

Logical Domains (LDoms) 1.0.2 Administrationshandbuch

Sun Microsystems, Inc.
www.sun.com

Teile-Nr.: 820-4451-10
Februar 2008, Version 01

Website für Kommentare zu diesem Dokument: <http://www.sun.com/hwdocs/feedback>

Copyright 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Kalifornien 95054, USA. Alle Rechte vorbehalten.

Die in dem hier beschriebenen Produkt enthaltene Technologie ist geistiges Eigentum von Sun Microsystems, Inc. Im Besonderen können diese geistigen Eigentumsrechte ohne Einschränkung eines oder mehrere der unter <http://www.sun.com/patents> aufgelisteten US-Patente sowie eines oder mehrere zusätzliche Patente oder schwebende Patentanmeldungen in den USA und anderen Ländern beinhalten.

Rechte der Regierung der USA – Kommerzielle Software. Für bei der Regierung beschäftigte Benutzer gelten die Standardlizenzvereinbarung von Sun Microsystems, Inc. sowie die einschlägigen Bestimmungen des FAR und seine Ergänzungen.

Teile des Produkts sind möglicherweise von Berkeley BSD-Systemen abgeleitet, für die von der University of California eine Lizenz erteilt wurde. UNIX ist in den USA und in anderen Ländern eine eingetragene Marke, für die X/Open Company, Ltd. die ausschließliche Lizenz erteilt.

Sun, Sun Microsystems, das Sun-Logo, Java, Solaris, JumpStart, OpenBoot, Sun Fire, Netra, SunSolve, Sun BluePrints, Sun Blade, Sun Ultra und SunVTS sind Dienstleistungsmarken, Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern.

Alle SPARC-Marken werden unter Lizenz verwendet und sind Marken bzw. eingetragene Marken von SPARC International, Inc. in den USA und anderen Ländern. Produkte, die SPARC-Marken tragen, basieren auf einer von Sun Microsystems, Inc. entwickelten Architektur.

Das Adobe PostScript-Logo ist eine Marke von Adobe Systems, Incorporated.

Die in diesem Wartungshandbuch genannten Produkte und enthaltenen Informationen unterliegen den Ausfuhrbeschränkungen der US-amerikanischen Exportkontrollgesetze und zusätzlich evtl. Aus- und Einfuhrbeschränkungen anderer Länder. Die Nutzung dieser Produkte, auf direkte oder indirekte Weise, für die Herstellung oder Verbreitung nuklearer, chemischer oder biologischer Waffen oder Raketen sowie nuklearer maritimer Waffen ist strengstens untersagt. Der Export oder Rückexport in Länder, die einem US-Embargo unterliegen, oder an Personen und Körperschaften, die auf der US-Exportausschlussliste stehen, einschließlich (jedoch nicht beschränkt auf) der Liste nicht zulässiger Personen und speziell ausgewiesener Staatsangehöriger, ist strengstens untersagt.

SUN ÜBERNIMMT KEINE GEWÄHR FÜR DIE RICHTIGKEIT UND VOLLSTÄNDIGKEIT DES INHALTS DIESER DOKUMENTATION. EINE HAFTUNG FÜR EXPLIZITE ODER IMPLIZIERTE BEDINGUNGEN, DARSTELLUNGEN UND GARANTIEEN, EINSCHLIESSLICH MÖGLICHER MARKTWERTGARANTIEEN, DER ANGEMESSENHEIT FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHT-VERLETZBARKEIT, WIRD HIERMIT IN DEM GESETZLICH ZULÄSSIGEN RAHMEN ABGELEHNT.



Adobe PostScript

Inhalt

Vorwort xvii

1. Überblick über die Logical Domains-Software 1

Hypervisor und Logical Domains 1

Logical Domains Manager 3

Rollen für Logical Domains 4

Befehlszeilenoberfläche (CLI, Command-Line Interface) 4

Virtuelle Eingabe/Ausgabe 5

Virtuelles Netzwerk 6

Virtuelle Speicherung 6

Virtuelle Konsolen 6

Dynamische Neukonfiguration 6

Verzögerte Neukonfiguration 7

Persistente Konfigurationen 8

2. Sicherheit 9

Sicherheitsaspekte 9

Solaris Security Toolkit und der Logical Domains Manager 10

Hardening 11

Minimieren von logischen Domains 12

Autorisierung	13
Prüfung	14
Konformität	14

3. Installieren und Aktivieren der Software 15

Upgrade von Solaris OS 15

Sichern und Wiederherstellen der Logical Domains-Vorgabendatenbankdatei 15

Ausführen eines Live-Upgrades in der Steuerdomain 16

Upgrade auf LDOMs 1.0.2-Software 16

- ▼ So führen Sie ein Upgrade von LDOMs 1.0-Software auf LDOMs 1.0.2-Software durch 16

Erstinstallation der Software in der Steuerdomain 18

- ▼ So installieren Sie Solaris 10 OS 19
- ▼ So aktualisieren Sie die Systemfirmware 20
- ▼ So aktualisieren Sie die Systemfirmware ohne einen FTP-Server 21
- ▼ So rüsten Sie die Systemfirmware ab 22

Herunterladen des Logical Domains Manager und des Solaris Security Toolkit 22

- ▼ So laden Sie den Logical Domains Manager, das Solaris Security Toolkit und die Logical Domains MIB herunter 22

Installieren des Logical Domains Manager und des Solaris Security Toolkit 23

Verwenden des Installationsskripts zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software 24

- ▼ So führen Sie eine Installation mit dem Skript `install-ldm` ohne Optionen durch 25
- ▼ So führen Sie eine Installation mit dem Skript `install-ldm` und der Option `-d` durch 28
- ▼ So führen Sie eine Installation mit dem Skript `install-ldm` und der Option `-d none` durch. 29
- ▼ So führen Sie eine Installation mit dem Skript `install-ldm` und der Option `-p` durch 30

Verwenden von JumpStart zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software	30
▼ So richten Sie einen JumpStart-Server ein	31
▼ So führen Sie eine Installation mit der JumpStart-Software durch	31
Manuelles Installieren des Logical Domains Manager und des Solaris Security Toolkit	33
▼ So führen Sie eine manuelle Installation der Logical Domains Manager (LDoms) 1.0.2-Software durch	34
▼ (<i>Optional</i>) So führen Sie eine manuelle Installation der Solaris Security Toolkit 4.2-Software durch	34
▼ (<i>Optional</i>) So führen Sie ein manuelles Hardening der Steuerdomain durch	35
▼ So überprüfen Sie das Hardening	35
▼ So machen Sie das Hardening rückgängig	36
Aktivieren des Logical Domains Manager-Daemons	36
▼ So aktivieren Sie den Logical Domains Manager-Daemon	37
Erstellen von Autorisierung und Profilen und Zuweisen von Rollen für Benutzerkonten	37
Verwalten der Benutzerautorisierung	38
▼ So fügen Sie eine Autorisierung für einen Benutzer hinzu	38
▼ So löschen Sie alle Autorisierungen für einen Benutzer	38
Verwalten von Benutzerprofilen	39
▼ So fügen Sie ein Profil für einen Benutzer hinzu	39
▼ So löschen Sie alle Profile für einen Benutzer	39
Zuweisen von Rollen zu Benutzern	39
▼ So erstellen Sie eine Rolle und weisen dem Benutzer eine Rolle zu	40

4. Einrichten von Diensten und Logical Domains 41

Ausgabemeldungen 41

Sun UltraSPARC T1-Prozessoren 41

Sun UltraSPARC T2-Prozessoren 42

Erzeugen von Standarddiensten 42

- ▼ So erzeugen Sie Standarddienste 42

Erstkonfiguration der Steuerdomain 44

- ▼ So richten Sie die Steuerdomain ein 44

Neustart zur Verwendung von Logical Domains 46

- ▼ So führen Sie einen Neustart zur Verwendung von Logical Domains durch 46

Aktivierung des Netzwerkbetriebs zwischen der Steuer-/Servicedomain und anderen Domains 46

- ▼ So konfigurieren Sie den virtuellen Switch als primäre Schnittstelle 47

Aktivierung des virtuellen Netzwerk-Terminalserver-Daemons 48

- ▼ So aktivieren Sie den virtuellen Netzwerk-Terminalserver-Daemon 48

Erzeugen und Starten einer Gastdomain 49

- ▼ So erzeugen und starten Sie eine Gastdomain 49

Jumpstarten einer Gastdomain 53

5. Weitere Informationen und Aufgaben 55

Einschränkungen bei der Eingabe von Namen am CLI 55

Dateinamen (*file*) und Variablennamen (*var_name*) 55

Namen virtueller Plattenserver *file|device* und virtueller Switchgeräte. 55

Konfigurationsname (*config_name*) 56

Alle anderen Namen 56

Verwenden der `ldm list`-Unterbefehle 56

Maschinenlesbare Ausgabe 56

- ▼ So zeigen Sie die Syntax für `ldm`-Unterbefehle an 57

Flag-Definitionen 59

Definition einer Nutzungsstatistik 60

Beispiele verschiedener Listen 60

- ▼ So zeigen Sie Softwareversionen an (`-v`) 60

- ▼ So erzeugen Sie eine kurze Liste 61

- ▼ So erzeugen Sie eine lange Liste (-l) 61
- ▼ So erzeugen Sie eine erweiterte Liste (-e) 63
- ▼ So erzeugen Sie eine syntaktisch analysierbare, maschinenlesbare Liste (-p) 65
- ▼ So zeigen Sie den Status einer Domain an 65
- ▼ So listen Sie eine Variable 65
- ▼ So listen Sie Bindungen 66
- ▼ So listen Sie Konfigurationen 67
- ▼ So listen Sie Geräte 67
- ▼ So listen Sie Dienste 69

Listen von Einschränkungen 69

- ▼ So listen Sie Einschränkungen für eine Domain 69
- ▼ So listen Sie Einschränkungen im XML-Format 70
- ▼ So listen Sie Einschränkungen in einem maschinenlesbaren Format 71

Bei dem Befehl `ldm stop-domain` kann es zu einer Zeitüberschreitung kommen, wenn die Domain an der Auslastungsgrenze läuft 72

Bestimmung des Namens der einem virtuellen Netzwerkgerät entsprechenden Solaris-Netzwerkschnittstelle 73

- ▼ So finden Sie den Namen der Solaris OS-Netzwerkschnittstelle 73

Automatische oder manuelle Zuweisung von MAC-Adressen 74

Bereich der MAC-Adressen, die der Logical Domains-Software zugewiesen werden 75

Algorithmus für die automatische Zuweisung von MAC-Adressen 75

Erkennung doppelter MAC-Adressen 76

Freigegebene MAC-Adressen 77

Manuelle Zuweisung von MAC-Adressen 77

- ▼ So ordnen Sie eine MAC-Adresse manuell zu 78

Zuordnung von CPU und Speicheradressen 78

CPU-Zuordnung 78

▼ So ermitteln Sie die CPU-Nummer	79
Speicherzuordnung	79
▼ So ermitteln Sie die reale Speicheradresse	79
Beispiele für CPU- und Speicherzuordnung	80
So wird der Split PCI-Express-Bus für die Nutzung mehrerer Logical Domains konfiguriert	81
▼ So wird eine Split-PCI-Konfiguration erzeugt	82
Aktivierung des Umgehungsmodus einer E/A-MMU auf einem PCI-Bus	85
Verwenden von Konsolengruppen	85
▼ So kombinieren Sie mehrere Konsolen in einer Gruppe	86
Verschieben einer Logical Domain von einem Server auf einen anderen	86
▼ So richten Sie Domains ein, die verschoben werden sollen	87
▼ So verschieben Sie die Domain	87
Entfernen von Logical Domains	87
▼ So entfernen Sie alle Gast-Logical Domains	88
Betrieb des Solaris OS mit Logical Domains	89
OpenBoot-Firmware nach dem Starten von Solaris OS nicht verfügbar, wenn der Domainbetrieb aktiviert ist	89
Neustarten eines Servers	89
▼ So speichern Sie zunächst Ihre aktuellen Logical Domain-Konfigurationen auf dem Systemcontroller	90
Ergebnis des OpenBoot-Befehls <code>power-off</code>	90
Ergebnis von Unterbrechungen bei der Ausführung von Solaris OS	90
Ergebnisse des Anhaltens oder Neustartens der Steuerdomain	91
Einige <code>format (1M)</code> -Befehlsoptionen funktionieren bei virtuellen Platten nicht	92
Verwenden von LDomS mit ALOM CMT	93
▼ So setzen Sie die Logical Domain-Konfiguration auf die Standard- oder eine andere Konfiguration zurück	94
Aktivieren und Verwenden der BSM-Auditing (Basic Security Modul)	94

- ▼ So verwenden Sie das Finish Script `enable-bsm.fin` 95
- ▼ So verwenden Sie den Solaris OS-Befehl `bsmconv(1M)` 96
- ▼ So überprüfen Sie, dass das BSM-Auditing aktiviert ist 96
- ▼ So deaktivieren Sie die Überwachung 96
- ▼ So drucken Sie eine Protokollausgabe 97
- ▼ So drehen Sie Überwachungsprotokolle 97

Konfigurieren von virtuellen Switches und Servicedomains für NAT und Routing 97

- ▼ So richten Sie den virtuellen Switch für die Konnektivität zu externen Domains ein 98

Verwenden des ZFS mit virtuellen Platten 99

Erzeugen einer virtuellen Platte als Schicht über einem ZFS-Volume 99

- ▼ So erzeugen Sie eine virtuelle Platte als Schicht über einem ZFS-Volume 99

Verwenden des ZFS über eine virtuelle Platte 100

- ▼ So verwenden Sie ein ZFS über eine virtuelle Platte 101

Verwenden des ZFS für Boot-Platten 102

- ▼ So verwenden Sie ein ZFS für Boot-Platten 102

Verwenden von Volume-Managern in einer Logical Domains-Umgebung 104

Verwenden von virtuellen Platten als Schicht über einem Volume-Manager 104

Verwenden von virtuellen Platten als Schicht über einem SVM 106

Verwenden von virtuellen Platten bei installiertem VxVM 107

Verwenden eines Volume-Managers als Schicht über einer virtuellen Platte 107

Verwenden des ZFS als Schicht über einer virtuellen Platte 108

Verwenden des SVM als Schicht über einer virtuellen Platte 108

Verwenden eines VxVM als Schicht über einer virtuellen Platte 108

Konfigurieren von IPMP in einer Logical Domains-Umgebung 108

Konfigurieren von virtuellen Netzwerkgeräten in eine IPMP-Gruppe einer Logical Domain hinein 109

Konfigurieren und Verwenden von IPMP in der Servicedomain 110

Glossar 113

Abbildungen

- [ABBILDUNG 1-1](#) Hypervisor mit Unterstützung für zwei Logical Domains 2
- [ABBILDUNG 5-1](#) Zwei virtuelle Netzwerke, die mit separaten virtuellen Switch-Instanzen verbunden sind 109
- [ABBILDUNG 5-2](#) Jedes virtuelle Netzwerkgerät ist mit einer anderen Servicedomain verbunden 110
- [ABBILDUNG 5-3](#) Zwei als Teil einer IPMP-Gruppe konfigurierte Netzwerkschnittstellen 111

Tabellen

TABELLE 1-1	Rollen von logischen Domains	4
TABELLE 2-1	ldm – Unterbefehle und Benutzerautorisierung	13
TABELLE 5-1	Erwartetes Verhalten beim Halten oder Neustarten der Steuerdomain (primary)	91

Codebeispiele

CODEBEISPIEL 3-1	Verzeichnisstruktur für heruntergeladene Logical Domains 1.0.2-Software	22
CODEBEISPIEL 3-2	Ausgabe einer Solaris-Konfiguration für LDOMs, für die ein Hardening durchgeführt wurde	26
CODEBEISPIEL 3-3	Ausgabe bei der Auswahl eines angepassten Konfigurationsprofils	27
CODEBEISPIEL 3-4	Ausgabe bei erfolgreicher Ausführung des Skripts <code>install-ldm -d</code>	28
CODEBEISPIEL 3-5	Ausgabe bei erfolgreicher Ausführung des Skripts <code>install-ldm -d none</code>	29
CODEBEISPIEL 5-1	Syntax für alle <code>ldm</code> -Unterbefehle	57
CODEBEISPIEL 5-2	Installierte Softwareversionen	60
CODEBEISPIEL 5-3	Kurze Liste aller Domains	61
CODEBEISPIEL 5-4	Lange Liste aller Domains	61
CODEBEISPIEL 5-5	Erweiterte Liste aller Domains	63
CODEBEISPIEL 5-6	Maschinenlesbare Ausgabe	65
CODEBEISPIEL 5-7	Domainstatus	65
CODEBEISPIEL 5-8	Variablenliste für eine Domain	65
CODEBEISPIEL 5-9	Bindungsliste für eine Domain	66
CODEBEISPIEL 5-10	Konfigurationsliste	67
CODEBEISPIEL 5-11	Liste aller Server-Ressourcen	67
CODEBEISPIEL 5-12	Dienstliste	69
CODEBEISPIEL 5-13	Einschränkungsliste für eine Domain	69
CODEBEISPIEL 5-14	Einschränkungen für eine Domain im XML-Format	70
CODEBEISPIEL 5-15	Einschränkungen für alle Domains in einem maschinenlesbaren Format	71

Vorwort

Das *Logical Domains (LDoms) 1.0.2 Administrationshandbuch* enthält detaillierte Informationen und Prozeduren, in denen ein allgemeiner Überblick gegeben wird und Sicherheitsaspekte, die Installation, Konfiguration, Änderung und Ausführung allgemeiner Aufgaben für die Logical Domains Manager 1.0.2-Software auf unterstützten Servern, Blades und Servermodulen beschrieben werden. Eine genaue Liste erhalten Sie in den *Versionshinweisen zu Logical Domains (LDoms) 1.0.2* unter „Unterstützte Server“. Dieses Handbuch richtet sich an Systemadministratoren auf diesen Servern mit Praxiskenntnissen von UNIX®-Systemen und des Solaris™-Betriebssystems (Solaris OS).

Vorausgehende Informationen

Wenn Sie noch über keine Praxiskenntnisse der UNIX-Befehle und -Vorgehensweise und Ihres Solaris-Betriebssystems verfügen, lesen Sie die Benutzer- und Systemadministrator-Dokumentation zu Solaris OS im Lieferumfang Ihrer Systemhardware, und ziehen Sie eine Schulung für UNIX-Systemadministratoren in Erwägung.

Aufbau dieses Handbuchs

[Kapitel 1](#) enthält eine Übersicht über die Logical Domains-Software.

[Kapitel 2](#) beschreibt das Solaris Security Toolkit, und wie es Sicherheit für das Solaris OS in logischen Domains gewährleisten kann.

Kapitel 3 beschreibt detaillierte Vorgehensweisen für die Aktualisierung oder Installation und Aktivierung der Logical Domains Manager-Software.

Kapitel 4 beschreibt detailliert Vorgehensweisen für das Einrichten von Diensten und logischen Domains.

Kapitel 5 enthält zusätzliche Informationen und Vorgehensweisen für die Ausführung allgemeiner Aufgaben bei der Verwendung der Logical Domains-Software zu Verwaltung von logischen Domains.

Das **Glossar** enthält eine Liste der LDoms-spezifischen Abkürzungen, Akronyme, Begriffe und Definitionen.

Verwenden von UNIX-Befehlen

Dieses Dokument enthält unter Umständen keine Informationen zu grundlegenden UNIX-Befehlen und -Verfahren (z. B. das Herunterfahren oder Starten des Systems und das Konfigurieren von Geräten). Weitere Informationen hierzu finden Sie unter:

- Software-Dokumentationen, die Sie mit Ihrem System erhalten haben
- Dokumentationen zum Solaris-Betriebssystem unter

<http://docs.sun.com>

Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
C-Shell	<i>Computername%</i>
C-Shell-Superuser	<i>Computername#</i>
Bourne-Shell und Korn-Shell	<i>\$</i>
Bourne-Shell- und Korn-Shell-Superuser	<i>#</i>

Typografische Konventionen

Schriftart*	Bedeutung	Beispiele
AaBbCc123	Namen von Befehlen, Dateien und Verzeichnissen; Meldungen auf dem Bildschirm	Bearbeiten Sie die Datei <i>.login</i> . Mithilfe von <i>ls -a</i> können Sie alle Dateien auflisten. <i>%</i> Sie haben Post.
AaBbCc123	Ihre Eingabe, wenn sich diese von Meldungen auf dem Bildschirm abheben soll	<i>%</i> su Passwort:
<i>AaBbCc123</i>	Buchtitel, neue Wörter oder Ausdrücke, betonte Wörter. Ersetzen Sie die Befehlszeilen-Variablen durch tatsächliche Namen oder Werte.	Siehe Kapitel 6 im <i>Benutzerhandbuch</i> . Diese Optionen werden als <i>Klassenoptionen</i> bezeichnet. Geben Sie zum Löschen einer Datei rm <i>dateiname</i> ein.

*. Ihr Browser verwendet möglicherweise andere Einstellungen.

Zugehörige Dokumentation

Das *Logical Domains (LDDoms) 1.0.2 – Administrationshandbuch* und die *Versionshinweise* finden Sie unter:

<http://docs.sun.com>

Den *Beginners Guide to LDoms: Understanding and Deploying Logical Domains Software* finden Sie auf der Sun BluePrints™-Site.

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

Zu Ihrem Server, Ihrer Software oder Solaris OS gehörige Dokumente erhalten Sie unter:

<http://docs.sun.com>

Geben Sie den Namen des Servers, der Software oder Solaris OS in das Suchfeld ein, um die benötigten Dokumente zu suchen.

Anwendung	Titel	Teile- nummer	Format	Ver- zeichnis
Versionshinweise zu LDoms	<i>Versionshinweise zu Logical Domains (LDoms) Version 1.0.2</i>	820-3599-10	HTML PDF	Online
Solaris Man Pages für LDoms	Solaris 10 Reference Manual Collection: <ul style="list-style-type: none">• Man Page zu <code>drd(1M)</code>• Man Page zu <code>vntsd(1M)</code>	nicht anwendbar	HTML	Online
LDoms-Man Page	Man Page zu <code>ldm(1M)</code> <i>Logical Domains (LDoms) 1.0.2 Manager Man Page Guide</i>	nicht anwendbar 819-7679-10	SGML PDF	Online Online
Grundlagen zur Logical Domains-Software	<i>Beginners Guide to LDoms: Understanding and Deploying Logical Domains Software</i>	820-0832-20	PDF	Online
Administration für LDoms MIB	<i>Logical Domains (LDoms) MIB 1.0.2 Administrationshandbuch</i>	820-2319-10	HTML PDF	Online
Versionshinweise zu LDoms MIB	<i>Versionshinweise zu Logical Domains (LDoms) MIB 1.0.2</i>	820-2320-10	HTML PDF	Online
Solaris OS, einschließlich Installation mithilfe von JumpStart™, und unter Verwendung des Dienstprogramms für die Dienstverwaltung (Service Management Facility, SMF)	Solaris 10 Collection	nicht anwendbar	HTML PDF	Online
Sicherheit	<i>Solaris Security Toolkit 4.2 Administration Guide</i>	819-1402-10	HTML PDF	Online

Anwendung	Titel	Teile- nummer	Format	Ver- zeichnis
Sicherheit	<i>Solaris Security Toolkit 4.2 Reference Manual</i>	819- 1503-10	HTML PDF	Online
Sicherheit	<i>Solaris Security Toolkit 4.2 Release Notes</i>	819- 1504-10	HTML PDF	Online
Sicherheit	<i>Solaris Security Toolkit 4.2 Man Page Guide</i>	819- 1505-10	HTML PDF	Online

Dokumentation, Support und Schulung

Funktion von Sun	URL
Dokumentation	http://docs.sun.com
Support	http://www.sun.com/support
Schulung	http://www.sun.com/training

Websites von Drittherstellern

Sun ist nicht verantwortlich für die Verfügbarkeit der in diesem Dokument angeführten Websites von Drittherstellern. Sun unterstützt keine Inhalte, Werbung, Produkte oder sonstige Materialien, die auf oder über solche Websites oder Ressourcen verfügbar sind, und übernimmt keine Verantwortung oder Haftung dafür. Sun ist nicht verantwortlich oder haftbar für tatsächliche oder vermeintliche Schäden oder Verluste, die durch oder in Verbindung mit der Verwendung von über solche Websites oder Ressourcen verfügbaren Inhalten, Waren oder Dienstleistungen bzw. dem Vertrauen darauf entstanden sind.

Ihre Meinung ist gefragt

Sun bemüht sich um eine stetige Verbesserung seiner Dokumentation und ist deshalb an Ihrer Meinung und Ihren Anregungen interessiert. Sie können Ihre Kommentare über folgende Adresse einreichen:

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

Geben Sie bitte mit Ihrem Kommentar Titel und Teilenummer des Dokuments an:

Logical Domains (LDoms) 1.0.2 Administrationshandbuch, Teilenummer 820-4451-10.

Überblick über die Logical Domains-Software

Dieses Kapitel enthält einen kurzen Überblick über die Logical Domains-Software. Die gesamte Solaris OS-Funktionalität, die zur Verwendung der Logical Domains-Technologie von Sun erforderlich ist, befindet sich in der Solaris 10 11/06-Version (Minimum) sowie einigen zusätzlich erforderlichen Patches. Jedoch sind für die Verwendung von logischen Domains die Systemfirmware und der Logical Domains Manager ebenfalls erforderlich. Spezifische Details finden Sie in den *Versionshinweisen zu Logical Domains (LDoms) 1.0.2* unter „Erforderliche und empfohlene Software“.

Hypervisor und Logical Domains

Dieser Abschnitt bietet einen kurzen Überblick über SPARC®-Hypervisor und die davon unterstützten logischen Domains.

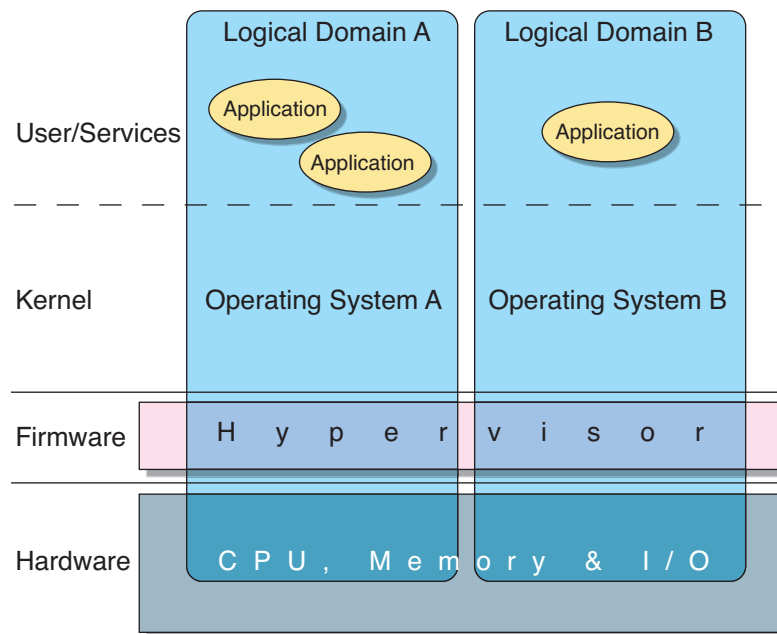
Der SPARC-Hypervisor ist eine kleine Firmwareschicht, die eine stabile virtualisierte Maschinenarchitektur bietet, auf die ein Betriebssystem geschrieben werden kann. Sun-Server, die Hypervisor einsetzen, bieten Hardwarefunktionen, die die Kontrolle des Hypervisors über die Aktivitäten eines logischen Betriebssystems steuern.

Bei einer logischen Domain handelt es sich um eine diskrete logische Gruppierung mit eigenem Betriebssystem, eigenen Ressourcen und eigener Identität innerhalb eines einzelnen Computersystems. Jede logische Domain lässt sich autonom erstellen, löschen, neu konfigurieren und neu starten, ohne dass ein Neustart des Servers (Power Cycle) erforderlich ist. Sie können eine Vielzahl von Anwendungsprogrammen in unterschiedlichen logischen Domains aus Leistungs- und Sicherheitsgründen unabhängig voneinander ausführen.

Jede logische Domain darf nur diejenigen Serverressourcen verfolgen und damit interagieren, die ihr vom Hypervisor zur Verfügung gestellt wurden. Mithilfe des Logical Domains Manager gibt der Systemadministrator an, welche Aktionen der Hypervisor über die Steuerdomain durchführen soll. Auf diese Weise erzwingt der Hypervisor die Aufteilung der Ressourcen eines Servers und stellt mehreren Betriebssystemumgebungen eingeschränkte Untermengen zur Verfügung. Dies ist der grundlegende Mechanismus für die Erstellung logischer Domains. Das folgende Diagramm zeigt den Hypervisor mit Unterstützung für zwei logische Domains. Außerdem zeigt es die Schichten, aus denen die Logical Domains-Funktionalität besteht.

- Anwendungen oder Benutzer/Dienste
- Kernel oder Betriebssysteme
- Firmware oder Hypervisor
- Hardware, einschließlich CPU, Speicher und E/A

ABBILDUNG 1-1 Hypervisor mit Unterstützung für zwei Logical Domains



Die Anzahl und Funktionen der logischen Domain, die ein bestimmter SPARC-Hypervisor unterstützt, sind serverabhängig. Der Hypervisor kann Untermengen der gesamten CPU-, Arbeitsspeicher- und E/A-Ressourcen eines Servers einer bestimmten logischen Domain zuweisen. Dies ermöglicht die Unterstützung mehrerer Betriebssysteme gleichzeitig, wobei sich jedes innerhalb seiner eigenen Domain befindet. Ressourcen lassen sich zwischen unterschiedlichen logischen

Domains mit einer beliebigen Granularität neu anordnen. So kann beispielsweise Arbeitsspeicher einer logischen Domain mit einer 8-Kilobyte-Granularität zugewiesen werden.

Jede virtuelle Maschine lässt sich als völlig unabhängige Maschine mit eigenen Ressourcen verwalten. Zum Beispiel:

- Kernel, Patches und Optimierungsparameter
- Benutzerkonten und Administratoren
- Platten
- Netzwerkschnittstellen, MAC-Adressen und IP-Adressen

Alle virtuellen Maschinen lassen sich unabhängig voneinander anhalten, starten und neu starten, ohne dass ein Neustart des Servers erforderlich ist.

Die Hypervisor-Software ist dafür verantwortlich, dass die Trennung zwischen logischen Domains aufrechterhalten bleibt. Außerdem stellt sie Logical Domain Channels (LDC) zur Verfügung, damit logische Domains miteinander kommunizieren können. Mithilfe der Logical Domain Channels sind Domains in der Lage, sich gegenseitig Dienste zur Verfügung zu stellen, z. B. Netzwerk- oder Plattendienste.

Der Systemcontroller ist für die Überwachung und Ausführung der physikalischen Maschine verantwortlich, jedoch nicht für die Verwaltung der virtuellen Maschine. Der Logical Domains Manager führt die virtuelle Maschine aus.

Logical Domains Manager

Der Logical Domains Manager dient zur Erstellung und Verwaltung von logischen Domains. Es kann nur einen Logical Domains Manager pro Server geben. Der Logical Domains Manager ist für die Zuordnung logischer Domains zu physikalischen Ressourcen verantwortlich.

Rollen für Logical Domains

Alle logischen Domains sind gleich, mit Ausnahme der Rollen, die Sie für diese festlegen. Logische Domains können mehrere Rollen ausführen.

TABELLE 1-1 Rollen von logischen Domains

Domainrolle	Beschreibung
Steuerdomain	Domain, in der der Logical Domains Manager ausgeführt wird. Auf diese Weise können Sie andere logische Domains erstellen und verwalten sowie anderen Domains virtuelle Ressourcen zuweisen. Pro Server ist nur eine Steuerdomain zulässig. Die erste Domain, die bei der Installation der Logical Domains-Software erstellt wird, ist eine Steuerdomain und hat die Bezeichnung <i>primary</i> .
Servicedomain	Domain, die anderen Domains virtuelle Gerätedienste zur Verfügung stellt, z. B. virtuelle Switches, einen virtuellen Konsolenkonzentrator und einen virtuellen Plattenserver.
E/A-Domain	Domain, die direkter Eigentümer von physikalischen E/A-Geräten ist und direkten Zugriff darauf hat, z. B. eine Netzwerkkarte in einem PCI Express-Controller. Nutzt die Geräte gemeinsam mit anderen Domains in Form von virtuellen Geräten, wenn die E/A-Domain auch die Steuerdomain ist. Die Anzahl der zulässigen E/A-Domains hängt von Ihrer Plattformarchitektur ab. Wenn Sie z. B. einen Sun UltraSPARC® T1-Prozessor verwenden, sind maximal zwei E/A-Domains möglich, von der eine die Steuerdomain sein muss.
Gastdomain	Diese Domain wird von der Steuerdomain verwaltet und verwendet Dienste aus der E/A und den Servicedomains.

Wenn Sie über ein vorhandenes System verfügen und bereits ein Betriebssystem und andere Software auf Ihrem Server ausgeführt werden, dann wird diese nach der Installation von Logical Domains Manager zu Ihrer Steuerdomain. Es ist eventuell sinnvoll, einige der Anwendungen aus der Steuerdomain nach ihrer Einrichtung zu entfernen, und einen Lastausgleich der Anwendungen innerhalb der Domains durchzuführen, um eine optimale Nutzung Ihres Systems zu erreichen.

Befehlszeilenoberfläche (CLI, Command-Line Interface)

Der Logical Domains Manager bietet eine Befehlszeilenoberfläche (CLI) zum Erstellen und Konfigurieren von logischen Domains durch den Systemadministrator. Die CLI besteht aus einem einzelnen Befehl, `ldm(1M)`, mit mehreren Unterbefehlen.

Zur Verwendung der Logical Domains Manager-CLI muss der Logical Domains Manager-Daemon, `ldmd`, aktiv sein. Der Befehl `ldm(1M)` und seine Unterbefehle werden im Detail auf der Man Page zu `ldm(1M)` und unter *Logical Domains (LDoms) Manager 1.0.2 – Hilfeseiten zur Online-Dokumentation* beschrieben. Die Man Page `ldm(1M)` ist Bestandteil des `SUNWldm`-Pakets und wird bei der Installation des `SUNWldm`-Pakets mit installiert.

Zur Ausführung des `ldm`-Befehls muss sich das Verzeichnis `/opt/SUNWldm/bin` in Ihrer UNIX `$PATH`-Variablen befinden. Um auf die Man Page zu `ldm(1M)` zuzugreifen, fügen Sie den Verzeichnispfad `/opt/SUNWldm/man` zur Variablen `$MANPATH` hinzu. Beide werden wie folgt angezeigt:

```
$ 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)
```

Virtuelle Eingabe/Ausgabe

In einer Logical Domains-Umgebung kann ein Administrator bis zu 32 Domains auf einem Sun Fire- oder SPARC Enterprise T1000 oder T2000 Server bereitstellen. Obwohl jeder Domain dediziert CPUs und Arbeitsspeicher zugewiesen werden können, macht es die begrenzte Anzahl von E/A-Bussen und physikalischer E/A-Steckplätze in diesen Systemen unmöglich, allen Domains exklusiven Zugriff auf Platten- und Netzwerkgeräte zur Verfügung zu stellen. Obwohl sich einige physikalische Geräte durch Splitten des PCI Express® (PCI-E)-Busses gemeinsam nutzen lassen (siehe [„So wird der Split PCI-Express-Bus für die Nutzung mehrerer Logical Domains konfiguriert“ auf Seite 81](#)), reicht dies nicht aus, um allen Domains exklusiven Zugriff auf Geräte zur Verfügung zu stellen. Dieser Mangel an direktem physikalischen E/A-Gerätezugriff wird durch die Implementierung eines virtualisierten E/A-Modells adressiert.

Alle logischen Domains ohne direkten E/A-Zugriff werden mit virtuellen E/A-Geräten konfiguriert, die mit einer Servicedomain kommunizieren. Diese wird als Dienst ausgeführt, um Zugriff auf ein physikalisches Gerät oder seine Funktionen zu exportieren. In diesem Client-Server-Modell kommunizieren virtuelle E/A-Geräte entweder miteinander oder mit einem entsprechenden Dienst über domainübergreifende Kommunikationskanäle, die als Logical Domain Channels (LDCs) bezeichnet werden. In der Logical Domains 1.0.2-Software umfasst die E/A-Funktionalität Unterstützung für den virtuellen Netzwerkbetrieb, Speicherung und Konsolen.

Virtuelles Netzwerk

Die Unterstützung für virtuelle Netzwerke wird über zwei Komponenten implementiert: das virtuelle Netzwerk und das virtuelle Netzwerk-Switchgerät. Das virtuelle Netzwerkgerät (`vnet`) emuliert ein Ethernet-Gerät und kommuniziert mit anderen `vnet`-Geräten im System über einen Point-to-Point-Channel. Das virtuelle Switchgerät (`vsw`) funktioniert hauptsächlich als [De]multiplexor aller eingehenden und ausgehenden Pakete des virtuellen Netzwerks. Das `vsw`-Gerät kommuniziert direkt mit einem physikalischen Netzwerkadapter in einer Servicedomain und sendet und empfängt Pakete im Auftrag eines virtuellen Netzwerks. Das `vsw`-Gerät funktioniert auch als einfacher Layer-2-Switch und vermittelt Pakete zwischen damit verbundenen `vnet`-Geräten innerhalb des Systems.

Virtuelle Speicherung

Mithilfe der virtuellen Speicherinfrastruktur können logische Domains auf Speicher auf Blockebene zugreifen, der diesen nicht direkt über ein Client-Server-Modell zugeordnet wurde. Sie besteht aus zwei Komponenten: Einem virtuellen Plattenclient (`vdcc`), der als Blockeinheitenschnittstelle exportiert wird und einem virtuellen Plattendienst (`vdss`), der Plattenanforderungen im Auftrag des virtuellen Plattenclients verarbeitet und diese an den physikalischen Speicher übermittelt, der sich in der Servicedomain befindet. Obwohl die virtuellen Platten als reguläre Platten in der Clientdomain angezeigt werden, erfolgt die Weiterleitung aller Plattenoperationen an die physikalische Platte über den virtuellen Plattendienst.

Virtuelle Konsolen

In einer Logical Domains-Umgebung wird Konsolen-E/A aus allen Domains, mit Ausnahme der `primary`-Domain, an eine Servicedomain umgeleitet, in der der virtuelle Konsolenkonzentrator (`vcc`) und der virtuelle Netzwerk-Terminalserver-Dienst anstatt des Systemcontrollers ausgeführt werden. Der virtuelle Konsolenkonzentrator fungiert als Konzentrador für den Konsolenverkehr aller Domains und kommuniziert mit dem virtuellen Netzwerk-Terminalserver-Daemon (`vntsd`). Weiterhin exportiert er den Zugriff auf jede Konsole über einen UNIX-Socket.

Dynamische Neukonfiguration

Dynamische Neukonfiguration bezeichnet die Möglichkeit, Ressourcen bei aktivem Betriebssystem hinzuzufügen oder zu entfernen. Das Solaris 10 OS unterstützt nur das Hinzufügen oder Entfernen einer virtuellen CPU (`vcpu`). Die dynamische Neukonfiguration von Speicher und Eingabe/Ausgabe wird im Solaris 10 OS nicht

unterstützt. Zur Verwendung der dynamischen Neukonfiguration in der Logical Domains Manager-CLI muss der dynamische Neukonfigurations-Daemon für Logical Domains `drd(1M)` in der zu ändernden Domain aktiv sein.

Verzögerte Neukonfiguration

Im Gegensatz zu dynamischen Neukonfigurationsoperationen, die sofort stattfinden, treten verzögerte Neukonfigurationsvorgänge erst nach dem nächsten Neustart des Betriebssystems oder Anhalten oder Starten der logischen Domain in Kraft, wenn kein OS ausgeführt wird. Alle Hinzufügen- oder Entfernen-Operationen in aktiven logischen Domains, mit Ausnahme der Unterbefehle `add-vcpu`, `set-vcpu`, und `remove-vcpu`, werden als verzögerte Neukonfigurationsvorgänge angesehen. Dies gilt auch für den Unterbefehl `set-vswitch` in einer aktiven logischen Domain.

Wenn bei Verwendung eines Sun UltraSPARC T1-Prozessors der Logical Domains Manager das erste Mal installiert und aktiviert wird (oder Sie die Konfiguration auf `factory-default` zurücksetzen), wird der LDom Manager im Konfigurationsmodus ausgeführt. In diesem Modus werden Konfigurationsanfragen zwar akzeptiert und in die Warteschlange gestellt, jedoch nicht beantwortet. Auf diese Weise kann eine neue Konfiguration generiert und im Systemcontroller gespeichert werden, ohne den Zustand der aktiven Maschine zu beeinflussen. Hierbei kommt es zu keinen Behinderungen durch Einschränkungen, die im Zusammenhang mit verzögerten Neukonfigurationen und Neustarts von E/A-Domains auftreten.

Sobald sich eine verzögerte Neukonfiguration für eine bestimmte logische Domain in Ausführung befindet, werden alle anderen Neukonfigurationsanfragen für diese logische Domain ebenfalls verzögert, bis die Domain neu gestartet oder angehalten und gestartet wird. Wenn weiterhin eine verzögerte Neukonfiguration für eine logische Domain aussteht, werden Neukonfigurationsanfragen für andere logische Domains stark eingeschränkt und schlagen mit einer entsprechenden Fehlermeldung fehl.

Obwohl sogar Versuche, virtuelle E/A-Geräte aus einer aktiven logischen Domain zu entfernen, als verzögerte Neukonfigurationsoperationen behandelt werden, treten einige Konfigurationsänderungen sofort in Kraft. Dies bedeutet, dass das Gerät nicht mehr funktioniert, sobald die entsprechende Logical Domains Manager CLI-Operation aufgerufen wird.

Der Logical Domains Manager-Unterbefehl `remove-reconf` bricht verzögerte Neukonfigurationsoperationen ab. Verzögerte Neukonfigurationsoperationen können mit dem Befehl `ldm list-domain` aufgelistet werden. Weitere Informationen zur Verwendung der verzögerten Neukonfigurationsfunktion finden Sie auf der Man Page zu `ldm(1M)` oder unter *Logical Domains (LDoms) Manager 1.0.2 – Hilfeseiten zur Online-Dokumentation*.

Hinweis – Die Verwendung des Befehls `ldm remove-reconf` ist nicht möglich, wenn andere `ldm remove-*`-Befehle für virtuelle E/A-Geräte ausgegeben wurden. Unter diesen Umständen schlägt der Befehl `ldm remove-reconf` fehl.

Persistente Konfigurationen

Die aktuelle Konfiguration einer logischen Domain lässt sich auf dem Systemcontroller (SC) mit den Logical Domains Manager CLI-Befehlen speichern. Sie können eine Konfiguration hinzufügen, die zu verwendende Konfiguration angeben, eine Konfiguration entfernen sowie die Konfigurationen auf dem Systemcontroller auflisten. (Weitere Informationen finden Sie auf der Man Page zu `ldm(1M)` oder unter *Logical Domains (LDoms) Manager 1.0.2 – Hilfeseiten zur Online-Dokumentation*.) Darüber hinaus gibt es einen ALOM CMT Version 1.3-Befehl, mit dem Sie eine zu startende Konfiguration auswählen können (siehe „[Verwenden von LDoms mit ALOM CMT](#)“ auf Seite 93).

Sicherheit

Dieses Kapitel beschreibt die Solaris Security Toolkit-Software und wie Sie damit die Sicherheit des Solaris OS in Ihren logischen Domains gewährleisten können.

Sicherheitsaspekte

Die Solaris Security Toolkit-Software, inoffiziell auch als JASS-Toolkit (JumpStart™ Architecture and Security Scripts) bezeichnet, bietet einen automatisierten, erweiterbaren und skalierbaren Mechanismus zum Aufbau und zur Beibehaltung eines sicheren Solaris OS-Systems. Das Solaris Security Toolkit bietet Sicherheit für Geräte, die für die Verwaltung Ihres Server wichtig sind, einschließlich der Steuerdomain im Logical Domains Manager.

Das Solaris Security Toolkit 4.2-Softwarepaket, `SUNWjass`, bietet die Grundlage zur Sicherung des Solaris-Betriebssystems Ihrer Steuerdomain durch den Einsatz des `install-lbm`-Skripts, das Folgendes ermöglicht:

- Automatisches Hardening Ihrer Steuerdomain durch das Solaris Security Toolkit mithilfe des Logical Domains Manager-Installationsskripts (`install-lbm`) und des für den Logical Domains Manager spezifischen Steuertreibers (`ldm_control-secure.driver`),
- Auswahl eines alternativen Treibers bei Verwendung des Installationsskripts,
- Auswahl keines Treibers bei Verwendung des Installationsskripts und Ihres eigenen Solaris-Hardening.

Das `SUNWjass`-Paket befindet sich beim Logical Domains (LDMs) Manager 1.0.2-Softwarepaket, `SUNWldm`, auf der Software-Download-Website von Sun. Sie haben die Möglichkeit, das Solaris Security Toolkit 4.2-Softwarepaket zusammen mit der Logical Domains Manager 1.0.2-Software herunterzuladen und zu installieren. Das Solaris Security Toolkit 4.2-Softwarepaket enthält die erforderlichen Patches, damit die Solaris Security Toolkit-Software zusammen mit dem Logical Domains Manager

funktioniert. Sobald Sie die Software installiert haben, können Sie mithilfe der Solaris Security Toolkit 4.2-Software das Hardening Ihres Systems durchführen. In [Kapitel 3](#) erfahren Sie, wie Sie das Solaris Security Toolkit installieren und konfigurieren, um das Hardening Ihrer Steuerdomain vorzunehmen.

Im Anschluss werden die Sicherheitsfunktionen aufgelistet, die Benutzern des Logical Domains Manager vom Solaris Security Toolkit zur Verfügung gestellt werden:

- *Hardening* – Hierbei werden die Solaris OS-Konfigurationen verändert, um die Sicherheit eines Systems unter Verwendung der Solaris Security Toolkit 4.2-Software mit den erforderlichen Patches zu verbessern, damit das Solaris Security Toolkit mit dem Logical Domains Manager zusammenarbeiten kann.
- *Minimieren* – Hierbei wird die minimale Anzahl der Solaris OS-Kernpakete installiert, die für LDoms- und LDoms Management Information Base (MIB)-Unterstützung erforderlich sind.
- *Autorisierung* – Hierbei wird Autorisierung des für Logical Domains Manager angepassten RBAC-Modells (Role-Based Access Control) von Solaris OS eingerichtet.
- *Prüfung* – Hierbei wird das für Logical Domains Manager angepasste Basic Security Modul zur Identifizierung der Quelle der Sicherheitsänderungen am System verwendet, um zu ermitteln, was, wann, von wem an welcher Komponente durchgeführt wurde.
- *Konformität* – Hierbei wird mithilfe der Prüfungsfunktion des Solaris Security Toolkit ermittelt, ob die Konfiguration eines Systems mit einem vordefinierten Sicherheitsprofil konform ist.

Solaris Security Toolkit und der Logical Domains Manager

In [Kapitel 3](#) erfahren Sie, wie Sie das Solaris Security Toolkit installieren und für die Zusammenarbeit mit dem Logical Domains Manager konfigurieren. Das Solaris Security Toolkit wird in der Regel in der Steuerdomain installiert, wo auch der Logical Domains Manager ausgeführt wird. Sie können das Solaris Security Toolkit auch in anderen logischen Domains installieren. Der einzige Unterschied besteht darin, dass Sie den `ldm_control-secure.driver` für das Hardening der Steuerdomain verwenden, und einen anderen Treiber, z. B. `secure.driver`, für das Hardening der anderen logischen Domains. Dies liegt daran, dass `ldm_control-secure.driver` spezifisch für die Steuerdomain gilt. Der `ldm_control-secure.driver` basiert auf dem `secure.driver` und wurde für

die Verwendung mit dem Logical Domains Manager angepasst und getestet. Weitere Informationen zum `secure.driver` finden Sie im *Solaris Security Toolkit 4.2 Reference Manual*.

Hardening

Der Treiber (`ldm_control-secure.driver`), den das Solaris Security Toolkit für das Hardening des Solaris OS in der Steuerdomain verwendet, wurde speziell angepasst, damit der Logical Domains Manager mit dem OS ausgeführt werden kann. Der `ldm_control-secure.driver` entspricht dem `secure.driver`, der im *Solaris Security Toolkit 4.2 Reference Manual* beschrieben wird.

Der `ldm_control-secure.driver` bietet eine Grundkonfiguration für die Steuerdomain eines Systems, auf dem die Logical Domains Manager-Software ausgeführt wird. Er bietet absichtlich weniger Systemdienste als für eine Solaris OS-Domain typisch ist, wodurch die Steuerdomain für Logical Domains Manager-Operationen anstatt für die allgemeine Verwendung reserviert ist.

Das `install-ldm`-Skript installiert die Logical Domains Manager-Software, falls diese noch nicht installiert ist, und aktiviert die Software.

Im Anschluss folgt eine kurze Zusammenfassung der anderen bedeutenden Änderungen gegenüber `secure.driver`.

- Die Ausführung des Telnet-Servers ist deaktiviert. Sie können stattdessen Secure Shell (`ssh`) verwenden. Sie können weiterhin den Telnet-Client für den Zugriff auf virtuelle Konsolen verwenden, die vom virtuellen Netzwerk-Terminalserver-Daemon von Logical Domains (`vntsd`) gestartet wurden. Wenn z. B. eine virtuelle Konsole aktiv ist, die am TCP-Port 5001 auf dem lokalen System empfangsbereit ist, können Sie auf diese wie folgt zugreifen.

```
# telnet localhost 5001
```

Anweisungen zur Aktivierung von `vntsd` finden Sie unter „[Aktivieren des Logical Domains Manager-Daemons](#)“ auf Seite 37. Diese wird nicht automatisch aktiviert.

- Es wurden folgende Skripts zum Beenden hinzugefügt. Sie ermöglichen die Installation und das Starten des Logical Domains Manager. Einige dieser zusätzlichen Skripts müssen allen angepassten Treibern hinzugefügt werden, die Sie erstellen, und andere sind optional. Die Skripts sind entsprechend markiert (erforderlich oder optional).
 - `install-ldm.fin` – Installiert das `SUNWldm`-Paket. (*Erforderlich*)
 - `enable-ldmd.fin` – Aktiviert den Logical Domains Manager-Daemon (`ldmd`). (*Erforderlich*)

- `enable-ssh-root-login.fin` – Ermöglicht dem Superuser die direkte Anmeldung über die Secure Shell (`ssh`). (*Optional*)
- Die folgenden Dateien haben sich geändert. Diese Änderungen sind in von Ihnen angepassten Treibern optional und sind entsprechend markiert.
 - `/etc/ssh/sshd_config` – root-Kontozugriff ist für das gesamte Netzwerk zulässig. Diese Datei wird in keinem Treiber verwendet. (*Optional*)
 - `/etc/ipf/ipf.conf` – UDP-Port 161 (SNMP) ist geöffnet. (*Optional*)
 - `/etc/host.allow` – Der Secure Shell-Daemon (`sshd`) ist für das gesamte Netzwerk geöffnet, nicht nur für das lokale Teilnetz. (*Optional*)
- Die folgenden Skripts zum Beenden sind deaktiviert (auskommentiert). Sie sollten das `disable-rpc.fin`-Skript in allen angepassten Treibern auskommentieren. Die anderen Änderungen sind optional. Die Skripts sind entsprechend markiert (erforderlich oder optional).
 - `enable-ipfilter.fin` – Der IP-Filter (ein Netzwerk-IP-Filter) ist nicht aktiviert. (*Optional*)
 - `disable-rpc.fin` – Lässt den RPC-Dienst (Remote Procedure Call) deaktiviert. Der RPC-Dienst wird von vielen anderen Systemdiensten verwendet, z. B. NIS (Network Information Service) und NFS (Network File System). (*Erforderlich*)
 - `disable-sma.fin` – Lässt den System Management Agent (NET-SNMP) aktiviert. (*Optional*)
 - `disable-ssh-root-login.fin` – `ssh-root`-Anmeldung kann nicht deaktiviert werden.
 - `set-term-type.fin` – nicht benötigtes Legacy-Skript (*Optional*)

Minimieren von logischen Domains

Das Solaris OS kann je nach Ihren Anforderungen mit einer unterschiedlichen Anzahl von Paketen konfiguriert werden. Durch die Minimierung wird dieser Paketsatz auf das absolute Minimum reduziert, das zum Ausführen Ihrer gewünschten Anwendungen benötigt wird. Die Minimierung ist wichtig, da dadurch die Anzahl der Software-Anwendungen reduziert wird, die potenzielle Sicherheitsanfälligkeiten enthalten können, und der Aufwand, der mit der ordnungsgemäßen Aktualisierung der installierten Software über Patches verbunden ist. Der Minimierungsvorgang für logische Domains umfasst JumpStart™-Unterstützung für ein minimiertes Solaris OS, das nach wie vor vollständige Unterstützung für alle Domains bietet.

Im Solaris Security Toolkit ist ein JumpStart-Profil (`minimal-ldm_control.profile`) enthalten. Es dient zur Minimierung einer logischen Domain für LDoms und installiert alle Solaris OS-Pakete, die für LDoms- und LDoms MIB-Unterstützung erforderlich sind. Wenn Sie die LDoms-MIB in der

Steuerdomain verwenden möchten, müssen Sie dieses Paket separat hinzufügen, nachdem Sie die LDoms- und Solaris Security Toolkit-Pakete installiert haben. Es wird nicht automatisch zusammen mit der anderen Software installiert. Weitere Informationen zur Installation und Verwendung der LDoms-MIB finden Sie im *Logical Domains (LDoms) Management Information Base 1.0.2 Administrationshandbuch*.

Autorisierung

Die Autorisierung für den Logical Domains Manager umfasst zwei Ebenen:

- Lesen – ermöglicht das Anzeigen, jedoch nicht das Ändern der Konfiguration
- Lesen und Schreiben – ermöglicht das Anzeigen und Ändern der Konfiguration

Die Änderungen werden nicht am Solaris OS durchgeführt, sondern der Autorisierungsdatei durch das Paketskript `postinstall` bei der Installation des Logical Domains Manager hinzugefügt. Analog dazu werden die Autorisierungseinträge durch das Paketskript `preremove` entfernt.

In der folgenden Tabelle sind die `ldm`-Unterbefehle mit der entsprechenden Benutzerautorisierung aufgelistet, die zur Durchführung der Befehle benötigt werden.

TABELLE 2-1 `ldm` – Unterbefehle und Benutzerautorisierung

ldm-Unterbefehl*	Benutzerautorisierung
add-*	solaris.ldoms.write
bind-domain	solaris.ldoms.write
list	solaris.ldoms.read
list-*	solaris.ldoms.read
panic-domain	solaris.ldoms.write
remove-*	solaris.ldoms.write
set-*	solaris.ldoms.write
start-domain	solaris.ldoms.write
stop-domain	solaris.ldoms.write
unbind-domain	solaris.ldoms.write

*, Bezieht sich auf alle Ressourcen, die Sie hinzufügen, auflisten, entfernen oder einstellen können.

Prüfung

Die Prüfung der CLI-Befehle von Logical Domains Manager erfolgt mithilfe der BSM-Prüfung (Basic Security Modul) von Solaris OS. Ausführliche Informationen zum Solaris OS BSM Auditing finden Sie im Solaris 10 *System Administration Guide: Security Services*.

BSM-Prüfung ist nicht standardmäßig für den Logical Domains Manager aktiviert, jedoch wird die entsprechende Infrastruktur bereitgestellt. Sie haben zwei Möglichkeiten, um die BSM-Prüfung zu aktivieren:

- Ausführen des Skripts zum Beenden `enable-bsm.fin` im Solaris Security Toolkit.
- Verwenden des Solaris OS-Befehls `bsmconv(1M)`.

Weitere Informationen zum Aktivieren, Überprüfen, Deaktivieren, Drucken und Rotieren von Protokollen über BSM-Prüfung mit dem Logical Domains Manager finden Sie unter „[Aktivieren und Verwenden der BSM-Auditing \(Basic Security Modul\)](#)“ auf Seite 94.

Konformität

Das Solaris Security Toolkit verfügt über eigene Prüfungsfunktionen. Die Solaris Security Toolkit-Software kann die Sicherheitslage eines beliebigen Systems mit Solaris OS automatisch validieren, indem es einen Vergleich mit einem vordefinierten Sicherheitsprofil durchführt. Weitere Informationen zu dieser Konformitätsfunktion finden Sie im *Solaris Security Toolkit 4.2 Administration Guide* unter „Auditing System Security“.

Installieren und Aktivieren der Software

In diesem Kapitel wird beschrieben, wie Sie die Logical Domains Manager 1.0.2-Software und andere Software in einer Steuerdomain auf unterstützten Servern installieren und aktivieren. Eine Liste der unterstützten Server erhalten Sie in den *Versionshinweisen zu Logical Domains (LDoms) 1.0.2* unter „Unterstützte Server“.

Die für Sie relevanten Informationen in diesem Kapitel hängen von Ihrer Plattform ab. Wenn Sie die Logical Domains-Software auf einer neuen Sun UltraSPARC T2-Plattform verwenden, sollte die gesamte Software bereits werkseitig installiert sein.

Upgrade von Solaris OS

Dieser Abschnitt enthält Informationen zum Sichern und Wiederherstellen der Logical Domains-Vorgabendatenbankdatei und zur Durchführung eines Live-Upgrades in der Steuerdomain.

Sichern und Wiederherstellen der Logical Domains-Vorgabendatenbankdatei

Jedes Mal, wenn Sie das Betriebssystem der Steuerdomain aktualisieren, müssen Sie die Logical Domains-Vorgabendatenbankdatei sichern und wiederherstellen. Diese Datei befindet sich unter `/var/opt/SUNWldm/ldom-db.xml`.

Hinweis – Sie müssen die Datei `/var/opt/SUNWldm/ldom-db.xml` ebenfalls sichern und wiederherstellen, wenn Sie andere Vorgänge vornehmen, die Dateidaten der Steuerdomain zerstören, wie beispielsweise einen Plattenwechsel.

Ausführen eines Live-Upgrades in der Steuerdomain

Falls Sie ein Live-Upgrade in der Steuerdomain ausführen, empfiehlt es sich, in der Datei `/etc/lu/synclist` die folgende Zeile einzufügen:

<code>/var/opt/SUNWldm/ldom-db.xml</code>	<code>OVERWRITE</code>
---	------------------------

Auf diese Weise wird die Datenbank beim Wechsel zwischen zwei Boot-Umgebungen automatisch von der aktiven Boot-Umgebung in die neue Boot-Umgebung kopiert. Weitere Informationen über `/etc/lu/synclist` und die Synchronisierung der Dateien zwischen Boot-Umgebungen finden Sie unter „Synchronisieren von Dateien zwischen Boot-Umgebungen“ im *Solaris 10 8/07 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades*.

Upgrade auf LDomS 1.0.2-Software

Bestehende LDomS 1.0.1-Konfigurationen funktionieren mit LDomS 1.0.2-Software. Sie brauchen das folgende Verfahren also nicht durchzuführen, falls Sie ein Upgrade von LDomS 1.0.1-Software auf LDomS 1.0.2-Software vornehmen. Falls Sie jedoch eine bestehende LDomS 1.0-Konfiguration mit LDomS 1.0.2-Software verwenden möchten, müssen Sie das folgende Verfahren durchführen.

▼ So führen Sie ein Upgrade von LDomS 1.0-Software auf LDomS 1.0.2-Software durch

Vorhandene LDomS 1.0-Konfigurationen funktionieren *nicht* in LDomS 1.0.2. Die folgenden Schritte beschreiben eine Methode zur Speicherung und Neuerstellung einer Konfiguration mithilfe von XML-Einschränkungsdateien und der Option `-i` des Befehls `ldm start-domain`. Bei dieser Methode werden die tatsächlichen Verknüpfungen nicht beibehalten, nur die Einschränkungen, die zur Erstellung

dieser Bindungen verwendet wurden. Dies bedeutet, dass die Domains nach dieser Prozedur zwar über die gleichen virtuellen Ressourcen verfügen, diese jedoch nicht unbedingt mit denselben physikalischen Ressourcen verknüpft sind.

Der grundlegende Prozess besteht in der Speicherung der Einschränkungsinformationen für jede Domain in einer XML-Datei, die nach dem Upgrade wieder an den Logical Domains Manager ausgegeben werden können, um die gewünschte Konfiguration neu zu erstellen. Diese Vorgehensweise funktioniert für Gastdomains, jedoch nicht für die Steuerdomain. Obwohl Sie die Einschränkungen der Steuerdomain (`primary`) in einer XML-Datei speichern können, lassen sich diese nicht wieder in den Befehl `ldm start-domain -i` integrieren.

1. Aktualisieren Sie auf die neuste Version von Solaris OS. Weitere Informationen finden Sie in Schritt 2, „[So installieren Sie Solaris 10 OS](#)“ auf Seite 19.
2. Erstellen Sie für jede Domain eine XML-Datei mit den Einschränkungen der Domain.

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

3. Zeigen Sie eine Liste der logischen Domainkonfigurationen auf dem Systemcontroller an.

```
# ldm ls-config
```

4. Entfernen Sie alle logischen Domainkonfigurationen, die auf dem Systemcontroller gespeichert sind.

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

5. Deaktivieren Sie den Logical Domains Manager-Daemon (`ldmd`).

```
# svcadm disable ldmd
```

6. Entfernen Sie das Logical Domains Manager-Paket (`SUNWldm`).

```
# pkgrm SUNWldm
```

7. Entfernen Sie das Solaris Security Toolkit-Paket (`SUNWjass`), wenn Sie dieses verwenden.

```
# pkgrm SUNWjass
```

8. Führen Sie ein Flash-Update der Firmware durch. Eine Beschreibung der gesamten Prozedur finden Sie unter „[So aktualisieren Sie die Systemfirmware](#)“ auf Seite 20 oder „[So aktualisieren Sie die Systemfirmware ohne einen FTP-Server](#)“ auf Seite 21.
9. Laden Sie das LDomS 1.0.2-Softwarepaket herunter.
Anweisungen zum Herunterladen und Installieren des Logical Domains Manager, des Solaris Security Toolkit und des Logical Domains MIB erhalten Sie unter „[So laden Sie den Logical Domains Manager, das Solaris Security Toolkit und die Logical Domains MIB herunter](#)“ auf Seite 22.
10. Konfigurieren Sie die `primary`-Domain manuell neu. Anweisungen dazu finden Sie unter „[So richten Sie die Steuerdomain ein](#)“ auf Seite 44.
11. Führen Sie die folgenden Befehle für die XML-Datei jeder Gastdomain aus, die Sie in Schritt 2 erstellt haben.

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

Erstinstallation der Software in der Steuerdomain

Die erste Domain, die bei Installation der Logical Domains Manager-Software erstellt wird, ist die Steuerdomain. Die erste Domain trägt die Bezeichnung `primary`, die sich nicht ändern lässt. Die folgenden Hauptkomponenten werden in der Steuerdomain installiert.

- Solaris 10 OS. Installieren Sie bei Bedarf alle Patches, die in den *Versionshinweisen zu Logical Domains (LDoms) 1.0.2* empfohlen werden. Siehe „[So installieren Sie Solaris 10 OS](#)“ auf Seite 19.
- Systemfirmware, Version 6.5, für Ihre Sun UltraSPARC T1-Plattform oder Systemfirmware, Version 7.0, für Ihre Sun UltraSPARC T2-Plattform. Siehe „[So aktualisieren Sie die Systemfirmware](#)“ auf Seite 20.
- Logical Domain Manager 1.0.2-Software. Siehe „[Installieren des Logical Domains Manager und des Solaris Security Toolkit](#)“ auf Seite 23.
- (Optional) Solaris Security Toolkit 4.2-Software. Siehe „[Installieren des Logical Domains Manager und des Solaris Security Toolkit](#)“ auf Seite 23.

- (Optional) Logical Domains (LDMs) Management Information Base (MIB)-Softwarepaket. Weitere Informationen zur Installation und Verwendung der LDMs-MIB finden Sie im *Logical Domains (LDMs) MIB 1.0.2 Administrationshandbuch*.

Solaris OS und die Systemfirmware müssen auf Ihrem Server installiert sein, bevor Sie den Logical Domains Manager installieren. Nach der Installation von Solaris OS, der Systemfirmware und des Logical Domains Manager wird die ursprüngliche Domain zur Steuerdomain.

▼ So installieren Sie Solaris 10 OS

Installieren Sie Solaris 10 OS, falls es noch nicht installiert wurde. Informationen zur Ermittlung des Solaris-Betriebssystems, das Sie für diese Version der Logical Domains Software verwenden sollten, finden Sie in den *Versionshinweisen von Logical Domains (LDMs) 1.0.2* unter „Erforderliche Software“. Vollständige Anweisungen zur Installation von Solaris OS finden Sie im Installationshandbuch für Solaris 10 OS. Sie können die Installation an die Erfordernisse Ihres Systems anpassen.

Hinweis – Für logische Domains können Sie Solaris OS nur auf eine ganze Platte oder in einer Datei installieren, die als Blockeinheit installiert wurde.

1. Installieren Sie Solaris 10 OS.

Die Minimierung ist optional. Das Solaris Security Toolkit enthält das folgende JumpStart-Minimierungsprofil für Logical Domains-Software:

```
/opt/SUNWjass/Profiles/minimal-ldm_control.profile
```

2. Installieren Sie die erforderlichen Patches bei Installation von Solaris 10 11/06 OS. Eine Liste der erforderlichen Patches finden Sie in den *Versionshinweisen zu Logical Domains (LDMs) 1.0.2* unter „Erforderliche Solaris 10 11/06 OS-Patches“.

Hinweis – Wenn Sie ein Betriebssystem in einer anderen Sprache als Englisch in einer Gastdomain installieren, muss die Sprache des Konsolenterminals dem für das Installationsprogramm des Betriebssystems erforderlichen Standardgebietsschema entsprechen. Beispielsweise erfordert das Installationsprogramm für Solaris OS die Gebietsschemata „EUC“, während das Linux-Installationsprogramm möglicherweise Unicode-Gebietsschemata benötigt.

▼ So aktualisieren Sie die Systemfirmware

Sie finden die Systemfirmware für Ihre Plattform auf der SunSolve-Site:

<http://sunsolve.sun.com>

Eine Liste der von unterstützten Servern benötigten Firmware finden Sie in den *Versionshinweisen zu Logical Domains (LDoms) 1.0.2* unter „Erforderliche Systemfirmware-Patches“.

Diese Prozedur beschreibt, wie Sie die Systemfirmware mithilfe des Befehls `flashupdate(1M)` auf Ihrem Systemcontroller aktualisieren.

- Wenn Sie keinen Zugriff auf einen lokalen FTP-Server haben, lesen Sie den Abschnitt [„So aktualisieren Sie die Systemfirmware ohne einen FTP-Server“](#) auf Seite 21.
- Wenn Sie die Systemfirmware von der Steuerdomain aus aktualisieren möchten, lesen Sie die Versionshinweise Ihrer Systemfirmware.

Weitere Informationen zum Installieren und Aktualisieren der Systemfirmware für diese Server finden Sie in den Administrationshandbüchern oder Produkthinweisen für die unterstützten Server.

1. Fahren Sie den Hostserver herunter und trennen Sie die Verbindung mit dem entsprechenden, an den Systemcontroller angeschlossenen Managementport: seriell oder Netzwerkport.

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

2. Aktualisieren Sie die Systemsoftware mithilfe des Befehls `flashupdate(1M)` (abhängig von Ihrem Server).

```
sc> flashupdate -s IP-address -f Pfad/Sun_System_Firmware-  
x_x_x_build_nn-server-name.bin  
username: ihre_benutzer-id  
password: ihr_passwort
```

Wobei:

- *IP-address* ist die IP-Adresse Ihres FTP-Servers.
- *Pfad* ist der Speicherort in SunSolvesm oder Ihr eigenes Verzeichnis, aus dem Sie das Systemfirmware-Abbild abrufen können.
- *x_x_x* ist die Versionsnummer der Systemfirmware.
- *nn* ist die Build-Nummer dieser Version.
- *server-name* ist der Name Ihres Servers. Der *server-name* für den Sun Fire T2000-Server lautet z. B. `Sun_Fire_T2000`.

3. Setzen Sie den Systemcontroller zurück:

```
sc> resetsc -y
```

4. Schalten Sie den Host-Server ein, und fahren Sie ihn hoch.

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

▼ So aktualisieren Sie die Systemfirmware ohne einen FTP-Server

Wenn Sie keinen Zugriff auf einen lokalen FTP-Server haben, um Firmware auf den Systemcontroller hochzuladen, können Sie das Dienstprogramm `sysfwdownload` verwenden, das im Lieferumfang Ihres Systemfirmware-Upgradepakets auf der SunSolve-Site verfügbar ist:

<http://sunsolve.sun.com>

1. Führen Sie die folgenden Befehle im Solaris OS aus:

```
# cd firmwareverzeichnis  
# sysfwdownload systemfirmwaredatei
```

2. Fahren Sie die Solaris OS-Instanz herunter.

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

3. Schalten Sie aus, und aktualisieren Sie die Firmware auf dem Systemcontroller.

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

4. Setzen Sie den Systemcontroller zurück, und schalten Sie ihn ein.

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

▼ So rüsten Sie die Systemfirmware ab

Nachdem Sie die Systemfirmware für die Verwendung mit der Logical Domains-Software aktualisiert haben, können Sie die Firmware wieder auf die ursprüngliche Nicht-Logical Domains-Firmware abrüsten.

- Führen Sie den Befehl `flashupdate(1M)` aus, und geben Sie den Pfad zur ursprünglichen Nicht-Logical Domains-Firmware an.

Herunterladen des Logical Domains Manager und des Solaris Security Toolkit

▼ So laden Sie den Logical Domains Manager, das Solaris Security Toolkit und die Logical Domains MIB herunter

1. Laden Sie die tar-Datei (`LDoms_Manager-1_0_2.zip`) mit dem Logical Domains Manager-Paket (`SUNWldm`), das Solaris Security Toolkit (`SUNWjass`) und Installationsskript (`install-ldm`) sowie das Logical Domains Management Information Base-Paket (`SUNWldmib.v`) von der Sun Software Download-Site herunter. Sie finden die Software auf folgender Website:

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

2. Entpacken Sie die zip-Datei.

```
$ unzip LDoms_Manager-1_0_2.zip
```

Die Verzeichnisstruktur für die heruntergeladene Software entspricht in etwa der folgenden:

CODEBEISPIEL 3-1 Verzeichnisstruktur für heruntergeladene Logical Domains 1.0.2-Software

```
LDoms_Manager-1_0_2/  
  Install/  
    install-ldm  
  Legal/
```

```
Ldoms_1.0.2_Entitlement.txt
Ldoms_1.0.2_SLA_Entitlement.txt
Product/
  SUNWjass/
  SUNWldm.v/
  SUNWldmib.v
README
```

Installieren des Logical Domains Manager und des Solaris Security Toolkit

Sie können den Logical Domains Manager und das Solaris Security Toolkit auf folgende drei Arten installieren:

- Installieren der Pakete und Patches mithilfe des Installationsskripts. Dadurch wird automatisch die Logical Domains Manager- und die Solaris Security Toolkit-Software installiert. Siehe „[Verwenden des Installationsskripts zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software](#)“ auf Seite 24.
- Pakete mithilfe von JumpStart installieren. Siehe „[Verwenden von JumpStart zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software](#)“ auf Seite 30.
- Jedes Paket manuell installieren. Siehe „[Manuelles Installieren des Logical Domains Manager und des Solaris Security Toolkit](#)“ auf Seite 33.

Hinweis – Bedenken Sie, dass Sie nach der Installation der LDoms- und Solaris Security Toolkit-Pakete das LDoms MIB-Softwarepaket automatisch installieren müssen. Es wird nicht automatisch zusammen mit den anderen Paketen installiert. Weitere Informationen zur Installation und Verwendung der LDoms-MIB finden Sie im *Logical Domains (LDoms) Management Information Base 1.0.2 Administrationshandbuch*.

Verwenden des Installationsskripts zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software

Bei Verwendung des Installationsskripts `install-ldm` haben Sie mehrere Optionen zur Ausführung des Skripts. Diese werden in den nachfolgenden Prozeduren beschrieben.

- **Bei Verwendung des Skripts `install-ldm` ohne Optionen werden folgende Aktionen automatisch durchgeführt:**
 - Überprüft, ob es sich bei der Solaris OS-Version um Solaris 10 11/06 handelt.
 - Überprüft, ob die Paketunterverzeichnisse `SUNWldm/` und `SUNWjass/` vorhanden sind.
 - Überprüft, ob die erforderlichen Solaris Logical Domains-Treiberpakete, `SUNWldomu` und `SUNWldomu`, vorhanden sind.
 - Überprüft, dass die Pakete `SUNWldm` und `SUNWjass` nicht installiert sind.

Hinweis – Wenn das Skript während der Installation eine frühere Version von `SUNWjass` erkennt, müssen Sie diese entfernen. Es ist *nicht* erforderlich, frühere Hardening-Aktionen Ihres Solaris OS rückgängig zu machen.

- Installiert die Logical Domains Manager 1.0.2-Software (`SUNWldm`-Paket).
- Installiert die Solaris Security Toolkit 4.2-Software, einschließlich der erforderlichen Patches (`SUNWjass`-Paket).
- Überprüft, dass alle Pakete installiert sind.
- Aktiviert den Logical Domains Manager-Daemon (`ldmd`).
- Führt ein Hardening des Solaris OS in der Steuerdomain mit dem Solaris Security Toolkit `ldm_control-secure.driver` oder einem der anderen ausgewählten Treiber durch, die auf `-secure.driver` enden.
- **Wenn Sie das Skript `install-ldm` mit der Option `-d` verwenden**, können Sie einen Solaris Security Toolkit-Treiber verwenden, der nicht in `-secure.driver` endet. Diese Option führt automatisch alle in der vorherigen Auswahl aufgelisteten Funktionen plus zusätzlicher Option aus:
 - Führt ein Hardening des Solaris OS in der Steuerdomain mit dem für das Solaris Security Toolkit angepassten Treiber durch, den Sie angeben, z. B. `server-secure-meinname.driver`.
- **Wenn Sie das Skript `install-ldm` mit der Option `-d` ausführen und `none` angeben**, besagt dies, dass Sie *kein* Hardening des Solaris OS in Ihrer Steuerdomain mithilfe des Solaris Security Toolkit durchführen möchten. Diese Option führt automatisch alle in der vorherigen Auswahl aufgelisteten

Funktionen ohne das Hardening aus. Es wird nicht empfohlen, dass Sie den Einsatz des Solaris Security Toolkits umgehen, außer für den Fall, dass Sie ein Hardening Ihrer Steuerdomain mithilfe eines anderen Prozesses beabsichtigen.

- **Die Verwendung des Skripts `install-lbm` mit der Option `-p`** gibt an, dass Sie nur Aktionen nach der Installation durchführen möchten, nämlich das Aktivieren des Logical Domains Manager-Daemons (`ldmd`) und das Ausführen des Solaris Security Toolkit. Sie verwenden diese Option beispielsweise, wenn die Pakete `SUNWldm` und `SUNWjass` auf Ihrem Server vorinstalliert sind. Siehe „[So führen Sie eine Installation mit dem Skript `install-lbm` und der Option `-p` durch](#)“ auf Seite 30.

▼ So führen Sie eine Installation mit dem Skript `install-lbm` ohne Optionen durch

- **Führen Sie das Installationsskript ohne Optionen aus.**

Das Installationsskript ist Teil des `SUNWldm`-Pakets und befindet sich im Unterverzeichnis `Install`.

```
# Install/install-lbm
```

- a. Wenn ein oder mehrere Pakete bereits installiert sind, erhalten Sie diese Meldung.

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

Wenn Sie nur Aktionen nach der Installation durchführen möchten, gehen Sie zum Abschnitt „[So führen Sie eine Installation mit dem Skript `install-lbm` und der Option `-p` durch](#)“ auf Seite 30.

- b. Wenn der Prozess erfolgreich war, erhalten Sie ähnliche Meldungen wie in den folgenden Beispielen:
 - Codebeispiel 3-2 zeigt eine erfolgreiche Ausführung des Skripts `install-lbm`, wenn Sie das folgende Standard-Sicherheitsprofil wählen:
 - a) Ausgabe einer Solaris-Konfiguration für LDomS, für die ein Hardening durchgeführt wurde (empfohlen)
 - Codebeispiel 3-3 zeigt eine erfolgreiche Ausführung des Skripts `install-lbm`, wenn Sie das folgende Sicherheitsprofil wählen:
 - c) Ihr benutzerdefiniertes Solaris-Sicherheitskonfigurationsprofil

Die zu Ihrer Auswahl angezeigten Treiber enden mit `-secure.driver`. Wenn Sie einen angepassten Treiber programmieren, der nicht in `-secure.driver` endet, müssen Sie diesen mit der Option `install-lbm -d` angeben. (Siehe „So führen Sie eine Installation mit dem Skript `install-lbm` und der Option `-d` durch“ auf Seite 28.)

CODEBEISPIEL 3-2 Ausgabe einer Solaris-Konfiguration für LDoms, für die ein Hardening durchgeführt wurde

```
# Install/install-lbm
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.

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 lbm_control-secure.driver.
Please wait. . .
/opt/SUNWjass/bin/jass-execute -q -d lbm_control-secure.driver
Executing driver, lbm_control-secure.driver
```


CODEBEISPIEL 3-2 Ausgabe einer Solaris-Konfiguration für LDoms, für die ein Hardening durchgeführt wurde (*Fortsetzung*)

```
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.
```

CODEBEISPIEL 3-3 Ausgabe bei der Auswahl eines angepassten Konfigurationsprofils

```
# 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.
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.
```

CODEBEISPIEL 3-3 Ausgabe bei der Auswahl eines angepassten Konfigurationsprofils (*Fortsetzung*)

```
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.
```

▼ So führen Sie eine Installation mit dem Skript
`install-ldm` und der Option `-d` durch

- Führen Sie das Installationsskript mit der Option `-d` aus, um einen mit dem Solaris Security Toolkit angepassten Hardening-Treiber anzugeben, z. B. `server-secure-myname.driver`.

Das Installationsskript ist Teil des `SUNWldm`-Pakets und befindet sich im Unterverzeichnis `Install`.

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

Wenn der Prozess erfolgreich war, erhalten Sie ähnliche Meldungen wie im Codebeispiel 3-4.

CODEBEISPIEL 3-4 Ausgabe bei erfolgreicher Ausführung des Skripts `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.
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.
```

CODEBEISPIEL 3-4 Ausgabe bei erfolgreicher Ausführung des Skripts `install-ldm -d` (Fortsetzung)

```
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.
```

▼ So führen Sie eine Installation mit dem Skript `install-ldm` und der Option `-d none` durch.

- Führen Sie das Installationsskript mit der Option `-d none` aus, um anzugeben, dass *kein* Hardening Ihres Systems mit einem Solaris Security Toolkit-Treiber durchgeführt werden soll.

Das Installationsskript ist Teil des `SUNWldm`-Pakets und befindet sich im Unterverzeichnis `Install`.

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

Wenn der Prozess erfolgreich war, erhalten Sie ähnliche Meldungen wie im Codebeispiel 3-5.

CODEBEISPIEL 3-5 Ausgabe bei erfolgreicher Ausführung des Skripts `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.

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.
```

▼ So führen Sie eine Installation mit dem Skript `install-ldm` und der Option `-p` durch

Sie können diese Option verwenden, wenn die Pakete `SUNWldm` und `SUNWjass` auf Ihrem Server vorinstalliert sind und Sie nur Aktionen nach der Installation durchführen möchten, nämlich das Aktivieren des Logical Domains Manager-Daemons (`ldmd`) und das Ausführen des Solaris Security Toolkit.

- **Führen Sie das Installationsskript mit der Option `-p` durch, wenn Sie nur die Aktionen nach der Installation durchführen möchten, nämlich: Aktivieren von `ldmd` und Ausführen des Solaris Security Toolkit, um ein Hardening Ihres Systems durchzuführen.**

```
# 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.
```

Verwenden von JumpStart zum Installieren der Logical Domains Manager 1.0.2- und Solaris Security Toolkit 4.2-Software

Ausführliche Informationen zur Verwendung von JumpStart finden Sie unter *JumpStart Technology: Effective Use in the Solaris Operating Environment*.



Achtung – Unterbrechen Sie die Verbindung mit der virtuellen Konsole *nicht* während einer Netzwerkinstallation.

▼ So richten Sie einen JumpStart-Server ein

- Wenn Sie bereits einen JumpStart-Server eingerichtet haben, fahren Sie mit dem Abschnitt „[So führen Sie eine Installation mit der JumpStart-Software durch](#)“ auf [Seite 32](#) dieses Administrationshandbuchs fort.
- Wenn Sie noch keinen JumpStart-Server eingerichtet haben, müssen Sie dies nachholen.

Ausführliche Informationen zu diesem Vorgang finden Sie im *Solaris 10 11/06 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien*. Sie finden dieses Installationshandbuch unter folgender Adresse:

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

1. **Lesen Sie Kapitel 3 „Vorbereiten von benutzerdefinierten JumpStart-Installationen (Vorgehen)“ im *Solaris 10 11/06 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien*, und führen Sie die folgenden Schritte durch.**
 - a. Lesen Sie die Aufgabenübersicht unter „Übersicht über die Schritte: Vorbereiten von benutzerdefinierten JumpStart-Installationen“.
 - b. Richten Sie vernetzte Systeme mit den Verfahren unter „Erstellen eines Profilservers für vernetzte Systeme“ ein.
 - c. Erstellen Sie die `rules`-Datei mit dem Verfahren unter „Erstellen der Datei `rules`“.
2. **Validieren Sie die `rules`-Datei mit dem Verfahren unter „Validieren der Datei `rules`“.**

Das Solaris Security Toolkit enthält die folgenden Profile und Skripts zum Beenden. Weitere Informationen zu Profilen und Skripts zum Beenden finden Sie im *Solaris Security Toolkit 4.2 Reference Manual*.

▼ So führen Sie eine Installation mit der JumpStart-Software durch

1. Wechseln Sie in das Verzeichnis, in das Sie das Solaris Security Toolkit-Paket (SUNWjass) heruntergeladen haben.

```
# cd /Pfad-von-download
```

2. Installieren Sie SUNWjass zum Erstellen der JumpStart-Verzeichnisstruktur (jumpstart).

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

3. Tragen Sie in die Datei
/jumpstart/opt/SUNWjass/Sysidcfg/Solaris_10/sysidcfg Ihre
Netzwerkumgebung ein.

4. Kopieren Sie die Datei
/jumpstart/opt/SUNWjass/Drivers/user.init.SAMPLE in die Datei
/jumpstart/opt/SUNWjass/Drivers/user.init.

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

5. Tragen Sie in die Datei user.init Ihre Pfade ein.
6. Um das Solaris Security Toolkit-Paket (SUNWjass) auf dem Zielsystem während einer JumpStart-Installation zu installieren, müssen Sie das Paket im Verzeichnis JASS_PACKAGE_MOUNT ablegen, das in Ihrer Datei user.init definiert ist. Beispiel:

```
# cp -r /Pfad/to/LDoms_Manager-1_0_2/Product/SUNWjass  
/jumpstart/opt/SUNWjass/Packages
```

7. Um das Logical Domains Manager-Paket (SUNWldm.v) auf dem Zielsystem während einer JumpStart-Installation zu installieren, müssen Sie das Paket aus dem Download-Bereich im Verzeichnis JASS_PACKAGE_MOUNT ablegen, das in Ihrer Datei user.init definiert ist. Beispiel:

```
# cp -r /Pfad/to/LDoms_Manager-1_0_2/Product/SUNWldm.v  
/jumpstart/opt/SUNWjass/Packages
```

8. Wenn Probleme mit einem Multihome-JumpStart-Server auftreten, passen Sie die beiden Einträge in der Datei user.init für JASS_PACKAGE_MOUNT und JASS_PATCH_MOUNT an den korrekten Pfad für die Verzeichnisse

JASS_HOME_DIR/Patches und JASS_HOME_DIR/Packages an. Weitere Informationen erhalten Sie in den Kommentaren in der Datei user.init.SAMPLE.

9. Verwenden Sie den `ldm_control-secure.driver` als Basistreiber für die Logical Domains Manager-Steuerdomain.

Weitere Informationen zur Anpassung des Treibers für Ihre Zwecke finden Sie im *Solaris Security Toolkit 4.2 Reference Manual*. Der Haupttreiber im Solaris Security Toolkit, der dem `ldm_control-secure.driver` entspricht, ist der `secure.driver`.

10. Nach Durchführung der Änderungen im `ldm_control-secure.driver` ist ein entsprechender Eintrag in der `rules-Datei` erforderlich.

- Wenn Sie die LDOMs-Steuerdomain minimieren möchten, geben Sie das `minimal-ldm-control.profile` in Ihrer `rules-Datei` wie im folgenden Beispiel an.

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

Hinweis – Bedenken Sie, dass Sie nach der Installation der LDOMs- und Solaris Security Toolkit-Pakete das LDOMs MIB-Softwarepaket automatisch installieren müssen. Es wird nicht automatisch zusammen mit den anderen Paketen installiert. Weitere Informationen zur Installation und Verwendung der LDOMs-MIB finden Sie im *Logical Domains (LDMs) Management Information Base 1.0.2 Administrationshandbuch*.

- Wenn Sie die LDOMs-Steuerdomain nicht minimieren möchten, sollte Ihr Eintrag wie im folgenden Beispiel aussehen.

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

11. Wenn Sie Hardening-Vorgänge während der JumpStart-Installation rückgängig machen möchten, müssen Sie den folgenden SMF-Befehl ausführen, um den Logical Domains Manager neu zu starten.

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

Manuelles Installieren des Logical Domains Manager und des Solaris Security Toolkit

Führen Sie die folgenden Schritte durch, um den Logical Domains Manager und die Solaris Security Toolkit-Software manuell zu installieren:

- „So führen Sie eine manuelle Installation der Logical Domains Manager (LDoms) 1.0.2-Software durch“ auf Seite 34.
- „(Optional) So führen Sie eine manuelle Installation der Solaris Security Toolkit 4.2-Software durch“ auf Seite 34.
- „(Optional) So führen Sie ein manuelles Hardening der Steuerdomain durch“ auf Seite 35.

▼ So führen Sie eine manuelle Installation der Logical Domains Manager (LDoms) 1.0.2-Software durch

Laden Sie die Logical Domains Manager 1.0.2-Software, das `SUNWldm`-Paket, von der Sun Software Download-Site herunter. Spezifische Anweisungen dazu finden Sie unter „So laden Sie den Logical Domains Manager, das Solaris Security Toolkit und die Logical Domains MIB herunter“ auf Seite 22.

1. Verwenden Sie den Befehl `pkgadd(1M)`, um das Paket `SUNWldm.v` zu installieren. Verwenden Sie die Option `-G`, um das Paket nur in der globalen Zone zu installieren, und die Option `„-d“`, um den Pfad zu dem Verzeichnis anzugeben, das das `SUNWldm.v`-Paket enthält.

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

2. Beantworten Sie alle Fragen in den interaktiven Eingabeaufforderungen mit `y` für yes (ja).
3. Prüfen Sie mit dem Befehl `pkginfo(1)`, ob das Paket `SUNWldm` für die Logical Domains Manager 1.0.2-Software installiert ist.

Im Anschluss sehen Sie ein Beispiel für Versionsinformationen (REV).

```
# pkginfo -l SUNWldm | grep VERSION
VERSION=1.0.2,REV=2007.08.23.10.20
```

▼ (Optional) So führen Sie eine manuelle Installation der Solaris Security Toolkit 4.2-Software durch

Wenn Sie Ihr System sichern möchten, laden Sie das Paket `SUNWjass` herunter, und installieren Sie es. Die erforderlichen Patches (122608-03 und 125672-01) sind im `SUNWjass`-Paket enthalten. Spezifische Anweisungen zum Herunterladen der Software finden Sie unter „So laden Sie den Logical Domains Manager, das Solaris Security Toolkit und die Logical Domains MIB herunter“ auf Seite 22.

Weitere Informationen zu Sicherheitsaspekten bei Verwendung der Logical Domains Manager-Software finden Sie in Kapitel [Kapitel 2](#). Weitere Referenzquellen finden Sie in der Solaris Security Toolkit 4.2-Dokumentation unter:

<http://docs.sun.com>

1. Verwenden Sie den Befehl `pkgadd(1M)`, um das Paket `SUNWjass` zu installieren.

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

2. Prüfen Sie mit dem Befehl `pkginfo(1)`, ob das Paket `SUNWjass` für die Solaris Security Toolkit 4.2-Software installiert ist.

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

▼ (Optional) So führen Sie ein manuelles Hardening der Steuerdomain durch

Führen Sie diese Schritte nur aus, wenn Sie das Solaris Security Toolkit 4.2-Paket installiert haben.

Hinweis – Wenn Sie das Solaris Security Toolkit für das Hardening der Steuerdomain verwenden, werden viele Systemdienste deaktiviert und bestimmte Einschränkungen für den Netzwerkzugriff eingeführt. Lesen Sie den Abschnitt „[Zugehörige Dokumentation](#)“ auf Seite [xix](#) in diesem Handbuch, um weiterführende Solaris Security Toolkit 4.2-Dokumentation zu finden.

1. Führen Sie ein Hardening mithilfe von `ldm_control-secure.driver` durch.

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

Sie können auch andere Treiber verwenden, um ein Hardening Ihres Systems durchzuführen, oder Treiber anpassen, um die Sicherheit Ihrer Umgebung anzupassen. Weitere Informationen zu Treibern und deren Anpassung finden Sie im *Solaris Security Toolkit 4.2 Reference Manual*.

2. Beantworten Sie alle Fragen in den interaktiven Eingabeaufforderungen mit `y` für `yes` (ja).
3. Fahren Sie den Server herunter, und starten Sie ihn neu, damit das Hardening in Kraft tritt.

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

▼ So überprüfen Sie das Hardening

- **Prüfen Sie, ob der Logical Domains-Hardening-Treiber (ldom_control-secure.driver) das Hardening korrekt angewendet hat.**

Wenn Sie einen anderen Treiber überprüfen möchten, ersetzen Sie den Namen in diesem Beispiel mit dem Namen dieses Treibers.

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

▼ So machen Sie das Hardening rückgängig

1. **Machen Sie auf das Solaris Security Toolkit angewendete Konfigurationsänderungen rückgängig.**

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

Sie werden vom Solaris Security Toolkit gefragt, welche Hardening-Vorgänge Sie rückgängig machen möchten.

2. **Wählen Sie die Hardening-Vorgänge aus, die Sie rückgängig machen möchten.**
3. **Starten Sie das System neu, damit die Konfiguration ohne Hardening in Kraft tritt.**

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

Hinweis – Wenn Sie Hardening-Vorgänge während einer JumpStart-Installation rückgängig machen möchten, müssen Sie die folgenden SMF-Befehle ausführen, um den Logical Domains Manager und den virtuellen Netzwerk-Terminalserver-Daemon neu zu starten.

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

Aktivieren des Logical Domains Manager-Daemons

Das Installationsskript `install-ldm` aktiviert automatisch den Logical Domains Manager-Daemon (`ldmd`). Bei einer manuellen Installation der Logical Domains Manager-Software müssen Sie den Logical Domains Manager-Daemon, `ldmd`, aktivieren, mit dem Sie die logischen Domains erstellen, ändern und steuern können.

▼ So aktivieren Sie den Logical Domains Manager-Daemon

1. Verwenden Sie den Befehl `svcadm(1M)`, um den Logical Domains Manager-Daemon, `ldmd`, zu aktivieren.

```
# svcadm enable ldmd
```

2. Prüfen Sie mit dem Befehl `ldm list`, ob der Logical Domains Manager aktiv ist.

Sie erhalten ähnliche Meldungen wie im folgenden Beispiel für die `factory-default`-Konfiguration. Beachten Sie, dass für die `primary` Domain der Status `active` angezeigt wird, was bedeutet, dass der Logical Domains Manager aktiv ist.

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

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

Erstellen von Autorisierung und Profilen und Zuweisen von Rollen für Benutzerkonten

Mithilfe des für Logical Domains Manager angepassten RBAC-Modells (Role-Based Access Control) von Solaris OS werden Autorisierung und Profile angepasst und Rollen für Benutzerkonten zugewiesen. Weitere Informationen zu RBAC finden Sie in der Solaris 10 System Administrator Collection.

Die Autorisierung für den Logical Domains Manager umfasst zwei Ebenen:

- Lesen – ermöglicht das Anzeigen, jedoch nicht das Ändern der Konfiguration
- Lesen und schreiben – ermöglicht das Anzeigen und Ändern der Konfiguration

Im Anschluss werden die Logical Domains-Einträge aufgelistet, die der Solaris OS-Datei `/etc/security/auth_attr` automatisch hinzugefügt werden:

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

Verwalten der Benutzerautorisierung

▼ So fügen Sie eine Autorisierung für einen Benutzer hinzu

Führen Sie die nachfolgenden Schritte nach Bedarf aus, um in der Datei `/etc/security/auth_attr` Autorisierungen für Logical Domains Manager-Benutzer hinzuzufügen. Da der Superuser bereits über `solaris.*`-Autorisierung verfügt, besitzt er auch Berechtigungen für `solaris.ldoms.*`-Autorisierungen.

1. Erstellen Sie ein lokales Benutzerkonto für jeden Benutzer, der Autorisierung für die Verwendung der `ldm(1M)`-Unterbefehle benötigt.

Hinweis – Um Logical Domains Manager-Autorisierung für einen Benutzer hinzuzufügen, muss ein lokales (Nicht-LDAP)-Konto für diesen Benutzer erstellt werden. Einzelheiten finden Sie in der Solaris 10 System Administrator Collection.

2. Führen Sie einen der folgenden Schritte aus, je nachdem, welche `ldm(1M)`-Unterbefehle Sie für den Benutzer freigeben möchten.

In [TABELLE 2-1](#) erhalten Sie eine Liste der `ldm(1M)`-Befehle und ihrer Benutzerautorisierungen.

- Fügen Sie eine Nur-Lese-Autorisierung für einen Benutzer mithilfe des Befehls `usermod(1M)` hinzu.

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

- Fügen Sie eine Lese- und Schreib-Autorisierung für einen Benutzer mithilfe des Befehls `usermod(1M)` hinzu.

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

▼ So löschen Sie alle Autorisierungen für einen Benutzer

- Löschen Sie alle Autorisierungen für ein lokales Benutzerkonto (die einzig mögliche Option).

```
# usermod -A `` benutzername
```

Verwalten von Benutzerprofilen

Mit dem Paket `SUNWldm` werden zwei systemdefinierte RBAC-Profilen in der Datei `/etc/security/prof_attr` hinzugefügt. Diese dienen zur Autorisierung des Zugriffs auf Logical Domains Manager durch Nicht-Superuser. Die zwei LDoms-spezifischen Profile lauten wie folgt:

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

Eines der vorausgehenden Profile lässt sich einem Benutzerkonto über folgende Prozedur zuordnen.

▼ So fügen Sie ein Profil für einen Benutzer hinzu

- Fügen Sie ein administratives Profil für ein lokales Benutzerkonto hinzu, z. B. LDoms Management.

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

▼ So löschen Sie alle Profile für einen Benutzer

- Löschen Sie alle Profile für ein lokales Benutzerkonto (die einzig mögliche Option).

```
# usermod -P `` benutzername
```

Zuweisen von Rollen zu Benutzern

Der Vorteil dieses Verfahrens besteht darin, dass nur Benutzer, denen eine bestimmte Rolle zugewiesen wurde, diese Rolle auch übernehmen können. Für das Übernehmen einer Rolle ist ein Passwort erforderlich, falls der Rolle ein Passwort zugewiesen wurde. Dies ermöglicht eine zweistufige Sicherheit. Wenn dem Benutzer keine Rolle zugewiesen wurde, kann dieser die Rolle nicht übernehmen (über den Befehl `su rollenname`), selbst wenn der Benutzer über das korrekte Passwort verfügt.

▼ So erstellen Sie eine Rolle und weisen dem Benutzer eine Rolle zu

1. Erstellen Sie eine Rolle.

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

2. Weisen Sie der Rolle ein Passwort zu.

```
# passwd ldm_read
```

3. Weisen Sie die Rolle einem Benutzer zu, z. B. *user_1*.

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

4. Weisen Sie dem Benutzer ein Passwort zu (*user_1*).

```
# passwd user_1
```

5. Weisen Sie nur Zugriff auf das Konto *user_1* zu, das als *ldm_read*-Konto festgelegt werden soll.

```
# su user_1
```

6. Geben Sie bei Aufforderung das Benutzerpasswort ein.

7. Überprüfen Sie die Benutzer-ID und den Zugriff auf die `ldm_read`-Rolle.

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

8. Gewähren Sie dem Benutzer Zugriff für `ldm`-Unterbefehle, die über Leseautorisierung verfügen.

```
# su ldm_read
```

9. Geben Sie bei Aufforderung das Benutzerpasswort ein.

10. Geben Sie den Befehl `id` ein, um den Benutzer anzuzeigen.

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


Einrichten von Diensten und Logical Domains

In diesem Kapitel werden die Vorgehensweisen zum Einrichten von Standardservices, der Steuerdomain und Gastdomains beschrieben.

Ausgabemeldungen

Von den Befehlen, die Sie verwenden, um Standarddienste zu erzeugen und die Steuerdomain (primary-Domain) einzurichten, erhalten Sie, je nach Ihrer Plattform, verschiedene Ausgabemeldungen:

- Sun UltraSPARC T1-Prozessoren
- Sun UltraSPARC T2-Prozessoren

Sun UltraSPARC T1-Prozessoren

Nach Eingabe der Einrichtungsbefehle für die primary-Domain erhalten Sie folgende Meldung, wenn Sie einen Server mit Sun UltraSPARC T1-Prozessor verwenden:

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.

Sun UltraSPARC T2-Prozessoren

Erste Operation – Nach der ersten Operation an einem Gerät oder für einen Dienst an der `primary`-Domain erhalten Sie die folgende Meldung, wenn Sie einen Server mit Sun UltraSPARC T2-Prozessor verwenden:

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

Weitere Operationen bis zum Neustart – Nach jeder weiteren Operation an der `primary`-Domain erhalten Sie bis zum Neustart folgende Meldung, wenn Sie einen Server mit Sun UltraSPARC T2-Prozessor verwenden:

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

Erzeugen von Standarddiensten

Zunächst müssen die folgenden virtuellen Standarddienste erzeugt werden, damit sie später verwendet werden können:

- `vdiskserver` – virtueller Plattenserver
- `vswitch` – virtueller Switchdienst
- `vconscon` – virtueller Konsolenkonzentrator

▼ So erzeugen Sie Standarddienste

1. **Erzeugen Sie einen virtuellen Plattenserver (`vds`), so dass virtuelle Platten in eine Logical Domain importiert werden können.**

Beispielsweise wird durch den folgenden Befehl ein virtueller Plattenserver (`primary-vds0`) der Steuerdomain (`primary`) hinzugefügt.

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

2. Erzeugen Sie einen virtuellen Konsolenkonzentratordienst (`vcc`) zur Verwendung durch den virtuellen Netzwerk-Terminalserver-Daemon (`vntsd`) und als Konzentrador für alle Logical Domain-Konsolen.

Beispielsweise würde durch den folgenden Befehl ein virtueller Konsolenkonzentratordienst (`primary-vcc0`) mit einem Port-Bereich zwischen 5000 und 5100 der Steuerdomain (`primary`) hinzugefügt werden.

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

3. Erzeugen Sie einen virtuellen Switchdienst (`vsw`), um den Netzwerkbetrieb zwischen virtuellen Netzwerk (`vnet`)-Geräten in Logical Domains zu ermöglichen. Weisen Sie dem virtuellen Switch einen GLDv3-konformen Netzwerkadapter zu, falls jede der Logical Domains über den virtuellen Switch aus dem System heraus kommunizieren muss.

Beispielsweise würde mit dem folgenden Befehl der Steuerdomain (`primary`) ein virtueller Switchdienst (`primary-vsw0`) auf dem Netzwerkadapertreiber `e1000g0` hinzugefügt werden.

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

Dieser Befehl weist dem virtuellen Switch automatisch eine MAC-Adresse zu. Sie können Ihre eigene MAC-Adresse als Option zum Befehl `ldm add-vsw` angeben. In diesem Fall müssen Sie jedoch auch sicherstellen, dass die festgelegte MAC-Adresse nicht mit einer bereits vorhandenen MAC-Adresse in Konflikt steht.

Ersetzt der hinzugefügte virtuelle Switch den darunter liegenden physikalischen Adapter als primäre Netzwerkschnittstelle, muss ihm die MAC-Adresse des physikalischen Adapters zugewiesen werden, so dass der Dynamic Host Configuration Protocol (DHCP)-Server der Domain dieselbe IP-Adresse zuweist. Siehe „[Aktivierung des Netzwerkbetriebs zwischen der Steuer-/Servicedomain und anderen Domains](#)“ auf Seite 46.

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

4. Überprüfen Sie, dass die Dienste unter Verwendung des Unterbefehls `list-services` erzeugt wurden. Ihr Ergebnis sollte in etwa wie das folgende aussehen.

```
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

Erstkonfiguration der Steuerdomain

Zunächst werden alle Systemressourcen der Steuerdomain zugewiesen. Um die Erzeugung anderer Logical Domains zu ermöglichen, müssen Sie einige dieser Ressourcen freigeben.

Hinweis – Die Meldungen, die der LDom Manager im Konfigurationsmodus in den folgenden Beispielen ausgibt, gelten nur für Sun UltraSPARC T1-Prozessoren.

▼ So richten Sie die Steuerdomain ein

Hinweis – Dieser Vorgang enthält Beispiele von Ressourcen, die für Ihre Steuerdomain eingerichtet werden können. Die Zahlen sind reine Beispiele und die verwendeten Werte gelten unter Umständen nicht für Ihre Steuerdomain.

1. Weisen Sie der Steuerdomain Kryptographieressourcen zu.

Hinweis – Wenn Sie in der Steuerdomain Kryptographiegeräte haben, können Sie die CPU nicht dynamisch rekonfigurieren. Wenn Sie also keine Kryptographiegeräte haben, stellen Sie `set-mau` auf 0.

In dem folgenden Beispiel würde der Steuerdomain `primary` eine Kryptographieressource zugewiesen werden. Hiermit würden die restlichen Kryptographieressourcen einer Gastdomain weiterhin zur Verfügung stehen.

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

2. Weisen Sie der Steuerdomain virtuelle CPUs zu.

Beispielsweise würde der folgende Befehl der Steuerdomain `primary` 4 virtuelle CPUs zuweisen. Hiermit würden die restlichen virtuellen CPUs einer Gastdomain weiter zur Verfügung stehen.

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

3. Weisen Sie der Steuerdomain Speicher zu.

Beispielsweise würde der folgende Befehl der Steuerdomain `primary` 1 GB Speicher zuweisen. Hiermit würde der restliche Speicher einer Gastdomain weiterhin zur Verfügung stehen.

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

Hinweis – Wenn Sie zur Bereitstellung von Plattendiensten das ZFS nicht nutzen, sollte 1 GB Speicher ausreichen. Wenn Sie für die Bereitstellung von Plattendiensten das ZFS nutzen, weisen Sie einen kompletten Kern aus 4 virtuellen CPUs und mindestens 4 GB Speicher zu. Für stärkere E/A-Belastungen kann es sein, dass Sie weitere komplette Kerne zuweisen müssen.

4. Fügen Sie dem Systemcontroller (SC) eine Logical Domain-Maschinenkonfiguration hinzu.

Beispielsweise würde der folgende Befehl eine Konfiguration mit der Bezeichnung `initial` hinzufügen.

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

Hinweis – Derzeit ist die Anzahl der auf dem SC speicherbaren Konfigurationen, die Konfiguration `factory-default` nicht mitgezählt, auf 8 beschränkt.

5. Überprüfen Sie, dass die Konfiguration beim nächsten Neustart genutzt werden kann.

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

Dieser Listen-Unterbefehl zeigt, dass der Konfigurationssatz `factory-default` momentan verwendet wird und dass der Konfigurationssatz `initial` nach dem nächsten Neustart verwendet wird.

Neustart zur Verwendung von Logical Domains

Sie müssen Ihre Steuer-/Servicedomain neu starten, damit die Konfigurationsänderungen wirksam werden und die Ressourcen zur Verwendung durch andere Logical Domains freigegeben werden.

▼ So führen Sie einen Neustart zur Verwendung von Logical Domains durch

- Fahren Sie die `primary`-Domain herunter, die in unserem Beispiel auch die Servicedomain ist.

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

Hinweis – Mit dem angegebenen Befehl können die vorgenommenen Änderungen während des Neustarts wirksam werden, und mit dem Befehl `ldm list-config` wird noch dasselbe Ergebnis wie vor dem Neustart angezeigt. Damit der Befehl `ldm list-config` die angezeigte Konfiguration aktualisieren kann, sind ein Herunterfahren und Neustart erforderlich.

Aktivierung des Netzwerkbetriebs zwischen der Steuer-/Servicedomain und anderen Domains

Standardmäßig ist der Netzwerkbetrieb zwischen Steuer-/Servicedomain und anderen Domains im System deaktiviert. Um ihn zu aktivieren, sollte das virtuelle Switchgerät als Netzwerkgerät konfiguriert werden. Der virtuelle Switch kann entweder das darunter liegende physikalische Gerät (in diesem Beispiel `e1000g0`) als primäre Schnittstelle ersetzen oder als zusätzliche Netzwerkschnittstelle in der Domain konfiguriert werden.

Hinweis – Führen Sie folgende Konfigurationsschritte von der Domain-Konsole aus durch, da der Vorgang die Netzwerkverbindung zur Domain zeitweise unterbrechen könnte.

▼ So konfigurieren Sie den virtuellen Switch als primäre Schnittstelle

1. Drucken Sie die Adressierungsinformationen für alle Schnittstellen aus.

```
primary# ifconfig -a
```

2. Schließen Sie den virtuellen Switch an. In diesem Beispiel ist der zu konfigurierende virtuelle Switch `vsw0`.

```
primary# ifconfig vsw0 plumb
```

3. (Optional) Um die Liste aller Instanzen des virtuellen Switch in der Domain zu erhalten, können Sie diese auflisten.

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

4. Trennen Sie das physikalische Netzwerkgerät (`net-dev`) ab, das dem virtuellen Switch, in diesem Beispiel `e1000g0`, zugewiesen ist.

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

5. Um Eigenschaften des physikalischen Netzwerkgeräts (`e1000g0`) zum virtuellen Switch (`vsw0`) zu migrieren, gehen Sie wie folgt vor:

- Ist der Netzwerkbetrieb auf eine statische IP-Adresse konfiguriert, verwenden Sie die IP-Adresse und Netzmaske von `e1000g0` erneut für `vsw0`.

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

- Ist der Netzwerkbetrieb auf DHCP konfiguriert, aktivieren Sie DHCP für `vsw0`.

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

6. Nehmen Sie die erforderlichen Modifikationen an der Konfigurationsdatei vor, um diese Änderung festzuschreiben.

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

Hinweis – Bei Bedarf können Sie auch den virtuellen Switch sowie das physikalische Netzwerkgerät konfigurieren. Schließen Sie in diesem Fall den virtuellen Switch wie in Schritt 2 an und trennen Sie das physikalische Gerät nicht ab (überspringen Sie Schritt 4). Der virtuelle Switch muss anschließend entweder mit einer statischen IP-Adresse konfiguriert werden oder von einem DHCP-Server eine dynamische IP-Adresse erhalten.

Aktivierung des virtuellen Netzwerk-Terminalserver-Daemons

Um Zugriff auf die virtuelle Konsole jeder Logical Domain zu erhalten, müssen Sie den virtuellen Netzwerk-Terminalserver-Daemon (`vntsd`) aktivieren. Weitere Informationen über die Verwendung dieses Daemons finden Sie in der Sammlung des Solaris 10 OS Referenzhandbuchs oder auf der `vntsd (1M)` man-Seite.

▼ So aktivieren Sie den virtuellen Netzwerk-Terminalserver-Daemon

Hinweis – Kontrollieren Sie, dass Sie auf der Steuerdomain den Standarddienst `vconscon` erzeugt haben, bevor Sie `vntsd` aktivieren. Weitere Informationen finden Sie unter „[Erzeugen von Standarddiensten](#)“ auf Seite 42.

1. Um den virtuellen Netzwerk-Terminalserver-Daemon `vntsd (1M)` zu aktivieren, verwenden Sie den Befehl `svcadm (1M)`.

```
# svcadm enable vntsd
```


2. Um zu überprüfen, ob `vntsd` aktiviert ist, verwenden Sie den Befehl `svcs` (1).

```
# 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)
```

Erzeugen und Starten einer Gastdomain

Auf der Gastdomain muss ein Betriebssystem laufen, das sowohl die `sun4v`-Plattform als auch die vom Hypervisor präsentierten virtuellen Geräte versteht. Derzeit ist dies mindestens das Betriebssystem Solaris 10 11/06. Nähere Informationen zu konkreten Patches, die eventuell erforderlich sind, finden Sie in den *Versionshinweisen zu Logical Domains (LDDoms) 1.0.2*. Wenn Sie Standarddienste erzeugt und Ressourcen von der Steuerdomain neu zugewiesen haben, können Sie eine Gastdomain erzeugen und starten.

▼ So erzeugen und starten Sie eine Gastdomain

1. Erzeugen Sie eine Logical Domain.

Beispielsweise würde der folgende Befehl eine Gastdomain mit dem Namen `ldg1` erzeugen.

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

2. Fügen Sie der Gastdomain CPUs hinzu.

Beispielsweise würde der folgende Befehl der Gastdomain `ldg1` vier virtuelle CPUs hinzufügen.

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

3. Fügen Sie der Gastdomain Speicher hinzu.

Beispielsweise würde der folgende Befehl der Gastdomain `ldg1` 512 MB Speicher hinzufügen.

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

4. Fügen Sie der Gastdomain ein virtuelles Netzwerkgerät hinzu.

Beispielsweise würde der folgende Befehl der Gastdomain `ldg1` ein virtuelles Netzwerkgerät mit diesen Informationen hinzufügen.

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

Wobei:

- `vnet1` der eindeutige Name einer Schnittstelle zur Logical Domain ist, die der Instanz dieses virtuellen Netzwerkgeräts auf nachfolgende Unterbefehle `set-vnet` bzw. `remove-vnet` hin zugewiesen werden.
- `primary-vsw0` der Name eines vorhandenen Netzwerkdienstes (virtueller Switch) ist, zu dem eine Verbindung hergestellt werden soll.

5. Legen Sie das Gerät fest, das vom virtuellen Plattenserver als virtuelle Platte für die Gastdomain exportiert werden soll.

Sie können eine physikalische Platte, ein Plattensegment, Volumes oder eine Datei als Blockgerät exportieren. Der Export von Loopback (`lofi`)-Geräten als Blockgeräte wird in dieser Version der Logical Domains-Software nicht unterstützt. Das folgende Beispiel zeigt eine physikalische Platte und eine Datei.

- **Beispiel einer physikalischen Platte.** Im ersten Beispiel wird eine physikalische Platte mit diesen Informationen hinzugefügt.

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

Wobei:

- `/dev/dsk/c0t0d0s2` der Pfadname des aktuellen physikalischen Geräts ist. Beim Hinzufügen eines Geräts muss der Pfadname mit dem Gerätenamen gepaart werden.
- `vol1` ein eindeutiger Name ist, den Sie für das Gerät festlegen müssen, das dem virtuellen Plattenserver hinzugefügt wird. Der Gerätenamen muss für die Instanz dieses virtuellen Plattenservers eindeutig sein, da dieser Name von diesem virtuellen Plattenserver zu den Clients exportiert wird, die ihn dann hinzufügen. Beim Hinzufügen eines Geräts muss der Gerätenamen mit dem Pfadnamen des aktuellen Geräts gepaart werden.
- `primary-vds0` der Name des virtuellen Plattenservers ist, dem dieses Gerät hinzugefügt wird.

- **Beispiel einer Datei:** In diesem zweiten Beispiel wird eine Datei als Blockgerät exportiert.

```
primary$ ldm add-vdsdev Pfad-zur-Datei/Dateiname vol1@primary-vds0
```

Wobei:

- *Pfad-zur-Datei/Dateiname* der Pfadname der aktuellen, als Blockgerät exportierten Datei ist. Beim Hinzufügen eines Geräts muss der Pfadname mit dem Gerätenamen gepaart werden.
- **vol1** ein eindeutiger Name ist, den Sie für das Gerät festlegen müssen, das dem virtuellen Plattenserver hinzugefügt wird. Der Gerätenamen muss für die Instanz dieses virtuellen Plattenservers eindeutig sein, da dieser Name von diesem virtuellen Plattenserver zu den Clients exportiert wird, die ihn dann hinzufügen. Beim Hinzufügen eines Geräts muss der Gerätenamen mit dem Pfadnamen des aktuellen Geräts gepaart werden.
- **primary-vds0** der Name des virtuellen Plattenservers ist, dem dieses Gerät hinzugefügt wird.

6. Fügen Sie der Gastdomain eine virtuelle Platte hinzu.

Im folgenden Beispiel wird der Gastdomain **ldg1** eine virtuelle Platte hinzugefügt.

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

Wobei:

- **vdisk1** der Name der virtuellen Platte ist.
- **vol1** der Name des vorhandenen Geräts des virtuellen Plattenservers ist, zu dem eine Verbindung hergestellt werden soll.
- **primary-vds0** der Name des vorhandenen virtuellen Plattenservers ist, zu dem eine Verbindung hergestellt werden soll.

Hinweis – Virtuelle Platten sind allgemeine Blockgeräte, die durch verschiedene Arten physikalischer Geräte, Volumen oder Dateien abgesichert sind. Eine virtuelle Platte ist jedoch nicht bedeutungsgleich mit einer SCSI-Platte und schließt daher die Ziel-ID in der Plattenbezeichnung aus. Virtuelle Platten in einer Logical Domain haben folgendes Format: *cNdNsN*, wobei *cN* der virtuelle Controller, *dN* die Nummer der virtuellen Platte und *sN* das Segment ist.

7. Setzen Sie die Variablen auto-boot und boot-device für die Gastdomain.

Der erste Beispielbefehl setzt auto-boot\? für die Gastdomain ldg1 auf true.

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

Der zweite Beispielbefehl setzt boot-device für die Gastdomain ldg1 auf vdisk.

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

8. Binden Sie Ressourcen an die Gastdomain ldg1 und listen Sie dann die Domain, um ihre Bindung zu kontrollieren.

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

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

9. Um den Konsolenanschluss der Gastdomain zu finden, können sie sich die Ausgabe des o. a. Unterbefehls list-domain ansehen.

In der Spalte Cons sehen Sie, dass die Konsolenausgabe der Logical Domain guest 1 (ldg1) an Port 5001 gebunden ist.

10. Starten Sie die Gastdomain ldg1.

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

11. Stellen Sie die Verbindung zur Konsole einer Gastdomain her. Hierfür gibt es mehrere Möglichkeiten.

- Sie können sich bei der Steuerdomain anmelden und die Verbindung zum Konsolenanschluss direkt am Local Host herstellen:

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

- Sie können die Verbindung jedoch auch über ein Netzwerk herstellen, wenn es im SMF-Manifest vntsd(1M) aktiviert ist. Beispiel:

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

Ein Dienstprogramm für die Dienstverwaltung (SMF-Manifest) ist eine XML-Datei, die den Dienst beschreibt. Nähere Informationen über das Erstellen eines SMF-Manifests finden Sie in der Solaris 10-Sammlung für Systemadministratoren.

Hinweis – Um über die Konsole in einer Gastdomain auf ein nichtenglisches OS zugreifen zu können, muss die Sprache des Konsolenterminals dem vom OS erforderlichen Standardgebietsschema entsprechen.

Jumpstarten einer Gastdomain

Um eine Gastdomain zu jumpstarten, verwendet man in der Regel eine normale JumpStart-Routine mit folgenden Profilsyntaxänderungen an einer normalen Solaris OS-JumpStart-Routine, die speziell für LDoms angepasst wurden, wie in den folgenden zwei Beispielen dargestellt ist.

Normales JumpStart-Profil

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

Die Bezeichnungen virtueller Plattengeräte in einer Logical Domain unterscheiden sich von denen physikalischer Plattengeräte dahingehend, dass sie keine Ziel-ID (tN) im Gerätenamen aufweisen. Anstelle des normalen Formats $cNtNdNsN$ haben die Bezeichnungen virtueller Plattengeräte das Format $cNdNsN$, wobei cN der virtuelle Controller, dN die Nummer der virtuellen Platte und sN das Segment ist. Verändern Sie Ihr JumpStart-Profil wie im folgenden Profilbeispiel entsprechend.

Aktuelles Profil, dass für eine Logical Domain verwendet wird

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


Weitere Informationen und Aufgaben

Dieses Kapitel enthält Informationen und Aufgaben in Verbindung mit der Nutzung der Logical Domains-Software, die nicht in den vorigen Kapiteln erläutert wurden.

Einschränkungen bei der Eingabe von Namen am CLI

In den folgenden Abschnitten werden die Einschränkungen beschrieben, die für die Eingabe von Namen am CLI des Logical Domains Managers bestehen.

Dateinamen (*file*) und Variablennamen (*var_name*)

- Das erste Zeichen muss ein Buchstabe, eine Zahl oder ein Schrägstrich (/) sein.
- Anschließend können Buchstaben, Zahlen oder Interpunktionszeichen folgen.

Namen virtueller Plattenserver *file | device* und virtueller Switchgeräte.

- Muss Buchstaben, Zahlen oder Interpunktionszeichen enthalten.

Konfigurationsname (*config_name*)

Der Konfigurationsname der Logical Domain (*config_name*), die Sie einer auf dem Systemcontroller gespeicherten Konfiguration zuweisen, darf nicht mehr als 64 Zeichen haben.

Alle anderen Namen

Die restlichen Namen, wie der Name der Logical Domain (*ldom*), Namen von Diensten (*vswitch_name*, *service_name*, *vdpcs_service_name* und *vcc_name*), Namen virtueller Netzwerke (*if_name*) oder Namen virtueller Platten (*disk_name*) müssen folgendes Format haben:

- Das erste Zeichen muss ein Buchstabe oder eine Zahl sein.
- Anschließend können Buchstaben, Zahlen oder eines des folgenden Zeichen folgen: `'-_+#.::~~()'`

Verwenden der `ldm list`-Unterbefehle

In diesem Abschnitt erfahren Sie mehr über die Verwendung der Syntax für `ldm`-Unterbefehle, die Definition einiger Ausgabebedingungen wie Flags und Nutzungsstatistiken, und Sie finden einige Ausgabebeispiele.

Maschinenlesbare Ausgabe

Verwenden Sie für die Erstellung von Scripts, bei denen die Befehlsausgabe `ldm list` verwendet wird, *immer* die Option `-p`, um die Ausgabe in maschinenlesbare Form zu bringen. Weitere Informationen finden Sie unter „[So erzeugen Sie eine syntaktisch analysierbare, maschinenlesbare Liste \(-p\)](#)“ auf Seite 65.

▼ So zeigen Sie die Syntax für ldm-Unterbefehle an

- Um sich die Syntax aller ldm-Unterbefehle anzusehen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-1 Syntax für alle ldm-Unterbefehle

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

CODEBEISPIEL 5-1 Syntax für alle ldm-Unterbefehle (Fortsetzung)

```
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 <vdppcc_name> <service_name> <ldom>
    remove-vdpcc [-f] <vdppcc_name> <ldom>

vdpcs         ( ndpsldcs )
    add-vdpcs <vdppcs_name> <ldom>
    remove-vdpcs [-f] <vdppcs_name>

vdiskserverdevice ( vdsdev )
```

CODEBEISPIEL 5-1 Syntax für alle ldm-Unterbefehle (Fortsetzung)

```
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
```

Flag-Definitionen

In der Ausgabe für eine Domain können folgende Flags angezeigt werden:

- Platzhalter
- c Steuerdomain
- d Verzögerte Neukonfiguration
- n normal

s	Start oder Stopp
t	Übergang
v	Virtuelle E/A-Domain

Wenn Sie für den Befehl die lange (-l)-Option verwenden, werden die Flags ausgeschreiben. Falls nicht, sehen Sie nur die Abkürzungsbuchstaben.

Die Werte der Flag-Auflistung sind positionsabhängig. Nachfolgend sind von links nach rechts die Werte angeführt, die in jeder der fünf Spalten erscheinen können:

Spalte 1	Spalte 2	Spalte 3	Spalte 4	Spalte 5
s oder -	n oder t	d oder -	c oder -	v oder -

Definition einer Nutzungsstatistik

Die Nutzungsstatistik nach virtuellen CPU (UTIL) wird mit der langen Option (-l) des Befehls `ldm list` angezeigt. Die Statistik entspricht der prozentualen Zeitdauer seit der Anzeige der letzten Statistik, die die virtuelle CPU benötigt hat, um für das Gastbetriebssystem Befehle auszuführen. Es wird immer davon ausgegangen, dass eine virtuelle CPU für ein Gastbetriebssystem Befehle ausführt, es sei denn, es wurde an den Hypervisor geliefert. Liefert das Gastbetriebssystem keine virtuellen CPU an den Hypervisor, wird die CPU-Nutzung im Gastbetriebssystem immer als 100 % angezeigt.

Die für eine Logical Domain ausgegebene Nutzungsstatistik ist der Mittelwert der Nutzungen virtueller CPU für die virtuellen CPU in der Domain.

Beispiele verschiedener Listen

▼ So zeigen Sie Softwareversionen an (-V)

- Um die aktuell installierten Softwareversionen in einer Liste wie der folgenden anzuzeigen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-2 Installierte Softwareversionen

```
primary$ ldm -v

Logical Domain Manager (v 1.0.2)
Hypervisor control protocol v 1.0
```

CODEBEISPIEL 5-2 Installierte Softwareversionen (Fortsetzung)

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

▼ So erzeugen Sie eine kurze Liste

- Um eine kurze Liste aller Domains zu erzeugen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-3 Kurze Liste aller Domains

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

▼ So erzeugen Sie eine lange Liste (-l)

- Um eine lange Liste aller Domains zu erzeugen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-4 Lange Liste aller Domains

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			

CODEBEISPIEL 5-4 Lange Liste aller Domains (*Fortsetzung*)

vsw0	08:00:20:aa:bb:e0		e1000g0	switch@0	prog,promisc		
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					

▼ So erzeugen Sie eine erweiterte Liste (-e)

- Um eine erweiterte Liste aller Domains zu erzeugen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-5 Erweiterte Liste aller Domains

```
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                    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

VLDCC
```

CODEBEISPIEL 5-5 Erweiterte Liste aller Domains (Fortsetzung)

NAME			SERVICE			DESC		
hvctl1			primary@primary			hvctl1		
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			

▼ So erzeugen Sie eine syntaktisch analysierbare, maschinenlesbare Liste (-p)

- Um eine syntaktisch analysierbare, maschinenlesbare Liste aller Domains zu erzeugen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-6 Maschinenlesbare Ausgabe

```
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=
```

▼ So zeigen Sie den Status einer Domain an

- Um den Status einer Domain anzuzeigen (z. B. der Gastdomain ldg1), gehen Sie wie folgt vor:

CODEBEISPIEL 5-7 Domainstatus

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

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

▼ So listen Sie eine Variable

- Um eine Variable (z. B. boot-device) für eine Domain zu listen (z. B. für ldg1), gehen Sie wie folgt vor:

CODEBEISPIEL 5-8 Variablenliste für eine Domain

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

▼ So listen Sie Bindungen

- Um Ressourcen zu listen, die für eine Domain gebunden sind (z. B. ldg1), gehen Sie wie folgt vor:

CODEBEISPIEL 5-9 Bindungsliste für eine Domain

```
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

▼ So listen Sie Konfigurationen

- Um Logical Domain-Konfigurationen zu listen, die auf dem SC gespeichert sind, gehen Sie wie folgt vor:

CODEBEISPIEL 5-10 Konfigurationsliste

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

Bedeutung der Bezeichnungen

Die rechts vom Konfigurationsnamen angegebenen Bezeichnungen haben folgende Bedeutung:

- current - aktuell verwendete Konfiguration
- next - bei nächsten Neustart (Power Cycle) zu verwendende Konfiguration

▼ So listen Sie Geräte

- Um alle gebundenen und nicht gebundenen Server-Ressourcen zu listen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-11 Liste aller Server-Ressourcen

```
primary$ ldm list-devices -a
VCPU
  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
```

CODEBEISPIEL 5-11 Liste aller Server-Ressourcen (*Fortsetzung*)

18	100		
19	100		
20	100		
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

▼ So listen Sie Dienste

- Um die verfügbaren Dienste zu listen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-12 Dienstliste

```
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
```

Listen von Einschränkungen

Für den Logical Domains Manager sind Einschränkungen eine oder mehrere Ressourcen, die einer bestimmten Domain zugewiesen werden sollen. Je nach verfügbaren Ressourcen erhalten Sie entweder alle Ressourcen, deren Hinzufügung zu einer Domain Sie angefordert haben, oder Sie erhalten keine von diesen. Mit dem Unterbefehl `list-constraints` können Sie solche Ressourcen listen, deren Zuweisung zu der Domain Sie angefordert haben.

▼ So listen Sie Einschränkungen für eine Domain

- Um Einschränkungen für eine Domain (z. B. `ldg1`) zu listen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-13 Einschränkungsliste für eine Domain

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

VCPU
  COUNT
  1

MEMORY
  SIZE
  512M
```

CODEBEISPIEL 5-13 Einschränkungsliste für eine Domain (*Fortsetzung*)

NETWORK			
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		

▼ So listen Sie Einschränkungen im XML-Format

- Um Einschränkungen für eine bestimmte Domain (z. B. `ldg1`) im XML-Format zu listen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-14 Einschränkungen für eine Domain im XML-Format

```
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>
```

CODEBEISPIEL 5-14 Einschränkungen für eine Domain im XML-Format (Fortsetzung)

```
<vdisk_name>vdisk0</vdisk_name>
<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>
```

▼ So listen Sie Einschränkungen in einem maschinenlesbaren Format

- Um Einschränkungen für alle Domains in einem syntaktisch analysierbaren Format zu listen, gehen Sie wie folgt vor:

CODEBEISPIEL 5-15 Einschränkungen für alle Domains in einem maschinenlesbaren Format

```
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
|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

```

Bei dem Befehl `ldm stop-domain` kann es zu einer Zeitüberschreitung kommen, wenn die Domain an der Auslastungsgrenze läuft

Bei dem Befehl `ldm stop-domain` kann es zu einer Zeitüberschreitung kommen, bevor die Domain vollständig herunterfahren kann. Tritt dies ein, gibt der Logical Domains Manager eine Fehlermeldung wie die folgende aus:

```
LDom ldg8 stop notification failed
```

Die Domain könnte aber die Anforderung zum Herunterfahren immer noch verarbeiten. Verwenden Sie den Befehl `ldm list-domain`, um den Status der Domain zu überprüfen. Beispiel:

```
# ldm list-domain ldg8
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg8	active	s----	5000	22	3328M	0.3%	1d 14h 31m

Die vorstehende Liste zeigt die Domain als aktiv an, wobei jedoch das Flag `s` besagt, dass die Domain dabei ist zu stoppen. Dies sollte ein Übergangszustand sein.

Das folgende Beispiel zeigt, dass die Domain hier gestoppt hat:

```
# ldm list-domain ldg8
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
ldg8	bound	-----	5000	22	3328M		

Bestimmung des Namens der einem virtuellen Netzwerkgerät entsprechenden Solaris-Netzwerkschnittstelle

Es ist nicht möglich, den Namen einer Solaris-Netzwerkschnittstelle, die einem gegebenen virtuellen Gerät entspricht, direkt auf einem Gast anhand der Ausgabe über die `ldm list`-* Befehle zu bestimmen. Dies ist jedoch mit einer Kombination der Ausgabe des Befehls `ldm list -l` und der Einträge unter `/devices` auf dem Solaris OS-Gast möglich.

▼ So finden Sie den Namen der Solaris OS-Netzwerkschnittstelle

In diesem Beispiel enthält die Gastdomain `ldg1` zwei virtuelle Netzwerkgeräte, `net-a` und `net-c`, und wir möchten den Namen der Solaris OS-Netzwerkschnittstelle in `ldg1` finden, die `net-c` entspricht.

1. **Verwenden Sie den Befehl `ldm`, um die Instanz des virtuellen Netzwerkgeräts für `net-c` zu finden.**

```
# 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
...
#
```

Die Instanz des virtuellen Netzwerkgeräts für `net-c` lautet `network@2`.

2. Um die entsprechende Netzwerkschnittstelle auf `ldg1` zu finden, melden Sie sich bei `ldg1` an und suchen Sie den Eintrag für diese Instanz unter `/devices`.

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

Der Name der Netzwerkschnittstelle ist der Teil des Eintrags nach dem Doppelpunkt, d. h. `vnet1`.

3. Schließen Sie `vnet1` an, um zu sehen, dass sie die MAC-Adresse `00:14:4f:f8:dd:68` hat, wie sie in der Ausgabe `ldm list -l` für `net-c` in Schritt 1 erscheint.

```
# 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
#
```

Automatische oder manuelle Zuweisung von MAC-Adressen

Für die Logical Domains, virtuellen Switches und virtuellen Netzwerke, die Sie benutzen möchten, benötigen Sie eine entsprechende Anzahl an Media Access Control (MAC)-Adressen. Die Zuweisung von MAC-Adressen für eine Logical Domain, ein virtuelles Netzwerk (`vnet`) und einen virtuellen Switch (`vswitch`) können Sie dem Logical Domains Manager überlassen oder diese MAC-Adressen aus Ihrem eigenen Pool zugewiesener MAC-Adressen manuell zuweisen. Die `ldm`-Unterbefehle, mit denen MAC-Adressen festgelegt werden, sind `add-domain`, `add-vsw`, `set-vsw`, `add-vnet` und `set-vnet`. Wenn Sie in diesen Unterbefehlen keine MAC-Adresse angeben, weist der Logical Domains Manager automatisch eine solche zu.

Der Vorteil, dem Logical Domains Manager die Zuweisung von MAC-Adressen zu überlassen, liegt darin, dass er genau den MAC-Adressenblock nutzt, der zur Verwendung mit Logical Domains bestimmt ist. Zudem erkennt und verhindert der Logical Domains Manager die Kollision von MAC-Adressen mit Instanzen anderer Logical Domains Manager auf demselben Subnet. Damit entfällt für Sie die Aufgabe, Ihren Pool an MAC-Adressen selbst verwalten zu müssen.

Die Zuweisung von MAC-Adressen erfolgt, sobald eine Logical Domain erzeugt oder ein Netzwerkgerät in eine Domain konfiguriert wird. Zudem bleibt die Zuweisung so lange erhalten, bis das Gerät oder die Logical Domain selbst entfernt wird.

In diesem Abschnitt sollen folgende Themen diskutiert werden:

- „Bereich der MAC-Adressen, die der Logical Domains-Software zugewiesen werden“ auf Seite 75
- „Algorithmus für die automatische Zuweisung von MAC-Adressen“ auf Seite 75
- „Erkennung doppelter MAC-Adressen“ auf Seite 76
- „Freigegebene MAC-Adressen“ auf Seite 77
- „Manuelle Zuweisung von MAC-Adressen“ auf Seite 77

Bereich der MAC-Adressen, die der Logical Domains-Software zugewiesen werden

Logical Domains wurden dem folgenden 512 kB großen Block MAC-Adressen zugewiesen:

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

Die niedrigeren 256 kB Adressen werden vom Logical Domains Manager für die **automatische Zuweisung von MAC-Adressen** verwendet, wobei es *nicht* möglich ist, eine Adresse in diesem Bereich anzufordern:

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

Sie können die obere Hälfte dieses Bereichs für die **manuelle Zuweisung von MAC-Adressen** verwenden:

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

Algorithmus für die automatische Zuweisung von MAC-Adressen

Wird bei dem Erzeugen einer Logical Domain oder eines Netzwerkgeräts keine MAC-Adresse angegeben, ordnet und weist der Logical Domains Manager dieser Logical Domain oder dem Netzwerkgerät automatisch eine MAC-Adresse zu. Um diese MAC-Adresse zu erhalten, versucht der Logical Domains Manager mehrmals, eine Adresse auszuwählen und prüft diese auf mögliche Kollisionen.

Bevor er eine mögliche Adresse auswählt, prüft der Logical Domains Manager, ob er hierfür eine vor kurzem freigegebene, automatisch zugewiesene Adresse in einer Datenbank findet (siehe „[Freigegebene MAC-Adressen](#)“ auf Seite 77). Ist dies der Fall, wählt der Logical Domains Manager seine Kandidatenadresse aus der Datenbank.

Steht keine vor kurzem freigegebene Adresse zur Verfügung, wird die MAC-Adresse zufällig aus dem 256 k-Bereich an für diesen Zweck reservierten Adressen ausgewählt. Die Auswahl der MAC-Adresse erfolgt zufällig, um die Wahrscheinlichkeit zu verringern, dass eine doppelte MAC-Adresse als Kandidat ausgewählt wird.

Anschließend wird überprüft, ob die ausgewählte Adresse bereits bei anderen Logical Domains Managern auf anderen Systemen existiert, um zu verhindern, dass doppelte MAC-Adressen tatsächlich zugewiesen werden. Eine Beschreibung des verwendeten Algorithmus findet sich unter „[Erkennung doppelter MAC-Adressen](#)“ auf Seite 76. Liegt bereits eine Zuweisung für diese Adresse vor, wiederholt der Logical Domains Manager den Vorgang und wählt eine andere Adresse, die er dann wiederum auf Kollisionen überprüft. Dies geschieht, bis eine noch nicht bereits zugeordnete MAC-Adresse gefunden wird oder ein Zeitlimit von 30 s abgelaufen ist. Wird das Zeitlimit erreicht, schlägt die Erzeugung des Geräts fehl, und es wird eine Fehlermeldung wie die folgende angezeigt:

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

Erkennung doppelter MAC-Adressen

Um zu verhindern, dass dieselbe MAC-Adresse verschiedenen Geräten zugeordnet wird, nimmt ein Logical Domains Manager Verbindung zu anderen Logical Domains Managern in anderen Systemen auf und schickt über die Standardnetzwerkschnittstelle der Domain eine Multicastmeldung mit der Adresse, die er dem Gerät zuweisen möchte. Er wartet dann eine Sekunde auf Rückmeldungen. Ist diese MAC-Adresse bereits einem anderen Gerät auf einem anderen LDoms-aktivierten System zugewiesen, schickt der Logical Domains Manager in diesem System eine Rückmeldung, die die betreffende MAC-Adresse enthält. Erhält der abfragende Logical Domains Manager eine Rückmeldung, weiß er, dass die gewählte MAC-Adresse bereits vergeben ist, wählt eine andere und fängt von vorne an.

Standardmäßig werden diese Multicastmeldungen nur an andere Manager auf demselben Subnetz geschickt; die Gültigkeitsdauer (time-to-live, TTL) ist 1. Die TTL lässt sich mit Hilfe der Service Management Facilities (SMF)-Eigenschaft `ldmd/hops` konfigurieren.

Jeder Logical Domains Manager hat folgende Aufgaben:

- Empfang von Multicastmeldungen
- Beobachtung der seinen Domains zugewiesenen MAC-Adressen
- Suche nach Duplikaten
- Rückmeldung, so dass keine Duplikate entstehen

Ist der Logical Domains Manager in einem System aus irgendeinem Grund abgeschaltet, können während dieser Zeit doppelte MAC-Adressen entstehen.

Die automatisch MAC-Zuweisung erfolgt zu dem Zeitpunkt, da die Logical Domain oder das Netzwerkgerät erzeugt wird, und hält an, bis das Gerät oder die Logical Domain entfernt wird.

Freigegebene MAC-Adressen

Wird eine Logical Domain oder ein Gerät entfernt, mit der bzw. mit dem eine automatisch erzeugte MAC-Adresse verbunden ist, wird diese MAC-Adresse in einer Datenbank vor kurzem freigegebener MAC-Adressen gespeichert, um möglicherweise später auf diesem System erneut verwendet zu werden. Diese MAC-Adressen werden gespeichert, um zu verhindern, dass der Pool an Internet Protocol (IP)-Adressen eines Dynamic Host Configuration Protocol (DHCP)-Servers ausgeschöpft werden. Die Zuordnung von IP-Adressen durch DHCP-Server geschieht immer für eine begrenzte Dauer (die Leasedauer). Diese Leasedauer wird häufig längerfristig konfiguriert, in der Regel auf Stunden oder Tage. Werden Netzwerkgeräte schnell erzeugt und entfernt, ohne dass der Logical Domains Manager automatisch zugeordnete MAC-Adressen wieder verwendet, kann es vorkommen, dass die Anzahl zugeordneter MAC-Adressen einen typisch konfigurierten DHCP-Servers bald überlastet.

Ein Logical Domains Manager, der aufgefordert wird, automatisch eine MAC-Adresse für eine Logical Domain oder ein Netzwerkgerät zu beziehen, sucht zunächst in der Datenbank freigegebener MAC-Adressen, ob er eine zuvor zugewiesene MAC-Adresse wieder verwenden kann. Ist dies möglich, wird der Algorithmus zur Erkennung doppelter MAC-Adressen gestartet. Wurde die MAC-Adresse seit ihrer Freigabe niemandem zugewiesen, wird sie wieder verwendet und aus der Datenbank gelöscht. Wird eine Kollision festgestellt, wird die Adresse einfach aus der Datenbank gelöscht. Der Logical Domains Manager versucht es in diesem Fall mit der nächsten Adresse in der Datenbank oder wählt, falls keine verfügbar ist, zufällig eine neue MAC-Adresse aus.

Manuelle Zuweisung von MAC-Adressen

Im folgenden Vorgang erfahren Sie, wie Sie eine MAC-Adresse manuell erzeugen.

▼ So ordnen Sie eine MAC-Adresse manuell zu

1. Konvertieren Sie den Subnetzteil der IP-Adresse des physikalischen Hosts in das Hexadezimalsystem, und speichern Sie das Ergebnis.

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

27

2. Bestimmen Sie die Anzahl der vorhandenen Domains, ohne die Steuerdomain.

```
# /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

Es gibt eine Gastdomain, und Sie müssen die zu erzeugende Domain einrechnen, so dass sich 2 Domains ergeben.

3. Hängen Sie die konvertierte IP-Adresse (27) an den Vendor String (0x08020ab), gefolgt von 10 plus der Anzahl Logical Domains (hier 2), so dass sich 12 ergeben.

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

Zuordnung von CPU und Speicheradressen

Die Solaris Fault Management Architecture (FMA) meldet CPU-Fehler in Form der Nummern der physikalischen CPU und Speicherfehler in Form physikalischer Speicheradressen.

Wenn Sie feststellen möchten, innerhalb welcher Logical Domain ein Fehler aufgetreten ist, und die entsprechende Nummer der virtuellen CPU oder reale Speicheradresse wissen möchten, müssen Sie eine Zuordnung vornehmen.

CPU-Zuordnung

Die Domain und die Nummer der virtuellen CPU innerhalb der Domain, die der Nummer einer physikalischen CPU entspricht, lässt sich wie folgt ermitteln.

▼ So ermitteln Sie die CPU-Nummer

1. Erzeugen Sie eine lange, syntaktisch analysierbare Liste aller Domains.

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

2. Suchen Sie in den VCPU-Abschnitten der Liste nach dem Eintrag mit einem pid-Feld, das der Nummer der physikalischen CPU entspricht.
 - Wenn Sie einen solchen Eintrag finden, befindet sich die CPU in der Domain, unter der der Eintrag angeführt ist, und die Nummer der virtuellen CPU steht im Feld vid des Eintrags.
 - Wenn Sie keinen solchen Eintrag finden, befindet sich die CPU in keiner Domain.

Speicherzuordnung

Die Domain und die reale Speicheradresse in der Domain, die einer bestimmten physikalischen Speicheradresse (PA) entsprechen, lassen sich wie folgt ermitteln.

▼ So ermitteln Sie die reale Speicheradresse

1. Erzeugen Sie eine lange, syntaktisch analysierbare Liste aller Domains.

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

2. Suchen Sie in den MEMORY- Abschnitten der Liste nach der Zeile, in der die PA in den Inklusivbereich pa bis $(pa + size - 1)$ fällt: d. h. $pa \leq PA < (pa + size - 1)$. Hier beziehen sich pa und $size$ auf die Werte in den entsprechenden Feldern in der Zeile.
 - Wenn Sie einen solchen Eintrag finden, liegt die PA in der Domain, unter der der Eintrag angeführt ist, und es ergibt sich die entsprechende reale Adresse innerhalb der Domain aus $ra + (PA - pa)$.
 - Wenn Sie keinen solchen Eintrag finden, befindet sich die PA in keiner Domain.

Beispiele für CPU- und Speicherzuordnung

Nehmen wir als Beispiel eine Logical Domain-Konfiguration wie die im [CODEBEISPIEL 5-16](#) dargestellte, bei der Sie die Domain und die virtuelle CPU ermitteln möchten, die der physikalischen CPU-Nummer 5 entspricht, und die Domain und reale Adresse herausbekommen möchten, die der physikalischen Adresse 0x7e816000 entspricht.

Wenn Sie in den VCPU-Einträge der Liste einen Eintrag suchen, dessen `pid`-Feld gleich 5 ist, können Sie unter der Logical Domain `ldg1` folgenden Eintrag finden:

Daher liegt die Nummer der physikalischen CPU 5 in der Domain `ldg1` und hat innerhalb der Domain die virtuelle CPU-Nummer 1.

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

In den MEMORY-Einträgen der Liste finden Sie unter der Domain `ldg2` folgenden Eintrag:

ra=0x80000000 pa=0x78000000 size=1073741824

Wobei: $0x78000000 \leq 0x7e816000 \leq (0x78000000 + 1073741824 - 1)$, d. h. $pa \leq PA \leq (pa + size - 1)$.

Daher liegt die PA in der Domain `ldg2` und die entsprechende reale Adresse lautet $0x80000000 + (0x7e816000 - 0x78000000) = 0xe816000$.

CODEBEISPIEL 5-16 Lange, syntaktisch analysierbare Liste von Logical Domains-Konfigurationen

```
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=0x80000000|pa=0x80000000|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
|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
```

So wird der Split PCI-Express-Bus für die Nutzung mehrerer Logical Domains konfiguriert

Hinweis – Bei Sun UltraSPARC T-2-basierten Servern wie den Servern Sun SPARC Enterprise T5120 und T5220 würde man der Logical Domain eher eine Netzwerkschnittstellen-Einheit (NIU) zuweisen als wie folgt vorzugehen.

Der PCI-Express (PCI-E)-Bus auf einem Sun UltraSPARC T1-basierten Server weist zwei Anschlüsse auf, an die verschiedene Endknotengeräte angeschlossen sind. Diese lassen sich auf einem Server anhand der Namen `pci@780 (bus_a)` und `pci@7c0 (bus_b)` identifizieren. In einer Multidomain-Umgebung kann der PCI-E-Bus mit dem Logical Domains Manager darauf programmiert werden, jeden Endknoten einer separaten Domain zuzuweisen. So ist es dann möglich, mehr als eine Domain mit direktem Zugriff auf physikalische Geräte zu aktivieren, statt mit einer E/A-Virtualisierung zu arbeiten.

Beim Einschalten des Logical Domains-Systems verwendet die Steuerdomain (`primary`)-Domain alle Ressourcen der physikalischen Geräte, so dass die `primary`-Domain beide Endknoten des PCI-E-Busses besitzt.



Achtung – Alle internen Platten auf den unterstützten Servern werden an einem der Endknoten angeschlossen. Wird eine Steuerdomain von einer internen Platte gestartet, darf dieser Endknoten nicht von der Domain entfernt werden. Weiterhin muss sichergestellt werden, dass man nicht den Endknoten mit dem primären Netzwerkanschluss entfernt. Wenn Sie den falschen Endknoten von der Steuer- oder Servicedomain entfernen, könnte diese Domain nicht mehr auf benötigte Geräte zugreifen und wäre nicht mehr verwendbar. Liegt der primäre Netzwerkanschluss auf einem anderen Bus als die Systemplatte, muss das Netzkabel in einen Onboard-Netzwerkanschluss umgesteckt und der virtuelle Switch (`vsw`) mit dem Logical Domains Manager neu konfiguriert werden, so dass dieser Änderung Rechnung getragen wird.

▼ So wird eine Split-PCI-Konfiguration erzeugt

Das hier gezeigte Beispiel gilt für einen Sun Fire T2000-Server. Dieser Vorgang kann auch bei anderen Sun UltraSPARC T1-basierten Servern wie einem Sun Fire T1000-Server und einem Netra T2000-Server verwendet werden. Die Anweisungen für andere Server können sich von diesen zwar etwas unterscheiden, aber die grundlegenden Prinzipien lassen sich dem Beispiel durchaus entnehmen. Das Wichtigste ist, dass Sie den Endknoten mit der Boot-Platte behalten und den anderen Endknoten von der `primary`-Domain entfernen und ihn einer anderen Domain zuweisen müssen.

1. Überprüfen Sie, dass die `primary`-Domain beide Endknoten des PCI-Express-Busses besitzt.

```
primary# ldm list-bindings primary
...
IO
      DEVICE                PSEUDONYM          OPTIONS
```

```
pci@780          bus_a
pci@7c0          bus_b
...
```

2. Ermitteln Sie den Gerätepfad der Boot-Platte, die behalten werden muss.

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

3. Ermitteln Sie das physikalische Gerät, mit dem die Blockeinheit `c1t0d0s0` verlinkt ist.

```
primary# ls -l /dev/dsk/c1t0d0s0
lrwxrwxrwx  1 root    root          65 Feb  2 17:19 /dev/dsk/c1t0d0s0 -> ../
../devices/pci@7c0/pci@0/pci@1/pci@0,2/LSILogic,sas@2/sd@0,0:a
```

In diesem Beispiel liegt das physikalische Gerät für die Boot-Platte für die Domain `primary` unter dem Endknoten `pci@7c0`, was in unserer früheren Listung `bus_b` entspricht. Das heißt, dass wir `bus_a` (`pci@780`) auf dem PCI-Express-Bus einer anderen Domain zuweisen können.

4. Prüfen Sie `/etc/path_to_inst`, um den physikalischen Pfad der Onboard-Netzwerkanschlüsse zu finden.

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

5. Entfernen Sie den Endknoten, der nicht die Boot-Platte enthält (in diesem Beispiel `pci@780`), aus der `primary`-Domain.

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

6. Fügen Sie diese gesplittete PCI-Konfiguration (in diesem Beispiel `split-cfg`) dem Systemcontroller hinzu.

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

Weiterhin wird festgelegt, dass diese Konfiguration (`split-cfg`) nach dem nächsten Neustart verwendet werden soll.

Hinweis – Derzeit ist die Anzahl der auf dem SC speicherbaren Konfigurationen, die Konfiguration `factory-default` nicht mitgezählt, auf 8 beschränkt.

7. Starten Sie die `primary`-Domain neu, so dass die Änderung wirksam wird.

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

8. Fügen Sie den Endknoten (in diesem Beispiel `pci@780`) der Domain hinzu, die einen direkten Zugriff benötigt (in diesem Beispiel `ldg1`).

```
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.

Wenn Sie eine Infiniband-Karte haben, kann es sein, dass Sie den Umgehungsmodus auf dem Bus `pci@780` deaktivieren müssen. Informationen dazu, ob Sie den Umgehungsmodus aktivieren sollten, finden Sie unter „Aktivierung des Umgehungsmodus einer E/A-MMU auf einem PCI-Bus“ auf Seite 85.

9. Starten Sie die Domain `ldg1` neu, so dass die Änderung wirksam wird.

Alle Domains müssen für diesen Neustart deaktiviert werden. Wenn Sie diese Domain zum ersten Mal konfigurieren, ist die Domain noch deaktiviert.

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

10. Kontrollieren Sie, dass der korrekte Endknoten noch der `primary`-Domain zugewiesen ist und dass der korrekte Endknoten der Domain `ldg1` zugewiesen ist.

```
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	

...

Diese Ausgabe bestätigt, dass der PCI-E-Endknoten `bus_b` und die unter ihm angeführten Geräte der `primary`-Domain sowie `bus_a` und dessen Geräte `ldg1` zugewiesen wurden.

Aktivierung des Umgehungsmodus einer E/A-MMU auf einem PCI-Bus

Wenn Sie eine Infiniband Host Channel Adapter (HCA)-Karte haben, kann es sein, dass Sie den Umgehungsmodus der E/A-Speicherverwaltungseinheit (MMU) einschalten müssen. Standardmäßig steuert die Logical Domains-Software PCI-E-Transaktionen so, dass ein bestimmtes E/A-Gerät oder eine PCI-Express-Option nur auf den physikalischen Speicher zugreifen kann, der innerhalb der E/A-Domain zugewiesen wurde. Jeder Versuch, auf Speicher einer anderen Gastdomain zuzugreifen, wird von der E/A-MMU verhindert. Dies sorgt für eine höhere Sicherheit zwischen der E/A-Domain und allen anderen Domains. Sollte dennoch der seltene Fall eintreten, dass eine PCI-E- oder PCI-X-Optionskarte bei abgeschaltetem Umgehungsmodus der E/A-MMU nicht lädt oder funktioniert, können Sie mit dieser Option den E/A-MMU-Umgehungsmodus einschalten. Wenn Sie den Umgehungsmodus einschalten, besteht jedoch kein von der Hardware erzwungener Schutz gegen Speicherzugriffe aus der E/A-Domain.

Die Option `bypass=on` schaltet den Umgehungsmodus der E/A-MMU ein. Dieser Umgehungsmodus sollte nur aktiviert werden, wenn alle Gastdomains der betreffenden E/A-Domain und den E/A-Geräten innerhalb dieser E/A-Domain vertrauen. Dieses Beispiel zeigt, wie der Umgehungsmodus eingeschaltet wird.

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

Die Ausgabe zeigt unter `OPTIONS` `bypass=on`.

Verwenden von Konsolengruppen

Der virtuelle Netzwerk-Terminalserver-Daemon `vntsd` (1M) ermöglicht mehreren Domainkonsolen den Zugriff über einen einzigen TCP-Port. Zum Zeitpunkt der Domain-Erzeugung weist der Logical Domains Manager jeder Konsole einen eindeutigen TCP-Port zu, indem er für diese Domainkonsole eine neue Standardgruppe anlegt. Der TCP-Port wird dann der Konsolengruppe, nicht der Konsole selbst zugewiesen. Die Konsole kann mit Hilfe des Unterbefehls `set-vcons` an eine vorhandene Gruppe gebunden werden.

▼ So kombinieren Sie mehrere Konsolen in einer Gruppe

1. Binden Sie die Konsolen für die Domains in einer Gruppe.

Das folgende Beispiel zeigt, wie Sie die Konsole für drei verschiedene Domains (ldg1, ldg2, and ldg3) an dieselbe Konsolengruppe (group1) binden.

```
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. Verbinden Sie den assoziierten TCP-Port (in diesem Beispiel localhost am Port 5000).

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

Sie werden aufgefordert, eine der Domainkonsolen auszuwählen.

3. Listen Sie die Domains innerhalb der Gruppe, indem Sie 1 (list) wählen.

```
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
```

Hinweis – Um die Konsole einer anderen Gruppe oder der Instanz vcc neu zuweisen zu können, darf die Domain nicht verbunden sein, d. h. sie muss inaktiviert sein. Nähere Informationen über die Konfigurierung und Verwendung von SMF zur Verwaltung von vntsd und zur Verwendung von Konsolengruppen finden sich auf der Solaris 10 OS vntsd (1M)-Man Page.

Verschieben einer Logical Domain von einem Server auf einen anderen

Es ist möglich, eine nicht in Betrieb befindliche Logical Domain von einem Server auf einen anderen zu verlagern. Um diesen Ablauf zu vereinfachen, sollte vorher dieselbe Domain auf zwei Servern eingerichtet werden. Eigentlich muss die Domain

selbst nämlich nicht verschoben werden, es muss nur ihre Bindung auf einem Server aufgehoben und gestoppt werden, dann auf dem anderen Server neu hergestellt und gestartet werden.

▼ So richten Sie Domains ein, die verschoben werden sollen

1. Erzeugen Sie eine Domain mit demselben Namen auf zwei Servern, z. B. `domainA1` auf `serverA` und `serverB`.
2. Fügen Sie beiden Servern ein virtuelles Plattenservergerät und eine virtuelle Platte hinzu. Der virtuelle Plattenserver öffnet das darunter liegende Gerät als Bestandteil der Bindung für den Export.
3. Binden Sie die Domain nur auf einem Server, z. B. `serverA`. Lassen Sie die Domain auf dem anderen Server deaktiviert.

▼ So verschieben Sie die Domain

1. Heben Sie die Bindung der Domain auf `serverA` auf und stoppen sie.
2. Binden und starten Sie die Domain auf `serverB`.

Binden der Domain

Hinweis – Ressourcen werden erst benötigt, wenn die Domain gebunden ist.

Entfernen von Logical Domains

In diesem Abschnitt wird beschrieben, wie man alle Gastdomains entfernt und zu einer einzigen OS-Instanz umkehrt, die den gesamten Server steuert.

▼ So entfernen Sie alle Gast-Logical Domains

1. Listen Sie alle auf dem Systemcontroller vorhandenen Logical Domain-Konfigurationen.

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

2. Entfernen Sie alle Konfigurationen (*config_name*), die vorher auf dem Systemcontroller (SC) gespeichert wurden. Verwenden Sie für jede dieser Konfigurationen den folgenden Befehl.

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

Wenn Sie alle zuvor auf dem SC gespeicherten Konfigurationen gelöscht haben, wäre die beim nächsten Neustart der Steuerdomain (primary) zu verwendende Domain die mit der Bezeichnung *factory-default*.

3. Stoppen Sie alle Gastdomains mit der Option *-a*.

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

4. Listen Sie alle Domains, um alle an Gastdomains gebundenen Ressourcen zu sehen.

```
primary# ldm ls
```

5. Trennen Sie alle an Gastdomains gebundenen Ressourcen. Verwenden Sie hierfür für jede in Ihrem System konfigurierte Gastdomain (*ldom*) den Befehl `ldm unbind-domain`.

Hinweis – Es kann sein, dass Sie die Bindung einer E/A-Domain in einer Split-PCI-Konfiguration nicht aufheben können, wenn sie Dienste erbringt, die von der Steuerdomain benötigt werden. Überspringen Sie in diesem Fall diesen Schritt.

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

6. Stoppen Sie die Steuerdomain.

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


7. Starten Sie den Systemcontroller neu, so dass die Konfiguration `factory-default` geladen wird.

```
sc> poweroff  
sc> poweron
```

Betrieb des Solaris OS mit Logical Domains

In diesem Abschnitt werden die Verhaltensänderungen unter Solaris OS beschrieben, die auftreten, nachdem der Logical Domains Manager eine Instanz einer Konfiguration erzeugt hat, d. h. der Domainbetrieb aktiviert wurde.

Hinweis – Erörterungen dazu, ob der Domainbetrieb aktiviert ist oder nicht, beziehen sich auf Sun UltraSPARC T1-basierte Plattformen. Andernfalls ist der Domainbetrieb immer aktiviert.

OpenBoot-Firmware nach dem Starten von Solaris OS nicht verfügbar, wenn der Domainbetrieb aktiviert ist

Bei aktiviertem Domainbetrieb ist die OpenBoot-Firmware nicht verfügbar, nachdem Solaris OS gestartet wurde, da die Firmware aus dem Arbeitsspeicher entfernt wurde.

Um die OK-Eingabeaufforderung in Solaris OS zu erreichen, müssen Sie die Domain anhalten. Verwenden Sie den Solaris OS-Befehl `halt`, um die Domain anzuhalten.

Neustarten eines Servers

Bei Wartungsarbeiten, die Sie auf einem System durchführen, auf dem LDoms-Software läuft, und für die ein Neustart des Servers erforderlich ist, müssen Sie zuerst die aktuellen Logical Domain-Konfigurationen auf dem Systemcontroller speichern.

▼ So speichern Sie Ihre aktuellen Logical Domain-Konfigurationen auf dem Systemcontroller

- Verwenden Sie folgenden Befehl.

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

Ergebnis des OpenBoot-Befehls `power-off`

Durch den OpenBoot-Befehl™ `power-off` wird ein System *nicht* abgeschaltet. Zum Abschalten eines Systems mit laufender OpenBoot-Firmware ist der Befehl `poweroff` Ihres Systemcontrollers oder Systemprozessors zu verwenden. Der OpenBoot-Befehl `power-off` zeigt folgende Meldung:

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

Ergebnis von Unterbrechungen bei der Ausführung von Solaris OS

Ist der Domainbetrieb nicht aktiviert, springt Solaris OS normalerweise zur OpenBoot-Eingabeaufforderung, wenn eine Unterbrechungsanweisung ausgegeben wird. Das in diesem Abschnitt beschriebene Verhalten tritt in zwei Situationen auf:

1. Sie drücken die Tastensequenz „L1-A“, während das Eingabegerät auf `keyboard` gesetzt ist.
2. Sie geben den Befehl `send break` ein, während sich die virtuelle Konsole an der `telnet`-Eingabeaufforderung befindet.

Ist der Domainbetrieb aktiviert, erhalten Sie nach diesen Unterbrechungsarten die folgende Eingabeaufforderung.

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

Geben Sie den Buchstaben ein, der bezeichnet, wie das System nach dieser Art von Unterbrechung verfahren soll.

Ergebnisse des Anhaltens oder Neustartens der Steuerdomain

Die folgende Tabelle enthält Angaben zum erwarteten Verhalten beim Halten oder Neustarten der Steuerdomain (primary).

Hinweis – Die Frage in [TABELLE 5-1](#), ob der Domainbetrieb aktiviert ist, gilt nur bei Sun UltraSPARC T1-Prozessoren. Bei anderen Prozessoren ist der Domainbetrieb immer aktiviert.

TABELLE 5-1 Erwartetes Verhalten beim Halten oder Neustarten der Steuerdomain (primary)

Befehl	Domain-betrieb aktiviert?	Andere Domain konfiguriert?	Verhalten
halt	Deaktiviert	nicht anwendbar	Bei Sun UltraSPARC T1-Prozessoren: Bricht ab und kehrt zur ok-Eingabeaufforderung zurück.
	Aktiviert	Nein	Bei Sun UltraSPARC T1-Prozessoren: Siehe Meldung unter 02. Bei Sun UltraSPARC T2-Prozessoren: Host ausgeschaltet und bleibt aus, bis er am SC eingeschaltet wird.
	Aktiviert	Ja	Führt einen Warmstart durch und fährt hoch, wenn die Variable auto-boot?=true. Führt einen Warmstart durch und hält an der ok-Eingabeaufforderung, wenn die Variable auto-boot?=false.
reboot	Deaktiviert	nicht anwendbar	Bei Sun UltraSPARC T1-Prozessoren: Schaltet den Host aus und wieder ein.
	Aktiviert	Nein	Bei Sun UltraSPARC T1-Prozessoren: Schaltet den Host aus und wieder ein. Bei Sun UltraSPARC T2-Prozessoren: Startet den Host neu, keine Abschaltung.
	Aktiviert	Ja	Bei Sun UltraSPARC T1-Prozessoren: Schaltet den Host aus und wieder ein. Bei Sun UltraSPARC T2-Prozessoren: Startet den Host neu, keine Abschaltung.

TABELLE 5-1 Erwartetes Verhalten beim Halten oder Neustarten der Steuerdomain
(primary)
(Fortsetzung)

Befehl	Domain- betrieb aktiviert?	Andere Domain konfiguriert?	Verhalten
shutdown -i 5	Deaktiviert	nicht anwendbar	Bei Sun UltraSPARC T1-Prozessoren: Schaltet den Host aus.
	Aktiviert	Nein	Host ausgeschaltet und bleibt aus, bis er am SC eingeschaltet wird.
	Aktiviert	Ja	Führt Soft-Reset und Neustart aus.

Einige format (1M)-Befehlsoptionen funktionieren bei virtuellen Platten nicht

Der Befehl `format (1)` des Betriebssystems Solaris funktioniert nicht in Gastdomains, für die virtuelle Platten eingerichtet sind.

- Einige Unterbefehle wie `label`, `verify` oder `inquiry` funktionieren bei virtuellen Platten nicht.
- Beim Befehl `format (1M)` kann es sein, dass Meldungen wie die folgenden angezeigt werden:
 - `Inquiry failed`
 - `Disk unformatted`
 - `Current disk is unformatted`
 - `Drive type unknown`
- Der Befehl `format (1M)` stürzt ab, wenn Sie eine virtuelle Platte mit einer Extensible Firmware Interface (EFI)-Plattenbezeichnung auswählen.
- Beim Ausführen des Befehls `format (1M)` in einer Gastdomain werden alle virtuellen Platten als unformatiert betrachtet, auch wenn sie korrekt formatiert wurden und eine gültige Plattenbezeichnung aufweisen.

Zum Abrufen oder Einrichten des Volumeninhaltsverzeichnisses (VTOC) einer virtuellen Platte verwenden Sie anstelle des Befehls `format(1M)` die Befehle `prtvtoc(1M)` und `fmthard(1M)`. Sie können den Befehl `format (1M)` auch von der Servicedomain auf realen Platten aus verwenden.

Verwenden von LDoms mit ALOM CMT

Im folgenden Abschnitt finden Sie Informationen, die Sie bei Verwendung des Advanced Lights Out Manager (ALOM) chip multithreading (CMT) mit dem Logical Domains Manager kennen sollten. Weitere Informationen zur ALOM CMT-Software finden Sie im *Handbuch zum Advanced Lights Out Management (ALOM) CMT v1.3*.



Achtung – Die ALOM CMT-Dokumentation bezieht sich nur auf jeweils eine Domain, so dass Sie daran denken müssen, dass der Logical Domains Manager mehrere Domains einführt. Wird eine Logical Domain neu gestartet, kann es sein, dass die E/A-Dienste für Gastdomains erst zur Verfügung stehen, nachdem die Steuerdomain neu gestartet wurde. Dies liegt daran, dass die Steuerdomain in der Logical Domains Manager 1.0.2-Software als Servicedomain arbeitet. Gastdomains scheinen während des Neustarts einzufrieren. Nachdem die Steuerdomain vollständig neu gestartet wurde, nehmen die Gastdomains ihren normalen Betrieb wieder auf. Gastdomains müssen nur abgeschaltet werden, wenn der komplette Server abgeschaltet werden soll.

Für den vorhandenen ALOM CMT-Befehl steht eine weitere Option zur Verfügung.

<code>bootmode [normal reset_nvram bootscript=strong config="config-name"]</code>

Die Option `config="config-name"` ermöglicht Ihnen, die Konfiguration beim nächsten Einschalten auf eine andere Konfiguration umzustellen, z. B. auch auf die Werkskonfiguration `factory-default`.

Sie können den Befehl ausführen, wenn der Host ein- oder ausgeschaltet ist. Er wird wirksam, wenn der Host das nächste Mal zurückgesetzt oder eingeschaltet wird.

▼ So setzen Sie die Logical Domain-Konfiguration auf die Standard- oder eine andere Konfiguration zurück

- Setzen Sie mit diesem Befehl der ALOM CMT-Software die Logical Domain-Konfiguration beim nächsten Einschalten auf die standardmäßige Werkskonfiguration zurück.

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

Sie können weiterhin andere Konfigurationen auswählen, die mit dem Logical Domains Manager mit dem Befehl `ldm add-config` erstellt und auf dem Systemcontroller (SC) gespeichert wurden. Der im Befehl `ldm add-config` des Logical Domains Managers angegebene Name kann verwendet werden, um diese Konfiguration mit dem ALOM CMT-Befehl `bootmode` auszuwählen. Nehmen wir einmal an, Sie möchten die Konfiguration mit dem Namen `ldm-config1` speichern:

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

Nähere Informationen über den Befehl `ldm add-config` finden Sie auf der `ldm (1M)`-Man Page oder im *Logical Domains (LDoms) Manager 1.0.2 Man Page-Handbuch*.

Aktivieren und Verwenden der BSM-Auditing (Basic Security Modul)

Der Logical Domains Manager nutzt die Überwachungsfähigkeiten des Basic Security Modules (BSM) des Betriebssystems Solaris. BSM-Auditing bietet die Mittel, den Verlauf von Aktionen und Ereignissen auf Ihrer Steuerdomain zu überprüfen, um festzustellen, was geschehen ist. Der Verlauf wird in einem Protokoll festgehalten, das aussagt, was wann von wem und mit welchen Auswirkungen getan wurde.

Wenn Sie diese Überwachungsfähigkeit nutzen möchten, finden Sie in diesem Abschnitt Informationen, wie Überwachungsprotokolle aktiviert, überprüft, deaktiviert, gedruckt, ausgegeben und gedreht werden. Weitere Informationen über das BSM-Auditing finden Sie im *Handbuch für Systemadministratoren: Sicherheitsdienste* von Solaris 10.

Es gibt zwei Möglichkeiten, das BSM-Auditing zu aktivieren. Wenn Sie die Überwachung deaktivieren möchten, vergewissern Sie sich, dass Sie dasselbe Verfahren wie beim Aktivieren verwenden. Aktivieren Sie das BSM-Auditing

- mit Hilfe des Finish-Skripts `enable-bsm.fin` aus dem Solaris Security Toolkit.
Das Skript `enable-bsm.fin` wird vom `ldm_control-secure.driver` standardmäßig nicht verwendet. Sie müssen das Finish-Skript in Ihrem gewählten Treiber aktivieren.
- Verwenden des Solaris OS-Befehls `bsmconv(1M)`.

Hier finden Sie die Vorgänge für beide Verfahren.

▼ So verwenden Sie das Finish Script `enable-bsm.fin`

1. **Kopieren Sie den `ldm_control-secure.driver` zum `my-ldm.driver`, wobei `my-ldm.driver` der Name Ihrer Kopie des `ldm_control-secure.driver` ist.**
2. **Kopieren Sie den `ldm_control-config.driver` zum `my-ldm-config.driver`, wobei `my-ldm-config.driver` der Name Ihrer Kopie des `ldm_control-config.driver` ist.**
3. **Kopieren Sie den `ldm_control-hardening.driver` zum `my-ldm-hardening.driver`, wobei `my-ldm-hardening.driver` der Name Ihrer Kopie des `ldm_control-hardening.driver` ist.**
4. **Bearbeiten Sie `my-ldm.driver`, so dass er auf die neue Konfiguration und die Hardening-Treiber `my-ldm-control.driver` und `my-ldm-hardening.driver` verweist.**
5. **Bearbeiten Sie `my-ldm-hardening.driver` und entfernen Sie im Treiber das Pfundzeichen (#) am Anfang der folgenden Zeile.**

```
enable-bsm.fin
```

6. **Führen Sie `my-ldm.driver` aus.**

```
# /opt/SUNWjass/bin/jass-execute -d my-ldm.driver
```

7. **Starten Sie das Betriebssystem Solaris neu, damit die Änderungen der Überwachung wirksam werden.**

▼ So verwenden Sie den Solaris OS-Befehl `bsmconv(1M)`

1. Fügen Sie `vs` in der `flags:-Zeile` der Datei `/etc/security/audit_control` ein.
2. Führen Sie den Befehl `bsmconv(1M)` aus.

```
# /etc/security/bsmconv
```

Weitere Informationen über diesen Befehl finden Sie in der Solaris 10 Referenzhandbuchsammlung oder auf der Man Page.

3. Starten Sie das Betriebssystem Solaris neu, damit die Änderung der Überwachung wirksam wird.

▼ So überprüfen Sie, dass das BSM-Auditing aktiviert ist

1. Geben Sie folgenden Befehl ein.

```
# auditconfig -getcond
```

2. Überprüfen Sie, dass in der Ausgabe `audit condition = auditing` erscheint.

▼ So deaktivieren Sie die Überwachung

Es gibt zwei Möglichkeiten, die Überwachung zu deaktivieren, was davon abhängt, wie es aktiviert wurde. Siehe „[Aktivieren und Verwenden der BSM-Auditing \(Basic Security Modul\)](#)“ auf Seite 94.

1. Folgende Vorgehensweisen bieten sich an:
 - Widerrufen Sie die Hardening-Ausführung des Solaris Security Toolkits, mit der das BSM-Auditing aktiviert wurde.

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

- Verwenden Sie den Solaris OS-Befehl `bsmunconv(1M)`.

```
# /etc/security/bsmunconv
```


2. Starten Sie das Betriebssystem Solaris neu, damit die Deaktivierung der Überwachung wirksam wird.

▼ So drucken Sie eine Protokollausgabe

- Wählen Sie eine der folgenden Möglichkeiten, um die BSM-Protokollausgabe zu drucken.
 - Verwenden Sie die Solaris OS-Befehle `audireduce (1M)` und `praudit (1M)`, um die Protokollausgabe zu drucken. Beispiel:

```
# auditreduce -c vs | praudit
# auditreduce -c vs -a 20060502000000 | praudit
```

- Verwenden Sie den Solaris OS-Befehl `praudit -x`, um eine XML-Ausgabe zu drucken.

▼ So drehen Sie Überwachungsprotokolle

- Verwenden Sie den Solaris OS-Befehl `audit -n`, um Überwachungsprotokolle zu drehen.

Konfigurieren von virtuellen Switches und Servicedomains für NAT und Routing

Der virtuelle Switch (`vswitch`) ist ein Schicht-2-Switch, der in der Servicedomain auch als Netzwerkgerät verwendet werden kann. Der virtuelle Switch lässt sich so konfigurieren, dass er in verschiedenen Logical Domains nur als Switch zwischen virtuellen Netzwerk (`vnet`)-Geräten fungiert, jedoch keine Konnektivität über ein physikalisches Gerät zu einem Netzwerk außerhalb des Systems hat. In diesem Modus ermöglicht der Anschluss des `vswitch` als Netzwerkgerät und die Aktivierung des IP-Routings in der Servicedomain, dass virtuelle Netzwerke außerhalb des Systems unter Verwendung der Servicedomain als Router kommunizieren können. Dieser Betriebsmodus ist sehr wichtig, um die externe Konnektivität zu Domains herstellen zu können, wenn der physikalische Netzwerkadapter nicht GLDv3-konform ist.

Vorteile dieser Konfiguration:

- Der virtuelle Switch muss kein physikalisches Gerät direkt benutzen und kann externe Konnektivität bieten, auch wenn das zu Grunde liegende Gerät nicht GLDv3-konform ist.
- Die Konfiguration kann die IP-Routing- und Filterfähigkeiten des Betriebssystems Solaris nutzen.

▼ So richten Sie den virtuellen Switch für die Konnektivität zu externen Domains ein

1. **Erzeugen Sie einen virtuellen Switch, dem kein physikalisches Gerät zugeordnet ist.**

Achten Sie beim Zuweisen von Adressen darauf, dass der virtuelle Switch eine eindeutige MAC-Adresse hat.

```
primary# ldm add-vsw [mac-addr=xxxxxxxxxxxxxx] primary-vsw0 primary
```

2. **Schließen Sie den virtuellen Switch als Netzwerkgerät zusätzlich zum physikalischen Netzwerkgerät an, das von der Domain verwendet wird.**

Nähere Informationen über das Anschließen des virtuellen Switches finden Sie unter [„So konfigurieren Sie den virtuellen Switch als primäre Schnittstelle“](#) auf Seite 47.

3. **Konfigurieren Sie das virtuelle Switchgerät bei Bedarf für das DHCP.**

Nähere Informationen über die Konfiguration des virtuellen Switchgeräts für das DHCP finden Sie unter [„So konfigurieren Sie den virtuellen Switch als primäre Schnittstelle“](#) auf Seite 47.

4. **Erzeugen Sie bei Bedarf die Datei `/etc/dhcp.vsw`.**

5. **Konfigurieren Sie das IP-Routing in der Servicedomain und richten Sie die erforderlichen Routing-Tabellen in allen Domains ein.**

Weitere Informationen hierzu finden Sie im Abschnitt über „Paketweiterleitung und Routing auf IPv4-Netzwerken“ in Kapitel 5 „Konfiguration von TCP/IP-Netzwerkdiensten und IPv4-Verwaltung“ im *Handbuch für Systemadministratoren: IP-Dienste* der Solaris Express Systemadministrator-Sammlung.

Verwenden des ZFS mit virtuellen Platten

In diesem Abschnitt werden folgende Themen über die Verwendung des Zettabyte File System (ZFS) mit virtuellen Platten auf Logical Domains beschrieben:

- „Erzeugen einer virtuellen Platte als Schicht über einem ZFS-Volume“ auf Seite 99
- „Verwenden des ZFS über eine virtuelle Platte“ auf Seite 100
- „Verwenden des ZFS für Boot-Platten“ auf Seite 102

Erzeugen einer virtuellen Platte als Schicht über einem ZFS-Volume

Der folgende Vorgang beschreibt, wie Sie ein ZFS-Volume in einer Servicedomain erzeugen und dieses Volume anderen Domains als virtuelle Platte zur Verfügung stellen. In diesem Beispiel ist die Servicedomain identisch mit der Steuerdomain und heißt `primary`. Die Gastdomain heißt z. B. `ldg1`. Die Eingabeaufforderungen in jedem Schritt zeigen, in welcher Domain der Befehl ausgeführt werden soll.

▼ So erzeugen Sie eine virtuelle Platte als Schicht über einem ZFS-Volume

1. Erzeugen Sie einen ZFS-Speicherpool (`zpool`).

```
primary# zpool create -f tank1 c2t42d1
```

2. Erzeugen Sie ein ZFS-Volume.

```
primary# zfs create -V 100m tank1/myvol
```

3. Überprüfen Sie, dass der `zpool` (in diesem Beispiel `tank1`) und das ZFS-Volume (in diesem Beispiel `tank/myvol`) erzeugt wurden.

```
primary# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPOINT
tank1	100M	43.0G	24.5K	/tank1
tank1/myvol	22.5K	43.1G	22.5K	-

4. Konfigurieren Sie einen Dienst, der tank1/myvol als virtuelle Platte exportiert.

```
primary# ldm add-vdsdev /dev/zvol/rdisk/tank1/myvol zvol@primary-vds0
```

5. Fügen Sie die exportierte Platte einer anderen Domain (in diesem Beispiel ldg1) hinzu.

```
primary# ldm add-vdisk vdisk zvol@primary-vds0 ldg1
```

6. Starten Sie auf der anderen Domain (in diesem Beispiel ldg1) die Domain und achten Sie darauf, dass die neue virtuelle Platte sichtbar ist (Sie müssen hierfür eventuell den Befehl devfsadm ausführen).

In diesem Beispiel erscheint die neue Platte als /dev/rdsk/c2d2s0.

```
ldg1# newfs /dev/rdsk/c2d2s0
newfs: construct a new file system /dev/rdsk/c2d2s0: (y/n)? y
Warning: 4096 sector(s) in last cylinder unallocated
Warning: 4096 sector(s) in last cylinder unallocated
/dev/rdsk/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

Hinweis – Ein ZFS-Volume wird als virtuelles Plattensegment zu einer Logical Domain exportiert. Daher ist es nicht möglich, entweder den Befehl `format` zu verwenden oder das Betriebssystem Solaris auf einer zvol-gesicherten virtuellen Platte zu installieren.

Verwenden des ZFS über eine virtuelle Platte

Der folgende Vorgang zeigt, wie das ZFS direkt von einer Domain als Schicht über einer virtuellen Platte verwendet werden kann. Auf virtuellen Platten können Sie im Betriebssystem Solaris 10 mit den Befehlen `zpool(1M)` und `zfs(1M)` ZFS-Pools, Dateisysteme und Volumes erstellen. Obwohl das Speicher-Back-End ein anderes ist (virtuelle statt physikalische Platten), besteht bei der Verwendung des ZFS kein Unterschied.

Zusätzlich können Sie, wenn Sie bereits ein vorhandenes ZFS-Dateisystem haben, dieses von einer Servicedomain exportieren und in einer anderen Domain verwenden.

In diesem Beispiel ist die Servicedomain identisch mit der Steuerdomain und heißt `primary`. Die Gastdomain heißt z. B. `ldg1`. Die Eingabeaufforderungen in jedem Schritt zeigen, in welcher Domain der Befehl ausgeführt werden soll.

▼ So verwenden Sie ein ZFS über eine virtuelle Platte

1. Erstellen Sie einen ZFS-Pool (in diesem Fall `tank`) und überprüfen Sie anschließend, ob es erstellt wurde.

```
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. Erstellen Sie ein ZFS-Dateisystem (in diesem Fall `tank/test`) und überprüfen Sie anschließend, ob es erstellt wurde.

In diesem Beispiel wird das Dateisystem als Schicht über der Platte `c2t42d0` erstellt, indem auf der Servicedomain der folgende Befehl ausgeführt wird.

```
primary# zfs create tank/test
primary# zfs list
```

NAME	USED	AVAIL	REFER	MOUNTPPOINT
tank	106K	43.1G	25.5K	/tank
tank/test	24.5K	43.1G	24.5K	/tank/test

3. Exportieren Sie den ZFS-Pool (in diesem Fall `tank`).

```
primary# zpool export tank
```

4. Konfigurieren Sie einen Dienst, mit dem die physikalische Platte als virtuelle Platte `c2t42d0s2` exportiert wird.

```
primary# ldm add-vdsdev /dev/rdsk/c2t42d0s2 volz@primary-vds0
```

5. Fügen Sie die exportierte Platte einer anderen Domain (in diesem Beispiel `ldg1`) hinzu.

```
primary# ldm add-vdisk vdiskz volz@primary-vds0 ldg1
```

6. Starten Sie auf der anderen Domain (in diesem Beispiel `ldg1`) die Domain und achten Sie darauf, dass die neue virtuelle Platte sichtbar ist (Sie müssen hierfür eventuell den Befehl `devfsadm` ausführen).

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	

Der ZFS-Pool (in diesem Beispiel `tank/test`) ist nun importiert und kann von der Domain `ldg1` verwendet werden.

Verwenden des ZFS für Boot-Platten

In Logical Domains können Sie ein ZFS-Dateisystem mit einer größeren Datei als die virtuellen Platten verwenden.

Hinweis – Ein ZFS-Dateisystem benötigt mehr Speicher als die Servicedomain. Dies müssen Sie berücksichtigen, wenn Sie die Servicedomain konfigurieren.

Das ZFS aktiviert:

- das schnelle Klonen eines Dateisystems
- die Verwendung der Klone zur Bereitstellung zusätzlicher Domains
- die Netzinstallation auf Platte auf Dateien und Dateien innerhalb eines ZFS-Dateisystems

▼ So verwenden Sie ein ZFS für Boot-Platten

Sie können wie folgt vorgehen, um ZFS-Platten für Logical Domains zu erstellen und auch, um einen Schnappschuss von ihnen zu erstellen und sie für andere Domains zu klonen.

1. Reservieren Sie auf der `primary`-Domain eine komplette Platte oder ein komplettes Segment als Speicherplatz für den ZFS-Pool. In Schritt 2 wird Segment 5 einer Platte verwendet.
2. Erzeugen Sie einen ZFS-Pool, z. B. `ldomspool`.

```
# zpool create ldomspool /dev/dsk/c0t0d0s5
```

3. Erzeugen Sie ein ZFS-Dateisystem für die erste Domain (in diesem Beispiel `ldg1`).

```
# zfs create ldomspool/ldg1
```

4. Legen Sie für diese Domain eine Datei als Platte an.

```
# mkfile 1G /ldomspool/ldg1/bootdisk
```

5. Geben Sie die Datei als dasjenige Gerät an, das beim Erzeugen der Domain verwendet werden soll.

```
primary# ldm add-vdsdev /ldomspool/ldg1/bootdisk voll@primary-vds0
primary# ldm add-vdisk vdisk1 voll@primary-vds0 ldg1
```

6. Starten Sie die Domain `ldg1` und führen Sie eine Netzinstallation auf `vdisk1` durch. Diese Datei fungiert als komplette Platte und kann Partitionen aufweisen, d. h. separate Partitionen für `root`, `usr`, `home`, `dump` und `swap`.
7. Nach Abschluss der Installation fertigen Sie einen Schnappschuss des Dateisystems an.

```
# zfs snapshot ldomspool/ldg1@initial
```

Hinweis – Geschieht dies, bevor die Domain neu startet, werden weder der Domainstatus als Teil des Schnappschusses gespeichert, noch andere Klone, die von dem Schnappschuss erzeugt werden sollen.

8. Erzeugen Sie zusätzliche Klone aus dem Schnappschuss und verwenden Sie diese als Boot-Platte für andere Domains (in diesem Beispiel `ldg2` und `ldg3`).

```
# zfs clone ldomspool/ldg1@initial ldomspool/ldg2
# zfs clone ldomspool/ldg1@initial ldomspool/ldg3
```

9. Überprüfen Sie, dass alle Klone erfolgreich erzeugt wurden.

# 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

Hinweis – Kontrollieren Sie, dass der ZFS-Pool ausreichend Platz für die zu erstellenden Klone aufweist. ZFS arbeitet mit copy-on-write und nutzt Platz aus dem Pool nur, wenn die Blöcke im Klon geändert werden. Auch nach dem Starten der Domain verwenden die Klone nur einen geringen Teil des für die Platte benötigten Platzes (da die meisten der Binärdaten des Betriebssystems mit denen im ursprünglichen Schnappschuss identisch sind).

Verwenden von Volume-Managern in einer Logical Domains-Umgebung

In diesem Abschnitt sollen folgende Themen beschrieben werden:

- „Verwenden von virtuellen Platten als Schicht über einem Volume-Manager“ auf Seite 104
- „Verwenden eines Volume-Managers als Schicht über einer virtuellen Platte“ auf Seite 107

Verwenden von virtuellen Platten als Schicht über einem Volume-Manager

Jedes Volume aus einem Zettabyte File System (ZFS), Solaris™ Volume Manager (SVM) oder Veritas Volume Manager (VxVM) lässt sich von einer Servicedomain als virtuelle Platte in eine Gastdomain exportieren. Das exportierte Volume erscheint als virtuelle Platte mit einem Segment (s0) in der Gastdomain.

Hinweis – Im restlichen Teil dieses Abschnitts soll mit einem SVM-Volume als Beispiel gearbeitet werden. Die Diskussion gilt jedoch auch für ZFS- und VxVM-Volumes.

Exportiert eine Servicedomain beispielsweise das SVM-Volume `/dev/md/dsk/d0` zu `domain1`, und betrachtet `domain1` diese virtuellen Platten als `/dev/dsk/c0d2*`, verfügt nur `domain1` über ein `s0`-Gerät, nämlich `/dev/dsk/c0d2s0`.

Die virtuelle Platte in der Gastdomain (z. B. `/dev/dsk/c0d2s0`) ist direkt dem verbundenen Volume zugeordnet (z. B. `/dev/md/dsk/d0`), und die auf der virtuellen Platte von der Gastdomain aus gespeicherten Daten werden direkt auf dem verbundenen Volume ohne zusätzlichen Metadaten gespeichert. Auf die so auf der virtuellen Platte von der Gastdomain aus gespeicherten Daten kann auch direkt von der Servicedomain aus über das verbundene Volume zugegriffen werden.

Beispiele:

- Wird das SVM-Volume `d0` von der `primary`-Domain zu `domain1` exportiert, sind für die Konfiguration von `domain1` einige zusätzliche Schritte erforderlich.

```
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
```

- Nachdem `domain1` gebunden und gestartet wurde, erscheint das exportierte Volume z. B. als `/dev/dsk/c0d2s0` und kann verwendet werden.

```
domain1# newfs /dev/rdsk/c0d2s0
domain1# mount /dev/dsk/c0d2s0 /mnt
domain1# echo test-domain1 > /mnt/file
```

- Nachdem `domain1` gestoppt und getrennt wurde, können Sie von der `primary`-Domain aus über ein SVM-Volume `d0` direkt auf die auf der virtuellen Platte von `domain1` aus gespeicherten Daten zugreifen.

```
primary# mount /dev/md/dsk/d0 /mnt
primary# cat /mnt/file
test-domain1
```

Hinweis – Mit dem Befehl `format (1M)` ist eine solche virtuelle Platte nicht zu sehen, lässt sich nicht partitionieren und kann nicht als Installationsplatte für das Betriebssystem Solaris verwendet werden. Nähere Informationen zu diesem Thema finden Sie unter [„Einige format \(1M\)-Befehlsoptionen funktionieren bei virtuellen Platten nicht“](#) auf Seite 92.

Verwenden von virtuellen Platten als Schicht über einem SVM

Wenn ein gespiegeltes oder RAID-Volume des SVM von einer anderen Domain als virtuelle Platte verwendet wird und eine Komponente des SVM-Volumes ausfällt, kann die Wiederherstellung des SVM-Volumes mit dem Befehl `metareplace` oder mithilfe einer Hot-Spare-Funktion nicht gestartet werden. Der Befehl `metastat` betrachtet das Volume als in der Resynchronisierung, doch schreitet der Vorgang nicht voran.

Beispiel: `/dev/md/dsk/d0` ist ein RAID SVM-Volume, das als virtuelle Platte zu einer anderen Domain exportiert wurde, und `d0` ist mit einigen Hot-Spare-Geräten konfiguriert. Fällt eine Komponente von `d0` aus, ersetzt der SVM diese mit einer Hot-Spare-Komponente und resynchronisiert das SVM-Volume. Die Resynchronisierung wird jedoch nicht gestartet. Das Volume wird zwar als in Resynchronisierung gemeldet, doch schreitet der Vorgang nicht voran.

```
# 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
```

In einem solchen Fall muss die Domain, welche das SVM-Volume als virtuelle Platte nutzt, gestoppt und getrennt werden, damit die Resynchronisierung abgeschlossen werden kann. Anschließend kann das SVM-Volume mit dem Befehl `metasynch` resynchronisiert werden.

```
# metasynch d0
```

Verwenden von virtuellen Platten bei installiertem VxVM

Ist der Veritas Volume Manager (VxVM) auf Ihrem System installiert, müssen Sie sicherstellen, dass die Funktion Veritas Dynamic Multipathing (DMP) auf den physikalischen Platten oder Partitionen, die Sie als virtuelle Platten exportieren möchten, nicht aktiviert ist. Andernfalls erhalten Sie in `/var/adm/messages` eine Fehlermeldung, wenn Sie eine Domain binden, die eine solche Platte verwendet.

```
vd_setup_vd(): ldi_open_by_name(/dev/dsk/c4t12d0s2) = errno 16
vds_add_vd(): Failed to add vdisk ID 0
```

Sie können überprüfen, ob Veritas DMP aktiviert ist, indem Sie die Multipathing-Information in der Ausgabe des Befehls `vxdisk list` suchen. Beispiel:

```
# 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
```

Ist Veritas DMP auf einer Platte oder einem Segment aktiviert, die bzw. das sie als virtuelle Platte exportieren wollen, müssen Sie DMP mithilfe des Befehls `vxddmpadm` deaktivieren. Beispiel:

```
# vxddmpadm -f disable path=/dev/dsk/c4t12d0s2
```

Verwenden eines Volume-Managers als Schicht über einer virtuellen Platte

In diesem Abschnitt werden folgende Situationen in der Logical Domains-Umgebung beschrieben:

- „Verwenden des ZFS als Schicht über einer virtuellen Platte“ auf Seite 108
- „Verwenden des SVM als Schicht über einer virtuellen Platte“ auf Seite 108
- „Verwenden eines VxVM als Schicht über einer virtuellen Platte“ auf Seite 108

Verwenden des ZFS als Schicht über einer virtuellen Platte

Mit dem ZFS lässt sich jede virtuelle Platte verwenden. Ein ZFS-Speicherpool (`zpool`) kann in jede Domain importiert werden, die alle Speichergeräte sieht, die zu diesem `zpool` gehören, egal ob die Domain alle diese Geräte als virtuelle oder reale Geräte betrachtet.

Verwenden des SVM als Schicht über einer virtuellen Platte

Im lokalen SVM-Plattensatz lässt sich jede virtuelle Platte verwenden. Beispiel: Eine virtuelle Platte kann zum Speichern der SVM-Metadatenbank (`metadb`) des lokalen Plattensatzes oder zum Erzeugen von SVM-Volumes im lokalen Plattensatz verwendet werden.

Derzeit können Sie nur virtuelle Platten mit dem lokalen Plattensatz verwenden, jedoch nicht mit einem gemeinsamen Plattensatz (`metaset`). In einem gemeinsamen SVM-Plattensatz können keine virtuellen Platten hinzugefügt werden. Der Versuch, eine virtuelle Platte einem gemeinsamen SVM-Plattensatz hinzuzufügen, schlägt fehl, und es wird eine Fehlermeldung wie die folgende ausgegeben.

```
# metaset -s test -a c2d2
metaset: domain1: test: failed to reserve any drives
```

Verwenden eines VxVM als Schicht über einer virtuellen Platte

VxVM funktioniert derzeit bei virtuellen Platten nicht. Die VxVM-Software kann in einer Domain installiert werden, in der virtuelle Platten vorhanden sind, doch VxVM kann keine dieser verfügbaren virtuellen Platten sehen.

Konfigurieren von IPMP in einer Logical Domains-Umgebung

Das Internet Protocol Network Multipathing (IPMP) bietet Fehlertoleranz und Belastungsausgleich über mehrere Netzwerk-Schnittstellenkarten hinweg. Durch Verwendung von IPMP können Sie eine oder mehrere Schnittstellen in einer IP-Multipathing-Gruppe konfigurieren. Nach der Konfigurierung von IPMP überwacht

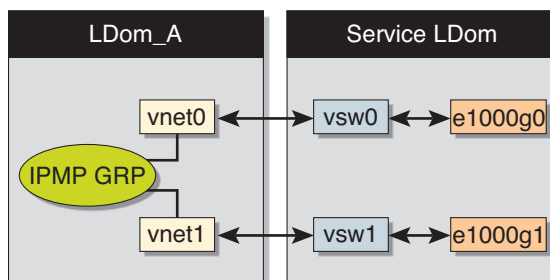
das System automatisch die Schnittstellen in der IPMP-Gruppe auf Ausfälle. Fällt eine Schnittstelle in der Gruppe aus oder wird zu Wartungszwecken entfernt, migriert IPMP automatisch oder bricht bei ausgefallenen IP-Adressen der Schnittstelle ab. In einer Logical Domains-Umgebung können entweder die physikalischen oder die virtuellen Netzwerkschnittstellen für Failover mithilfe von IPMP konfiguriert werden.

Konfigurieren von virtuellen Netzwerkgeräten in eine IPMP-Gruppe einer Logical Domain hinein

Eine Logical Domain lässt sich auf Fehlertoleranz konfigurieren, indem man seine virtuellen Netzwerkgeräte zu einer IPMP-Gruppe konfiguriert. Beim Einrichten einer IPMP-Gruppe mit virtuellen Netzwerkgeräten in einer Active-Standby-Konfiguration wird die Gruppe so eingerichtet, dass eine sondenbasierte Erkennung genutzt wird. Link-basierte Erkennung und Failover für virtuelle Netzwerkgeräte werden in der Logical Domains 1.0.2-Software derzeit nicht unterstützt.

Das folgende Diagramm zeigt zwei virtuelle Netzwerke (vnet1 und vnet2), die in der Servicedomain mit separaten virtuellen Switch-Instanzen (vsw0 und vsw1) verbunden sind, die ihrerseits zwei verschiedene physische Schnittstellen (e1000g0 und e1000g1) nutzen. Bei Ausfall einer physikalischen Schnittstelle erkennt die IP-Schicht in LDom_A durch die sondenbasierte Erkennung den Ausfall und die fehlende Konnektivität auf dem entsprechenden vnet, bricht automatisch ab und schaltet automatisch zum sekundären vnet-Gerät um.

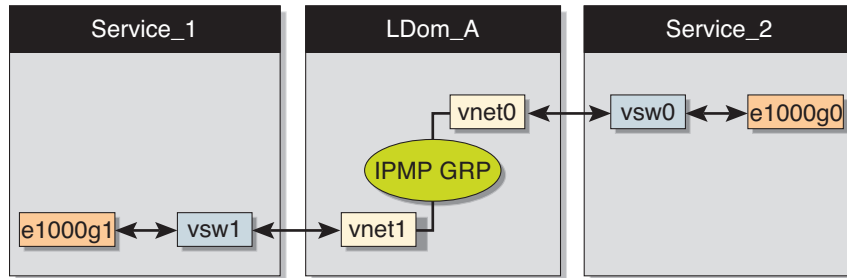
ABBILDUNG 5-1 Zwei virtuelle Netzwerke, die mit separaten virtuellen Switch-Instanzen verbunden sind



Eine weitere Zuverlässigkeit lässt sich in der Logical Domain erreichen, wenn Sie jedes virtuelle Netzwerkgerät (vnet0 und vnet1) mit virtuellen Switch-Instanzen in verschiedenen Servicedomains verbinden (siehe Abbildung im folgenden Diagramm). Mithilfe einer Split-PCI-Konfiguration können zwei Servicedomains (Service_1 und Service_2) mit zwei virtuellen Switch-Instanzen (vsw1 und

vsw2) eingerichtet werden. In diesem Fall kann LDom_A neben Ausfällen bei der Netzwerkhardware auch Ausfälle virtueller Netzwerke erkennen und nach dem Absturz oder Abschaltung einer Servicedomain ein Failover auslösen.

ABBILDUNG 5-2 Jedes virtuelle Netzwerkgerät ist mit einer anderen Servicedomain verbunden



Nähere Informationen über die Konfiguration und Verwendung von IPMP-Gruppen finden Sie im Solaris 10 *Handbuch für Systemadministratoren: IP-Dienste*.

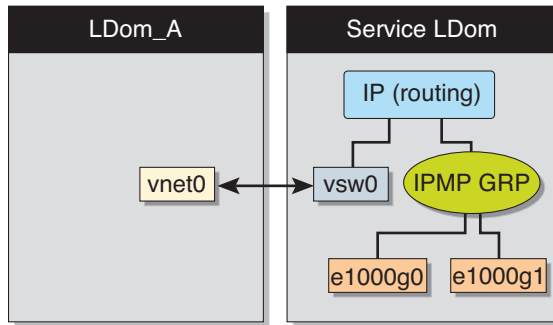
Konfigurieren und Verwenden von IPMP in der Servicedomain

Die Erkennung von Netzwerkausfällen und deren Wiederherstellung kann in einer Logical Domains-Umgebung durch die Konfiguration der physikalischen Schnittstellen in der Servicedomain in eine IPMP-Gruppe hinein eingerichtet werden. Konfigurieren Sie hierzu den virtuellen Switch in der Servicedomain als Netzwerkgerät und die Servicedomain selbst so, dass sie als IP-Router fungiert (Nähere Informationen zum Einrichten des IP-Routings finden Sie im Solaris 10 *Handbuch für Systemadministratoren: IP-Dienste*).

Einmal konfiguriert, schickt der virtuelle Switch alle Pakete, die aus virtuellen Netzwerken stammen (und für einen externen Rechner bestimmt sind) an seine IP-Schicht, statt sie direkt über das physikalische Gerät zu senden. Beim Ausfall einer physikalischen Schnittstelle erkennt die IP-Schicht den Ausfall und leitet die Pakete automatisch über die sekundäre Schnittstelle um.

Da physikalische Schnittstellen direkt in eine IPMP-Gruppe hinein konfiguriert werden, lässt sich die Gruppe entweder für eine Link-basierte oder für eine sondenbasierte Erkennung einrichten. Das folgende Diagramm zeigt zwei Netzwerkschnittstellen (e1000g0 und e1000g1), die als Teil einer IPMP-Gruppe konfiguriert wurden. Die virtuelle Switch-Instanz (vsw0) wurde als Netzwerkgerät angeschlossen, um die Pakete an seine IP-Schicht zu schicken.

ABBILDUNG 5-3 Zwei als Teil einer IPMP-Gruppe konfigurierte Netzwerkschnittstellen



Glossar

In dieser Liste werden die Begriffe und Abkürzungen in der Logical Domains-Dokumentation erläutert.

A

ALOM CMT Abkürzung für Advanced Lights Out Manager Chip Multithreading, das auf dem Systemcontroller ausgeführt wird und die Überwachung und Steuerung Ihres CMT-Servers ermöglicht.

Autorisierung Konfiguration von Autorisierung mithilfe von Solaris OS RBAC.

B

bge Broadcom Gigabit Ethernet-Treiber auf Broadcom BCM57xx-Geräten.

BSM Abkürzung für Basic Security Module, das Basissicherheitsmodul.

C

CLI Abkürzung für Command-Line Interface (Befehlszeilenoberfläche)

config Name der auf dem Systemcontroller gespeicherten Konfiguration einer logischen Domain.

- CMT** Abkürzung für Chip Multithreading.
- CPU** Abkürzung für Central Processing Unit (zentrale Verarbeitungseinheit)
- CWQ** Abkürzung für Control Word Queue (Mitteilungs-Warteschlange); Kryptographieeinheit für Sun UltraSPARC T2-basierte Plattformen.
-

D

- DHCP** Abkürzung für Dynamic Host Configuration Protocol.
- DMP** Abkürzung für Dynamic Multipathing (Veritas).
- DR** Abkürzung für Dynamic Reconfiguration (dynamische Neukonfiguration).
- drd(1M)** Dynamischer Neukonfigurations-Daemon für Logical Domains Manager (Solaris 10 OS).
- DS** Domain Services Modul (Solaris 10 OS)
-

E

- e1000g** Treiber für Intel PRO/1000 Gigabit-Familie von Netzwerkschnittstellencontrollern.
- E/A-Domain** Domain, die direkter Eigentümer von physikalischen E/A-Geräten ist und direkten Zugriff darauf hat und diese Geräte mit anderen logischen Domains in Form von virtuellen Geräten gemeinsam nutzt.
- EFI** Abkürzung für Extensible Firmware Interface (erweiterbare Firmware-Schnittstelle).
- Einschränkungen** Für den Logical Domains Manager sind Einschränkungen eine oder mehrere Ressourcen, die einer bestimmten Domain zugeordnet werden sollen. Sie erhalten entweder alle Ressourcen, die einer Domain zugeordnet werden sollen, oder Sie erhalten gar keine, je nachdem, welche Ressourcen verfügbar sind.
- ETM** Abkürzung für Encoding Table Management Modul (Solaris 10 OS).

F

- FC_AL** Abkürzung für Fiber Channel Arbitrated Loop.
- FMA** Abkürzung für Fault Management Architecture.
- fmd(1M)** Abkürzung für Fault Manager-Daemon (Solaris 10 OS).
- FTP** Abkürzung für File Transfer Protocol.

G

- Gastdomain** Verwendet Dienste aus der E/A und den Servicedomains und wird von der Steuerdomain verwaltet.
- GLDv3** Abkürzung für Generic LAN Driver Version 3.

H

- Hardening** Verändern der Solaris OS-Konfiguration zur Verbesserung der Sicherheit.
- HDD** Abkürzung für Hard Disk Drive (Festplattenlaufwerk).
- Hypervisor** Firmware-Schicht, die zwischen dem Betriebssystem und der Hardware-Schicht zwischengeschaltet ist.

I

- IB** Infiniband
- io** E/A-Geräte, wie interne Platten und PCI-Express (PCI-E)-Controller sowie damit verbundene Adapter und Geräte.
- ioctl** input/output control call (Eingabe/Ausgabe-Kontrollaufruf)
- IP** Internet Protocol
- IPMP** Internet Protocol Network Multipathing

K

kaio	kernel asynchronous input/output
KB	Kilobyte
Konformität	Ermitteln, ob die Konfiguration eines Systems mit einem vordefinierten Sicherheitsprofil konform ist.
KU	Kernel Update

L

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDC	Logical Domain Channel
ldm(1M)	Logical Domain Manager-Dienstprogramm
ldmd	Logical Domains Manager
Logische Domain	Diskrete logische Gruppierung mit eigenem Betriebssystem, eigenen Ressourcen und eigener Identität innerhalb eines einzelnen Computersystems.
Logical Domains (LDoms) Manager	Bietet eine Befehlszeilenoberfläche zur Erstellung und Verwaltung logischer Domains und Zuordnung von Ressourcen zu Domains.

M

MAC	Speichermedien-Zugriffssteuerungsadresse (Media Access Control), die LDoms automatisch oder die Sie manuell zuweisen können.
MAU	Modular Arithmetic Unit (modulare Arithmetikeinheit); Kryptographiegerät für Sun UltraSPARC T1-basierte Plattformen.
MB	Megabyte
MD	Maschinenbeschreibung in der Serverdatenbank

<code>mem, memory</code>	Speichereinheit – Standardgröße in Byte oder Angabe in Gigabyte (G), Kilobyte (K) oder Megabyte (M). Virtualisierter Speicher des Servers, der der Gastdomain zugewiesen werden kann.
MMF	Multimode Fiber
MIB	Management Information Base
Minimieren	Installation der minimalen Anzahl an erforderlichen Solaris OS-Kernpaketen.
MMU	Memory Management Unit (Speicherverwaltungseinheit)
<code>mtu</code>	Maximum Transmission Unit (Maximalübertragungseinheit)

N

NAT	Network Address Translation
NDPSS	Netra Data Plane Software Suite 1.1
<code>ndpsldcc</code>	Netra Data Plane Software Logical Domain Channel Client. <i>Siehe auch</i> <code>vdppcc</code> .
<code>ndpsldcs</code>	Netra Data Plane Software Logical Domain Channel Service. <i>Siehe auch</i> <code>vdpcs</code> .
NFS	Network File System (Netzwerkdateisystem)
NIS	Abkürzung für Network Information Services (Netzwerkinformationsdienste).
NIU	Abkürzung für Network Interface Unit (Sun SPARC Enterprise T5120- und T5220-Server), Netzwerkschnittstellen-Einheit
NTS	Abkürzung für Network Terminal Server (Netzwerk-Terminalserver).
NVRAM	Abkürzung für Non-Volatile Random-Access Memory (nicht flüchtiger Direktzugriffsspeicher).
<code>nxge</code>	Treiber für Sun x8 Express 1/10G Ethernet Adapter

O

OS	Betriebssystem (Operating System)
-----------	-----------------------------------

P

PA	Physikalische Adresse
PCI	Peripheral Component Interconnect-Bus
PCI-E	PCI Express-Bus
PCI-X	PCI Extended-Bus
PICL	Abkürzung für Platform Information and Control Library (Plattform- Informations- und Steuerbibliothek).
picld(1M)	PICL-Daemon
PRI	Priorität
Prüfung	Die Verwendung des Solaris OS-BSM, um die Quelle von Sicherheitsänderungen zu identifizieren.

R

RA	Abkürzung für Real Address (tatsächliche Adresse).
RAID	Redundant Array of Inexpensive Disks
RBAC	Role-Based Access Control
RPC	Remote Procedure Call

S

SC	Systemcontroller, entspricht Systemprozessor
SCSI	Small Computer System Interface
Servicedomain	Logische Domain, die Geräte, z. B. virtuelle Switches, virtuelle Konsolenkonzentratoren und virtuelle Plattenserver anderen logischen Domains zur Verfügung stellt.
SMA	System Management Agent

SMF	Service Management Facility von Solaris 10 OS
SNMP	Simple Network Management Protocol
SP	Systemprozessor, entspricht Systemcontroller
SSH	Secure Shell
<code>ssh(1)</code>	Secure Shell-Befehl
<code>sshd(1M)</code>	Secure Shell-Daemon
Steuerdomain	Domain, die andere logische Domains und Dienste erstellt und steuert.
SunVTS	Sun Validation Test Suite
SVM	Solaris Volume Manager

T

TCP	Abkürzung für Transmission Control Protocol.
------------	--

U

UDP	User Datagram Protocol
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair

V

vBSC	virtual Blade System Controller
<code>vcc, vconscn</code>	Virtueller Konsolenkonzentratordienst mit einem spezifischen Portbereich für die Zuweisung zu Gastdomains.
<code>vcons, vconsole</code>	Virtuelle Konsole für den Zugriff auf Meldungen auf Systemebene. Eine Verbindung wird über den <code>vconscn</code> -Dienst in der Steuerdomain an einem bestimmten Port hergestellt.

<code>vcpu</code>	virtual central processing unit (virtuelle zentrale Verarbeitungseinheit). Jeder der Kerne eines Servers wird als virtuelle CPU dargestellt. So verfügt z. B. ein 8-Kern-Sun Fire T2000-Server über 32 virtuelle CPUs, die zwischen logischen Domains zugewiesen werden können.
<code>vdc</code>	virtual disk client (virtueller Plattenclient)
<code>vdpccl</code>	Virtual Data Plane Channel-Client in einer NDPS-Umgebung.
<code>vdpcsl</code>	Virtual Data Plane Channel-Dienst in einer NDPS-Umgebung.
<code>vdisk</code>	Bei virtuellen Platten handelt es sich um Blockeinheiten, denen unterschiedliche Arten von Geräten, Volumes oder Dateien zu Grunde liegen.
<code>vds, vdiskserver</code>	Virtuelle Plattenserver ermöglichen den Import von virtuellen Platten in die logische Domain.
<code>vdsdev, vdiskserverdevice</code>	Das virtuelle Plattenservergerät wird vom virtuellen Plattenserver exportiert. Das Gerät kann entweder eine ganze Platte sein, ein Segment auf einer Platte oder ein Plattenvolume.
<code>vnet</code>	Das virtuelle Netzwerkgerät implementiert ein virtuelles Ethernet-Gerät und kommuniziert mit anderen <code>vnet</code> -Geräten im System über den virtuellen Netzwerkschalt (vswitch).
<code>vntsd(1M)</code>	Virtueller Netzwerk-Terminalserver-Daemon für Logical Domains-Konsolen (Solaris 10 OS).
<code>vsw, vswitch</code>	Virtueller Netzwerkschalt, der die virtuellen Netzwerkgeräte mit dem externen Netzwerk verbindet sowie Pakete zwischen diesen vermittelt.
VTOC	Abkürzung für Volume Table Of Contents, ein Volume-Inhaltsverzeichnis.
VxVM	Veritas Volume Manager

W

WAN Abkürzung für Wide-Area Network.

X

XFP Abkürzung für eXtreme Fast Path.

XML Abkürzung für Extensible Markup Language (engl. für "erweiterbare Auszeichnungssprache").

Z

ZFS Abkürzung für Zettabyte File System (Solaris 10 OS).

zpool(1M) ZFS-Speicherpool.

