au domaine ldg2 et correspond à l'adresse réelle $0x8000000 + (0x7e816000 - 0x78000000) = 0xe816000$.

EXEMPLE DE CODE 5-16 Longue liste analysable de configurations de domaines logiques

```
primary$ ldm ls -l -p
VERSION 1.0
DOMAIN|name=primary|state=active|flags=normal,control,vio-service|cons=
SP|ncpu=4|mem=1073741824|util=0.6|uptime=64801|softstate=Solaris running
VCPU
|vid=0|pid=0|util=0.9|strand=100
|vid=1|pid=1|util=0.5|strand=100
|vid=2|pid=2|util=0.6|strand=100
|vid=3|pid=3|util=0.6|strand=100
MEMORY
|ra=0x8000000|pa=0x8000000|size=1073741824
IO
|dev=pci@780|alias=bus_a
|dev=pci@7c0|alias=bus_b
VDS|name=primary-vds0|nclients=2
|vol=disk-ldg1|opts=|dev=/opt/ldoms/testdisk.1
|vol=disk-ldg2|opts=|dev=/opt/ldoms/testdisk.2
VCC|name=primary-vcc0|nclients=2|port-range=5000-5100
VSW|name=primary-vsw0|nclients=2|mac-addr=00:14:4f:fb:42:5c|net-dev=
e1000g0|dev=switch@0|mode=prog,promisc
VCONS|type=SP
DOMAIN|name=ldg1|state=active|flags=normal|cons=5000|ncpu=2|mem=
805306368|util=29|uptime=903|softstate=Solaris running
VCPU
|vid=0|pid=4|util=29|strand=100
|vid=1|pid=5|util=29|strand=100
MEMORY
|ra=0x8000000|pa=0x48000000|size=805306368
VARIABLES
|auto-boot?=true
```

EXEMPLE DE CODE 5-16 Longue liste analysable de configurations de domaines logiques (*suite*)

```
|boot-device=/virtual-devices@100/channel-devices@200/disk@0
VNET|name=net|dev=network@0|service=primary-vsw0@primary|mac-addr=
00:14:4f:f9:8f:e6
VDISK|name=vdisk-1|vol=disk-ldg1@primary-vds0|dev=disk@0|server=primary
VCONS|group=group1|service=primary-vcc0@primary|port=5000
DOMAIN|name=ldg2|state=active|flags=normal|cons=5001|ncpu=3|mem=
1073741824|util=35|uptime=775|softstate=Solaris running
VCPU
|vid=0|pid=6|util=35|strand=100
|vid=1|pid=7|util=34|strand=100
|vid=2|pid=8|util=35|strand=100
MEMORY
|ra=0x8000000|pa=0x78000000|size=1073741824
VARIABLES
|auto-boot?=true
|boot-device=/virtual-devices@100/channel-devices@200/disk@0
VNET|name=net|dev=network@0|service=primary-vsw0@primary|mac-addr=
00:14:4f:f9:8f:e7
VDISK|name=vdisk-2|vol=disk-ldg2@primary-vds0|dev=disk@0|server=primary
VCONS|group=group2|service=primary-vcc0@primary|port=5000
```

Configuration du bus Split PCI Express pour utiliser plusieurs domaines logiques

Remarque – Pour les serveurs Sun UltraSPARC T-2, tels que Sun SPARC Enterprise T5120 et T5220, vous assigneriez une unité d’interface réseau NIU (Network Interface Unit) au domaine logique plutôt qu’utiliser cette procédure.

Le bus PCI-E (PCI Express) sur un serveur Sun UltraSPARC T1 comprend deux ports avec plusieurs périphériques terminaux qui leur sont connectés. Ceux-ci sont identifiés sur un serveur avec les noms `pci@780` (`bus_a`) et `pci@7c0` (`bus_b`). Dans un environnement avec plusieurs domaines, le bus PCI-E peut être programmé pour assigner chaque nœud terminal à un domaine séparé en utilisant Logical Domains Manager. Par conséquent, vous pouvez activer plusieurs domaines avec un accès direct aux périphériques physiques au lieu d’utiliser la virtualisation E/S.

Lorsque le système Logical Domains est sous tension, le domaine de contrôle (`primary`) utilise toutes les ressources des périphériques physiques, si bien que les deux nœuds terminaux du bus PCI-E appartiennent au domaine principal.



Attention – Tous les disques internes des serveurs pris en charge sont reliés à un seul nœud terminal. Si un domaine de contrôle est initialisé à partir d'un disque interne, ne supprimez pas ce nœud terminal du domaine. Assurez-vous aussi de ne pas supprimer le nœud terminal avec le port principal du réseau. Si vous supprimez le mauvais nœud terminal du domaine de contrôle ou de service, ce domaine ne sera plus capable d'accéder aux périphériques demandés et deviendra inutilisable. Si le port principal du réseau est sur un bus différent de celui du disque système, déplacez le câble réseau vers un port réseau intégré et utilisez Logical Domains Manager pour reconfigurer le commutateur virtuel (vsw) afin de refléter ce changement.

▼ Procédure de création d'une configuration Split PCI

L'exemple affiché ici est relatif à un serveur Sun Fire T2000. Cette procédure peut également être utilisée sur d'autres serveurs Sun UltraSPARC T1, tels que Sun Fire T1000 et Netra T2000. Les instructions pour les autres serveurs peuvent différer légèrement des suivantes, mais cet exemple vous donne les principes de base. Vous devez surtout conserver le nœud terminal qui possède le disque d'initialisation et supprimer l'autre nœud terminal du domaine principal et l'assigner à un autre domaine.

1. Vérifiez que le domaine `primary` possède les deux nœuds terminaux du bus PCI Express.

```
primary# ldm list-bindings primary
...
IO
    DEVICE          PSEUDONYM      OPTIONS
    pci@780         bus_a
    pci@7c0         bus_b
...
```

2. Déterminez le chemin du périphérique du disque d'initialisation qui doit être conservé.

```
primary# df /
/                (/dev/dsk/c1t0d0s0 ): 1309384 blocks   457028 files
```

3. Déterminez le périphérique physique auquel le périphérique de bloc `clt0d0s0` est relié.

```
primary# ls -l /dev/dsk/clt0d0s0
lrwxrwxrwx  1 root      root          65 Feb  2 17:19 /dev/dsk/clt0d0s0 -> ../
../devices/pci@7c0/pci@0/pci@1/pci@0,2/LSILogic,sas@2/sd@0,0:a
```

Dans cet exemple, le périphérique physique pour le disque d'initialisation du domaine `primary` se trouve sous le nœud terminal `pci@7c0`, qui correspond à notre précédent listage de `bus_b`. Cela signifie que nous pouvons assigner `bus_a` (`pci@780`) du bus PCI-Express à un autre domaine.

4. Vérifiez `/etc/path_to_inst` pour trouver le chemin physique des ports réseau intégrés.

```
primary# grep e1000g /etc/path_to_inst
```

5. Supprimez le nœud terminal ne contenant pas le disque d'initialisation (`pci@780` dans cet exemple) du domaine `primary`.

```
primary# ldm remove-io pci@780 primary
```

6. Ajoutez cette configuration Split PCI (`split-cfg` dans cet exemple) au contrôleur système.

```
primary# ldm add-config split-cfg
```

Cette configuration (`split-cfg`) est également définie comme la prochaine configuration à utiliser après le redémarrage.

Remarque – Actuellement, le nombre de configurations pouvant être enregistrées sur le contrôleur système est limité à 8, sans compter la configuration `factory-default`.

7. Redémarrez le domaine `primary` pour que le changement prenne effet.

```
primary# shutdown -i6 -g0 -y
```

8. Ajoutez le nœud terminal (pci@780 dans cet exemple) au domaine (ldg1 dans cet exemple) ayant besoin d'un accès direct.

```
primary# ldm add-io pci@780 ldg1
Notice: the LDom Manager is running in configuration mode. Any
configuration changes made will only take effect after the machine
configuration is downloaded to the system controller and the
host is reset.
```

Si vous avez une carte Infiniband, il vous faudra peut-être activer le mode évitement sur le bus pci@780. Consultez la section « [Activation du mode évitement MMU E/S sur un bus PCI](#) », page 86 pour savoir si vous devez activer le mode évitement.

9. Redémarrez le domaine ldg1 pour que le changement prenne effet.

Tous les domaines doivent être inactifs pour ce redémarrage. Si c'est la première fois que vous configurez ce domaine, il est inactif.

```
ldg1# shutdown -i6 -g0 -y
```

10. Confirmez que le nœud terminal correct est toujours assigné au domaine primary et que le nœud terminal correct est assigné au domaine ldg1.

```
primary# ldm list-bindings primary
NAME          STATE  FLAGS  CONS  VCPU  MEMORY  UTIL  UPTIME
primary       active -n-cv  SP    4     4G      0.4%  18h 25m
...
IO
  DEVICE      PSEUDONYM  OPTIONS
  pci@7c0     bus_b
...
-----
NAME          STATE  FLAGS  CONS  VCPU  MEMORY  UTIL  UPTIME
ldg1          active -n---  5000  4     2G      10%   35m
...
IO
  DEVICE      PSEUDONYM  OPTIONS
  pci@780     bus_a
...
```

Ce résultat confirme que le nœud terminal PCI-E bus_b et les périphériques au-dessous de celui-ci sont assignés au domaine primary, et que bus_a et ses périphériques sont assignés au domaine ldg1.

Activation du mode évitement MMU E/S sur un bus PCI

Si vous avez une carte Infiniband HCA (Host Channel Adapter), il vous faudra peut-être activer le mode d'évitement de l'unité de gestion mémoire MMU (Memory Management Unit) E/S. Par défaut, le logiciel Logical Domains contrôle les transactions PCI-E de telle sorte qu'un périphérique E/S donné ou une option PCI-E puisse accéder uniquement à la mémoire physique assignée au sein du domaine E/S. L'unité MMU E/S empêche toute tentative d'accès à la mémoire d'un autre domaine hôte. Cela confère un niveau de sécurité plus élevé entre le domaine E/S et les autres domaines. Cependant, dans le rare cas où la carte d'option PCI-E ou PCI-X ne se charge pas ou ne fonctionne pas lorsque le mode évitement MMU E/S est désactivé, cette option vous permet d'activer ce dernier. Toutefois, si vous activez le mode évitement, la protection mise en œuvre au niveau matériel des accès mémoire à partir du domaine n'existe plus.

L'option `bypass=on` active le mode évitement de MMU E/S. Vous ne devez activer le mode évitement que si le domaine E/S respectif et les périphériques E/S au sein de celui-ci sont validés par l'ensemble des domaines hôtes. Cet exemple active le mode évitement.

```
primary# ldm add-io bypass=on pci@780 ldg1
```

Le résultat indique `bypass=on` sous `OPTIONS`.

Utilisation des groupes de consoles

Le démon de serveur de terminal réseau virtuel, `vntsd(1M)`, vous permet de fournir l'accès à plusieurs consoles de domaines en utilisant un seul port TCP. Au moment de la création d'un domaine, Logical Domains Manager assigne un port TCP unique à chaque console en créant un nouveau groupe par défaut pour cette console du domaine. Le port TCP est ensuite assigné au groupe de consoles plutôt qu'à la console elle-même. Vous pouvez lier la console à un groupe existant à l'aide de la sous-commande `set-vcons`.

▼ Procédure de combinaison de plusieurs consoles dans un groupe

1. Liez les consoles pour les domaines dans un seul groupe.

L'exemple suivant montre la liaison de la console pour trois domaines différents (ldg1, ldg2 et ldg3) au même groupe de consoles (group1).

```
primary# ldm set-vcons group=group1 service=primary-vcc0 ldg1
primary# ldm set-vcons group=group1 service=primary-vcc0 ldg2
primary# ldm set-vcons group=group1 service=primary-vcc0 ldg3
```

2. Connectez-vous au port TCP associé (localhost au port 5000 dans cet exemple).

```
# telnet localhost 5000
primary-vnts-group1: h, l, c{id}, n{name}, q:
```

Vous êtes invité à choisir l'une des consoles du domaine.

3. Listez les domaines du groupe en sélectionnant l'option l (list).

```
primary-vnts-group1: h, l, c{id}, n{name}, q: 1
DOMAIN ID          DOMAIN NAME          DOMAIN STATE
0                   ldg1                  online
1                   ldg2                  online
2                   ldg3                  online
```

Remarque – Pour réassigner la console à un autre groupe ou à une autre instance vcc, le domaine doit être dissocié, donc doit être dans l'état inactif. Reportez-vous à la page de manuel du SE Solaris 10 vntsd(1M) pour en savoir plus sur la configuration et l'utilisation de SMF pour gérer vntsd et sur l'utilisation des groupes de consoles.

Déplacement d'un domaine logique d'un serveur à l'autre

Vous pouvez déplacer un domaine logique, qui n'est pas en cours d'exécution, d'un serveur vers un autre. Avant de déplacer le domaine, si vous configurez le même domaine sur l'autre serveur, le déplacement sera plus simple. En fait, vous ne déplacez pas le domaine à proprement parler ; simplement, vous dissociez et arrêtez le domaine sur un serveur, puis le liez et le démarrez sur l'autre serveur.

▼ Procédure de configuration des domaines en vue d'un déplacement

1. Créez un domaine portant le même nom sur deux serveurs, par exemple, `domaineA1` sur `serveurA` et `serveurB`.
2. Ajoutez un périphérique serveur de disque virtuel et un disque virtuel sur les deux serveurs. Le serveur de disque virtuel ouvre le périphérique sous-jacent pour l'exportation lors du processus de liaison.
3. Liez le domaine uniquement sur un serveur, par exemple, `serveurA`. Laissez le domaine inactif sur l'autre serveur.

▼ Procédure de déplacement du domaine

1. Dissociez et arrêtez le domaine sur `serveurA`.
2. Liez et démarrez le domaine sur `serveurB`.

Remarque – Aucune ressource n'est utilisée tant que le domaine n'est pas lié.

Suppression de domaines logiques

Cette section décrit comment supprimer tous les domaines hôtes et revenir à une seule instance du SE qui contrôle l'intégralité du serveur.

▼ Procédure de suppression de tous les domaines logiques hôtes

1. Listez toutes les configurations de domaine logique sur le contrôleur système.

```
primary# ldm ls-config
```

2. Supprimez toutes les configurations (*config_name*) précédemment enregistrées sur le contrôleur système (SC). Utilisez la commande suivante pour chacune de ces configurations.

```
primary# ldm rm-config config_name
```

Une fois toutes les configurations précédemment enregistrées sur le contrôleur système supprimées, le domaine `factory-default` sera le prochain à utiliser au redémarrage du domaine de contrôle (`primary`).

3. Arrêtez tous les domaines hôtes en utilisant l'option `-a`.

```
primary# ldm stop-domain -a
```

4. Listez tous les domaines pour voir toutes les ressources attachées aux domaines hôtes.

```
primary# ldm ls
```

5. Libérez toutes les ressources attachées aux domaines hôtes. Pour cela, utilisez la commande `ldm unbind-domain` pour chaque domaine hôte (*ldom*) configuré sur votre système.

Remarque – Vous risquez de ne pas pouvoir dissocier un domaine E/S dans une configuration Split PCI s'il fournit des services requis par le domaine de contrôle. Dans ce cas, ignorez cette étape.

```
primary# ldm unbind-domain ldom
```

6. Arrêtez le domaine de contrôle.

```
primary# shutdown -i1 -g0 -y
```

7. Éteignez puis remettez sous tension le contrôleur système pour que la configuration `factory-default` soit rechargée.

```
SC> poweroff  
SC> poweron
```

Fonctionnement du SE Solaris avec Logical Domains

Cette section décrit les changements suivants dans l'utilisation du SE Solaris qui se produisent après qu'une configuration créée par Logical Domains Manager est instanciée, c'est-à-dire, que la mise en domaine est activée :

- « Arrêt puis remise sous tension d'un serveur », page 90
- « Résultat d'une commande `OpenBoot power-off` », page 91
- « Résultat d'une commande `shutdown` du SE Solaris », page 91
- « Résultat d'une combinaison de touches d'interruption du SE Solaris (L1-A) », page 91
- « Résultats de la halte ou du redémarrage du domaine de contrôle », page 92
- « Certaines options de la commande `format(1M)` ne fonctionnent pas avec des disques virtuels », page 93

Arrêt puis remise sous tension d'un serveur

Chaque fois que vous effectuez une maintenance sur un système exécutant le logiciel LDoms qui requiert l'arrêt puis la remise sous tension du serveur, il vous faut d'abord réaliser la procédure suivante.

▼ Procédure d'enregistrement des configurations de domaine logique actuelles sur le contrôleur système

- Utilisez la commande suivante.

```
# ldm add-config config_name
```

Résultat d'une commande OpenBoot power-off

La commande OpenBoot™ power-off ne met *pas* un système hors tension. Pour mettre hors tension un système durant l'exécution du microprogramme OpenBoot, utilisez la commande poweroff de votre contrôleur système ou processeur système. La commande OpenBoot power-off affiche le message suivant :

```
NOTICE: power-off command is not supported, use appropriate  
NOTICE: command on System Controller to turn power off.
```

Résultat d'une commande shutdown du SE Solaris

Si le démon Logical Domains Manager (ldmd) n'est pas activé, le SE Solaris se rend normalement à l'invite OpenBoot après l'invocation d'une commande shutdown(1M). Si le démon Logical Domains Manager (ldmd) est activé, vous obtenez l'invite suivante après l'arrêt.

```
r)eboot, o)k prompt, h)alt?
```

Tapez la lettre qui représente l'opération que le système doit effectuer après l'arrêt.

Résultat d'une combinaison de touches d'interruption du SE Solaris (L1-A)

Si le démon Logical Domains Manager (ldmd) n'est pas activé, le SE Solaris se rend normalement à l'invite OpenBoot après l'appui d'une combinaison de touches d'interruption (L1-A). Si le démon Logical Domains Manager (ldmd) est activé, vous obtenez l'invite suivante après ce type d'interruption.

```
c)ontinue, s)ync, r)eboot, h)alt?
```

Tapez la lettre qui représente l'opération que le système doit effectuer après ce type d'interruption.

Résultats de la halte ou du redémarrage du domaine de contrôle

Remarque – La question du [TABLEAU 5-1](#) demandant si le démon Logical Domains Manager (ldmd) est activé s’applique uniquement aux processeurs Sun UltraSPARC T1. ldmd est toujours activé sur les processeurs Sun UltraSPARC T2.

Le tableau suivant indique le comportement prévu pour la halte ou le redémarrage du domaine de contrôle (primary).

TABLEAU 5-1 Comportement prévu pour la halte ou le redémarrage du domaine de contrôle (primary)

Commande	ldmd activé ?	Autre domaine configuré ?	Comportement
halt	Désactivé	S/O	Pour les processeurs Sun UltraSPARC T1 : Déclenche l’invite ok.
	Activé	Non	Pour les processeurs Sun UltraSPARC T1 : Voir le message dans « Résultat d’une commande OpenBoot power-off », page 91. Pour les processeurs Sun UltraSPARC T2 : Hôte mis hors tension et demeure éteint jusqu’à la remise sous tension sur le SC.
	Activé	Oui	Réinitialisation à chaud et démarrage si auto-boot?=true. Réinitialisation à chaud et halte à l’invite ok si auto-boot?=false.
Redémarrage	Désactivé	S/O	Pour les processeurs Sun UltraSPARC T1 : Met l’hôte hors tension puis sous tension.
	Activé	Non	Pour les processeurs Sun UltraSPARC T1 : Met l’hôte hors tension puis sous tension. Pour les processeurs Sun UltraSPARC T2 : Redémarre l’hôte sans mise hors tension.
	Activé	Oui	Pour les processeurs Sun UltraSPARC T1 : Met l’hôte hors tension puis sous tension. Pour les processeurs Sun UltraSPARC T2 : Redémarre l’hôte sans mise hors tension.

TABEAU 5-1 Comportement prévu pour la halte ou le redémarrage du domaine de contrôle (primary) (suite)

Commande	ldmd activé ?	Autre domaine configuré ?	Comportement
shutdown -i 5	Désactivé	S/O	Pour les processeurs Sun UltraSPARC T1 : Met l'hôte hors tension.
	Activé	Non	Hôte mis hors tension et demeure éteint jusqu'à la remise sous tension sur le SC.
	Activé	Oui	Réinitialisation à chaud et redémarrage.

Si vous tapez **halt** à l'invite du SE Solaris, vous obtenez l'invite suivante.

```
r)eboot, o)k prompt, h)alt?
```

Si vous sélectionnez h)alt ou r)eboot, le comportement du Tableau 5-1 s'applique. Si vous sélectionnez l'invite o)k, le domaine est réinitialisé puis revient à l'invite ok. Cela est différent de l'affichage de l'invite ok lorsque la mise en domaine est désactivée.

Une réinitialisation à chaud redémarre le domaine avec l'implication du contrôleur système ou du contrôleur système blade virtuel (vBSC). Il en résulte une réinitialisation à chaud de la structure PCI.

Certaines options de la commande format(1M) ne fonctionnent pas avec des disques virtuels

La commande format(1M) du SE Solaris ne fonctionne pas sur un domaine hôte avec des disques virtuels :

- Certaines sous-commandes, telles que label, verify ou inquiry échouent avec des disques virtuels.
- La commande format(1M) risque d'afficher des messages tels que :
 - Inquiry failed
 - Disk unformatted
 - Current disk is unformatted
 - Drive type unknown
- La commande format(1M) s'arrête brutalement lorsque vous sélectionnez un disque virtuel qui porte une étiquette de disque EFI (extensible firmware interface, interface de microprogramme extensible).

- Si vous exécutez la commande `format(1M)` sur un domaine hôte, tous les disques virtuels sont vus comme non formatés, même s'ils sont correctement formatés et possèdent une étiquette de disque valide.

Pour obtenir ou définir la table des matières de volume (VTOC) d'un disque virtuel, utilisez la commande `prvtoc(1M)` et la commande `fmthard(1M)` au lieu de la commande `format(1M)`. Vous pouvez également utiliser la commande `format(1M)` à partir du domaine de service sur les disques réels.

Utilisation de LDoms avec ALOM CMT

Cette section décrit ce qu'il faut savoir pour utiliser le multithreading de puce (CMT, chip multithreading) d'Advanced Lights Out Manager (ALOM) avec Logical Domains Manager. Pour plus d'informations sur l'utilisation du logiciel ALOM CMT, reportez-vous au *Advanced Lights Out Management (ALOM) CMT v1.3 Guide*.



Attention – La documentation ALOM CMT fait référence à un seul domaine, vous devez donc être conscient que Logical Domains Manager introduit plusieurs domaines. Si un domaine logique est redémarré, les services E/S pour les domaines hôtes risquent de ne pas être disponibles tant que le domaine de contrôle n'a pas redémarré. Cela est dû au fait que le domaine de contrôle fonctionne comme un domaine de service dans le logiciel Logical Domains Manager 1.0.1. Les domaines hôtes semblent se geler durant le processus de redémarrage. Une fois le domaine de contrôle complètement redémarré, les domaines hôtes reprennent leurs opérations normales. Il est nécessaire d'arrêter les domaines hôtes uniquement lorsque le serveur entier va être mis hors tension.

Une option supplémentaire est disponible pour la commande ALOM CMT actuelle.

```
bootmode [normal|reset_nvram|bootscript=strong|config="config-name"]
```

L'option `config="config-name"` vous permet de définir la configuration à la prochaine mise sous tension selon une autre configuration, dont la configuration de livraison `factory-default`.

Vous pouvez invoquer la commande, que l'hôte soit sous tension ou hors tension. Elle prendra effet à la prochaine réinitialisation ou mise sous tension de l'hôte.

▼ Procédure de réinitialisation de la configuration du domaine logique à celle par défaut ou à une autre

- Pour réinitialiser la configuration du domaine logique à la prochaine mise sous tension selon la configuration par défaut de livraison, exécutez cette commande dans le logiciel ALOM CMT.

```
sc> bootmode config="factory-default"
```

Vous pouvez également sélectionner d'autres configurations créées avec Logical Domains Manager à l'aide de la commande `ldm add-config` et enregistrées sur le contrôleur système (SC). Le nom que vous spécifiez dans la commande Logical Domains Manager `ldm add-config` peut être utilisé pour sélectionner la configuration avec la commande ALOM CMT `bootmode`. Par exemple, supposons que vous ayez enregistré la configuration sous le nom `ldm-config1` :

```
sc> bootmode config="ldm-config1"
```

Reportez-vous à la page de manuel `ldm(1M)` ou au *Logical Domains (LDoms) Manager 1.0.1 Man Page Guide* pour plus d'informations sur la commande `ldm add-config`.

Activation et utilisation de l'audit BSM

Logical Domains Manager utilise la fonction d'audit du module de sécurité de base BSM (Basic Security module) du SE Solaris. L'audit BSM fournit les moyens d'examiner l'historique des actions et des événements sur votre domaine de contrôle afin de déterminer ce qui s'est passé. Dans l'historique est consigné ce qui est effectué, quand, par qui et ce qui a été touché.

Si vous voulez utiliser cette fonction d'audit, cette section explique comment activer, vérifier, désactiver, imprimer et faire un roulement des journaux d'audit. Vous pouvez trouver des informations supplémentaires sur l'audit BSM dans la documentation Solaris 10 *System Administration Guide: Security Services*.

Vous pouvez activer l'audit BSM de deux façons. Pour désactiver l'audit, veillez à utiliser la même méthode que celle appliquée pour l'activer. Les deux méthodes sont les suivantes :

- Utilisez le script `enable-bsm`.fin de Solaris Security Toolkit.

Par défaut, `ldm_control-secure.driver` n'utilise pas le script `enable-
bsm.fin`. Vous devez activer ce script sur le pilote que vous avez choisi.

- Utilisez la commande `bsmconv(1M)` du SE Solaris.

Voici les procédures pour les deux méthodes.

▼ Procédure d'utilisation du script `enable- bsm.fin`

1. Copiez `ldm_control-secure.driver` vers *my-ldm.driver*, où *my-ldm.driver* est le nom de votre copie de `ldm_control-secure.driver`.
2. Copiez `ldm_control-config.driver` vers *my-ldm-config.driver*, où *my-ldm-config.driver* est le nom de votre copie de `ldm_control-config.driver`.
3. Copiez `ldm_control-hardening.driver` vers *my-ldm-hardening.driver*, où *my-ldm-hardening.driver* est le nom de votre copie de `ldm_control-hardening.driver`.
4. Éditez *my-ldm.driver* pour faire référence aux nouveaux pilotes de configuration et de sécurisation, *my-ldm-control.driver* et *my-ldm-hardening.driver*, respectivement.
5. Éditez *my-ldm-hardening.driver* et supprimez le signe dièse (#) au début de la ligne suivante dans le pilote.

```
enable-bsm.fin
```

6. Exécutez *my-ldm.driver*.

```
# /opt/SUNWjass/bin/jass-execute -d my-ldm.driver
```

7. Redémarrez le SE Solaris pour que l'audit prenne effet.

▼ Procédure d'utilisation de la commande `bsmconv(1M)` du SE Solaris

1. Ajoutez `vs` dans la ligne `flags` du fichier `/etc/security/audit_control`.

2. Exécutez la commande `bsmconv(1M)`.

```
# /etc/security/bsmconv
```

Pour plus d'informations sur cette commande, reportez-vous à la documentation Solaris 10 Reference Manual Collection ou à la page de manuel.

3. Redémarrez le système d'exploitation Solaris pour que l'audit prenne effet.

▼ Procédure permettant de vérifier que l'audit BSM est activé

1. Saisissez la commande suivante.

```
# auditconfig -getcond
```

2. Vérifiez que `audit condition = auditing` apparaît dans le résultat.

▼ Procédure de désactivation de l'audit

Vous pouvez désactiver l'audit de deux manières, selon la façon dont vous l'avez activé. Pour plus d'informations, reportez-vous à la section « [Activation et utilisation de l'audit BSM](#) », page 95.

1. Effectuez l'une des opérations suivantes.

- Annulez l'exécution de sécurisation de Solaris Security Toolkit qui a activé l'audit BSM.

```
# /opt/SUNWjass/bin/jass-execute -u
```

- Utilisez la commande `bsmunconv(1M)` du SE Solaris.

```
# /etc/security/bsmunconv
```

2. Redémarrez le SE Solaris pour que la désactivation de l'audit prenne effet.

▼ Procédure d'impression du résultat d'audit

- Utilisez l'une des opérations suivantes pour imprimer le résultat d'audit BSM.

- Utilisez les commandes du SE Solaris `auditreduce(1M)` et `praudit(1M)` pour imprimer le résultat d'audit. Par exemple :

```
# auditreduce -c vs | praudit
# auditreduce -c vs -a 20060502000000 | praudit
```

- Utilisez la commande du SE Solaris `praudit -x` pour imprimer le résultat XML.

▼ Procédure de roulement des journaux d'audit

- Utilisez la commande du SE Solaris `audit -n` pour faire un roulement des journaux d'audit.

Configuration du commutateur virtuel et du domaine de service pour NAT et routage

Le commutateur virtuel (`vswitch`) est un commutateur de couche 2, qui est également utilisable comme périphérique réseau dans le domaine de service. Vous pouvez configurer le commutateur virtuel pour qu'il agisse uniquement comme un commutateur entre les périphériques réseau virtuels (`vnet`) sur les divers domaines logiques, mais sans connectivité avec un réseau particulier via un périphérique physique. Dans ce mode, le raccordement de `vswitch` en tant que périphérique réseau, en activant le routage IP dans le domaine de service, permet aux réseaux virtuels de communiquer en utilisant le domaine de service comme un routeur. Ce mode de fonctionnement est essentiel pour fournir la connectivité externe aux domaines lorsque l'adaptateur du réseau physique n'est pas compatible GLDv3.

Les avantages de cette configuration sont les suivants :

- Le commutateur virtuel ne nécessite pas l'utilisation d'un périphérique physique directement et peut fournir une connectivité externe même si le périphérique sous-jacent n'est pas compatible GLDv3.
- La configuration peut tirer avantage des capacités de routage et de filtrage IP du SE Solaris.

▼ Procédure de configuration du commutateur virtuel afin de fournir la connectivité externe aux domaines

1. Créez un commutateur virtuel sans périphérique physique associé.

Si vous assignez une adresse, vérifiez que le commutateur virtuel possède une adresse MAC unique.

```
primary# ldm add-vsw [mac-addr=xxxxxxxxxxxx] primary-vsw0 primary
```

2. Raccordez le commutateur virtuel en tant que périphérique réseau en plus du périphérique réseau physique utilisé par le domaine.

Reportez-vous à la section « [Procédure de configuration du commutateur](#) », page 47 pour plus d'informations sur le raccordement du commutateur virtuel.

3. Configurez le périphérique commutateur virtuel pour DHCP, si nécessaire.

Reportez-vous à la section « [Procédure de configuration du commutateur](#) », page 47 pour plus d'informations sur la configuration du périphérique commutateur virtuel pour DHCP.

4. Créez le fichier `/etc/dhcp.vsw`, si nécessaire.

5. Configurez le routage IP dans le domaine de service et installez les tables de routage requises dans tous les domaines.

Pour plus d'informations sur cette procédure, reportez-vous à la section « Packet Forwarding and Routing on IPv4 Networks » du chapitre 5 « Configuring TCP/IP Network Services and IPv4 Administration » du manuel *System Administration Guide: IP Services* de Solaris Express System Administrator Collection.

Utilisation de ZFS avec des disques virtuels

Cette section décrit les sujets suivants concernant l'utilisation du système de fichiers ZFS (Zettabyte File System) avec des disques virtuels sur des domaines logiques :

- « [Création d'un disque virtuel sur un volume ZFS](#) », page 100
- « [Utilisation de ZFS sur un disque virtuel](#) », page 101
- « [Utilisation de ZFS sur des disques d'initialisation](#) », page 103

Création d'un disque virtuel sur un volume ZFS

Les procédures suivantes expliquent comment créer un volume ZFS dans un domaine de service et le rendre disponible aux autres domaines en tant que disque virtuel. Dans cet exemple, le domaine de service, identique au domaine de contrôle, est nommé `primary`. Le domaine hôte est nommé `ldg1`, par exemple. Les invites de chaque étape montrent dans quel domaine la commande est exécutée.

▼ Procédure de création d'un disque virtuel sur un volume ZFS

1. Créez un pool de stockage ZFS (`zpool`).

```
primary# zpool create -f tank1 c2t42d1
```

2. Créez un volume ZFS.

```
primary# zfs create -V 100m tank1/myvol
```

3. Vérifiez que le `zpool` (`tank1` dans cet exemple) et le volume ZFS (`tank1/myvol` dans cet exemple) ont été créés.

```
primary# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPOINT
tank1	100M	43.0G	24.5K	/tank1
tank1/myvol	22.5K	43.1G	22.5K	-

4. Configurez un service qui exporte `tank1/myvol` en tant que disque virtuel.

```
primary# ldm add-vdsdev /dev/zvol/rdisk/tank1/myvol zvol@primary-vds0
```

5. Ajoutez le disque exporté à un autre domaine (`ldg1` dans cet exemple).

```
primary# ldm add-vdisk vdisk zvol@primary-vds0 ldg1
```

6. Sur l'autre domaine (`ldg1` dans cet exemple), démarrez le domaine et assurez-vous que le nouveau disque virtuel est visible (il vous faudra peut-être exécuter la commande `devfsadm`).

Dans cet exemple, le nouveau disque apparaît comme `/dev/rdisk/c2d2s0`.

```
ldg1# newfs /dev/rdisk/c2d2s0
newfs: construct a new file system /dev/rdisk/c2d2s0: (y/n)? y
Warning: 4096 sector(s) in last cylinder unallocated
```

```
Warning: 4096 sector(s) in last cylinder unallocated
/dev/rdisk/c2d2s0: 204800 sectors in 34 cylinders of 48 tracks, 128 sectors
100.0MB in 3 cyl groups (14 c/g, 42.00MB/g, 20160 i/g) super-block backups
(for fsck -F ufs -o b=#) at: 32, 86176, 172320,

ldg1# mount /dev/dsk/c2d2s0 /mnt

ldg1# df -h /mnt
Filesystem                size      used   avail capacity  Mounted on
/dev/dsk/c2d2s0           93M       1.0M    82M        2%   /mnt
```

Remarque – Un volume ZFS est exporté vers un domaine logique en tant que tranche de disque virtuel. Par conséquent, il n'est pas possible d'utiliser la commande `format` ni d'installer le SE Solaris sur un disque virtuel s'appuyant sur un `zvol`.

Utilisation de ZFS sur un disque virtuel

La procédure suivante montre comment utiliser directement ZFS à partir d'un domaine sur un disque virtuel. Vous pouvez créer des pools, des systèmes de fichiers et des volumes ZFS sur des disques virtuels à l'aide des commandes du SE Solaris 10 `zpool(1M)` et `zfs(1M)`. Bien que l'arrière-plan de stockage soit différent (des disques virtuels au lieu de disques physiques), il n'y a pas de changement dans l'utilisation de ZFS.

De plus, si vous avez déjà un système de fichiers ZFS, vous pouvez l'exporter à partir d'un domaine de service pour l'utiliser dans un autre domaine.

Dans cet exemple, le domaine de service, identique au domaine de contrôle, est nommé `primary`. Le domaine hôte est nommé `ldg1`, par exemple. Les invites de chaque étape montrent dans quel domaine la commande sera exécutée.

▼ Procédure d'utilisation de ZFS sur un disque virtuel

1. Créez un pool ZFS (`tank` dans cet exemple), puis vérifiez qu'il a été créé.

```
primary# zpool create -f tank c2t42d0
primary# zpool list
NAME                SIZE      USED   AVAIL    CAP    HEALTH   ALTROOT
tank                43.8G     108K    43.7G     0%    ONLINE   -
```

2. Créez un système de fichiers ZFS (tank/test dans cet exemple), puis vérifiez qu'il a été créé.

Dans cet exemple, le système de fichiers est créé sur le disque c2t42d0 en exécutant la commande suivante sur le domaine de service.

```
primary# zfs create tank/test
primary# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPOINT
tank	106K	43.1G	25.5K	/tank
tank/test	24.5K	43.1G	24.5K	/tank/test

3. Exportez le pool ZFS (tank dans cet exemple).

```
primary# zpool export tank
```

4. Configurez un service qui exporte le disque physique c2t42d0s2 en tant que disque virtuel.

```
primary# ldm add-vdsdev /dev/rdisk/c2t42d0s2 volz@primary-vds0
```

5. Ajoutez le disque exporté à un autre domaine (ldg1 dans cet exemple).

```
primary# ldm add-vdisk vdiskz volz@primary-vds0 ldg1
```

6. Sur l'autre domaine (ldg1 dans cet exemple), démarrez le domaine et assurez-vous que le nouveau disque virtuel est visible (il vous faudra peut-être exécuter la commande devfsadm), puis importez le pool ZFS.

```
ldg1# zpool import tank
ldg1# zpool list
```

NAME	SIZE	USED	AVAIL	CAP	HEALTH	ALTROOT
tank	43.8G	214K	43.7G	0%	ONLINE	-

```
ldg1# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPOINT
tank	106K	43.1G	25.5K	/tank
tank/test	24.5K	43.1G	24.5K	/tank/test

```
ldg1# df -hl -F zfs
```

Filesystem	size	used	avail	capacity	Mounted on
tank	43G	25K	43G	1%	/tank
tank/test	43G	24K	43G	1%	/tank/test

Le pool ZFS (tank/test dans cet exemple) est maintenant importé et utilisable à partir du domaine ldg1.

Utilisation de ZFS sur des disques d'initialisation

Vous pouvez utiliser un système de fichiers ZFS avec un fichier volumineux comme les disques virtuels dans des domaines logiques.

Remarque – Un système de fichiers ZFS requiert plus de mémoire dans le domaine de service. Tenez en compte lors de la configuration du domaine de service.

ZFS permet de :

- Cloner un système de fichiers rapidement
- Utiliser les clones pour approvisionner des domaines supplémentaires
- L'installation réseau vers disque sur des fichiers et des fichiers au sein d'un système de fichiers ZFS

▼ Procédure d'utilisation de ZFS sur des disques d'initialisation

Vous pouvez utiliser la procédure suivante afin de créer des disques ZFS pour des domaines logiques ; vous pouvez également créer leur image instantanée et les cloner pour d'autres domaines.

1. Sur le domaine `primary`, réservez un disque entier ou une tranche à utiliser comme stockage pour le pool ZFS. L'étape 2 utilise la tranche 5 d'un disque.
2. Créez un pool ZFS, par exemple `ldomspool`.

```
# zpool create ldomspool /dev/dsk/c0t0d0s5
```

3. Créez un système de fichiers ZFS pour le premier domaine (`ldg1` dans cet exemple).

```
# zfs create ldomspool/ldg1
```

4. Créez un fichier qui sera le disque pour ce domaine.

```
# mkfile 1G /ldomspool/ldg1/bootdisk
```

5. Spécifiez le fichier comme étant le périphérique à utiliser lors de la création du domaine.

```
primary# ldm add-vdsdev /ldomspool/ldg1/bootdisk vol1@primary-vds0
primary# ldm add-vdisk vdisk1 vol1@primary-vds0 ldg1
```

6. Initialisez le domaine `ldg1` et faites une installation réseau (`net install`) vers `vdisk1`. Le fichier fonctionne comme un disque entier et peut posséder des partitions, en l'occurrence, des partitions distinctes pour `root`, `usr`, `home`, `dump` et `swap`.
7. Une fois l'installation terminée, créez l'image instantanée du système de fichiers.

```
# zfs snapshot ldomspool/ldg1@initial
```

Remarque – La création de l'instantané avant le redémarrage du domaine n'enregistre pas l'état du domaine dans l'instantané ou dans les clones créés à partir de l'instantané.

8. Créez des clones supplémentaires à partir de l'instantané et utilisez celui-ci en tant que disque d'initialisation pour d'autres domaines (`ldg2` et `ldg3` dans cet exemple).

```
# zfs clone ldomspool/ldg1@initial ldomspool/ldg2
# zfs clone ldomspool/ldg1@initial ldomspool/ldg3
```

9. Vérifiez que tout a été créé correctement.

```
# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPOINT
ldomspool	1.07G	2.84G	28.5K	/ldomspool
ldomspool/ldg1	1.03G	2.84G	1.00G	/ldomspool/ldg1
ldomspool/ldg1@initial	23.0M	-	1.00G	-
ldomspool/ldg2	23.2M	2.84G	1.00G	/ldomspool/ldg2
ldomspool/ldg3	21.0M	2.84G	1.00G	/ldomspool/ldg3

Remarque – Assurez-vous que le pool ZFS dispose d'un espace suffisant pour les clones créés. ZFS utilise la copie-écriture et emploie l'espace du pool uniquement lorsque les blocs sont modifiés dans le clone. Même après l'initialisation du domaine, les clones n'utilisent qu'un faible pourcentage nécessaire pour le disque (puisque la plupart des fichiers binaires du système d'exploitation sont identiques à ceux de l'instantané `initial`).

Utilisation des gestionnaires de volume dans un environnement Logical Domains

Les sujets suivants sont traités dans cette section :

- « Utilisation de disques virtuels sur des gestionnaires de volume », page 105
- « Utilisation de gestionnaires de volume sur des disques virtuels », page 108

Utilisation de disques virtuels sur des gestionnaires de volume

Tout système de fichiers ZFS (Zettabyte File System) ou gestionnaire de volume SVM (Solaris™ Volume Manager) ou VxVM (Veritas Volume Manager) peut être exporté à partir d'un domaine de service vers un domaine hôte en tant que disque virtuel. Le volume exporté apparaît comme un disque virtuel avec une seule tranche (s0) dans le domaine hôte.

Remarque – Le reste de cette section utilise un volume SVM comme exemple. Cependant, les explications s'appliquent également aux volumes ZFS et VxVM.

Par exemple, si un domaine de service exporte le volume SVM `/dev/md/dsk/d0` vers `domain1` et si `domain1` voit ce disque virtuel comme `/dev/dsk/c0d2*`, alors `domain1` possède uniquement un périphérique `s0`, en l'occurrence, `/dev/dsk/c0d2s0`.

Le disque virtuel du domaine hôte (par exemple, `/dev/dsk/c0d2s0`) est directement mappé au volume associé (par exemple, `/dev/md/dsk/d0`), et les données stockées sur le disque virtuel à partir du domaine hôte sont directement stockées sur le volume associé sans métadonnées supplémentaires. Ainsi, les données stockées sur le disque virtuel à partir du domaine hôte sont également accessibles directement à partir du domaine de service via le volume associé.

Exemples :

- Si le volume SVM `d0` est exporté à partir du domaine `primary` vers `domain1`, alors la configuration de `domain1` nécessite quelques étapes supplémentaires.

```
primary# metainit d0 3 1 c2t70d0s6 1 c2t80d0s6 1 c2t90d0s6
primary# ldm add-vdsdev /dev/md/dsk/d0 vol3@primary-vds0
primary# ldm add-vdisk vdisk3 vol3@primary-vds0 domain1
```

- Une fois domain1 lié et démarré, le volume exporté apparaît comme /dev/dsk/c0d2s0, par exemple, et vous pouvez l'utiliser.

```
domain1# newfs /dev/rdisk/c0d2s0
domain1# mount /dev/dsk/c0d2s0 /mnt
domain1# echo test-domain1 > /mnt/file
```

- Une fois domain1 arrêté et dissocié, les données stockées sur le disque virtuel à partir de domain1 sont accessibles directement à partir du domaine principal via le volume SVM d0.

```
primary# mount /dev/md/dsk/d0 /mnt
primary# cat /mnt/file
test-domain1
```

Remarque – Un tel disque virtuel n'est pas visible par la commande `format(1M)`, et ne peut être partitionné, ni utilisé comme un disque d'installation pour le SE Solaris. Reportez-vous à la section « [Certaines options de la commande `format\(1M\)` ne fonctionnent pas avec des disques virtuels](#) », page 93 pour plus d'informations à ce sujet.

Remarque sur l'utilisation des disques virtuels sur un volume SVM

Lorsqu'un volume SVM RAID ou miroir est utilisé en tant que disque virtuel par un autre domaine, s'il y a une panne sur l'un des composants de ce volume, la récupération de celui-ci à l'aide de la commande `metareplace` ou en utilisant un disque hot spare ne démarre pas. La commande `metastat` voit le volume comme étant en cours de resynchronisation, mais sans progression de celle-ci.

Par exemple, /dev/md/dsk/d0 est un volume SVM RAID exporté en tant que disque virtuel vers un autre domaine, et d0 est configuré avec quelques périphériques hot spare. Si un composant de d0 tombe en panne, SVM remplace ce composant par un hot spare et resynchronise le volume SVM. Cependant, la resynchronisation ne démarre pas. Le volume est signalé comme étant en cours de resynchronisation, mais sans progression de celle-ci.

```
# metastat d0
d0: RAID
    State: Resyncing
    Hot spare pool: hsp000
    Interlace: 32 blocks
    Size: 20097600 blocks (9.6 GB)
```

```
Original device:
  Size: 20100992 blocks (9.6 GB)
Device                               Start Block  Dbase   State Reloc
c2t2d0s1                             330         No      Okay   Yes
c4t12d0s1                             330         No      Okay   Yes
/dev/dsk/c10t600C0FF0000000000015153295A4B100d0s1 330         No      Resyncing Yes
```

Dans un tel cas, le domaine utilisant le volume SVM comme un disque virtuel doit être arrêté et dissocié pour terminer la resynchronisation. Le volume SVM peut alors être resynchronisé en utilisant la commande `metasync`.

```
# metasync d0
```

Remarque sur l'utilisation des disques virtuels lorsque VxVM est installé

Lorsque le gestionnaire de volume VxVM (Veritas Volume Manager) est installé sur votre système, vous devez vous assurer que le multiacheminement dynamique DMP (Dynamic Multipathing) Veritas n'est pas activé sur les disques physiques ou les partitions que vous voulez exporter en tant que disques virtuels. Sinon, vous obtenez une erreur dans `/var/adm/messages` lors de la liaison d'un domaine utilisant un tel disque.

```
vd_setup_vd(): ldi_open_by_name(/dev/dsk/c4t12d0s2) = errno 16
vds_add_vd(): Failed to add vdisk ID 0
```

Vous pouvez vérifier si DMP Veritas est activé en contrôlant les informations de multiacheminement dans le résultat de la commande `vxdisk list`, par exemple :

```
# vxdisk list Disk_3
Device:      Disk_3
devicetag:   Disk_3
type:        auto
info:        format=none
flags:       online ready private autoconfig invalid
pubpaths:    block=/dev/vx/dmp/Disk_3s2 char=/dev/vx/rdmp/Disk_3s2
guid:        -
udid:        SEAGATE%5FST336753LSUN36G%5FDISKS%5F3032333948303144304E0000
site:        -
Multipathing information:
numpaths:    1
c4t12d0s2    state=enabled
```

Si DMP Veritas est activé sur un disque ou une tranche que vous voulez exporter en tant que disque virtuel, vous devez désactiver DMP à l'aide de la commande `vxddmpadm`. Par exemple :

```
# vxddmpadm -f disable path=/dev/dsk/c4t12d0s2
```

Utilisation de gestionnaires de volume sur des disques virtuels

Cette section décrit les situations suivantes dans l'environnement Logical Domains :

- « [Utilisation de ZFS sur des disques virtuels](#) », page 108
- « [Utilisation de SVM sur des disques virtuels](#) », page 108
- « [Utilisation de VxVM sur des disques virtuels](#) », page 109

Utilisation de ZFS sur des disques virtuels

Tout disque virtuel est utilisable avec ZFS. Un pool de stockage ZFS (`zpool`) peut être importé dans un domaine qui voit tous les périphériques de stockage appartenant au `zpool`, que ce domaine les voit comme des périphériques virtuels ou comme des périphériques réels.

Utilisation de SVM sur des disques virtuels

Tout disque virtuel est utilisable dans l'ensemble des disques locaux SVM. Par exemple, un disque virtuel peut être utilisé pour le stockage de la base de métadonnées SVM (`metadb`) de l'ensemble des disques locaux ou pour la création de volumes SVM dans cet ensemble.

Actuellement, vous pouvez utiliser les disques virtuels uniquement avec l'ensemble des disques locaux, mais pas avec un ensemble de disques partagés (`metaset`). Vous ne pouvez pas ajouter de disques virtuels dans un ensemble de disques partagés SVM. Si vous essayez d'ajouter un disque virtuel dans un ensemble de disques partagés SVM, vous obtenez une erreur similaire à la suivante :

```
# metaset -s test -a c2d2
metaset: domain1: test: failed to reserve any drives
```

Utilisation de VxVM sur des disques virtuels

Actuellement, VxVM ne fonctionne pas avec des disques virtuels. Vous pouvez installer le logiciel VxVM dans un domaine possédant des disques virtuels, mais VxVM n'a pas la capacité de les voir comme disques disponibles.

Configuration d'IPMP dans un environnement Logical Domains

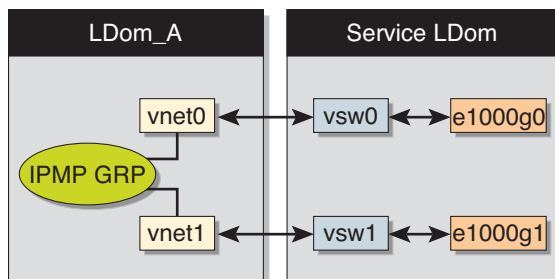
Le multiacheminement IPMP (Internet Protocol Network Multipathing) fournit la tolérance de pannes et l'équilibrage de charge sur de multiples cartes d'interface réseau. En utilisant IPMP, vous pouvez configurer une ou plusieurs interfaces dans un groupe de multiacheminement IP. Après la configuration IPMP, le système contrôle automatiquement les interfaces du groupe IPMP pour détecter les pannes. Si une interface du groupe tombe en panne ou est retirée pour maintenance, IPMP migre ou bascule automatiquement les adresses IP de cette interface. Dans un environnement Logical Domains, vous pouvez configurer les interfaces physiques ou virtuelles pour le basculement en utilisant IPMP.

Configuration de périphériques réseau virtuels dans un groupe IPMP au sein d'un domaine logique

Il est possible de configurer un domaine logique pour la tolérance de pannes en configurant ses périphériques réseau virtuels en groupe IPMP. Pour configurer un groupe IPMP avec des périphériques réseau virtuels, dans une configuration active de réserve, configurez-le afin qu'il utilise la détection par investigation. Actuellement, le logiciel Logical Domains 1.0.1 ne prend pas en charge la détection et le basculement par liaison pour les périphériques réseau virtuels.

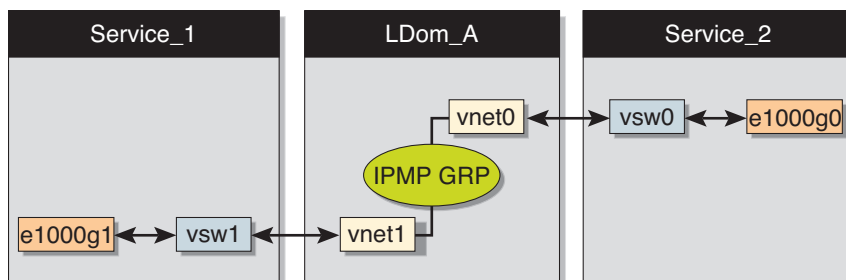
Le diagramme suivant montre deux réseaux virtuels (vnet1 et vnet2) connectés à deux instances de commutateur virtuel distinctes (vsw0 et vsw1) dans le domaine de service, qui, à leur tour, utilisent deux interfaces physiques différentes (e1000g0 et e1000g1). En cas de panne d'une interface physique, la couche IP dans LDom_A détecte la panne et la perte de connectivité sur le réseau vnet correspondant par une détection basée sur investigation, et bascule automatiquement vers le périphérique vnet secondaire.

FIGURE 5-1 Deux réseaux virtuels connectés à des instances de commutateur virtuel distinctes



Il est possible d'obtenir une plus grande fiabilité dans le domaine logique en connectant chaque périphérique réseau virtuel (vnet0 et vnet1) à des instances de commutateur virtuel dans des domaines de service différents (comme indiqué dans le diagramme suivant). Il est possible de configurer deux domaines de service (Service_1 et Service_2) avec des instances de commutateur virtuel (vsw1 et vsw2) en utilisant une configuration Split PCI. Dans ce cas, en plus de la panne matérielle réseau, LDom_A peut détecter une panne de réseau virtuel et déclencher un basculement suite à une interruption brutale ou à un arrêt du domaine de service.

FIGURE 5-2 Connexion des périphériques réseau virtuels à différents domaines de service



Reportez-vous à la documentation *Solaris 10 System Administration Guide: IP Services* pour en savoir plus sur la configuration et l'utilisation des groupes IPMP.

Configuration et utilisation d'IPMP dans un domaine de service

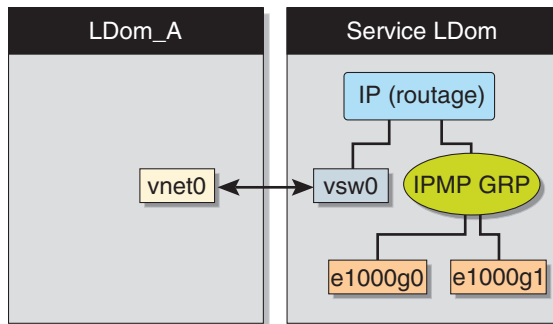
Il est également possible de configurer la détection de panne réseau et la reprise dans un environnement Logical Domains en configurant les interfaces physiques en groupe IPMP dans le domaine de service. Pour cela, configurez le commutateur virtuel dans le

domaine de service en tant que périphérique réseau, puis configurez le domaine de service pour qu'il agisse en tant que routeur IP. (Voir la documentation Solaris 10 *System Administration Guide: IP Services* pour plus d'informations sur la configuration du routage IP).

Une fois configuré, le commutateur virtuel envoie tous les paquets émanant des réseaux virtuels (et destinés à une machine externe) à sa couche IP, au lieu de les envoyer directement via le périphérique physique. En cas de panne d'une interface physique, la couche IP détecte la panne et réachemine automatiquement les paquets via l'interface secondaire.

Étant donné que les interfaces physiques sont configurées directement en groupe IPMP, le groupe peut être configuré pour une détection soit par liaison, soit par investigation. Le diagramme suivant montre deux interfaces réseau (e1000g0 et e1000g1) configurées comme appartenant à un groupe IPMP. L'instance de commutateur virtuel (vsw0) a été raccordée à un périphérique réseau pour envoyer les paquets à sa couche IP.

FIGURE 5-3 Deux interfaces réseau configurées en groupe IPMP



Glossaire

Cette liste définit la terminologie, les abréviations et les acronymes utilisés dans la documentation relative à Logical Domains 1.0.1.

A

- ALOM CMT** Advanced Lights Out Manager, technologie de multithreading de puce s'exécutant sur le contrôleur système et permettant de surveiller et de contrôler le serveur CMT
- AP** Adresse physique
- AR** Adresse réelle
- Audit** Fonction utilisant le BSM du SE Solaris pour identifier l'origine des modifications de sécurité
- Autorisation** Fonction permettant de définir des autorisations à l'aide du RBAC du SE Solaris

B

- bge** Broadcom Gigabit Ethernet, pilote Ethernet Gigabit Broadcom des périphériques Broadcom BCM57xx
- BSM** Basic Security module, module de sécurité de base

C

CLI	Command-Line Interface, interface de ligne de commande
CMT	Multithreading de puce
Compatibilité	Fonction permettant de déterminer si une configuration d'un système est conforme à un profil de sécurité prédéfini
Config	Nom de la configuration de domaine logique enregistrée sur le contrôleur système
Contraintes	Dans le logiciel Logical Domains Manager, les contraintes représentent une ou plusieurs ressources à affecter à un domaine spécifique. En fonction de la disponibilité des ressources, vous recevez toutes celles que vous souhaitez ajouter à un domaine ou vous n'en recevez aucune.
CPU	Central Processing Unit, unité de calcul centrale
CWQ	Control Word Queue, unité cryptographique pour plates-formes Sun UltraSPARC T2

D

DHCP	Abréviation de Dynamic Host Configuration Protocol
DMP	Dynamic Multipathing (Veritas), multiacheminement dynamique
DO	Description de l'ordinateur dans la base de données des serveurs
Domaine de contrôle	Domaine qui crée et gère d'autres domaines logiques et d'autres services.
Domaine d'E/S	Domaine détenant et ayant un accès direct aux périphériques d'E/S physiques et partageant ces périphériques avec les autres domaines logiques sous forme de périphériques virtuels
Domaine de service	Domaine logique fournissant des services de périphérique (tels que des commutateurs virtuels, des connecteurs de consoles virtuelles et des serveurs de disques virtuels) à d'autres domaines logiques
Domaine hôte	Domaine géré par le domaine de contrôle et qui utilise les services des domaines d'E/S et de service.
Domaine logique	Regroupement logique discret doté de son propre système d'exploitation, de ses propres ressources et de sa propre identité au sein d'un seul système informatique

- drd(1M)** Dynamic reconfiguration daemon, démon de reconfiguration dynamique de Logical Domains Manager (SE Solaris 10)
- DS** Domain Services module, module des services de domaine (SE Solaris 10)
-

E

- e1000g** Pilote pour la famille de contrôleurs d'interface réseau Intel PRO/1000 Gigabit
- EFI** Extensible Firmware interface, interface microprogramme extensible
- E/S** Périphériques d'E/S, tels que des disques internes et des contrôleurs PCI-Express (PCI-E) et les adaptateurs et périphériques associés
- ETM** Encoding Table Management module, module de gestion de tables d'encodage (SE Solaris 10)
-

F

- FC_AL** Fiber Channel Arbitrated Loop, boucle arbitrée Fibre Channel
- FMA** Fault Management Architecture, architecture de gestion des pannes
- fmd(1M)** Fault Manager daemon, démon du gestionnaire de pannes (SE Solaris 10)
- FTP** File Transfer Protocol, protocole de transfert de fichier
-

G

- GLDv3** Generic LAN Driver version 3, pilote LAN générique version 3
-

H

- HDD** Hard Disk Drive, unité de disque dur
- Hyperviseur** Couche microprogramme entre le système d'exploitation et la couche matérielle

I

- IB** Infiniband
- ioctl** input/output control call, appel de contrôle d'entrée/sortie
- IP** Internet Protocol, protocole Internet
- IPMP** Internet Protocol Network Multipathing, multiacheminement sur réseau IP

K

- kaio** Kernel asynchronous input/output, entrée/sortie asynchrone du noyau
- Ko** Kilo-octet
- KU** Kernel Update, mise à jour du noyau

L

- LAN** Local-Area Network, réseau local
- LDAP** Lightweight Directory Access Protocol, protocole léger d'accès aux répertoires
- LDC** Logical Domain Channel, canal de domaine logique
- ldm(1M)** Utilitaire Logical Domain Manager
- ldmd** Démon de Logical Domains Manager
- Logical Domains (LDoms) Manager** Logiciel doté d'une CLI permettant de créer et de gérer des domaines et de leur affecter des ressources

M

MAC	Media access control address, adresse de contrôle d'accès aux médias pouvant être affectée automatiquement par LDoms ou que vous pouvez affecter manuellement
MAU	Modular Arithmetic Unit, unité cryptographique pour plates-formes Sun UltraSPARC T1
<code>mem, memory</code>	Unité de mémoire : taille par défaut en octets, en giga-octets (G), en kilo-octets (K) ou en méga-octets (M). Mémoire serveur virtualisée pouvant être allouée aux domaines hôtes.
MIB	Management Information Base, informations de la base de données de gestion
Minimisation	Fonction permettant d'installer le nombre minimum de packages de SE Solaris de base nécessaire
MMF	Multimode Fiber, fibre multimode
MMU	Memory Management Unit, unité de gestion de la mémoire
Mo	Méga-octet
<code>mtu</code>	Maximum Transmission Unit, unité de transmission maximale

N

NAT	Network Address Translation, traduction d'adresse réseau
<code>ndpsldcc</code>	Netra Data Plane Software Logical Domain Channel Client, client du canal de domaine logique de Netra Data Plane Software. <i>Voir aussi</i> <code>vdpc</code> .
<code>ndpsldcs</code>	Netra Data Plane Software Logical Domain Channel Service, service de canal de domaine logique de Netra Data Plane Software. <i>Voir aussi</i> <code>vdpcs</code> .
NDPSS	Abréviation de Netra Data Plane Software Suite
NFS	Network File System, système de fichiers réseau
NIS	Network Information Services, services d'information réseau
NIU	Network Interface Unit, unité d'interface de réseau (serveurs Sun SPARC Enterprise T5120 et T5220)
NTS	Network Terminal Server, serveur de terminal réseau

NVRAM Non-volatile Random Access Memory, mémoire vive non volatile
nxge Pilote pour l'adaptateur Ethernet Sun x8 Express 1/10G

P

PCI Peripheral Component Interconnect Bus, bus PCI
PCI-E Bus PCI-Express
PCI-X Extension du bus PCI
PICL Platform Information and Control Library, bibliothèque de contrôle et d'informations des plates-formes
picld(1M) Démon de PICL
PRI Priorité

R

RAID Abréviation de Redundant Array of Inexpensive Disks
RBAC Role-Based Access Control, contrôle d'accès basé sur les rôles
RD Reconfiguration dynamique
RPC Remote Procedure Call, appel de procédure à distance

S

SC System Controller, contrôleur système (similaire à processeur système)
SCSI Abréviation de Small Computer System Interface
SE Système d'exploitation
Sécurisation Fonction permettant de modifier des configurations du SE Solaris afin d'améliorer la sécurité
SMA System Management Agent, agent de gestion système

SMF	Service Management Facility, utilitaire de gestion de services du SE Solaris 10
SNMP	Simple Network Management Protocol, protocole de gestion de réseau simple
SP	System Processor, processeur système (similaire à contrôleur système)
SSH	Secure Shell, shell sécurisé
<code>ssh(1)</code>	Commande de shell sécurisé
<code>sshd(1M)</code>	Démon du shell sécurisé
SunVTS	Abréviation de Sun Validation Test Suite
SVM	Abréviation de Solaris Volume Manager

T

TCP	Transmission Control Protocol, protocole de contrôle des transmissions
------------	--

U

UDP	Abréviation de User Datagram Protocol
USB	Universal Serial Bus, bus série universel
UTP	Unshielded Twisted Pair, paire torsadée non blindée

V

vBSC	Virtual Blade System Controller, contrôleur système de lame virtuelle
<code>vcc, vconscon</code>	Virtual console concentrator service, service de concentrateur de consoles virtuelles doté d'une plage de numéros de port spécifique à affecter aux domaines hôtes
<code>vcons, vconsole</code>	Virtual console, console virtuelle permettant d'accéder aux messages système. Une connexion s'effectue en connectant le service <code>vconscon</code> du domaine de contrôle à un port spécifique.

<code>vcpu</code>	Virtual central Processing Unit, unité de calcul centrale virtuelle. Chaque cœur d'un serveur est représenté par une CPU virtuelle. Par exemple, un serveur Sun Fire T2000 8 cœurs dispose de 32 CPU virtuelles pouvant être affectées entre les domaines logiques.
<code>vdc</code>	Virtual Disk Client, client de disque virtuel
<code>vdppcc</code>	Virtual data plane channel client, client du canal de plan de données virtuelles dans un environnement NDPS
<code>vdpcs</code>	Virtual data plane channel service, service du canal de plan de données virtuelles dans un environnement NDPS
<code>vdisk</code>	Virtual disks, les disques virtuels sont des périphériques en mode bloc génériques basés sur plusieurs types de périphériques, volumes ou fichiers physiques.
<code>vds, vdiskserver</code>	virtual disk server, serveur de disque virtuel qui permet d'importer des disques virtuels dans un domaine logique.
<code>vdsdev, vdiskserverdevice</code>	virtual disk server device, périphérique serveur de disque virtuel qui est exporté par le serveur de disque virtuel. Il peut s'agir d'un disque entier, d'une tranche de disque, d'un fichier ou d'un volume de disque.
<code>vnet</code>	Virtual network device, périphérique réseau virtuel qui implémente un périphérique Ethernet virtuel et communique avec d'autres périphériques <code>vnet</code> du système à l'aide du commutateur réseau virtuel (<code>vswitch</code>).
<code>vntsd(1M)</code>	Virtual network terminal server daemon, démon du serveur de terminal réseau virtuel des consoles Logical Domains (SE Solaris 10)
<code>vsw, vswitch</code>	Virtual network switch, commutateur réseau virtuel qui connecte les périphériques réseau virtuels au réseau externe et commute les paquets entre eux.
VTOC	Volume table of contents, tables des matières du volume
VxVM	Abréviation de Veritas Volume Manager

W

WAN Wide-Area Network, réseau étendu

X

XFP Abréviation de eXtreme Fast Path

XML Extensible Markup Language, langage de balisage extensible

Z

ZFS Zettabyte File System, système de fichiers zettaoctet (SE Solaris 10)

zpool(1M) Pool de stockage ZFS

