Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation



Teilenr.: 821–2332–10 September 2010 Copyright © 2010, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehne Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065, USA.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

AMD, Opteron, das AMD-Logo und das AMD-Opteron-Logo sind Marken oder eingetragene Marken von Advanced Micro Devices. Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. UNIX ist eine durch X/Open Company, Ltd lizenzierte, eingetragene Marke.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Copyright © 2010, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de la décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédé sous license par X/Open Company, Ltd.

Inhalt

	Vorwort	9
Teil I	Planung der Netzwerkinstallation	13
1	Informationen zur Planung einer Solaris-Installation	15
	Informationen zur Planung und zu den Systemanforderungen	15
2	Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)	17
	Vorteile der Vorkonfiguration von Systemkonfigurationsinformationen	17
	Vorkonfiguration mit der Datei sysidcfg	18
	▼ So erstellen Sie eine sysidcfg-Konfigurationsdatei	20
	Syntaxregeln für die Datei sysidcfg	22
	Schlüsselwörter in der Datei sysidcfg	22
	SPARC: Vorkonfigurieren der Power Management-Informationen	42
3	Vorkonfigurieren mit einem Naming Service oder DHCP	45
	Auswählen eines Naming Service	45
	Vorkonfiguration mit dem Naming Service	47
	▼ So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS vor	48
	▼ So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS+ vor	50
	Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service	
	(Vorgehen)	52
	Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter	53

Teil II	Installation über ein LAN
4	Installieren über das Netzwerk (Übersicht)
	Einführung in die Netzwerkinstallation
	Für die Installation über ein Netzwerk erforderliche Server
	x86: Überblick über das Booten und Installieren über das Netzwerk mit PXE
	x86: Was ist PXE?
	x86: Richtlinien für das Booten mit PXE
5	Installieren über das Netzwerk mithilfe von DVDs (Vorgehen)
	Übersicht der Schritte: Installieren über das Netzwerk mithilfe von DVDs
	Erstellen eines Installationsservers mithilfe einer DVD
	▼ So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver
	Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes
	\blacksquare So erstellen Sie einen Boot-Server in einem Teilnetz mithilfe eines DVD-Abbildes
	Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild
	▼ So fügen Sie über das Netzwerk zu installierende Systeme mit add_install_client hinzu (DVD)
	Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds
	▼ SPARC: So installieren Sie den Client über das Netzwerk (DVDs)
	▼ x86: So installieren Sie den Client über das Netzwerk mit GRUB (DVDs)
6	Installieren über das Netzwerk mithilfe von CDs (Vorgehen)
	Übersicht der Schritte: Installieren über das Netzwerk mithilfe von CDs
	Erstellen eines Installationsservers mit SPARC- bzw. x86-CDs
	▼ SPARC: So erstellen Sie mit einer SPARC- bzw. x86-CD einen Installationsserver
	Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes
	▼ So erstellen Sie einen Boot-Server in einem Teilnetz mithilfe eines CD-Abbildes

▼ So fügen Sie über das Netzwerk zu installierende Systeme mit add_install	l_client hinzu
(CDs)	
Installieren des Systems über das Netzwerk mithilfe eines CD-Abbilds	116
▼ SPARC: So installieren Sie den Client über das Netzwerk (CDs)	
▼ x86: So installieren Sie den Client über das Netzwerk mit GRUB (CDs)	

7	Patchen des Miniroot-Abbilds (Vorgehen)	
	Patchen des Miniroot-Abbilds (Vorgehen)	
	Informationen zum Miniroot-Abbild (Übersicht)	
	▼ So patchen Sie das Miniroot-Abbild	
	Patchen des Miniroot-Abbilds (Beispiel)	
	Patchen des Miniroot-Abbilds	
8	Installieren über das Netzwerk (Beispiele)	
	Netzwerkinstallation über das gleiche Teilnetz (Beispiele)	
9	Installation über das Netzwerk (Befehlsreferenz)	
	Befehle für die Installation über das Netzwerk	
	x86: GRUB-Menübefehle für die Installation	
Teil III	Installation über ein WAN	
10	WAN-Boot (Übersicht)	151
	Was ist WAN-Boot?	
	Wann ist WAN-Boot sinnvoll?	
	Wie funktioniert WAN-Boot (Übersicht)	
	Ereignisabfolge bei einer WAN-Boot-Installation	
	Schutz der Daten während einer WAN-Boot-Installation	
	Von WAN-Boot unterstützte Sicherheitskonfigurationen (Übersicht)	

11	Vorbereiten der Installation mit WAN-Boot (Planung)	
	WAN-Boot - Voraussetzungen und Richtlinien	159
	Webserver-Software - Voraussetzungen und Richtlinien	161
	Serverkonfigurationsoptionen	
	Speichern von Installations- und Konfigurationsdateien im Dokument-Root-Verzeichnis	
	Speichern von Konfigurations- und Sicherheitsinformationen in der /etc/netboot-Hierarchie	

	Speichern des Programms wanboot-cgi	168
	Voraussetzungen für digitale Zertifikate	168
	Sicherheitslücken bei der Arbeit mit WAN-Boot	169
	Zusammenstellen der Informationen für WAN-Boot-Installationen	169
12	Installieren mit WAN-Boot (Vorgehen)	173
	Installieren über ein regional erweitertes Netzwerk (WAN) (Übersicht der Schritte)	173
	Konfiguration des WAN-Boot-Servers	177
	Erstellen des Dokument-Root-Verzeichnisses	178
	Erzeugen der WAN-Boot-Miniroot	178
	Überprüfen des Clients auf WAN-Boot-Unterstützung	181
	Installation des wanboot-Programms auf dem WAN-Boot-Server	183
	Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server	186
	Kopieren des WAN-Boot-CGI-Programms auf den WAN-Boot-Server	189
	igvee (Optional) So konfigurieren Sie den WAN-Boot-Protokollserver	190
	(Optional) Schützen der Daten mit HTTPS	191
	▼ (Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung	192
	▼ (Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel	195
	Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation	197
	▼ So erzeugen Sie das Solaris Flash-Archiv	198

igvee So erzeugen Sie das Solaris Flash-Archiv	198
▼ So erzeugen Sie die Datei sysidcfg	200
▼ So erstellen Sie das Profil	201
▼ So erstellen Sie die Datei rules	203
(Optional) Erzeugen von Begin- und Finish-Skripten	206
Erstellen der Konfigurationsdateien	207
igvee So erzeugen Sie die Systemkonfigurationsdatei	207
▼ So erzeugen Sie die Datei wanboot . conf	209
$(Optional) \ Bereitstellung \ von \ Konfigurations informationen \ mit \ einem \ DHCP-Server \$	214

13	SPARC: Installation mit WAN-Boot (Vorgehen)	
	Übersicht der Schritte: Installation eines Clients mit WAN-Boot	215
	Vorbereitung des Clients für eine WAN-Boot-Installation	216
	▼ So überprüfen Sie den Gerätealias net im Client-OBP	
	Installation von Schlüsseln auf dem Client	

	Installation des Clients	224
	igvee So nehmen Sie eine ungeführte WAN-Boot-Installation vor	225
	igvee So nehmen Sie eine interaktive WAN-Boot-Installation vor	227
	▼ So nehmen Sie eine WAN-Boot-Installation mit einem DHCP-Server vor	231
	\blacksquare So nehmen Sie eine WAN-Boot-Installation mit lokalen CDs vor	233
14	SPARC: Installation mit WAN-Boot (Beispiele)	239
	Konfiguration des Beispielstandorts	240
	Erstellen des Dokument-Root-Verzeichnisses	241
	Erzeugen der WAN-Boot-Miniroot	241
	Überprüfen des Client-OBP auf WAN-Boot-Unterstützung	241
	Installation des wanboot-Programms auf dem WAN-Boot-Server	242
	Erstellen Sie die /etc/netboot-Hierarchie.	242
	Kopieren des Programms wanboot-cgi auf den WAN-Boot-Server	243
	(Optional) Konfigurieren des WAN-Boot-Servers als Anmeldeserver	243
	Konfiguration des WAN-Boot-Servers für die Verwendung von HTTPS	243
	Liefern des vertrauenswürdigen Zertifikats an den Client	244
	(Optional) Einsatz von privatem Schlüssel und Zertifikat zur Client-Authentifizierung	244
	Erzeugen der Schlüssel für Server und Client	245
	Erzeugen des Solaris Flash-Archivs	245
	Erzeugen der Datei sysidcfg	246
	Erstellen des Client-Profils	246
	Erzeugen und Überprüfen der Datei rules	247
	Erzeugen der Systemkonfigurationsdatei	247
	Erzeugen der Datei wanboot . conf	248
	Überprüfen des Gerätealias net im OBP	250
	Installation von Schlüsseln auf dem Client	250
	Installation des Clients	251

15	WAN-Boot (Referenz)	.253
	Befehle für die WAN-Boot-Installation	. 253
	OBP-Befehle	. 256
	Einstellungen und Syntax der Systemkonfigurationsdatei	. 257
	Parameter der Datei wanboot . conf und Syntax	. 258

Inhalt

 A Fehlerbehebung (Vorgehen) 26 Probleme beim Einrichten von Netzwerkinstallationen 26 Probleme beim Booten eines Systems 26 Booten von Medien, Fehlermeldungen 26 Booten von Medien, allgemeine Probleme 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, allgemeine Probleme 27 Neuinstallation von Solaris 27 ▼ x86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke 27 Upgrade von Solaris 27 Durchführen eines Upgrade, Fehlermeldungen 27 ✓ so setzen Sie ein Upgrade, allgemeine Probleme 27 ✓ so setzen Sie ein Upgrade nach einem Fehlschlag fort 27 ✓ Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm 28 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt 28 ✓ So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD 28 	IV	Anhänge	263
Probleme beim Einrichten von Netzwerkinstallationen 26 Probleme beim Booten eines Systems 26 Booten von Medien, Fehlermeldungen 26 Booten von Medien, allgemeine Probleme 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, allgemeine Probleme 26 Booten vom Netzwerk, Statistication von Solaris 27 Neuinstallation von Solaris 27 Vgrade von Solaris 27 Upgrade von Solaris 27 Durchführen eines Upgrade, Fehlermeldungen 27 Durchführen eines Upgrade, Fehlermeldungen 27 V So setzen Sie ein Upgrade, allgemeine Probleme 27 V So setzen Sie ein Upgrade nach einem Fehlschlag fort 27 V So setzen Sie eine Upgrade mit Solaris Live Upgrade und Veritas VxVm 28 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt 28 V So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD 28	A	Fehlerbehebung (Vorgehen)	265
Probleme beim Booten eines Systems 26 Booten von Medien, Fehlermeldungen 26 Booten von Medien, allgemeine Probleme 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, Jalgemeine Probleme 26 Booten vom Netzwerk, allgemeine Probleme 27 Neuinstallation von Solaris 27 Var86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke 27 Upgrade von Solaris 27 Durchführen eines Upgrade, Fehlermeldungen 27 Durchführen eines Upgrade, allgemeine Probleme 27 V So setzen Sie ein Upgrade nach einem Fehlschlag fort 27 x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB 27 Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm 28 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt 28 So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD 28		Probleme beim Einrichten von Netzwerkinstallationen	265
 Booten von Medien, Fehlermeldungen		Probleme beim Booten eines Systems	266
 Booten von Medien, allgemeine Probleme		Booten von Medien, Fehlermeldungen	266
Booten vom Netzwerk, Fehlermeldungen 26 Booten vom Netzwerk, allgemeine Probleme 27 Neuinstallation von Solaris 27 ▼ x86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke 27 Upgrade von Solaris 27 Durchführen eines Upgrade, Fehlermeldungen 27 Durchführen eines Upgrade, allgemeine Probleme 27 V So setzen Sie ein Upgrade nach einem Fehlschlag fort 27 x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB 27 × Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm 28 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt 28 So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD 28		Booten von Medien, allgemeine Probleme	267
 Booten vom Netzwerk, allgemeine Probleme		Booten vom Netzwerk, Fehlermeldungen	268
 Neuinstallation von Solaris		Booten vom Netzwerk, allgemeine Probleme	271
 ▼ x86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke		Neuinstallation von Solaris	272
Upgrade von Solaris 27 Durchführen eines Upgrade, Fehlermeldungen 27 Durchführen eines Upgrade, allgemeine Probleme 27 V So setzen Sie ein Upgrade nach einem Fehlschlag fort 27 x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB 27 V Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm 28 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt 28 V So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD 28		▼ x86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke	273
 Durchführen eines Upgrade, Fehlermeldungen		Upgrade von Solaris	274
 Durchführen eines Upgrade, allgemeine Probleme		Durchführen eines Upgrade, Fehlermeldungen	274
 So setzen Sie ein Upgrade nach einem Fehlschlag fort		Durchführen eines Upgrade, allgemeine Probleme	276
 x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB		igvee So setzen Sie ein Upgrade nach einem Fehlschlag fort	278
 Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm		x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB	278
 x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt		▼ Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm	280
 ▼ So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD		x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition ni standardmäßig erzeugt	cht 282
		▼ So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD	283
▼ So installieren Sie von der Solaris Software-1 CD oder einem		▼ So installieren Sie von der Solaris Software-1 CD oder einem	
Netzwerk-Installationsabbild		Netzwerk-Installationsabbild	283
K ANKINGTON DINOF INCLUDING MODE DINOCH MARANOL WAS DINOM DATIONAL WITHOUT AND A DINOT DINOT.	U	(Vorgehen)	285
(Vorgehen)		SPARC: Ausführen einer Installation oder eines Upgrade von einer entfernten DVD-ROM CD-ROM mithilfe des Solaris-Installationsprogramms	oder 285
 Austumen einer installation oder eines Opgrades von einem entremten System (Vorgehen) 28 SPARC: Ausführen einer Installation oder eines Upgrade von einer entfernten DVD-ROM ode CD-ROM mithilfe des Solaris-Installationsprogramms 		▼ SPARC: So führen Sie eine Installation oder ein Upgrade von einer entfernten DVD-Re oder CD-ROM aus	ОМ 286
 Austumen einer installation oder eines Opgrades von einem entrernten System (Vorgehen)		Glossar	289
 Austumentementerinstallation oder eines Opgrades von einem enterinten System (Vorgehen)		Index	305

Vorwort

Dieses Handbuch beschreibt die entfernte Installation von Solaris über ein LAN oder ein WAN.

Dieses Handbuch enthält keine Informationen zum Konfigurieren von Systemhardware und Peripheriegeräten.

Hinweis – Diese Solaris-Version unterstützt Systeme auf Basis der Prozessorarchitekturen SPARC und x86. Die unterstützten Systeme werden unter Solaris OS: Hardware Compatibility Lists (http://www.sun.com/bigadmin/hcl) aufgeführt. Eventuelle Implementierungsunterschiede zwischen den Plattformtypen sind in diesem Dokument angegeben.

In diesem Dokument bedeuten x86-bezogene Begriffe Folgendes:

- "x86" bezeichnet die weitere Familie an Produkten, die mit 64-Bit- und 32-Bit-x86-Architekturen kompatibel sind.
- "x64" bezieht sich insbesondere auf mit 32-Bit-x86-Architekturen kompatible CPUs.
- "32-Bit x86" weist auf spezifische, für 32-Bit-Systeme geltende Informationen zu x86-basierten Systemen hin.

Die unterstützten Systeme können Sie der Solaris OS: Hardware-Kompatibilitätsliste entnehmen.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich an Systemadministratoren, die für die Installation der Solaris-Software zuständig sind. Es umfasst weiterführende Informationen zur Installation von Solaris für Systemadministratoren in Unternehmen, die mehrere Solaris-Rechner in einer vernetzten Umgebung verwalten.

Grundlegende Informationen zur Installation finden Sie im Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen.

Verwandte Dokumentation

In Tabelle P–1 ist die Dokumentation für Systemadministratoren aufgeführt.

 TABELLE P-1
 Sind Sie ein Systemadministrator, der Solaris installiert?

Beschreibung	Informationen
Benötigen Sie die Systemvoraussetzungen oder Informationen zur allgemeinen Planung? Benötigen Sie eine allgemeine Übersicht zu Solaris ZFS-Installationen, zum Booten, zur Partitionierungstechnologie Solaris Zones oder zum Erstellen von RAID-1-Volumes?	Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
Müssen Sie ein System von einer DVD oder CD installieren? Das Solaris-Installationsprogramm führt Sie Schritt für Schritt durch die Installation.	Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen
Müssen Sie Ihr System patchen oder aktualisieren, und darf es dabei möglichst nicht zu einer Ausfallzeit kommen? Aktualisieren Sie Ihr System mit Solaris Live Upgrade, um die Ausfallzeit auf ein Minimum zu reduzieren.	Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades
Müssen Sie eine sichere Installation über das Netzwerk oder das Internet durchführen? Verwenden Sie WAN-Boot, um auf einem remoten Client zu installieren. Oder müssen Sie über das Netzwerk von einem Installationsabbild installieren? Das Solaris-Installationsprogramm führt Sie Schritt für Schritt durch die Installation.	Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation
Müssen Sie mehrere Systeme schnell aktualisieren oder patchen? Verwenden Sie die Solaris Flash-Software, um ein Solaris Flash-Archiv zu erstellen und eine Kopie des Betriebssystems auf Klonsystemen zu installieren.	Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation)
Müssen Sie Ihr System sichern?	Kapitel 23, "Backing Up and Restoring UFS File Systems (Overview)" in System Administration Guide: Devices and File Systems
Benötigen Sie Informationen zur Fehlerbehebung, eine Liste der bekannten Probleme oder eine Liste der Patches für diese Version?	Solaris Versionshinweise
Müssen Sie überprüfen, ob Ihr System für die Ausführung von Solaris geeignet ist?	SPARC: Solaris Handbuch zur Hardware-Plattform von Sun
Müssen Sie überprüfen, welche Pakete in dieser Version hinzugefügt, entfernt oder geändert wurden?	Solaris Package List
Müssen Sie überprüfen, ob Ihr System und Ihre Geräte mit Solaris SPARC- und x86-basierten Systemen und anderen Drittanbietern ausgeführt werden können?	Solaris Hardware Compatibility List for x86 Platforms

Dokumentation, Support und Schulung

Weitere Informationen finden Sie auf folgenden Websites:

- Dokumentation (http://docs.sun.com)
- Support(http://www.oracle.com/us/support/systems/index.html)
- Schulungen (http://education.oracle.com) Klicken Sie auf den Sun-Link in der linken Navigationsleiste.

Ihre Meinung ist gefragt

Ihre Kommentare und Vorschläge zur Qualität und Nützlichkeit der Dokumentation sind bei Oracle willkommen. Wenn Sie Fehler finden oder sonstige Verbesserungsvorschläge haben, klicken Sie unter http://docs.sun.com auf den Feedback-Link. Geben Sie den Titel und die Teilenummer der Dokumentation sowie das Kapitel, den Abschnitt und die Seitenzahl an, sofern vorhanden. Geben Sie an, ob Sie eine Antwort erwarten.

Oracle Technology Network (http://www.oracle.com/technetwork/index.html) bietet Ressourcen in Zusammenhang mit Oracle-Software:

- Besprechen Sie technische Probleme und Lösungen unter Discussion Forums (http://forums.oracle.com).
- Praktische Lernprogramme mit schrittweisen Anleitungen finden Sie unter Oracle By Example (http://www.oracle.com/technology/obe/start/index.html).
- Laden Sie Beispielcode (http://www.oracle.com/technology/sample_code/index.html) herunter.

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

Schriftart	Bedeutung	Beispiel
AaBbCc123	Die Namen von Befehlen, Dateien,	Bearbeiten Sie Ihre .login-Datei.
	Verzeichnissen sowie Bildschirmausgabe.	Verwenden Sie ls -a, um eine Liste aller Dateien zu erhalten.
		system% Sie haben eine neue Nachricht.

TABELLE P-2 Typografische Konventionen

Schriftart	Bedeutung	Beispiel
AaBbCc123	Von Ihnen eingegebene Zeichen (im Gegensatz	Computername% su
	zu auf dem Bildschirm angezeigten Zeichen)	Passwort:
aabbcc123	Platzhalter: durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet rm <i>Dateiname</i> .
AaBbCc123	Buchtitel, neue Ausdrücke; hervorgehobene Begriffe	Lesen Sie hierzu Kapitel 6 im Benutzerhandbuch.
		Ein <i>Cache</i> ist eine lokal gespeichert Kopie.
		Diese Datei nicht speichern.
		Hinweis: Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die UNIX-Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung variiert, abhängig von der Oracle Solaris-Version.

TABELLE P-3	Shell-	Eingal	beauff	orde	runge	en
-------------	--------	--------	--------	------	-------	----

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	\$
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	#
C-Shell	system%
C-Shell für Superuser	system#

TEIL I

Planung der Netzwerkinstallation

Dieser Teil beschreibt die Planung einer Installation über ein Netzwerk.

◆ ◆ ◆ KAPITEL 1

Informationen zur Planung einer Solaris-Installation

In diesem Buch wird die Ferninstallation von Solaris BS über ein LAN (lokalen Netzwerk) oder ein WAN (Wide Area Network) beschrieben.

In diesem Kapitel werden die Vorbereitungen für eine erfolgreiche Installation beschrieben. Viele Aufgaben zur Vorbereitung gelten für alle Solaris-Installationen. Aus diesem Grund werden sie in einem Master-Planungsdokument beschrieben.

Informationen zur Planung und zu den Systemanforderungen

Im Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades sind die Systemanforderungen und die allgemeinen Informationen zur Planung aufgeführt, beispielsweise Planungsrichtlinien für Dateisysteme, Planung von Upgrades und vieles weitere mehr. Die folgende Liste enthält eine Beschreibung der Kapitel im Planungshandbuch.

Beschreibung der Kapitel im Planungshandbuch	Referenz
In diesem Kapitel werden neue Funktionen in den Solaris-Installationsprogrammen beschrieben.	Kapitel 2, "Neuerungen in der Solaris-Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
In diesem Kapitel finden Sie Informationen zu den Entscheidungen, die Sie treffen müssen, bevor Sie das Betriebssystem Solaris installieren oder ein Upgrade ausführen. Beispielsweise finden Sie hier Informationen, wenn Sie sich entscheiden müssen, ob ein Installationsabbild im Netzwerk oder eine DVD zur Installation verwendet werden soll. Darüber hinaus können Sie hier Beschreibungen aller Solaris-Installationsprogramme nachlesen.	Kapitel 3, "Installation und Upgrade von Solaris (Roadmap)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
Dieses Kapitel befasst sich mit den Systemvoraussetzungen für eine Installation oder ein Upgrade des Betriebssystems (BS) Solaris. Außerdem enthält es allgemeine Richtlinien für die Planung der Zuordnung von Speicherplatz und Standard-Swap-Platz. Hier finden Sie auch Informationen zu den Einschränkungen bei Upgrades.	Kapitel 4, "Systemvoraussetzungen, Richtlinien und Upgrades (Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

Beschreibung der Kapitel im Planungshandbuch	Keterenz
Dieses Kapitel enthält Checklisten, mit deren Hilfe Sie die Informationen zusammenstellen können, die Sie für eine Installation bwz. ein Upgrade benötigen. Diese Informationen sind insbesondere bei einer interaktiven Installation von Nutzen. Alle Informationen, die Sie für eine interaktive Installation benötigen, befinden sich in einer Checkliste.	Kapitel 5, "Zusammenstellen von Informationen vor einer Installation bzw. einem Upgrade (Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
Dieses Buch enthält Beschreibungen und Vergleiche der verschiedenen Technologien zur Installation oder Aktualisierung des Betriebssystems Solaris. Außerdem finden Sie hier Richtlinien und Anforderungen zu diesen Technologien. Diese Kapitel enthalten Informationen zu ZFS-Installationen, zum Booten, der Partitionierungstechnologie Solaris Zones und RAID-1-Volumes, die während der Installation angelegt werden können.	Teil II, "Installationen in Verbindung mit ZFS, Booten, Solaris Zones und RAID-1-Volumes" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

◆ ◆ ◆ KAPITEL 2

Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)

In diesem Kapitel wird beschrieben, wie Sie die Systeminformationen mithilfe der Datei sysidcfg vorkonfigurieren. Durch das Vorkonfigurieren der Systeminformationen können Sie vermeiden, dass Sie während der Installation von Solaris dazu aufgefordert werden, diese Informationen einzugeben. In diesem Kapitel wird außerdem beschrieben, wie Sie die Informationen für Power Management vorkonfigurieren können. Dieses Kapitel enthält die folgenden Abschnitte:

- "Vorteile der Vorkonfiguration von Systemkonfigurationsinformationen" auf Seite 17
- "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18
- "SPARC: Vorkonfigurieren der Power Management-Informationen" auf Seite 42

Vorteile der Vorkonfiguration von Systemkonfigurationsinformationen

Bei allen Installationsverfahren müssen Konfigurationsinformationen über das System bereitgestellt werden, zum Beispiel die Peripheriegeräte, der Host-Name, die IP-Adresse (Internet Protocol) und der Naming Service. Bevor Sie die Installationstools zur Eingabe von Konfigurationsinformationen auffordern, prüfen sie, ob diese Konfigurationsinformationen bereits an anderer Stelle gespeichert sind.

Zum Vorkonfigurieren von Systeminformationen können Sie eines der folgenden Verfahren wählen.

Vorkonfigurationsdatei oder -dienst	Beschreibung	Weitere Informationen
sysidcfg	Konfigurieren Sie den Domänennamen, die Netzmaske, DHCP, IPv6 und andere Parameter mithilfe von Schlüsselwörtern in der sysidcfg-Datei.	"Vorkonfiguration mit der Datei sysidcfg" auf Seite 18
Naming Service	Richten Sie den Host-Namen und die IP-Adressen ein, indem Sie die Systeminformationen in Ihrem Naming Service vorkonfigurieren.	"Vorkonfiguration mit dem Naming Service" auf Seite 47
DHCP	DHCP ermöglicht es, dass ein Host-System in einem TCP/IP-Netzwerk beim Booten des Systems automatisch für das Netzwerk konfiguriert wird. DHCP verwaltet IP-Adressen, indem sie je nach Bedarf an Clients vergeben werden.	"Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52

TABELLE 2–1	Vorkonfigurationso	ptionen
-------------	--------------------	---------

Ausführliche Informationen zur Auswahl einer Methode zur Vorkonfiguration finden Sie unter "Auswählen eines Naming Service" auf Seite 45.

Wenn das Solaris-Installationsprogramm oder das benutzerdefinierte JumpStart-Installationsprogramm vorkonfigurierte Systeminformationen findet, fordert es nicht zur Eingabe dieser Informationen auf. Angenommen, Sie möchten die aktuelle Solaris-Release auf mehreren Systemen installieren und nicht jedes Mal zur Eingabe der Zeitzone aufgefordert werden. In diesem Fall können Sie die Zeitzone in der Datei sysidcfg oder den Naming Service-Datenbanken angeben. Wenn Sie die aktuelle Solaris-Release jetzt installieren, werden Sie vom Installationsprogramm nicht aufgefordert, eine Zeitzone einzugeben.

Vorkonfiguration mit der Datei sysidcfg

In der Datei sysidcfg können Sie zum Vorkonfigurieren eines Systems eine Reihe von Schlüsselwörtern angeben. Die Schlüsselwörter sind in "Schlüsselwörter in der Datei sysidcfg" auf Seite 22 beschrieben. Hinweis – Das Schlüsselwort name_service in der Datei sysidcfg richtet während der Installation des Betriebssystems Solaris den Naming Service automatisch ein. Diese Einstellung hat Vorrang vor den SMF-Services, die zuvor für site.xml eingerichtet wurden. Aus diesem Grund müssen Sie Ihren Naming Service nach der Installation eventuell zurücksetzen.

Für jedes System, für das verschiedene Konfigurationsinformationen gelten sollen, müssen Sie eine eigene sysidcfg-Datei anlegen. Sie können zum Beispiel mit einer sysidcfg-Datei die Zeitzone auf allen Systemen vorkonfigurieren, die derselben Zeitzone zugewiesen werden sollen. Wenn Sie jedoch für jedes dieser Systeme ein anderes Root-Passwort (Superuser-Passwort) konfigurieren wollen, müssen Sie für jedes System eine eigene sysidcfg-Datei anlegen.

Sie können für die Datei sysidcfg einen der folgenden Speicherorte wählen.

NFS-Dateisystem	Wenn Sie die Datei sysidcfg in ein gemeinsam genutztes NFS-Dateisystem stellen, müssen Sie beim Einrichten des Systems zur Installation über das Netzwerk die Option -p des Befehls add_install_client(1M) verwenden. Mit der Option -p geben Sie an, wo das System die Datei sysidcfg bei der Installation der aktuelle Solaris-Release finden kann.
UFS- oder PCFS-Diskette	Speichern Sie die Datei sysidcfg im Root-Verzeichnis (/) der Diskette.
	Wenn Sie eine benutzerdefinierte JumpStart-Installation ausführen und eine sysidcfg-Datei auf einer Diskette verwenden wollen, müssen Sie die sysidcfg-Datei auf die Profildiskette stellen. Anleitungen zum Erstellen einer Profildiskette für Standalone-Systeme" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.
	Sie können jeweils nur eine sysidcfg-Datei in ein Verzeichnis oder auf eine Diskette stellen. Wenn Sie mehr als eine sysidcfg-Datei anlegen, müssen Sie jede Datei in ein eigenes Verzeichnis oder auf eine eigene Diskette stellen.
HTTP- oder HTTPS-Server	Wenn Sie eine WAN-Boot-Installation durchführen möchten, stellen Sie die Datei sysidcfg in das Dokument-Root-Verzeichnis auf dem Webserver.

TABELLE 2-2 sysidcfg-Speicherorte

Sie können den Naming Service oder DHCP zum Vorkonfigurieren Ihres Systems verwenden. Weitere Informationen finden Sie in Kapitel 3, "Vorkonfigurieren mit einem Naming Service oder DHCP".

So erstellen Sie eine sysidcfg-Konfigurationsdatei

- 1 Erstellen Sie eine Datei mit der Bezeichnung sysidcfg in einem Texteditor, und geben Sie die gewünschten Schlüsselwörter ein.
- 2 Stellen Sie die Datei sysidcfg den Clients zur Verfügung, indem Sie einen der in Tabelle 2–2 beschriebenen Speicherorte verwenden.

Beispiel 2–1 SPARC: sysidcfg-Datei

Im Folgenden sehen Sie eine sysidcfg-Beispieldatei für ein SPARC-System. Host-Name, IP-Adresse und Netzmaske dieses Systems wurden durch Bearbeitung des Naming Service vorkonfiguriert. Da alle Systemkonfigurationsinformationen in dieser Datei vorkonfiguriert sind, können Sie mit einem benutzerdefinierten JumpStart-Profil eine benutzerdefinierte JumpStart-Installation ausführen. In diesem Beispiel wird der NFSv4-Domänename automatisch vom Naming Service abgeleitet. Da das Schlüsselwort service_profile in diesem Beispiel nicht enthalten ist, wird die Konfiguration für die Netzwerkdienste während der Installation nicht geändert.

```
keyboard=US-English
system locale=en US
timezone=US/Central
terminal=sun-cmd
timeserver=localhost
name service=NIS {domain name=marguee.central.example.com
                  name server=nmsvr2(172.31.112.3)}
nfs4 domain=dynamic
root password=m4QPOWNY
network interface=hme0 {hostname=host1
                       default route=172.31.88.1
                       ip address=172.31.88.210
                       netmask=255.255.0.0
                       protocol ipv6=no}
security_policy=kerberos {default_realm=example.com
                          admin server=krbadmin.example.com
                          kdc=kdc1.example.com,
                          kdc2.example.com}
```

Beispiel 2–2 x86: sysidcfg-Datei

Die folgende Beispieldatei sysidofg ist für eine Gruppe von x86-basierten Systemen. In diesem Beispiel wird der NFSv4-Domänenname mit example.com angegeben. Dieser benutzerdefinierte Name überschreibt den Standardnamen. Weiterhin sind in diesem Beispiel die Netzwerkdienste deaktiviert oder auf lokale Verbindungen beschränkt.

Beispiel 2-3 sysidcfg-Datei zur Konfiguration mehrerer Schnittstellen

In der folgenden Beispieldatei sysidcfg sind die Konfigurationsinformationen für die Netzwerkschnittstellen eri0 und eri1 angegeben. Die Schnittstelle eri0 wird als primäre Netzwerkschnittstelle und eri1 als sekundäre Netzwerkschnittstelle konfiguriert. In diesem Beispiel wird der NFSv4-Domänename automatisch vom Naming Service abgeleitet.

```
timezone=US/Pacific
system locale=C
terminal=xterms
timeserver=localhost
network interface=eri0 {primary
                        hostname=host1
                        ip address=192.168.2.7
                        netmask=255.255.255.0
                        protocol ipv6=no
                        default_route=192.168.2.1}
network interface=eri1 {hostname=host1-b
                        ip address=192.168.3.8
                        netmask=255.255.255.0
                        protocol_ipv6=no
                        default route=NONE}
root password=JE2C35JGZi4B2
security policy=none
name service=NIS {domain name=domain.example.com
                  name server=nis-server(192.168.2.200)}
nfs4 domain=dynamic
```

Weitere Informationen:

Fortsetzen der Installation

Wenn Sie die sysidcfg-Datei in einer netzwerkgestützten Installation verwenden möchten, müssen Sie einen Installationsserver einrichten und das System als Installationsclient hinzufügen. Weitere Informationen finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Wenn Sie die sysidcfg-Datei in einer WAN-Boot-Installation verwenden möchten, sind einige zusätzliche Schritte erforderlich. Weitere Informationen finden Sie in Kapitel 10, "WAN-Boot (Übersicht)".

Wenn Sie die sysidcfg-Datei in einer benutzerdefinierten JumpStart-Installation verwenden möchten, müssen Sie ein Profil sowie eine rules.ok-Datei erstellen. Weitere Informationen

finden Sie in Kapitel 2, "Benutzerdefinierte JumpStart-Installation (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

```
Siehe auch Nähere Informationen zur sysidcfg-Datei finden Sie auf der Manpage sysidcfg(4).
```

Syntaxregeln für die Datei sysidcfg

In der Datei sysidcfg können Sie zwei Typen von Schlüsselwörtern verwenden: abhängige und unabhängige. Abhängige Schlüsselwörter sind nur innerhalb unabhängiger Schlüsselwörter garantiert eindeutig. Ein abhängiges Schlüsselwort existiert nur, wenn es über das zugehörige unabhängige Schlüsselwort identifiziert wird.

In diesem Beispiel ist name_service das unabhängige Schlüsselwort, domain_name und name server sind die abhängigen Schlüsselwörter:

```
name_service=NIS {domain_name=marquee.central.example.com
name_server=connor(192.168.112.3)}
```

Syntaxregel	Beispiel
Unabhängige Schlüsselwörter können in beliebiger Reihenfolge aufgeführt werden.	pointer=MS-S display=ati {size=15-inch}
Bei Schlüsselwörtern wird nicht zwischen Groß- und Kleinschreibung unterschieden.	TIMEZONE=US/Central terminal=sun-cmd
Stellen Sie alle abhängigen Schlüsselwörter in geschweifte Klammern ({}), um sie mit dem zugehörigen unabhängigen Schlüsselwort zu verbinden.	<pre>name_service=NIS {domain_name=marquee.central.example.com name_server=connor(192.168.112.3)}</pre>
Werte können Sie wahlweise in Hochkommas (') oder Anführungszeichen (") stellen.	<pre>network_interface='none'</pre>
Für alle Schlüsselwörter außer network_interface gilt, dass nur je eine Instanz eines Schlüsselworts gültig ist. Wenn Sie ein Schlüsselwort mehr als einmal angeben, wird nur die erste Instanz verwendet.	name_service=NIS name_service=DNS

Schlüsselwörter in der Datei sysidcfg

In Tabelle 2–3 sind die Schlüsselwörter zur Konfiguration der Systeminformationen in der Datei sysidcfg aufgeführt.

Konfigurationsinformationen	Schlüsselwort
Tastaturlayout und -sprache	"Das Schlüsselwort keyboard" auf Seite 28
Naming Service, Domänename, Namenserver	"Das Schlüsselwort name_service" auf Seite 29
Netzwerkschnitt- stelle, Host-Name, IP-Adresse (Internet Protocol), Netzmaske, DHCP, IPv6	"Schlüsselwort network_interface" auf Seite 32
Domänennamendefinition für NFSv4	"nfs4_domain-Schlüsselwort" auf Seite 38
Root-Passwort	"Das Schlüsselwort root_password" auf Seite 39
Sicherheitsrichtlinie	"Das Schlüsselwort security_policy" auf Seite 39
Netzwerk-Sicherheitsprofil	"service_profile-Schlüsselwort" auf Seite 40
Sprache für das Installationsprogramm und den Desktop	"Das Schlüsselwort system_locale" auf Seite 41
Terminaltyp	"Das Schlüsselwort terminal" auf Seite 41
Zeitzone	"Das Schlüsselwort timezone" auf Seite 41
Datum und Uhrzeit	"Das Schlüsselwort timeserver" auf Seite 42
Einrichten der automatischen Registrierung	"Schlüsselwort auto_reg" auf Seite 23

 TABELLE 2-3
 In sysidcfg zu verwendende Schlüsselwörter

In den folgenden Abschnitten sind die Schlüsselwörter beschrieben, die Sie in der Datei sysidcfg verwenden können.

Schlüsselwort auto_reg

Ab Oracle Solaris 10 9/10 können Sie mit dem Schlüsselwort auto_reg die automatische Registrierung einrichten oder deaktivieren.

Was ist die automatische Registrierung?

Die automatische Registrierung von Oracle Solaris ist neu in Oracle Solaris 10 9/10. Wenn Sie Ihr System installieren oder aufrüsten, werden beim Neustart Konfigurationsdaten Ihres Systems automatisch über die vorhandene Service-Tag-Technologie an das Oracle-Produktregistrierungssystem weitergeleitet. Diese Service-Tag-Daten über Ihr System helfen Oracle beispielsweise bei der Verbesserung von Kunden-Support und -Service. Weitere Informationen zu Service-Tags finden Sie unter http://wikis.sun.com/display/ ServiceTag/Sun+Service+Tag+FAQ.

Sie können dieselben Konfigurationsdaten zum Erstellen und Verwalten Ihres eigenen Systeminventars verwenden. Wenn Sie sich über eine der nachstehenden Registrierungsoptionen mit Ihren Support-Berechtigungsnachweisen registrieren, verfügen Sie über eine einfache Möglichkeit, Ihre eigenen Systeme zu inventarisieren, indem Sie die Service-Tags für die Systeme und die auf den Systemen installierten Softwareprodukte aufzeichnen und verfolgen. Anweisungen zum Verfolgen Ihrer registrierten Produkte finden Sie unter http://wikis.sun.com/display/SunInventory/Sun+Inventory.

Sie können angeben, dass die Konfigurationsdaten anonym an das Oracle-Produktregistrierungssystem gesendet werden, sodass über die an Oracle gesendeten Konfigurationsdaten keine Verbindung zum Namen des Kunden hergestellt werden kann. Außerdem haben Sie die Möglichkeit, die automatische Registrierung zu deaktivieren.

Weitere Informationen zur automatischen Registrierung finden Sie unter "Automatische Registrierung von Oracle Solaris" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Schlüsselwort auto_reg

Mit dem Schlüsselwort auto_reg in der Datei sysidcfg können Sie vor einer automatischen Installation oder einem automatischen Upgrade Ihre Support-Berechtigungsnachweise für die automatische Registrierung bereitstellen, eine anonyme Registrierung festlegen oder die automatische Registrierung deaktivieren. Wenn Sie diese Schlüsselwörter in der Datei sysidcfg nicht festlegen, werden Sie zur Eingabe Ihrer Berechtigungsnachweise aufgefordert oder müssen sich während der Installation oder dem Upgrade registrieren.

Im folgenden Beispiel sehen Sie die allgemeine Syntax für das Schlüsselwort auto_reg.

```
auto_reg=[anon |none |noproxy |all |disable ] {
oracle_user=username
oracle_pw=oracle-password
http_proxy_host=hostname
http_proxy_port=port-number
http_proxy_user=proxy-username
htty_proxy_pw=proxy-password
}
```

Geben Sie für die Verwendung dieses Schlüsselworts zunächst einen grundlegenden Registrierungstyp an, indem Sie einen der folgenden Werte auswählen: anon, none, noproxy, all oder disable (siehe Beschreibung in der folgenden Tabelle). Geben Sie anschließend mit den folgenden weiteren Schlüsselwörtern spezifische My Oracle Support-Berechtigungsnachweise sowie Ihre Proxy-Informationen für die automatische Registrierung an.

Schlüsselwort	Werte
auto_reg	auto_reg lautet das primäre Schlüsselwort. Verwenden Sie eines der folgenden Werte für dieses Schlüsselwort, um die zu verwendende Art der automatischen Registrierung anzugeben.
	Anonyme Registrierung – Werte anon oder none
	 Bei Verwendung des Werts anon oder none werden die Service-Tags anonym bei Oracle registriert. Eine anonyme Registrierung bedeutet, dass über die an Oracle gesendeten Konfigurationsdaten keine Verbindung zum Namen eines Kunden oder einer Person hergestellt werden kann. Wenn My Oracle Support-Berechtigungsnachweise während der Installation bereitgestellt werden, werden diese Berechtigungsnachweise ignoriert und die Registrierung bleibt anonym. Wenn Sie Proxy-Informationen entweder in der Datei sysidcfg oder bei entsprechender Aufforderung während der Installation oder dem Upgrade bereitstellen möchten, verwenden Sie den Wert anon.
	 Wenn Sie keine Proxy-Informationen in der Datei sysidcfg bereitstellen möchten, verwenden Sie den Wert none. Dadurch werden die während einer Installation oder eines Upgrades bereitgestellten Proxy-Informationen ignoriert.
	Registrierung mit Support-Berechtigungsnachweisen – Werte noproxy oder all
	Bei Verwendung des Werts noproxy oder all werden die Service-Tags mithilfe Ihrer My Oracle Support-Berechtigungsnachweise bei Oracle registriert, wenn Sie das System nach einer Installation oder einem Upgrade neu starten. Die My Oracle Support-Berechtigungsnachweise müssen Sie entweder in der Datei sysidcfg oder bei entsprechender Aufforderung während der Installation oder dem Upgrade angeben.
	 Wenn Sie Proxy-Informationen entweder in der Datei sysidcfg oder bei entsprechender Aufforderung während der Installation oder dem Upgrade bereitstellen möchten, verwenden Sie den Wert all.
	 Wenn Sie keine Proxy-Informationen in der Datei sysidcfg bereitstellen möchten, verwenden Sie den Wert noproxy. Dadurch werden die während einer Installation oder eines Upgrades bereitgestellten Proxy-Informationen ignoriert.
	Deaktivieren der automatischen Registrierung – disable
	Wenn Sie den Wert disable verwenden, wird die automatische Registrierung deaktiviert. Nach einer Deaktivierung müssen Sie die automatische Registrierung mit dem Befehl regadm erneut aktivieren. Weitere Informationen entnehmen Sie bitte der Man Page regadm(1M).

TABELLE 2-4	auto	reg – Schlüsselwö	rter und Werte
-------------	------	-------------------	----------------

Weitere Beispiele für diese Werte finden Sie in den folgenden Abschnitten.

Schlüsselwort	Werte
Sekundäre Schlüsselwörter:	Verwenden Sie die folgenden Schlüsselwörter und Werte im Hauptschlüsselwort auto_reg, um entweder My Oracle Support-Berechtigungsnachweise oder Proxy-Informationen bereitzustellen.
oracle_user	username – Geben Sie Ihren My Oracle Support-Benutzernamen an. Beispiel: oracle_user=myusername.
oracle_pw	oracle_password – Geben Sie Ihr My Oracle Support-Passwort in einfachem, unverschlüsseltem Text an. Beispiel: oracle_pw=j32js94jrjsW.
http_proxy_host	hostname – Geben Sie Ihren Proxy-Hostname an. Beispiel: http_proxy_host=sss.com.
http_proxy_port	<pre>port_number - Geben Sie Ihren Proxy-Port an. Beispiel: http_proxy_port=8050.</pre>
http_proxy_user	proxy_username – Geben Sie Ihren Proxy-Benutzernamen an. Beispiel: http_proxy_user=proxyusername.
htty_proxy_pw	proxy_password – Geben Sie Ihr Proxy-Passwort in einfachem, unverschlüsseltem Text an. Beispiel: http_proxy_pw=sej47875WSjs.

 TABELLE 2-4
 auto_reg - Schlüsselwörter und Werte
 (Fortsetzung)

Diese Informationen finden Sie auch auf der Man Page sysidcfg(4).

Beispiele für anonyme Registrierung

Verwenden Sie die Werte anon oder none für die anonyme Registrierung. Eine anonyme Registrierung bedeutet, dass über die an Oracle gesendeten Konfigurationsdaten keine Verbindung zum Namen eines Kunden oder einer Person hergestellt werden kann. Wenn My Oracle Support-Berechtigungsnachweise während der Installation bereitgestellt werden, werden diese Berechtigungsnachweise ignoriert und die Registrierung bleibt anonym.

Weitere Informationen zur Angabe von Proxy-Informationen finden Sie unter dem Wert anon. Wenn Sie keine Proxy-Informationen angeben möchten, verwenden Sie den Wert none.

Im folgenden Beispiel bedeutet der Wert anon, dass Ihre Service-Tags anonym bei Oracle registriert werden. Sie müssen Proxy-Informationen entweder in der Datei sysidcfg angeben (siehe folgendes Beispiel) oder bei entsprechender Aufforderung während der Installation oder dem Upgrade.

```
auto_reg=anon {
http_proxy_host=sss.com
http_proxy_port=8040
http_proxy_user=myproxyusername
htty_proxy_pw=si329jehId
}
```

Im folgenden Beispiel wird durch den Wert none festgelegt, dass Ihre Service-Tags anonym bei Oracle registriert wurden und dass Sie keine Proxy-Informationen angeben möchten. Dadurch werden die während einer Installation oder eines Upgrades bereitgestellten Proxy-Informationen ignoriert.

auto_reg=none

Beispiele für Registrierung mit Support-Berechtigungsnachweisen

Durch den Wert noproxy oder all werden Ihre Service-Tags mithilfe der My Oracle Support-Berechtigungsnachweise bei Oracle registriert, wenn Sie das System nach einer Installation oder einem Upgrade neu starten.

Weitere Informationen zur Angabe von Proxy-Informationen finden Sie unter dem Wert all. Wenn Sie keine Proxy-Informationen angeben möchten, verwenden Sie den Wert noproxy. Betrachten Sie hierzu folgende Beispiele.

Im folgenden Beispiel bedeutet der Wert all, dass Ihre Service-Tags mithilfe der My Oracle Support-Berechtigungsnachweise bei Oracle registriert werden, wenn Sie das System nach einer Installation oder einem Upgrade neu starten. Die My Oracle Support-Berechtigungsnachweise müssen Sie wie in diesem Beispiel beschrieben oder bei entsprechender Aufforderung während der Installation oder dem Upgrade angeben. Durch Verwendung des Werts all müssen Sie die Proxy-Informationen wie im folgenden Beispiel beschrieben oder bei entsprechender Aufforderung während der Installation oder dem Upgrade angeben.

```
auto_reg=all {
  oracle_user=myusername
  oracle_pw=ajsi349EKS987
  http_proxy_host=sss.com
  http_proxy_port=8030
  http_proxy_user=myproxyusername
  htty_proxy_pw=adjsi2934IEls
 }
```

Im folgenden Beispiel bedeutet der Wert noproxy, dass Ihre Service-Tags mithilfe der My Oracle Support-Berechtigungsnachweise bei Oracle registriert werden, wenn Sie das System nach einer Installation oder einem Upgrade neu starten. Die My Oracle Support-Berechtigungsnachweise müssen Sie wie im folgenden Beispiel beschrieben oder bei entsprechender Aufforderung während der Installation oder dem Upgrade angeben. Da Sie jedoch den Wert noproxy verwendet haben, brauchen Sie keine Proxy-Informationen anzugeben. Dadurch werden die während einer Installation oder eines Upgrades bereitgestellten Proxy-Informationen ignoriert.

```
auto_reg=noproxy {
oracle_user=myusername
oracle_pw=sie7894KEdjs2
}
```

Beispiel für Deaktivieren der automatischen Registrierung

Im folgenden Beispiel wird durch den Wert disable festgelegt, dass die automatische Registrierung deaktiviert ist. Mit dem Befehl regadm aktivieren Sie die automatische Registrierung erneut. Weitere Informationen entnehmen Sie bitte der Man Page regadm (1M).

auto_reg=disable

Das Schlüsselwort keyboard

Das Tool sysidkdb konfiguriert Ihre USB-Sprache und das entsprechende Tastaturlayout.

Dabei wird das folgende Verfahren ausgeführt:

- Wenn sich die Tastatur selbst identifiziert, werden Tastatursprache und -layout während der Installation automatisch konfiguriert.
- Bei Tastaturen ohne Selbsterkennung zeigt das Tool sysidkdb während der Installation eine Liste der unterstützten Tastaturlayouts an, damit Sie für die Tastaturkonfiguration ein Layout auswählen können.

Hinweis – PS/2-Tastaturen können sich nicht selbst konfigurieren. Sie werden aufgefordert, das Tastaturlayout während der Installation auszuwählen.

Sie können die Tastatursprache und die entsprechenden Tastaturlayoutinformationen mithilfe des Schlüsselwortes keyboard konfigurieren. Jede Sprache hat ein eigenes Tastaturlayout. Mit dem folgenden Befehl wählen Sie die Sprache und das entsprechende Layout.

keyboard=keyboard_layout

Der folgende Eintrag stellt beispielsweise Deutsch als Tastatursprache und das entsprechende Tastaturlayout für die deutsche Sprache ein:

keyboard=German

Der für *Tastaturlayout* verwendete Wert muss gültig sein. Anderenfalls ist eine Interaktion während der Installation erforderlich. Die gültigen Werte für *Tastaturlayout* sind in der Datei /usr/share/lib/keytables/type_6/kbd_layouts definiert.

SPARC nur – In früheren Versionen hat eine USB-Tastatur während der Installation den Selbstidentifikationswert 1 angenommen. Aus diesem Grund wurden alle Tastaturen, die sich nicht selbst identifizierten, während der Installation mit U.S.-amerikanischem Layout konfiguriert. Wenn sich die Tastatur nicht selbst identifiziert und Sie verhindern möchten, dass die Eingabeaufforderung während der JumpStart-Installationsmethode angezeigt wird, müssen Sie die Tastatursprache in der Datei sysidcfg auswählen. Bei der JumpStart-Installationsmethode wird standardmäßig die Sprache U.S. Englisch installiert. Um eine andere Sprache und das entsprechende Tastaturlayout auszuwählen, legen Sie den Tastatureintrag in Ihrer sysidcfg-Datei wie im oben stehenden Beispiel gezeigt fest.

Weitere Informationen finden Sie in den Manpages sysidcfg(4) und sysidtool (1M).

Das Schlüsselwort name_service

Mit dem Schlüsselwort name_service können Sie den Naming Service, den Domänennamen und den Namenserver für das System konfigurieren. In folgendem Beispiel sehen Sie die allgemeine Syntax für das Schlüsselwort name_service.

Wählen Sie nur einen Wert für name_service. Fügen Sie je nach Bedarf alle oder auch keines der Schlüsselwörter domain_name,name_server und der optionalen Schlüsselwörter ein. Wenn Sie kein Schlüsselwort verwenden, lassen Sie die geschweiften Klammern ({}) weg.

Hinweis – Die Option name_service in der Datei sysidcfg richtet den Naming Service automatisch während der Installation des Betriebssystems Solaris ein. Diese Einstellung hat Vorrang vor den SMF-Services, die zuvor für site.xml eingerichtet wurden. Aus diesem Grund müssen Sie Ihren Naming Service nach der Installation eventuell zurücksetzen.

In den nachfolgenden Abschnitten wird die Schlüsselwortsyntax zum Konfigurieren des Systems für einen bestimmten Naming Service dargestellt.

NIS-Syntax für das Schlüsselwort name service

Mit der folgenden Syntax konfigurieren Sie ein System für die Verwendung des NIS-Naming Service.

name_service=NIS	<pre>{domain_name=domain-name name_server=hostname(ip-address)}</pre>
Domain-Name	Gibt den Domain-Namen an
Host-Name	Gibt den Host-Namen des Namenservers an
IP-Adresse	Gibt die IP-Adresse des Namenservers an

BEISPIEL 2-4 Angeben eines NIS-Servers mit dem Schlüsselwort name_service

Im folgenden Beispiel wird ein NIS-Server mit dem Domain-Namen west.example.com angegeben. Der Host-Name des Servers lautet timber und dessen IP-Adresse 192.168.2.1.

Weitere Informationen zum NIS-Naming Service finden Sie in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).*

NIS+-Syntax für das Schlüsselwort name_service

Mit der folgenden Syntax konfigurieren Sie ein System für die Verwendung des NIS-Namen-Service.

name_service=NIS+	<pre>{domain_name=domain-name name_server=hostname(ip-address)}</pre>
Domain-Name	Gibt den Domain-Namen an
Host-Name	Gibt den Host-Namen des Namenservers an
IP-Adresse	Gibt die IP-Adresse des Namenservers an

BEISPIEL 2-5 Angeben eines NIS+-Servers mit dem Schlüsselwort name_service

Im folgenden Beispiel wird ein NIS+-Server mit dem Domain-Namen west.example.com angegeben. Der Host-Name des Servers lautet timber und dessen IP-Adresse 192.168.2.1.

Weitere Informationen zum NIS+-Naming Service finden Sie in *System Administration Guide: Naming and Directory Services (NIS+).*

DNS-Syntax für das Schlüsselwort name_service

Mit der folgenden Syntax konfigurieren Sie das System für die Verwendung von DNS.

domain_name=*Domain-Name* Gibt den Domain-Namen an.

name_server=IP-Adresse	Gibt die IP-Adresse des DNS-Servers an. Sie können bis zu drei IP-Adressen als Werte für das Schlüsselwort name_server angeben.
search=Domain-Name	(Optional) Gibt zusätzliche Domains an, die nach Naming Service-Informationen durchsucht werden sollen. Sie können die Namen von bis zu sechs zu durchsuchenden Domains angeben. Die Gesamtlänge eines Sucheintrags darf 250 Zeichen nicht überschreiten.

BEISPIEL 2-6 Angeben eines DNS-Servers mit dem Schlüsselwort name_service

Im folgenden Beispiel wird ein DNS-Server mit dem Domain-Namen west.example.com angegeben. Die IP-Adressen des Servers lauten 10.0.1.10 und 10.0.1.20.example.com und east.example.com werden als zusätzlich nach Naming Service-Informationen zu durchsuchende Domains aufgeführt.

Weitere Informationen zum DNS-Naming Service finden Sie in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).*

LDAP-Syntax für das Schlüsselwort name service

Mit der folgenden Syntax konfigurieren Sie das System für die Verwendung von LDAP.

name_service=LDAP	<pre>{domain_name=domain_name profile=profile_name profile_server=ip_address proxy_dn="proxy_bind_dn" proxy_password=password}</pre>
Domain-Name	Gibt den Domain-Namen des LDAP-Servers an.
Profilname	Gibt den Namen des LDAP-Profils an, das Sie zur Konfiguration des Systems verwenden möchten.
IP-Adresse	Gibt die IP-Adresse des LDAP-Profilservers an.
Proxy-Bind-DN	(Optional) Gibt den Proxy-Bind-DN (Distinguished Name) an. Der Wert <i>Proxy-Bind-DN</i> muss in doppelte Hochkommas gesetzt werden.
Passwort	(Optional) Gibt das Client-Passwort für den Proxy an.

BEISPIEL 2-7 Angeben eines LDAP-Servers mit dem Schlüsselwort name_service

Im nachfolgenden Beispiel wird ein LDAP-Server mit den folgenden Konfigurationsinformationen angegeben:

BEISPIEL 2-7 Angeben eines LDAP-Servers mit dem Schlüsselwort name_service (Fortsetzung)

- Der Domain-Name lautet west.example.com.
- Das Installationsprogramm konfiguriert das System auf Grundlage des LDAP-Profils mit dem Namen default.
- Die IP-Adresse des LDAP-Servers lautet 172.31.2.1.
- Der Proxy-Bind-DN umfasst die folgenden Informationen:
 - Der gemeinsame Name f
 ür den Eintrag lautet proxyagent.
 - Die organisatorische Einheit ist profile.
 - Die Proxydomain beinhaltet die Domain-Komponenten west, example und com.
- Das Proxy-Passwort lautet password.

```
name_service=LDAP {domain_name=west.example.com
    profile=default
    profile_server=172.31.2.1
    proxy_dn="cn=proxyagent,ou=profile,
    dc=west,dc=example,dc=com"
    proxy_password=password}
```

Weitere Informationen zur Verwendung von LDAP finden Sie in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).*

Schlüsselwort network_interface

Verwenden Sie das Schlüsselwort network_interface für die folgenden Vorgänge.

- Angeben eines Host-Namens
- Angeben einer IP-Adresse
- Angeben der Standard-Routeradresse
- Angeben eines Netzmaskenwerts
- Konfigurieren der Netzwerkschnittstelle mit DHCP
- Aktivieren von IPv6 auf der Netzwerkschnittstelle

In den folgenden Abschnitten erfahren Sie, wie Sie mit dem Schlüsselwort network_interface die Systemschnittstellen konfigurieren.

Syntax für nicht vernetzte Systeme

Zum Deaktivieren der Netzwerkfunktion des Systems setzen Sie den Wert von network_interface auf none. Beispiel:

network_interface=none

Syntax für die Konfiguration einer einzelnen Schnittstelle

network interface=PRIMARY or value

Eine einzelne Schnittstelle lässt sich mithilfe des Schlüsselworts network_interface auf folgende Arten konfigurieren:

 Mit DHCP – Sie können einen DHCP-Server in Ihrem Netzwerk einsetzen, um die Netzwerkschnittstelle zu konfigurieren. Informationen zur Verwendung eines DHCP-Servers während der Installation finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Verwenden Sie folgende Syntax für das Schlüsselwort network_interface, wenn Sie eine einzelne Schnittstelle des Systems mithilfe des DHCP-Servers konfigurieren möchten.

{dhcp prot	ocol_ipv6= <i>yes-or-no</i> }
PRIMARY	Weist das Installationsprogramm an, die erste funktionsbereite Schnittstelle zu konfigurieren, die im System gefunden wird und keine Loopback-Schnittstelle ist. Die Reihenfolge ist mit der Reihenfolge in der Anzeige des Befehls ifconfig identisch. Wenn keine funktionsbereite Schnittstelle vorhanden ist, wird die erste Nicht-Loopback-Schnittstelle konfiguriert. Wird keine Nicht-Loopback-Schnittstelle gefunden, bleibt das System unvernetzt.
Wert	Weist das Installationsprogramm an, eine spezifische Schnittstelle wie beispielsweise hme0 oder eri1 zu konfigurieren.
protocol_ipv6= <i>yes-oder-no</i>	Weist das Installationsprogramm an, in der Systemkonfiguration festzulegen, ob das System mit IPv6 arbeitet oder nicht.
	Bei WAN-Boot-Installationen muss der Wert protocol_ipv6=no gesetzt werden.

 Ohne DHCP – Wenn Sie DHCP nicht zum Konfigurieren der Netzwerkschnittstelle verwenden möchten, können Sie die Konfigurationsinformationen in der Datei sysidcfg festlegen. Verwenden Sie die folgende Syntax, um das Installationsprogramm anzuweisen, eine einzelne Schnittstelle des Systems ohne DHCP zu konfigurieren.

```
network_interface=PRIMARY or value
    {hostname=host_name
    default_route=ip_address
    ip_address=ip_address
    netmask=netmask
    protocol_ipv6=yes_or_no}
```

PRIMARY

Weist das Installationsprogramm an, die erste funktionsbereite Schnittstelle zu konfigurieren, die

	im System gefunden wird und keine Loopback-Schnittstelle ist. Die Reihenfolge ist mit der Reihenfolge in der Anzeige des Befehls ifconfig identisch. Wenn keine funktionsbereite Schnittstelle vorhanden ist, wird die erste Nicht-Loopback-Schnittstelle konfiguriert. Wird keine Nicht-Loopback-Schnittstelle gefunden, bleibt das System unvernetzt.
	Hinweis – Verwenden Sie das Schlüsselwort PRIMARY nicht zur Konfiguration mehrerer Schnittstellen.
Wert	Weist das Installationsprogramm an, eine spezifische Schnittstelle wie beispielsweise hme0 oder eri1 zu konfigurieren.
hostname=Host-Name	(Optional) Gibt den Host-Namen des Systems an.
default_route= <i>IP_Adresse</i> or NONE	(Optional) Gibt die IP-Adresse des Standard-Routers an. Wenn Sie möchten, dass das Installationsprogramm den Router mithilfe des ICMP-Router-Ermittlungsprotokolls automatisch ermittelt, geben Sie dieses Schlüsselwort nicht an.
	Hinweis – Sollte das Installationsprogramm den Router nicht ermitteln können, werden Sie während der Installation zur Eingabe der Router-Informationen aufgefordert.
ip address=IP-Adresse	(Optional) Gibt die IP-Adresse des Systems an.
netmask= <i>Netzmaske</i>	(Optional) Gibt den Netzmaskenwert für das System an.
protocol_ipv6= <i>yes_oder_no</i>	(Optional) Weist das Installationsprogramm an, in der Systemkonfiguration festzulegen, ob das System mit IPv6 arbeitet oder nicht.

Hinweis – Für eine ungeführte benutzerdefinierte JumpStart-Installation müssen Sie einen Wert für das Schlüsselwort protocol_ipv6 angeben.

Bei WAN-Boot-Installationen muss der Wert protocol_ipv6=no gesetzt werden.

Je nach Bedarf können Sie eine beliebige Kombination oder keines der Schlüsselwörter hostname, ip_address und netmask angeben. Wenn Sie keins der Schlüsselwörter verwenden, lassen Sie die geschweiften Klammern ({}) weg.

BEISPIEL 2-8 Konfiguration einer einzelnen Schnittstelle mithilfe von DHCP und dem Schlüsselwort network_interface

Im folgenden Beispiel wird das Installationsprogramm angewiesen, die Netzwerkschnittstelle eri0 mithilfe von DHCP zu konfigurieren. Die IPv6-Unterstützung wird nicht aktiviert.

network_interface=eri0 {dhcp protocol_ipv6=no}

BEISPIEL 2-9 Konfiguration einer einzelnen Schnittstelle durch Angabe von Konfigurationsinformationen mit dem Schlüsselwort network_interface

In diesem Beispiel wird die Schnittstelle eri@mit den folgenden Einstellungen konfiguriert:

- Der Host-Name wird auf host1 gesetzt.
- Die IP-Adresse wird auf 172.31.88.100 gesetzt.
- Die Netzmaske wird auf 255.255.255.0 gesetzt.
- Die IPv6-Unterstützung wird an der Schnittstelle nicht aktiviert.

Syntax für die Konfiguration mehrerer Schnittstellen

In der sysidcfg-Datei können mehrere Netzwerkschnittstellen konfiguriert werden. Fügen Sie für jede zu konfigurierende Schnittstelle einen network_interface-Eintrag in die Datei sysidcfg ein.

Mit dem Schlüsselwort network_interface können Sie mehrere Schnittstellen auf folgende Arten konfigurieren:

 Mit DHCP – Sie können einen DHCP-Server in Ihrem Netzwerk einsetzen, um eine Netzwerkschnittstelle zu konfigurieren. Informationen zur Verwendung eines DHCP-Servers während der Installation finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52. Verwenden Sie folgende Syntax für das Schlüsselwort network_interface, wenn Sie eine Netzwerkschnittstelle des Systems mithilfe des DHCP-Servers konfigurieren möchten.

network_interface= <i>value</i> {prim dh	ary cp protocol_ipv6= <i>yes-or-no</i> }
Wert	Weist das Installationsprogramm an, eine spezifische Schnittstelle wie beispielsweise hme0 oder eri1 zu konfigurieren.
primary	(Optional) Gibt Wert als primäre Schnittstelle an.
protocol_ipv6= <i>yes-oder-no</i>	Weist das Installationsprogramm an, in der Systemkonfiguration festzulegen, ob das System mit IPv6 arbeitet oder nicht.
	Hinweis – Bei WAN-Boot-Installationen muss der Wert protocol ipv6=no gesetzt werden.

 Ohne DHCP – Wenn Sie DHCP nicht zum Konfigurieren der Netzwerkschnittstelle verwenden möchten, können Sie die Konfigurationsinformationen in der Datei sysidcfg festlegen. Verwenden Sie die folgende Syntax, um das Installationsprogramm anzuweisen, mehrere Schnittstellen ohne DHCP zu konfigurieren.

<pre>network_interface=value {primary hostname=host_name</pre>		
Wert	Weist das Installationsprogramm an, eine spezifische Schnittstelle wie beispielsweise hme oder eril zu konfigurieren.	90≘
primary	(Optional) Gibt <i>Wert</i> als primäre Schnittstelle an.	Ż
hostname=Host-Name	(Optional) Gibt den Host-Namen des Systems an.	5
default_route= <i>IP_Adresse</i> or N	NE (Optional) Gibt die IP-Adresse des Standard-Routers an. Wenn Sie möchten, das das Installationsprogramm den Router mithil des ICMP-Router-Ermittlungsprotokolls automatisch ermittelt, geben Sie dieses Schlüsselwort nicht an.	s fe
	Wenn Sie in der Datei sysidcfg mehrere Schnittstellen konfigurieren, setzen Sie	
defeult neute NONE für alle selven dären

	Schnittstellen, die keine statische Standard-Route verwenden.		
	Hinweis – Sollte das Installationsprogramm den Router nicht ermitteln können, werden Sie während der Installation zur Eingabe der Router-Informationen aufgefordert.		
ip_address= <i>IP-Adresse</i>	(Optional) Gibt die IP-Adresse des Systems an.		
netmask= <i>Netzmaske</i>	(Optional) Gibt den Netzmaskenwert für das System an.		
protocol_ipv6= <i>yes_oder_no</i>	(Optional) Weist das Installationsprogramm an in der Systemkonfiguration festzulegen, ob das System mit IPv6 arbeitet oder nicht.		
	Hinweis – Für eine ungeführte benutzerdefinierte JumpStart-Installation müssen Sie einen Wert für das Schlüsselwort protocol_ipv6 angeben.		
	Bei WAN-Boot-Installationen muss der Wert protocol_ipv6=no gesetzt werden.		

Je nach Bedarf können Sie eine beliebige Kombination oder keines der Schlüsselwörter hostname, ip_address und netmask angeben. Wenn Sie keins der Schlüsselwörter verwenden, lassen Sie die geschweiften Klammern ({}) weg.

In derselben sysidcfg-Datei können Sie bestimmte Schnittstellen per DHCP konfigurieren lassen und für andere Schnittstellen die Konfigurationsinformationen direkt in der Datei angeben.

 $\textbf{BEISPIEL 2-10} \quad \text{Konfiguration mehrerer Schnittstellen mit dem Schlüsselwort network_interface}$

In diesem Beispiel werden die Netzwerkschnittstellen eri0 und eri1 wie folgt konfiguriert.

- eri0 wird mithilfe des DHCP-Servers konfiguriert. Die IPv6-Unterstützung wird auf eri0 nicht aktiviert.
- eril ist die primäre Netzwerkschnittstelle. Der Host-Name wird auf host1, die IP-Adresse auf 172.31.88.100 und die Netzmaske auf 255.255.255.0 gesetzt. Die IPv6-Unterstützung wird auf eril nicht aktiviert.

BEISPIEL 2-10 Konfiguration mehrerer Schnittstellen mit dem Schlüsselwort network_interface (*Fortsetzung*)

nfs4_domain-Schlüsselwort

Geben Sie das Schlüsselwort nfs4_domain in der Datei sysidcfg an, damit Sie während der Installation nicht zur Eingabe eines NFSv4-Domänennamens aufgefordert werden. Dieses Schlüsselwort unterdrückt die Auswahl eines Domänennamens während der Installationsprozesses. Verwenden Sie die folgende Syntax:

nfs4_domain=dynamic or custom_domain_name

dynamic	Dieses reservierte Schlüsselwort leitet den NFSv4-Domänennamen dynamisch von der Naming Services-Konfiguration ab. Beispiel:		
	nfs4_domain=dynamic		
	In diesem Beispiel wird der Domänenname vom Naming Service abgeleitet.		
	Das reservierte Schlüsselwort dynamic ist unabhängig von der Groß-/Kleinschreibung.		
	Hinweis – Standardmäßig verwendet NFSv4 einen Domänennamen, der automatisch von den Naming Services des Systems abgeleitet wird. Der Domänenname ist für die meisten Konfigurationen ausreichend. In einigen wenigen Fällen könnten domänenübergreifende Einhängepunkte dazu führen, das Dateien keinen speziellen Eigentümer aufweisen, da kein gemeinsamer Domänenname vorhanden ist. Um eine solche Situation zu vermeiden, können Sie den standardmäßigen Domänennamen außer Kraft setzen und einen benutzerdefinierten Domänennamen auswählen.		
benutzerdefinierter_Domänenname	Dieser Wert setzt den standardmäßigen Domänennamen außer Kraft.		

Bei diesen Wert muss es sich um einen gültigen benutzerdefinierten Domänennamen handeln. Ein gültiger Domänenname setzt sich ausschließlich aus alphanumerischen Zeichen, Punkten, Unterstrichen und Bindestrichen zusammen. Das erste Zeichen muss ein Buchstabe sein. Beispiel:

nfs4_domain=*example.com*

Dieses Beispiel legt den vom nfsmapid-Dämon verwendeten Wert mit *example.com* fest. Diese Auswahl setzt den standardmäßigen Domänennamen außer Kraft.

Hinweis – In vorherigen Versionen wurden Skripten verwendet, damit Benutzer während der Installation nicht zur Eingabe des NFSv4-Domänennamens aufgefordert wurden.

Bei einer JumpStart-Installation unter Solaris 10 können Sie das JumpStart-Beispielskript set_nfs4_domain verwenden, um die NFSv4-Aufforderung während der Installation zu unterdrücken. Dieses Skript ist nicht mehr erforderlich. Verwenden Sie stattdessen das sysidcfg-Schlüsselwort nfs4_domain.

In früheren Versionen wurde die Datei /etc/.NFS4inst_state.domain vom sysidnfs4-Programm erstellt. Diese Datei würde die Aufforderung zur Eingabe eines NFSv4-Domänennamens während der Installation unterdrücken. Diese Datei wird nicht mehr erstellt. Verwenden Sie stattdessen das sysidcfg-Schlüsselwort nfs4_domain.

Das Schlüsselwort root_password

Das Root-Passwort für das System können Sie in der Datei sysidcfg angeben. Verwenden Sie das Schlüsselwort root_password mit der folgenden Syntax, um das Root-Passwort anzugeben:

root_password=encrypted-password

verschlüsseltes_Passwort ist das verschlüsselte Passwort, wie es in der Datei /etc/shadow erscheint.

Das Schlüsselwort security_policy

Sie können das Schlüsselwort security_policy in der Datei sysidcfg angeben, um das System für die Verwendung des Netzwerk-Authentifizierungsprotokolls Kerberos zu konfigurieren. Wenn Sie das System für die Verwendung von Kerberos konfigurieren möchten, verwenden Sie folgende Syntax:

FQDN gibt den vollständig qualifizierten Domain-Namen des Kerberos-Standardbereichs, den Administrationsserver oder das KDC (Key Distribution Center) an. Sie müssen mindestens ein und maximal drei KDCs angeben.

Wenn Sie diese Sicherheitsrichtlinie nicht für das System festlegen möchten, setzen Sie security_policy=NONE.

Weitere Informationen zum Netzwerk-Authentifizierungsprotokoll Kerberos finden Sie in *System Administration Guide: Security Services*.

BEISPIEL 2-11 Konfiguration des Systems für die Verwendung von Kerberos mit dem Schlüsselwort security_policy

In diesem Beispiel wird das System mit den folgenden Informationen für die Verwendung von Kerberos konfiguriert:

- Der Kerberos-Standardbereich lautet example.com.
- Der Kerberos-Administrationsserver lautet krbadmin.example.com.
- Die zwei KDCs sind kdc1.example.com und kdc2.example.com.

```
security_policy=kerberos
```

```
{default_realm=example.COM
  admin_server=krbadmin.example.com
  kdc=kdc1.example.com,
  kdc2.example.com}
```

service_profile-Schlüsselwort

Mit dem Schlüsselwort service_profile können Sie ein sichereres System installieren, indem Sie die Netzwerkdienste einschränken. Diese Sicherheitsfunktion steht nur bei der Erstinstallation zur Verfügung. Bei einem Upgrade werden alle zuvor eingerichteten Dienste beibehalten.

Verwenden Sie eine der folgenden Syntax-Optionen, um dieses Schlüsselwort einzurichten.

```
service_profile=limited_net
```

service_profile=open

limited_net legt fest, dass alle Netzwerkdienste (mit Ausnahme von Secure Shell) entweder deaktiviert oder so eingerichtet werden, dass sie nur auf lokale Anfragen reagieren. Nach der Installation können einzelne Netzwerkdienste mithilfe der Befehle svcadm und svccfg aktiviert werden.

open legt fest, dass keine Änderungen an Netzwerkdiensten während der Installation vorgenommen werden.

Wenn das Schlüsselwort service_profile nicht in der Datei sysidcfg angegeben ist, werden während der Installation keine Änderungen am Status der Netzwerkdienste vorgenommen.

Die Netzwerkdienste können nach der Installation entweder mithilfe des Befehls netservices open aktiviert werden, oder Sie aktivieren einzelne Dienste mithilfe von SMF-Befehlen. Siehe "Ändern der Sicherheitseinstellungen nach der Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Weitere Informationen zum Einschränken der Netzwerksicherheit während der Installation finden Sie unter "Planung der Netzwerksicherheit" in *Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades*. Siehe auch die folgenden Manpages:

- netservices(1M)
- svcadm(1M)
- svccfg(1M)-Befehle

Das Schlüsselwort system_locale

Mit dem Schlüsselwort system_locale lässt sich die Sprache angeben, in der das Installationsprogramm und der Desktop angezeigt werden sollen. Zum Angeben einer Sprachumgebung verwenden Sie die folgende Syntax.

system_locale=locale

Sprachumgebung gibt die Sprache an, in der das System die Installationsmeldungen und Fenster anzeigen soll. Eine Liste der gültigen Werte für die Sprachumgebung finden Sie im Verzeichnis /usr/lib/locale oder im *International Language Environments Guide*.

Das Schlüsselwort terminal

Mit dem Schlüsselwort terminal können Sie einen Terminaltyp für das System angeben. Zum Angeben eines Terminaltyps verwenden Sie die folgende Syntax:

terminal=terminal_type

Terminaltyp gibt den Terminaltyp für das System an. Eine Liste der gültigen Terminalwerte finden Sie in den Unterverzeichnissen von /usr/share/lib/terminfo.

Das Schlüsselwort timezone

Mit dem Schlüsselwort timezone lässt sich die Zeitzone des Systems festlegen. Verwenden Sie die folgende Syntax.

timezone=*timezone*

In diesem Beispiel gibt *Zeitzone* den Zeitzonenwert für das System an. In den Verzeichnissen und Dateien im Verzeichnis /usr/share/lib/zoneinfo finden Sie gültige Werte für die Zeitzone. Der Wert *Zeitzone* ist der Pfadname relativ zum Verzeichnis /usr/share/lib/zoneinfo. Sie können außerdem jede gültige Olson-Zeitzone angeben.

BEISPIEL 2-12 Konfiguration der Systemzeitzone mit dem Schlüsselwort timezone

Im folgenden Beispiel wird die Zeitzone auf die US-amerikanische Mountain-Standardzeit gesetzt.

timezone=US/Mountain

Das Installationsprogramm konfiguriert das System so, dass es die Zeitzoneninformationen in /usr/share/lib/zoneinfo/US/Mountain verwendet.

Das Schlüsselwort timeserver

Mit dem Schlüsselwort timeserver können Sie das System angeben, von dem das zu installierende System Datums- und Uhrzeitinformationen erhalten soll.

Wählen Sie eine der folgenden Methoden zum Setzen des Schlüsselworts timeserver:

- Setzen Sie timeserver=localhost, damit das System sich selbst als Zeitserver dient. Wenn Sie localhost als Zeitserver angeben, wird die Systemuhrzeit als die richtige Uhrzeit angenommen.
- Um ein anderes System als Zeitserver festzulegen, geben Sie mit dem Schlüsselwort timeserver entweder den Host-Namen oder die IP-Adresse des Zeitservers an. Verwenden Sie die folgende Syntax.

timeserver=hostname or ip-address

Host-Name ist der Host-Name des Zeitserversystems. *IP-Adresse* gibt die IP-Adresse des Zeitservers an.

SPARC: Vorkonfigurieren der Power Management-Informationen

Mithilfe der als Bestandteil von Solaris gelieferten *Power Management*-Software können Sie nach 30 Minuten Leerlauf den Systemstatus automatisch speichern und das System abschalten lassen. Wenn Sie die aktuelle Solaris-Release auf einem System installieren, das Version 2 der Energy Star-Richtlinien der EPA entspricht, also zum Beispiel auf einem Sun4U-System, wird die Power Management-Software standardmäßig installiert. Während einer Solaris-Installationsprogramm-Installation werden Sie vom Installationsprogramm gefragt, ob Sie die Power Management-Software aktivieren oder deaktivieren möchten. Beim Solaris-Textinstallationsprogramm erfolgt diese Abfrage nach abgeschlossener Installation und einem Systemneustart.

Hinweis – Verfügt Ihr System über Energy Star Version 3 oder höher, so werden Sie nicht um diese Information gebeten.

Bei einer interaktiven Installation können Sie die Power Management-Informationen nicht vorkonfigurieren, um die Eingabeaufforderung zu umgehen. Bei einer benutzerdefinierten JumpStart-Installation können Sie die Power Management-Informationen dagegen vorkonfigurieren, indem Sie mit einem Finish-Skript auf dem System eine /autoshutdownoder /noautoshutdown-Datei anlegen. Beim Systemneustart aktiviert die Datei /autoshutdown Power Management, während die Datei /noautoshutdown Power Management deaktiviert.

Mit der folgenden Zeile in einem Finish-Skript wird die Power Management-Software aktiviert und die Eingabeaufforderung nach dem Systemneustart wird unterdrückt.

touch /a/autoshutdown

Eine Beschreibung von Finish-Skripten finden Sie unter "Erstellen von Finish-Skripten" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

◆ ◆ ◆ KAPITEL 3

Vorkonfigurieren mit einem Naming Service oder DHCP

In diesem Kapitel werden die Verfahren zum Vorkonfigurieren der Systeminformationen mit einem Naming Service oder DHCP beschrieben. Dieses Kapitel enthält die folgenden Abschnitte:

- "Auswählen eines Naming Service" auf Seite 45
- "Vorkonfiguration mit dem Naming Service" auf Seite 47
- "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52

Auswählen eines Naming Service

Zum Vorkonfigurieren von Systemkonfigurationsinformationen können Sie eins der folgenden Verfahren wählen. Fügen Sie die Systemkonfigurationsinformationen wahlweise ein in:

Eine sysidcfg-Datei auf einem entfernten System oder einer Diskette

Hinweis – Die Option name_service in der Datei sysidcfg richtet den Naming Service automatisch während der Installation des Betriebssystems Solaris ein. Diese Einstellung überschreibt die SMF-Services, die zuvor für site.xml eingerichtet wurden. Aus diesem Grund müssen Sie Ihren Naming Service nach der Installation eventuell zurücksetzen.

- Die am Standort verfügbare Naming Service-Datenbank
- Wenn an Ihrem Standort mit DHCP gearbeitet wird, können Sie auch einige Systeminformationen auf dem DHCP-Server des Standorts vorkonfigurieren. Informationen darüber, wie Sie einen DHCP-Server zum Vorkonfigurieren von Systeminformationen verwenden können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Ermitteln Sie mithilfe der folgenden Tabelle, ob Sie die Systemkonfigurationsinformationen anhand einer sysidcfg-Datei oder einer Naming Service-Datenbank vorkonfigurieren sollten.

Vorkonfigurierbare Systeminformationen	Lässt sich mit sysidcfg-Datei vorkonfigurieren?	Lässt sich mit Naming Service vorkonfigurieren?
Naming Service	Ja	Ja
Domain-Name	Ja	Nein
Namen-Server	Ja	Nein
Netzwerkschnittstelle	Ja	Nein
Host-Name	Ja	Ja
	Da diese Informationen systemspezifisch sind, sollten Sie den Naming Service bearbeiten, statt für jedes System eine eigene sysidcfg-Datei zu erstellen.	
IP-Adresse (Internet Protocol)	Ja	Ja
	Da diese Informationen systemspezifisch sind, sollten Sie den Naming Service bearbeiten, statt für jedes System eine eigene sysidcfg-Datei zu erstellen.	
Netzmaske	Ja	Nein
DHCP	Ja	Nein
IPv6	Ja	Nein
Standardroute	Ja	Nein
Root-Passwort	Ja	Nein
Sicherheitsrichtlinie	Ja	Nein
Sprache (Sprachumgebung) für das	Ja	Ja, wenn NIS oder NIS+
Installationsprogramm und den Desktop		Nein, wenn DNS oder LDAP
Terminaltyp	Ja	Nein
Zeitzone	Ja	Ja
Datum und Uhrzeit	Ja	Ja

TABELLE 3–1 Verfahren der Vorkonfiguration von Systemkonfigurationsinformationen

ABELLE 3-1 Verfahren der Vorkonfiguration von Systemkonfigurationsinformationen (Fortsetzung)					
Vorkonfigurierbare Systeminformationen	Lässt sich mit sysidcfg-Datei vorkonfigurieren?	Lässt sich mit Naming Service vorkonfigurieren?			
Web-Proxy	Nein	Nein			
	Diese Informationen können Sie mit dem Solaris-Installationsprogramm konfigurieren, allerdings nicht mithilfe der Datei sysidcfg oder des Naming Service.				
x86: Monitortyp	Ja	Nein			
x86: Tastatursprache, Tastaturlayout	Ja	Nein			
x86: Grafikkarte, Farbtiefe, Auflösung, Bildschirmformat	Ja	Nein			
x86: Zeigegerät, Anzahl an Tasten, IRQ-Stufe	Ja	Nein			
SPARC: Power Management (automatische Systemabschaltung)	Nein	Nein			
Das Power Management kann weder mit der sysidcfg-Datei noch per Naming Service vorkonfiguriert werden. Unter "SPARC: Vorkonfigurieren der Power Management-Informationen" auf Seite 42 finden Sie nähere Informationen.					

Vorkonfiguration mit dem Naming Service

In der folgenden Tabelle finden Sie eine Übersicht der Naming Service-Datenbanken, die Sie bearbeiten und mit Daten füllen müssen, um die Systeminformationen vorzukonfigurieren.

Vorzukonfigurierende Systeminformationen	Naming Service-Datenbank
Host-Name und IP-Adresse (Internet Protocol)	hosts
Datum und Uhrzeit	hosts. Geben Sie den timehost-Alias neben dem Host-Namen des Systems an, das Datum und Uhrzeit für die zu installierenden Systeme bereitstellt.
Zeitzone	timezone
Netzmaske	netmasks

Mit dem Namen-Service DNS oder LDAP kann die Sprachumgebung für ein System nicht vorkonfiguriert werden. Wenn Sie den Naming Service NIS oder NIS+ verwenden, führen Sie zum Vorkonfigurieren der Sprachumgebung für ein System das für den jeweiligen Naming Service relevante Verfahren aus:

Hinweis – Um Ihre Sprachumgebung erfolgreich mit NIS oder NIS+ vorzukonfigurieren, müssen die folgenden Anforderungen erfüllt sein:

Sie müssen das System mit dem folgenden Befehl vom Netzwerk aus booten:

ok boot net

Sie können Optionen mit diesem Befehl angegeben. Weitere Informationen finden Sie in Schritt 2 des Verfahrens "SPARC: So installieren Sie den Client über das Netzwerk (DVDs)" auf Seite 89.

 Der NIS- oder NIS+-Server muss während des gesamten Installationsprozesses verfügbar sein.

Wenn diese Anforderungen erfüllt sind, verwendet das Installationsprogramm die vorkonfigurierten Einstellungen und fordert während der Installation nicht zur Eingabe einer Sprachumgebung auf. Wenn eine diese Anforderungen nicht erfüllt ist, fordert das System während der Installation zur Eingabe einer Sprachumgebung auf.

- "So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS vor" auf Seite 48
- "So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS+ vor" auf Seite 50

So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS vor

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim Namenserver an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

- 2 Ändern Sie /var/yp/Makefile, um die Sprachumgebungen hinzuzufügen.
 - a. Fügen Sie die folgende Shell-Prozedur nach der letzten Variable.time-Shell-Prozedur ein.

```
| $(MAKEDBM) - $(YPDBDIR)/$(DOM)/locale.byname; \
    touch locale.time; \
    echo "updated locale"; \
    if [ ! $(NOPUSH) ]; then \
        $(YPPUSH) locale.byname; \
        echo "pushed locale"; \
    else \
    :; \
    fi \
else \
    echo "couldn't find $(DIR)/locale"; \
fi
```

- b. Suchen Sie die Zeichenkette all: und fügen Sie am Ende der Variablenliste das Wort locale ein.
 - all: passwd group hosts ethers networks rpc services protocols \
 netgroup bootparams aliases publickey netid netmasks c2secure \
 timezone auto.master auto.home locale
- c. Fügen Sie hinter den letzten Eintrag dieser Art, gegen Ende der Datei, die Zeichenkette locale: locale.time in einer neuen Zeile ein.

```
passwd: passwd.time
group: group.time
hosts: hosts.time
ethers: ethers.time
networks: networks.time
rpc: rpc.time
services: services.time
protocols: protocols.time
netgroup: netgroup.time
bootparams: bootparams.time
aliases: aliases.time
publickey: publickey.time
netid: netid.time
passwd.adjunct: passwd.adjunct.time
group.adjunct: group.adjunct.time
netmasks: netmasks.time
timezone: timezone.time
auto.master: auto.master.time
auto.home: auto.home.time
locale: locale.time
```

- d. Speichern Sie die Datei.
- 3 Erstellen Sie die Datei /etc/locale und geben Sie jeweils einen Eintrag für jede Domäne bzw. jedes spezifische System ein:
 - Geben Sie locale Domänename ein.

Der folgende Eintrag legt zum Beispiel fest, dass in der Domain example.com Französisch als Standardsprache gilt:

fr example.com

Hinweis – Eine Liste der gültigen Sprachumgebungen finden Sie in *International Language Environments Guide*.

• Oder geben Sie locale Systemname ein.

In dem folgenden Beispiel wird festgelegt, dass auf dem System myhost Französisch (Belgien) als Standardsprache gilt:

fr_BE myhost

Hinweis – Die Sprachumgebungen stehen auf der Solaris-DVD oder der Solaris Software-1 CD zur Verfügung.

4 Legen Sie die Maps an:

cd /var/yp; make

Systeme, die über eine Domain oder einzeln in der Map locale angegeben sind, werden so eingerichtet, dass darauf die Standardsprachumgebung verwendet wird. Die angegebene Standardsprachumgebung wird während der Installation und nach dem Neustart des Systems vom Desktop verwendet.

Weitere Fortsetzen der Installation

Informationen:

Wenn Sie den NIS-Namen-Service in einer netzwerkgestützten Installation verwenden möchten, müssen Sie einen Installationsserver einrichten und das System als Installationsclient hinzufügen. Weitere Informationen finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Wenn Sie den NIS-Namen-Service in einer benutzerdefinierten JumpStart-Installation verwenden möchten, müssen Sie ein Profil sowie eine rules.ok-Datei erstellen. Weitere Informationen finden Sie in Kapitel 2, "Benutzerdefinierte JumpStart-Installation (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationszenarien.

Siehe auch Weitere Informationen zum NIS-Naming Service finden Sie in Teil III, "NIS Setup and Administration" in System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).

So nehmen Sie die Vorkonfiguration der Sprachumgebung mit NIS+ vor

Im folgenden Verfahren wird davon ausgegangen, dass bereits eine NIS+-Domain eingerichtet ist. Das Einrichten der NIS+-Domäne ist in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* dokumentiert.

- 1 Melden Sie sich als Superuser oder als ein Benutzer in der NIS+-Administrationsgruppe beim Namen-Server an.
- 2 Erstellen Sie die locale-Tabelle:

```
# nistbladm -D access=og=rmcd,nw=r -c locale_tbl name=SI,nogw=
locale=,nogw= comment=,nogw= locale.org_dir.'nisdefaults -d'
```

3 Fügen Sie die erforderlichen Einträge zur locale-Tabelle hinzu.

```
# nistbladm -a name=namelocale=locale comment=comment
locale.org_dir.'nisdefaults -d'
```

Name	Der Name der Domain oder eines bestimmten Systems, für die bzw. das eine Standardsprachumgebung vorkonfiguriert werden soll.
Sprachumgebung	Die Sprachumgebung, die auf dem System installiert und nach dem Neustart auf dem Desktop verwendet werden soll. Eine Liste der gültigen Sprachumgebungen finden Sie in <i>International Language Environments</i> <i>Guide</i> .
Kommentar	Das Anmerkungsfeld. Stellen Sie Anmerkungen, die mehr als ein Wort umfassen, in Anführungszeichen.

Hinweis – Die Sprachumgebungen stehen auf der Solaris-DVD oder der Solaris Software-1 CD zur Verfügung.

Systeme, die über eine Domain oder einzeln in der Tabelle Locale angegeben sind, werden so eingerichtet, dass darauf die Standardsprachumgebung verwendet wird. Die angegebene Standardsprachumgebung wird während der Installation und nach dem Neustart des Systems vom Desktop verwendet.

Weitere Fortsetzen der Installation

Informationen:

Wenn Sie den NIS+-Namen-Service in einer netzwerkgestützten Installation verwenden möchten, müssen Sie einen Installationsserver einrichten und das System als Installationsclient hinzufügen. Weitere Informationen finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Wenn Sie den NIS+-Namen-Service in einer benutzerdefinierten JumpStart-Installation verwenden möchten, müssen Sie ein Profil sowie eine rules.ok-Datei erstellen. Weitere Informationen finden Sie in Kapitel 2, "Benutzerdefinierte JumpStart-Installation (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationszenarien.

Siehe auch Weitere Informationen zum NIS+-Naming Service finden Sie in *System Administration Guide: Naming and Directory Services (NIS+).*

Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)

Mit dem Dynamic Host Configuration Protocol (DHCP) können Host-Systeme in einem TCP/IP-Netzwerk beim Booten automatisch für das Netzwerk konfiguriert werden. Der DHCP-Service funktioniert nach dem Client/Server-Prinzip. Konfigurationsinformationen für Clients werden auf Servern gespeichert und den Clients auf Anforderung zur Verfügung gestellt. Diese Informationen umfassen die IP-Adressen der Clients sowie Informationen über die den Clients zur Verfügung stehenden Netzwerkdienste.

Einer der Hauptvorteile von DHCP ist die Fähigkeit, IP-Adressenzuweisungen per Leasing zu verwalten. Beim Leasing können momentan unbenutzte IP-Adressen zurückgezogen und an andere Clients vergeben werden. Dadurch kommt ein Standort mit weniger IP-Adressen aus, als für die Zuweisung permanenter IP-Adressen an jeden einzelnen Client erforderlich sind.

Mit dem DHCP können Sie Solaris BS auf bestimmten Clientsystemen in Ihrem Netzwerk installieren. Alle SPARC-basierten Systeme, die vom Betriebssystem Solaris unterstützt werden, und x86-basierte Systeme, die die Hardware-Anforderungen zum Ausführen von Solaris BS erfüllen, können diese Funktion nutzen.

Die nachfolgende Übersicht zeigt, welche Schritte Sie durchführen müssen, damit Clients Installationsparameter per DHCP abrufen können.

Aufgabe	Beschreibung	Anweisungen
Richten Sie einen Installationsserver ein.	Richten Sie einen Solaris-Server zur Unterstützung von Clients ein, die Solaris aus dem Netzwerk installieren müssen.	Kapitel 4, "Installieren über das Netzwerk (Übersicht)"
Richten Sie Clientsysteme für die Solaris-Installation per DHCP über das Netzwerk ein.	Aktivieren Sie mit add_install_client -d die DHCP-Unterstützung für die Netzwerkinstallation einer Client-Klasse (z. B. Systeme eines bestimmten Typs) oder eines bestimmten, über seine ID angegebenen Clients.	Mit der Solaris-DVD: "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82 Mit den Solaris-CDs: "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110 add_install_client(1M)

 TABELLE 3-2
 Übersicht der Schritte: Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service

Aufgabe	Beschreibung	Anweisungen
Bereiten Sie Ihr Netzwerk für die Arbeit mit dem DHCP-Service vor.	Entscheiden Sie, wie der DHCP-Server konfiguriert werden soll.	Kapitel 13, "Planungen für den DHCP-Service (Aufgaben)" in Systemverwaltungshandbuch: IP Services
Konfigurieren Sie den DHCP-Server.	Verwenden Sie DHCP-Manager zur Konfiguration des DHCP-Servers.	Kapitel 14, "Konfiguration des DHCP-Services (Aufgaben)" in Systemverwaltungshandbuch: IP Services
Erzeugen Sie DHCP-Optionen für Installationsparameter sowie Makros, die diese Optionen enthalten.	Erzeugen Sie mit DHCP-Manager oder dhtadm neue Herstelleroptionen und Makros, die der DHCP-Server zur Weitergabe von Installationsinformationen an die Clients verwenden kann.	"Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter" auf Seite 53

TABELLE 3-2Übersicht der Schritte: Vorkonfiguration der Systemkonfigurationsinformationen mit demDHCP-Service(Fortsetzung)

Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter

Beim Hinzufügen von Clients auf dem Installationsserver mit dem Skript add_install_client -d meldet das Skript DHCP-Konfigurationsinformationen an die Standardausgabe. Diese Informationen sind beim Erzeugen der für die Übergabe von Installationsinformationen an Clients erforderlichen Optionen und Makros hilfreich.

Die Makros in Ihrem DHCP-Dienst lassen sich zur Durchführung verschiedener Installationsarten anpassen:

- Klassenspezifische Installationen Sie können den DHCP-Dienst anweisen, auf allen Clients einer bestimmten Klasse eine Netzwerkinstallation durchzuführen. Denkbar ist beispielsweise, dass Sie einen DHCP-Makro definieren, der auf allen im Netzwerk befindlichen Sun Blade-Systemen dieselbe Installation vornimmt. Eine klassenspezifische Installation richten Sie auf der Grundlage der Befehlsausgabe von add_install_client -d ein.
- Netzwerkspezifische Installationen Sie können den DHCP-Service anweisen, für alle Clients in einem bestimmten Netzwerk eine Installation über das Netzwerk auszuführen. Sie können beispielsweise ein DHCP-Makro definieren, das die gleiche Installation auf allen Systemen im Netzwerk 192.168.2 ausführt.
- Client-spezifische Installationen Sie können den DHCP-Dienst anweisen, auf einem Client mit einer bestimmten Ethernet-Adresse eine Netzwerkinstallation durchzuführen. Beispielsweise können Sie einen DHCP-Makro definieren, der eine spezifische Installation

auf dem Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf durchgeführt wird. Eine Client-spezifische Installation richten Sie auf der Grundlage der Befehlsausgabe von add_install_client -d -e *Ethernet-Adresse* ein.

Weitere Informationen zum Einrichten von Clients zur Nutzung eines DHCP-Server für Installationen über das Netzwerk finden Sie in den folgenden Vorgehensweisen.

- Netzwerkinstallationen mit DVD siehe "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82.
- Netzwerkinstallationen mit CDs siehe "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110.

DHCP-Optionen und Makrowerte

Um DHCP-Clients aus dem Netzwerk zu installieren, müssen Sie Herstellerkategorie-Optionen erzeugen, mit welchen Informationen übergeben werden können, die zum Installieren von Solaris benötigt werden. In der folgenden Tabelle werden gebräuchliche DHCP-Optionen zur Installation eines DHCP-Clients beschrieben.

- Zum Konfigurieren und Installieren x86-basierter Systeme können Sie die in Tabelle 3–3 aufgeführten DHCP-Optionen verwenden. Diese Optionen sind nicht plattormspezifisch und können zur Installation des Betriebssystems Solaris auf einer Reihe x86-basierter Systeme genutzt werden. Mit dieser Optionen können Sie Solaris 10 auf x86-basierten Systemen mithilfe von DHCP installieren. Eine vollständige Liste der Standardoptionen finden Sie in der Manpage dhcp_inittab(4).
- In Tabelle 3–4 sind Optionen zur Installation von Sun-Clientsystemen aufgeführt. Die in dieser Tabelle aufgeführten Hersteller-Client-Klassen geben an, auf welche Klasse von Clients eine Option anwendbar ist. Bei diesen Hersteller-Client-Klassen handelt es sich nur um Beispiele. Geben Sie bitte die Client-Klassen der tatsächlich über das Netzwerk zu installierenden Clients an. Hinweise zur Ermittlung der Herstellerklasse von Clients finden Sie unter "Arbeiten mit DHCP-Optionen (Übersicht der Schritte)" in Systemverwaltungshandbuch: IP Services.

Ausführliche Informationen zu DHCP-Optionen bietet der Abschnitt "DHCP-Optionsinformationen" in *Systemverwaltungshandbuch: IP Services*.

Name der Option	Code	Datentyp	Granularität	Maximum	Beschreibung
BootFile	entf.	ASCII	1	1	Pfad zur Boot-Datei des Clients
BootSrvA	entf.	IP-Adresse	1	1	IP-Adresse des Boot-Servers
DNSdmain	15	ASCII	1	0	DNS-Domänenname
DNSserv	6	IP-Adresse	1	0	Liste mit DNS-Namenservern

TABELLE 3-3 Werte für DHCP-Standardoptionen

Name der Option	Code	Datentyp	Granularität	Maximum	Beschreibung
NISdmain	40	ASCII	1	0	NIS-Domänenname
NISservs	41	IP-Adresse	1	0	IP-Adresse des NIS-Servers
NIS+dom	64	ASCII	1	0	NIS+-Domänenname
NIS+serv	65\~%	IP-Adresse	1	0	IP-Adresse des NIS+-Servers
Router	3	IP-Adresse	1	0	IP-Adresse von Netzwerk-Routern

 TABELLE 3-3
 Werte für DHCP-Standardoptionen
 (Fortsetzung)

TABELLE 3-4 Werte für die Erzeugung von Herstellerkategorie-Optionen für Solaris-Clients

Name	Code	Datentyp	Granularität	Maximum	Hersteller-Client-Klasse *	Beschreibung

Die folgenden Herstellerkategorie-Optionen sind erforderlich, um die Unterstützung von Solaris-Installationsclients auf einem DHCP-Server zu aktivieren. Die Optionen werden in den Startskripten der Solaris-Clients verwendet.

Hinweis – Bei diesen Hersteller-Client-Klassen handelt es sich nur um Beispiele. Geben Sie bitte die Client-Klassen der tatsächlich über das Netzwerk zu installierenden Clients an.

SrootIP4	2	IP-Adresse	1	1	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	IP-Adresse des Root-Servers
SrootNM	3	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Host-Name des Root-Servers
SrootPTH	4	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zum Root-Verzeichnis des Clients auf dem Root-Server
SinstIP4	10	IP-Adresse	1	1	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	IP-Adresse des JumpStart-Installationsservers
SinstNM	11	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Host-Name des Installationsservers
SinstPTH	12	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zum Installationsabbild auf dem Installationsserver

Die folgenden Optionen können von den Startskripten der Clients verwendet werden, sind aber nicht erforderlich.

Hinweis – Bei diesen Hersteller-Client-Klassen handelt es sich nur um Beispiele. Geben Sie bitte die Client-Klassen der tatsächlich über das Netzwerk zu installierenden Clients an.

TABELLE 3-4	Werte für d	lie Erzeugung v	(Fortsetzung)			
Name	Code	Datentyp	Granularität	Maximum	Hersteller-Client-Klasse *	Beschreibung
SrootOpt	1	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	NFS-Mount-Optionen für das Root-Dateisystem des Clients
SbootFIL	7	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zur Boot-Datei des Clients
SbootRS	9	ZAHL	2	1	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Vom Standalone-Boot-Programm zum Laden des Kernels benötigte NFS-Lesezugriffsgröße
SsysidCF	13	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zur Datei sysidcfg im Format <i>Server:/Pfad</i>
SjumpsCF	14	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zur JumpStart-Konfigurationsdate im Format <i>Server:/Pfad</i>
SbootURI	16	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zur Standalone-Boot-Datei oder zur WAN-Boot-Datei. Für die Standalone-Boot-Datei verwenden Sie folgendes Format:
						tftp://inetboot.sun4u
						Das Format für die WAN-Boot-Datei lautet:
						http://Host.Domain/Pfad_ zur_Datei
						Diese Option kann verwendet werden, um die Einstellungen BootFile und siaddr außer Kraft zu setzen und eine Standalone-Boot-Datei abzurufen. Unterstützte Protokolle: tftp (inetboot), http (wanboot). Verwenden Sie beispielsweise dieses Format: tftp://inetboot.sun4u

TABELLE 3–4 W	erte für d	die Erzeugung v	on Hersteller	kategorie-Op	tionen für Solaris-Clients	(Fortsetzung)
Name	Code	Datentyp	Granularität	Maximum	Hersteller-Client-Klasse *	Beschreibung
SHTTPproxy	17	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	IP-Adresse und Port-Nummer des Proxy-Servers in Ihrem Netzwerk. Diese Option ist nur dann erforderlich, wenn ein Client über ein WAN bootet und im lokalen Netzwerk ein Proxy-Server verwendet wird. Verwenden Sie beispielsweise dieses Format: 198.162.10.5:8080

TABELLE 3-4	Werte für die Erzeugung von Herstellerkategorie-Optionen für Solaris-Clients	(Fortsetzun

Die folgenden Optionen kommen in den Startskripten von Solaris-Clients derzeit nicht zum Einsatz. Um sie zu verwenden, müssen Sie die Startskripten bearbeiten.

Hinweis - Bei diesen Hersteller-Client-Klassen handelt es sich nur um Beispiele. Geben Sie bitte die Client-Klassen der tatsächlich über das Netzwerk zu installierenden Clients an.

SswapIP4	5	IP-Adresse	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.186pc	IP-Adresse des Swap-Servers
SswapPTH	6	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Pfad zur Swap-Datei des Clients auf dem Swap-Server
Stz	8	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.186pc	Zeitzone für den Client
Sterm	15	ASCII-Text	1	0	SUNW.Sun-Blade-1000, SUNW.Sun-Fire-880, SUNW.i86pc	Terminaltyp

Nachdem Sie Optionen erstellt haben, können Sie Makros erstellen, die diese Optionen enthalten. Die folgende Tabelle zeigt Beispielmakros zur Unterstützung der Solaris-Installation für Clients.

TABELLE 3-5 Beispielmakros zur Unterstützung von Netzwerkinstallationsclients

Makroname	Enthält diese Optionen und Makros
Solaris	SrootIP4, SrootNM, SinstIP4, SinstNM
sparc	SrootPTH, SinstPTH
sun4u	Solaris- und sparc-Makros
sun4v	Solaris- und sparc-Makros

Makroname	Enthält diese Optionen und Makros			
і86рс	Solaris-Makro, SrootPTH, SinstPTH, SbootFIL			
SUNW.i86pc	i86pc-Makro			
	Hinweis – Die Hersteller-Client-Klasse SUNW. 186pc gilt nur für Solaris-Release 10 3/05 und kompatible Versionen.			
SUNW.Sun-Blade-1000	sun4u-Makro, SbootFIL			
SUNW.Sun-Fire-880	sun4u-Makro, SbootFIL			
PXEClient:Arch:00000:UNDI:00200BootSrvA,BootFile				
<i>xxx.xxx.xxx.xxx</i> , Netzwerkadressenmakros	Vorhandene Netzwerkadressenmakros sind um die Option BootSrvA zu erweitern. Mit dem Wert von BootSrvA ist der tftboot-Server anzugeben.			
01 <i>Client-MAC-Adresse</i> Client-spezifische Makros (z. B. 010007E9044ABF)	BootSrvA,BootFile			

 TABELLE 3-5
 Beispielmakros zur Unterstützung von Netzwerkinstallationsclients
 (Fortsetzung)

Die in der vorigen Tabelle aufgeführten Makronamen stimmen mit den Hersteller-Client-Klassen der über das Netzwerk zu installierenden Clients überein. Diese Namen sind Beispiele für Clients, die in einem Netzwerk vorhanden sein könnten. Hinweise zur Ermittlung der Herstellerklasse von Clients finden Sie unter "Arbeiten mit DHCP-Optionen (Übersicht der Schritte)" in *Systemverwaltungshandbuch: IP Services*.

Diese Optionen und Makros lassen sich mit folgenden Methoden erzeugen:

- Erzeugen Sie die Optionen und Makros in DHCP-Manager. Anweisungen zum Erzeugen von Optionen und Makros in DHCP-Manager finden Sie unter "Erzeugen von Installationsoptionen und -makros mit DHCP-Manager" auf Seite 59.
- Schreiben Sie ein Skript, das die Optionen und Makros durch den Befehl dhtadm erzeugt. Unter "Schreiben von Skripten zum Erzeugen von Optionen und Makros anhand von dhtadm" auf Seite 61 erfahren Sie, wie Skripten zum Erzeugen dieser Optionen und Makros geschrieben werden.

Bitte beachten Sie, dass die Gesamtgröße der Herstelleroptionen, die einem bestimmten Client zugestellt werden, 255 Byte nicht überschreiten darf. Diese Länge schließt Optionscodes und Längeninformationen ein. Dies ist eine Einschränkung der aktuellen Solaris-Implementierung des DHCP-Protokolls. Im Allgemeinen sollten Sie nur die Mindestmenge der erforderlichen Anbieterinformationen übergeben. Sie sollten kurze Pfadnamen für Optionen verwenden, die Pfadnamen verlangen. Dies lässt sich beispielsweise erreichen, indem Sie symbolische Links für lange Pfade anlegen und dann die (kürzeren) Namen der Links verwenden.

Erzeugen von Installationsoptionen und -makros mit DHCP-Manager

Sie können den DHCP Manager verwenden, um die in Tabelle 3–4 aufgeführten Optionen und die in Tabelle 3–5 aufgeführten Makros zu erstellen.

So erzeugen Sie Optionen zur Unterstützung der Solaris-Installation (DHCP-Manager)

Bevor Sie beginnen Führen Sie die folgenden Schritte aus, bevor Sie DHCP-Makros für Ihre Installation erstellen.

- Fügen Sie die Clients hinzu, die Sie mit DHCP als Installationsclients Ihres Netzwerkinstallationsservers installieren möchten. Informationen, wie Sie einen Client zu einem Installationserver hinzufügen, finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".
- Konfigurieren Sie den DHCP-Server. Falls Sie den DHCP-Server nicht konfiguriert haben, können Sie die Vorgehensweise in Kapitel 13, "Planungen für den DHCP-Service (Aufgaben)" in Systemverwaltungshandbuch: IP Services nachlesen.
- 1 Melden Sie sich als Superuser beim DHCP-Serversystem an, oder nehmen Sie eine entsprechende Rolle an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

2 Starten Sie DHCP Manager.

/usr/sadm/admin/bin/dhcpmgr &

Das DHCP-Manager-Fenster wird angezeigt.

- 3 Wählen Sie das Register "Optionen" im DHCP-Manager.
- 4 Wählen Sie "Erstellen" im Menü "Bearbeiten" aus.

Das Dialogfeld "Option erstellen" wird angezeigt.

5 Geben Sie den Namen für die erste Option und anschließend die Werte für diese Option ein.

Überprüfen Sie mithilfe der Ausgabe des Befehls add_install_client, Tabelle 3–3 und Tabelle 3–4 die Namen und Werte der Optionen, die Sie erstellen müssen. Beachten Sie dabei bitte, dass die Hersteller-Client-Klassen nur Beispielwerte sind. Erzeugen Sie Klassen, die den tatsächlichen Client-Typ der Clients wiedergeben, die vom DHCP-Service Solaris-Installationsparameter erhalten müssen. Hinweise zur Ermittlung der Herstellerklasse von Clients finden Sie unter "Arbeiten mit DHCP-Optionen (Übersicht der Schritte)" in *Systemverwaltungshandbuch: IP Services*.

6 Wenn Sie alle Werte eingegeben haben, klicken Sie auf "OK".

7 Wählen Sie im Register "Optionen" die soeben erzeugte Option aus.

8 Wählen Sie im Menü "Bearbeiten" den Befehl "Duplizieren".

Das Dialogfeld "Option duplizieren" wird angezeigt.

9 Geben Sie einen Namen für eine weitere Option ein, und ändern Sie die Werte entsprechend.

Die Werte für Code, Datentyp, Granularität und Maximum müssen in den meisten Fällen geändert werden. Werte finden Sie in Tabelle 3–3 und Tabelle 3–4.

10 Wiederholen Sie Schritt 7 bis Schritt 9 für jede zu erzeugende Option.

Nun können Sie, wie im Folgenden erläutert, Makros erstellen, um die Optionen an Netzwerkinstallationsclients zu übergeben.

Hinweis – Sie brauchen diese Optionen nicht in die Datei /etc/dhcp/inittab eines Solaris-Clients einzufügen, da sie dort bereits vorhanden sind.

So erzeugen Sie Makros zur Unterstützung der Solaris-Installation (DHCP-Manager)

Bevor Sie beginnen

Führen Sie die folgenden Schritte aus, bevor Sie DHCP-Makros für Ihre Installation erstellen.

- Fügen Sie die Clients hinzu, die Sie mit DHCP als Installationsclients Ihres Netzwerkinstallationsservers installieren möchten. Informationen, wie Sie einen Client zu einem Installationserver hinzufügen, finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".
- Konfigurieren Sie den DHCP-Server. Falls Sie den DHCP-Server nicht konfiguriert haben, können Sie die Vorgehensweise in Kapitel 13, "Planungen für den DHCP-Service (Aufgaben)" in Systemverwaltungshandbuch: IP Services nachlesen.
- Erstellen Sie die DHCP-Optionen, die in Ihrem Makro verwendet werden sollen. Eine Anleitung zum Erstellen von DHCP-Optionen finden Sie in "So erzeugen Sie Optionen zur Unterstützung der Solaris-Installation (DHCP-Manager)" auf Seite 59.
- 1 Wählen Sie das Register "Makros" im DHCP-Manager.

2 Wählen Sie "Erstellen" im Menü "Bearbeiten" aus.

Das Dialogfeld "Makro erstellen" wird angezeigt.

3 Geben Sie den Namen für ein Makro ein.

Die Namen von Makros, die verwendet werden können, finden Sie in Tabelle 3–5.

4 Klicken Sie auf die Schaltfläche "Auswählen".

Das Dialogfeld "Option auswählen" wird angezeigt.

5 Wählen Sie in der Kategorieliste den Eintrag "Hersteller".

Es werden die von Ihnen erzeugten Herstelleroptionen angezeigt.

6 Wählen Sie eine Option aus, die in das Makro eingefügt werden soll, und klicken Sie auf "OK".

7 Geben Sie einen Wert für die Option ein.

Datentypen der Optionen finden Sie in Tabelle 3–3 und Tabelle 3–4. Nutzen Sie auch die vonadd_install_client -d ausgegebenen Informationen.

8 Wiederholen Sie Schritt 6 bis Schritt 7 für jede hinzuzufügende Option.

Um ein weiteres Makro hinzuzufügen, geben Sie **Include** als Optionsnamen ein und dann den Makronamen als Optionswert.

9 Wenn das Makro fertig gestellt ist, klicken Sie auf "OK".

Weitere Fortsetzen der Installation

Wenn Sie DHCP in einer netzwerkgestützten Installation verwenden möchten, müssen Sie einen Installationsserver einrichten und das System als Installationsclient hinzufügen. Weitere Informationen finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Wenn Sie DHCP in einer WAN-Boot-Installation verwenden möchten, sind einige zusätzliche Schritte erforderlich. Weitere Informationen finden Sie in Kapitel 10, "WAN-Boot (Übersicht)".

Wenn Sie DHCP in einer benutzerdefinierten JumpStart-Installation verwenden möchten, müssen Sie ein Profil sowie eine rules.ok-Datei erstellen. Weitere Informationen finden Sie in Kapitel 2, "Benutzerdefinierte JumpStart-Installation (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationszenarien.

Siehe auch Weitere Informationen zu DHCP finden Sie in Teil III, "DHCP" in *Systemverwaltungshandbuch: IP Services.*

Schreiben von Skripten zum Erzeugen von Optionen und Makros anhand von dhtadm

Sie können ein Skript in der Korn Shell erstellen, indem Sie das in Beispiel 3–1 dargestellte Beispiel entsprechend abändern, um alle in Tabelle 3–3 und Tabelle 3–4 aufgeführten Optionen und einige nützliche Makros zu erstellen. Dabei müssen Sie alle in Anführungszeichen stehenden IP-Adressen und Werte in die für Ihr Netzwerk geltenden IP-Adressen, Servernamen und Pfade abändern. Außerdem müssen Sie mit dem Schlüssel Vendor= die entsprechende Client-Klasse angeben. Aus der Meldung von add_install_client -d ersehen Sie die zur Anpassung des Skripts erforderlichen Informationen. BEISPIEL 3-1 Beispielskript zur Unterstützung der Netzwerkinstallation

Load the Solaris vendor specific options. We'll start out supporting # the Sun-Blade-1000, Sun-Fire-880, and i86 platforms. Note that the # SUNW.i86pc option only applies for the Solaris 10 3/05 release. # Changing -A to -M would replace the current values, rather than add them. dhtadm -A -s SrootOpt -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,1,ASCII,1,0' dhtadm -A -s SrootIP4 -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,2,IP,1,1' dhtadm -A -s SrootNM -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,3,ASCII,1,0' dhtadm -A -s SrootPTH -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,4,ASCII,1,0' dhtadm -A -s SswapIP4 -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,5, IP, 1, 0' dhtadm -A -s SswapPTH -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,6,ASCII,1,0' dhtadm -A -s SbootFIL -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,7,ASCII,1,0' dhtadm -A -s Stz -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,8,ASCII,1,0' dhtadm -A -s SbootRS -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,9,NUMBER,2,1' dhtadm -A -s SinstIP4 -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,10,IP,1,1' dhtadm -A -s SinstNM -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,11,ASCII,1,0' dhtadm -A -s SinstPTH -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,12,ASCII,1,0' dhtadm -A -s SsysidCF -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,13,ASCII,1,0' dhtadm -A -s SiumpsCF -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,14,ASCII,1,0' dhtadm -A -s Sterm -d \ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,15,ASCII,1,0' dhtadm -A -s SbootURI -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,16,ASCII,1,0' dhtadm -A -s SHTTPproxy -d ∖ 'Vendor=SUNW.Sun-Blade-1000 SUNW.Sun-Fire-880 SUNW.i86pc,17,ASCII,1,0' # Load some useful Macro definitions. # Define all Solaris-generic options under this macro named Solaris. dhtadm -A -m Solaris -d ∖ ':SrootIP4=10.21.0.2:SrootNM="blue2":SinstIP4=10.21.0.2:SinstNM="red5":' # Define all sparc-platform specific options under this macro named sparc. dhtadm -A -m sparc -d ∖ ':SrootPTH="/export/sparc/root":SinstPTH="/export/sparc/install":' # Define all sun4u architecture-specific options under this macro named sun4u. # (Includes Solaris and sparc macros.) dhtadm -A -m sun4u -d ':Include=Solaris:Include=sparc:' # Solaris on IA32-platform-specific parameters are under this macro named i86pc. # Note that this macro applies only for the Solaris 10 3/05 release. dhtadm -A -m i86pc -d ∖ ':Include=Solaris:SrootPTH="/export/i86pc/root":SinstPTH="/export/i86pc/install"\ :SbootFIL="/platform/i86pc/kernel/unix":' # Solaris on IA32 machines are identified by the "SUNW.i86pc" class. All # clients identifying themselves as members of this class will see these # parameters in the macro called SUNW.i86pc, which includes the i86pc macro. # Note that this class only applies for the Solaris 10 3/05 release.

BEISPIEL 3–1 Beispielskript zur Unterstützung der Netzwerkinstallation (Fortsetzung)

```
dhtadm -A -m SUNW.i86pc -d ':Include=i86pc:'
# Sun-Blade-1000 platforms identify themselves as part of the
# "SUNW.Sun-Blade-1000" class.
# All clients identifying themselves as members of this class
# will see these parameters.
dhtadm -A -m SUNW.Sun-Blade-1000 -d \
':SbootFIL="/platform/sun4u/kernel/sparcv9/unix":\
Include=sun4u:'
# Sun-Fire-880 platforms identify themselves as part of the "SUNW.Sun-Fire-880" class.
# All clients identifying themselves as members of this class will see these parameters.
dhtadm -A -m SUNW.Sun-Fire-880 -d ∖
':SbootFIL="/platform/sun4u/kernel/sparcv9/unix":Include=sun4u:'
# Add our boot server IP to each of the network macros for our topology served by our
# DHCP server. Our boot server happens to be the same machine running our DHCP server.
dhtadm -M -m 10.20.64.64 -e BootSrvA=10.21.0.2
dhtadm -M -m 10.20.64.0 -e BootSrvA=10.21.0.2
dhtadm -M -m 10.20.64.128 -e BootSrvA=10.21.0.2
dhtadm -M -m 10.21.0.0 -e BootSrvA=10.21.0.2
dhtadm -M -m 10.22.0.0
                       -e BootSrvA=10.21.0.2
# Make sure we return host names to our clients.
dhtadm -M -m DHCP-servername -e Hostname= NULL VALUE
# Create a macro for PXE clients that want to boot from our boot server.
# Note that this macro applies for the Solaris 10 3/05 release.
dhtadm -A -m PXEClient:Arch:00000:UNDI:002001 -d \
:BootFile=nbp.i86pc:BootSrvA=10.21.0.2:
# Create a macro for PXE clients that want to boot from our boot server.
# Note that this macro applies for the Solaris 10 2/06 release.
dhtadm -A -m PXEClient:Arch:00000:UNDI:002001 -d \
:BootFile=i86pc:BootSrvA=10.21.0.2:
# Create a macro for the x86 based client with the Ethernet address 00:07:e9:04:4a:bf
# to install from the network by using PXE.
dhtadm -A -m 010007E9044ABF -d :BootFile=010007E9044ABF:BootSrvA=10.21.0.2:
# The client with this MAC address is a diskless client. Override the root settings
# which at the network scope setup for Install with our client's root directory.
dhtadm -A -m 0800201AC25E -d \
':SrootIP4=10.23.128.2:SrootNM="orange-svr-2":SrootPTH="/export/root/10.23.128.12":'
```

Führen Sie dhtadm als Superuser im Batch-Modus aus. Geben Sie den Namen des Skripts mit den zu dhcptab hinzuzufügenden Optionen und Makros an. Wenn Ihr Skript beispielsweise netinstalloptions heißt, geben Sie folgenden Befehl ein:

dhtadm -B netinstalloptions

Clients, die mit einer der in der Zeichenkette Vendor= aufgeführten Client-Klassen bezeichnet sind, können nun per DHCP über das Netzwerk installiert werden.

Weitere Informationen über die Verwendung des Befehls dhtadm finden Sie in dhtadm(1M). Näheres zur Datei dhcptab entnehmen Sie bitte der Manpage dhcptab(4).

TEIL II

Installation über ein LAN

Dieser Teil beschreibt, wie Sie ein System im lokalen Netzwerk (LAN) installieren.

• • • KAPITEL 4

Installieren über das Netzwerk (Übersicht)

Verwenden Sie dieses Kapitel als eine Einführung in das Verfahren zum Einrichten des lokalen Netzwerks und der Systeme, wenn Sie die Solaris-Software über das Netzwerk und nicht über DVD oder CD installieren möchten. In diesem Kapitel finden Sie einen Überblick über die folgenden Themen.

- "Einführung in die Netzwerkinstallation" auf Seite 67
- "x86: Überblick über das Booten und Installieren über das Netzwerk mit PXE" auf Seite 70

Wie Sie einen Client über ein WAN (Wide Area Network) installieren können, erfahren Sie in Kapitel 10, "WAN-Boot (Übersicht)".

Einführung in die Netzwerkinstallation

In diesem Abschnitt finden Sie die Informationen, die Sie benötigen, wenn Sie eine Installation über ein Netzwerk ausführen wollen. Dank der Netzwerkinstallationsfunktionen können Sie die Solaris-Software von einem System, dem Installationsserver, aus installieren, das Zugriff auf die Abbilder der aktuelle Solaris-Release-Datenträger hat. Dazu kopieren Sie den Inhalt der aktuelle Solaris-Release-DVD oder -CDs auf die Festplatte des Installationsservers. Danach können Sie die Solaris-Software mit jedem der Solaris-Installationsverfahren vom Netzwerk aus installieren.

Für die Installation über ein Netzwerk erforderliche Server

Wenn Sie Solaris über ein Netzwerk installieren wollen, müssen die folgenden Server im Netzwerk mit den zu installierenden Systemen vorhanden sein.

- Installationsserver Ein vernetztes System, das die aktuelle Solaris-Release-Datenträgerabbilder enthält, von denen aus Sie die aktuelle Solaris-Release auf anderen Systemen im Netzwerk installieren können. Zum Erstellen eines Installationsservers kopieren Sie die Abbilder von den folgenden Datenträgern:
 - Solaris-DVD
 - Solaris Software-CDs

Hinweis – Ab Version Oracle Solaris 109/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Nachdem Sie die Abbilder von den Solaris Software-CDs kopiert haben, können Sie auch ein Abbild von den Solaris Languages-CDs kopieren, sofern Sie dies für die Installation benötigen.

Sie können auf einem einzigen Installationsserver Datenträgerabbilder für verschiedene Solaris-Releases und für mehrere Plattformen bereitstellen, indem Sie die entsprechenden Abbilder auf die Festplatte des Installationsservers kopieren. So kann ein einziger Installationsserver zum Beispiel die Datenträgerabbilder für die SPARC- und die x86-Plattform enthalten.

Nähere Informationen zum Erstellen eines Installationsservers finden Sie in den folgenden Abschnitten.

- "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76
- "SPARC: So erstellen Sie mit einer SPARC- bzw. x86-CD einen Installationsserver" auf Seite 103
- Boot-Server Ein Serversystem, das Clientsystemen im gleichen Netzwerk-Teilnetz mit den zum Booten notwendigen Informationen versorgt, damit das BS installiert werden kann. Bei dem Boot- und dem Installationsserver handelt es sich normalerweise um dasselbe System. Wenn das System, auf dem aktuelle Solaris-Release installiert werden soll, sich jedoch in einem anderen Teilnetz als der Installationsserver befindet und Sie nicht DHCP verwenden, ist ein Boot-Server für dieses Teilnetz erforderlich.

Auf einem einzigen Boot-Server können Sie aktuelle Solaris-Release-Boot-Software für mehrere Versionen, einschließlich der aktuelle Solaris-Release-Boot-Software für verschiedene Plattformen, bereitstellen. So können Sie zum Beispiel auf einem SPARC-Boot-Server die Solaris 9- und aktuelle Solaris-Release-Boot-Software für SPARC-basierte Systeme zur Verfügung stellen. Auf diesem SPARC-Boot-Server kann außerdem die aktuelle Solaris-Release-Boot-Software für x86-basierte Systeme bereitgestellt werden. Hinweis – Wenn Sie mit DHCP arbeiten, brauchen Sie keinen separaten Boot-Server einzurichten. Weitere Informationen finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Nähere Informationen zum Erstellen eines Boot-Servers finden Sie in den folgenden Abschnitten.

- "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80
- Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107
- (Optional) DHCP-Server Ein Server, der mithilfe des Dynamic Host Configuration Protocol (DHCP) Netzwerkparameter, die für die Installation erforderlich sind, bereitstellt. Sie können DHCP-Server zur Konfiguration und Installation spezifischer Clients, aller Clients in einem bestimmten Netzwerk oder einer gesamten Client-Klasse konfigurieren. Wenn Sie mit DHCP arbeiten, brauchen Sie keinen separaten Boot-Server einzurichten.

Nachdem Sie den Installationsserver eingerichtet haben, fügen Sie Clients mit dem Befehl add_install_client und der Option -d zum Netzwerk hinzu. Mit der Option -d können Sie Clientsysteme für die Installation von Solaris über das Netzwerk mithilfe von DHCP einrichten.

Informationen zu den DHCP-Optionen für Installationsparameter finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

 (Optional) Namen-Server – Ein System, das zur Verwaltung einer verteilten Netzwerkdatenbank, wie zum Beispiel DNS, NIS, NIS+ oder LDAP, dient. Eine solche Datenbank enthält Informationen zu Systemen im Netzwerk.

Einzelheiten zum Erstellen eines Namen-Servers finden Sie in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Hinweis – Beim Boot- und Installationsserver kann es sich um dasselbe oder verschiedene Systeme handeln.

Abbildung 4–1 zeigt die normalerweise für Installationen über das Netzwerk eingesetzten Server. Bitte beachten Sie, dass dieses Beispielnetzwerk keinen DHCP-Server enthält.



ABBILDUNG 4-1 Server für die Installation über ein Netzwerk

x86: Überblick über das Booten und Installieren über das Netzwerk mit PXE

In diesem Abschnitt finden Sie einen Überblick über das Preboot Execution Environment (PXE).

x86: Was ist PXE?

Beim PXE-Netzwerkstart handelt es sich um einen "direkten" Netzwerkstart. Hierfür ist auf dem Clientsystem kein Boot-Datenträger erforderlich. PXE ermöglicht die Installation von x86-basierten Clients über das Netzwerk unter Verwendung von DHCP.

Der PXE-Netzwerkstart ist nur bei Geräten möglich, welche die Spezifikation Intel Preboot Execution Environment erfüllen. Ob Ihr System den PXE-Netzwerkstart unterstützt, entnehmen Sie bitte der Dokumentation des Hardwareherstellers.

x86: Richtlinien für das Booten mit PXE

Zum Booten über das Netzwerk mithilfe von PXE benötigen Sie folgende Systeme:

- Einen Installationsserver
- Einen DHCP-Server
- Einen x86-Client mit Unterstützung für PXE

Wenn Sie beabsichtigen, einen Client mit PXE über das Netzwerk zu installieren, beachten Sie die folgenden Punkte:

- Richten Sie in dem Teilnetz, in dem sich der zu installierende Client befindet, nur einen DHCP-Server ein. Der PXE-Netzwerkstart funktioniert in Teilnetzen mit mehreren DHCP-Servern nicht ordnungsgemäß.
- In einigen frühen Versionen der PXE-Firmware treten eine Reihe von Problemen auf. Wenn Sie Schwierigkeiten mit einem bestimmten PXE-Adapter haben, sollten Sie auf der Website des Hersteller Informationen zum Upgrade der Firmware abrufen. Weitere Informationen entnehmen Sie bitte den Manpages elxl(7D) und iprb(7D).
◆ ◆ ◆ KAPITEL 5

Installieren über das Netzwerk mithilfe von DVDs (Vorgehen)

In diesem Kapitel wird beschrieben, wie Sie das Netzwerk und die Systeme mithilfe einer DVD einrichten, wenn Sie die Solaris-Software über das Netzwerk installieren wollen. Bei einer Installation über das Netzwerk können Sie die Solaris-Software von einem System, dem Installationsserver, aus installieren, das Zugriff auf die Datenträgerabbilder der aktuellen Solaris-Release hat. Dazu kopieren Sie den Inhalt der DVD der aktuellen Solaris-Release auf die Festplatte des Installationsservers. Danach können Sie die Solaris-Software mit jedem der Solaris-Installationsverfahren vom Netzwerk aus installieren.

In diesem Kapitel werden die folgenden Themen behandelt:

- "Übersicht der Schritte: Installieren über das Netzwerk mithilfe von DVDs" auf Seite 74
- "Erstellen eines Installationsservers mithilfe einer DVD" auf Seite 76
- "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80
- "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82
- "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88

Hinweis –

Ab der Solaris-Version 10 11/06 können Sie die Netzwerkeinstellungen bei der Erstinstallation so einrichten, dass alle Netzwerkdienste mit Ausnahme von Secure Shell entweder deaktiviert werden oder nur auf lokale Anfragen reagieren. Diese Sicherheitsoption ist jedoch nur während der Erstinstallation und nicht bei einem Upgrade verfügbar. Bei einem Upgrade werden alle zuvor eingerichteten Dienste beibehalten. Falls erforderlich, können Sie die Netzwerkdienste nach einem Upgrade mithilfe des Befehls netservices einschränken. Siehe "Planung der Netzwerksicherheit" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Die Netzwerkdienste können nach der Installation entweder mithilfe des Befehls netservices open aktiviert werden, oder Sie aktivieren einzelne Dienste mithilfe von SMF-Befehlen. Siehe "Ändern der Sicherheitseinstellungen nach der Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Ab Solaris-Release 10&;10/08 hat sich die Struktur der Solaris-DVD und der Solaris Software-1 CD für die SPARC-Plattform geändert. Slice 0 befindet sich nicht mehr auf der obersten Hierarchieebene der Verzeichnisstruktur. Deswegen sind die Strukturen der x86und SPARC-DVDs sowie der Solaris Software-1 CD jetzt gleich. Diese Strukturänderung vereinfacht das Einrichten eines Installationsservers bei verschiedenen Plattformen wie z.B. SPARC-Installationsserver und x86-Medien.

Übersicht der Schritte: Installieren über das Netzwerk mithilfe von DVDs

Aufgabe	Beschreibung	Siehe
(nur x86): Vergewissern Sie sich, dass das System PXE unterstützt.	Wenn Sie ein x86-basiertes System über das Netzwerk installieren wollen, müssen Sie sicherstellen, dass Ihr Rechner PXE zum Booten ohne lokalen Boot-Datenträger nutzen kann. Wenn Ihr x86-basiertes System PXE nicht unterstützt, muss es von einer lokalen DVD bzw. CD gebootet werden.	Lesen Sie dazu in der Dokumentation des Herstellers Ihres BIOS-Systems nach.
Wählen Sie ein Installationsverfahren.	Das BS Solaris bietet verschiedene Installations- oder Upgrade-Verfahren. Wählen Sie das Installationsverfahren, das für Ihre Umgebung am besten geeignet ist.	"Auswählen eines Solaris-Installationsverfahrens in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

TABELLE 5-1 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe einer DVD

Aufgabe	Beschreibung	Siehe
Stellen Sie Informationen zu Ihrem System zusammen.	Verwenden Sie die Checkliste, und füllen Sie das Arbeitsblatt aus, um alle Informationen zusammenzustellen, die Sie für die Installation bzw. das Upgrade benötigen.	Kapitel 5, "Zusammenstellen von Informationen vor einer Installation bzw. einem Upgrade (Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
(Optional) Führen Sie eine Vorkonfiguration der Systeminformationen aus.	Sie können die Systeminformationen vorkonfigurieren und so vermeiden, dass Sie während des Installations- bzw. Upgrade-Vorgangs dazu aufgefordert werden, diese Informationen einzugeben.	Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)"
Erstellen Sie einen Installationsserver.	Kopieren Sie die Solaris-DVD mit dem Befehl setup_install_server(1M) auf die Festplatte des Installationsservers.	"Erstellen eines Installationsservers mithilfe einer DVD" auf Seite 76
(Optional) Erstellen Sie einen Boot-Server.	Wenn Sie Systeme über das Netzwerk installieren möchten, die sich in einem anderen Teilnetz als der Installationsserver befinden, müssen Sie im Teilnetz der Systeme einen Boot-Server erstellen, damit die Systeme gebootet werden können. Verwenden Sie zum Einrichten eines Boot-Servers den Befehl setup_install_server mit der Option -b. Wenn Sie mit DHCP (Dynamic Host Configuration Protocol) arbeiten, benötigen Sie keinen Boot-Server.	"Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80
Fügen Sie die über das Netzwerk zu installierenden Systeme hinzu.	Richten Sie mit dem Befehl add_install_client jedes über das Netzwerk zu installierende System ein. Jedes System, das Sie installieren möchten, muss in der Lage sein, den Installationsserver, gegebenenfalls den Boot-Server und die Konfigurationsinformationen zu finden.	"Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82
(Optional) Konfiguration des DHCP-Servers.	Wenn DHCP Parameter zur Systemkonfiguration und -installation bereitstellen soll, müssen Sie zuerst den DHCP-Server konfigurieren und dann die für die gewünschte Installation erforderlichen Optionen und Makros erstellen.	Kapitel 13, "Planungen für den DHCP-Service (Aufgaben)" in Systemverwaltungshandbuch: IP Services
	Hinweis – Wenn Sie ein x86-basiertes System über das Netzwerk mithilfe von PXE installieren möchten, müssen Sie einen DHCP-Server konfigurieren.	"Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52

 TABELLE 5-1
 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe einer DVD (Fortsetzung)

Aufgabe	Beschreibung	Siehe
Installieren Sie das System über das Netzwerk.	Die Installation beginnt mit dem Booten des Systems über das Netzwerk.	"Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88

 TABELLE 5-1
 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe einer DVD (Fortsetzung)

Erstellen eines Installationsservers mithilfe einer DVD

Der Installationsserver enthält das Installationsabbild, das für die Installation von Systemen über das Netzwerk benötigt wird. Wenn Sie die Solaris-Software über das Netzwerk auf einem System installieren wollen, müssen Sie einen Installationsserver erstellen. Sie brauchen nicht in jedem Fall einen Boot-Server einzurichten.

- Wenn Sie die Installationsparameter über DHCP bereitstellen oder wenn sich der Installationsserver und die Clients im selben Teilnetz befinden, benötigen Sie keinen Boot-Server.
- Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Sie können auch für jedes Teilnetz einen Installationsserver einrichten, doch für Installationsserver benötigen Sie mehr Festplattenspeicher.

So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver

Hinweis – Bei diesem Verfahren wird davon ausgegangen, dass Volume Manager auf dem System ausgeführt wird. Wenn Sie den Volume Manager nicht zum Verwalten von Medien verwenden, lesen Sie bitte *System Administration Guide: Devices and File Systems*.

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem System an, das der Installationsserver werden soll.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Das System muss über ein DVD-ROM-Laufwerk verfügen und Teil des Netzwerks und des Naming Service am Standort sein. Wenn Sie einen Naming Service verwenden, muss sich das System außerdem bereits in einem Service wie NIS, NIS+, DNS oder LDAP befinden. Wenn Sie keinen Naming Service verwenden, müssen Sie die Informationen über dieses System in Übereinstimmung mit den Richtlinien des jeweiligen Standorts verteilen.

- 2 Legen Sie die Solaris-DVD in das Laufwerk des Systems ein.
- 3 Erstellen Sie ein Verzeichnis, in das Sie das DVD-Abbild stellen können.
 - # mkdir -p install_dir_path

Install_Verz_pfad gibt das Verzeichnis an, in das das DVD-Abbild kopiert werden soll.

4 Wechseln Sie in das Verzeichnis Tools auf dem eingehängten Datenträger.

cd /cdrom/cdrom0/Solaris_10/Tools

5 Kopieren Sie das Abbild der DVD im Laufwerk auf die Festplatte des Installationsservers.

./setup_install_server install_dir_path

Ins_verz_pfad Gibt das Verzeichnis an, in das das DVD-Abbild kopiert werden soll.

Hinweis – Der Befehl setup_install_server gibt an, ob ausreichend Festplattenspeicher für die Solaris Software-Abbilder vorhanden ist. Um den verfügbaren Festplattenspeicher zu ermitteln, verwenden Sie den Befehl df -kl.

- 6 Entscheiden Sie, ob der Installationsserver zum Einhängen verfügbar sein muss.
 - Wenn sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet oder Sie mit DHCP arbeiten, brauchen Sie keinen Boot-Server zu erstellen. Fahren Sie mit Schritt 7 fort.
 - Wenn sich das zu installierende System nicht in demselben Teilnetz wie der Installationsserver befindet und Sie nicht mit DHCP arbeiten, gehen Sie wie folgt vor.
 - a. Überprüfen Sie, ob der Pfad zum Abbild auf dem Installationsserver korrekt zur gemeinsamen Nutzung freigegeben ist.

```
# share | grep install_dir_path
```

```
Ins_verz_pfad Gibt den Pfad zu dem Installationsverzeichnis an, in welches das DVD-Abbild kopiert wurde.
```

- Wenn der Pfad zum Verzeichnis auf dem Installationsserver angezeigt wird und in den Optionen anon=0 erscheint, fahren Sie mit Schritt 7 fort.
- Wenn der Pfad zum Verzeichnis auf dem Installationsserver nicht angezeigt wird oder anon=0 in den Optionen nicht erscheint, fahren Sie hier fort.

b. Machen Sie den Installationsserver für den Bootserver verfügbar.

Fügen Sie diesen Eintrag mithilfe des Befehls share in die Datei /etc/dfs/dfstab ein. share -F nfs -o ro,anon=0 -d "install server directory" *install_dir_path*

- c. Prüfen Sie, ob der nfsd-Dämon läuft.
 - Wenn auf dem Installationsserver die aktuelle Solaris-Release oder eine kompatible Version ausgeführt wird, geben Sie den folgenden Befehl ein.

```
# svcs -l svc:/network/nfs/server:default
```

Wenn der nfsd-Dämon online ist, fahren Sie mit Schritt d fort. Wenn der nfsd-Dämon nicht online ist, starten Sie ihn.

- # svcadm enable svc:/network/nfs/server
- Wenn auf dem Installationsserver Solaris 9 oder eine kompatible Version läuft, geben Sie den folgenden Befehl ein.

ps -ef | grep nfsd

Wenn der nfsd-Dämon läuft, fahren Sie mit Schritt d fort. Wenn der nfsd-Dämon nicht läuft, starten Sie ihn.

/etc/init.d/nfs.server start

- d. Geben Sie den Installationsserver zur gemeinsamen Nutzung frei.
 - # shareall
- 7 Wechseln Sie in das Root-Verzeichnis (/).

cd /

- 8 Lassen Sie die Solaris-DVD auswerfen.
- 9 (Optional) Patchen Sie die Dateien in der Miniroot des vom Befehl setup_install_server erstellten Netzwerkinstallationsabbilds.

Das Anwenden von Patches ist möglicherweise erforderlich, wenn es bei einem Boot-Abbild zu Problemen kommt. Eine schrittweise Anleitung finden Sie in Kapitel 7, "Patchen des Miniroot-Abbilds (Vorgehen)".

- 10 Entscheiden Sie, ob Sie einen Boot-Server erstellen müssen.
 - Wenn Sie mit DHCP arbeiten oder sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet, brauchen Sie keinen Boot-Server zu erstellen. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82 fort.

 Wenn Sie nicht mit DHCP arbeiten und sich das zu installierende System in einem anderen Teilnetz als der Installationsserver befindet, müssen Sie einen Boot-Server erstellen. Fahren Sie mit "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80 fort.

Beispiel 5–1 SPARC: Erstellen eines Installationsservers mithilfe einer DVD

Das folgende Beispiel zeigt, wie Sie einen Installationsserver erstellen, indem Sie die Solaris-DVD in das Verzeichnis /export/home/dvd des Installationsservers kopieren. Dabei wird vorausgesetzt, dass auf dem Installationsserver die aktuelle Solaris-Release ausgeführt wird.

```
# mkdir -p /export/home/dvd
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./setup_install_server /export/home/dvd
```

Falls Sie einen separaten Boot-Server benötigen, müssen Sie den Installationsserver für den Boot-Server verfügbar machen.

Fügen Sie diesen Eintrag mithilfe des Befehls share in die Datei /etc/dfs/dfstab ein.

share -F nfs -o ro,anon=0 -d "install server directory" /export/home/dvdsparc

Überprüfen Sie, ob der nfsd-Dämon online ist. Ist dies nicht der Fall, dann starten Sie den nfsd-Dämon und geben ihn frei.

```
# svcs -l svc:/network/nfs/server:default
# svcadm enable svc:/network/nfs/server
# shareall
# cd /
```

Weitere Fortsetzen der Installation

Informationen:

Nachdem Sie den Installationsserver eingerichtet haben, müssen Sie den Client als Installationsclient hinzufügen. Informationen zum Hinzufügen der zu installierenden Clientsysteme über das Netzwerk finden Sie in "So fügen Sie über das Netzwerk zu installierende Systeme mit add install client hinzu (DVD)" auf Seite 83.

Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Informationen hierzu finden Sie in "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80.

Siehe auch Nähere Informationen zu den Befehlen setup_install_server und add_to_install_server finden Sie in install_scripts(1M).

Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes

Sie müssen einen Installationsserver erstellen, um die Solaris-Software über ein Netzwerk auf einem System zu erstellen. Sie brauchen nicht in jedem Fall einen Boot-Server einzurichten. Ein Boot-Server enthält so viel Boot-Software, dass Systeme vom Netzwerk aus gebootet werden können, und danach führt der Installationsserver die Installation der Solaris-Software durch.

- Wenn Sie die Installationsparameter über DHCP bereitstellen oder wenn sich der Installationsserver und der Client im selben Teilnetz befinden, benötigen Sie keinen Boot-Server. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82 fort.
- Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Sie können auch für jedes Teilnetz einen Installationsserver erstellen, doch für Installationsserver benötigen Sie mehr Festplattenspeicher.

So erstellen Sie einen Boot-Server in einem Teilnetz mithilfe eines DVD-Abbildes

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem System an, das der Boot-Server für das Teilnetz werden soll.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Das System muss Zugriff auf ein entferntes aktuelle Solaris-Release-Datenträgerabbild haben, das sich normalerweise auf dem Installationsserver befindet. Wenn Sie einen Naming Service verwenden, muss sich das System außerdem im Naming Service befinden. Wenn Sie keinen Naming Service verwenden, müssen Sie die Informationen über dieses System in Übereinstimmung mit den Richtlinien des jeweiligen Standorts verteilen.

2 Hängen Sie die Solaris-DVD vom Installationsserver aus ein.

mount -F nfs -o ro server_name:path /mnt

Server_Name: Pfad

Der Name des Installationsservers und der absolute Pfad zu dem Abbild des Datenträgers

- 3 Erstellen Sie ein Verzeichnis für das Boot-Abbild.
 - # mkdir -p boot_dir_path

Boot-Verzeichnispfad Gibt das Verzeichnis an, in das die Boot-Software kopiert werden soll.

- 4 Wechseln Sie in das Verzeichnis Tools im Abbild der Solaris-DVD:
 - # cd /mnt/Solaris_10/Tools
- 5 Kopieren Sie die Boot-Software auf den Boot-Server.

```
# ./setup_install_server -b boot_dir_path
```

- b	Gibt an, dass das System als Boot-Server eingerichtet werden soll.
Boot-Verzeichnispfad	Gibt das Verzeichnis an, in das die Boot-Software kopiert werden soll.

Hinweis – Der Befehl setup_install_server gibt an, ob ausreichend Festplattenspeicher für die Abbilder vorhanden ist. Um den verfügbaren Festplattenspeicher zu ermitteln, verwenden Sie den Befehl df -kl.

6 Wechseln Sie in das Root-Verzeichnis (/).

cd /

7 Hängen Sie das Installationsabbild aus.

umount /mnt

Jetzt können Sie die Systeme einrichten, die über das Netzwerk installiert werden sollen. Siehe "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82

Beispiel 5-2 Erstellen eines Boot-Servers in einem Teilnetz (DVD)

Das folgende Beispiel zeigt, wie Sie einen Boot-Server in einem Teilnetz erstellen. Mit diesen Befehlen wird die Boot-Software vom Solaris-DVD-Abbild in das Verzeichnis /export/home/dvdsparc auf der lokalen Festplatte eines Boot-Servers namens crystal kopiert.

```
# mount -F nfs -o ro crystal:/export/home/dvdsparc /mnt
# mkdir -p /export/home/dvdsparc
# cd /mnt/Solaris_10/Tools
# ./setup_install_server -b /export/home/dvdsparc
# cd /
# umount /mnt
```

Weitere Informationen:	Fortsetzen der Installation		
	Nachdem Sie den Boot-Server eingerichtet haben, müssen Sie den Client als Installationsclient hinzufügen. Informationen zum Hinzufügen von Clients, die über das Netzwerk installiert werden sollen, finden Sie in "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82.		
Siehe auch	Nähere Informationen zum Befehl setup_install_server finden Sie in install_scripts(1M).		

Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild

Nachdem Sie einen Installationsserver und gegebenenfalls einen Boot-Server erstellt haben, müssen Sie die Systeme einrichten, die über das Netzwerk installiert werden sollen. Alle über das Netzwerk zu installierenden Systeme müssen die folgenden Informationen finden können:

- Einen Installationsserver
- Einen Boot-Server, sofern erforderlich
- Die sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren
- Einen Naming Server, wenn Sie Systeminformationen mittels eines Naming Service vorkonfigurieren
- Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden.

Verwenden Sie das folgende add_install_client-Verfahren zum Einrichten von Installationsservern und Clients. Beachten Sie auch die Beispiele für Folgendes:

- Wenn Sie DHCP zum Einrichten der Installationsparameter f
 ür einen SPARC-Client verwenden, lesen Sie Beispiel 5–3.
- Schlagen Sie unter Beispiel 5–4 nach, wenn sich Installationsserver und Client im selben Teilnetz befinden.
- Schlagen Sie unter Beispiel 5–5 nach, wenn sich Installationsserver und Client nicht im selben Teilnetz befinden und Sie kein DHCP verwenden .
- Wenn Sie DHCP zum Einrichten der Installationsparameter f
 ür x86-Clients verwenden, lesen Sie Beispiel 5–6.
- Wenn Sie einen bestimmten seriellen Anschluss zur Anzeige der Ausgabe während der Installation auf einem x86-basierten System verwenden, lesen Sie Beispiel 5–7.

Weitere Optionen für diesen Befehl finden Sie in der Manpage add_install_client(1M).

So fügen Sie über das Netzwerk zu installierende Systeme mit add_install_client hinzu (DVD)

Nach der Erstellung eines Installationsservers müssen Sie die einzelnen über das Netzwerk zu installierenden Systeme einrichten.

Wenden Sie das folgende add_install_client-Verfahren an, um einen über das Netzwerk zu installierenden x86-Client einzurichten.

Bevor Sie
beginnenWenn Sie einen Boot-Server verwenden, muss das Installationsabbild auf dem
Installationsserver zur gemeinsamen Nutzung freigegeben sein, und die entsprechenden
Dienste müssen laufen. Siehe "So erstellen Sie einen SPARC-Installationsserver mit SPARC
oder x86 DVD-Medien" Schritt 6.

Alle zu installierenden Systeme müssen in der Lage sein, folgende Server und Informationen zu finden:

- Installationsserver
- Boot-Server, sofern erforderlich
- sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren
- Einen Naming Server, wenn Sie Systeminformationen mittels eines Naming Service vorkonfigurieren
- Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden.
- 1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem Installationsserver oder Boot-Server an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

- 2 Wenn Sie mit dem Naming Service NIS, NIS+, DNS oder LDAP arbeiten, stellen Sie sicher, dass die folgenden Informationen über das zu installierende System zum Naming Service hinzugefügt wurden.
 - Hostname
 - IP-Adresse

Ethernet-Adresse

Weitere Informationen zu Namen-Services finden Sie im System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).

- 3 Fügt den Client zur /etc/ethers-Datei des Installationsservers hinzu.
 - a. Suchen Sie die ethers-Adresse auf dem Client. Die /etc/ethers-Map wird der lokalen Datei entnommen.

ifconfig -a grep ether ether 8:0:20:b3:39:1d

- b. Öffnen Sie die /etc/ethers-Datei in einem Editor auf dem Installationsserver. Fügen Sie die Adresse der Liste hinzu.
- Wechseln Sie in das Verzeichnis Tools im Abbild der Solaris-DVD. 4

cd /install_dir_path/Solaris_10/Tools

Ins verz pfad Gibt den Pfad zum Verzeichnis Tools an.

- 5 Richten Sie das Clientsystem ein, das über das Netzwerk installiert werden soll.
 - # ./add_install_client -d -s install_server:install_dir_path \
 - -c jumpstart_server:jumpstart_dir_path -p sysid_server:path \ -t boot_image_path -b "boot-property=value" \

 - -e ethernet_address client_name platform_group

- d

Gibt an, dass der Client die Parameter für die Installation über das Netzwerk über DHCP abrufen soll. Wenn Sie nur die Option -d angeben, richtet der Befehl add install client die Installationsinformationen für Clientsysteme derselben Klasse ein, z. B. für alle SPARC-Clientsysteme. Um gezielt die Installationsinformationen für einen bestimmten Client einzurichten, geben Sie die Option -d und die Option -e an.

Verwenden Sie für x86-Clients diese Option, um die Systeme mithilfe von PXE über das Netzwerk zu booten. Diese Option listet die DHCP-Optionen auf, die Sie auf dem DHCP-Server erstellen müssen.

Weitere Informationen zur klassenspezifischen Installation unter Verwendung von DHCP finden Sie unter "Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter" auf Seite 53.

```
- s Installationsserver: Inst verzeichnispfad
  Gibt den Namen und den Pfad des Installationsservers an.
```

- Inst server ist der Host-Name des Installationsservers.
- Inst verz pfad ist der absolute Pfad zum Abbild der Solaris-DVD.

- c Jumpstart-Server : Jumpstart-Verz_pfad

Gibt ein JumpStart-Verzeichnis für die benutzerdefinierte JumpStart-Installation an. *Jumpstart-Server* ist der Host-Name des Servers, auf dem sich das JumpStart-Verzeichnis befindet. *Jumpstart-Verz_pfad* ist der absolute Pfad zum JumpStart-Verzeichnis.

-p Sysid-Server: Pfad

Gibt den Pfad zur sysidcfg-Datei zum Vorkonfigurieren der Systeminformationen an. *Sysid-Server* ist der gültige Host-Name oder die IP-Adresse für den Server, auf dem sich die Datei befindet. *Pfad* ist der absolute Pfad zu dem Verzeichnis, das die Datei sysidcfg enthält.

-t Boot-Abbild-Pfad

Gibt den Pfad zu einem alternativen Boot-Abbild an, wenn Sie ein anderes Boot-Abbild als das im Verzeichnis Tools im aktuelle Solaris-Release-Netzwerkinstallationsabbild, auf der CD oder DVD verwenden möchten.

-b "Boot-Eigenschaft= Wert"

Nur x86-basierte Systeme: Ermöglicht es, den Wert einer Boot-Eigenschaftenvariablen zum Booten des Clients über das Netzwerk festzulegen. Die Option -b muss zusammen mit der Option -e verwendet werden.

In eeprom(1M) sind die Boot-Optionen beschrieben.

-e Ethernet-Adresse

Gibt die Ethernet-Adresse des zu installierenden Clients an. Mit dieser Option können Sie Installationsinformationen für einen spezifischen Client (z. B. eine Boot-Datei für diesen Client) angeben.

Das Präfix nbp. wird in Namen für Boot-Dateien nicht verwendet. Wenn Sie zum Beispiel für einen x86-basierten Client -e 00:07:e9:04:4a:bf angeben, erstellt der Befehl die Boot-Datei 010007E9044ABF.i86pc im Verzeichnis /tftpboot. Die aktuelle Solaris-Release unterstützt jedoch die Verwendung von Legacy-Bootdateien mit dem Präfix nbp.

Weitere Informationen zur Client-spezifischen Installation unter Verwendung von DHCP finden Sie unter "Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter" auf Seite 53.

Client-Name

Dies ist der Name des Systems, das über das Netzwerk installiert werden soll. Hierbei handelt es sich *nicht* um den Host-Namen des Installationsservers.

Plattformgruppe

Dies ist die Plattformgruppe des Systems, das über das Netzwerk installiert werden soll. Weitere Informationen finden Sie unter "Plattformnamen und -gruppen" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Beispiel 5–3 SPARC: Hinzufügen eines SPARC-Installationsclients auf einen SPARC-Installationsserver bei Verwendung von DHCP (DVD)

Das folgende Beispiel zeigt, wie Sie einen Installationsclient hinzufügen, wenn Sie zum Bereitstellen der Installationsparameter im Netzwerk DHCP verwenden. Der Installationsclient heißt basil und ist ein Ultra 5-System. Das Dateisystem /export/home/dvdsparc/Solaris 10/Tools enthält den Befehl add install client.

Näheres zum Einrichten von Installationsparametern für Netzwerkinstallationen mit DHCP finden Sie unter "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

sparc_install_server# cd /export/home/dvdsparc/Solaris_10/Tools
sparc_install_server# ./add_install_client -d basil sun4u

Beispiel 5–4 Hinzufügen eines Installationsclients, der sich im selben Teilnetz wie sein Server befindet (DVD)

Das nachfolgende Beispiel veranschaulicht, wie Sie einen Installationsclient hinzufügen, der sich in demselben Teilnetz wie der Installationsserver befindet. Der Installationsclient heißt basil und ist ein Ultra 5-System. Das Dateisystem /export/home/dvdsparc/ enthält den Befehl add_install_client.

install_server# cd /export/home/dvdsparc/Solaris_10/Tools
install_server# ./add_install_client basil sun4u

Beispiel 5–5 Hinzufügen eines Installationsclients zu einem Boot-Server (DVD)

Das folgende Beispiel zeigt, wie Sie einen Installationsclient zu einem Boot-Server hinzufügen. Der Installationsclient heißt rose und ist ein Ultra 5-System. Führen Sie den Befehl auf dem Boot-Server aus. Mit der Option - s wird der Installationsserver namens rosemary angegeben. Dieser enthält ein Abbild der Solaris Operating System for SPARC Platforms-DVD im Verzeichnis/export/home/dvdsparc.

boot_server# cd /export/home/dvdsparc/Solaris_10/Tools
boot_server# ./add_install_client -s rosemary:/export/home/dvdsparc rose sun4u

Beispiel 5–6 x86: Hinzufügen eines einzelnen x86-Installationsclients auf einem x86-Installationsserver bei Verwendung von DHCP (DVDs)

Das folgende Beispiel zeigt, wie Sie einen x86-Installationsclient zu einem Installationsserver hinzufügen, wenn Sie zum Bereitstellen der Installationsparameter im Netzwerk DHCP verwenden.

 Mit der Option -d wird angegeben, dass die Clients zur Konfiguration das DHCP-Protokoll verwenden sollen. Wenn Sie mittels PXE über das Netzwerk booten wollen, müssen Sie das DHCP-Protokoll verwenden.

- Mit der Option e wird festgelegt, dass diese Installation nur auf dem Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf durchgeführt wird.
- Die Option s gibt an, dass die Clients von dem Installationsserver namens rosemary aus installiert werden sollen.

Im Verzeichnis /export/home/dvdx86 dieses Servers befindet sich ein Solaris Operating System for x86 Platforms-DVD-Abbild.

```
x86_install_server# cd /export/boot/dvdx86/Solaris_10/Tools
x86_install_server# ./add_install_client -d -e 00:07:e9:04:4a:bf \
-s rosemary:/export/home/dvdx86 i86pc
```

Die obigen Befehle richten den Client mit der Ethernet-Adresse 00:07:e9:04:4a:bf als Installationsclient ein. Auf dem Installationsserver wird die Boot-Datei 010007E9044ABF.i86pc erstellt. In früheren Solaris-Versionen hieß diese Boot-Datei nbp.010007E9044ABF.i86pc.

Näheres zum Einrichten von Installationsparametern für Netzwerkinstallationen mit DHCP finden Sie unter "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Beispiel 5–7 x86: Angeben einer während der Netzwerkinstallation zu verwendenden seriellen Konsole (DVD)

Das folgende Beispiel zeigt, wie einem Installationsserver ein x86-Installationsclient hinzugefügt und die zur Installation zu verwendende serielle Konsole angegeben wird. In diesem Beispiel wird der Installationsclient auf die folgende Weise eingerichtet:

- Die Option -d gibt an, dass der Client f
 ür die Verwendung von DHCP zum Festlegen von Installationsparametern eingerichtet ist.
- Mit der Option e wird festgelegt, dass diese Installation nur auf dem Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf durchgeführt wird.
- Die Option b weist das Installationsprogramm an, den seriellen Anschluss ttya als Einund Ausgabegerät zu verwenden.

Fügen Sie den Client mit den folgenden Befehlen hinzu.

```
install server# cd /export/boot/dvdx86/Solaris_10/Tools
install server# ./add_install_client -d -e "00:07:e9:04:4a:bf" \
-b "console=ttya" i86pc
```

Die Manpage eeprom(1M) bietet eine vollständige Beschreibung der Boot-Eigenschaftenvariablen und -werte, die Sie mit der Option -b angeben können.

Weitere Fortsetzen der Installation

Bei Verwendung eines DHCP-Servers zur Installation eines x86-basierten Clients über das Netzwerk müssen Sie den DHCP-Server konfigurieren und die in der Ausgabe des Befehls add_install_client -d aufgeführten Optionen und Makros erstellen. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen konfigurieren können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

x86-basierte Systeme: Wenn Sie keinen DHCP-Server verwenden, müssen Sie das System von einer lokalen Solaris-DVD oder Solaris-CD booten.

Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds

Nachdem Sie das System als Installationsclient hinzugefügt haben, können Sie es über das Netzwerk installieren. Dieser Abschnitt beschreibt die folgenden Schritte:

- Eine Anleitung zum Booten und Installieren SPARC-basierter Systeme über das Netzwerk finden Sie in "SPARC: So installieren Sie den Client über das Netzwerk (DVDs)" auf Seite 89.
- Eine Anleitung zum Booten und Installieren x86-basierter Systeme über das Netzwerk finden Sie in "x86: So installieren Sie den Client über das Netzwerk mit GRUB (DVDs)" auf Seite 91.

Siehe auch Weitere Informationen zum Befehl add_install_client entnehmen Sie bitte der Manpage install_scripts(1M).

SPARC: So installieren Sie den Client über das Netzwerk (DVDs)

Bevor Sie beginnen Für dieses Verfahren wird vorausgesetzt, dass Sie zuvor die folgenden Schritte durchführen:

- Richten Sie einen Installationsserver ein. Eine Anleitung zum Erstellen eines Installationsservers von DVD finden Sie in "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76.
- Richten Sie je nach Bedarf einen Boot-Server oder einen DHCP-Server ein. Wenn sich das zu installierende System und der Installationsserver nicht im gleichen Teilnetz befinden, müssen Sie entweder einen Boot-Server einrichten oder einen DHCP-Server verwenden. Eine Anleitung zum Einrichten eines Boot-Servers finden Sie in "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen einrichten können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.
- Stellen Sie die f
 ür die Installation ben
 ötigten Informationen zusammen bzw. nehmen Sie eine Vorkonfiguration vor. Hierzu k
 önnen Sie sich einer oder mehrerer der folgenden Methoden bedienen:
 - Sammeln Sie die Informationen in "Checkliste f
 ür die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Hinweis – Wenn bereits nicht-globale Zonen auf Ihrem System installiert sind, sollten Sie Solaris Live Upgrade zum Aktualisieren oder Patchen Ihres Systems verwenden. Andere Programme zum Aktualisieren des Systems benötigen eventuell deutlich mehr Zeit, da die für die Aktualisierung erforderliche Zeit linear mit der Anzahl an installierten nicht-globalen Zonen ansteigt.

Informationen zum Durchführen eines Upgrades mit Solaris Live Upgrade finden Sie in Teil I, "Ausführen eines Upgrades mit Solaris Live Upgrade" in *Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades*.

- Erstellen Sie eine sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren. Informationen zur Erstellung einer sysidcfg-Datei finden Sie in "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18.
- Richten Sie einen Naming Server für die Vorkonfiguration der Systeminformationen ein. Informationen zum Vorkonfigurieren von Informationen mit einem Naming Service finden Sie in "Vorkonfiguration mit dem Naming Service" auf Seite 47.
- Erzeugen Sie ein Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden. Informationen zum Einrichten einer benutzerdefinierten JumpStart-Installation finden Sie in Kapitel 3,

"Vorbereiten von benutzerdefinierten JumpStart-Installationen (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

1 Schalten Sie das Clientsystem ein.

Wenn das Clientsystem bereits läuft, schalten Sie es auf Run-Level 0.

Die Eingabeaufforderung ok wird angezeigt.

2 Booten Sie das System über das Netzwerk.

 Um die Installation mit der interaktiven Solaris-Installationsoberfläche durchzuführen, geben Sie folgenden Befehl ein.

ok boot net

 Um die Installation mit der interaktiven Solaris-Textinstallation in einer Desktop-Sitzung durchzuführen, geben Sie folgenden Befehl ein.

ok boot net - text

 Um die Installation mit der interaktiven Solaris-Textinstallation in einer Konsolensitzung durchzuführen, geben Sie folgenden Befehl ein.

ok boot net - nowin

Das System bootet über das Netzwerk.

3 Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

- Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Konfigurationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
- Wenn Sie nicht alle Systeminformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Konfigurationsfragen zu beantworten.

Hinweis – Wenn sich die Tastatur selbst identifiziert, wird das Tastaturlayout während der Installation automatisch konfiguriert. Wenn sich die Tastatur nicht selbst identifiziert, können Sie während der Installation in einer Liste der unterstützten Tastaturlayouts auswählen.

PS/2-Tastaturen können sich nicht selbst konfigurieren. Sie werden aufgefordert, das Tastaturlayout während der Installation auszuwählen.

Weitere Informationen finden Sie unter "Das Schlüsselwort keyboard" auf Seite 28.

Bei Verwendung der grafischen Benutzeroberfläche erscheint nach dem Bestätigen der Systemkonfigurationsinformationen der Begrüßungsbildschirm von Solaris.

- 4 Beantworten Sie alle Fragen, wenn Sie dazu aufgefordert werden, um die Installation abzuschließen.
 - Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Installationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2,,,Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
 - Wenn Sie nicht alle Installationsinformationen vorkonfigurieren, verwenden Sie die "Checkliste f
 ür die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Installationsfragen zu beantworten.
- Siehe auchInformationen zum Abschließen einer interaktiven Installation mit der
Solaris-Installations-GUI finden Sie unter "So führen Sie eine Installation bzw. ein Upgrade mit
dem Solaris-Installationsprogramm mit GRUB aus" in Oracle Solaris 10 9/10
Installationshandbuch: Grundinstallationen.

x86: So installieren Sie den Client über das Netzwerk mit GRUB (DVDs)

Die Solaris-Installationsprogramme für x86-basierte Systeme verwenden den GRUB-Bootloader. Hier wird beschrieben, wie Sie ein x86-basiertes System über das Netzwerk mithilfe des GRUB-Bootloaders installieren können. Allgemeine Informationen zum Bootloader GRUB finden Sie in Kapitel 7, "SPARC- und x86-basiertes Booten (Überblick und Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Zur Installation des Systems über das Netzwerk müssen Sie das Clientsystem anweisen, über das Netzwerk zu booten. Den PXE-Netzwerkstart aktivieren Sie auf dem Clientsystem anhand des BIOS-Setup-Programms im System-BIOS, anhand des Netzwerkkarten-BIOS oder mit

Hilfe von beiden. Bei einigen Systemen ist außerdem die Bootgeräte-Prioritätsliste so anzupassen, dass vor anderen Bootgeräten ein Start über das Netzwerk versucht wird. Hinweise zu den einzelnen Setup-Programmen entnehmen Sie bitte der jeweiligen Herstellerdokumentation oder den beim Booten angezeigten Anweisungen für das Setup-Programm.

Bevor Sie beginnen Für dieses Verfahren wird vorausgesetzt, dass Sie zuvor die folgenden Schritte durchführen:

- Richten Sie einen Installationsserver ein. Eine Anleitung zum Erstellen eines Installationsservers von DVD finden Sie in "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76.
- Richten Sie je nach Bedarf einen Boot-Server oder einen DHCP-Server ein. Wenn sich das zu installierende System und der Installationsserver nicht im gleichen Teilnetz befinden, müssen Sie entweder einen Boot-Server einrichten oder einen DHCP-Server verwenden. Eine Anleitung zum Einrichten eines Boot-Servers finden Sie in "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen einrichten können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.
- Stellen Sie die f
 ür die Installation ben
 ötigten Informationen zusammen bzw. nehmen Sie eine Vorkonfiguration vor. Hierzu k
 önnen Sie sich einer oder mehrerer der folgenden Methoden bedienen:
 - Sammeln Sie die Informationen in "Checkliste f
 ür die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Hinweis – Wenn bereits nicht-globale Zonen auf Ihrem System installiert sind, sollten Sie Solaris Live Upgrade zum Aktualisieren oder Patchen Ihres Systems verwenden. Andere Programme zum Aktualisieren des Systems benötigen eventuell deutlich mehr Zeit, da die für die Aktualisierung erforderliche Zeit linear mit der Anzahl an installierten nicht-globalen Zonen ansteigt.

Informationen zum Durchführen eines Upgrades mit Solaris Live Upgrade finden Sie in Teil I, "Ausführen eines Upgrades mit Solaris Live Upgrade" in *Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades*.

- Erstellen Sie eine sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren. Informationen zur Erstellung einer sysidcfg-Datei finden Sie in "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18.
- Richten Sie einen Naming Server für die Vorkonfiguration der Systeminformationen ein. Informationen zum Vorkonfigurieren von Informationen mit einem Naming Service finden Sie in "Vorkonfiguration mit dem Naming Service" auf Seite 47.

 Erzeugen Sie ein Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden. Informationen zum Einrichten einer benutzerdefinierten JumpStart-Installation finden Sie in Kapitel 3, "Vorbereiten von benutzerdefinierten JumpStart-Installationen (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Außerdem wird bei diesem Verfahren davon ausgegangen, dass Ihr System über das Netzwerk booten kann.

1 Starten Sie das System.

2 Geben Sie die Tastenkombination zum Aufrufen des System-BIOS ein.

Einige PXE-fähige Netzwerkkarten ermöglichen einen PXE-Start, wenn als Antwort auf eine kurze Eingabeaufforderung beim Booten eine bestimmte Tastenkombination betätigt wird.

3 Im System-BIOS geben Sie an, dass das System über das Netzwerk booten soll.

Informationen zum Festlegen der Boot-Priorität im BIOS entnehmen Sie bitte der Dokumentation zu Ihrer Hardware.

4 Beenden Sie das BIOS.

Das System bootet über das Netzwerk. Das GRUB-Menü wird angezeigt.

Hinweis – Je nach Konfiguration Ihres Netzwerkinstallationsservers kann sich das auf Ihrem System angezeigte GRUB-Menü von dem im folgenden Beispiel angezeigten Menü unterscheiden.

```
GNU GRUB version 0.95 (631K lower / 2095488K upper memory)
+------+
| Solaris 10 9/10 /cdrom0
|
|
|
+-----+
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

- 5 Wählen Sie die entsprechende Installationsoption aus.
 - Zur Installation des Betriebssystems Solaris über das Netzwerk wählen Sie aus dem Menü den entsprechenden Solaris-Eintrag aus. Drücken Sie dann die Eingabetaste.

Wählen Sie diesen Eintrag, wenn Sie das Betriebssystem Solaris von dem in "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76 erstellten Netzwerkinstallationsserver aus installieren wollen.

Führen Sie die folgenden Anweisungen aus, um das Betriebssystem Solaris über das Netzwerk mit spezifischen Boot-Argumenten zu installieren.

Es kann sein, dass Sie spezifische Boot-Argumente einstellen müssen, wenn Sie die Gerätekonfiguration während der Installation ändern wollen und diese Boot-Argumente vorher nicht mit dem Befehl add_install_client (siehe "So fügen Sie über das Netzwerk zu installierende Systeme mit add_install_client hinzu (DVD)" auf Seite 83) angegeben haben.

a. Wählen Sie im GRUB-Menü die Installationsoption, die geändert werden soll. Drücken Sie dann die Taste \"e\".

Im GRUB-Menü werden Boot-Befehle angezeigt, die ungefähr dem folgenden Text entsprechen.

kernel /I86pc.Solaris_10/multiboot kernel/unix \
-B install_media=192.168.2.1:/export/cdrom0/boot \
module /platform/i86pc/boot_archive

b. Wählen Sie mit den Pfeiltasten den Boot-Eintrag aus, der geändert werden soll. Drücken Sie dann die Taste "e".

Der zu bearbeitende Boot-Befehl wird im GRUB-Bearbeitungsfenster angezeigt.

c. Geben Sie die gewünschten Boot-Argumente bzw. -Optionen ein.

Die Befehlssyntax für das Grub-Bearbeitungsmenü ist wie folgt:

grub edit>kernel /image_directory/multiboot kernel/unix/ \
install [url|ask] -B options install_media=media_type

Informationen zu Boot-Argumenten und der Befehlssyntax finden Sie in Tabelle 9–1.

d. Drücken Sie die Eingabetaste, um die Änderungen zu übernehmen und zum GRUB-Menü zurückzukehren.

Hinweis – Drücken Sie die Escape-Taste, um die Änderungen zu verwerfen und zum GRUB-Menü zurückzukehren.

Das GRUB-Menü wird angezeigt. Die am Boot-Befehl vorgenommenen Änderungen sind jetzt sichtbar.

e. Drücken Sie im GRUB-Benutzermenü die Taste b, um die Installation zu beginnen.

Das Solaris-Installationsprogramm überprüft die Standard-Boot-Festplatte, um zu ermitteln, ob die Voraussetzungen für eine Installation bzw. ein Upgrade des Systems erfüllt sind. Wenn die Solaris-Installation die Systemkonfiguration nicht erkennen kann, werden Sie vom Programm zur Eingabe der fehlenden Informationen aufgefordert.

Nach Abschluss der Überprüfung wird die Installationsauswahl angezeigt.

6 Wählen Sie eine Installationsart aus.

In der Installationsauswahl sehen Sie die folgenden Optionen:

Select the type of installation you want to perform:

1 Solaris Interactive
2 Custom JumpStart
3 Solaris Interactive Text (Desktop session)
4 Solaris Interactive Text (Console session)
5 Apply driver updates
6 Single user shell
Enter the number of your choice followed by the <ENTER> key.
Alternatively, enter custom boot arguments directly.
If you wait 30 seconds without typing anything,
an interactive installation will be started.

- Wählen Sie eine der folgenden Optionen, um das Betriebssystem Solaris zu installieren.
 - Wenn Sie die Installation mit der interaktiven Solaris-Installations-GUI vornehmen möchten, geben Sie 1ein und drücken dann die Eingabetaste.
 - Für eine Installation mit dem interaktiven textbasierten Installationsprogramm in einer Desktop-Sitzung geben Sie 3 ein und drücken dann die Eingabetaste.

Wählen Sie diese Installationsart aus, um die standardmäßige Aktivierung des GUI-Installationsprogramms außer Kraft zu setzen und das textbasierte Installationsprogramm auszuführen.

• Für eine Installation mit dem interaktiven textbasierten Installationsprogramm in einer Konsolensitzung geben Sie 4 ein und drücken dann die Eingabetaste.

Wählen Sie diese Installationsart aus, um die standardmäßige Aktivierung des GUI-Installationsprogramms außer Kraft zu setzen und das textbasierte Installationsprogramm auszuführen.

Wenn Sie eine ungeführte, benutzerdefinierte JumpStart-Installation (Option 2) durchführen möchten, lesen Sie den Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Ausführliche Informationen zur Solaris-Installations-GUI und dem textbasierten Installationsprogramm finden Sie in "Systemvoraussetzungen und Empfehlungen" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Das System konfiguriert die Geräte und Schnittstellen und sucht Konfigurationsdateien. Das Installationsprogramm beginnt. Setzen Sie die Installation mit Schritt 7 fort.

Wählen Sie eine der folgenden Optionen, um vor der Installation Systemverwaltungsaufgaben durchzuführen.

• Aktualisieren von Treibern oder Installation eines Install Time Update (ITU): Datenträger einlegen, "5" eingeben, Eingabetaste betätigen.

Damit das Betriebssystem Solaris auf Ihrem System laufen kann, ist unter Umständen eine Aktualisierung von Treibern bzw. die Installation eines ITU erforderlich. Folgen Sie den Anweisungen für die Aktualisierung des Treibers bzw. ITUs, um die Aktualisierung vorzunehmen.

Ausführen von Systemverwaltungsaufgaben: "6" eingeben, Eingabetaste betätigen.

Wenn Sie vor der Installation Systemverwaltungsaufgaben durchführen wollen, müssen Sie ein einzelnes User Shell-Fenster öffnen. Informationen zu den Systemverwaltungsaufgaben, die vor der Installation ausgeführt werden können, finden Sie in *System Administration Guide: Basic Administration*.

Nachdem Sie die Systemverwaltungsaufgaben abgeschlossen haben, wird wieder die vorherige Liste mit Optionen angezeigt. Wählen Sie die gewünschte Option, um die Installation fortzusetzen.

7 Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

- Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Konfigurationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
- Wenn Sie nicht alle Systeminformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Konfigurationsfragen zu beantworten.

Hinweis – Wenn sich die Tastatur selbst identifiziert, wird das Tastaturlayout während der Installation automatisch konfiguriert. Wenn sich die Tastatur nicht selbst identifiziert, können Sie während der Installation in einer Liste der unterstützten Tastaturlayouts auswählen.

Weitere Informationen finden Sie unter "Das Schlüsselwort keyboard" auf Seite 28.

Hinweis – Während der Installation können Sie den standardmäßigen NFSv4-Domänennamen wählen. Alternativ können Sie einen benutzerdefinierten NFSv4-Domänennamen angeben. Weitere Informationen finden Sie unter "nfs4_domain-Schlüsselwort" auf Seite 38.

Bei Verwendung der grafischen Benutzeroberfläche des Installationsprogramms erscheint nach dem Bestätigen der Systemkonfigurationsinformationen der Begrüßungsbildschirm von Solaris.

- 8 Beantworten Sie alle Fragen, wenn Sie dazu aufgefordert werden, um die Installation abzuschließen.
 - Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Installationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
 - Wenn Sie nicht alle Installationsinformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Installationsfragen zu beantworten.
- 9 Nachdem das System über das Netzwerk gebootet und installiert wurde, weisen Sie es an, künftig von der Festplatte zu booten.

Hinweis – Nachdem das System nach der Installation neu gebootet hat, führt das GRUB-Menü die installierten Betriebssysteme auf. Hierzu gehört auch das neu installierte Betriebssystem Solaris. Wählen Sie Betriebssystem aus, mit dem gebootet werden soll. Wenn Sie keine Auswahl vornehmen, wird die Standardauswahl verwendet.

Weitere Weitere Schritte

Informationen:

Wenn auf Ihrem Rechner mehrere Betriebssysteme installiert sind, müssen Sie dem GRUB-Bootloader mitteilen, mit welcher Priorität diese Betriebssysteme gebootet werden sollen, . Weitere Informationen finden Sie unter "Modifying Boot Behavior on x86 Based Systems" in *System Administration Guide: Basic Administration*.

Siehe auch Informationen zum Abschließen einer interaktiven Installation mit der Solaris-Installations-GUI finden Sie unter "So führen Sie eine Installation bzw. ein Upgrade mit dem Solaris-Installationsprogramm mit GRUB aus" in Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen.

► ◆ ◆ KAPITEL 6

Installieren über das Netzwerk mithilfe von CDs (Vorgehen)

In diesem Kapitel wird beschrieben, wie Sie das Netzwerk und die Systeme mithilfe einer CD einrichten, wenn Sie die Solaris-Software über das Netzwerk installieren wollen. Bei einer Installation über das Netzwerk können Sie die Solaris-Software von einem System, dem Installationsserver, aus installieren, das Zugriff auf die Datenträgerabbilder der aktuellen Solaris-Release hat. Dazu kopieren Sie den Inhalt der CDs auf die Festplatte des Installationsservers. Danach können Sie die Solaris-Software mit jedem der Solaris-Installationsverfahren vom Netzwerk aus installieren. In diesem Kapitel werden die folgenden Themen behandelt:

Hinweis – Ab Version Oracle Solaris 109/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

- "Übersicht der Schritte: Installieren über das Netzwerk mithilfe von CDs" auf Seite 100
- "Erstellen eines Installationsservers mit SPARC- bzw. x86-CDs" auf Seite 102
- "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107
- "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110
- "Installieren des Systems über das Netzwerk mithilfe eines CD-Abbilds" auf Seite 116

Hinweis –

Ab der Solaris-Version 10 11/06 können Sie die Netzwerkeinstellungen bei der Erstinstallation so einrichten, dass alle Netzwerkdienste mit Ausnahme von Secure Shell entweder deaktiviert werden oder nur auf lokale Anfragen reagieren. Diese Sicherheitsoption ist jedoch nur während der Erstinstallation und nicht bei einem Upgrade verfügbar. Bei einem Upgrade werden alle zuvor eingerichteten Dienste beibehalten. Falls erforderlich, können Sie die Netzwerkdienste nach einem Upgrade mithilfe des Befehls netservices einschränken. Siehe "Planung der Netzwerksicherheit" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Die Netzwerkdienste können nach der Installation entweder mithilfe des Befehls netservices open aktiviert werden, oder Sie aktivieren einzelne Dienste mithilfe von SMF-Befehlen. Siehe "Ändern der Sicherheitseinstellungen nach der Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Ab Solaris-Release 10&;10/08 hat sich die Struktur der Solaris-DVD und der Solaris Software-1 CD für die SPARC-Plattform geändert. Slice 0 befindet sich nicht mehr auf der obersten Hierarchieebene der Verzeichnisstruktur. Deswegen sind die Strukturen der x86und SPARC-DVDs sowie der Solaris Software-1 CD jetzt gleich. Diese Strukturänderung vereinfacht das Einrichten eines Installationsservers bei verschiedenen Plattformen wie z.B. SPARC-Installationsserver und x86-Medien.

Übersicht der Schritte: Installieren über das Netzwerk mithilfe von CDs

Aufgabe	Beschreibung	Siehe
(nur x86): Vergewissern Sie sich, dass das System PXE unterstützt.	Wenn Sie ein x86-basiertes System über das Netzwerk installieren wollen, müssen Sie sicherstellen, dass Ihr Rechner PXE zum Booten ohne lokalen Boot-Datenträger nutzen kann. Wenn Ihr x86-basiertes System PXE nicht unterstützt, muss es von einer lokalen DVD bzw. CD gebootet werden.	Lesen Sie dazu in der Dokumentation des Herstellers Ihres BIOS-Systems nach.
Wählen Sie ein Installationsverfahren.	Das BS Solaris bietet verschiedene Installations- oder Upgrade-Verfahren. Wählen Sie das Installationsverfahren, das für Ihre Umgebung am besten geeignet ist.	"Auswählen eines Solaris-Installationsverfahrens in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

TABELLE 6-1 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe von CDs

Aufgabe	Beschreibung	Siehe
Stellen Sie Informationen zu Ihrem System zusammen.	Verwenden Sie die Checkliste, und füllen Sie das Arbeitsblatt aus, um alle Informationen zusammenzustellen, die Sie für die Installation bzw. das Upgrade benötigen.	Kapitel 5, "Zusammenstellen von Informationen vor einer Installation bzw. einem Upgrade (Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades
(Optional) Führen Sie eine Vorkonfiguration der Systeminformationen aus.	Sie können die Systeminformationen vorkonfigurieren und so vermeiden, dass Sie während des Installations- bzw. Upgrade-Vorgangs dazu aufgefordert werden, diese Informationen einzugeben.	Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformatione (Vorgehen)"
Erstellen Sie einen Installationsserver.	Kopieren Sie die Solaris Software-1 CD mit dem Befehl setup_install_server(1M) auf die Festplatte des Installationsservers. Kopieren Sie weitere Solaris Software-CDs und die Solaris Languages-CD mit dem Befehl add_to_install_server(1M) auf die Festplatte des Installationsservers.	"Erstellen eines Installationsservers mit SPARC- bzw. x86-CDs" auf Seite 102
(Optional) Erstellen Sie einen Boot-Server.	Wenn Sie Systeme über das Netzwerk installieren möchten, die sich in einem anderen Teilnetz als der Installationsserver befinden, müssen Sie im Teilnetz der Systeme einen Boot-Server erstellen, damit die Systeme gebootet werden können. Verwenden Sie den Befehl setup_install_server mit der Option -b, um einen Bootserver einzurichten. Bei Verwendung des Dynamic Host Configuration Protocol (DHCP) ist kein Bootserver erforderlich.	"Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107
Fügen Sie die über das Netzwerk zu installierenden Systeme hinzu.	Richten Sie mit dem Befehl add_install_client jedes über das Netzwerk zu installierende System ein. Jedes System, das Sie installieren möchten, muss in der Lage sein, den Installationsserver, gegebenenfalls den Boot-Server und die Konfigurationsinformationen zu finden.	"Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110

 TABELLE 6-1
 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe von CDs (Fortsetzung)

Aufgabe	Beschreibung	Siehe
(Optional) Konfiguration des DHCP-Servers.	 Wenn DHCP Parameter zur Systemkonfiguration und -installation bereitstellen soll, müssen Sie zuerst den DHCP-Server konfigurieren und dann die für die gewünschte Installation erforderlichen Optionen und Makros erstellen. Hinweis – Wenn Sie ein x86-basiertes System über das Netzwerk mithilfe von PXE installieren möchten, müssen Sie einen DHCP-Server konfigurieren. 	Kapitel 13, "Planungen für den DHCP-Service (Aufgaben)" in <i>Systemverwaltungshandbuch:</i> <i>IP Services</i> "Vorkonfiguration der Systemkonfigurationsinformation mit dem DHCP-Service (Vorgehen)" auf Seite 52
Installieren Sie das System über das Netzwerk.	Die Installation beginnt mit dem Booten des Systems über das Netzwerk.	"Installieren des Systems über das Netzwerk mithilfe eines CD-Abbilds" auf Seite 116

 TABELLE 6-1
 Übersicht der Schritte: Einrichten eines Installationsservers mithilfe von CDs (Fortsetzung)

Erstellen eines Installationsservers mit SPARC- bzw. x86-CDs

Der Installationsserver enthält das Installationsabbild, das für die Installation von Systemen über das Netzwerk benötigt wird. Wenn Sie die Solaris-Software über das Netzwerk auf einem System installieren wollen, müssen Sie einen Installationsserver erstellen. Sie brauchen nicht in jedem Fall einen Boot-Server einzurichten.

Hinweis – Ab Version Oracle Solaris 10 9/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

- Wenn Sie die Installationsparameter über DHCP bereitstellen oder wenn sich der Installationsserver und die Clients im selben Teilnetz befinden, benötigen Sie keinen separaten Boot-Server.
- Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Sie können auch für jedes Teilnetz einen Installationsserver erstellen, doch für Installationsserver benötigen Sie mehr Festplattenspeicher.

SPARC: So erstellen Sie mit einer SPARC- bzw. x86-CD einen Installationsserver

Hinweis – Bei diesem Verfahren wird davon ausgegangen, dass Volume Manager auf dem System ausgeführt wird. Wenn Sie den Volume Manager nicht zum Verwalten von Medien verwenden, lesen Sie bitte *System Administration Guide: Devices and File Systems*.

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem System an, das der Installationsserver werden soll.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Das System muss über ein CD-ROM-Laufwerk verfügen und Teil des Netzwerks und des Naming Service am Standort sein. Wenn Sie einen Naming Service verwenden, muss sich das System außerdem bereits in einem Naming Service wie NIS, NIS+, DNS oder LDAP befinden. Wenn Sie keinen Naming Service verwenden, müssen Sie die Informationen über dieses System in Übereinstimmung mit den Richtlinien des jeweiligen Standorts verteilen.

- 2 Legen Sie die Solaris Software-1 CD in das Laufwerk des Systems ein.
- 3 Erstellen Sie ein Verzeichnis für das CD-Abbild.

mkdir -p install_dir_path
Ins_verz_pfad Gibt das Verzeichnis an, in das das CD-Abbild kopiert werden soll.

4 Wechseln Sie in das Verzeichnis Tools auf dem eingehängten Datenträger.

cd /cdrom/cdrom0/Solaris_10/Tools

5 Kopieren Sie das Abbild der CD im Laufwerk auf die Festplatte des Installationsservers.

./setup_install_server install_dir_path

Ins_verz_pfad Gibt das Verzeichnis an, in das das CD-Abbild kopiert werden soll.

Hinweis – Der Befehl setup_install_server gibt an, ob ausreichend Festplattenspeicher für die Solaris Software-Datenträgerabbilder vorhanden ist. Um den verfügbaren Festplattenspeicher zu ermitteln, verwenden Sie den Befehl df -kl.

- 6 Entscheiden Sie, ob der Installationsserver zum Einhängen verfügbar sein muss.
 - Wenn sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet oder Sie mit DHCP arbeiten, brauchen Sie keinen Boot-Server zu erstellen. Fahren Sie mit Schritt 7 fort.
 - Wenn sich das zu installierende System nicht in demselben Teilnetz wie der Installationsserver befindet und Sie nicht mit DHCP arbeiten, gehen Sie wie folgt vor.
 - a. Überprüfen Sie, ob der Pfad zum Abbild auf dem Installationsserver korrekt zur gemeinsamen Nutzung freigegeben ist.

```
      # share | grep install_dir_path
      Ins_verz_pfad
      Gibt den Pfad zu dem Installationsverzeichnis an, in welches das CD-Abbild kopiert wurde.
```

- Wenn der Pfad zum Verzeichnis auf dem Installationsserver angezeigt wird und in den Optionen anon=0 erscheint, fahren Sie mit Schritt 7 fort.
- Wenn der Pfad zum Verzeichnis auf dem Installationsserver nicht angezeigt wird oder anon=0 in den Optionen nicht erscheint, fahren Sie hier fort.
- b. Machen Sie den Installationsserver für den Bootserver verfügbar.

Fügen Sie diesen Eintrag mithilfe des Befehls share in die Datei /etc/dfs/dfstab ein. share -F nfs -o ro,anon=0 -d "install server directory" *install_dir_path*

- c. Prüfen Sie, ob der nfsd-Dämon läuft.
 - Geben Sie den folgenden Befehl ein, wenn auf dem Installationsserver die aktuelle Solaris-Release oder eine kompatible Version ausgeführt wird.

```
# svcs -l svc:/network/nfs/server:default
```

Wenn der nfsd-Dämon online ist, fahren Sie mit Schritt d fort. Wenn der nfsd-Dämon nicht online ist, starten Sie ihn.

svcadm enable svc:/network/nfs/server

 Wenn auf dem Installationsserver Solaris 9 oder eine kompatible Version läuft, geben Sie den folgenden Befehl ein.

ps -ef | grep nfsd

Wenn der nfsd-Dämon läuft, fahren Sie mit Schritt d fort. Wenn der nfsd-Dämon nicht läuft, starten Sie ihn.

```
# /etc/init.d/nfs.server start
```

- d. Geben Sie den Installationsserver zur gemeinsamen Nutzung frei.
 # shareall
- 7 Wechseln Sie in das Root-Verzeichnis (/).
 # cd /
- 8 Lassen Sie die Solaris Software-1 CD auswerfen.
- 9 Legen Sie die Solaris Software 2-CD in das CD-ROM-Laufwerk des Systems ein.
- 10 Wechseln Sie in das Verzeichnis Tools auf dem eingehängten Datenträger.
 # cd /cdrom/cdrom0/Solaris_10/Tools
- Kopieren Sie die CD im CD-ROM-Laufwerk auf die Festplatte des Installationsservers.
 # ./add_to_install_server install_dir_path
 Ins_verz_pfad Gibt das Verzeichnis an, in das das CD-Abbild kopiert werden soll.
- 12 Wechseln Sie in das Root-Verzeichnis (/).
 # cd /
- 13 Lassen Sie die Solaris Software 2-CD auswerfen.
- 14 Wiederholen Sie Schritt 9 bis Schritt 13 für jede Solaris Software-CD, die Sie installieren möchten.
- 15 Legen Sie die Solaris Languages-CD in das CD-ROM-Laufwerk des Systems ein.
- 16 Wechseln Sie in das Verzeichnis Tools auf dem eingehängten Datenträger. # cd /cdrom/cdrom0/Solaris_10/Tools
- Kopieren Sie die CD im CD-ROM-Laufwerk auf die Festplatte des Installationsservers.
 # ./add_to_install_server install_dir_path
 Ins_verz_pfad Gibt das Verzeichnis an, in das das CD-Abbild kopiert werden soll.
- 18 Lassen Sie die CD auswerfen.
- 19 Wiederholen Sie Schritt 15 bis Schritt 18 für die zweite Solaris Languages-CD.
- 20 Wechseln Sie in das Root-Verzeichnis (/). # cd /

21 (Optional) Patchen Sie die Dateien in der Miniroot des vom Befehl setup_install_server erstellten Netzwerkinstallationsabbilds.

Das Anwenden von Patches ist möglicherweise erforderlich, wenn es bei einem Boot-Abbild zu Problemen kommt. Eine schrittweise Anleitung finden Sie in Kapitel 7, "Patchen des Miniroot-Abbilds (Vorgehen)".

- 22 Entscheiden Sie, ob Sie einen Boot-Server erstellen müssen.
 - Wenn Sie mit DHCP arbeiten oder sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet, brauchen Sie keinen Boot-Server zu erstellen. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110 fort.
 - Wenn Sie nicht mit DHCP arbeiten und sich der Client nicht in demselben Teilnetz wie der Installationsserver befindet, müssen Sie einen Boot-Server erstellen. Fahren Sie mit "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107 fort.

Beispiel 6–1 x86: Erstellen eines Installationsservers mit CDs

Das folgende Beispiel zeigt, wie Sie einen Installationsserver erstellen, indem Sie die folgenden CDs in das Verzeichnis /export/home/cdimage des Installationsservers kopieren. Dabei wird vorausgesetzt, dass auf dem Installationsserver die aktuelle Solaris-Release ausgeführt wird.

- Solaris Software-CDs
- Solaris Languages-CDs

Legen Sie die Solaris Software-1 CD in das CD-ROM-Laufwerk des Systems ein.

```
# mkdir -p /export/home/cdimage
# cd /cdrom/cdrom0/Solaris_10/Tools
```

```
# ./setup_install_server /export/home/cdimage
```

- Bei einem separaten Boot-Server führen Sie bitte diese zusätzlichen Schritte durch:
 - 1. Machen Sie den Installationsserver für den Bootserver verfügbar.

Fügen Sie diesen Eintrag mithilfe des Befehls share in die Datei /etc/dfs/dfstab ein.

share -F nfs -o ro,anon=0 -d "install server directory" /export/home/cdimage

2. Überprüfen Sie, ob der nfsd-Dämon online ist. Ist dies nicht der Fall, dann starten Sie den nfsd-Dämon und geben ihn frei.

```
# svcs -l svc:/network/nfs/server:default
# svcadm enable svc:/network/nfs/server
# shareall
```

3. Fahren Sie wie folgt fort.

 Wenn Sie keinen Boot-Server benötigen oder die Schritte für einen separaten Boot-Server durchgeführt haben, fahren Sie bitte fort.

cd /

Lassen Sie die Solaris Software-1 CD auswerfen. Legen Sie die Solaris Software - 2-CD in das CD-ROM-Laufwerk ein.

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdimage
# cd /
```

Wiederholen Sie diese Befehle für jede Solaris Software-CD, die Sie installieren möchten.

Legen Sie die Solaris Languages-CD in das CD-ROM-Laufwerk des Systems ein.

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdimage
```

Lassen Sie die CD auswerfen.

Wiederholen Sie die vorigen Befehle für jede Solaris Languages-CD.

Weitere Fortsetzen der Installation

Informationen:

Nachdem Sie den Installationsserver eingerichtet haben, müssen Sie den Client als Installationsclient hinzufügen. Informationen zum Hinzufügen der zu installierenden Clientsysteme über das Netzwerk finden Sie in "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110.

Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Informationen hierzu finden Sie in "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107.

Siehe auch Nähere Informationen zu den Befehlen setup_install_server und add_to_install_server finden Sie in install_scripts(1M).

Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes

Sie müssen einen Installationsserver erstellen, im die Solaris-Software über ein Netzwerk auf einem System zu erstellen. Sie brauchen nicht in jedem Fall einen Boot-Server einzurichten. Ein

Boot-Server enthält so viel Boot-Software, dass Systeme vom Netzwerk aus gebootet werden können, und danach führt der Installationsserver die Installation der Solaris-Software durch.

Hinweis – Ab Version Oracle Solaris 10 9/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

- Wenn Sie die Installationsparameter über DHCP bereitstellen oder wenn sich der Installationsserver und die Clients im selben Teilnetz befinden, benötigen Sie keinen Boot-Server. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110 fort.
- Wenn sich der Installationsserver und die Clients nicht im selben Teilnetz befinden und Sie nicht mit DHCP arbeiten, müssen Sie für jedes Teilnetz einen eigenen Boot-Server einrichten. Sie können auch für jedes Teilnetz einen Installationsserver erstellen, doch für Installationsserver benötigen Sie mehr Festplattenspeicher.

So erstellen Sie einen Boot-Server in einem Teilnetz mithilfe eines CD-Abbildes

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem System an, das der Boot-Server für das Teilnetz werden soll.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

Das System muss über ein lokales CD-ROM-Laufwerk verfügen oder Zugriff auf die entfernten Datenträgerabbilder der aktuellen Solaris-Release haben, die sich normalerweise auf dem Installationsserver befinden. Wenn Sie einen Naming Service verwenden, muss sich das System im Naming Service befinden. Wenn Sie keinen Naming Service verwenden, müssen Sie die Informationen über dieses System in Übereinstimmung mit den Richtlinien des jeweiligen Standorts verteilen.

2 Hängen Sie das Abbild der Solaris Software-1 CD vom Installationsserver ein.

mount -F nfs -o ro server_name:path /mnt

Server_Name: Pfad Der Name des Installationsservers und der absolute Pfad zu dem Abbild des Datenträgers
3 Erstellen Sie ein Verzeichnis für das Boot-Abbild.

```
# mkdir -p boot_dir_pathBoot-Verzeichnispfad Gibt das Verzeichnis an, in das die Boot-Software kopiert werden soll.
```

- 4 Wechseln Sie im Abbild der Solaris Software-1 CD in das Verzeichnis Tools. # cd /mnt/Solaris_10/Tools
- 5 Kopieren Sie die Boot-Software auf den Boot-Server.

```
      # ./setup_install_server -b boot_dir_path

      -b
      Gibt an, dass das System als Boot-Server eingerichtet werden soll.

      Boot-Verzeichnispfad
      Gibt das Verzeichnis an, in das die Boot-Software kopiert werden soll.
```

Hinweis – Der Befehl setup_install_server gibt an, ob ausreichend Festplattenspeicher für die Abbilder vorhanden ist. Um den verfügbaren Festplattenspeicher zu ermitteln, verwenden Sie den Befehl df -kl.

6 Wechseln Sie in das Root-Verzeichnis (/).

cd /

- 7 Hängen Sie das Installationsabbild aus.
 - # umount /mnt

Beispiel 6-2 Erstellen eines Boot-Servers in einem Teilnetz mithilfe von CDs

Das folgende Beispiel zeigt, wie Sie einen Boot-Server in einem Teilnetz erstellen. Mit diesen Befehlen kopieren Sie die Boot-Software vom Solaris Software for SPARC Platforms -1-CD-Abbild in das Verzeichnis /export/install/boot auf der lokalen Festplatte des Systems.

```
# mount -F nfs -o ro crystal:/export/install/boot /mnt
# mkdir -p /export/install/boot
# cd /mnt/Solaris_10/Tools
# ./setup_install_server -b /export/install/boot
# cd /
# umount /mnt
```

In diesem Beispiel wird die CD eingelegt und automatisch eingehängt, bevor der Befehl ausgeführt wird. Nach Ausführung des Befehls wird die CD entfernt.

Weitere Informationen:	Fortsetzen der Installation			
inormationen.	Nachdem Sie den Boot-Server eingerichtet haben, müssen Sie den Client als Installationsclient hinzufügen. Informationen zum Hinzufügen der zu installierenden Clientsysteme über das Netzwerk finden Sie in "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110.			
Siehe auch	Nähere Informationen zum Befehl setup_install_server finden Sie in install_scripts(1M).			

Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild

Nachdem Sie einen Installationsserver und gegebenenfalls einen Boot-Server erstellt haben, müssen Sie die Systeme einrichten, die über das Netzwerk installiert werden sollen. Alle über das Netzwerk zu installierenden Systeme müssen die folgenden Informationen finden können:

Hinweis – Ab Version Oracle Solaris 10 9/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

- Einen Installationsserver
- Einen Boot-Server, sofern erforderlich
- Die sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren
- Einen Naming Server, wenn Sie Systeminformationen mittels eines Naming Service vorkonfigurieren
- Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden.

Verwenden Sie das folgende add_install_client-Verfahren zum Einrichten von Installationsservern und Clients.

Weitere Optionen für diesen Befehl finden Sie in der Manpage add_install_client(1M).

So fügen Sie über das Netzwerk zu installierende Systeme mit add_install_client hinzu (CDs)

Nach der Erstellung eines Installationsservers müssen Sie die einzelnen über das Netzwerk zu installierenden Systeme einrichten.

Wenden Sie das folgende add_install_client-Verfahren an, um einen über das Netzwerk zu installierenden x86-Client einzurichten.

Bevor SieWenn Sie einen Boot-Server eingerichtet haben, müssen Sie sich vergewissern, dass das
Installationsabbild auf dem Installationsserver zur gemeinsamen Nutzung freigegeben ist.
Lesen Sie das Verfahren "So erstellen Sie einen Installationsserver," Schritt 6.

Alle zu installierenden Systeme müssen in der Lage sein, folgende Server und Informationen zu finden:

- Einen Installationsserver
- Einen Boot-Server, sofern erforderlich
- Die sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren
- Einen Naming Server, wenn Sie Systeminformationen mittels eines Naming Service vorkonfigurieren
- Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden.
- 1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle bei dem Installationsserver oder Boot-Server an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

- 2 Wenn Sie mit dem Naming Service NIS, NIS+, DNS oder LDAP arbeiten, stellen Sie sicher, dass die folgenden Informationen über das zu installierende System zum Naming Service hinzugefügt wurden.
 - Hostname
 - IP-Adresse
 - Ethernet-Adresse

Weitere Informationen zu Namen-Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Wechseln Sie im Abbild der CD der aktuellen Solaris-Release auf dem Installationsserver in das 3 Verzeichnis Tools, indem Sie Folgendes eingeben:

cd /install_dir_path/Solaris_10/Tools

Ins_verz_pfad Gibt den Pfad zum Verzeichnis Tools an.

- Fügt den Client zur /etc/ethers-Datei des Installationsservers hinzu. 4
 - a. Suchen Sie die ethers-Adresse auf dem Client. Die /etc/ethers-Map wird der lokalen Datei entnommen.

```
# ifconfig -a grep ether
ether 8:0:20:b3:39:1d
```

- b. Öffnen Sie die /etc/ethers-Datei in einem Editor auf dem Installationsserver. Fügen Sie die Adresse der Liste hinzu.
- 5 Richten Sie das Clientsystem ein, das über das Netzwerk installiert werden soll.
 - # ./add install client -d -s install_server:install_dir_path \
 - -c jumpstart_server:jumpstart_dir_path -p sysid_server:path \
 -t boot_image_path -b "network_boot_variable=value" \

 - -e ethernet_address client_name platform_group

- d

Gibt an, dass der Client die Parameter für die Installation über das Netzwerk per DHCP abrufen soll. Wenn Sie nur die Option -d angeben, richtet der Befehl add install client die Installationsinformationen für Clientsysteme derselben Klasse ein, z. B. für alle SPARC-Clientsysteme. Um gezielt die Installationsinformationen für einen bestimmten Client einzurichten, geben Sie die Option - d und die Option - e an.

Verwenden Sie für x86-Clients diese Option, um die Systeme mithilfe von PXE über das Netzwerk zu booten. Diese Option listet die DHCP-Optionen auf, die Sie auf dem DHCP-Server erstellen müssen.

Weitere Informationen zur klassenspezifischen Installation unter Verwendung von DHCP finden Sie unter "Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter" auf Seite 53.

- s Installationsserver:Inst_verzeichnispfad

Gibt den Namen und den Pfad des Installationsservers an.

- Installationsserver ist der Host-Name des Installationsservers.
- *Inst_verz_pfad* ist der absolute Pfad zum Abbild der CD der aktuellen Solaris-Release.

- c Jumpstart-Server: Jumpstart-Verz_pfad

Gibt ein JumpStart-Verzeichnis für die benutzerdefinierte JumpStart-Installation an. Jumpstart-Server ist der Host-Name des Servers, auf dem sich das JumpStart-Verzeichnis befindet. Jumpstart-Verz_pfad ist der absolute Pfad zum JumpStart-Verzeichnis.

-p Sysid-Server: Pfad

Gibt den Pfad zur sysidcfg-Datei zum Vorkonfigurieren der Systeminformationen an. *Sysid-Server* ist der gültige Host-Name oder die IP-Adresse für den Server, auf dem sich die Datei befindet. *Pfad* ist der absolute Pfad zu dem Verzeichnis, das die Datei sysidcfg enthält.

-t Boot-Abbild-Pfad

Gibt den Pfad zu einem alternativen Boot-Abbild an, wenn Sie ein anderes Boot-Abbild als das im Verzeichnis \"Tools\" im aktuelle Solaris-Release-Netzwerkinstallationsabbild, auf der CD oder DVD verwenden möchten.

-b "Boot-Eigenschaft= Wert"

Nur x86-basierte Systeme: Ermöglicht es, den Wert einer Boot-Eigenschaftenvariablen zum Booten des Clients über das Netzwerk festzulegen. Die Option -b muss zusammen mit der Option -e verwendet werden.

In eeprom(1M) sind die Boot-Optionen beschrieben.

-e Ethernet-Adresse

Gibt die Ethernet-Adresse des zu installierenden Clients an. Mit dieser Option können Sie Installationsinformationen für einen spezifischen Client (z. B. eine Boot-Datei für diesen Client) angeben.

Das Präfix nbp. wird in Namen für Boot-Dateien nicht verwendet. Wenn Sie zum Beispiel für einen x86-basierten Client -e 00:07:e9:04:4a:bf angeben, erstellt der Befehl die Boot-Datei 010007E9044ABF.i86pc im Verzeichnis /tftpboot. Die aktuelle Solaris-Release unterstützt jedoch die Verwendung von Legacy-Bootdateien mit dem Präfix nbp.

Weitere Informationen zur Client-spezifischen Installation unter Verwendung von DHCP finden Sie unter "Erzeugen von DHCP-Optionen und -Makros für Solaris-Installationsparameter" auf Seite 53.

Client-Name

Dies ist der Name des Systems, das über das Netzwerk installiert werden soll. Hierbei handelt es sich *nicht* um den Host-Namen des Installationsservers.

Plattformgruppe

Dies ist die Plattformgruppe des Systems, das über das Netzwerk installiert werden soll. Eine detaillierte Liste der Plattformgruppen finden Sie in "Plattformnamen und -gruppen" in *Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.*

Beispiel 6–3 SPARC: Hinzufügen eines SPARC-Installationsclients auf einen SPARC-Installationsserver bei Verwendung von DHCP (CDs)

Das folgende Beispiel zeigt, wie Sie einen Installationsclient hinzufügen, wenn Sie zum Bereitstellen der Installationsparameter im Netzwerk DHCP verwenden. Der Installationsclient heißt basil und ist ein Ultra 5-System. Das Dateisystem /export/home/cdsparc/Solaris_10/Tools enthält den Befehladd_install client.

Näheres zum Einrichten von Installationsparametern für Netzwerkinstallationen mit DHCP finden Sie unter "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

sparc_install_server# cd /export/home/cdsparc/Solaris_10/Tools
sparc_install_server# ./add_install_client -d basil sun4u

Beispiel 6–4 Hinzufügen eines Installationsclients, der sich im selben Teilnetz wie sein Server befindet (CDs)

Das folgende Beispiel zeigt, wie Sie einen Installationsclient hinzufügen, der sich im selben Teilnetz wie der Installationsserver befindet. Der Installationsclient heißt basil und ist ein Ultra 5-System. Das Dateisystem /export/home/cdsparc/Solaris_10/Tools enthält den Befehl add_install_client.

install_server# cd /export/home/cdsparc/Solaris_10/Tools
install_server# ./add_install_client basil sun4u

Beispiel 6–5 Hinzufügen eines Installationsclients zu einem Boot-Server (CDs)

Das folgende Beispiel zeigt, wie Sie einen Installationsclient zu einem Boot-Server hinzufügen. Der Installationsclient heißt rose und ist ein Ultra 5-System. Führen Sie den Befehl auf dem Boot-Server aus. Mit der Option - s wird der Installationsserver namens rosemary angegeben. Dieser enthält ein Abbild der aktuelle Solaris-Release-CD im Verzeichnis /export/home/cdsparc.

boot_server# cd /export/home/cdsparc/Solaris_10/Tools boot_server# ./add_install_client -s rosemary:/export/home/cdsparc rose sun4u

Beispiel 6–6 x86: Hinzufügen eines einzelnen x86-Installationsclients auf einem x86-Installationsserver bei Verwendung von DHCP (CDs)

Der GRUB-Bootloader verwendet nicht den DHCP-Klassennamen SUNW. i86pc. Das folgende Beispiel veranschaulicht, wie Sie zu einem Installationsserver einen x86-Installationsclient hinzufügen können, wenn für das Einstellen der Installationsparameter auf dem Netzwerk DHCP verwendet wird.

- Mit der Option d wird angegeben, dass die Clients zur Konfiguration das DHCP-Protokoll verwenden sollen. Wenn Sie mittels PXE über das Netzwerk booten wollen, müssen Sie das DHCP-Protokoll verwenden.
- Mit der Option e wird festgelegt, dass diese Installation nur auf dem Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf durchgeführt wird.

 Die Option - s gibt an, dass die Clients von dem Installationsserver namens rosemary aus installiert werden sollen.

Im Verzeichnis /export/home/cdx86 dieses Servers befindet sich ein Solaris Operating System for x86 Platforms-DVD-Abbild:

```
x86_install_server# cd /export/boot/cdx86/Solaris_10/Tools
x86_install_server# ./add_install_client -d -e 00:07:e9:04:4a:bf \
-s rosemary:/export/home/cdx86 i86pc
```

Die obigen Befehle richten einen Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf als Installationsclient ein. Auf dem Installationsserver wird die Boot-Datei 010007E9044ABF.i86pc erstellt. In früheren Solaris-Versionen hieß diese Boot-Datei nbp.010007E9044ABF.i86pc.

Näheres zum Einrichten von Installationsparametern für Netzwerkinstallationen mit DHCP finden Sie unter "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Beispiel 6–7 x86: Angeben einer während der Netzwerkinstallation zu verwendenden seriellen Konsole (CDs)

Das folgende Beispiel zeigt, wie einem Installationsserver ein x86-Installationsclient hinzugefügt und die zur Installation zu verwendende serielle Konsole angegeben wird. In diesem Beispiel wird der Installationsclient auf die folgende Weise eingerichtet:

- Die Option -d gibt an, dass der Client f
 ür die Verwendung von DHCP zum Festlegen von Installationsparametern eingerichtet ist.
- Mit der Option e wird festgelegt, dass diese Installation nur auf dem Client mit der Ethernet-Adresse 00:07:e9: 04:4a: bf durchgeführt wird.
- Die Option b weist das Installationsprogramm an, den seriellen Anschluss ttya als Einund Ausgabegerät zu verwenden.

Fügen Sie den Client hinzu.

```
install server# cd /export/boot/cdx86/Solaris_10/Tools
install server# ./add_install_client -d -e "00:07:e9:04:4a:bf" \
-b "console=ttya" i86pc
```

Die Manpage eeprom(1M) bietet eine vollständige Beschreibung der Boot-Eigenschaftenvariablen und -werte, die Sie mit der Option -b angeben können.

Weitere Fortsetzen der Installation

Informationen:

Bei Verwendung eines DHCP-Servers zur Installation eines x86-basierten Clients über das Netzwerk müssen Sie den DHCP-Server konfigurieren und die in der Ausgabe des Befehls add_install_client -d aufgeführten Optionen und Makros erstellen. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen konfigurieren können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

x86-basierte Systeme: Wenn Sie keinen DHCP-Server verwenden, müssen Sie das System von einer lokalen Solaris-DVD oder Solaris-CD booten.

Siehe auch Weitere Informationen zum Befehl add_install_client entnehmen Sie bitte der Manpage install_scripts(1M).

Installieren des Systems über das Netzwerk mithilfe eines CD-Abbilds

Hinweis – Ab Version Oracle Solaris 10 9/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

Nachdem Sie das System als Installationsclient hinzugefügt haben, können Sie es über das Netzwerk installieren. Dieser Abschnitt beschreibt die folgenden Schritte:

- Eine Anleitung zum Booten und Installieren SPARC-basierter Systeme über das Netzwerk finden Sie in "SPARC: So installieren Sie den Client über das Netzwerk (CDs)" auf Seite 116.
- Eine Anleitung zum Booten und Installieren x86-basierter Systeme über das Netzwerk finden Sie in "x86: So installieren Sie den Client über das Netzwerk mit GRUB (CDs)" auf Seite 119.

SPARC: So installieren Sie den Client über das Netzwerk (CDs)

Bevor Sie beginnen Für dieses Verfahren wird vorausgesetzt, dass Sie zuvor die folgenden Schritte durchführen:

- Richten Sie einen Installationsserver ein. Eine Anleitung zum Erstellen eines Installationsservers von CD finden Sie in "SPARC: So erstellen Sie mit einer SPARC- bzw. x86-CD einen Installationsserver" auf Seite 103.
- Richten Sie je nach Bedarf einen Boot-Server oder einen DHCP-Server ein. Wenn sich das zu installierende System und der Installationsserver nicht im gleichen Teilnetz befinden, müssen Sie entweder einen Boot-Server einrichten oder einen DHCP-Server verwenden. Eine Anleitung zum Einrichten eines Boot-Servers finden Sie in "Erstellen eines

Boot-Servers in einem Teilnetz mithilfe eines CD-Abbildes" auf Seite 107. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen einrichten können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

- Stellen Sie die f
 ür die Installation ben
 ötigten Informationen zusammen bzw. nehmen Sie eine Vorkonfiguration vor. Hierzu k
 önnen Sie sich einer oder mehrerer der folgenden Methoden bedienen:
 - Sammeln Sie die Informationen in "Checkliste f
 ür die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.
 - Erstellen Sie eine sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren. Informationen zur Erstellung einer sysidcfg-Datei finden Sie in "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18.
 - Richten Sie einen Naming Server f
 ür die Vorkonfiguration der Systeminformationen ein. Informationen zum Vorkonfigurieren von Informationen mit einem Naming Service finden Sie in "Vorkonfiguration mit dem Naming Service" auf Seite 47.
 - Erzeugen Sie ein Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden. Informationen zum Einrichten einer benutzerdefinierten JumpStart-Installation finden Sie in Kapitel 3, "Vorbereiten von benutzerdefinierten JumpStart-Installationen (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

1 Schalten Sie das Clientsystem ein.

Wenn das Clientsystem bereits läuft, schalten Sie es auf Run-Level 0.

Die Eingabeaufforderung ok wird angezeigt.

- 2 Booten Sie das System über das Netzwerk.
 - Um die Installation mit der interaktiven Solaris-Installationsoberfläche durchzuführen, geben Sie folgenden Befehl ein.

ok **boot net**

- Um die Installation mit der interaktiven Solaris-Textinstallation in einer Desktop-Sitzung durchzuführen, geben Sie folgenden Befehl ein.
 ok boot net - text
- Um die Installation mit der interaktiven Solaris-Textinstallation in einer Konsolensitzung durchzuführen, geben Sie folgenden Befehl ein.

ok boot net - nowin

Das System bootet über das Netzwerk.

3 Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

- Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Konfigurationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
- Wenn Sie nicht alle Systeminformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Konfigurationsfragen zu beantworten.

Hinweis – Wenn sich die Tastatur selbst identifiziert, wird das Tastaturlayout während der Installation automatisch konfiguriert. Wenn sich die Tastatur nicht selbst identifiziert, können Sie während der Installation in einer Liste der unterstützten Tastaturlayouts auswählen.

PS/2-Tastaturen können sich nicht selbst konfigurieren. Sie werden aufgefordert, das Tastaturlayout während der Installation auszuwählen.

Weitere Informationen finden Sie unter "Das Schlüsselwort keyboard" auf Seite 28.

Hinweis – Während der Installation können Sie den standardmäßigen NFSv4-Domänennamen wählen. Alternativ können Sie einen benutzerdefinierten NFSv4-Domänennamen angeben. Weitere Informationen finden Sie unter "NFSv4-Domänenname kann während der Installation konfiguriert werden " in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Bei Verwendung der grafischen Benutzeroberfläche erscheint nach dem Bestätigen der Systemkonfigurationsinformationen der Begrüßungsbildschirm von Solaris.

- 4 Beantworten Sie alle Fragen, wenn Sie dazu aufgefordert werden, um die Installation abzuschließen.
 - Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Installationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
 - Wenn Sie nicht alle Installationsinformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Installationsfragen zu beantworten.

Siehe auch Informationen zum Abschließen einer interaktiven Installation mit der Solaris-Installations-GUI finden Sie unter "So führen Sie eine Installation bzw. ein Upgrade mit dem Solaris-Installationsprogramm mit GRUB aus" in Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen.

x86: So installieren Sie den Client über das Netzwerk mit GRUB (CDs)

Hinweis – Ab Version Oracle Solaris 10 9/10 wird nur eine DVD bereitgestellt. Solaris Software-CDs werden nicht mehr bereitgestellt.

Siehe "Installieren des Systems über das Netzwerk mithilfe eines DVD-Abbilds" auf Seite 88.

Die Solaris-Installationsprogramme für x86-basierte Systeme verwenden den GRUB-Bootloader. Hier wird beschrieben, wie Sie ein x86-basiertes System über das Netzwerk mithilfe des GRUB-Bootloaders installieren können. Allgemeine Informationen zum Bootloader GRUB finden Sie in Kapitel 7, "SPARC- und x86-basiertes Booten (Überblick und Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Zur Installation des Systems über das Netzwerk müssen Sie das Clientsystem anweisen, über das Netzwerk zu booten. Den PXE-Netzwerkstart aktivieren Sie auf dem Clientsystem anhand des BIOS-Setup-Programms im System-BIOS, anhand des Netzwerkkarten-BIOS oder mit Hilfe von beiden. Bei einigen Systemen ist außerdem die Bootgeräte-Prioritätsliste so anzupassen, dass vor anderen Bootgeräten ein Start über das Netzwerk versucht wird. Hinweise zu den einzelnen Setup-Programmen entnehmen Sie bitte der jeweiligen Herstellerdokumentation oder den beim Booten angezeigten Anweisungen für das Setup-Programm.

Bevor Sie beginnen Für dieses Verfahren wird vorausgesetzt, dass Sie zuvor die folgenden Schritte durchführen:

- Richten Sie einen Installationsserver ein. Eine Anleitung zum Erstellen eines Installationsservers von DVD-finden Sie in "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76.
- Richten Sie je nach Bedarf einen Boot-Server oder einen DHCP-Server ein. Wenn sich das zu installierende System und der Installationsserver nicht im gleichen Teilnetz befinden, müssen Sie entweder einen Boot-Server einrichten oder einen DHCP-Server verwenden. Eine Anleitung zum Einrichten eines Boot-Servers finden Sie in "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80. Informationen darüber, wie Sie einen DHCP-Server für Netzwerkinstallationen einrichten können, finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

- Stellen Sie die f
 ür die Installation ben
 ötigten Informationen zusammen bzw. nehmen Sie eine Vorkonfiguration vor. Hierzu k
 önnen Sie sich einer oder mehrerer der folgenden Methoden bedienen:
 - Sammeln Sie die Informationen in "Checkliste f
 ür die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.
 - Erstellen Sie eine sysidcfg-Datei, wenn Sie Systeminformationen mittels einer sysidcfg-Datei vorkonfigurieren. Informationen zur Erstellung einer sysidcfg-Datei finden Sie in "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18.
 - Richten Sie einen Naming Server für die Vorkonfiguration der Systeminformationen ein. Informationen zum Vorkonfigurieren von Informationen mit einem Naming Service finden Sie in "Vorkonfiguration mit dem Naming Service" auf Seite 47.
 - Erzeugen Sie ein Profil im JumpStart-Verzeichnis auf dem Profilserver, wenn Sie das benutzerdefinierte JumpStart-Installationsverfahren verwenden. Informationen zum Einrichten einer benutzerdefinierten JumpStart-Installation finden Sie in Kapitel 3, "Vorbereiten von benutzerdefinierten JumpStart-Installationen (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Außerdem wird bei diesem Verfahren davon ausgegangen, dass Ihr System über das Netzwerk booten kann.

1 Starten Sie das System.

2 Geben Sie die Tastenkombination zum Aufrufen des System-BIOS ein.

Einige PXE-fähige Netzwerkkarten ermöglichen einen PXE-Start, wenn als Antwort auf eine kurze Eingabeaufforderung beim Booten eine bestimmte Tastenkombination betätigt wird.

3 Im System-BIOS geben Sie an, dass das System über das Netzwerk booten soll.

Informationen zum Festlegen der Boot-Priorität im BIOS entnehmen Sie bitte der Dokumentation zu Ihrer Hardware.

4 Beenden Sie das BIOS.

Das System bootet über das Netzwerk. Das GRUB-Menü wird angezeigt.

Hinweis – Je nach Konfiguration Ihres Netzwerkinstallationsservers kann sich das auf Ihrem System angezeigte GRUB-Menü von dem im folgenden Beispiel angezeigten Menü unterscheiden.

Use the ^ and v keys to select which entry is highlighted. Press enter to boot the selected OS, 'e' to edit the commands before booting, or 'c' for a command-line.

- 5 Wählen Sie die entsprechende Installationsoption aus.
 - Zur Installation des Betriebssystems Solaris über das Netzwerk wählen Sie aus dem Menü den entsprechenden Solaris-Eintrag aus. Drücken Sie dann die Eingabetaste.

Wählen Sie diesen Eintrag, wenn Sie das Betriebssystem Solaris von dem in "So erstellen Sie mit einer SPARC- oder -DVD einen x86-Installationsserver" auf Seite 76 erstellten Netzwerkinstallationsserver aus installieren wollen.

 Führen Sie die folgenden Anweisungen aus, um das Betriebssystem Solaris über das Netzwerk mit spezifischen Boot-Argumenten zu installieren.

Es kann sein, dass Sie spezifische Boot-Argumente einstellen müssen, wenn Sie die Gerätekonfiguration während der Installation ändern wollen und diese Boot-Argumente vorher nicht mit dem Befehl add_install_client (siehe "So fügen Sie über das Netzwerk zu installierende Systeme mit add_install_client hinzu (DVD)" auf Seite 83) angegeben haben.

a. Wählen Sie im GRUB-Menü die Installationsoption, die geändert werden soll. Drücken Sie dann die Taste \"e\".

Im GRUB-Menü werden Boot-Befehle angezeigt, die ungefähr dem folgenden Text entsprechen.

kernel /I86pc.Solaris_10/multiboot kernel/unix \
-B install_media=192.168.2.1:/export/cdrom0/boot \
module /platform/i86pc/boot_archive

b. Wählen Sie mit den Pfeiltasten den Boot-Eintrag aus, der geändert werden soll. Drücken Sie dann die Taste "e".

Der zu bearbeitende Boot-Befehl wird im GRUB-Bearbeitungsfenster angezeigt.

c. Geben Sie die gewünschten Boot-Argumente bzw. -Optionen ein.

Die Befehlssyntax für das Grub-Bearbeitungsmenü ist wie folgt:

grub edit>kernel /image_directory/multiboot kernel/unix/ \
install [url|ask] -B options install_media=media_type

Informationen zu Boot-Argumenten und der Befehlssyntax finden Sie in Tabelle 9-1.

d. Drücken Sie die Eingabetaste, um die Änderungen zu übernehmen und zum GRUB-Menü zurückzukehren.

Das GRUB-Menü wird angezeigt. Die am Boot-Befehl vorgenommenen Änderungen sind jetzt sichtbar.

e. Drücken Sie im GRUB-Benutzermenü die Taste b, um die Installation zu beginnen.

Das Solaris-Installationsprogramm überprüft die Standard-Boot-Festplatte, um zu ermitteln, ob die Voraussetzungen für eine Installation bzw. ein Upgrade des Systems erfüllt sind. Wenn die Solaris-Installation die Systemkonfiguration nicht erkennen kann, werden Sie vom Programm zur Eingabe der fehlenden Informationen aufgefordert.

Nach Abschluss der Überprüfung wird die Installationsauswahl angezeigt.

6 Wählen Sie eine Installationsart aus.

In der Installationsauswahl sehen Sie die folgenden Optionen:

Select the type of installation you want to perform:

1 Solaris Interactive 2 Custom JumpStart 3 Solaris Interactive Text (Desktop session) 4 Solaris Interactive Text (Console session) 5 Apply driver updates 6 Single user shell Enter the number of your choice followed by the <ENTER> key. Alternatively, enter custom boot arguments directly.

If you wait 30 seconds without typing anything, an interactive installation will be started.

- Wählen Sie eine der folgenden Optionen, um das Betriebssystem Solaris zu installieren.
 - Wenn Sie die Installation mit der interaktiven Solaris-Installations-GUI vornehmen möchten, geben Sie 1ein und drücken dann die Eingabetaste.
 - Für eine Installation mit dem interaktiven textbasierten Installationsprogramm in einer Desktop-Sitzung geben Sie 3 ein und drücken dann die Eingabetaste.

Wählen Sie diese Installationsart aus, um die standardmäßige Aktivierung des GUI-Installationsprogramms außer Kraft zu setzen und das textbasierte Installationsprogramm auszuführen.

• Für eine Installation mit dem interaktiven textbasierten Installationsprogramm in einer Konsolensitzung geben Sie 4 ein und drücken dann die Eingabetaste.

Wählen Sie diese Installationsart aus, um die standardmäßige Aktivierung des GUI-Installationsprogramms außer Kraft zu setzen und das textbasierte Installationsprogramm auszuführen.

Wenn Sie eine ungeführte, benutzerdefinierte JumpStart-Installation (Option 2) durchführen möchten, lesen Sie den Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien. Ausführliche Informationen zur Solaris-Installations-GUI und dem textbasierten Installationsprogramm finden Sie in "Systemvoraussetzungen und Empfehlungen" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Das System konfiguriert die Geräte und Schnittstellen und sucht nach Konfigurationsdateien. Das Installationsprogramm startet. Setzen Sie die Installation mit Schritt 7 fort.

- Wählen Sie eine der folgenden Optionen, um vor der Installation Systemverwaltungsaufgaben durchzuführen.
 - Aktualisieren von Treibern oder Installation eines Install Time Update (ITU): Datenträger einlegen, "5" eingeben, Eingabetaste betätigen.

Damit das Betriebssystem Solaris auf Ihrem System laufen kann, ist unter Umständen eine Aktualisierung von Treibern bzw. die Installation eines ITU erforderlich. Folgen Sie den Anweisungen für die Aktualisierung des Treibers bzw. ITUs, um die Aktualisierung vorzunehmen.

Ausführen von Systemverwaltungsaufgaben:"6" eingeben, Eingabetaste betätigen.

Wenn Sie vor der Installation Systemverwaltungsaufgaben durchführen wollen, müssen Sie ein einzelnes User Shell-Fenster öffnen. Informationen zu den Systemverwaltungsaufgaben, die vor der Installation ausgeführt werden können, finden Sie in *System Administration Guide: Basic Administration*.

Nachdem Sie die Systemverwaltungsaufgaben abgeschlossen haben, wird wieder die vorherige Liste mit Optionen angezeigt. Wählen Sie die gewünschte Option, um die Installation fortzusetzen.

7 Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

- Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Konfigurationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2, "Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
- Wenn Sie nicht alle Systeminformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Konfigurationsfragen zu beantworten.

Hinweis – Wenn sich die Tastatur selbst identifiziert, wird das Tastaturlayout während der Installation automatisch konfiguriert. Wenn sich die Tastatur nicht selbst identifiziert, können Sie während der Installation in einer Liste der unterstützten Tastaturlayouts auswählen.

Weitere Informationen finden Sie unter "Das Schlüsselwort keyboard" auf Seite 28.

Hinweis – Während der Installation können Sie den standardmäßigen NFSv4-Domänennamen wählen. Alternativ können Sie einen benutzerdefinierten NFSv4-Domänennamen angeben. Weitere Informationen finden Sie unter "NFSv4-Domänenname kann während der Installation konfiguriert werden" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Bei Verwendung der grafischen Benutzeroberfläche des Installationsprogramms erscheint nach dem Bestätigen der Systemkonfigurationsinformationen der Begrüßungsbildschirm von Solaris.

- 8 Beantworten Sie alle Fragen, wenn Sie dazu aufgefordert werden, um die Installation abzuschließen.
 - Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Installationsinformationen ab. Weitere Informationen finden Sie in Kapitel 2,,,Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)".
 - Wenn Sie nicht alle Installationsinformationen vorkonfigurieren, verwenden Sie die "Checkliste für die Installation" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades, um eventuell verbleibende Installationsfragen zu beantworten.
- 9 Nachdem das System über das Netzwerk gebootet und installiert wurde, weisen Sie es an, künftig von der Festplatte zu booten.

Hinweis – Nachdem das System nach der Installation neu gebootet hat, führt das GRUB-Menü die installierten Betriebssysteme auf. Hierzu gehört auch das neu installierte Betriebssystem Solaris. Wählen Sie Betriebssystem aus, mit dem gebootet werden soll. Wenn Sie keine Auswahl vornehmen, wird die Standardauswahl verwendet.

Weitere Weitere Schritte

Wenn auf Ihrem Rechner mehrere Betriebssysteme installiert sind, müssen Sie dem GRUB-Bootloader mitteilen, mit welcher Priorität diese Betriebssysteme gebootet werden sollen, . Weitere Informationen finden Sie in "Modifying Boot Behavior by Editing the GRUB Menu at Boot Time" in *System Administration Guide: Basic Administration*.

Siehe auch Informationen zum Abschließen einer interaktiven Installation mit der Solaris-Installations-GUI finden Sie unter "So führen Sie eine Installation bzw. ein Upgrade mit dem Solaris-Installationsprogramm mit GRUB aus" in *Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen*.

Patchen des Miniroot-Abbilds (Vorgehen)

KAPITEL 7

Dieses Kapitel enthält eine schrittweise Anleitung sowie ein Beispiel für das Patchen des Miniroot-Abbilds beim Einrichten eines Installationsservers.

In diesem Kapitel werden die folgenden Themen behandelt:

- "Patchen des Miniroot-Abbilds (Vorgehen)" auf Seite 127
- "Patchen des Miniroot-Abbilds (Beispiel)" auf Seite 130

Patchen des Miniroot-Abbilds (Vorgehen)

Es kann sein, dass Sie die Dateien in der Miniroot des vom Befehl setup_install_server erstellten Netzwerkinstallationsabbilds patchen müssen.

Informationen zum Miniroot-Abbild (Übersicht)

Die Miniroot ist ein minimales bootfähiges Root-Dateisystem (/), dass sich auf dem Solaris-Installationsdatenträger befindet. Eine Miniroot besteht aus der gesamten Solaris-Software, die zum Booten des Systems für eine Installation bzw. ein Upgrade benötigt wird. Die Miniroot-Software wird vom Installationsdatenträger zum Ausführen einer vollständigen Installation des Betriebssystems Solaris verwendet. Die Miniroot läuft nur während des Installationsvorgangs.

Es kann sein, dass Sie die Miniroot vor der Installation patchen müssen, wenn das Boot-Abbild beim Booten Probleme hat oder Sie Unterstützung für Treiber bzw. Hardware installieren müssen. Beim Patchen des Miniroot-Abbilds wird das Patch nicht auf dem System installiert, auf dem das Betriebssystem Solaris installiert wird, und auch nicht auf dem System, auf dem der Befehl patchadd ausgeführt wird. Das Patchen des Miniroot-Abbilds dient lediglich zum Installieren von Unterstützung für Treiber und Hardware für den Prozess, der die eigentliche Installation des Betriebssystems Solaris ausführt. Hinweis – Dieser Vorgang ist nur zum Patchen der Miniroot und nicht zum Patchen des vollständigen Netzwerkinstallationsabbilds gedacht. Wenn Sie das Netzwerkinstallationsabbild patchen müssen, sollten Sie dies erst nach dem Abschluss der Installation ausführen.

So patchen Sie das Miniroot-Abbild

Gehen Sie wie folgt vor, um das Miniroot-Abbild einer Netzwerkinstallation zu patchen.

Hinweis – Bei diesen Schritten wird davon ausgegangen, dass Sie ein System auf Ihrem Netzwerk haben, das die aktuelle Solaris-Release ausführt und das System über das Netzwerk zugänglich ist.

1 Melden Sie sich als Superuser oder als ein anderer Benutzer mit entsprechenden Rechten bei einem System an, auf dem die aktuelle Solaris-Release ausgeführt wird.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

2 Wechseln Sie in das Verzeichnis Tools des Installationsabbilds, das Sie in Schritt 5 erstellt hatten.

cd install-server-path/install-dir-path/Solaris_10/Tools

Inst-Server-Pfad Der Pfad zum Installationsserver in Ihrem Netzwerk, z. B. /net/installserver-1.

3 Erstellen Sie ein neues Installationsabbild und platzieren Sie das Abbild auf dem System, das die aktuelle Solaris-Release ausführt.

./setup_install_server remote_install_dir_path

Remote_Inst_Verz_Pfad Gibt den Pfad auf die aktuelle Solaris-Release an, in denen das neue Installationsabbild erstellt wird.

Dieser Befehl erstellt ein neues Installationsabbild auf der aktuellen Solaris-Release. Um dieses Installationsabbild zu patchen, müssen Sie dieses Abbild vorübergehend auf einem System platzieren, auf dem die aktuelle Solaris-Release ausgeführt wird.

- 4 Entpacken Sie auf der aktuellen Solaris-Release das Boot-Archiv für die Netzwerkinstallation.
 - # /boot/solaris/bin/root_archive unpackmedia remote_install_dir_path \
 destination_dir

Remote_Inst_Verz_Pfad Gibt den Pfad zum Netzwerkinstallationsabbild der aktuellen Solaris-Release an.

Ziel_VerzGibt den Pfad zum Verzeichnis an, das das entpackte Boot-Archiv
enthält.

- 5 Patchen Sie auf der aktuellen Solaris-Release das entpackte Boot-Archiv.
 - # patchadd -C destination_dir path-to-patch/patch-id
 - Pfad-zum-PatchLegt den Pfad zum Patch, das hinzugefügt werden soll, fest, zum Beispiel
/var/sadm/spool.
 - *patch-id* Legt die ID des anzuwendenden Patches fest.

Mit der Befehlsoption patchadd -M können Sie mehrere Patches angeben. Nähere Informationen entnehmen Sie bitte der Manpage patchadd(1M).



Achtung – Verwenden Sie den Befehl patchadd - C nicht, es sei denn, Sie haben die Patch README-Anweisungen gelesen oder mit dem Sun-Support vor Ort gesprochen.

- 6 Packen Sie auf der aktuellen Solaris-Release das Boot-Archiv.
 - # /boot/solaris/bin/root_archive packmedia remote_install_dir_path \
 destination_dir
- 7 Kopieren Sie die gepatchten Archive in das Installationsabbild auf dem Installationsserver.
 - # cd remote_install_dir_path
 - # find boot Solaris_10/Tools/Boot | cpio -pdum \
 install-server-path/install_dir_path

Nächste Schritte Nachdem Sie den Installationsserver eingerichtet und die Miniroot gepatcht haben, kann es sein, dass Sie einen Boot-Server einrichten oder zusätzliche Systeme über das Netzwerk installieren müssen.

- Wenn Sie mit DHCP arbeiten oder sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet, brauchen Sie keinen Boot-Server zu erstellen. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82 fort.
- Wenn Sie *nicht* mit DHCP arbeiten und sich das zu installierende System in einem anderen Teilnetz als der Installationsserver befindet, müssen Sie einen Boot-Server erstellen. Fahren Sie mit "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80 fort.

Patchen des Miniroot-Abbilds (Beispiel)

In diesem Beispiel werden die Schritte zum Patchen eines Miniroot-Abbilds zum Erstellen einer modifizierten Miniroot beschrieben.

Patchen des Miniroot-Abbilds

In diesem Beispiel führen Sie das Entpacken und Packen der Miniroot auf einem System durch, auf dem die aktuelle Solaris-Release installiert ist.

So modifizieren Sie die Miniroot (Beispiel)

Dieser Vorgang zeigt die Installation eines Kernel-Update-Patches (KU) auf einem Miniroot-Abbild von Solaris 10 9/10. Gehen Sie wie auf dem System, auf dem das Betriebssystem Solaris 10 installiert ist, wie folgt vor und berücksichtigen Sie dabei folgende Aspekte.

- jmp-start1 Der Netzwerkinstallationsserver, auf dem das Betriebssystem Solaris 9 installiert ist
- v20z-1 Ein System auf dem das Betriebssystem Solaris 10 mit GRUB installiert ist
- v20z-1:/export/mr der Speicherort der ungepackten Miniroot
- v20z-1:/export/u1 das Installationsabbild, das zum Modifizieren erstellt wurde

Das Netzwerkinstallationsabbild befindet sich unter /net/jmpstart1/export/images/solaris_10_u1/Solaris_10/Tools .

1 Melden Sie sich als Superuser oder als ein anderer Benutzer mit entsprechenden Rechten bei einem System an, auf dem die aktuelle Solaris-Release ausgeführt wird.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

2 Wechseln Sie in das Verzeichnis, in dem Sie die Miniroot entpacken und das Netzwerkinstallationabbild installieren möchten.

cd /net/server-1/export

3 Legen Sie das Installations- und das Miniroot-Verzeichnis an.

mkdir /export/ul /export/mr

4 Wechseln Sie in das Verzeichnis "Tools", in dem sich die Installationsabbilder von Solaris 10 9/10 befinden.

```
# cd /net/jmp-start1/export/images/solaris_10/Solaris_10/Tools
```

5 Erstellen Sie ein neues Installationsabbild und platzieren Sie das Abbild auf dem System, das die aktuelle Solaris-Release ausführt.

./setup_install_server /export/ul
Verifying target directory...
Calculating the required disk space for the Solaris_10 product
Calculating space required for the installation boot image
Copying the CD image to disk...
Copying Install Boot Image hierarchy...
Install Server setup complete

Das Einrichten des Installationsservers ist jetzt abgeschlossen.

6 Führen Sie den folgenden Befehl aus, um die Miniroot zu entpacken.

/boot/solaris/bin/root_archive unpackmedia /export/ul /export/mr

7 Wechseln Sie die Verzeichnisse.

```
# cd /export/mr/sbin
```

8 Erstellen Sie Kopien der Dateien rc2 und sulogin.

```
# cp rc2 rc2.orig
# cp sulogin sulogin.orig
```

9 Installieren Sie alle erforderlichen Patches in der Miniroot.

patchadd -C /export/mr /export patchid

Patch-ID legt die ID des anzuwendenden Patches fest.

In diesem Beispiel werden fünf Patches auf die Miniroot angewendet.

patchadd -C /export/mr /export/118344-14
patchadd -C /export/mr /export/122035-05
patchadd -C /export/mr /export/119043-10
patchadd -C /export/mr /export/123840-04
patchadd -C /export/mr /export/118855-36

- **10** Exportieren Sie die Variable SVCCFG_REPOSITORY.
 - # export SVCCFG_REPOSITORY=/export/mr/etc/svc/repository.db



Achtung – Die Variable *SVCCFG_REPOSITORY* muss auf das Verzeichnis der Datei repository.db der entpackten Miniroot zeigen. In diesem Beispiel ist dies das Verzeichnis /export/mr/etc/svc. Die Datei repository.db befindet sich im Verzeichnis /etc/svc der entpackten Miniroot. Wenn Sie diese Variable nicht exportieren, wird das Live-Repository modifiziert und ein Live-System deswegen am Booten gehindert.

11 Modifizieren Sie die Datei repository.db der Miniroot.

```
# svccfg -s system/manifest-import setprop start/exec = :true
# svccfg -s system/filesystem/usr setprop start/exec = :true
# svccfg -s system/identity:node setprop start/exec = :true
# svccfg -s system/device/local setprop start/exec = :true
# svccfg -s network/loopback:default setprop start/exec = :true
# svccfg -s metwork/physical:default setprop start/exec = :true
# svccfg -s milestone/multi-user setprop start/exec = :true
```

Weitere Informationen finden Sie in der Manpage svccfg(1M).

12 Wechseln Sie die Verzeichnisse. Stellen Sie dann die ursprünglichen Kopien der Dateien rc2.orig und sulogin.orig wieder her.

```
# cd /export/mr/sbin
# mv rc2.orig rc2
# mv sulogin.orig sulogin
```

13 Packen Sie die modifizierte Miniroot, die die von Ihnen vorgenommenen Änderungen enthält. Kopieren Sie die modifizierte Miniroot in das Verzeichnis / export/u1.

/boot/solaris/bin/root_archive packmedia /export/ul /export/mr

Durch diesen Schritt werden das Verzeichnis /export/u1/boot/miniroot und einige andere erforderliche Dateien ersetzt.

- Nächste Schritte Nachdem Sie den Installationsserver eingerichtet und die Miniroot gepatcht haben, kann es sein, dass Sie einen Boot-Server einrichten oder zusätzliche Systeme über das Netzwerk installieren müssen.
 - Wenn Sie mit DHCP arbeiten oder sich das zu installierende System in demselben Teilnetz wie der Installationsserver befindet, brauchen Sie keinen Boot-Server zu erstellen. Sie sind jetzt fertig. Fahren Sie mit "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem DVD-Abbild" auf Seite 82 fort.
 - Wenn Sie *nicht* mit DHCP arbeiten und sich das zu installierende System in einem anderen Teilnetz als der Installationsserver befindet, müssen Sie einen Boot-Server erstellen. Fahren Sie mit "Erstellen eines Boot-Servers in einem Teilnetz mithilfe eines DVD-Abbildes" auf Seite 80 fort.

♦ KAPITEL 8

Installieren über das Netzwerk (Beispiele)

In diesem Kapitel finden Sie Beispiele, in denen die Verwendung von DVDs oder CDs zur Installation des Betriebssystems Solaris über das Netzwerk veranschaulicht werden.

Für alle Beispiele in diesem Kapitel gelten die folgenden Voraussetzungen.

- Der Installationsserver
 - Ist ein Netzwerk-Installationsabbild.
 - Führt die aktuelle Solaris-Release aus.
 - Ist bereits Teil des Netzwerks und Naming Service am Standort.
- Sie haben alle zur Installation erforderlichen Informationen zusammengetragen oder vorkonfiguriert. Weitere Informationen finden Sie in Kapitel 5, "Zusammenstellen von Informationen vor einer Installation bzw. einem Upgrade (Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades.

Wählen Sie ein Beispiel von einer der folgenden zusätzlichen Optionen aus.

- "Netzwerkinstallation über das gleiche Teilnetz (Beispiele)" auf Seite 134
 - Der Installationsclient befindet sich im gleichen Teilnetz wie der Installationsserver. Aus diesem Grund brauchen Sie keinen Installationsserver zu erstellen.
 - Die Netzwerkinstallation verwendet eine grafische Benutzeroberfläche (GUI) in einer Desktop-Sitzung.
- Network Installation Over a Different Subnet (Examples TBD)
 - Der Installationsclient befindet sich in einem anderen Teilnetz als der Installationsserver. Aus diesem Grund müssen Sie einen Boot-Server erstellen.
 - Die Netzwerkinstallation verwendet ein textbasiertes Installationsprogramm in einer Desktop-Sitzung

Netzwerkinstallation über das gleiche Teilnetz (Beispiele)

Dieser Abschnitt enthält die folgenden Beispiele.

- Beispiel 8-1: SPARC: Installieren im gleichen Teilnetz (mit DVDs)
- Beispiel 8-2: SPARC: Installieren im gleichen Teilnetz (mit CDs)
- Beispiel 8–3: x86: Installieren im gleichen Teilnetz (mit DVDs)
- Beispiel 8-4: x86: Installieren im gleichen Teilnetz (mit CDs)

BEISPIEL 8-1 SPARC: Installieren im gleichen Teilnetz (mit DVDs)

In diesem Beispiel wird ein SPARC-Installationsserver mit SPARC DVDs erstellt.

Für dieses Beispiel gelten die folgenden Voraussetzungen:

- Der Installationsclient befindet sich im gleichen Teilnetz wie der Installationsserver.
- Die Netzwerkinstallation verwendet eine grafische Benutzeroberfläche (GUI) in einer Desktop-Sitzung.
- Die allgemeinen Voraussetzungen für dieses Beispiel können Sie in Kapitel 8, "Installieren über das Netzwerk (Beispiele)" nachlesen.
- 1. Erstellen und Einrichten eines SPARC-Installationsservers

Das folgende Beispiel zeigt, wie Sie einen Installationsserver erstellen, indem Sie die Solaris-DVD in das Verzeichnis /export/home/dvdsparc des Installationsservers kopieren:

- a. Legen Sie die Solaris-DVD in das Laufwerk des SPARC-Systems ein.
- b. Verwenden Sie den folgenden Befehl zum Erstellen eines Verzeichnisses, in dem das DVD-Abbild gespeichert wird. Dieser Befehl wechselt zum Tools-Verzeichnis auf dem eingehängten Datenträger. Dann kopiert der Befehl das DVD-Abbild im Laufwerk auf die Festplatte des Installationsservers.

```
# mkdir -p /export/home/dvdsparc
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./setup_install_server /export/home/dvdsparc
```

2. Installieren des Systems mit einem Netzwerk-Installationsabbild

In diesem Beispiel verwenden Sie die interaktive grafische Benutzeroberfläche zur Installation von Solaris.

- a. Booten Sie das System über das Netzwerk.
- b. Um die Installation mit der interaktiven Solaris-Installationsoberfläche durchzuführen, geben Sie folgenden Befehl ein.

```
ok bootnet - install
```

Das System wird über das Netzwerk installiert.

BEISPIEL 8-1 SPARC: Installieren im gleichen Teilnetz (mit DVDs) (Fortsetzung)

c. Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration. Wenn Sie alle Systemkonfigurationsinformationen vorkonfiguriert haben, fragt das Installationsprogramm keine Konfigurationsinformationen ab.

Nachdem Sie die System-Konfigurationsinformationen bestätigt haben, wird der Solaris-Willkommenbildschirm angezeigt. Die Installation ist abgeschlossen.

Eine ausführlichere Erklärung der in diesem Beispiel verwendeten Netzwerk-Installationsverfahren finden Sie in Kapitel 5, "Installieren über das Netzwerk mithilfe von DVDs (Vorgehen)".

BEISPIEL 8-2 SPARC: Installieren im gleichen Teilnetz (mit CDs)

In diesem Beispiel wird ein SPARC-Installationsserver mit SPARC-CDs erstellt.

Für dieses Beispiel gelten die folgenden Voraussetzungen:

- Der Installationsclient befindet sich im gleichen Teilnetz wie der Installationsserver.
- Die Netzwerkinstallation verwendet eine grafische Benutzeroberfläche (GUI) in einer Desktop-Sitzung.
- Die allgemeinen Voraussetzungen für dieses Beispiel können Sie in Kapitel 8, "Installieren über das Netzwerk (Beispiele)" nachlesen.

1. Erstellen und Einrichten eines SPARC-Installationsservers

Das folgende Beispiel zeigt, wie Sie einen Installationsserver erstellen können, indem Sie die CDs in das Verzeichnis /export/home/cdsparc des Installationsservers kopieren.

- a. Legen Sie die Solaris Software for SPARC Platforms 1-CD in das CD-ROM-Laufwerk des Systems ein.
- b. Verwenden Sie den folgenden Befehl zum Erstellen eines Verzeichnisses, in dem das CD-Abbild gespeichert wird. Der Befehl wechselt zum Tools-Verzeichnis auf dem eingehängten Datenträger und kopiert das Abbild vom Laufwerk auf die Festplatte des Installationsservers.

```
# mkdir -p /export/home/cdsparc
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./setup_install_server /export/home/cdsparc
# cd /
```

2. Fügen Sie die über das Netzwerk zu installierenden Systeme hinzu.

- a. Legen Sie die Solaris Software for SPARC Platforms 2-CD ins CD-ROM-Laufwerk ein.
- b. Verwenden Sie dazu den folgenden Befehl: Der Befehl wechselt zum Tools-Verzeichnis auf der eingehängten CD. Der Befehl kopiert den Inhalt der CD im CD-ROM-Laufwerk auf die Festplatte des Installationsservers. Dann wechselt der Befehl zum Root-Verzeichnis (/).

BEISPIEL 8-2 SPARC: Installieren im gleichen Teilnetz (mit CDs) (Fortsetzung)

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdsparc
# cd /
```

- c. Wiederholen Sie diese Befehle für jede Solaris Software-CD, die Sie installieren möchten.
- d. Legen Sie die erste Solaris Languages for SPARC Platforms-CD in das CD-ROM-Laufwerk ein.

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdsparc
```

- e. Lassen Sie die CD auswerfen.
- f. Wiederholen Sie diese Befehle für jede Solaris Languages for SPARC Platforms-CD-CD, die Sie installieren möchten.
- 3. Installieren des Systems mit einem Netzwerk-Installationsabbild
 - a. Booten Sie das System über das Netzwerk.
 - b. Um die Installation mit der interaktiven Solaris-Installationsoberfläche durchzuführen, geben Sie folgenden Befehl ein.

ok boot net

Das System wird über das Netzwerk installiert.

c. Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

Nachdem Sie die System-Konfigurationsinformationen bestätigt haben, wird der Solaris-Willkommenbildschirm angezeigt. Die Installation ist abgeschlossen.

Eine ausführlichere Erklärung der in diesem Beispiel verwendeten Netzwerk-Installationsverfahren finden Sie in Kapitel 6, "Installieren über das Netzwerk mithilfe von CDs (Vorgehen)".

BEISPIEL 8-3 x86: Installieren im gleichen Teilnetz (mit DVDs)

In diesem Beispiel wird ein x86-Installationsserver mit x86-DVDs erstellt.

Für dieses Beispiel gelten die folgenden Voraussetzungen:

- Der Installationsclient befindet sich im gleichen Teilnetz wie der Installationsserver.
- Die Netzwerkinstallation verwendet eine grafische Benutzeroberfläche (GUI) in einer Desktop-Sitzung.
- Die allgemeinen Voraussetzungen für dieses Beispiel können Sie in Kapitel 8, "Installieren über das Netzwerk (Beispiele)" nachlesen.
- 1. Erstellen und Einrichten eines x86-Installationsservers

BEISPIEL 8-3 x86: Installieren im gleichen Teilnetz (mit DVDs) (Fortsetzung)

Das folgende Beispiel zeigt, wie Sie einen x86-Installationsserver erstellen, indem Sie die Solaris Operating System for x86 Platforms-DVD in das Verzeichnis /export/home/dvdx86 des Installationsservers kopieren:

- a. Legen Sie die Solaris-DVD in das Laufwerk des Systems ein.
- b. Verwenden Sie dazu den folgenden Befehl: Der Befehl erstellt ein Verzeichnis, in dem das Boot-Abbild gespeichert wird. Dann wechselt der Befehl zum Tools-Verzeichnis auf dem eingehängten Datenträger. Als Nächstes wird mit dem Befehl setup_install_server der Inhalt des Datenträgers auf die Festplatte des Installationsservers kopiert:

```
# mkdir -p /export/home/dvdx86
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./setup_install_server /export/home/dvdx86
```

c. Machen Sie den Installationsserver für den Bootserver verfügbar.

Fügen Sie diesen Eintrag mithilfe des Befehls share in die Datei /etc/dfs/dfstab ein.

share -F nfs -o ro,anon=0 -d "install server directory" install_dir_path

d. Überprüfen Sie, ob der nfsd-Dämon online ist. Ist dies nicht der Fall, dann starten Sie den nfsd-Dämon und geben ihn frei.

```
# svcs -l svc:/network/nfs/server:default
# svcadm enable svc:/network/nfs/server
# shareall
# cd /
```

Hinweis – Wenn auf dem Installationsserver Solaris 9 BS oder eine kompatible Version läuft, geben Sie den folgenden Befehl ein:

```
# ps -ef | grep nfsd
```

Bei dieser älteren Versionen setzen Sie, wenn der nfsd-Dämon ausgeführt wird, mit dem nächsten Schritt fort. Wenn der nfsd-Dämon nicht ausgeführt wird, starten Sie ihn.

/etc/init.d/nfs.server start

2. Fügen Sie die über das Netzwerk zu installierenden Systeme hinzu.

Das Dateisystem /export/home/dvdx86/ enthält den Befehl add_install_client . Der Installationsclient heißt basil und ist ein x86-System.

a. Fügt den Client zur /etc/ethers-Datei des Installationsservers hinzu.

Suchen Sie die ethers-Adresse auf dem Client. Die /etc/ethers-Map wird der lokalen Datei entnommen.

BEISPIEL 8-3 x86: Installieren im gleichen Teilnetz (mit DVDs) (Fortsetzung)

ifconfig -a grep ether
ether 8:0:20:b3:39:1d

Öffnen Sie die /etc/ethers-Datei in einem Editor auf dem Installationsserver. Fügen Sie die Adresse der Liste hinzu.

b. Verwenden Sie dazu den folgenden Befehl: Der Befehl wechselt zum Tools-Verzeichnis im Solaris-DVD-Abbild. Darüber hinaus richtet dieser Befehl das Clientsystem so ein, dass es über das Netzwerk installiert werden kann.

install_server# cd /export/home/dvdx86/Solaris_10/Tools
install_server# ./add_install_client basil i86pc

3. Installieren des Systems mit einem Netzwerk-Installationsabbild

Die Solaris-Installationsprogramme für x86-basierte Systeme verwenden den GRUB-Bootloader. In diesem Beispiel wird ein x86-basierte System mit dem GRUB-Bootloader über das Netzwerk installiert.

a. Im System-BIOS geben Sie an, dass das System über das Netzwerk booten soll.

Nachdem Sie das BIOS verlassen haben, wird das System über das Netzwerk installiert. Das GRUB-Menü wird angezeigt.

b. Zur Installation des Betriebssystems Solaris über das Netzwerk wählen Sie aus dem Menü den entsprechenden Solaris-Eintrag aus. Drücken Sie dann die Eingabetaste.

Der Installations-Auswahlbildschirm wird angezeigt.

c. Für eine Installation mit der grafischen interaktiven Solaris-Installationsoberfläche geben Sie 1 ein, und drücken dann die Eingabetaste.

Das Installationsprogramm startet.

d. Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

Nachdem Sie die System-Konfigurationsinformationen bestätigt haben, wird der Solaris-Willkommenbildschirm angezeigt.

Nachdem das System über das Netzwerk gebootet und installiert wurde, weisen Sie es an, künftig von der Festplatte zu booten.

Hinweis – Nachdem das System nach der Installation neu gebootet hat, führt das GRUB-Menü die installierten Betriebssysteme auf. Hierzu gehört auch das neu installierte Betriebssystem Solaris. Wählen Sie Betriebssystem aus, mit dem gebootet werden soll. Wenn Sie keine Auswahl vornehmen, wird die Standardauswahl verwendet.

Weitere Informationen finden Sie in den folgenden Referenzen.

Verfahren	Referenz
Ausführlichere Beschreibung der in diesem Beispiel verwendeten Netzwerk-Installationsverfahren	Kapitel 5, "Installieren über das Netzwerk mithilfe von DVDs (Vorgehen)"
Informationen zur Installation mit der grafischen interaktiven Solaris-Installationsoberfläche	"So führen Sie eine Installation bzw. ein Upgrade mit dem Solaris-Installationsprogramm mit GRUB aus" in Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen
Allgemeine Informationen zum GRUB-Bootloader	Kapitel 7, "SPARC- und x86-basiertes Booten (Überblick und Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

BEISPIEL 8-3 x86: Installieren im gleichen Teilnetz (mit DVDs) (Fortsetzung)

BEISPIEL 8-4 x86: Installieren im gleichen Teilnetz (mit CDs)

In diesem Beispiel wird ein x86-Installationsserver mit x86-CDs erstellt.

Für dieses Beispiel gelten die folgenden Voraussetzungen:

- Der Installationsclient befindet sich im gleichen Teilnetz wie der Installationsserver.
- Die Netzwerkinstallation verwendet eine grafische Benutzeroberfläche (GUI) in einer Desktop-Sitzung.
- Die allgemeinen Voraussetzungen für dieses Beispiel können Sie in Kapitel 8, "Installieren über das Netzwerk (Beispiele)" nachlesen.

1. Erstellen und Einrichten eines x86-Installationsservers

Das folgende Beispiel zeigt, wie Sie einen Installationsserver erstellen, indem Sie die folgenden CDs in das Verzeichnis /export/home/cdx86 des Installationsservers kopieren.

- a. Legen Sie die Solaris Software-1 CD in das Laufwerk des Systems ein.
- b. Verwenden Sie dazu den folgenden Befehl: Der Befehl erstellt ein Verzeichnis für das CD-Abbild und wechselt zum Tools-Verzeichnis auf dem eingehängten Datenträger. Dann kopiert dieser Befehl das Abbild auf dem Laufwerk auf die Festplatte des Installationsservers.

mkdir -p /export/home/dvdx86
cd /cdrom/cdrom0/Solaris_10/Tools
./setup_install_server /export/home/cdx86

- c. Legen Sie die Solaris Software 2-CD in das CD-ROM-Laufwerk des Systems ein.
- d. Verwenden Sie dazu den folgenden Befehl: Der Befehl wechselt zum Tools-Verzeichnis auf der eingehängten CD. Dann kopiert der Befehl den Inhalt der CD im CD-ROM-Laufwerk auf die Festplatte des Installationsservers und verwechselt zum Root-Verzeichnis (/).

BEISPIEL 8-4 x86: Installieren im gleichen Teilnetz (mit CDs) (Fortsetzung)

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdx86
# cd /
```

- e. Wiederholen Sie diese Befehle für jede Solaris Software-CD, die Sie installieren möchten.
- f. Legen Sie die Solaris Languages-CD in das CD-ROM-Laufwerk des Systems ein.
- g. Verwenden Sie dazu den folgenden Befehl: Der Befehl wechselt zum Tools-Verzeichnis auf der eingehängten CD. Dann kopiert der Befehl den Inhalt der CD im CD-ROM-Laufwerk auf die Festplatte des Installationsservers.

```
# cd /cdrom/cdrom0/Solaris_10/Tools
# ./add_to_install_server /export/home/cdx86
```

- h. Lassen Sie die CD auswerfen.
- i. Wiederholen Sie diese Befehle für jede Solaris Languages for SPARC Platforms-CD-CD, die Sie installieren möchten.
- 2. Fügen Sie die über das Netzwerk zu installierenden Systeme hinzu.

In diesem Beispiel heißt der Installationsclient basil und ist ein x86-System. Das Dateisystem /export/home/cdx86/Solaris_10/Tools enthält den Befehl add_install_client.

a. Fügt den Client zur /etc/ethers-Datei des Installationsservers hinzu. Suchen Sie die ethers-Adresse auf dem Client. Die /etc/ethers-Map wird der lokalen Datei entnommen.

```
# ifconfig -a grep ether
ether 8:0:20:b3:39:1d
```

- b. Öffnen Sie die /etc/ethers-Datei in einem Editor auf dem Installationsserver. Fügen Sie die Adresse der Liste hinzu.
- c. Verwenden Sie dazu den folgenden Befehl: Der Befehl wechselt zum Tools-Verzeichnis im aktuelle Solaris-Release CD-Abbild auf dem Installationsserver. Dann fügt der Befehl das zu installierende Clientsystem über das Netzwerk hinzu.

install_server# cd /export/home/cdx86/Solaris_10/Tools
install_server# ./add_install_client basil i86pc

3. Installieren des Systems mit einem Netzwerk-Installationsabbild

Hier wird beschrieben, wie Sie ein x86-basiertes System mithilfe des GRUB-Bootloaders über das Netzwerk installieren können.

a. Im System-BIOS geben Sie an, dass das System über das Netzwerk booten soll.

Nachdem Sie das BIOS verlassen haben, wird das System über das Netzwerk installiert. Das GRUB-Menü wird angezeigt.

b. Zur Installation des Betriebssystems Solaris über das Netzwerk wählen Sie aus dem Menü den entsprechenden Solaris-Eintrag aus. Drücken Sie dann die Eingabetaste.

Der Installations-Auswahlbildschirm wird angezeigt.

BEISPIEL 8-4 x86: Installieren im gleichen Teilnetz (mit CDs) (Fortsetzung)

c. Für eine Installation mit der grafischen interaktiven Solaris-Installationsoberfläche geben Sie 1 ein, und drücken dann die Eingabetaste.

Das Installationsprogramm startet.

d. Wenn Sie dazu aufgefordert werden, beantworten Sie die Fragen zur Systemkonfiguration.

Nachdem Sie die System-Konfigurationsinformationen bestätigt haben, wird der Solaris-Willkommenbildschirm angezeigt.

e. Nachdem das System über das Netzwerk gebootet und installiert wurde, weisen Sie es an, künftig von der Festplatte zu booten.

Hinweis – Nachdem das System nach der Installation neu gebootet hat, führt das GRUB-Menü die installierten Betriebssysteme auf. Hierzu gehört auch das neu installierte Betriebssystem Solaris. Wählen Sie Betriebssystem aus, mit dem gebootet werden soll. Wenn Sie keine Auswahl vornehmen, wird die Standardauswahl verwendet.

Weitere Informationen finden Sie in den folgenden Referenzen.

Verfahren	Referenz
Ausführlichere Beschreibung der in diesem Beispiel verwendeten Netzwerk-Installationsverfahren	Kapitel 6, "Installieren über das Netzwerk mithilfe von CDs (Vorgehen)"
Informationen zur Installation mit der grafischen interaktiven Solaris-Installationsoberfläche	"So führen Sie eine Installation bzw. ein Upgrade mit dem Solaris-Installationsprogramm mit GRUB aus" in Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen
Allgemeine Informationen zum GRUB-Bootloader	Kapitel 7, "SPARC- und x86-basiertes Booten (Überblick und Planung)" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades

♦ ♦ ♦ KAPITEL 9

Installation über das Netzwerk (Befehlsreferenz)

In diesem Kapitel sind die Befehle aufgelistet, die Sie zum Einrichten der Installation über das Netzwerk verwenden. Dieses Kapitel enthält die folgenden Themen:

- "Befehle für die Installation über das Netzwerk" auf Seite 143
- "x86: GRUB-Menübefehle für die Installation" auf Seite 145

Befehle für die Installation über das Netzwerk

In diesem Kapitel sind die Befehle aufgelistet, die Sie zum Installieren der Solaris-Software über das Netzwerk verwenden. Zudem ist angegeben, für welche Plattform die einzelnen Befehle relevant sind.

Befehl	Plattform	Beschreibung
add_install_client	Alle	Ein Befehl, mit dem ein Installations- oder Boot-Server aus dem Netzwerk Informationen für eine Installation über das Netzwerk erhält. In der Manpage add_install_client(1M) finden Sie weitere Informationen.
<pre>setup_install_server</pre>	Alle	Ein Skript, das die aktuelle Solaris-Release-DVD oder -CDs auf die lokale Festplatte eines Installationsservers bzw. die Boot-Software auf einen Boot-Server kopiert. Weitere Informationen entnehmen Sie bitte der Manpage setup_install_server(1M).
(nur CDs) add_to_install_server	Alle	Ein Skript, das zusätzliche Packages innerhalb einer Produktverzeichnisstruktur auf den CDs auf die lokale Festplatte eines vorhandenen Installationsservers kopiert. Weitere Informationen entnehmen Sie bitte der Manpage add_to_install_server(1M).

Befehl	Plattform	Beschreibung
mount	Alle	Ein Befehl zum Einhängen von Dateisystemen und Anzeigen der eingehängten Dateisysteme, einschließl. des Dateisystems auf der Solaris-DVD bzw. Solaris Software und der Solaris Languages-CDs. Weitere Informationen finden Sie in der Manpage mount(1M).
showmount -e	Alle	Ein Befehl, der alle freigegebenen Dateisysteme anzeigt, die sich auf einem entfernten System befinden. Weitere Informationen finden Sie in der Manpage showmount(1M).
uname -i	Alle	Ein Befehl zum Ermitteln des Plattformnamens des Systems, also zum Beispiel SUNW, Ultra-5_10 oder i86pc. Den Plattformnamen des Systems benötigen Sie möglicherweise beim Installieren der Solaris-Software. Weitere Informationen finden Sie in der Manpage uname(1).
patchadd -C Netzwerkinstallationsabbild	Alle	Ein Befehl zum Hinzufügen von Patches zu den Dateien, die sich in der Miniroot (Solaris_10/Tools/Boot) in einem Netzwerkinstallationsabbild einer DVD oder CD befinden, das Sie mit setup_install_server erstellt haben. So können Sie Patches auf Solaris-Installationsbefehle und andere für die Miniroot spezifische Befehle anwenden. <i>Netzwerk-Installationsabbild</i> ist der absolute Pfadname des Abbildes für die Installation über das Netzwerk.
		 Achtung - Verwenden Sie den Befehl patchadd - C nicht, es sei denn, Sie haben die Patch README-Anweisungen gelesen oder mit dem Sun-Support vor Ort gesprochen. Weitere Informationen finden Sie hier: Kapitel 7, "Patchen des Miniroot-Abbilds (Vorgehen)" Weitere Informationen finden Sie in der Manpage patchadd(1M).
reset	SPARC	Ein OpenBoot-PROM-Befehl zum Zurücksetzen und Neustarten des Systems. Wenn beim Booten eine Reihe von Fehlermeldungen zu I/O-Interrupts ausgegeben werden, drücken Sie die Tasten Stop und A gleichzeitig und geben Sie dann an der Eingabeaufforderung ok oder der PROM-Eingabeaufforderung > reset ein.
banner	SPARC	Ein OpenBoot-PROM-Befehl zum Anzeigen von Systeminformationen wie der Modellbezeichnung, der Ethernet-Adresse und des installierten Hauptspeichers. Diesen Befehl können Sie nur an der Eingabeaufforderung ok oder der PROM-Eingabeaufforderung > absetzen.
x86: GRUB-Menübefehle für die Installation

Durch Bearbeiten der entsprechenden Befehle im GRUB-Menü können Sie das Booten und die Installation Ihres Systems anpassen. In diesem Abschnitt werden einige Befehle und Argumente beschrieben, die Sie in die Befehle des GRUB-Menüs einfügen können.

Im GRUB-Menü rufen Sie die GRUB-Befehlszeile auf, indem Sie an der Eingabeaufforderung b eingeben. Eine der folgenden Ausgabe ähnliche Befehlszeile wird angezeigt.

```
kernel /Solaris_10_x86/multiboot kernel/unix
-B install_media=192.168.2.1:/export/cdrom0/boot
module /platform/i86pc/boot_archive
```

Sie können diese Befehlszeile zur benutzerspezifischen Anpassung des Boot- bzw. Installationsvorgangs bearbeiten. In der folgenden Liste sind einige gebräuchliche Befehle aufgeführt, die Sie verwenden können. Eine vollständige Liste der Boot-Argumente, die Sie mit der Option - B verwenden können, finden Sie auf der Manpage eeprom(1M).

Hinweis – Um mehrere Argumente mit der Option - B hinzuzufügen, trennen Sie die Argumente mit einem Komma.

TABELLE 9-1 x86: GRUB-Menübefehle und Optionen

Befehl/Option	Beschreibung und Beispiele
install	Fügen Sie diese Option vor der Option -B ein, um eine benutzerdefinierte JumpStart-Installation auszuführen.
	kernel /Solaris_10_x86/multiboot install -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive

Befehl/Option	Beschreibung und Beispiele
<i>URL</i> ask	 Gibt die Adresse der benutzerdefinierten JumpStart-Dateien an oder fordert zu deren Eingabe auf. Diese Optionen müssen mit der Option install eingefügt werden. URL - der Pfad zu den Dateien. Sie können einen URL für Dateien an folgenden Speicherorten angeben:
	 Lokale Festplatte
	file://jumpstart_dir_path/compressed_config_file Beispiel:
	kernel /Solaris_10_x86/multiboot install file://jumpstart/config.tar -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
	■ NFS-Server
	nfs://server_name:IP_address/jumpstart_dir_path/compressed_config_file Beispiel:
	kernel /Solaris_10_x86/multiboot install myserver:192.168.2.1/jumpstart/config.tar -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
	■ HTTP-Server
	http://server_name:IP_address/jumpstart_dir_path/ compressed_config_file&proxy_info
	 Wenn Sie eine sysidofg-Datei in die komprimierte Konfigurationsdatei aufgenommen haben, müssen Sie wie im folgenden Beispiel die IP-Adresse des Server- angeben, auf dem sich die Datei befindet:
	kernel /Solaris_10_x86/multiboot install http://192.168.2.1/jumpstart/config.tar -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
	 Wenn Sie die komprimierte Konfigurationsdatei auf einem HTTP-Server hinter einer Firewall gespeichert haben, müssen Sie während des Boot-Vorgangs einen Proxy-Server angeben. Sie brauchen keine IP-Adresse für den Server anzugeben, auf dem sich die Datei befindet. Sie müssen jedoch wie im folgenden Beispiel eine IP-Adresse für den Proxy-Server angeben:
	kernel /Solaris_10_x86/multiboot install http://www.shadow.com/jumpstart/config.tar&proxy=131.141.6.151 -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive

Befehl/Option	Beschreibung und Beispiele
URL ask (Fortsetzung)	 ask - Bei Verwendung dieser Option mit der Option install gibt diese Option an, dass Sie das Installationsprogramm nach dem Booten und Herstellen der Verbindung zum Netzwerk nach dem Ort der komprimierten Konfigurationsdatei fragen soll. Bei Verwendung dieser Option können Sie keine vollständig automatische JumpStart-Installation durchführen. Wenn Sie durch Drücken der Eingabetaste die Eingabeaufforderung umgehen, konfiguriert das Solaris-Installationsprogramm die Netzwerkparameter interaktiv. Danach fordert Sie das Installationsprogramm zur Eingabe des Speicherorts der komprimierten Konfigurationsdatei auf.
	Im folgenden Beispiel wird eine benutzerspezifische JumpStart-Installation durchgeführt. Danach bootet das System von einem Netzwerkinstallationsabbild. Sie werden nach dem Herstellen der Verbindung des Systems zum Netzwerk aufgefordert, den Ort der Konfigurationsdatei anzugeben.
	<pre>kernel /Solaris_10_x86/multiboot install ask -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive</pre>
dhcp	Fügen Sie diese Option vor der Option -B ein, um die Installationsprogramme anzuweisen, Netzwerkinstallationsinformationen, die zum Booten des Systems benötigt werden, von einem DHCP-Server abzurufen. Wenn Sie dhcp weglassen und somit angeben, dass kein DHCP-Server verwendet werden soll, verwendet das System die Datei /etc/bootparams oder die Datenbank bootparams des Naming Service. Sie würden zum Beispiel nicht dhcp angeben, wenn Sie eine statische IP-Adresse beibehalten wollen.
	kernel /Solaris_10_x86/multiboot dhcp -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
- text	Fügen Sie diese Option vor der Option -B ein, wenn in einer Desktop-Sitzung eine textbasierte Installation durchgeführt werden soll.
	kernel /Solaris_10_x86/multiboot - text -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
- nowin	Fügen Sie diese Option vor der Option -B ein, wenn in einer Konsolensitzung eine textbasierte Installation durchgeführt werden soll.
	kernel /Solaris_10_x86/multiboot - nowin -B install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive

 TABELLE 9-1
 x86: GRUB-Menübefehle und Optionen
 (Fortsetzung)

 TABELLE 9-1
 x86: GRUB-Menübefehle und Optionen
 (Fortsetzung)

Befehl/Option	Beschreibung und Beispiele
console= <i>serielle-Konsole</i>	Verwenden Sie dieses Argument mit der Option -B um das System anzuweisen, eine serielle Konsole wie z. B. ttya (COM1) oder ttyb (COM2) zu verwenden.
	kernel /Solaris_10_x86/multiboot -B console=ttya install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
ata-dma-enabled=[0 1]	Verwenden Sie dieses Argument mit der Option -B um während der Installation Geräte mit Advanced Technology Attachment- (ATA) bzw. Integrated Drive Electronics (IDE)-Funktionalität sowie direktem Speicherzugriff (Direct Memory Access, DMA) zu aktivieren bzw. deaktivieren.
	kernel /Solaris_10_x86/multiboot -B ata-dma-enabled=0 install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
acpi-enum=[0 1]	Verwenden Sie dieses Argument mit der Option -B, um Advanced Configuration and Power Interface (ACPI) Power Management zu aktivieren bzw. deaktivieren.
	kernel /Solaris_10_x86/multiboot -B acpi-enum=0 install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
atapi-cd-dma-enabled=[0 1]	Verwenden Sie dieses Argument mit der Option -B, um während der Installation für CD- bzw. DVD-Laufwerke direkten Speicherzugriff (DMA) zu aktivieren.
	kernel /Solaris_10_x86/multiboot -B atapi-cd-dma-enabled=0 install_media=192.168.2.1:/export/cdrom0/boot module /platform/i86pc/boot_archive
	Hinweis – Der DMA-Name <i>atapi</i> ist der aktuelle Variablenname für DMA. Änderungen an der Variable vorbehalten.

TEIL III

Installation über ein WAN

Dieser Teil beschreibt, wie Sie ein System mithilfe der WAN-Boot-Installation über ein WAN (Wide Area Network) installieren.

♦ ♦ ♦ KAPITEL 10

WAN-Boot (Übersicht)

Dieses Kapitel bietet eine Übersicht über das WAN-Boot-Installationsverfahren. Er umfasst die folgenden Themen:

- "Was ist WAN-Boot?" auf Seite 151
- "Wann ist WAN-Boot sinnvoll?" auf Seite 153
- "Wie funktioniert WAN-Boot (Übersicht)" auf Seite 153
- "Von WAN-Boot unterstützte Sicherheitskonfigurationen (Übersicht)" auf Seite 157

Was ist WAN-Boot?

Das WAN-Boot-Installationsverfahren ermöglicht es, Software unter Verwendung von HTTP über ein WAN (Wide Area Network) zu booten und zu installieren. Mit WAN-Boot können Sie Solaris über große, öffentliche Netzwerke, deren Infrastruktur möglicherweise nicht vertrauenswürdig ist, auf SPARC-Systemen installieren. Die Sicherheitsfunktionen von WAN-Boot schützen die Vertraulichkeit der Daten und stellen die Integrität des Installationsabbilds sicher.

Mit der WAN-Boot-Installationsmethode können Sie ein verschlüsseltes Solaris Flash-Archiv über ein öffentliches Netzwerk an einen entfernten SPARC-Client übertragen. Die WAN-Boot-Programme installieren das Clientsystem dann, indem sie eine benutzerdefinierte JumpStart-Installation durchführen. Die Integrität der Installation lässt sich mit privaten Schlüsseln zur Authentifizierung und Verschlüsselung der Daten schützen. Sie können die Installationsdaten und -dateien auch über eine sichere HTTP-Verbindung senden. Hierfür müssen Sie auf Ihren Systemen die Verwendung von digitalen Zertifikaten konfigurieren.

Bei einer WAN-Boot-Installation laden Sie die folgenden Informationen über eine HTTP- oder sichere HTTP-Verbindung von einem Webserver herunter und installieren ein SPARC-System.

 wanboot-Programm – Das wanboot-Programm ist das sekundäre Boot-Programm, das die WAN-Boot-Miniroot, die Client-Konfigurationsdateien und die Installationsdateien lädt. Das wanboot-Programm führt ähnliche Vorgänge wie die Boot-Unterprogramme ufsboot oder inetboot durch.

- WAN-Boot-Dateisystem WAN-Boot stützt sich bei der Konfiguration des Clients und zum Abrufen der auf dem Clientsystem zu installierenden Daten auf verschiedene Dateien. Diese Dateien befinden sich im Verzeichnis /etc/netboot des Webservers. Das Programm wanboot-cgi überträgt diese Dateien in Form eines Dateisystems, dem WAN-Boot-Dateisystem, an den Client.
- WAN-Boot-Miniroot Die WAN-Boot-Miniroot ist eine auf die WAN-Boot-Installation ausgerichtete Variante der Solaris-Miniroot. Wie die Solaris-Miniroot enthält die WAN-Boot-Miniroot einen Kernel und gerade so viel Software, wie zur Installation von Solaris erforderlich ist. Die WAN-Boot-Miniroot enthält einen Teilsatz der Software in der Solaris-Miniroot.
- Benutzerdefinierte JumpStart-Konfigurationsdateien Für die Installation des Systems überträgt WAN-Boot die Dateien sysidcfg, rules.ok sowie Profildateien an den Client. WAN-Boot führt dann auf Grundlage dieser Dateien eine benutzerdefinierte JumpStart-Installation auf dem Clientsystem durch.
- Solaris Flash-Archiv Ein Solaris Flash-Archiv ist eine Sammlung von Dateien, die von einem Master-System kopiert wurden. Mit einem solchen Archiv können Sie Clientsysteme installieren. WAN-Boot installiert mithilfe des benutzerdefinierten JumpStart-Verfahrens ein Solaris Flash-Archiv auf dem Clientsystem. Nach der Installation eines Archivs auf einem Clientsystem verfügt dieses System über genau dieselbe Konfiguration wie das Master-System.

Hinweis – Der Befehl flarcreate übt keinerlei Größenbeschränkungen mehr auf einzelne Dateien aus. Sie können ein Solaris Flash-Archiv erstellen, dass einzelne Dateien enthalten kann, die größer als 4 GB sind.

Weitere Informationen finden Sie unter "Erstellen eines Archivs, das große Dateien enthält" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).

Dann installieren Sie das Archiv mit dem benutzerdefinierten JumpStart-Verfahren auf dem Client.

Die oben aufgeführten Daten können Sie bei der Übertragung durch Schlüssel und digitale Zertifikate schützen.

In "Wie funktioniert WAN-Boot (Übersicht)" auf Seite 153 ist die Abfolge der bei einer WAN-Boot-Installation stattfindenden Ereignisse ausführlicher dargestellt.

Wann ist WAN-Boot sinnvoll?

Das WAN-Boot-Installationsverfahren ermöglicht es, an entfernten Standorten SPARC-Systeme zu installieren. Es bietet sich an, WAN-Boot für die Installation von entfernten Servern oder Clients einzusetzen, die nur über ein öffentliches Netzwerk zugänglich sind.

Für eine Installation von Systemen in Ihrem LAN (Local Area Network) erfordert das WAN-Boot-Installationsverfahren mehr Konfigurations- und Administrationsaufwand als nötig. Informationen, wie Sie Systeme über ein LAN installieren, finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Wie funktioniert WAN-Boot (Übersicht)

Bei der Installation eines entfernten SPARC-Clients mit WAN-Boot kommt eine Kombination von Servern, Konfigurationsdateien, CGI-Programmen (Common Gateway Interface) und Installationsdateien zum Einsatz. Dieser Abschnitt zeigt die allgemeine Abfolge der bei einer WAN-Boot-Installation stattfindenden Ereignisse.

Ereignisabfolge bei einer WAN-Boot-Installation

Abbildung 10–1 zeigt die grundlegende Reihenfolge der Ereignisse bei einer WAN-Boot-Installation. In dieser Abbildung ruft ein SPARC-Client über ein WAN Konfigurationsdaten und Installationsdateien von einem Webserver und einem Installationsserver ab.





1. Sie booten den Client auf eine der folgenden Arten:

- Booten aus dem Netzwerk durch Setzen von Netzwerkschnittstellen-Variablen im Open Boot PROM (OBP).
- Booten aus dem Netzwerk mit der DHCP-Option.
- Booten von einer lokalen CD-ROM.
- 2. Das Client-OBP erhält Konfigurationsinformationen aus einer dieser Quellen:
 - Von Boot-Argumentwerten, die vom Benutzer in die Befehlszeile eingegeben werden.
 - Vom DHCP-Server, sofern im Netzwerk DHCP verwendet wird.
- 3. Das Client-OBP fordert das sekundäre Boot-Programm wanboot an.

Das Client-OBP lädt das wanboot-Programm von einer der folgenden Quellen herunter:

- Von einem speziellen Webserver, dem WAN-Boot-Server, unter Verwendung von HTTP.
- Von einer lokalen CD-ROM (nicht abgebildet).
- 4. Das wanboot-Programm fordert die Client-Konfigurationsinformationen vom WAN-Boot-Server an.
- 5. Das wanboot-Programm lädt Konfigurationsdateien, die vom Programm wanboot-cgi übertragen werden, vom WAN-Boot-Server herunter. Die Konfigurationsdateien werden als WAN-Boot-Dateisystem an den Client übertragen.
- 6. Das wanboot-Programm fordert die WAN-Boot-Miniroot vom WAN-Boot-Server an.
- 7. Das wanboot-Programm lädt die WAN-Boot-Miniroot per HTTP oder sicheres HTTP vom WAN-Boot-Server herunter.
- 8. Das wanboot-Programm lädt den UNIX-Kernel aus der WAN-Boot-Miniroot und führt ihn aus.
- 9. Der UNIX-Kernel sucht das WAN-Boot-Dateisystem und hängt es zur Verwendung durch das Solaris-Installationsprogramm ein.
- 10. Das Installationsprogramm fordert ein Solaris Flash-Archiv und JumpStart-Dateien von einem Installationsserver an.

Das Installationsprogramm lädt das Archiv und die JumpStart-Dateien über eine HTTPoder HTTPS-Verbindung herunter.

11. Das Installationsprogramm installiert mit dem benutzerdefinierten JumpStart-Verfahren das Solaris Flash-Archiv auf dem Client.

Schutz der Daten während einer WAN-Boot-Installation

Das WAN-Boot-Installationsverfahren erlaubt den Einsatz von Hashing-Schlüsseln und digitalen Zertifikaten zum Schutz der Systemdaten während der Installation. In diesem Abschnitt werden die vom WAN-Boot-Installationsverfahren unterstützten Datenschutzmethoden kurz dargestellt.

Überprüfen der Datenintegrität mit einem Hashing-Schlüssel

Zum Schutz der Daten, die von einem WAN-Boot-Server an den Client übertragen werden, können Sie einen sog. HMAC-Schlüssel (Hashed Message Authentication Code) erstellen. Diesen Hashing-Schlüssel installieren Sie sowohl auf dem WAN-Boot-Server als auch auf dem Client. Der WAN-Boot-Server signiert mit diesem Schlüssel die an den Client zu übertragenden Daten. Der Client verwendet den Schlüssel dann zum Überprüfen der Integrität der vom WAN-Boot-Server übertragenen Daten. Nach der Installation eines Hashing-Schlüssels auf einem Client steht dieser Schlüssel dem Client für künftige WAN-Boot-Installationen zur Verfügung.

Anweisungen zur Verwendung eines Hashing-Schlüssels finden Sie in "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195.

Verschlüsseln von Daten mit Chiffrierschlüsseln

Mit WAN-Boot-Installationsverfahren können Sie Daten verschlüsseln, die vom WAN-Boot-Server an den Client gesendet werden. Mit den WAN-Boot-Dienstprogrammen können Sie eine 3DES(Triple Data Encryption Standard)- oder AES(Advanced Encryption Standard)-Verschlüsselung, den Chiffrierschlüssel, generieren. Diesen Schlüssel stellen Sie dann sowohl dem WAN-Boot-Server als auch dem Client zur Verfügung. Mit diesem Chiffrierschlüssel verschlüsselt WAN-Boot die vom WAN-Boot-Server an den Client übertragenen Daten. Der Client verwendet diesen Schlüssel dann zum Entschlüsseln der Konfigurations- und Sicherheitsdateien, die während der Installation übertragen werden.

Nach der Installation eines Chiffrierschlüssels auf einem Client steht dieser Schlüssel dem Client für künftige WAN-Boot-Installationen zur Verfügung.

Der Einsatz einer Verschlüsselung ist jedoch nicht an allen Standorten zulässig. Um festzustellen, ob die Verschlüsselung an Ihrem Standort möglich ist, wenden Sie sich bitte an Ihren Sicherheitsadministrator. Ist die Verschlüsselung an Ihrem Standort zulässig, fragen Sie Ihren Sicherheitsadministrator, ob Sie mit einer 3DES- oder AES-Verschlüsselung arbeiten sollen.

Anweisungen zur Verwendung eines Chiffrierschlüssels finden Sie in "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195.

Schutz von Daten durch HTTPS

WAN-Boot unterstützt den Einsatz von HTTPS (HTTP over Secure Sockets Layer) für die Übertragung von Daten zwischen WAN-Boot-Server und Client. Mit HTTPS können Sie bewirken, dass sich entweder nur der Server oder sowohl der Server als auch der Client während der Installation ausweisen müssen. HTTPS verschlüsselt außerdem die Daten, die bei der Installation vom Server an den Client übertragen werden.

Bei HTTPS kommen digitale Zertifikate zur Authentifizierung von Systemen zum Einsatz, die über das Netzwerk Daten austauschen. Ein digitales Zertifikat ist eine Datei, die ein Server- oder ein Clientsystem als vertrauenswürdigen Teilnehmer der Online-Kommunikation ausweist. Digitale Zertifikate können von externen Zertifizierungsstellen (CAs) angefordert oder durch Erzeugen einer eigenen Zertifizierungsstelle selbst generiert werden.

Damit der Client den Server als vertrauenswürdig akzeptiert und Daten von ihm annimmt, müssen Sie ein digitales Zertifikat auf dem Server installieren. Dann weisen Sie den Client an, dieses Zertifikat zu akzeptieren. Sie können auch festlegen, dass sich der Client gegenüber dem Server ausweist. Dafür stellen Sie dem Client ein digitales Zertifikat zur Verfügung. Anschließend weisen Sie den Server an, den Signierer des Zertifikats zu akzeptieren, wenn der Client das Zertifikat bei der Installation vorlegt.

Wenn Sie digitale Zertifikate bei der Installation einsetzen möchten, müssen Sie den Webserver für die Verwendung von HTTPS konfigurieren. Informationen über die Arbeit mit HTTPS entnehmen Sie bitte der Dokumentation Ihres Webservers.

Die Voraussetzungen für die Verwendung von digitalen Zertifikaten bei der WAN-Boot-Installation finden Sie in "Voraussetzungen für digitale Zertifikate" auf Seite 168. Anweisungen zur Verwendung von digitalen Zertifikaten bei der WAN-Boot-Installation finden Sie in "(Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung" auf Seite 192.

Von WAN-Boot unterstützte Sicherheitskonfigurationen (Übersicht)

WAN-Boot unterstützt verschiedene Sicherheitsstufen. Sie können die von WAN-Boot unterstützten Sicherheitsleistungsmerkmale im Hinblick auf die Anforderungen in Ihrem Netzwerk kombinieren. Eine Konfiguration mit einer höheren Sicherheit erfordert zwar mehr Administrationsaufwand, bedeutet aber auch einen besseren Schutz für Ihre Systemdaten. Für wichtigere Systeme oder Systeme, die über ein öffentliches Netzwerk installiert werden sollen, eignet sich die Konfiguration unter "Sichere WAN-Boot-Installationskonfiguration" auf Seite 158. Für etwas weniger wichtige Systeme oder Systeme in halb-privaten Netzwerken könnte die in "Unsichere WAN-Boot-Installationskonfiguration" auf Seite 158 beschriebene Konfiguration eine gute Lösung sein. In diesem Abschnitt werden die Konfigurationen für unterschiedliche Sicherheitsstufen bei der WAN-Boot-Installation kurz dargestellt. Darüber hinaus werden die in den verschiedenen Konfigurationen angewendeten Sicherheitsmechanismen beschrieben.

Sichere WAN-Boot-Installationskonfiguration

Diese Konfiguration schützt die Integrität der zwischen Server und Client übertragenen Daten und trägt zur Geheimhaltung des Übertragungsinhalts bei. In dieser Konfiguration kommen eine HTTPS-Verbindung und entweder der 3DES- oder der AES-Algorithmus zur Verschlüsselung der Client-Konfigurationsdateien zum Einsatz. Sie sieht auch vor, dass sich der Server bei der Installation gegenüber dem Client ausweist. Für eine sichere WAN-Boot-Installation gelten bezüglich der Sicherheitsfunktionen folgende Voraussetzungen:

- HTTPS auf WAN-Boot-Server und Installationsserver aktiviert
- HMAC SHA1-Hashing-Schlüssel auf WAN-Boot-Server und Client
- 3DES- oder AES-Verschlüsselung für WAN-Boot-Server und Client
- Digitales Zertifikat einer Zertifizierungsstelle für WAN-Boot-Server

Wenn Sie zusätzlich festlegen möchten, dass sich auch der Client bei der Installation ausweisen muss, sind auch diese Sicherheitsfunktionen erforderlich:

- Privater Schlüssel für den WAN-Boot-Server
- Digitales Zertifikat für den Client

Eine Liste der Schritte, die zur Installation mit dieser Konfiguration erforderlich sind, finden Sie in Tabelle 12–1.

Unsichere WAN-Boot-Installationskonfiguration

Diese Sicherheitskonfiguration bedeutet zwar den geringsten Administrationsaufwand, aber auch die geringste Sicherheit bei der Datenübertragung zwischen Webserver und Client. Sie müssen weder einen Hashing-Schlüssel noch eine Verschlüsselung oder digitale Zertifikate generieren. Auch muss der Webserver nicht für die Verwendung von HTTPS konfiguriert sein. Die Installationsdaten und -dateien werden aber über eine HTTP-Verbindung gesendet, die Ihre Installation gegenüber Ausspähversuchen im Netzwerk verwundbar macht.

Wenn Sie möchten, dass der Client die Integrität der übertragenen Daten überprüft, können Sie diese Konfiguration durch den Einsatz eines HMAC SHA1-Hashing-Schlüssels ergänzen. Beachten Sie aber bitte, dass das Solaris Flash-Archiv durch einen Hashing-Schlüssel nicht geschützt wird. Das Archiv wird bei der Installation schutzlos zwischen dem Server und dem Client übertragen.

Eine Liste der Schritte, die zur Installation mit dieser Konfiguration erforderlich sind, finden Sie in Tabelle 12–2.

♦ ♦ ♦ KAPITEL 11

Vorbereiten der Installation mit WAN-Boot (Planung)

In diesem Kapitel erfahren Sie, wie Sie Ihr Netzwerk für eine WAN-Boot-Installation vorbereiten. Er umfasst die folgenden Themen:

- "WAN-Boot Voraussetzungen und Richtlinien" auf Seite 159
- "Sicherheitslücken bei der Arbeit mit WAN-Boot" auf Seite 169
- "Zusammenstellen der Informationen f
 ür WAN-Boot-Installationen" auf Seite 169

WAN-Boot - Voraussetzungen und Richtlinien

In diesem Abschnitt werden die Systemvoraussetzungen für die Installation von WAN-Boot erläutert.

System und Beschreibung	Anforderungen
WAN-Boot-Server – Der WAN-Boot-Server ist ein Webserver, der das wanboot-Programm, die Konfigurations- und Sicherheitsdateien und die WAN-Boot-Miniroot bereitstellt.	 Betriebssystem – Solaris 9 12/03 BS, oder kompatible Version Muss als Webserver konfiguriert sein Webserver-Software muss HTTP 1.1 unterstützen Wenn Sie mit digitalen Zertifikaten arbeiten möchten, muss die Webserver-Software HTTPS unterstützen

TABELLE 11-1 Systemvoraussetzungen für WAN-Boot-Installationen

System und Beschreibung	Anforderungen
Installationsserver – Der Installationsserver stellt das Solaris Flash-Archiv und die JumpStart-Dateien bereit, die für die Installation des Clients benötigt werden.	 Verfügbarer Speicherplatz – Speicherplatz für jedes Solaris Flash-Archiv Laufwerk – CD-ROM- oder DVD-ROM-Laufwerk Betriebssystem – Solaris 9 12/03 BS, oder kompatible Version Sind Installationsserver und WAN-Boot-Server zwei unterschiedliche Systeme, muss der Installationsserver diese zusätzlichen Voraussetzungen erfüllen: Muss als Webserver konfiguriert sein
	 Webserver-Software muss HTTP 1.1 unterstützen
	 Wenn Sie mit digitalen Zertifikaten arbeiten möchten, muss die Webserver-Software HTTPS unterstützen
Clientsystem – Das entfernte System, das über ein WAN installiert werden soll	 Arbeitsspeicher - Mindestens 768 MB RAM CPU – Mindestens UltraSPARC II-Prozessor Festplatte – Mindestens 2 GB Speicherplatz auf der Festplatte
	 OBP – WAN-Boot-fähiger PROM Verfügt der Client nicht über einen geeigneten PROM, so muss er mit einem CD-ROM-Laufwerk ausgestattet sein. Wie Sie herausfinden können, ob der Client über ein PROM mit WAN-Boot-Unterstützung verfügt, erfahren Sie in "So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung" auf Seite 182.
(Optional) DHCP-Server – Für die Bereitstellung der Client-Konfigurationsinformationer	Wenn Sie mit einem SunOS-DHCP-Server arbeiten, müssen Sie folgende Schritte durchführen: Stufen Sie den Server zum EDHCP-Server herauf.
können Sie einen DHCP-Server einsetzen.	 Benennen Sie die Sun-Herstelleroptionen um, so dass die für Optionen geforderte Länge von acht Zeichen erfüllt ist. Weitere Informationen über die für die WAN-Installation spezifischen Sun-Herstelleroptionen finden Sie in "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214.
	Befindet sich der DHCP-Server in einem anderen Teilnetz als der Client, müssen Sie einen BOOTP-Relay-Agenten konfigurieren. Näheres zur Konfiguration eines BOOTP-Relay-Agenten finden Sie in Kapitel 14, "Konfiguration des DHCP-Services (Aufgaben)" in <i>Systemverwaltungshandbuch: IP Services</i> .

. 11 . 4 . (r. c. C TITANT D Ŧ

System und Beschreibung	Anforderungen
(optional) Protokollserver– Per Voreinstellung werden alle während einer WAN-Installation auftretenden Protokollmeldungen für das Booten und die Installation auf der Client-Konsole angezeigt. Um diese Meldungen auf einem anderen System anzeigen zu lassen, geben Sie ein System an, das als Protokollserver dienen soll.	Muss als Webserver konfiguriert sein. Hinweis – Wenn Sie bei der Installation mit HTTPS arbeiten, müssen Protokollserver und WAN-Boot-Server identisch sein.
(Optional) Proxy-Server – Sie können das Leistungsmerkmal WAN-Boot so konfigurieren, dass das Herunterladen der Installationsdaten und -dateien über einen HTTP-Proxy erfolgt.	Wenn die Installation per HTTPS vorgenommen wird, muss der Proxy-Server zum Tunneln von HTTPS konfiguriert sein.

Webserver-Software - Voraussetzungen und Richtlinien

Die Webserver-Software auf dem WAN-Boot- und dem Installationsserver muss die folgenden Voraussetzungen erfüllen:

- Betriebssystemvoraussetzungen WAN-Boot bietet ein CGI(Common Gateway Interface)-Programm (wanboot-cgi), das Daten und Dateien in das vom Clientsystem erwartete Format konvertiert. Für eine WAN-Boot-Installation mithilfe dieser Skripten muss die Webserver-Software unter Solaris 9 12/03 oder einer kompatiblen Version ausgeführt werden.
- Maximale Dateigröße Die Größe der über die HTTP-Verbindung übertragenen Dateien ist möglicherweise durch Ihre Webserver-Software begrenzt. Lesen Sie bitte in der Dokumentation Ihres Webservers nach, ob die Software Dateien in der Größe eines Solaris Flash-Archivs übertragen kann.

Hinweis – Der Befehl flarcreate übt keinerlei Größenbeschränkungen mehr auf einzelne Dateien aus. Sie können ein Solaris Flash-Archiv erstellen, dass einzelne Dateien enthalten kann, die größer als 4 GB sind.

Weitere Informationen finden Sie unter "Erstellen eines Archivs, das große Dateien enthält" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation). SSL-Unterstützung – Wenn Sie bei der WAN-Boot-Installation mit HTTPS arbeiten möchten, muss die Webserver-Software SSL Version 3 unterstützen.

Serverkonfigurationsoptionen

Sie können die Konfiguration der von WAN-Boot benötigten Server an die Anforderungen in Ihrem Netzwerk anpassen. Die erforderlichen Server können entweder auf einem System oder auf verschiedenen Systemen eingerichtet werden.

- Einzelner Server Wenn Sie die WAN-Boot-Daten und -Dateien zentral auf einem System verwalten möchten, können Sie alle Server auf demselben System einrichten. Sie können alle Server auf einem System verwalten und müssen nur ein System als Webserver konfigurieren. Unter Umständen unterstützt ein einzelner Server aber das hohe Datenaufkommen nicht, das bei zahlreichen gleichzeitig ablaufenden WAN-Boot-Installationen entstehen würde.
- Mehrere Server Für den Fall, dass Sie die Installationsdaten und -dateien an verschiedenen Stellen im Netzwerk verwalten möchten, besteht die Möglichkeit, die entsprechenden Server auf unterschiedlichen Systemen einzurichten. Sie können einen zentralen WAN-Boot-Server einrichten und mehrere Installationsserver für die Verwaltung von Solaris Flash-Archiven an verschiedenen Stellen im Netzwerk konfigurieren. Wenn Sie Installations- und Protokollserver auf unabhängigen Systemen einrichten, müssen Sie diese Systeme als Webserver konfigurieren.

Speichern von Installations- und Konfigurationsdateien im Dokument-Root-Verzeichnis

Das Programm wanboot - cgi überträgt bei der WAN-Boot-Installation die folgenden Dateien:

- wanboot-Programm
- WAN-Boot-Miniroot
- Dateien für die benutzerdefinierte JumpStart-Installation
- Solaris Flash-Archiv

Damit das Programm wanboot - cgi diese Dateien übertragen kann, müssen Sie sie in einem für die Webserver-Software zugänglichen Verzeichnis speichern. Eine Möglichkeit, die Dateien zugänglich zu machen, besteht darin, sie im *Dokument-Root-Verzeichnis* auf dem Webserver abzulegen.

Das Dokument-Root-Verzeichnis (auch primäres Dokumentverzeichnis genannt) ist das Verzeichnis auf dem Webserver, in dem Dateien gespeichert werden sollen, die für Client abrufbar sind. Dieses Verzeichnis können Sie mit der Webserver-Software benennen und konfigurieren. Genauere Informationen über die Einrichtung des Dokument-Root-Verzeichnisses auf dem Webserver entnehmen Sie bitte der Dokumentation Ihres Webservers.

Es bietet sich an, für die verschiedenen Installations- und Konfigurationsdateien eigene Unterverzeichnisse unter dem Dokument-Root-Verzeichnis anzulegen. So könnten Sie beispielsweise ein spezifisches Unterverzeichnis für jede zu installierende Client-Gruppe erzeugen. Wenn Sie beabsichtigen, im Netzwerk unterschiedliche Versionen von Solaris zu installieren, können Sie auch ein Unterverzeichnis pro Version erzeugen.

Abbildung 11–1 zeigt eine allgemeine Beispielstruktur für ein Dokument-Root-Verzeichnis. In diesem Beispiel befinden sich WAN-Boot-Server und Installationsserver auf demselben System. Auf dem Server wird die Webserver-Software Apache ausgeführt.



ABBILDUNG 11–1 Beispielstruktur eines Dokument-Root-Verzeichnisses

Das Dokument-Verzeichnis in diesem Beispiel weist die folgende Struktur auf:

- Das Verzeichnis /opt/apache/htdocs ist das Dokument-Root-Verzeichnis.
- Das WAN-Boot-Miniroot-Verzeichnis (miniroot) enthält die WAN-Boot-Miniroot.
- Das wanboot-Verzeichnis enthält das wanboot-Programm.
- Das Solaris Flash-Verzeichnis (flash) enthält die für die Installation des Clients erforderlichen JumpStart-Dateien und das Unterverzeichnis archives. Das Verzeichnis archives enthält das aktuelle Solaris-Release Flash-Archiv.

Hinweis – Sind WAN-Boot-Server und Installationsserver unterschiedliche Systeme, sollten Sie das Verzeichnis flash auf dem Installationsserver erzeugen. Vergewissern Sie sich, dass diese Dateien und Verzeichnisse für den WAN-Boot-Server zugänglich sind.

Wie Sie das Dokument-Root-Verzeichnis erzeugen, entnehmen Sie bitte der Dokumentation Ihres Webservers. Ausführliche Anweisungen zum Erzeugen und Speichern dieser Installationsdateien finden Sie in "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation" auf Seite 197.

Speichern von Konfigurations- und Sicherheitsinformationen in der /etc/netboot-Hierarchie

Das Verzeichnis /etc/netboot enthält die Konfigurationsinformationen, den privaten Schlüssel, das digitale Zertifikat und die Zertifizierungsstelle, die für eine WAN-Boot-Installation erforderlich sind. In diesem Abschnitt sind die Dateien und Verzeichnisse dargestellt, die Sie im Verzeichnis /etc/netboot erzeugen können, um Ihre WAN-Boot-Installation individuell anzupassen.

Anpassung des Aktionsbereichs der WAN-Boot-Installation

Während der Installation sucht das Programm wanboot-cgi im Verzeichnis /etc/netboot auf dem WAN-Boot-Server nach den Client-Informationen. Das Programm wanboot-cgi konvertiert diese Informationen in das WAN-Boot-Dateisystem und überträgt dieses dann an den Client. Mithilfe von Unterverzeichnissen, die Sie in /etc/netboot anlegen können, lässt sich der Aktionsbereich der WAN-Installation anpassen. Mit den folgenden Verzeichnisstrukturen definieren Sie, wie die Konfigurationsinformationen von den zu installierenden Clients gemeinsam verwendet werden sollen.

- Globale Konfiguration Sollen alle Clients in Ihrem Netzwerk dieselben Konfigurationsinformationen verwenden, dann speichern Sie die gemeinsam genutzten Dateien im Verzeichnis /etc/netboot.
- Netzwerk-spezifische Konfiguration Wenn nur die Computer in einem bestimmten Teilnetz Konfigurationsinformationen gemeinsam nutzen sollen, speichern Sie die gemeinsam zu nutzenden Konfigurationsdateien in einem Unterverzeichnis von /etc/netboot. Bei der Benennung des Unterverzeichnisses ist die Namenskonvention zu beachten.

/etc/netboot/net-ip

In diesem Beispiel ist *Netz-IP* die IP-Adresse des Teilnetzes der Clients. Wenn Sie die Konfigurationsdateien beispielsweise an alle Systeme im Teilnetz mit der IP-Adresse

192.168.255.0 freigeben möchten, erzeugen Sie ein Verzeichnis namens /etc/netboot/192.168.255.0. Speichern Sie dann die Konfigurationsdateien in diesem Verzeichnis.

 Client-spezifische Konfiguration – Wenn das Boot-Dateisystem von nur einem bestimmten Client verwendet werden soll, speichern Sie die Dateien in einem Unterverzeichnis von /etc/netboot Bei der Benennung des Unterverzeichnisses ist die Namenskonvention zu beachten.

/etc/netboot/net-ip/client-ID

In diesem Beispiel ist *Netz-IP* die IP-Adresse des Teilnetzes. *Client-ID* ist entweder die vom DHCP-Server zugewiesene oder eine benutzerdefinierte Client-ID. Wenn zum Beispiel ein System mit der Client-ID 010003BA152A42 im Teilnetz 192.168.255.0 systemspezifische Konfigurationsdateien verwenden soll, erzeugen Sie ein Verzeichnis namens /etc/netboot/192.168.255.0/010003BA152A42. Speichern Sie dann die entsprechenden Dateien in diesem Verzeichnis.

Angeben von Konfigurations- und Sicherheitsinformationen im Verzeichnis /etc/netboot

Zum Angeben der Konfigurations- und Sicherheitsinformationen erstellen Sie die folgenden Dateien und speichern sie im Verzeichnis /etc/netboot.

- wanboot.conf Diese Datei enthält die Client-Konfiguration f
 ür eine WAN-Boot-Installation.
- Systemkonfigurationsdatei (system.conf) Diese Systemkonfigurationsdatei enthält den Ort der Client-Datei sysidcfg und der benutzerdefinierten JumpStart-Dateien.
- keystore Diese Datei enthält den HMAC SHA1-Hashing-Schlüssel, die 3DES- bzw. AES-Verschlüsselung und den privaten SSL-Schlüssel des Clients.
- truststore Diese Datei enthält die digitalen Zertifikate der vom Client zu akzeptierenden Zertifikat-Signaturstellen. Diese vertrauenswürdigen Zertifikate weisen den Client an, den Server während der Installation als vertrauenswürdig zu akzeptieren.
- certstore Diese Datei enthält das digitale Zertifikat des Clients.

Hinweis – Die Datei certstore muss im Verzeichnis der Client-ID gespeichert sein. Weitere Informationen über Unterverzeichnisse von /etc/netboot finden Sie in "Anpassung des Aktionsbereichs der WAN-Boot-Installation" auf Seite 164.

Ausführliche Anweisungen zum Erstellen und Speichern dieser Dateien stehen Ihnen in folgenden Abschnitten zur Verfügung:

- "So erzeugen Sie die Systemkonfigurationsdatei" auf Seite 207
- So erzeugen Sie die Datei wanboot.conf" auf Seite 209

- "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195
- "(Optional) So verwenden Sie digitale Zertifikate f
 ür die Server- und Client-Authentifizierung" auf Seite 192

Freigeben von Konfigurations- und Sicherheitsinformationen im Verzeichnis /etc/netboot

Es besteht die Möglichkeit, dass Sie bei der Installation von Clients in Ihrem Netzwerk dieselben Sicherheits- und Konfigurationsdateien für mehrere Clients oder beispielsweise alle Clients eines Teilnetzes verwenden. Zur Freigabe dieser Dateien können Sie die Konfigurationsinformationen in den Verzeichnissen /etc/netboot/*Netz-IP/Client-ID*, /etc/netboot/*Netz-IP* und /etc/netboot bereitstellen. Das Programm wanboot-cgi durchsucht diese Verzeichnisse nach den Konfigurationsinformationen, die am besten auf den jeweiligen Client zutreffen, und verwendet diese Informationen für die Installation.

Das Programm wanboot-cgi sucht in dieser Reihenfolge nach Client-Informationen:

- 1. /etc/netboot/*Netz-IP/Client-ID* Zuerst sucht das Programm wanboot-cgi nach Client-spezifischen Konfigurationsinformationen. Wenn das Verzeichnis /etc/netboot/*Netz-IP/Client-ID* alle Client-Konfigurationsinformationen enthält, sucht das Programm wanboot-cgi an keiner weiteren Stelle im Verzeichnis /etc/netboot nach Konfigurationsinformationen.
- /etc/netboot/Netz-IP Wenn nicht alle erforderlichen Informationen im Verzeichnis /etc/netboot/Netz-IP/Client-ID gefunden werden können, sucht das Programm wanboot-cgi anschließend im Verzeichnis/etc/netboot/Netz-IP nach Teilnetz-Konfigurationsinformationen.
- 3. /etc/netboot Wenn die noch ausstehenden Angaben nicht im Verzeichnis /etc/netboot/*Netz-IP* zu finden sind, sucht das Programm wanboot-cgi dann im Verzeichnis /etc/netboot nach globalen Konfigurationsinformationen.

Abbildung 11–2 zeigt, wie Sie das Verzeichnis /etc/netboot einrichten können, um Ihre WAN-Boot-Installationen anzupassen.



ABBILDUNG 11-2 Beispiel für das Verzeichnis /etc/netboot

Das /etc/netboot-Verzeichnislayout in Abbildung 11–2 ermöglicht Ihnen, die folgenden WAN-Boot-Installationen durchzuführen.

- Wenn Sie Client 010003BA152A42 installieren, verwendet das Programm wanboot-cgi diese Dateien im Verzeichnis /etc/netboot/192.168.255.0/010003BA152A42:
 - system.conf
 - keystore
 - truststore
 - certstore

Anschließend verwendet das Programm wanboot-cgi die Datei wanboot.conf im Verzeichnis/etc/netboot/192.168.255.0.

- Wenn Sie einen Client im Teilnetz 192.168.255.0 installieren, verwendet das Programm wanboot-cgi die Dateien wanboot.conf, keystore und truststore im Verzeichnis /etc/netboot/192.168.255.0. Anschließend verwendet das Programm wanboot-cgi die Datei system.conf im Verzeichnis /etc/netboot.
- Wenn Sie einen Client installieren, der sich außerhalb des Teilnetzes 192.168.255.0 befindet, verwendet das Programm wanboot - cgi die folgenden Dateien im Verzeichnis /etc/netboot.
 - wanboot.conf
 - system.conf
 - keystore
 - truststore

Speichern des Programms wanboot-cgi

Das Programm wanboot - cgi überträgt die Daten und Dateien vom WAN-Boot-Server an den Client. Vergewissern Sie sich, dass sich das Programm in einem für den Client zugänglichen Verzeichnis auf dem WAN-Boot-Server befindet. Eine Möglichkeit, das Programm für den Client zugänglich zu machen, besteht darin, es im Verzeichnis cgi-bin des WAN-Boot-Servers zu speichern. Unter Umständen müssen Sie in der Konfiguration Ihrer Webserver-Software festlegen, dass das Programm wanboot - cgi als CGI-Programm verwendet wird. Informationen über die Voraussetzungen für CGI-Programme entnehmen Sie bitte der Dokumentation Ihres Webservers.

Voraussetzungen für digitale Zertifikate

Möchten Sie die WAN-Boot-Installation sicherer gestalten, können Sie mithilfe von digitalen Zertifikaten eine Server- und eine Client-Authentifizierung in den Vorgang einbinden. Auf der Grundlage von digitalen Zertifikaten kann WAN-Boot bei Online-Transaktionen die Identität des Servers oder des Clients feststellen. Digitale Zertifikate werden von einer Zertifizierungsstelle (CA) ausgestellt. Diese Zertifikate enthalten eine Seriennummer, Ablaufdaten, eine Kopie des öffentlichen Schlüssels des Zertifikatinhabers sowie die digitale Signatur der Zertifizierungsstelle.

Wenn Sie möchten, dass sich der Server oder sowohl der Server als auch der Client bei der Installation ausweisen, müssen Sie auf dem Server digitale Zertifikate installieren. Befolgen Sie beim Einsatz von digitalen Zertifikaten bitte diese Richtlinien:

- Bereits vorhandene digitale Zertifikate müssen als Teil einer PKCS#12-Datei (Public-Key Cryptography Standards #12) formatiert sein.
- Wenn Sie eigene Zertifikate erzeugen möchten, müssen Sie sie als PKCS#12-Dateien erstellen.
- Wenn Sie Ihre Zertifikate von externen Zertifizierungsstellen erhalten, fordern Sie sie im PKCS#12-Format an.

Ausführliche Anweisungen zur Verwendung von PKCS#12-Zertifikaten bei der WAN-Boot-Installation finden Sie in "(Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung" auf Seite 192.

Sicherheitslücken bei der Arbeit mit WAN-Boot

Es stehen zwar verschiedene Sicherheitsfunktionen für WAN-Boot zur Verfügung, die folgenden potenziellen Sicherheitsrisiken bleiben jedoch trotzdem bestehen:

- Denial of Service (DoS) Ein DoS-Angriff kann in den verschiedensten Formen erfolgen und hat immer das Ziel, Benutzer am Zugriff auf einen bestimmten Dienst zu hindern. Ein solcher DoS-Angriff kann entweder bewirken, dass ein Netzwerk mit großen Datenmengen überflutet wird oder dass limitierte Ressourcen aggressiv genutzt werden. Andere DoS-Angriffe manipulieren die zwischen den Systemen übertragenen Daten. Das WAN-Boot-Installationsverfahren bietet Servern oder Clients keinen Schutz vor DoS-Angriffen.
- Beschädigte Binärdateien auf Servern Das WAN-Boot-Installationsverfahren führt vor Beginn der Installation keine Integritätsprüfung der WAN-Boot-Miniroot oder des Solaris Flash-Archivs durch. Vergleichen Sie deshalb vor der Installation die Solaris-Binärdateien mit der Solaris-Fingerabdruckdatenbank unter http://sunsolve.sun.com.
- Datenschutz für Chiffrier- und Hashing-Schlüssel Wenn Sie WAN-Boot mit Verschlüsselung (Chiffrierschlüsseln) oder einem Hashing-Schlüssel einsetzen, müssen Sie den Schlüsselwert bei der Installation in die Befehlszeile eingeben. Ergreifen Sie die für Ihr Netzwerk erforderlichen Sicherheitsmaßnahmen zur Geheimhaltung dieser Schlüsselwerte.
- Beschädigung des Netzwerk-Naming Service Wenn in Ihrem Netzwerk ein Naming Service verwendet wird, überprüfen Sie die Integrität der Namenserver vor der Installation von WAN-Boot.

Zusammenstellen der Informationen für WAN-Boot-Installationen

Um Ihr Netzwerk für eine WAN-Boot-Installation zu konfigurieren, müssen Sie die verschiedensten Informationen zusammenstellen. Im Rahmen der Vorbereitung einer Installation über das WAN sollten Sie sich diese Angaben notieren.

Zum Aufzeichnen der WAN-Boot-Installationsinformationen für Ihr Netzwerk stehen Ihnen die folgenden Arbeitsblätter zur Verfügung:

- Tabelle 11–2
- Tabelle 11–3

Benötigte Information	Anmerkung
Angaben zum Installationsserver	
 Pfad zur WAN-Boot-Miniroot auf den Installationsserver Pfad zu den JumpStart-Dateien auf den Installationsserver 	n
Angaben zum WAN-Boot-Server	
 Pfad zum wanboot-Programm auf dem WAN-Boot-Server 	1
 URL des Programms wanboot - cgi auf WAN-Boot-Server 	dem
 Pfad zum Client-Unterverzeichnis in d /etc/netboot-Hierarchie auf dem WAN-Boot-Server 	ler
 (Optional) Dateiname der PKCS#12-Zertifikatdatei 	
 (Optional) Host-Namen aller f ür die WAN-Installation ben ötigten Systeme dem WAN-Boot-Server 	außer
 (Optional) IP-Adresse und TCP-Port-Nummer des Proxy-Servers Netzwerk 	im
Angaben zu nicht obligatorischen Servern URL des Skripts bootlog- coi auf dem	
Protokollserver	
 IP-Adresse und TCP-Port-Nummer de Proxy-Servers im Netzwerk 	25

TABELLE 11-2 Arbeitsblatt für die Zusammenstellung von Server-Informationen

TABELLE 11-3 Arbeitsblatt für die Zusammenstellung von Client-Informationen

Informationen	Anmerkung
IP-Adresse des Client-Teilnetzes	
IP-Adresse des Client-Routers	
IP-Adresse des Clients	
Client-Teilnetzmaske	
Host-Name des Clients	

 TABELLE 11-3
 Arbeitsblatt für die Zusammenstellung von Client-Informationen
 (Fortsetzung)

 Informationen
 Anmerkung

MAC-Adresse des Clients

♦ ♦ ♦ KAPITEL 12

Installieren mit WAN-Boot (Vorgehen)

In diesem Kapitel werden die folgenden Schritte zur Vorbereitung Ihres Netzwerks für eine WAN-Boot-Installation erläutert:

- "Installieren über ein regional erweitertes Netzwerk (WAN) (Übersicht der Schritte)" auf Seite 173
- "Konfiguration des WAN-Boot-Servers" auf Seite 177
- "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation" auf Seite 197
- "Erstellen der Konfigurationsdateien" auf Seite 207
- "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214
- "(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190

Installieren über ein regional erweitertes Netzwerk (WAN) (Übersicht der Schritte)

In den folgenden Tabellen sehen Sie die Schritte, die Sie zur Vorbereitung einer WAN-Boot-Installation durchführen müssen.

• Eine Liste der Schritte, die Sie zur Vorbereitung einer sicheren WAN-Boot-Installation durchführen müssen, finden Sie in Tabelle 12–1.

Eine Beschreibung einer sicheren WAN-Boot-Installation über HTTPS finden Sie unter "Sichere WAN-Boot-Installationskonfiguration" auf Seite 158.

• Eine Liste der Schritte, die Sie zur Vorbereitung einer unsicheren WAN-Boot-Installation durchführen müssen, finden Sie in Tabelle 12–2.

Eine Beschreibung einer unsicheren WAN-Boot-Installation finden Sie unter "Unsichere WAN-Boot-Installationskonfiguration" auf Seite 158.

Wenn Sie einen DHCP-Server oder einen Protokollserver verwenden möchten, führen Sie außerdem die Zusatzschritte aus, die am Ende der jeweiligen Tabelle angegeben sind.

Aufgabe	Beschreibung	Siehe
Entscheiden Sie, welche Sicherheitsfunktionen Sie bei der Installation einsetzen möchten.	Lesen Sie die Informationen über Sicherheitsfunktionen und -konfigurationen, um eine geeignete Sicherheitsstufe für Ihre WAN-Boot-Installation wählen zu können.	"Schutz der Daten während einer WAN-Boot-Installation" auf Seite 156
		"Von WAN-Boot unterstützte Sicherheitskonfigurationen (Übersicht)" auf Seite 157
Stellen Sie Informationen für die WAN-Boot-Installation zusammen.	Füllen Sie das Arbeitsblatt aus, damit Ihnen anschließend alle für die WAN-Boot-Installation benötigten Angaben vorliegen.	"Zusammenstellen der Informationen für WAN-Boot-Installationen" auf Seite 169
Erzeugen Sie auf dem WAN-Boot-Server das Dokument-Root-Verzeichnis.	Legen Sie das Dokument-Root-Verzeichnis und etwaige Unterverzeichnisse für die Konfigurations- und Installationsdateien an.	"Erstellen des Dokument-Root-Verzeichnisses" auf Seite 178
Erzeugen Sie die WAN-Boot-Miniroot.	Erzeugen Sie mit dem Befehl setup_install_server die WAN-Boot-Miniroot.	"SPARC: Erzeugen der WAN-Boot-Miniroot" auf Seite 178
Vergewissern Sie sich, dass das Clientsystem Unterstützung für WAN-Boot bietet.	Überprüfen Sie, ob das Client-OBP die Boot-Argumente für WAN-Boot unterstützt.	"So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung" auf Seite 182
Installieren Sie das wanboot-Programm auf dem WAN-Boot-Server.	Kopieren Sie das wanboot-Programm in das Dokument-Root-Verzeichnis auf dem WAN-Boot-Server.	"Installation des wanboot-Programms auf dem WAN-Boot-Server" auf Seite 183
Installieren Sie das Programm wanboot - cgi auf dem WAN-Boot-Server.	Kopieren Sie das Programm wanboot - cgi in das CGI-Verzeichnis auf dem WAN-Boot-Server.	"So kopieren Sie das Programm wanboot - cgi auf den WAN-Boot-Server" auf Seite 189
(Optional) Richten Sie den Protokollserver ein.	Konfigurieren Sie ein spezielles System für die Anzeige von Boot- und Installationsprotokoll- meldungen.	"(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190
Legen Sie die /etc/netboot-Hierarchie an.	Speichern Sie die für eine WAN-Boot-Installation erforderlichen Konfigurations- und Sicherheitsdateien in der /etc/netboot-Hierarchie.	"Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186

TABELLE 12-1 Übersicht der Schritte: Vorbereitung für eine sichere WAN-Boot-Installation

Aufgabe	Beschreibung	Siehe
Für eine sicherere WAN-Boot-Installation stellen Sie die Webserver-Konfiguration auf sicheres HTTP ein.	Ermitteln Sie die Webserver-Voraussetzungen für eine WAN-Installation per HTTPS.	"(Optional) Schützen der Daten mit HTTPS" auf Seite 191
Formatieren Sie digitale Zertifikate für eine sicherere WAN-Boot-Installation.	Teilen Sie eine PKCS#12-Datei in einen privaten Schlüssel und ein Zertifikat für die WAN-Installation auf.	"(Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung" auf Seite 192
Erzeugen Sie einen Hashing- und einen Chiffrierschlüssel für eine sicherere WAN-Boot-Installation.	Generieren Sie HMAC SHA1-, 3DES- oder AES-Schlüssel mit dem Befehl wanbootutil keygen.	"(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195
Erzeugen Sie das Solaris Flash-Archiv.	Erstellen Sie mit dem Befehl flar create ein Archiv der Software, die auf dem Client installiert werden soll.	"So erzeugen Sie das Solaris Flash-Archiv" auf Seite 198
Erzeugen Sie die Installationsdateien für die benutzerdefinierte JumpStart-Installation.	Erzeugen Sie die folgenden Dateien in einem Texteditor: • sysidcfg • Profil • rules.ok • begin scripts • finish scripts	"So erzeugen Sie die Datei sysidcfg" auf Seite 200 "So erstellen Sie das Profil" auf Seite 201 "So erstellen Sie die Datei rules" auf Seite 203 "(Optional) Erzeugen von Begin- und Finish-Skripten" auf Seite 206
Erzeugen Sie die Systemkonfigurationsdatei.	Geben Sie in der Datei system.conf die Konfigurationsinformationen an.	"So erzeugen Sie die Systemkonfigurationsdatei" auf Seite 207
Erzeugen Sie die WAN-Boot-Konfigurationsdatei.	Geben Sie in der Datei wanboot . conf die Konfigurationsinformationen an.	"So erzeugen Sie die Datei wanboot . conf" auf Seite 209
(Optional) Aktivieren Sie in der Konfiguration des DHCP-Servers die Unterstützung für die WAN-Boot-Installation.	Geben Sie auf dem DHCP-Server Sun-Herstelleroptionen und -Makros an.	"Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52

 TABELLE 12-1
 Übersicht der Schritte: Vorbereitung für eine sichere WAN-Boot-Installation

 (Fortsetzung)
 (Fortsetzung)

Aufgabe	Beschreibung	Siehe
Entscheiden Sie, welche Sicherheitsfunktionen Sie bei der Installation einsetzen möchten.	Lesen Sie die Informationen über Sicherheitsfunktionen und -konfigurationen, um eine geeignete Sicherheitsstufe für Ihre WAN-Boot-Installation wählen zu können.	"Schutz der Daten während einer WAN-Boot-Installation" auf Seite 156
		"Von WAN-Boot unterstützte Sicherheitskonfigurationen (Übersicht)" auf Seite 157
Stellen Sie Informationen für die WAN-Boot-Installation zusammen.	Füllen Sie das Arbeitsblatt aus, damit Ihnen anschließend alle für die WAN-Boot-Installation benötigten Angaben vorliegen.	"Zusammenstellen der Informationen für WAN-Boot-Installationen" auf Seite 169
Erzeugen Sie auf dem WAN-Boot-Server das Dokument-Root-Verzeichnis.	Legen Sie das Dokument-Root-Verzeichnis und etwaige Unterverzeichnisse für die Konfigurations- und Installationsdateien an.	"Erstellen des Dokument-Root-Verzeichnisses" auf Seite 178
Erzeugen Sie die WAN-Boot-Miniroot.	Erzeugen Sie mit dem Befehl setup_install_server die WAN-Boot-Miniroot.	"SPARC: Erzeugen der WAN-Boot-Miniroot" auf Seite 178
Vergewissern Sie sich, dass das Clientsystem Unterstützung für WAN-Boot bietet.	Überprüfen Sie, ob das Client-OBP die Boot-Argumente für WAN-Boot unterstützt.	"So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung" auf Seite 182
Installieren Sie das wanboot-Programm auf dem WAN-Boot-Server.	Kopieren Sie das wanboot-Programm in das Dokument-Root-Verzeichnis auf dem WAN-Boot-Server.	"Installation des wanboot-Programms auf dem WAN-Boot-Server" auf Seite 183
Installieren Sie das Programm wanboot - cgi auf dem WAN-Boot-Server.	Kopieren Sie das Programm wanboot - cgi in das CGI-Verzeichnis auf dem WAN-Boot-Server.	"So kopieren Sie das Programm wanboot - cgi auf den WAN-Boot-Server" auf Seite 189
(Optional) Richten Sie den Protokollserver ein.	Konfigurieren Sie ein spezielles System für die Anzeige von Boot- und Installationsprotokoll- meldungen.	"(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190
Legen Sie die /etc/netboot-Hierarchie an.	Speichern Sie die für eine WAN-Boot-Installation erforderlichen Konfigurations- und Sicherheitsdateien in der /etc/netboot-Hierarchie.	"Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186

 TABELLE 12-2
 Übersicht der Schritte: Vorbereitung für eine unsichere WAN-Boot-Installation

Aufgabe	Beschreibung	Siehe
(Optional) Generieren Sie einen Hashing-Schlüssel.	Erzeugen Sie mit dem Befehl wanbootutil keygen einen HMAC SHA1-Schlüssel.	"(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195
	Für unsichere Installationen mit Überprüfung der Datenintegrität generieren Sie in diesem Schritt einen HMAC SHA1-Hashing-Schlüssel.	
Erzeugen Sie das Solaris Flash-Archiv.	Erstellen Sie mit dem Befehl flar create ein Archiv der Software, die auf dem Client installiert werden soll.	"So erzeugen Sie das Solaris Flash-Archiv" auf Seite 198
Erzeugen Sie die Installationsdateien für die benutzerdefinierte JumpStart-Installation.	Erzeugen Sie die folgenden Dateien in einem Texteditor: sysidcfg profile rules.ok Begin-Skripten Finish-Skripten	"So erzeugen Sie die Datei sysidcfg" auf Seite 200
		"So erstellen Sie das Profil" auf Seite 201
		"So erstellen Sie die Datei rules" auf Seite 203
		"(Optional) Erzeugen von Begin- und Finish-Skripten" auf Seite 206
Erzeugen Sie die Systemkonfigurationsdatei.	Geben Sie in der Datei system.conf die Konfigurationsinformationen an.	"So erzeugen Sie die Systemkonfigurationsdatei" auf Seite 207
Erzeugen Sie die WAN-Boot-Konfigurationsdatei.	Geben Sie in der Datei wanboot . conf die Konfigurationsinformationen an.	"So erzeugen Sie die Datei wanboot . conf" auf Seite 209
(Optional) Aktivieren Sie in der Konfiguration des DHCP-Servers die Unterstützung für die WAN-Boot-Installation.	Geben Sie auf dem DHCP-Server Sun-Herstelleroptionen und -Makros an.	"Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52

 TABELLE 12-2
 Übersicht der Schritte: Vorbereitung für eine unsichere WAN-Boot-Installation (Fortsetzung)

Konfiguration des WAN-Boot-Servers

Beim WAN-Boot-Server handelt es sich um einen Webserver, der die Boot- und Konfigurationsdaten für die WAN-Boot-Installation bereitstellt. Eine Übersicht der Systemanforderungen für den WAN-Boot-Server finden Sie in Tabelle 11–1.

In diesem Abschnitt werden die folgenden Schritte beschrieben, die zur Konfiguration des WAN-Boot-Servers für eine WAN-Boot-Installation nötig sind:

- "Erstellen des Dokument-Root-Verzeichnisses" auf Seite 178
- "Erzeugen der WAN-Boot-Miniroot" auf Seite 178
- "Installation des wanboot-Programms auf dem WAN-Boot-Server" auf Seite 183
- "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186
- "Kopieren des WAN-Boot-CGI-Programms auf den WAN-Boot-Server" auf Seite 189
- "(Optional) Schützen der Daten mit HTTPS" auf Seite 191

Erstellen des Dokument-Root-Verzeichnisses

Damit die Webserver-Software auf dem WAN-Boot-Server die Konfigurations- und Installationsdateien bereitstellen kann, müssen Sie ihr Zugang zu diesen Dateien einräumen. Eine Möglichkeit, die Dateien zugänglich zu machen, besteht darin, sie im Dokument-Root-Verzeichnis auf dem WAN-Boot-Server zu speichern.

Wenn Sie die Konfigurations- und Installationsdateien in einem Dokument-Root-Verzeichnis zur Verfügung stellen möchten, müssen Sie dieses Verzeichnis zunächst anlegen. Wie Sie das Dokument-Root-Verzeichnis erzeugen, entnehmen Sie bitte der Dokumentation Ihres Webservers. Ausführliche Informationen zum Planen Ihres Dokument-Root-Verzeichnisses finden Sie unter "Speichern von Installations- und Konfigurationsdateien im Dokument-Root-Verzeichnis" auf Seite 162.

Im Abschnitt "Erstellen des Dokument-Root-Verzeichnisses" auf Seite 241 ist beispielhaft dargestellt, wie Sie ein Dokument-Root-Verzeichnis einrichten.

Nachdem Sie das Dokument-Root-Verzeichnis eingerichtet haben, erstellen Sie die WAN-Boot-Miniroot. Eine Anleitung hierzu finden Sie im Abschnitt "Erzeugen der WAN-Boot-Miniroot" auf Seite 178.

Erzeugen der WAN-Boot-Miniroot

WAN-Boot verwendet eine speziell auf die WAN-Boot-Installation ausgerichtete Solaris-Miniroot. Die WAN-Boot-Miniroot enthält einen Teilsatz der Software in der Solaris-Miniroot. Wenn Sie eine WAN-Boot-Installation durchführen möchten, müssen Sie die Miniroot von der Solaris-DVD oder der Solaris Software-1 CD auf den WAN-Boot-Server kopieren. Kopieren Sie die WAN-Boot-Miniroot mit dem Befehl setup_install_server und der Option -w vom Solaris-Softwaredatenträger auf die Festplatte des Systems.

SPARC: Erzeugen der WAN-Boot-Miniroot

Bei diesem Verfahren wird eine SPARC-WAN-Boot-Miniroot mit einem SPARC-Datenträger erzeugt. Wenn Sie eine SPARC-WAN-Boot-Miniroot von einem x86–basierten Server aus zur Verfügung stellen möchten, müssen Sie die Miniroot auf einem SPARC-System erzeugen. Nachdem Sie die Miniroot erzeugt haben, kopieren Sie sie in das Dokument-Root-Verzeichnis auf dem x86–basierten Server. Bevor Sie
beginnenBei diesem Verfahren wird davon ausgegangen, dass Volume Manager auf dem
WAN-Boot-Server läuft. Wenn Sie nicht den Volume Manager verwenden, lesen Sie System
Administration Guide: Devices and File Systems .

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim WAN-Boot-Server an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Das System muss die folgenden Voraussetzungen erfüllen:

- Es muss ein CD-ROM- oder DVD-ROM-Laufwerk aufweisen.
- Es muss Teil des Netzwerks und Naming Service des Standorts sein.

Wenn Sie einen Naming Service verwenden, muss sich das System außerdem bereits in einem Naming Service wie NIS, NIS+, DNS oder LDAP befinden. Wenn Sie keinen Naming Service verwenden, müssen Sie die Informationen über dieses System in Übereinstimmung mit den Richtlinien des jeweiligen Standorts verteilen.

2 Legen Sie die Solaris Software-1 CD oder die Solaris-DVD in das Laufwerk des Installationsservers ein.

3 Erzeugen Sie ein Verzeichnis für die WAN-Boot-Miniroot und das Solaris-Installationsabbild.

mkdir -p wan-dir-path install-dir-path

- p	Weist den Befehl mkdir an, alle erforderlichen übergeordneten Verzeichnisse für das gewünschte Verzeichnis zu erzeugen.
WAN_verz_pfad	Gibt das Verzeichnis auf dem Installationsserver an, in dem die WAN-Boot-Miniroot erzeugt werden soll. Dieses Verzeichnis muss Miniroots aufnehmen können, die in der Regel 250 MB groß sind.
Inst_verz_pfad	Gibt das Verzeichnis auf dem Installationsserver an, in welches das Solaris-Software-Abbild kopiert werden soll. Dieses Verzeichnis kann zu einem späteren Zeitpunkt in diesem Verfahren entfernt werden.

4 Wechseln Sie in das Verzeichnis Tools auf dem eingehängten Datenträger.

cd /cdrom/cdrom0/Solaris_10/Tools

In diesem Beispiel ist cdrom0 der Pfad zu dem Laufwerk mit dem BS-Datenträger.

5 Kopieren Sie die WAN-Boot-Miniroot und das Solaris-Software-Abbild auf die Festplatte des WAN-Boot-Servers.

./setup_install_server -w wan-dir-path install-dir-path

- WAN_verz_pfad Gibt das Verzeichnis an, in das die WAN-Boot-Miniroot kopiert werden soll.
 Inst_verz_pfad Gibt das Verzeichnis an, in welches das Solaris-Software-Abbild kopiert
- werden soll.

Hinweis – Der Befehl setup_install_server gibt an, ob ausreichend Festplattenspeicher für die Solaris Software-Datenträgerabbilder vorhanden ist. Um den verfügbaren Festplattenspeicher zu ermitteln, verwenden Sie den Befehl df -kl.

Der Befehl setup_install_server -w erzeugt die WAN-Boot-Miniroot und ein Netzwerkinstallationsabbild der Solaris-Software.

6 (Optional) Entfernen Sie das Netzwerkinstallationsabbild.

Für eine WAN-Installation mit Solaris Flash-Archiv brauchen Sie das Solaris-Software-Abbild nicht. Wenn Sie nicht beabsichtigen, das Netzwerkinstallationsabbild für weitere Netzwerkinstallationen einzusetzen, haben Sie also die Möglichkeit, Speicherplatz auf der Festplatte freizuräumen. Geben Sie folgenden Befehl ein, um das Netzwerkinstallationsabbild zu löschen.

rm -rf install-dir-path

- 7 Räumen Sie dem WAN-Boot-Server auf eine der folgenden Weisen Zugang zur WAN-Boot-Miniroot ein.
 - Erzeugen Sie einen symbolischen Link auf die WAN-Boot-Miniroot im Dokument-Root-Verzeichnis des WAN-Boot-Servers.

# cd	/document-root-directory/miniroot

ln -s /wan-dir-path/miniroot .

Dok_Root-Verz/miniroot	Gibt das Verzeichnis im Dokument-Root-Verzeichnis des
	WAN-Boot-Servers an, in dem Sie die Verknüpfung zur
	WAN-Boot-Miniroot erzeugen möchten.
/WAN verz pfad/miniroot	Gibt den Pfad zur WAN-Boot-Miniroot an.

 Verschieben Sie die WAN-Boot-Miniroot in das Dokument-Root-Verzeichnis auf dem WAN-Boot-Server.

mv /wan-dir-path/miniroot /document-root-directory/miniroot/miniroot-name

<pre>WAN_verz_pfad/miniroot</pre>	Gibt den Pfad zur WAN-Boot-Miniroot an.
/Dok_Root-Verz/miniroot/	Gibt den Pfad zum WAN-Boot-Miniroot-Verzeichnis im Dokument-Root-Verzeichnis des WAN-Boot-Servers
	an.
Miniroot-Name

Steht für den Namen der WAN-Boot-Miniroot. Geben Sie der Datei einen aussagefähigen Namen, beispielsweise miniroot.s10_sparc.

Beispiel 12–1 Erzeugen der WAN-Boot-Miniroot

Kopieren Sie die WAN-Boot-Miniroot und das Solaris-Software-Abbild mit dem Befehl setup_install_server(1M) und der Option -w in das Verzeichnis /export/install/Solaris_10 von wanserver-1.

Legen Sie den Solaris Software-Datenträger in das an wanserver - 1 angeschlossene Laufwerk ein. Geben Sie die folgenden Befehle ein.

```
wanserver-1# mkdir -p /export/install/cdrom0
wanserver-1# cd /cdrom/cdrom0/Solaris_10/Tools
wanserver-1# ./setup_install_server -w /export/install/cdrom0/miniroot \
/export/install/cdrom0
```

Verschieben Sie die WAN-Boot-Miniroot in das Dokument-Root-Verzeichnis (/opt/apache/htdocs/) des WAN-Boot-Servers. In diesem Beispiel lautet der Name der WAN-Boot-Minirootminiroot.s10_sparc.

```
wanserver-1# mv /export/install/cdrom0/miniroot/miniroot \
/opt/apache/htdocs/miniroot/miniroot.s10_sparc
```

```
Weitere<br/>Informationen:Fortsetzen der WAN-Boot-InstallationNachdem Sie die WAN-Boot-Miniroot erstellt haben, müssen Sie prüfen, ob das OpenBoot<br/>PROM (OBP) auf dem Client WAN-Bootvorgänge unterstützt. Wie das geht, erfahren Sie im<br/>Abschnitt "Überprüfen des Clients auf WAN-Boot-Unterstützung" auf Seite 181.Siehe undNähren Information und Steinen Befehl estere singetelle esteren fin den Sie in<br/>
```

Siehe auch Nähere Informationen zum Befehl setup_install_server finden Sie in install_scripts(1M).

Überprüfen des Clients auf WAN-Boot-Unterstützung

Für eine WAN-Boot-Installation ohne Benutzereingriff muss das Client-OpenBoot PROM (OBP) Unterstützung für WAN-Boot bieten. Sollte dies nicht der Fall sein, können Sie die WAN-Boot-Installation durchführen, indem Sie die erforderlichen Programme lokal auf einer CD bereitstellen.

Ob der Client WAN-Bootvorgänge unterstützt, können Sie anhand seiner OBP-Konfigurationsvariablen ermitteln. Gehen Sie dazu wie im Folgenden beschrieben vor.

So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung

Mit dem folgenden Verfahren können Sie feststellen, ob das Client-OBP Unterstützung für WAN-Boot bietet.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Überprüfen Sie die OBP-Konfigurationsvariablen auf WAN-Boot-Unterstützung.

eeprom | grep network-boot-arguments

- Wenn die Variable network-boot-arguments angezeigt wird oder der obige Befehl die Ausgabe network-boot-arguments: data not available liefert, bietet das OBP Unterstützung für WAN-Boot-Installationen. Sie müssen das OBP vor der WAN-Boot-Installation also nicht aktualisieren.
- Liefert der vorige Befehl keine Ausgabe, bedeutet dies, dass das OBP WAN-Boot-Installationen nicht unterstützt. In diesem Fall müssen Sie eine der nachfolgenden Maßnahmen ergreifen.
 - Aktualisieren Sie das Client-OBP. Bei Clients, die über ein WAN-Boot-Installationen unterstützendes OBP verfügen, können Sie Informationen zum Aktualisieren des OBP in der Systemdokumentation nachlesen.

Hinweis – Nicht alle Client-OBPs unterstützen WAN-Boot. Für diese Clients verwenden Sie die nächste Option.

 Wenn Sie die erforderlichen Vorbereitungsschritte abgeschlossen haben und bereit zur Client-Installation sind, führen Sie die WAN-Boot-Installation von der Solaris Software-CD1 oder DVD aus. Diese Option funktioniert in Fällen, bei denen das aktuelle OBP das WAN-Booten nicht unterstützt.

Wie Sie den Client von CD1 booten, erfahren Sie in "So nehmen Sie eine WAN-Boot-Installation mit lokalen CDs vor" auf Seite 233. Informationen zu den restlichen Vorbereitungsschritten finden Sie im Abschnitt "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186.

Beispiel 12–2 Überprüfen des Client-OBP auf Unterstützung für WAN-Boot

Mit dem folgenden Befehl stellen Sie fest, ob das Client-OBP Unterstützung für WAN-Boot bietet.

eeprom | grep network-boot-arguments
network-boot-arguments: data not available

Die Ausgabe network-boot-arguments: data not available in diesem Beispiel weist darauf hin, dass das Client-OBP Unterstützung für WAN-Boot-Installationen bietet.

Weitere
Informationen:Fortsetzen der WAN-Boot-InstallationWenn Sie überprüft haben, dass das Client-OBP WAN-Boot unterstützt, müssen Sie das
Programm wanboot auf den WAN-Boot-Server kopieren. Eine Anleitung hierzu finden Sie im

Abschnitt "Installation des wanboot-Programms auf dem WAN-Boot-Server" auf Seite 183. Sollte das Client-OBP hingegen keine Unterstützung für wanboot bieten, ist dieser Schritt überflüssig. Stattdessen stellen Sie das wanboot-Programm auf dem Client auf einer lokalen CD bereit. Der nächste Schritt im Installationsprozess ist im Abschnitt "Erstellen der

/etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186 beschrieben.

Siehe auch Weitere Informationen zum Befehl setup_install_server finden Sie in Kapitel 4, "Installieren über das Netzwerk (Übersicht)".

Installation des wanboot-Programms auf dem WAN-Boot-Server

Für die Installation des Clients kommt in WAN-Boot ein spezielles Unterprogramm (wanboot) zum Einsatz. Das wanboot-Programm lädt die WAN-Boot-Miniroot, die Client-Konfigurationsdateien und die für eine WAN-Boot-Installation erforderlichen Installationsdateien.

Das wanboot-Programm muss dem Client während der WAN-Boot-Installation zur Verfügung gestellt werden. Hierzu haben Sie folgende Möglichkeiten:

 Wenn der Client-PROM WAN-Boot unterstützt, können Sie das Programm vom WAN-Boot-Server auf den Client übertragen. In diesem Falle müssen Sie das wanboot-Programm auf dem WAN-Boot-Server installieren.

Wie Sie herausfinden, ob das Client-PROM WAN-Boot unterstützt, ist im Abschnitt "So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung" auf Seite 182 beschrieben. Wenn der Client-PROM keine Unterstützung für WAN-Boot bietet, müssen Sie dem Client das Programm auf einer lokalen CD zur Verfügung stellen. In diesem Fall setzen Sie die Installationsvorbereitung wie unter "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186 beschrieben fort.



SPARC: Installation des wanboot-Programms auf dem WAN-Boot-Server

Dieses Verfahren beschreibt, wie Sie das wanboot-Programm von den Solaris-Datenträgern auf den WAN-Boot-Server kopieren.

Bei diesem Verfahren wird davon ausgegangen, dass Volume Manager auf dem WAN-Boot-Server läuft. Wenn Sie nicht den Volume Manager verwenden, lesen Sie *System Administration Guide: Devices and File Systems*.

Bevor Sie
beginnenVergewissern Sie sich, dass das Clientsystem Unterstützung für WAN-Boot bietet. Die
erforderlichen Schritte hierzu sind unter "So überprüfen Sie das Client-OBP auf
WAN-Boot-Unterstützung" auf Seite 182 beschrieben.

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim Installationsserver an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

- 2 Legen Sie die Solaris Software-1 CD oder die Solaris-DVD in das Laufwerk des Installationsservers ein.
- 3 Wechseln Sie in das Plattformverzeichnis sun4u auf der Solaris Software-1 CD oder der Solaris-DVD.

cd /cdrom/cdrom0/Solaris_10/Tools/Boot/platform/sun4u/

4 Kopieren Sie das wanboot-Programm auf den Installationsserver.

cp wanboot /document-root-directory/wanboot/wanboot-name

Dokument-Root-Verz Steht für das Dokument-Root-Verzeichnis auf dem WAN-Boot-Server.

- *Wanboot-Name* Gibt den Namen des wanboot-Programms an. Geben Sie der Datei einen aussagefähigen Namen, beispielsweise wanboot.s10_sparc.
- 5 Räumen Sie dem WAN-Boot-Server auf eine der folgenden Weisen Zugang zum wanboot-Programm ein.

 Erzeugen Sie einen symbolischen Link auf das wanboot-Programm im Dokument-Root-Verzeichnis des WAN-Boot-Servers.

# cd # ln	/document-root-directory/wanbc -s /wan-dir-path/wanboot .	pot	
Doku	ument-Root-Verz/wanboot	Gibt das Verzeichnis im Dokument-Root-Verzeichnis des WAN-Boot-Servers an, in dem Sie die Verknüpfung zum wanboot-Programm erzeugen möchten.	
/WA	<i>N_verz_pfad/</i> wanboot	Gibt den Pfad zum wanboot-Programm an.	
Verso WAN	Verschieben Sie die WAN-Boot-Miniroot in das Dokument-Root-Verzeichnis auf dem WAN-Boot-Server.		
<pre># mv /wan-dir-path/wanboot /document-root-directory/wanboot/wanboot-name</pre>			
WAN	<i>I_verz_pfad/</i> wanboot	Gibt den Pfad zum wanboot-Programm an.	
Doku	<i>ment-Root-Verz/</i> wanboot/	Gibt den Pfad zum wanboot-Programmverzeichnis im Dokument-Root-Verzeichnis des WAN-Boot-Servers an.	
Wan	boot-Name	Gibt den Namen des wanboot-Programms an. Geben Sie der Datei einen aussagefähigen Namen, beispielsweise wanboot.s10 sparc.	

Beispiel 12–3 Installation des wanboot-Programms auf dem WAN-Boot-Server

Zum Installieren des wanboot-Programms auf dem WAN-Boot-Server kopieren Sie das Programm vom Solaris Software-Datenträger in das Dokument-Root-Verzeichnis des WAN-Boot-Servers.

Legen Sie die Solaris-DVD oder die Solaris Software-1 CD in das an wanserver-1 angeschlossene Laufwerk ein, und geben Sie folgende Befehle ein:

wanserver-1# cd /cdrom/cdrom0/Solaris_10/Tools/Boot/platform/sun4u/ wanserver-1# cp wanboot /opt/apache/htdocs/wanboot/wanboot.s10_sparc

In diesem Beispiel lautet der Name des wanboot-Programms wanboot.s10_sparc.

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie das wanboot-Programm auf dem WAN-Boot-Server installiert haben, müssen Sie die /etc/netboot-Hierarchie auf dem WAN-Boot-Server erstellen. Dieser Schritt ist im Abschnitt "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186 beschrieben.

Siehe auch Einen Überblick über das wanboot-Programm erhalten Sie im Abschnitt "Was ist WAN-Boot?" auf Seite 151.

Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server

Während der Installation sucht WAN-Boot in der /etc/netboot-Hierarchie auf dem Webserver nach Installationsanweisungen. Dieses Verzeichnis enthält die Konfigurationsinformationen, den privaten Schlüssel, das digitale Zertifikat und die Zertifizierungsstelle, die für die WAN-Boot-Installation benötigt werden. Aus diesen Informationen bildet das Programm wanboot-cgi bei der Installation das WAN-Boot-Dateisystem. Anschließend überträgt das Programm wanboot-cgi das WAN-Boot-Dateisystem an den Client.

Mithilfe von Unterverzeichnissen, die Sie in /etc/netboot anlegen können, lässt sich der Aktionsbereich der WAN-Installation anpassen. Mit den folgenden Verzeichnisstrukturen definieren Sie, wie die Konfigurationsinformationen von den zu installierenden Clients gemeinsam verwendet werden sollen.

- Globale Konfiguration Sollen alle Clients in Ihrem Netzwerk dieselben Konfigurationsinformationen verwenden, dann speichern Sie die gemeinsam genutzten Dateien im Verzeichnis /etc/netboot.
- Netzwerk-spezifische Konfiguration Wenn nur die Computer in einem bestimmten Teilnetz Konfigurationsinformationen gemeinsam nutzen sollen, speichern Sie die gemeinsam zu nutzenden Konfigurationsdateien in einem Unterverzeichnis von /etc/netboot. Bei der Benennung des Unterverzeichnisses ist die Namenskonvention zu beachten.

/etc/netboot/net-ip

In diesem Beispiel ist Netz-IP die IP-Adresse des Teilnetzes der Clients.

 Client-spezifische Konfiguration – Wenn das Boot-Dateisystem von nur einem bestimmten Client verwendet werden soll, speichern Sie die Dateien in einem Unterverzeichnis von /etc/netboot Bei der Benennung des Unterverzeichnisses ist die Namenskonvention zu beachten.

/etc/netboot/net-ip/client-ID

In diesem Beispiel ist *Netz-IP* die IP-Adresse des Teilnetzes. *Client-ID* ist entweder die vom DHCP-Server zugewiesene oder eine benutzerdefinierte Client-ID.

Ausführliche Hinweise zur Planung dieser Konfigurationen finden Sie in "Speichern von Konfigurations- und Sicherheitsinformationen in der /etc/netboot-Hierarchie" auf Seite 164.

Das folgende Verfahren beschreibt, wie Sie die /etc/netboot-Hierarchie erstellen.

So erstellen Sie die /etc/netboot-Hierarchie auf dem WAN-Boot-Server

Gehen Sie wie folgt vor, um die /etc/netboot-Hierarchie zu erstellen.

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim WAN-Boot-Server an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

- 2 Erzeugen Sie das Verzeichnis / etc/netboot. # mkdir /etc/netboot
- 3 Setzen Sie die Berechtigungen für das Verzeichnis /etc/netboot auf 700.

chmod 700 /etc/netboot

- Setzen Sie den Eigentümer des Verzeichnisses /etc/netboot auf den Webserver-Eigentümer.
 # chown web-server-user: web-server-group /etc/netboot/
 Webserver-Benutzer Steht für den Benutzer, der Eigentümer des Webserver-Prozesses ist.
 Webserver-Gruppe Steht für die Gruppe, die Eigentümer des Webserver-Prozesses ist.
- 5 Beenden Sie den Superuser-Status. # exit
- 6 Nehmen Sie die Benutzerrolle des Webserver-Eigentümers an.
- 7 Erzeugen Sie in /etc/netboot ein Unterverzeichnis für den Client.

mkdir -p /etc/netboot/net-ip/client-ID

- p	Weist den Befehl mkdir an, alle erforderlichen übergeordneten Verzeichnisse für das gewünschte Verzeichnis zu erzeugen.
(Optional) Netz-IP	Die Netzwerk-IP-Adresse des Teilnetzes, in dem sich der Client befindet.
(Optional) Client-ID	Gibt die Client-ID an. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. Das <i>Client-ID</i> -Verzeichnis muss ein Unterverzeichnis des <i>Netz-IP</i> -Verzeichnisses sein.

Setzen Sie die Berechtigungen für jedes Verzeichnis in der /etc/netboot-Hierarchie auf 700. 8 # chmod 700 /etc/netboot/dir-name

Verz-Name Steht für den Namen eines Verzeichnisses in der /etc/netboot-Hierarchie.

Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server Beispiel 12–4

Das folgende Beispiel zeigt, wie die /etc/netboot-Hierarchie für den Client 010003BA152A42 im Teilnetz 192.168.198.0 erzeugt wird. In diesem Beispiel sind der Benutzer nobody und die Gruppe admin Eigentümer des Webserver-Prozesses.

Die Befehle in diesem Beispiel führen folgende Aktionen durch:

- Erzeugen Sie das Verzeichnis /etc/netboot.
- Setzen Sie die Berechtigungen für das Verzeichnis /etc/netboot auf 700.
- Setzen Sie den Besitzer des Webserver-Prozesses als Besitzer des Verzeichnisses /etc/netboot.
- Annehmen der Benutzerrolle des Webserver-Benutzers.
- Erzeugen Sie ein Unterverzeichnis in /etc/netboot mit dem Namen des Teilnetzes (192.168.198.0).
- Erzeugen eines Unterverzeichnisses im Teilnetzverzeichnis und benennen nach der Client-ID.
- Setzen Sie die Berechtigungen für die Unterverzeichnisse von /etc/netboot auf 700.

```
# cd /
# mkdir /etc/netboot/
# chmod 700 /etc/netboot
# chown nobody:admin /etc/netboot
# exit
server# su nobody
Password:
nobody# mkdir -p /etc/netboot/192.168.198.0/010003BA152A42
nobody# chmod 700 /etc/netboot/192.168.198.0
nobody# chmod 700 /etc/netboot/192.168.198.0/010003BA152A42
```

Fortsetzen der WAN-Boot-Installation Weitere

Informationen:

Nachdem Sie die /etc/netboot-Hierarchie erstellt haben, müssen Sie das WAN-Boot-CGI-Programm auf den WAN-Boot-Server kopieren. Dieser Schritt ist unter "Kopieren des WAN-Boot-CGI-Programms auf den WAN-Boot-Server" auf Seite 189 beschrieben.

Siehe auch For detailed planning information about how to design the /etc/netboot hierarchy, see "Speichern von Konfigurations- und Sicherheitsinformationen in der /etc/netboot-Hierarchie" auf Seite 164.

Kopieren des WAN-Boot-CGI-Programms auf den WAN-Boot-Server

Das Programm wanboot - cgi erzeugt die Datenströme, mit welchen die folgenden Dateien vom WAN-Boot-Server zum Client übertragen werden.

- wanboot-Programm
- WAN-Boot-Dateisystem
- WAN-Boot-Miniroot

Das Programm wanboot - cgi wird zusammen mit aktuelle Solaris-Release auf dem System installiert. Damit der WAN-Boot-Server auf dieses Programm zugreifen kann, kopieren Sie es in das Verzeichnis cgi-bin des WAN-Boot-Servers.

So kopieren Sie das Programm wanboot - cgi auf den WAN-Boot-Server

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim WAN-Boot-Server an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Kopieren Sie das Programm wanboot - cgi auf den WAN-Boot-Server.

cp /usr/lib/inet/wanboot/wanboot-cgi /WAN-server-root/cgi-bin/wanboot-cgi

/WAN-Server-Root Steht für das Root-Verzeichnis der Webserver-Software auf dem WAN-Boot-Server.

3 Setzen Sie auf dem WAN-Boot-Server die Berechtigungen f
ür das CGI-Programm auf 755. # chmod 755 /WAN-server-root/cgi-bin/wanboot-cgi

Weitere Fortsetzen der WAN-Boot-Installation

Informationen:

Nachdem Sie das WAN-Boot-CGI-Programm auf den WAN-Boot-Server kopiert haben, können Sie wahlweise einen Protokollserver einrichten. Die Vorgehensweise dazu ist unter "(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190 beschrieben. Wenn Sie keinen eigenen Protokollserver einrichten möchten, lesen Sie bitte in Abschnitt "(Optional) Schützen der Daten mit HTTPS" auf Seite 191 weiter. Dort erfahren Sie, wie Sie die Sicherheitsmerkmale einer WAN-Boot-Installation einrichten.

Siehe auch

Einen Überblick über das wanboot - cgi-Programm erhalten Sie im Abschnitt "Was ist WAN-Boot?" auf Seite 151.

(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver

Standardmäßig werden alle Protokollmeldungen beim WAN-Boot auf dem Clientsystem angezeigt, um eine schnelle Fehlerdiagnose bei Installationsproblemen zu ermöglichen.

Wenn die Boot- und Installationsprotokollmeldungen auf einem anderen System als dem Client aufgezeichnet werden sollen, müssen Sie einen Protokollserver (Logging-Server) einrichten. Soll der Protokollserver bei der Installation mit HTTPS arbeiten, muss der WAN-Boot-Server als Protokollserver konfiguriert werden.

Zum Konfigurieren des Protokollservers führen Sie die nachfolgenden Schritte durch.

1 Kopieren Sie das Skript bootlog-cgi in das CGI-Skriptverzeichnis des Protokollservers.

<pre># cp /usr/lib/inet/wanboot/boot</pre>	log-cgi \	log-server-root/ cgi-bin
Protokollserver-Root/cgi-bin	Steht für da	s Verzeichnis cgi-bin im
	Webserver-	Verzeichnis des Protokollservers.

2 Setzen Sie die Berechtigungen für das Skript bootlog-cgi auf 755.

chmod 755 log-server-root/cgi-bin/bootlog-cgi

3 Setzen Sie den Wert für den Parameter boot_logger in der Datei wanboot.conf. Geben Sie in der Datei wanboot.conf die URL des Skripts bootlog-cgi auf dem Protokollserver an.

Weitere Informationen zum Einstellen der Parameter in der Datei wanboot . conf finden Sie in "So erzeugen Sie die Datei wanboot . conf" auf Seite 209.

Während der Installation werden im Verzeichnis /tmp des Protokollservers Boot- und Installationsprotokollmeldungen aufgezeichnet. Die Protokolldatei erhält den Namen bootlog. *Host-Name*, wobei *Host-Name* der Host-Name des Clients ist.

Beispiel 12–5 Konfiguration eines Protokollservers für die WAN-Boot-Installation per HTTPS

Im folgenden Beispiel wird der WAN-Boot-Server als Protokollserver konfiguriert.



Weitere Informationen:

ere Fortsetzen der WAN-Boot-Installation

Nachdem Sie den Protokollserver eingerichtet haben, können Sie die WAN-Boot-Installation wahlweise so einrichten, dass digitale Zertifikate und Sicherheitsschlüssel verwendet werden. Die Einrichtung der Sicherheitsmerkmale einer WAN-Boot-Installation ist in "(Optional) Schützen der Daten mit HTTPS" auf Seite 191 beschrieben.

(Optional) Schützen der Daten mit HTTPS

Zum Schutz Ihrer Daten während der Übertragung vom WAN-Boot-Server auf den Client können Sie HTTPS (HTTP over Secure Sockets Layer) einsetzen. Wenn Sie die in "Sichere WAN-Boot-Installationskonfiguration" auf Seite 158 beschriebene sicherere Installationskonfiguration verwenden möchten, müssen Sie HTTPS auf Ihrem Webserver aktivieren.

Wenn Sie keine sichere WAN-Boot-Installation durchführen möchten, können Sie die Schritte in diesem Abschnitt überspringen. Fahren Sie in diesem Fall mit dem Abschnitt "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation" auf Seite 197 fort.

Führen Sie die folgenden Schritte durch, um die Webserver-Software auf dem WAN-Boot-Server auf die Verwendung von HTTPS einzustellen:

Aktivieren Sie die SSL-Unterstützung in Ihrer Webserver-Software.

Die Vorgehensweise zum Aktivieren der SSL-Unterstützung und der Client-Authentifizierung ist vom jeweiligen Webserver abhängig. Dieses Dokument enthält keine Anweisungen zum Aktivieren dieser Sicherheitsfunktionen auf dem Webserver. Die entsprechenden Informationen entnehmen Sie bitte der folgenden Dokumentation:

- Informationen zum Aktivieren von SSL auf den Webservern SunONE und iPlanet finden Sie in den Sun ONE- und iPlanet-Dokumentationsreihen unter http://docs.sun.com.
- Informationen zum Aktivieren von SSL auf dem Webserver Apache finden Sie im Apache Dokumentationsprojekt unter http://httpd.apache.org/docs-project/.
- Informationen zu hier nicht aufgeführter Webserver-Software entnehmen Sie bitte der Dokumentation zu Ihrer Webserver-Software.
- Installieren Sie digitale Zertifikate auf dem WAN-Boot-Server.

In "(Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung" auf Seite 192 erhalten Sie Informationen über die Verwendung von digitalen Zertifikaten mit WAN-Boot.. • Stellen Sie dem Client ein vertrauenswürdiges Zertifikat zur Verfügung.

In "(Optional) So verwenden Sie digitale Zertifikate für die Server- und Client-Authentifizierung" auf Seite 192 finden Sie Anweisungen zum Erstellen vertrauenswürdiger Zertifikate.

- Erzeugen Sie einen Hashing- und einen Chiffrierschlüssel.
 Anweisungen zum Generieren von Schlüsseln finden Sie in "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195.
- (Optional) Aktivieren Sie die Unterstützung für die Client-Authentifizierung in der Konfiguration der Webserver-Software.

Anweisungen hierzu entnehmen Sie bitte der Dokumentation zu Ihrem Webserver.

Dieser Abschnitt beschreibt, wie Sie digitale Zertifikate und Schlüssel bei Ihrer WAN-Boot-Installation verwenden können.

(Optional) So verwenden Sie digitale Zertifikate f ür die Server- und Client-Authentifizierung

Das WAN-Boot-Installationsverfahren erlaubt den Einsatz von PKCS#12-Dateien für eine Installation über HTTPS mit Server- oder sowohl Server- als auch Client-Authentifizierung. Die Voraussetzungen und Richtlinien für die Verwendung von PKCS#12-Dateien lesen Sie bitte unter "Voraussetzungen für digitale Zertifikate" auf Seite 168 nach.

Führen Sie folgende Schritte durch, um eine PKCS#12-Datei in der WAN-Boot-Installation zu verwenden:

- Teilen Sie die PKCS#12-Datei in einen privaten SSL-Schlüssel und ein vertrauenswürdiges Zertifikat auf.
- Fügen Sie das vertrauenswürdige Zertifikat in die Datei truststore des Clients in der /etc/netboot-Hierarchie ein. Dieses Zertifikat weist den Client an, den Server als vertrauenswürdig zu akzeptieren.
- (Optional) Fügen Sie den Inhalt der Datei des privaten SSL-Schlüssels in die Datei keystore des Clients in der /etc/netboot-Hierarchie ein.

Der Befehl wanbootutil stellt Optionen zum Durchführen der Schritte in der vorigen Liste zur Verfügung.

Wenn Sie keine sichere WAN-Boot-Installation durchführen möchten, können Sie dieses Verfahren überspringen. Fahren Sie in diesem Fall mit dem Abschnitt "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation" auf Seite 197 fort. Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat und einen privaten Schlüssel für den Client zu erstellen.

Bevor Sie Erzeugen Sie, bevor Sie eine PKCS#12-Datei aufteilen, geeignete Unterverzeichnisse in der /etc/netboot-Hierarchie auf dem WAN-Boot-Server.

- Einen Überblick über die /etc/netboot-Hierarchie finden Sie unter "Speichern von Konfigurations- und Sicherheitsinformationen in der /etc/netboot-Hierarchie" auf Seite 164.
- Anweisungen zum Erstellen der /etc/netboot-Hierarchie finden Sie unter "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186.
- 1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.
- 2 Extrahieren Sie das vertrauenswürdige Zertifikat aus der PKCS#12-Datei. Fügen Sie das Zertifikat in die Datei truststore des Clients in der /etc/netboot-Hierarchie ein.

wanbootutil p12split -i p12cert \
-t /etc/netboot/net-ip/client-ID/truststore

p12split

Option für den Befehl wanbootutil, die bewirkt, dass eine PKCS#12-Datei in separate Dateien für den privaten Schlüssel und das Zertifikat aufgeteilt wird.

-i pl2cert

Steht für den Namen der aufzuteilenden PKCS#12-Datei.

- -t/etc/netboot/ Netz-IP/Client-ID/truststore Fügt das Zertifikat in die Datei truststore des Clients ein. Netz-IP ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.
- 3 (Optional) Entscheiden Sie, ob Sie mit Client-Authentifizierung arbeiten möchten.
 - Wenn nein, fahren Sie mit dem Schritt "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195 fort.
 - Wenn ja, fahren Sie mit den nachfolgenden Schritten fort.
 - a. Fügen Sie das Client-Zertifikat in die Datei certstore des Clients ein.

```
# wanbootutil pl2split -i pl2cert -c \
/etc/netboot/net-ip/client-ID/certstore -k keyfile
```

p12split

Option für den Befehl wanbootutil, die bewirkt, dass eine PKCS#12-Datei in separate Dateien für den privaten Schlüssel und das Zertifikat aufgeteilt wird.

```
-i p12cert
```

Steht für den Namen der aufzuteilenden PKCS#12-Datei.

-c /etc/netboot/*Netz-IP/Client-ID*/certstore

Fügt das Client-Zertifikat in die Datei certstore des Clients ein. *Netz-IP* ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. *Client-ID* kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.

-k Schlüsseldatei

Steht für den Namen des privaten SSL-Schlüssels des Clients, der aus der aufgeteilten PKCS#12-Datei generiert werden soll.

b. Fügen Sie den privaten Schlüssel in die keystore-Datei des Clients ein.

```
# wanbootutil keymgmt -i -k keyfile \
-s /etc/netboot/net-ip/client-ID/keystore -o type=rsa
```

keymgmt -i

Fügt einen privaten SSL-Schlüssel in die Datei keystore des Clients ein.

-k Schlüsseldatei

Steht für den Namen der im vorigen Schritt erzeugten Schlüsseldatei des Clients.

- -s /etc/netboot/*Netz-IP/Client-ID*/keystore Gibt den Pfad zur Datei keystore des Clients an.
- -o type=rsa Legt den Schlüsseltyp als RSA fest

Beispiel 12–6 Generieren vertrauenswürdiger Zertifikate für die Server-Authentifizierung

In folgendem Beispiel wird der Client 010003BA152A42 im Teilnetz 192.168.198.0 unter Verwendung einer PKCS#12-Datei installiert. Dabei wird aus einer PKCS#12-Datei namens client.p12 ein Zertifikat extrahiert. Anschließend speichert der Befehl den Inhalt des vertrauenswürdigen Zertifikats in der Datei truststore des Clients.

Bevor Sie diese Befehle ausführen, müssen Sie die Benutzerrolle des Webserver-Benutzers annehmen. In diesem Beispiel die Benutzerrolle nobody.

```
server# su nobody
Password:
nobody# wanbootutil p12split -i client.p12 \
-t /etc/netboot/192.168.198.0/010003BA152A42/truststore
nobody# chmod 600 /etc/netboot/192.168.198.0/010003BA152A42/truststore
```

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie ein digitales Zertifikat erstellt haben, erzeugen Sie einen Hashing- und einen Chiffrierschlüssel. Die Vorgehensweise dazu ist in "(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel" auf Seite 195 beschrieben.

Siehe auch Nähere Informationen zum Erstellen von vertrauenswürdigen Zertifikaten finden Sie auf der Manpage wanbootutil(1M).

(Optional) So erzeugen Sie einen Hashing- und einen Chiffrierschlüssel

Wenn Sie Ihre Daten mit HTTPS übertragen möchten, müssen Sie einen HMAC SHA1-Hashing-Schlüssel und einen Chiffrierschlüssel (Verschlüsselung) erzeugen. Falls Sie beabsichtigen, die Installation über ein halbprivates Netzwerk vorzunehmen, können Sie sich auch gegen eine Verschlüsselung der Installationsdaten entscheiden. Mit einem HMAC SHA1-Hashing-Schlüssel kann die Integrität des wanboot-Programms überprüft werden.

Mit dem Befehl wanbootutil keygen können Sie diese Schlüssel generieren und im gewünschten /etc/netboot-Verzeichnis speichern.

Wenn Sie keine sichere WAN-Boot-Installation durchführen möchten, können Sie dieses Verfahren überspringen. Fahren Sie in diesem Fall mit dem Abschnitt "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation" auf Seite 197 fort.

Gehen Sie folgendermaßen vor, um einen Hashing-Schlüssel und einen Chiffrierschlüssel zu erzeugen.

- 1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.
- 2 Erzeugen Sie den HMAC SHA1-Masterschlüssel.

wanbootutil keygen -m
keygen -m
Erzeugt den HMAC SHA1-Masterschlüssel für den WAN-Boot-Server.

3 Erzeugen Sie aus dem Masterschlüssel den HMAC SHA1-Hashing-Schlüssel für den Client.

<pre># wanbootutil keygen -c -o [net=net-ip,{cid=client-ID,}]type=sha1</pre>		
- C	Generiert den Hashing-Schlüssel für den Client aus dem Masterschlüssel.	
- 0	Bedeutet, dass dem Befehl wanbootutil keygen weitere Optionen übergeben werden.	
(Optional) net= <i>Nezt-IP</i>	Gibt die IP-Adresse des Teilnetzes an, in dem sich der Client befindet. Wenn Sie die Option net nicht angeben, wird der Schlüssel in der Datei /etc/netboot/keystore gespeichert und steht allen WAN-Boot-Clients zur Verfügung.	
(Optional) cid= <i>Client-ID</i>	Gibt die Client-ID an. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID	

sein. Der Option cid muss ein gültiger net=-Wert vorangestellt werden. Wenn Sie die Option cid nicht zusammen mit net angeben, wird der Schlüssel in der Datei /etc/netboot/*Netz-IP*/keystore gespeichert. Dieser Schlüssel steht allen WAN-Boot-Clients im Teilnetz *Netz-IP* zur Verfügung.

type=sha1Weist das Dienstprogramm wanbootutil keygen an, einenHMAC SHA1-Hashing-Schlüssel für den Client zu erzeugen.

4 Entscheiden Sie, ob ein Chiffrierschlüssel für den Client generiert werden soll.

Einen Chiffrierschlüssel, also eine Verschlüsselung, brauchen Sie dann, wenn Sie eine WAN-Boot-Installation per HTTPS durchführen möchten. Bevor der Client eine HTTPS-Verbindung zum WAN-Boot-Server herstellt, überträgt der WAN-Boot-Server verschlüsselte Daten und Informationen an den Client. Mithilfe des Chiffrierschlüssels kann der Client diese Informationen entschlüsseln und bei der Installation auf sie zugreifen.

- Wenn Sie eine sicherere WAN-Installation per HTTPS mit Server-Authentifizierung durchführen möchten, fahren Sie mit dem nächsten Schritt fort.
- Wenn nur die Integrität des wanboot-Programms überprüft werden soll, benötigen Sie keine Verschlüsselung. Fahren Sie in diesem Fall mit Schritt 6 fort.

5 Chiffrierschlüssel für den Client erzeugen

<pre># wanbootutil keygen -c -o [net=net-ip,{cid=client-ID,}]type=key-type</pre>		
- C	Erzeugt den Chiffrierschlüssel für den Client.	
- 0	Bedeutet, dass dem Befehl wanbootutil keygen weitere Optionen übergeben werden.	
(Optional) net= <i>Nezt-IP</i>	Gibt die Netzwerk-IP-Adresse des Clients an. Wenn Sie die Option net nicht angeben, wird der Schlüssel in der Datei /etc/netboot/keystore gespeichert und steht allen WAN-Boot-Clients zur Verfügung.	
(Optional) cid= <i>Client-ID</i>	Gibt die Client-ID an. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. Der Option cid muss ein gültiger net=-Wert vorangestellt werden. Wenn Sie die Option cid nicht zusammen mit net angeben, wird der Schlüssel in der Datei /etc/netboot/ <i>Netz-IP</i> /keystore gespeichert. Dieser Schlüssel steht allen WAN-Boot-Clients im Teilnetz <i>Netz-IP</i> zur Verfügung.	
type= <i>Schlüsseltyp</i>	Weist das Dienstprogramm wanbootutil keygen an, einen Chiffrierschlüssel für den Client zu erzeugen. <i>Schlüsseltyp</i> kann	

den Wert 3des oder aes annehmen.

6 Installieren Sie die Schlüssel auf dem Clientsystem.

Anweisungen zur Installation der Schlüssel auf dem Client finden Sie unter "Installation von Schlüsseln auf dem Client" auf Seite 218.

Beispiel 12–7 Erzeugen der erforderlichen Schlüssel für die WAN-Boot-Installation per HTTPS

In folgendem Beispiel wird ein HMAC SHA1-Masterschlüssel für den WAN-Boot-Server generiert. Außerdem wird in diesem Beispiel ein HMAC SHA1-Hashing-Schlüssel und eine 3DES-Verschlüsselung für den Client 010003BA152A42 im Teilnetz 192.168.198.0 generiert.

Bevor Sie diese Befehle ausführen, müssen Sie die Benutzerrolle des Webserver-Benutzers annehmen. In diesem Beispiel die Benutzerrolle nobody.

server# su nobody
Password:
nobody# wanbootutil keygen -m
nobody# wanbootutil keygen -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
nobody# wanbootutil keygen -c -o net=192.168.198.0,cid=010003BA152A42,type=3des

Weitere
Informationen:Fortsetzen der WAN-Boot-InstallationNachdem Sie einen Hashing- und einen Chiffrierschlüssel erzeugt haben, müssen Sie die
Installationsdateien erzeugen. Die Anleitung hierzu finden Sie in "Erzeugen der Dateien für die
benutzerdefinierte JumpStart-Installation" auf Seite 197.Siehe auchEinen Überblick über Hashing- und Chiffrierschlüssel finden Sie in "Schutz der Daten während

einer WAN-Boot-Installation" auf Seite 156.

Nähere Informationen zum Erzeugen von Hashing- und Chiffrierschlüsseln finden Sie auf der Manpage wanbootutil(1M).

Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation

WAN-Boot installiert mithilfe des benutzerdefinierten JumpStart-Verfahrens ein Solaris Flash-Archiv auf dem Client. Die benutzerdefinierte JumpStart-Installation bietet eine Befehlszeilenschnittstelle, mit der Sie automatisch auf mehreren Systemen eine Installation ausführen können, und zwar basierend auf von Ihnen erstellten Profilen. Diese Profile definieren die spezifischen Software-Installationsanforderungen. Außerdem können Sie für die vor und nach der Installation erforderlichen Schritte Shell-Skripte verwenden. Dabei geben Sie selbst an, welche Profile und Skripte für die Installation bzw. das Upgrade verwendet werden sollen. Die Installation bzw. das Upgrade mit der benutzerdefinierten JumpStart-Installation wird dann auf der Grundlage der von Ihnen ausgewählten Profile und Skripte ausgeführt. Außerdem können Sie eine sysidcfg-Datei verwenden und die Konfigurationsinformationen vorkonfigurieren, so dass die benutzerdefinierte JumpStart-Installation völlig ohne Benutzereingriff abläuft.

Führen Sie die folgenden Schritte durch, um JumpStart-Dateien für eine WAN-Boot-Installation vorzubereiten.

- "So erzeugen Sie das Solaris Flash-Archiv" auf Seite 198
- "So erzeugen Sie die Datei sysidcfg" auf Seite 200
- "So erstellen Sie die Datei rules" auf Seite 203
- "So erstellen Sie das Profil" auf Seite 201
- "(Optional) Erzeugen von Begin- und Finish-Skripten" auf Seite 206

Ausführliche Informationen zur benutzerdefinierten JumpStart-Installation finden Sie in Kapitel 2, "Benutzerdefinierte JumpStart-Installation (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationszenarien.

So erzeugen Sie das Solaris Flash-Archiv

Die Installationsfunktion Solaris Flash bietet die Möglichkeit, eine Modellinstallation von Solaris auf einem einzigen System, dem Master-System, anzulegen. Sie können dann ein Solaris Flash-Archiv erzeugen, das ein genaues Abbild des Master-Systems ist. Das Solaris Flash-Archiv können Sie auf anderen Systemen im Netzwerk installieren, wodurch Klonsysteme erzeugt werden.

In diesem Abschnitt erfahren Sie, wie Sie ein Solaris Flash-Archiv erzeugen.

Bevor Sie beginnen

- ie Bevor Sie ein Solaris Flash-Archiv erzeugen, müssen Sie das Master-System einrichten.
 - Informationen zur Installation eines Mastersystems finden Sie unter "Installation des Mastersystems" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).
 - Ausführliche Informationen zu Solaris Flash-Archiven finden Sie in Kapitel 1, "Solaris Flash (Übersicht)" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).
 - Probleme mit Dateigrößen:

Lesen Sie bitte in der Dokumentation Ihres Webservers nach, ob die Software Dateien in der Größe eines Solaris Flash-Archivs übertragen kann.

- Lesen Sie bitte in der Dokumentation Ihres Webservers nach, ob die Software Dateien in der Größe eines Solaris Flash-Archivs übertragen kann.
- Der Befehl flarcreate übt keinerlei Größenbeschränkungen mehr auf einzelne Dateien aus. Sie können ein Solaris Flash-Archiv erstellen, dass einzelne Dateien enthalten kann, die größer als 4 GB sind.

Weitere Informationen finden Sie unter "Erstellen eines Archivs, das große Dateien enthält" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).

1 Starten Sie das Master-System.

Bringen Sie das Master-System in einen so weit wie möglich inaktiven Zustand. Versetzen Sie das System nach Möglichkeit in den Einzelbenutzermodus. Wenn das nicht möglich ist, fahren Sie alle Anwendungen, die archiviert werden sollen, sowie alle Anwendungen, die die Betriebssystemressourcen stark beanspruchen, herunter.

2 Legen Sie das Archiv mit dem Befehl flarcreate an.

flarcreate -n name [optional-parameters] document-root/flash/filename

Name	Der Name, den Sie dem Archiv geben. Der <i>Name</i> , den Sie angeben, ist der Wert des Schlüsselworts content_name.
optionale_Parameter	Es stehen verschiedene Optionen für den Befehl flarcreate zur Verfügung, die Ihnen eine Anpassung des Solaris Flash-Archivs ermöglichen. Ausführliche Beschreibungen dieser Optionen finden Sie in Kapitel 6, "Solaris Flash (Referenz)" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).
Dokument-Root/flash	Der Pfad zum Solaris Flash-Unterverzeichnis im Dokument-Root-Verzeichnis des Installationsservers.

Dateiname Der Name der Archivdatei.

Um Speicherplatz zu sparen, können Sie das Archiv komprimieren, indem Sie dem Befehl flar create die Option - c übergeben. Ein komprimiertes Archiv kann jedoch die Leistung der WAN-Boot-Installation beeinträchtigen. Weitere Informationen über die Herstellung komprimierter Archive entnehmen Sie bitte der Manpage flarcreate(1M).

- Wenn das Archiv erfolgreich angelegt wird, gibt der Befehl flarcreate den Exit-Code 0 zurück.
- Wenn das Anlegen des Archivs fehlschlägt, gibt der Befehl flarcreate einen Exit-Code ungleich 0 zurück.

Beispiel 12–8 Erstellen eines Solaris Flash-Archivs für eine WAN-Boot-Installation

In diesem Beispiel erstellen Sie ein Solaris Flash-Archiv, indem Sie das WAN-Boot-Serversystem mit dem Rechnernamen wanserver klonen. Das Archiv erhält den Namen sol_10_sparc und wird 1:1 vom Master-System kopiert. Es stellt ein exaktes Duplikat des Master-Systems dar. Das fertige Archiv wird in sol_10_sparc.flar gespeichert. Sie speichern das Archiv im Unterverzeichnis flash/archives des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.

wanserver# flarcreate -n sol_10_sparc \
/opt/apache/htdocs/flash/archives/sol_10_sparc.flar

 Weitere Informationen:
 Fortsetzen der WAN-Boot-Installation

 Nachdem Sie das Solaris Flash-Archiv erstellt haben, richten Sie die vorkonfigurierten Client-Informationen in der Datei sysidcfg ein. Die dazugehörige Anleitung finden Sie in "So erzeugen Sie die Datei sysidcfg" auf Seite 200.

Siehe auch Ausführliche Anweisungen zum Erstellen eines Solaris Flash-Archivs finden Sie in Kapitel 3, "Erstellen von Solaris Flash-Archiven (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Flash-Archive (Erzeugung und Installation).

Der Befehl flarcreate ist darüber hinaus auf der Manpage flarcreate(1M) beschrieben.

So erzeugen Sie die Datei sysidcfg

In der Datei sysidcfg können Sie zum Vorkonfigurieren eines Systems eine Reihe von Schlüsselwörtern angeben.

Gehen Sie folgendermaßen vor, um die Datei sysidcfg zu erzeugen.

Bevor Sie Erzeugen Sie das Solaris Flash-Archiv. Eine ausführliche Anleitung finden Sie in "So erzeugen Sie das Solaris Flash-Archiv" auf Seite 198.

- 1 Erzeugen Sie auf dem Installationsserver in einem Texteditor eine Datei namens sysidcfg.
- 2 Geben Sie die gewünschten sysidcfg-Schlüsselwörter ein.

Für ausführliche Informationen zu den sysidcfg-Schlüsselwörtern schlagen Sie bitte im Abschnitt "Schlüsselwörter in der Datei sysidcfg" auf Seite 22 nach.

3 Speichern Sie die Datei sysidcfg in einem für den WAN-Boot-Server zugänglichen Verzeichnis. Speichern Sie die Datei in einem dieser Verzeichnisse:

- Wenn sich der WAN-Boot-Server und der Installationsserver auf demselben System befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.
- Wenn sich WAN-Boot-Server und Installationsserver auf unterschiedlichen Systemen befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem Installationsserver.

Beispiel 12-9 sysidcfg-Datei für die WAN-Boot-Installation

Im Folgenden sehen Sie eine sysidcfg-Beispieldatei für ein SPARC-System. Host-Name, IP-Adresse und Netzmaske dieses Systems wurden durch Bearbeitung des Naming Service vorkonfiguriert.

Weitere
Informationen:Fortsetzen der WAN-Boot-InstallationNachdem Sie die sysidcfg-Datei erstellt haben, erstellen Sie ein benutzerdefiniertes
JumpStart-Profil für den Client. Die dazugehörige Anleitung finden Sie in "So erstellen Sie das
Profil" auf Seite 201.

Siehe auch Ausführlichere Informationen über Schlüsselwörter und Werte für die Datei sysidcfg finden Sie in "Vorkonfiguration mit der Datei sysidcfg" auf Seite 18.

So erstellen Sie das Profil

Bei einem Profil handelt es sich um eine Textdatei, aus welcher das Programm für die benutzerdefinierte JumpStart-Installation entnimmt, wie die Solaris-Software auf einem System installiert werden soll. Ein Profil definiert Elemente der Installation, wie zum Beispiel die zu installierende Softwaregruppe. Ausführliche Informationen zum Erstellen von Profilen finden Sie unter "Erstellen eines Profils" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Gehen Sie folgendermaßen vor, um das Profil zu erstellen.

Bevor Sie Erstellen Sie die sysidcfg-Datei für den Client. Eine ausführliche Anleitung finden Sie in "So erzeugen Sie die Datei sysidcfg" auf Seite 200.

1 Erzeugen Sie auf dem Installationsserver eine Textdatei. Geben Sie der Datei einen aussagekräftigen Namen.

Stellen Sie sicher, dass der Name des Profils wiedergibt, wie Sie das Profil zum Installieren der Solaris-Software auf einem System einsetzen wollen. So können Sie zum Beispiel die Profile basic_install, eng_profile oder user_profile anlegen.

2 Fügen Sie Schlüsselwörter und Werte zu dem Profil hinzu.

Eine Liste der Profil-Schlüsselwörter finden Sie unter "Profilschlüsselwörter und -werte" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Bei Profilschlüsselwörtern und deren Werten wird zwischen Groß- und Kleinschreibung unterschieden.

3 Speichern Sie das Profil in einem für den WAN-Boot-Server zugänglichen Verzeichnis.

Speichern Sie das Profil in einem dieser Verzeichnisse:

- Wenn sich der WAN-Boot-Server und der Installationsserver auf demselben System befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.
- Wenn sich der WAN-Boot-Server und der Installationsserver auf unterschiedlichen Systemen befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem Installations-Server.

4 Stellen Sie sicher, dass root Eigentümer des Profils ist und dass die Berechtigungen auf 644 gesetzt sind.

5 (Optional) Testen Sie das Profil.

Weitere Informationen zum Testen von Profilen finden Sie unter "Testen eines Profils" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Beispiel 12–10 Abrufen eines Solaris Flash-Archivs von einem sicheren HTTP-Server

Das Profil in folgendem Beispiel sieht vor, dass das Programm für die benutzerdefinierte JumpStart-Installation das Solaris Flash-Archiv von einem sicheren HTTP-Server abruft.

<pre># profile keywords</pre>	profile values
#	
install_type	flash_install
archive_location	https://192.168.198.2/sol_10_sparc.flar
partitioning	explicit
filesys	c0t1d0s0 4000 /
filesys	c0tld0s1 512 swap
filesys	c0t1d0s7 free /export/home

In der folgenden Liste sind einige Schlüsselwörter und Werte aus diesem Beispiel beschrieben.

install_type	Das Profil installiert ein Solaris Flash-Archiv auf dem Klonsystem. Wie bei einer Erst- bzw. Neuinstallation werden alle Dateien überschrieben.
archive_location	Das komprimierte Solaris Flash-Archiv wird von einem sicheren HTTP-Server abgerufen.
partitioning	Mit dem Wert explicit legen Sie fest, dass die Dateisystem-Slices von den filesys-Schlüsselwörtern definiert werden. Die Größe von Root (/) ist von der Größe des Solaris Flash-Archivs abhängig. Der swap-Bereich wird auf c0tld0s1 angelegt und seine Größe nach Bedarf automatisch festgelegt. /export/home ist vom verbleibenden Speicherplatz abhängig. /export/home wird auf c0tld0s7 angelegt.

Weitere Fortsetzen der WAN-Boot-Installation

Informationen:

Nachdem Sie ein Profil erstellt haben, müssen Sie die Datei rules erstellen und überprüfen. Eine Anleitung dazu finden Sie in "So erstellen Sie die Datei rules" auf Seite 203.

Siehe auch Weitere Informationen zum Erstellen eines Profils finden Sie unter "Erstellen eines Profils" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

> Ausführliche Informationen zu Profil-Schlüsselwörtern und -werten finden Sie unter "Profilschlüsselwörter und -werte" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

So erstellen Sie die Datei rules

Bei der Datei rules handelt es sich um eine Textdatei, die für jede Gruppe von Systemen, auf welchen Solaris installiert werden soll, eine Regel enthält. Jede Regel charakterisiert eine

Gruppe von Systemen auf der Grundlage von einem oder mehreren Systemattributen. Jede Regel verknüpft außerdem jede Gruppe mit einem Profil. Ein Profil ist eine Textdatei, in der definiert ist, wie die Solaris-Software auf den Systemen in der Gruppe installiert werden soll. Die folgende Regel legt zum Beispiel fest, dass das JumpStart-Programm die Informationen im Profil basic_prof zur Installation aller Systeme der Plattformgruppe sun4u verwenden soll.

karch sun4u - basic_prof -

Die Datei rules dient zum Generieren der Datei rules.ok, die für benutzerdefinierte JumpStart-Installationen erforderlich ist.

Ausführliche Informationen zum Erstellen einer rules-Datei finden Sie unter "Erstellen der Datei rules" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Gehen Sie folgendermaßen vor, um die Datei rules zu erzeugen.

Bevor Sie
beginnenErstellen Sie das Profil für den Client. Eine ausführliche Anleitung finden Sie in "So erstellen Sie
das Profil" auf Seite 201.

- 1 Erzeugen Sie auf dem Installationsserver eine Textdatei namens rules.
- 2 Fügen Sie für jede Gruppe von Systemen, die eingerichtet werden sollen, eine Regel in die Datei rules ein.

Ausführliche Informationen zum Erstellen einer rules-Datei finden Sie unter "Erstellen der Datei rules" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

- 3 Speichern Sie die Datei rules auf dem Installationsserver.
- 4 Validieren Sie die rules-Datei.
 - \$./check -p path -r file-name
 - p PfadValidiert die Datei rules unter Verwendung des Skripts check aus dem
Abbild der Solaris-Software anstelle des Skripts check auf dem System, mit
dem Sie arbeiten. Pfad ist der Pfad zu einem Abbild auf einer lokalen
Festplatte oder zu einer eingehängten Solaris-DVD oder Solaris Software-1
CD.

Verwenden Sie diese Option, um die neueste Version von check auszuführen, wenn auf dem System eine frühere Version von Solaris läuft.

- r *Dateiname* Gibt eine andere rules-Datei als die mit dem Namen rules an. Mit dieser Option können Sie die Gültigkeit einer Regel testen, bevor Sie die Regel in die Datei rules aufnehmen. Während das Skript check ausgeführt wird, werden Meldungen zur Validierung der Datei rules und der einzelnen Profile ausgegeben. Wenn keine Fehler auftreten, gibt das Skript Folgendes aus: The custom JumpStart configuration is ok. Das Skript check erzeugt die Datei rules.ok.

- 5 Speichern Sie die Datei rules.ok in einem für den WAN-Boot-Server zugänglichen Verzeichnis. Speichern Sie die Datei in einem dieser Verzeichnisse:
 - Wenn sich der WAN-Boot-Server und der Installationsserver auf demselben System befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.
 - Wenn sich der WAN-Boot-Server und der Installationsserver auf unterschiedlichen Systemen befinden, speichern Sie die Datei im Unterverzeichnis flash des Dokument-Root-Verzeichnisses auf dem Installations-Server.
- 6 Stellen Sie sicher, dass root Eigentümer der Datei rules.ok ist und dass die Berechtigungen auf 644 gesetzt sind.

Beispiel 12–11 Erstellen und Überprüfen der rules-Datei

Aus der Datei rules wählen die Programme für die benutzerdefinierte JumpStart-Installation das richtige Profil für das System wanclient-1 aus. Erzeugen Sie eine Textdatei namens rules. Fügen Sie dann Schlüsselwörter und Werte in diese Datei ein.

Die IP-Adresse des Clientsystems lautet 192.168.198.210, die Netzmaske 255.255.255.0. Mit dem Schlüsselwort network geben Sie an, welches Profil die Programme für die benutzerdefinierte JumpStart-Installation zur Installation des Clients verwenden sollen.

network 192.168.198.0 - wanclient_prof -

Die rules-Datei legt damit fest, dass die Programme für die benutzerdefinierte JumpStart-Installation das Profil wanclient_prof verwenden sollen, um die aktuelle Solaris-Release-Software auf dem Client zu installieren.

Nennen Sie diese Datei wanclient_rule.

Wenn Sie das Profil und die rules-Datei erzeugt haben, führen Sie das check-Skript aus, um die Gültigkeit der Dateien zu überprüfen.

wanserver# ./check -r wanclient_rule

Wenn das Skript check keine Fehler findet, erstellt es die Datei rules.ok.

Speichern Sie die Datei rules.ok im Verzeichnis /opt/apache/htdocs/flash/.

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie die Datei rules.ok erstellt haben, können Sie wahlweise Begin- und Finish-Skripten für Ihre Installation einrichten. Eine Anleitung hierzu finden Sie in "(Optional) Erzeugen von Begin- und Finish-Skripten" auf Seite 206.

Wenn Sie keine Begin- und Finish-Skripten einrichten möchten, setzen Sie die WAN-Boot-Installation mit dem Schritt "Erstellen der Konfigurationsdateien" auf Seite 207 fort.

Siehe auch Ausführliche Informationen zum Erstellen einer rules-Datei finden Sie unter "Erstellen der Datei rules" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Ausführliche Informationen zu den Schlüsselwörtern und Werten der rules-Datei finden Sie unter "Rule-Schlüsselwörter und -Werte" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

(Optional) Erzeugen von Begin- und Finish-Skripten

Begin- und Finish-Skripten sind benutzerdefinierte Bourne-Shell-Skripten, die Sie in der Datei rules angeben. Ein Begin-Skript führt bestimmte Aufgaben aus, bevor die Solaris-Software auf einem System installiert wird. Ein Finish-Skript führt bestimmte Aufgaben nach der Installation der Solaris-Software auf einem System auf, jedoch bevor das System erneut gebootet wird. Sie können diese Skripten nur verwenden, wenn Sie die Solaris-Software mit dem benutzerdefinierten JumpStart-Installationsverfahren installieren.

Mit Begin-Skripten lassen sich abgeleitete Profile erstellen. Finish-Skripten dienen zur Durchführung verschiedenster Vorgänge nach der Installation. Hierzu gehört das Hinzufügen von Dateien, Packages, Patches oder zusätzlicher Software.

Begin- und Finish-Skripten müssen in demselben Verzeichnis auf dem Installationsserver gespeichert werden wie die Dateien sysidcfg, rules.ok und die Profildateien.

- Weitere Informationen zum Erstellen von Begin-Skripten finden Sie unter "Erstellen von Begin-Skripten" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.
- Weitere Informationen zum Erstellen von Finish-Skripten finden Sie unter "Erstellen von Finish-Skripten" in Oracle Solaris 10 9/10 Installationshandbuch: Benutzerdefinierte JumpStart-Installation und komplexe Installationsszenarien.

Setzen Sie die Vorbereitung Ihrer WAN-Boot-Installation mit dem Schritt "Erstellen der Konfigurationsdateien" auf Seite 207 fort.

Erstellen der Konfigurationsdateien

Zur Ermittlung der Adressen der für die WAN-Boot-Installation benötigten Daten und Dateien stützt sich WAN-Boot auf folgende Dateien:

- Systemkonfigurationsdatei (system.conf)
- wanboot.conf

In diesem Abschnitt erfahren Sie, wie diese beiden Dateien erzeugt und gespeichert werden.

So erzeugen Sie die Systemkonfigurationsdatei

Mit der Systemkonfigurationsdatei leiten Sie die WAN-Boot-Installationsprogramme zu den folgenden Dateien:

- sysidcfg
- rules.ok
- Profil für die benutzerdefinierte JumpStart-Installation

Die Informationen für Installation und Konfiguration der Clients entnimmt WAN-Boot aus den Dateien, auf die in der Systemkonfigurationsdatei verwiesen wird.

Bei der Systemkonfigurationsdatei handelt es sich um eine Normaltextdatei, die nach diesem Muster formatiert sein muss:

setting=value

Führen Sie die nachfolgenden Schritte durch, um die WAN-Installationsprogramme mithilfe einer Systemkonfigurationsdatei zu den Dateien sysidcfg, rules.ok und den Profildateien zu leiten.

- Bevor Sie
beginnenBevor Sie die Systemkonfigurationsdatei erzeugen, müssen Sie zunächst die
Installationsdateien für Ihre WAN-Boot-Installation erstellen. Eine ausführliche Anleitung
hierzu finden Sie in "Erzeugen der Dateien für die benutzerdefinierte JumpStart-Installation"
auf Seite 197.
 - 1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.
 - 2 Erzeugen Sie eine Textdatei. Geben Sie der Datei einen aussagekräftigen Namen, z. B. sys-conf.s10–sparc.
 - 3 Fügen Sie die folgenden Einträge zur Systemkonfigurationsdatei hinzu.

SsysidCF=sysidcfg-Datei-URL

Diese Einstellung verweist auf das Verzeichnis flash auf dem Installationsserver, in dem sich die Datei sysidcfg befindet. Vergewissern Sie sich, dass diese URL mit dem Pfad zur Datei sysidcfg übereinstimmt, die Sie in "So erzeugen Sie die Datei sysidcfg" auf Seite 200 erzeugt haben.

Für WAN-Installationen per HTTPS ist der Wert auf eine gültige HTTPS-URL zu setzen.

SjumpsCF=jumpstart-Dateien-URL

Diese Einstellung zeigt auf das Solaris Flash-Verzeichnis auf dem Installationsserver, das die Datei rules.ok, die Profildatei sowie Begin- und Finish-Skripten enthält. Diese URL muss mit dem Pfad zu den JumpStart-Dateien übereinstimmen, die Sie in "So erstellen Sie das Profil" auf Seite 201 und "So erstellen Sie die Datei rules" auf Seite 203 erzeugt haben.

Für WAN-Installationen per HTTPS ist der Wert auf eine gültige HTTPS-URL zu setzen.

4 Speichern Sie diese Datei in einem für den WAN-Boot-Server zugänglichen Verzeichnis.

Zur Erleichterung der Administration bietet es sich an, die Datei im entsprechenden Client-Verzeichnis in der /etc/netboot-Hierarchie auf dem WAN-Boot-Server zu speichern.

5 Setzen Sie die Berechtigungen für die Systemkonfigurationsdatei auf 600.

# chmod 600 /path	/system-conf-file
Pfad	Steht für den Pfad zum Verzeichnis, das die Systemkonfigurationsdatei enthält.
Sys_konf_datei	Gibt den Namen der Systemkonfigurationsdatei an.

Beispiel 12–12 Systemkonfigurationsdatei für die WAN-Boot-Installation per HTTPS

Im folgenden Beispiel suchen die WAN-Boot-Programme auf dem Webserver http://www.Beispiel.com (Port 1234) nach der Datei sysidcfg und den JumpStart-Dateien. Der Webserver nutzt zum Verschlüsseln der Daten und Dateien während der Installation das sichere HTTP-Protokoll.

Die Datei sysidcfg und die Dateien der benutzerdefinierten JumpStart-Installation befinden sich im Unterverzeichnis flash das Dokument-Root-Verzeichnisses /opt/apache/htdocs.

SsysidCF=https://www.example.com:1234/flash
SjumpsCF=https://www.example.com:1234/flash

Beispiel 12–13 Systemkonfigurationsdatei für eine unsichere WAN-Boot-Installation

Im folgenden Beispiel suchen die WAN-Boot-Programme auf dem Webserver http://www.Beispiel.com nach der Datei sysidcfg und den JumpStart-Dateien. Der Webserver verwendet eine HTTP-Verbindung, und die Daten und Dateien sind während der Installation ungeschützt.

Die Datei sysidcfg und die JumpStart-Dateien befinden sich im Unterverzeichnis flash des Dokument-Root-Verzeichnisses htdocs.

SsysidCF=http://www.example.com/flash
SjumpsCF=http://www.example.com/flash

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie die Systemkonfigurationsdatei erstellt haben, erzeugen Sie die Datei wanboot.conf. Eine Anleitung dazu finden Sie in "So erzeugen Sie die Datei wanboot.conf" auf Seite 209.

So erzeugen Sie die Datei wanboot.conf

Die Datei wanboot . conf ist eine Konfigurationsdatei im Textformat, auf welche die WAN-Boot-Programme für die Durchführung einer WAN-Installation zugreifen. Sowohl das Programm wanboot - cgi als auch das Boot-Dateisystem und die WAN-Boot-Miniroot greifen für die Installation des Clientsystems auf die Informationen in der Datei wanboot . conf zu.

Speichern Sie die Datei wanboot.conf im entsprechenden Client-Unterverzeichnis der /etc/netboot-Hierarchie auf dem WAN-Boot-Server. Wie Sie den Aktionsbereich für Ihre WAN-Boot-Installation in der /etc/netboot-Hierarchie festlegen, erfahren Sie in "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186.

Wenn auf dem WAN-Boot-Server aktuelle Solaris-Release läuft, finden Sie in /etc/netboot/wanboot.conf.sample ein Beispiel für die Datei wanboot.conf.Diese Beispieldatei können Sie als Vorlage für Ihre WAN-Boot-Installation verwenden.

Die nachfolgenden Informationen müssen in der Datei wanboot.conf enthalten sein.

Informationstyp	Beschreibung
Angaben zum WAN-Boot-Server	 Pfad zum wanboot-Programm auf dem WAN-Boot-Server URL des Programms wanboot - cgi auf dem WAN-Boot-Server

Informationstyp	Beschreibung
Angaben zum Installationsserver	Pfad zur WAN-Boot-Miniroot auf dem Installationsserver
	 Pfad zur Systemkonfigurationsdatei auf dem WAN-Boot-Server, in der die Adressen der Datei sysidcfg und der JumpStart-Dateien angegeben sind
Sicherheitsinformationen	 Signaturtyp f ür das WAN-Boot-Dateisystem oder die WAN-Boot-Miniroot
	 Verschlüsselungstyp für das WAN-Boot-Dateisystem
	 Angabe, ob bei der WAN-Boot-Installation eine Server-Authentifizierung erfolgen muss oder nicht
	 Angabe, ob bei der WAN-Boot-Installation eine Client-Authentifizierung erfolgen muss oder nicht
Nicht obligatorische Angaben	 Zusätzliche Host-Namen, die bei der WAN-Boot-Installation für den Client aufgelöst werden müssen
	 URL des Skripts bootlog-cgi auf dem Protokollserver

Diese Informationen stellen Sie bereit, indem Sie die Parameter und die dazugehörigen Werte in folgendem Format aufführen:

parameter=value

Ausführliche Informationen über Parameter und Syntax für die Datei wanboot.conf entnehmen Sie bitte dem Abschnitt "Parameter der Datei wanboot.conf und Syntax" auf Seite 258.

Gehen Sie folgendermaßen vor, um die Datei wanboot. conf zu erzeugen.

1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.

2 Erzeugen Sie die Textdatei wanboot.conf.

Dabei können Sie entweder eine neue Datei namens wanboot.conf erstellen oder die in /etc/netboot/wanboot.conf.sample enthaltene Beispieldatei verwenden. Wenn Sie auf die Beispieldatei zurückgreifen, benennen Sie die Datei in wanboot.conf um, nachdem Sie alle Parameter hinzugefügt haben.

3 Geben Sie die geeigneten wanboot.conf-Parameter und -Parameterwerte für Ihre Installation ein.

Ausführliche Informationen über Parameter und Werte für die Datei wanboot.conf entnehmen Sie bitte dem Abschnitt "Parameter der Datei wanboot.conf und Syntax" auf Seite 258. 4 Speichern Sie die Datei wanboot.conf in dem passenden Unterverzeichnis in der /etc/netboot-Hierarchie.

Wie Sie die /etc/netboot-Hierarchie erzeugen, erfahren Sie in "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186.

5 Validieren Sie die wanboot.conf-Datei.

bootconfchk /etc/netboot/path-to-wanboot.conf/wanboot.conf

Pfad_zu_wanboot.confSteht f
ür den Pfad zur Datei wanboot . conf des Clients auf dem
WAN-Boot-Server.

- Wenn die Struktur der Datei wanboot.conf gültig ist, gibt der Befehl bootconfchk den Beendigungscode 0 zurück.
- Ist die Datei wanboot.conf hingegen ungültig, liefert der Befehl bootconfchk einen Beendigungscode ungleich Null.
- 6 Setzen Sie die Berechtigungen für die wanboot.conf-Datei auf 600.

chmod 600 /etc/netboot/path-to-wanboot.conf/wanboot.conf

Beispiel 12–14 wanboot.conf-Datei für die WAN-Boot-Installation per HTTPS

Die folgende wanboot.conf-Beispieldatei enthält Konfigurationsinformationen für eine WAN-Installation mit sicherem HTTP. Außerdem ist in der Datei wanboot.conf festgelegt, dass bei der Installation eine 3DES-Verschlüsselung zum Einsatz kommt.

```
boot_file=/wanboot/wanboot.s10_sparc
root_server=https://www.example.com:1234/cgi-bin/wanboot-cgi
root_file=/miniroot/miniroot.s10_sparc
signature_type=shal
encryption_type=3des
server_authentication=yes
client_authentication=no
resolve_hosts=
boot_logger=https://www.example.com:1234/cgi-bin/bootlog-cgi
system_conf=sys-conf.s10-sparc
```

Aus dieser wanboot.conf-Datei ergibt sich die folgende Konfiguration:

boot_file=/wanboot/wanboot.s10_sparc

Das sekundäre Boot-Programm heißt wanboot.s10_sparc. Dieses Programm befindet sich im Verzeichnis /wanboot des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.

root_server=https://www.example.com:1234/cgi-bin/wanboot-cgi

Die Adresse des Programms wanboot-cgi auf dem WAN-Boot-Server lautet https://www.Beispiel.com:1234/cgi-bin/wanboot-cgi. Der https-Teil der URL gibt an, dass diese WAN-Boot-Installation mit sicherem HTTP vorgenommen wird.

```
root file=/miniroot/miniroot.s10 sparc
  Die WAN-Boot-Miniroot heißt miniroot.s10 sparc. Die Miniroot befindet sich im
  Verzeichnis /miniroot des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.
signature type=sha1
  Das Programm wanboot.s10_sparc und das WAN-Boot-Dateisystem werden mit einem
  HMAC SHA1-Hashing-Schlüssel signiert.
encryption type=3des
  Das Programm wanboot.s10 sparc und das Boot-Dateisystem werden mit einem
  3DES-Schlüssel chiffriert.
server authentication=yes
  Der Server wird bei der Installation authentifiziert.
client authentication=no
  Der Client wird bei der Installation nicht authentifiziert.
resolve hosts=
  Es werden keine zusätzlichen Host-Namen für die WAN-Boot-Installation benötigt. Alle
  erforderlichen Dateien und Informationen sind im Dokument-Root-Verzeichnis auf dem
  WAN-Boot-Server vorhanden.
boot logger=https://www.example.com:1234/cgi-bin/bootlog-cgi
  (Optional) Boot- und Installationsprotokollmeldungen werden per sicherem HTTP auf dem
  WAN-Boot-Server aufgezeichnet.
  Anweisungen zur Einrichtung eines Protokollservers für die WAN-Boot-Installation finden
  Sie unter "(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190.
system conf=sys-conf.s10-sparc
```

Die Systemkonfigurationsdatei enthält die Speicherorte der Datei sysidcfg und der JumpStart-Dateien, die sich in einem Unterverzeichnis der /etc/netboot-Hierarchie befinden. Die Systemkonfigurationsdatei heißt sys-conf.s10–sparc.

Beispiel 12–15 wanboot.conf-Datei für die unsichere WAN-Boot-Installation

Die folgende wanboot.conf-Beispieldatei enthält Konfigurationsinformationen für eine weniger sichere WAN-Boot-Installation mit HTTP. Diese wanboot.conf-Datei gibt auch vor, dass bei der Installation weder ein Hashing-Schlüssel noch eine Verschlüsselung zum Einsatz kommen.

```
boot_file=/wanboot/wanboot.sl0_sparc
root_server=http://www.example.com/cgi-bin/wanboot-cgi
root_file=/miniroot/miniroot.sl0_sparc
signature_type=
encryption_type=
server_authentication=no
client_authentication=no
resolve hosts=
```

```
boot_logger=http://www.example.com/cgi-bin/bootlog-cgi
system_conf=sys-conf.sl0-sparc
```

Aus dieser wanboot.conf-Datei ergibt sich die folgende Konfiguration:

boot_file=/wanboot/wanboot.s10_sparc

Das sekundäre Boot-Programm heißt wanboot.s10_sparc. Dieses Programm befindet sich im Verzeichnis /wanboot des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.

```
root_server=http://www.example.com/cgi-bin/wanboot-cgi
```

Die Adresse des Programms wanboot-cgi auf dem WAN-Boot-Server lautet http://www.Beispiel.com/cgi-bin/wanboot-cgi. Die Installation erfolgt nicht über sicheres HTTP.

root_file=/miniroot/miniroot.s10_sparc

Die WAN-Boot-Miniroot heißt miniroot.s10_sparc. Die Miniroot befindet sich im Unterverzeichnis/miniroot des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.

signature_type=

Das Programm wanboot.s10_sparc und das WAN-Boot-Dateisystem werden nicht mit einem Hashing-Schlüssel signiert.

encryption_type=

Das Programm wanboot.s10_sparc und das WAN-Boot-Dateisystem werden nicht chiffriert.

server_authentication=no

Der Server wird bei der Installation weder durch Schlüssel noch Zertifikate authentifiziert.

client_authentication=no

Der Client wird bei der Installation weder durch Schlüssel noch Zertifikate authentifiziert.

resolve_hosts=

Es werden keine zusätzlichen Host-Namen für die Installation benötigt. Alle erforderlichen Dateien und Informationen sind im Dokument-Root-Verzeichnis auf dem WAN-Boot-Server vorhanden.

boot_logger=http://www.example.com/cgi-bin/bootlog-cgi

(Optional) Boot- und Installationsprotokollmeldungen werden auf dem WAN-Boot-Server aufgezeichnet.

Anweisungen zur Einrichtung eines Protokollservers für die WAN-Boot-Installation finden Sie unter "(Optional) So konfigurieren Sie den WAN-Boot-Protokollserver" auf Seite 190.

system_conf=sys-conf.s10-sparc

Die Systemkonfigurationsdatei, in der die Speicherorte der sysidcfg- und JumpStart-Dateien enthalten sind, heißt sys-conf.s10-sparc. Diese Datei befindet sich im entsprechenden Client-Unterverzeichnis in der /etc/netboot-Hierarchie.

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie die Datei wanboot. conf erstellt haben, können Sie wahlweise einen DHCP-Server für die Zusammenarbeit mit WAN-Boot einrichten. Eine Anleitung hierzu finden Sie in "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214.

Wenn Sie bei Ihrer WAN-Boot-Installation keinen DHCP-Server verwenden möchten, setzen Sie die WAN-Boot-Installation mit dem Schritt "So überprüfen Sie den Gerätealias net im Client-OBP" auf Seite 216 fort.

Siehe auch Ausführliche Beschreibungen von Parametern der Datei wanboot. conf und deren Werten finden Sie unter "Parameter der Datei wanboot. conf und Syntax" auf Seite 258 und der Manpage wanboot. conf(4).

(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server

Kommt in Ihrem Netzwerk ein DHCP-Server zum Einsatz, können Sie diesen so konfigurieren, dass er die folgenden Informationen zur Verfügung stellt:

- IP-Adresse des Proxy-Servers
- Adresse des Programms wanboot cgi

Sie können die folgenden DHCP-Herstelleroptionen in der WAN-Boot-Installation verwenden:

SHTTPproxy Steht für die IP-Adresse des Proxy-Servers im Netzwerk.

SbootURI Gibt die URL des Programms wanboot - cgi auf dem WAN-Boot-Server an.

Informationen zur Einstellung dieser Herstelleroptionen auf einem Solaris-DHCP-Server finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Ausführliche Informationen zum Einrichten eines Solaris DHCP-Servers finden Sie in Kapitel 14, "Konfiguration des DHCP-Services (Aufgaben)" in *Systemverwaltungshandbuch: IP Services*.

Zum weiteren Verlauf Ihrer WAN-Boot-Installation lesen Sie Kapitel 13, "SPARC: Installation mit WAN-Boot (Vorgehen)".

♦ ♦ ♦ KAPITEL 13

SPARC: Installation mit WAN-Boot (Vorgehen)

In diesem Kapitel wird die Durchführung einer WAN-Boot-Installation auf einem SPARC-Client dargestellt. Informationen zum Vorbereiten einer WAN-Boot-Installation finden Sie in Kapitel 12, "Installieren mit WAN-Boot (Vorgehen)".

Dieses Kapitel behandelt die folgenden Vorgänge:

- "Vorbereitung des Clients für eine WAN-Boot-Installation" auf Seite 216
- "Installation des Clients" auf Seite 224

Übersicht der Schritte: Installation eines Clients mit WAN-Boot

In der folgenden Tabelle sind die zur Einrichtung eines Clients über ein WAN erforderlichen Schritte aufgeführt.

Aufgabe	Beschreibung	Siehe
Bereiten Sie das Netzwerk für eine WAN-Boot-Installation vor.	Richten Sie die Server und Dateien ein, die für die WAN-Boot-Installation benötigt werden.	Kapitel 12, "Installieren mit WAN-Boot (Vorgehen) "
Vergewissern Sie sich, dass der Gerätealias net im Client-OBP richtig gesetzt ist.	Mit dem Befehl devalias überprüfen Sie, ob der Gerätealias net auf die primäre Netzwerkschnittstelle gesetzt ist.	"So überprüfen Sie den Gerätealias net im Client-OBP" auf Seite 216

TABELLE 13-1 Übersicht der Schritte: Durchführung einer WAN-Boot-Installation

Aufgabe	Beschreibung	Siehe
Stellen Sie dem Client Schlüssel zur Verfügung.	Sie stellen dem Client Schlüssel für die Installation zur Verfügung, indem Sie OBP-Variablen setzen oder Schlüsselwerte eingeben.	"Installation von Schlüsseln auf dem Client" auf Seite 218
	Dieser Schritt ist für die sichere Installationskonfiguration erforderlich. Für unsichere Installationen mit Überprüfung der Datenintegrität generieren Sie in diesem Schritt einen HMAC SHA1-Hashing-Schlüssel für den Client.	
Installieren Sie über ein WAN die Software auf dem Client.	Wählen Sie das für den Client geeignete Installationsverfahren.	"So nehmen Sie eine ungeführte WAN-Boot-Installation vor" auf Seite 225
		"So nehmen Sie eine interaktive WAN-Boot-Installation vor" auf Seite 227
		"So nehmen Sie eine WAN-Boot-Installation mit einem DHCP-Server vor" auf Seite 231
		"So nehmen Sie eine WAN-Boot-Installation mit lokalen CDs vor" auf Seite 233

 TABELLE 13-1
 Übersicht der Schritte: Durchführung einer WAN-Boot-Installation
 (Fortsetzung)

Vorbereitung des Clients für eine WAN-Boot-Installation

Führen Sie folgende Schritte durch, um den Client für die Installation vorzubereiten:

- "So überprüfen Sie den Gerätealias net im Client-OBP" auf Seite 216
- "Installation von Schlüsseln auf dem Client" auf Seite 218

So überprüfen Sie den Gerätealias net im Client-OBP

Zum Booten des Clients aus dem WAN mit dem Befehl boot net muss der Gerätealias net auf das primäre Netzwerkgerät des Clients gesetzt werden. Dieser Aliasname ist auf den meisten Systemen bereits richtig eingestellt. Ist der Alias jedoch nicht auf das Netzwerkgerät gesetzt, das verwendet werden soll, müssen Sie ihn ändern.

Weitere Informationen zum Ändern der Alias-Einstellungen finden Sie unter "The Device Tree" in *OpenBoot 3.x Command Reference Manual.*
Führen Sie die nachfolgenden Schritte durch, um den Gerätealias net auf dem Client zu überprüfen:

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim Client an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

2 Bringen Sie das System auf Run-Level 0.

init 0

Die Eingabeaufforderung ok wird angezeigt.

3 An der Eingabeaufforderung ok prüfen Sie die im OBP gesetzten Gerätealiasnamen.

ok **devalias**

Der Befehl devalias liefert Informationen wie in diesem Beispiel:

screen	/pci@lf,0/pci@l,1/SUNW,m64B@2
net	/pci@lf,0/pci@l,1/network@c,1
net2	/pci@lf,0/pci@l,1/network@5,1
disk	/pci@lf,0/pci@l/scsi@8/disk@0,0
cdrom	/pci@lf,0/pci@l,1/ide@d/cdrom@0,0:f
keyboard	/pci@lf,0/pci@l,1/ebus@l/su@14,3083f8
mouse	/pci@lf,0/pci@l,1/ebus@l/su@14,3062f8

- Wenn der Alias net auf das für die Installation zu verwendende Netzwerkgerät gesetzt ist, brauchen Sie ihn nicht ändern. Setzen Sie die Installation mit dem Schritt "Installation von Schlüsseln auf dem Client" auf Seite 218 fort.
- Ist net jedoch nicht auf das Netzwerkgerät gesetzt, das verwendet werden soll, müssen Sie den Alias ändern. Fahren Sie fort.

4 Ändern Sie den Gerätealias net.

Ändern Sie den Gerätealias net mit einem der folgenden Befehle:

Um net nur f
ür die aktuelle Installation zu setzen, verwenden Sie den Befehl devalias.

ok devalias net device-path

net *Gerätepfad* Weist dem Alias net das Gerät *Gerätepfad* zu.

• Um net dauerhaft zu setzen, greifen Sie auf den Befehl nvalias zurück.

ok nvalias net device-path

net Gerätepfad Weist das Gerät Gerätepfad dem net-Alias zu.

Beispiel 13-1 Überprüfen und Ändern des Gerätealias net

Mit den folgenden Befehlen wird der Gerätealias net überprüft und geändert.

Überprüfen Sie die Alias-Einstellungen.

/pci@1f,0/pci@1,1/SUNW,m64B@2
/pci@lf,0/pci@l,1/network@c,1
/pci@lf,0/pci@l,1/network@5,1
/pci@lf,0/pci@l/scsi@8/disk@0,0
/pci@lf,0/pci@l,1/ide@d/cdrom@0,0:f
/pci@lf,0/pci@l,1/ebus@l/su@l4,3083f8
/pci@lf,0/pci@l,1/ebus@l/su@l4,3062f8

Wenn die Netzwerkschnittstelle /pci@1f,0/pci@1,1/network@5,1 verwendet werden soll, geben Sie folgenden Befehl ein:

ok devalias net /pci@lf,0/pci@l,1/network@5,1

Weitere Fortsetzen der WAN-Boot-Installation

Informationen:

Nachdem Sie das Gerätealias net überprüft haben, fahren Sie mit einem der folgenden Schritte fort:

- Wenn Sie f
 ür Ihre Installation einen Hashing- und Chiffrierschl
 üssel verwenden, fahren Sie mit dem Schritt "Installation von Schl
 üsseln auf dem Client" auf Seite 218 fort.
- Wenn Sie eine ungesicherte Installation ohne Schlüssel durchführen, fahren Sie mit dem Schritt "Installation des Clients" auf Seite 224 fort.

Installation von Schlüsseln auf dem Client

Für eine sicherere WAN-Boot-Installation oder eine unsichere Installation mit Überprüfung der Datenintegrität müssen Schlüssel auf dem Client installiert werden. Die an den Client übertragenen Daten können mit einem Hashing-Schlüssel und einer Verschlüsselung (Chiffrierschlüssel) geschützt werden. Sie können diese Schlüssel mit den folgenden Methoden installieren:

- Setzen von OBP-Variablen Sie können den Variablen der OBP-Netzwerk-Boot-Argumente vor dem Booten des Clients Schlüsselwerte zuweisen. Diese Schlüssel stehen dem Client dann für zukünftige WAN-Boot-Installationen weiter zur Verfügung.
- Eingabe der Schlüsselwerte beim Booten Sie können an der Eingabeaufforderung boot des wanboot-Programms Schlüsselwerte setzen. Auf diese Art installierte Schlüssel stehen nur für die aktuelle WAN-Boot-Installation zur Verfügung.

Schlüssel können auch im OBP eines laufenden Clients installiert werden. Wenn Sie auf einem laufenden Client Schlüssel installieren möchten, muss auf dem System Solaris 9 12/03 oder eine kompatible Version ausgeführt werden.

Wenn Sie Schlüssel auf dem Client installieren, vergewissern Sie sich, dass die Schlüsselwerte nicht über eine unsichere Verbindung gesendet werden. Wenden Sie zur Geheimhaltung der Schlüsselwerte die an Ihrem Standort geltenden Sicherheitsrichtlinien an.

- Wie Sie den Variablen von OBP-Netzwerk-Boot-Argumenten Schlüsselwerte zuweisen, erfahren Sie in "So installieren Sie Schlüssel im Client-OBP" auf Seite 219.
- Anweisungen zur Installation von Schlüsseln während des Bootens finden Sie in "So nehmen Sie eine interaktive WAN-Boot-Installation vor" auf Seite 227.
- Anweisungen zur Installation von Schlüsseln im OBP eines laufenden Clients finden Sie in "So installieren Sie einen Hashing- und einen Chiffrierschlüssel auf einem laufenden Client" auf Seite 222.

So installieren Sie Schlüssel im Client-OBP

Sie können den Variablen der OBP-Netzwerk-Boot-Argumente vor dem Booten des Clients Schlüsselwerte zuweisen. Diese Schlüssel stehen dem Client dann für zukünftige WAN-Boot-Installationen weiter zur Verfügung.

Führen Sie die nachfolgenden Schritte aus, um Schlüssel im Client-OBP zu installieren.

Gehen Sie wie folgt vor, wenn Sie Variablen für OBP-Netzwerk-Boot-Argumente Schlüsselwerte zuweisen möchten:

1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.

2 Zeigen Sie für jeden Client den Schlüsselwert an.

# wanbootutil	keygen -d -c -o net=net-ip,cid=client-ID,type=key-type
Netz-IP	IP-Adresse des Teilnetzes, in dem sich der Client befindet.
Client-ID	ID des Clients, auf dem die Installation erfolgen soll. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.
Schlüsseltyp	Die Art des Schlüssels, der auf dem Client installiert werden soll. Gültige Schlüsseltypen sind 3des, aes und sha1.

Es wird der Hexadezimalwert des Schlüssels angezeigt.

3 Wiederholen Sie den vorigen Schritt für jeden Typ der zu installierenden Client-Schlüssel.

4 Bringen Sie das Clientsystem auf Run-Level 0.

init 0

Die Eingabeaufforderung ok wird angezeigt.

5 An der Eingabeaufforderung ok des Clients setzen Sie den Wert für den Hashing-Schlüssel. ok set-security-key wanboot-hmac-sha1 *key-value*

set-security-key	Installiert den Schlüssel auf dem Client.
wanboot-hmac-shal	Weist das OBP an, einen HMAC SHA1-Hashing-Schlüssel zu installieren.
Schlüsselwert	Steht für den in Schritt 2 angezeigten Hexadezimalwert.

Der HMAC SHA1-Hashing-Schlüssel wird im Client-OBP installiert.

6 Installieren Sie an der Eingabeaufforderung ok des Clients den Chiffrierschlüssel (die Verschlüsselung).

ok set-security-key wanboot-3des <i>key-value</i>		
set-security-key	Installiert den Schlüssel auf dem Client.	
wanboot-3des	Weist das OBP an, eine 3DES-Verschlüsselung zu installieren. Wenn Sie stattdessen eine AES-Verschlüsselung verwenden möchten, setzen Sie diesen Wert auf wanboot - aes.	
Schlüsselwert	Gibt den Hexadezimalwert an, der den Chiffrierschlüssel darstellt.	

Die 3DES-Verschlüsselung wird im Client-OBP installiert.

Mit der Installation der Schlüssel sind die Vorbereitungen für die Einrichtung des Clients abgeschlossen. Anweisungen zur Einrichtung des Clientsystems finden Sie in "Installation des Clients" auf Seite 224.

7 (Optional) Vergewissern Sie sich, dass die Schlüssel im Client-OBP gesetzt sind.

```
ok list-security-keys
Security Keys:
wanboot-hmac-shal
wanboot-3des
```

.

8 (Optional) Falls Sie einen Schlüssel löschen müssen, verwenden Sie dazu den folgenden Befehl:

ok **set-security-key** key-type

Schlüsseltyp Gibt den Schlüsseltyp an, der gelöscht werden soll. Verwenden Sie einen der Werte wanboot - hmac - sha1, wanboot - 3des oder wanboot - aes.

Beispiel 13–2 Installation von Schlüsseln im Client-OBP

Das folgende Beispiel zeigt, wie ein Hashing- und ein Chiffrierschlüssel im Client-OBP installiert werden.

Zeigen Sie auf dem WAN-Boot-Server die Schlüsselwerte an.

```
# wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
b482aaab82cb8d5631e16d51478c90079cc1d463
# wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=3des
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
```

Dieses Beispiel enthält folgende Informationen:

```
net=192.168.198.0
```

Die IP-Adresse des Teilnetzes, in dem sich der Client befindet.

```
cid=010003BA152A42
Die Client-ID.
```

```
b482aaab82cb8d5631e16d51478c90079cc1d463
Den Wert des HMAC SHA1-Hashing-Schlüssels des Clients.
```

```
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
Den Wert der 3DES-Verschlüsselung des Clients.
```

Kommt in Ihrer Installation eine AES-Verschlüsselung zum Einsatz, dann ändern Sie wanboot - 3des in wanboot - aes ab, um den Schlüsselwert anzuzeigen.

Installieren Sie die Schlüssel auf dem Clientsystem.

```
ok set-security-key wanboot-hmac-shal b482aaab82cb8d563le16d51478c90079ccld463
ok set-security-key wanboot-3des 9ebc7a57f240e97c9b940le9d3ae9b292943d3c143d07f04
```

Diese Befehle führen folgende Aktionen durch:

- Installation des HMAC SHA1-Hashing-Schlüssels mit dem Wert b482aaab82cb8d5631e16d51478c90079cc1d463 auf dem Client
- Installation des 3DES-Chiffrierschlüssels mit dem Wert
 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 auf dem Client

Wenn in der Installation eine AES-Verschlüsselung verwendet wird, ändern Sie wanboot - 3des in wanboot - aes ab.

Weitere Fortsetzen der WAN-Boot-Installation

Nachdem Sie die Schlüssel auf dem Client installiert haben, können Sie diesen über das WAN installieren. Die Anleitung hierzu finden Sie unter "Installation des Clients" auf Seite 224.

Siehe auch Nähere Informationen zum Anzeigen von Schlüsselwerten finden Sie auf der Manpage wanbootutil(1M).

So installieren Sie einen Hashing- und einen Chiffrierschlüssel auf einem laufenden Client

Sie können Schlüsselwerte auf einem laufenden System an der Eingabeaufforderung boot> des wanboot-Programms eingeben. Auf diese Art installierte Schlüssel stehen nur für die aktuelle WAN-Boot-Installation zur Verfügung.

Wenn Sie sowohl einen Hashing- als auch einen Chiffrierschlüssel im OBP eines laufenden Clients installieren möchten, gehen Sie nach dem folgenden Verfahren vor.

Bevor Sie Dabei wird Folgendes vorausgesetzt: **beginnen**

- Das Clientsystem ist eingeschaltet.
- Der Client ist über eine sichere Verbindung wie z. B. eine Secure Shell (ssh) zugänglich.
- 1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.

2 Zeigen Sie den Schlüsselwert für die Client-Schlüssel an.

wanbootutil keygen -d -c -o net=net-ip,cid=client-ID,type=key-type

- *Netz-IP* IP-Adresse des Teilnetzes, in dem sich der Client befindet.
- *Client-ID* ID des Clients, auf dem die Installation erfolgen soll. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.
- Schlüsseltyp Die Art des Schlüssels, der auf dem Client installiert werden soll. Gültige Schlüsseltypen sind 3des, aes und sha1.

Es wird der Hexadezimalwert des Schlüssels angezeigt.

- 3 Wiederholen Sie den vorigen Schritt für jeden Typ der zu installierenden Client-Schlüssel.
- 4 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden administrativen Rolle beim Client an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

5 Installieren Sie die erforderlichen Schlüssel auf dem laufenden Clientsystem.

```
# /usr/lib/inet/wanboot/ickey -o type=key-type
> key-value
```

SchlüsseltypDie Art des Schlüssels, der auf dem Client installiert werden soll. Gültige
Schlüsseltypen sind 3des, aes und sha1.

Schlüsselwert Steht für den in Schritt 2 angezeigten Hexadezimalwert.

6 Wiederholen Sie den vorigen Schritt für jeden Typ der zu installierenden Client-Schlüssel.

Nach dem Installieren der Schlüssel können Sie den Client installieren. Anweisungen zur Einrichtung des Clientsystems finden Sie in "Installation des Clients" auf Seite 224.

Beispiel 13–3 Installation von Schlüsseln im OBP eines laufenden Clientsystems

Das folgende Beispiel zeigt, wie Schlüssel im OBP eines laufenden Clients installiert werden.

Zeigen Sie auf dem WAN-Boot-Server die Schlüsselwerte an.

wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
b482aaab82cb8d5631e16d51478c90079cc1d463
wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=3des
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04

Dieses Beispiel enthält folgende Informationen:

net=192.168.198.0 Die IP-Adresse des Teilnetzes, in dem sich der Client befindet.

cid=010003BA152A42 Die Client-ID.

b482aaab82cb8d5631e16d51478c90079cc1d463 Den Wert des HMAC SHA1-Hashing-Schlüssels des Clients.

9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 Den Wert der 3DES-Verschlüsselung des Clients.

Wenn Sie in Ihrer Installation einen AES-Schlüssel verwenden, müssen Sie type=3des in type=aes ändern, damit der Schlüsselwert angezeigt wird.

Installieren Sie die Schlüssel im OBP des laufenden Clients.

/usr/lib/inet/wanboot/ickey -o type=shal b482aaab82cb8d5631e16d51478c90079cc1d463 # /usr/lib/inet/wanboot/ickey -o type=3des 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04

Diese Befehle führen folgende Aktionen durch:

- Installation des HMAC SHA1-Hashing-Schlüssels mit dem Wert b482aaab82cb8d5631e16d51478c90079cc1d463 auf dem Client
- Installation der 3DES-Verschlüsselung mit dem Wert
 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 auf dem Client wanclient-1

Weitere Informationen:	Fortsetzen der WAN-Boot-Installation	
	Nachdem Sie die Schlüssel auf dem Client installiert haben, können Sie diesen über das WAN installieren. Die Anleitung hierzu finden Sie unter "Installation des Clients" auf Seite 224.	
Siehe auch	Nähere Informationen zum Anzeigen von Schlüsselwerten finden Sie auf der Manpage wanbootutil $(1M)$.	
	Weitere Informationen zur Installation von Schlüsseln auf einem laufenden System finden Sie in ickey(1M).	

Installation des Clients

Wenn Sie die Vorbereitung des Netzwerks für die WAN-Boot-Installation abgeschlossen haben, können Sie eines der folgenden Verfahren wählen, um die Client-Installation vorzunehmen.

Methode	Beschreibung	Anweisungen
Ungeführte Installation	Dieses Installationsverfahren wenden Sie an, wenn vor dem Booten des Clients die Schlüssel auf ihm installiert und die Client-Konfigurationsinformatione festgelegt werden sollen.	 Um vor der Installation Schlüssel auf dem Client zu installieren, führen Sie den Schritt "Installation von Schlüsseln auf dem Client" auf Seite 218 aus.
		 Die Vorgehensweise f ür eine ungef ührte Installation ist in "So nehmen Sie eine ungef ührte WAN-Boot-Installation vor" auf Seite 225 beschrieben.
Interaktive Installation	Dieses Installationsverfahren wenden Sie an, wenn die Client-Konfigurationsinformatione beim Booten gesetzt werden sollen.	"So nehmen Sie eine interaktive WAN-Boot-Installation vor" n auf Seite 227

TABELLE 13–2 Verfahren für die Client-Installation

Methode	Beschreibung	Anweisungen
Installation mit einem DHCP-Server	Wenden Sie dieses Installationsverfahren an, wenn Sie den DHCP-Server des Netzwerks so konfiguriert haben, dass er bei der Installation die Client-Konfigurationsinformationen zur Verfügung stellt.	• Wie Sie einen DHCP-Server für eine WAN-Boot-Installation konfigurieren, erfahren Sie in "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214.
		 Wie Sie einen DHCP-Server bei der Installation verwenden, ist in "So nehmen Sie eine WAN-Boot-Installation mit einem DHCP-Server vor" auf Seite 231 beschrieben.
Installation mit lokaler CD	Wenn Ihr Client-OBP keine Unterstützung für WAN-Boot bietet, booten Sie den Client von einer lokalen Kopie der Solaris Software-CD.	 Wie Sie feststellen, ob das Client-OBP Unterstützung für WAN-Boot bietet, erfahren Sie in "So überprüfen Sie das Client-OBP auf WAN-Boot-Unterstützung" auf Seite 182.
		 Die Client-Installation anhand einer lokalen Kopie der Solaris Software-CD ist in "So nehmen Sie eine WAN-Boot-Installation mit lokalen CDs vor" auf Seite 233 beschrieben.

 TABELLE 13-2
 Verfahren für die Client-Installation
 (Fortsetzung)

So nehmen Sie eine ungeführte WAN-Boot-Installation vor

Dieses Installationsverfahren wenden Sie an, wenn Sie vorab sowohl die Schlüssel installieren als auch die Client-Konfigurationsinformationen festlegen möchten. Anschließend können Sie den Client über das WAN booten und eine ungeführte Installation vornehmen.

Bei diesem Verfahren wird davon ausgegangen, dass Sie entweder Schlüssel im Client-OBP installiert haben oder eine unsichere Installation durchführen. Wie Sie vor der Installation Schlüssel auf dem Client installieren, erfahren Sie in "Installation von Schlüsseln auf dem Client" auf Seite 218.

1 Wenn das Clientsystem läuft, schalten Sie es auf Run-Level 0.

init 0

Die Eingabeaufforderung ok wird angezeigt.

2 Setzen Sie an der Eingabeaufforderung ok auf dem Client die Variablen f ür die Netzwerk-Boot-Argumente im OBP.

```
ok setenv network-boot-arguments host-ip=client-IP,
router-ip=router-ip,subnet-mask=mask-value,
hostname=client-name,http-proxy=proxy-ip:port,
file=wanbootCGI-URL
```

Hinweis – Die Zeilenumbrüche in diesem Befehlsbeispiel dienen nur der Übersichtlichkeit. Geben Sie vor dem Ende des Befehls keinen Zeilenumbruch bzw. Wagenrücklauf ein.

setenv network-boot-arguments	Weist das OBP an, die folgenden Boot-Argumente zu setzen
host-ip= <i>Client-IP</i>	IP-Adresse des Clients
router-ip= <i>Router-IP</i>	IP-Adresse des Netzwerk-Routers
subnet-mask= <i>Maskenwert</i>	Maskenwert des Teilnetzes
hostname= <i>Client-Name</i>	Host-Name des Clients
(Optional) http-proxy= <i>Proxy-IP:Port</i>	Gibt die IP-Adresse und den Port des Proxy-Servers für das Netzwerk an.
file=wanbootCGI-URL	Gibt die URL des Programms wanboot - cgi auf dem Webserver an.

3 Booten Sie den Client.

ok boot net - install

net - install Weist den Client an, beim Booten über das WAN auf die Variablen der Netzwerk-Boot-Argumente zurückzugreifen.

Der Client wird über das WAN installiert. Wenn die WAN-Boot-Programme nicht alle erforderlichen Installationsinformationen finden, fordert wanboot Sie zur Eingabe der fehlenden Informationen auf. Geben Sie an der Eingabeaufforderung die benötigten Informationen ein.

Beispiel 13–4 Ungeführte WAN-Boot-Installation

Im folgenden Beispiel werden die Variablen der Netzwerk-Boot-Argumente für das Clientsystem myclient vor dem Booten des Systems gesetzt. In diesem Beispiel wird davon ausgegangen, dass auf dem Client bereits ein Hashing- und ein Chiffrierschlüssel installiert sind. Informationen zur Installation von Schlüsseln vor dem Booten über das WAN finden Sie in "Installation von Schlüsseln auf dem Client" auf Seite 218.

```
ok setenv network-boot-arguments host-ip=192.168.198.136,
router-ip=192.168.198.129,subnet-mask=255.255.255.192
hostname=myclient,file=http://192.168.198.135/cgi-bin/wanboot-cgi
ok boot net - install
Resetting ...
```

Sun Blade 100 (UltraSPARC-IIe), No Keyboard Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved. OpenBoot 4.x.build_28, 512 MB memory installed, Serial #50335475. Ethernet address 0:3:ba:e:f3:75, Host ID: 83000ef3.

```
Rebooting with command: boot net - install
Boot device: /pci@lf,0/network@c,1 File and args: - install
```

Es werden die folgenden Variablen gesetzt:

- Die IP-Adresse des Clients wird auf 192.168.198.136 gesetzt.
- Die IP-Adresse des Client-Routers wird auf 192.168.198.129 gesetzt.
- Die Teilnetzmaske des Clients wird auf 255.255.255.192 gesetzt.
- Der Host-Name des Clients wird auf seahag gesetzt.
- Das Programm wanboot cgi befindet sich unter http://192.168.198.135/cgi-bin/wanboot - cgi.

Siehe auch Weitere Informationen zum Einrichten der Netzwerk-Bootargumente finden Sie in set(1).

Weitere Informationen zum Booten eines Systems finden Sie in boot(1M).

So nehmen Sie eine interaktive WAN-Boot-Installation vor

Wenden Sie dieses Installationsverfahren an, wenn Sie während der Installation über die Befehlszeile sowohl die Schlüssel installieren als auch die Client-Konfigurationsinformationen setzen möchten. Bei diesem Verfahren wird davon ausgegangen, dass Sie die WAN-Installation per HTTPS vornehmen. Wenn Sie eine unsichere Installation ohne Schlüssel durchführen, zeigen Sie keine Client-Schlüssel an noch installieren Sie solche.

1 Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.

2 Zeigen Sie für jeden Client den Schlüsselwert an.

wanbootutil keygen -d -c -o net=net-ip,cid=client-ID,type=key-type

- *Netz-IP* Die IP-Adresse des Teilnetzes für den Client, auf dem die Installation erfolgen soll.
- *Client-ID* ID des Clients, auf dem die Installation erfolgen soll. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.
- Schlüsseltyp Die Art des Schlüssels, der auf dem Client installiert werden soll. Gültige Schlüsseltypen sind 3des, aes und sha1.

Es wird der Hexadezimalwert des Schlüssels angezeigt.

- 3 Wiederholen Sie den vorigen Schritt f
 ür jeden Typ der zu installierenden Client-Schl
 üssel.
- 4 Wenn das Clientsystem läuft, schalten Sie es auf Run-Level 0.
- 5 Setzen Sie an der Eingabeaufforderung ok auf dem Clientsystem die Variablen der Netzwerk-Boot-Argumente im OBP.

ok setenv network-boot-arguments host-ip=client-IP, router-ip=router-ip, subnet-mask=mask-value, hostname=client-name, http-proxy=proxy-ip:port, bootserver=wanbootCGI-URL

Hinweis – Die Zeilenumbrüche in diesem Befehlsbeispiel dienen nur der Übersichtlichkeit. Geben Sie vor dem Ende des Befehls keinen Zeilenumbruch bzw. Wagenrücklauf ein.

setenv network-boot-arguments	Weist das OBP an, die folgenden Boot-Argumente zu setzen:
host-ip= <i>Client-IP</i>	IP-Adresse des Clients
router-ip= <i>Router-IP</i>	IP-Adresse des Netzwerk-Routers
<pre>subnet-mask=Maskenwert</pre>	Maskenwert des Teilnetzes
hostname=Client-Name	Host-Name des Clients
(Optional) http-proxy=Proxy-IP:Port	Gibt die IP-Adresse und Port-Nummer des Proxy-Servers für das Netzwerk an

bootserver=wanbootCGI-URLGibt die URL des Programms wanboot-cgi auf dem
Webserver an.

Hinweis – Der URL-Wert für die Variable bootserver darf keine HTTPS-URL sein. Die URL muss mit http:// beginnen.

6 Booten Sie an der Eingabeaufforderung ok des Clients das System.

ok boot net -o prompt - install

```
net -o prompt - install Weist den Client an, über das Netzwerk zu booten und zu
installieren. Das Programm wanboot fordert den Benutzer zur
Eingabe von Client-Konfigurationsinformationen an der
Eingabeaufforderung boot> auf.
```

Die Eingabeaufforderung boot> wird angezeigt.

7 Installieren Sie den Chiffrierschlüssel.

boot> 3des=key-value

3des=Schlüsselwert

Gibt den Hexadezimalwert des in Schritt 2 angezeigten 3DES-Schlüssels an.

Wenn Sie mit AES-Verschlüsselung arbeiten, verwenden Sie folgendes Format:

boot> aes=key-value

8 Installieren Sie den Hashing-Schlüssel.

boot> shal=key-value

sha1=Schlüsselwert Gibt den in Schritt 2 angezeigten Hashing-Schlüsselwert an.

9 Geben Sie folgenden Befehl ein, um den Boot-Prozess fortzusetzen:

boot> **go**

Der Client wird über das WAN installiert.

10 Wenn Sie dazu aufgefordert werden, geben Sie über die Befehlszeile die benötigten Client-Konfigurationsinformationen an.

Wenn die WAN-Boot-Programme nicht alle erforderlichen Installationsinformationen finden, fordert wanboot Sie zur Eingabe der fehlenden Informationen auf. Geben Sie an der Eingabeaufforderung die benötigten Informationen ein.

Beispiel 13–5 Interaktive WAN-Boot-Installation

Im folgenden Beispiel fordert das wanboot-Programm den Benutzer während der Installation zum Setzen der Schlüsselwerte für das Clientsystem auf.

Zeigen Sie auf dem WAN-Boot-Server die Schlüsselwerte an.

wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
b482aaab82cb8d5631e16d51478c90079cc1d463
wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=3des
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04

Dieses Beispiel enthält folgende Informationen:

- net=192.168.198.0 Die IP-Adresse des Teilnetzes, in dem sich der Client befindet.
- cid=010003BA152A42 Die Client-ID.
- b482aaab82cb8d5631e16d51478c90079cc1d463 Den Wert des HMAC SHA1-Hashing-Schlüssels des Clients.
- 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 Den Wert der 3DES-Verschlüsselung des Clients.

Wenn Sie in Ihrer Installation einen AES-Schlüssel verwenden, müssen Sie type=3des in type=aes ändern, damit der Schlüsselwert angezeigt wird.

Setzen Sie die Variablen der Netzwerk-Boot-Argumente im OBP des Clients.

```
ok setenv network-boot-arguments host-ip=192.168.198.136,
router-ip=192.168.198.129,subnet-mask=255.255.255.192,hostname=myclient,
bootserver=http://192.168.198.135/cgi-bin/wanboot-cgi
```

Es werden die folgenden Variablen gesetzt:

- Die IP-Adresse des Clients wird auf 192.168.198.136 gesetzt.
- Die IP-Adresse des Client-Routers wird auf 192.168.198.129 gesetzt.
- Die Teilnetzmaske des Clients wird auf 255.255.255.192 gesetzt.
- Der Host-Name des Clients wird auf myclient gesetzt.
- Das Programm wanboot-cgi befindet sich unter http://192.168.198.135/cgi-bin/wanboot-cgi.

Booten Sie den Client und führen Sie die Installation auf ihm durch.

```
ok boot net -o prompt - install
Resetting ...
```

```
Sun Blade 100 (UltraSPARC-IIe), No Keyboard
Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved.
OpenBoot 4.x.build_28, 512 MB memory installed, Serial #50335475.
Ethernet address 0:3:ba:e:f3:75, Host ID: 83000ef3.
Rebooting with command: boot net -o prompt
Boot device: /pci@lf,0/network@c,1 File and args: -o prompt
boot> 3des=9ebc7a57f240e97c9b940le9d3ae9b292943d3c143d07f04
boot> sha1=b482aaab82cb8d5631e16d51478c90079cc1d463
boot> go
```

Diese Befehle führen folgende Aktionen durch:

- Installation der 3DES-Verschlüsselung mit dem Wert 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 auf dem Client wanclient-1
- Installation des HMAC SHA1-Hashing-Schlüssels mit dem Wert b482aaab82cb8d5631e16d51478c90079cc1d463 auf dem Client
- Start der Installation

Siehe auch Weitere Informationen zum Anzeigen von Schlüsselwerten finden Sie in wanbootutil(1M).

Weitere Informationen zum Einrichten der Netzwerk-Bootargumente finden Sie in set(1).

Weitere Informationen zum Booten eines Systems finden Sie in boot(1M).

So nehmen Sie eine WAN-Boot-Installation mit einem DHCP-Server vor

Wenn Sie über einen DHCP-Server verfügen, der für die Unterstützung von WAN-Boot-Optionen konfiguriert wurde, können Sie diesen zur Bereitstellung von Client-Konfigurationsinformationen während der Installation einsetzen. Wie Sie einen DHCP-Server für eine WAN-Boot-Installation konfigurieren, erfahren Sie in "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214.

Dabei wird Folgendes vorausgesetzt:

- Das Clientsystem läuft.
- Sie haben entweder Schlüssel auf dem Client installiert oder führen eine unsichere Installation durch.

Wie Sie vor der Installation Schlüssel auf dem Client installieren, erfahren Sie in "Installation von Schlüsseln auf dem Client" auf Seite 218.

 In der Konfiguration des DHCP-Servers haben Sie die Unterstützung für die WAN-Boot-Optionen SbootURI und SHTTPproxy aktiviert. Diese Optionen ermöglichen es dem DHCP-Server, die von WAN-Boot benötigten Konfigurationsinformationen zu liefern.

Informationen zum Festlegen von Installationsoptionen auf dem DHCP-Server finden Sie unter "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

1 Wenn das Clientsystem läuft, schalten Sie es auf Run-Level 0.

init 0

Die Eingabeaufforderung ok wird angezeigt.

2 Setzen Sie an der Eingabeaufforderung ok auf dem Client die Variablen für die Netzwerk-Boot-Argumente im OBP.

ok setenv network-boot-arguments dhcp,hostname=client-name

setenv network-boot-arguments	Weist das OBP an, die folgenden Boot-Argumente zu setzen:
dhcp	Weist das OBP an, zur Konfiguration des Clients auf den DHCP-Server zurückzugreifen.
hostname=Client-Name	Hiermit geben Sie den Host-Namen an, den Sie dem Client zuweisen möchten.

3 Booten Sie den Client über das Netzwerk.

ok boot net - install

net - install Weist den Client an, beim Booten über das WAN auf die Variablen der Netzwerk-Boot-Argumente zurückzugreifen.

Der Client wird über das WAN installiert. Wenn die WAN-Boot-Programme nicht alle erforderlichen Installationsinformationen finden, fordert wanboot Sie zur Eingabe der fehlenden Informationen auf. Geben Sie an der Eingabeaufforderung die benötigten Informationen ein.

Beispiel 13–6 WAN-Boot-Installation mit DHCP-Server

Im folgenden Beispiel stellt der DHCP-Server im Netzwerk die Client-Konfigurationsinformationen bereit. Der Host-Name des Clients lautet in diesem Beispiel myclient.

ok setenv network-boot-arguments dhcp, hostname=myclient

```
ok boot net - install
Resetting ...
```

Sun Blade 100 (UltraSPARC-IIe), No Keyboard Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved. OpenBoot 4.x.build_28, 512 MB memory installed, Serial #50335475. Ethernet address 0:3:ba:e:f3:75, Host ID: 83000ef3.

Rebooting with command: boot net - install Boot device: /pci@lf,0/network@c,1 File and args: - install

Siehe auch Weitere Informationen zum Einrichten der Netzwerk-Bootargumente finden Sie in set(1).

Weitere Informationen zum Booten eines Systems finden Sie in boot(1M).

Weitere Informationen zur Konfiguration eines DHCP-Servers finden Sie in "(Optional) Bereitstellung von Konfigurationsinformationen mit einem DHCP-Server" auf Seite 214.

So nehmen Sie eine WAN-Boot-Installation mit lokalen CDs vor

Wenn das Client-OBP keine Unterstützung für WAN-Boot bietet, können Sie die Installation mit der Solaris Software-1 CD im CD-ROM-Laufwerk des Clients durchführen. Bei Verwendung einer lokalen CD ruft der Client das wanboot-Programm nicht vom WAN-Boot-Server, sondern vom lokalen Datenträger ab.

Bei diesem Verfahren wird davon ausgegangen, dass Sie die WAN-Installation per HTTPS vornehmen. Wenn Sie eine unsichere Installation durchführen, zeigen Sie die Client-Schlüssel weder an noch installieren Sie solche.

Für eine WAN-Boot-Installation von einer lokalen CD befolgen Sie die nachfolgende Anleitung.

- Nehmen Sie auf dem WAN-Boot-Server den gleichen Benutzerstatus an wie der Webserver-Benutzer.
- 2 Zeigen Sie für jeden Client den Schlüsselwert an.

wanbootutil keygen -d -c -o net=net-ip,cid=client-ID,type=key-type

- *Netz-IP* Die Netzwerk-IP-Adresse des Clients, auf dem die Installation erfolgen soll.
- *Client-ID* Die ID des Clients, auf dem die Installation erfolgen soll. Die Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.
- Schlüsseltyp Die Art des Schlüssels, der auf dem Client installiert werden soll. Gültige Schlüsseltypen sind 3des, aes und sha1.

Es wird der Hexadezimalwert des Schlüssels angezeigt.

- 3 Wiederholen Sie den vorigen Schritt für jeden Typ der zu installierenden Client-Schlüssel.
- 4 Legen Sie die Solaris Software-1 CD in das CD-ROM-Laufwerk des Clients ein.
- 5 Schalten Sie das Clientsystem ein.
- 6 Booten Sie den Client von der CD.

ok boot cdrom	-o prompt -F wanboot - install
cdrom	Weist das OBP an, von der lokalen CD-ROM zu booten.
-o prompt	Weist das wanboot-Programm an, den Benutzer zur Eingabe von Client-Konfigurationsinformationen aufzufordern.
-F wanboot	Weist das OBP an, das wanboot-Programm von der CD-ROM zu laden.
- install	Weist den Client an, eine WAN-Boot-Installation durchzuführen.

Das OBP des Clients lädt das wanboot-Programm von der Solaris Software-1 CD. Das wanboot-Programm bootet das System, und die Eingabeaufforderung boot> wird angezeigt.

7 Geben Sie den Verschlüsselungswert ein.

boot> 3des=key-value

3des=SchlüsselwertGibt den Hexadezimalwert des in Schritt 2 angezeigten 3DES-Schlüssels
an.

Wenn Sie mit AES-Verschlüsselung arbeiten, verwenden Sie folgendes Format:

boot> aes=key-value

8 Geben Sie den Hashing-Schlüsselwert ein.

boot> sha1=key-value

sha1=Schlüsselwert Gibt den Hexadezimalwert des inSchritt 2 angezeigten Hashing-Schlüssels an.

9 Setzen Sie die Netzwerkschnittstellen-Variablen.

boot> variable=value[,variable=value*]

Geben Sie an der Eingabeaufforderung boot> die folgenden Variablen-Wert-Paare ein.

host-ip= <i>Client-IP</i>	IP-Adresse des Clients
router-ip= <i>Router-IP</i>	IP-Adresse des Netzwerk-Routers
subnet-mask=Maskenwert	Maskenwert des Teilnetzes
hostname= <i>Client-Name</i>	Host-Name des Clients

(Optional) http-proxy= <i>Proxy-IP:Port</i>	Gibt die IP-Adresse und Port-Nummer des Proxy-Servers für das Netzwerk an.
bootserver= <i>wanbootCGI-URL</i>	Gibt die URL des Programms wanboot - cgi auf dem Webserver an.
	Hinweis – Der URL-Wert für die Variable

Sie können diese Variablen mit den folgenden Methoden eingeben:

 Geben Sie an der Eingabeaufforderung boot> ein Variablen-Wert-Paar ein und drücken Sie die Eingabetaste.

muss mit http://beginnen.

boot> host-ip=client-IP
boot> subnet-mask=mask-value

 Geben Sie an der Eingabeaufforderung boot> alle Variablen-Wert-Paare in eine Zeile ein und drücken Sie die Eingabetaste. Trennen Sie die einzelnen Paare durch Kommata voneinander.

```
boot> host-ip=client-IP, subnet-mask=mask-value,
router-ip=router-ip, hostname=client-name,
http-proxy=proxy-ip:port, bootserver=wanbootCGI-URL
```

10 Geben Sie folgenden Befehl ein, um den Boot-Prozess fortzusetzen:

boot> go

Der Client wird über das WAN installiert. Wenn die WAN-Boot-Programme nicht alle erforderlichen Installationsinformationen finden, fordert wanboot Sie zur Eingabe der fehlenden Informationen auf. Geben Sie an der Eingabeaufforderung die benötigten Informationen ein.

Beispiel 13–7 Installation mit lokaler CD

Im folgenden Beispiel wird der Benutzer während der Installation vom wanboot-Programm auf einer lokalen CD dazu aufgefordert, die Netzwerkschnittstellen-Variablen für den Client zu setzen.

Zeigen Sie auf dem WAN-Boot-Server die Schlüsselwerte an.

```
# wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
b482aaab82cb8d5631e16d51478c90079cc1d463
# wanbootutil keygen -d -c -o net=192.168.198.0,cid=010003BA152A42,type=3des
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
```

Dieses Beispiel enthält folgende Informationen:

net=192.168.198.0 Die IP-Adresse des Teilnetzes, in dem sich der Client befindet.

```
cid=010003BA152A42
Die Client-ID.
```

```
b482aaab82cb8d5631e16d51478c90079cc1d463
Den Wert des HMAC SHA1-Hashing-Schlüssels des Clients.
```

```
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
Den Wert der 3DES-Verschlüsselung des Clients.
```

Wenn Sie in Ihrer Installation einen AES-Schlüssel verwenden, müssen Sie type=3des in type=aes ändern, damit der Schlüsselwert angezeigt wird.

Booten Sie den Client und führen Sie die Installation auf ihm durch.

```
ok boot cdrom -o prompt -F wanboot - install
Resetting ...
```

```
Sun Blade 100 (UltraSPARC-IIe), No Keyboard
Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved.
OpenBoot 4.x.build_28, 512 MB memory installed, Serial #50335475.
Ethernet address 0:3:ba:e:f3:75, Host ID: 83000ef3.
```

```
Rebooting with command: boot cdrom -F wanboot - install
Boot device: /pci@lf,0/network@c,1 File and args: -o prompt
```

boot> 3des=9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04

```
boot> sha1=b482aaab82cb8d5631e16d51478c90079cc1d463
```

boot> host-ip=192.168.198.124

boot> subnet-mask=255.255.255.128

boot> router-ip=192.168.198.1

```
boot> hostname=myclient
boot> client-id=010003BA152A42
```

boot> bootserver=http://192.168.198.135/cgi-bin/wanboot-cgi

boot> go

Diese Befehle führen folgende Aktionen durch:

- Einfügen der 3DES-Verschlüsselung mit dem Wert
 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 auf dem Client
- Angabe des HMAC SHA1-Hashing-Schlüssels mit dem Wert b482aaab82cb8d5631e16d51478c90079cc1d463 für den Client

- Die Client-IP-Adresse wird auf 192.168.198.124 gesetzt.
- Die Teilnetzmaske des Clients wird auf 255.255.255.128 gesetzt.
- Die IP-Adresse des Client-Routers wird auf 192.168.198.1gesetzt.
- Der Host-Name des Clients wird auf myclient gesetzt.
- Die Client-ID wird auf 010003BA152A42 gesetzt.
- Die Adresse des wanboot-cgi-Programms wird auf http://192.168.198.135/cgi-bin/wanboot-cgi/gesetzt.

Siehe auch Weitere Informationen zum Anzeigen von Schlüsselwerten finden Sie in wanbootutil(1M). Weitere Informationen zum Einrichten der Netzwerk-Bootargumente finden Sie in set(1). Weitere Informationen zum Booten eines Systems finden Sie in boot(1M).

♦ ♦ ♦ KAPITEL 14

SPARC: Installation mit WAN-Boot (Beispiele)

In diesem Kapitel sehen Sie ein Beispiel für eine Installation von Clientsystemen über ein WAN (Wide Area Network). Die Beispiele in diesem Kapitel zeigen, wie Sie eine sichere WAN-Boot-Installation über eine HTTPS-Verbindung vornehmen können.

- "Konfiguration des Beispielstandorts" auf Seite 240
- "Erstellen des Dokument-Root-Verzeichnisses" auf Seite 241
- "Erzeugen der WAN-Boot-Miniroot" auf Seite 241
- "Überprüfen des Client-OBP auf WAN-Boot-Unterstützung" auf Seite 241
- "Installation des wanboot-Programms auf dem WAN-Boot-Server" auf Seite 242
- "Erstellen Sie die /etc/netboot-Hierarchie." auf Seite 242
- "Kopieren des Programms wanboot cgi auf den WAN-Boot-Server" auf Seite 243
- "(Optional) Konfigurieren des WAN-Boot-Servers als Anmeldeserver" auf Seite 243
- "Konfiguration des WAN-Boot-Servers f
 ür die Verwendung von HTTPS" auf Seite 243
- "Liefern des vertrauenswürdigen Zertifikats an den Client" auf Seite 244
- "(Optional) Einsatz von privatem Schlüssel und Zertifikat zur Client-Authentifizierung" auf Seite 244
- "Erzeugen der Schlüssel für Server und Client" auf Seite 245
- "Erzeugen des Solaris Flash-Archivs" auf Seite 245
- "Erzeugen der Datei sysidcfg" auf Seite 246
- "Erstellen des Client-Profils" auf Seite 246
- "Erzeugen und Überprüfen der Datei rules" auf Seite 247
- "Erzeugen der Systemkonfigurationsdatei" auf Seite 247
- "Erzeugen der Datei wanboot.conf" auf Seite 248
- "Überprüfen des Gerätealias net im OBP" auf Seite 250
- "Installation von Schlüsseln auf dem Client" auf Seite 250
- "Installation des Clients" auf Seite 251

Konfiguration des Beispielstandorts

Abbildung 14–1 zeigt die Standortkonfiguration für dieses Beispiel.



Dieser Beispielstandort weist die folgenden Merkmale auf:

- Der Server wanserver 1 soll gleichzeitig als WAN-Boot- und Installationsserver konfiguriert werden.
- Die IP-Adresse von wanserver-1 lautet 192.168.198.2.
- Der Domain-Name von wanserver-1 lautet www.Beispiel.com.
- Auf wanserver 1 läuft die aktuelle Solaris-Release.
- Auf wanserver-1 läuft der Apache-Webserver. Die Konfiguration der Apache-Software auf wanserver-1 bietet HTTPS-Unterstützung.
- Der zu installierende Client heißt wanclient 1.
- wanclient-1 ist ein UltraSPARCII-System.
- Die Client-ID für wanclient 1 lautet 010003BA152A42.
- Die IP-Adresse von wanclient 1 lautet 192.168.198.210.
- Die IP-Adresse des Client-Teilnetzes lautet 192.168.198.0.
- Das Clientsystem wanclient-1 hat Internet-Zugang, ist aber nicht direkt an das Netzwerk angeschlossen, in dem sich wanserver-1 befindet.
- wanclient-1 ist ein neues System, auf dem aktuelle Solaris-Release installiert werden soll.

Erstellen des Dokument-Root-Verzeichnisses

Legen Sie im Dokument-Root-Verzeichnis (/opt/apache/htdocs) auf wanserver-1 folgende Verzeichnisse zum Speichern der Installationsdateien und -daten an.

Solaris Flash-Verzeichnis

wanserver-1# mkdir -p /opt/apache/htdocs/flash/

WAN-Boot-Miniroot-Verzeichnis

wanserver-1# mkdir -p /opt/apache/htdocs/miniroot/

wanboot-Programmverzeichnis

wanserver-1# mkdir -p /opt/apache/htdocs/wanboot/

Erzeugen der WAN-Boot-Miniroot

Kopieren Sie die WAN-Boot-Miniroot und das Solaris-Software-Abbild mit dem Befehl setup_install_server(1M) und der Option -w in das Verzeichnis /export/install/Solaris_10 von wanserver-1.

Legen Sie den Solaris Software-Datenträger in das an wanserver - 1 angeschlossene Laufwerk ein. Geben Sie die folgenden Befehle ein.

```
wanserver-1# mkdir -p /export/install/cdrom0
wanserver-1# cd /cdrom/cdrom0/Solaris_10/Tools
wanserver-1# ./setup_install_server -w /export/install/cdrom0/miniroot \
/export/install/cdrom0
```

Verschieben Sie die WAN-Boot-Miniroot in das Dokument-Root-Verzeichnis (/opt/apache/htdocs/) des WAN-Boot-Servers.

```
wanserver-1# mv /export/install/cdrom0/miniroot/miniroot \
/opt/apache/htdocs/miniroot/miniroot.s10_sparc
```

Überprüfen des Client-OBP auf WAN-Boot-Unterstützung

Ermitteln Sie, ob im OBP des Clients WAN-Boot-Unterstützung gegeben ist. Geben Sie dazu auf dem Clientsystem folgenden Befehl ein:

```
# eeprom | grep network-boot-arguments
network-boot-arguments: data not available
```

Die Ausgabe network-boot-arguments: data not available im vorigen Beispiel weist darauf hin, dass das Client-OBP WAN-Boot unterstützt.

Installation des wanboot-Programms auf dem WAN-Boot-Server

Zum Installieren des wanboot-Programms auf dem WAN-Boot-Server kopieren Sie das Programm vom Solaris Software-Datenträger in das Dokument-Root-Verzeichnis des WAN-Boot-Servers.

Legen Sie die Solaris-DVD oder die Solaris Software-1 CD in das an wanserver-1 angeschlossene Laufwerk ein, und geben Sie folgende Befehle ein:

wanserver-1# cd /cdrom/cdrom0/Solaris_10/Tools/Boot/platform/sun4u/ wanserver-1# cp wanboot /opt/apache/htdocs/wanboot/wanboot.s10_sparc

Erstellen Sie die /etc/netboot-Hierarchie.

Erzeugen Sie auf dem WAN-Boot-Server die wanclient-1-Unterverzeichnisse für das Verzeichnis /etc/netboot. Während der Installation rufen die WAN-Boot-Installationsprogramme Konfigurations- und Sicherheitsinformationen aus diesem Verzeichnis ab.

wanclient-1befindet sich im Teilnetz 192.168.198.0 und hat die Client-ID 010003BA152A42. Gehen Sie wie folgt vor, um ein entsprechendes Unterverzeichnis in /etc/netboot für wanclient-1 anzulegen.

- Erzeugen Sie das Verzeichnis /etc/netboot.
- Setzen Sie die Berechtigungen für das Verzeichnis /etc/netboot auf 700.
- Setzen Sie den Besitzer des Webserver-Prozesses als Besitzer des Verzeichnisses /etc/netboot.
- Annehmen der Benutzerrolle des Webserver-Benutzers.
- Erzeugen Sie ein Unterverzeichnis in /etc/netboot mit dem Namen des Teilnetzes (192.168.198.0).
- Erzeugen eines Unterverzeichnisses im Teilnetzverzeichnis und benennen nach der Client-ID.
- Setzen Sie die Berechtigungen f
 ür die Unterverzeichnisse von /etc/netboot auf 700.

```
wanserver-1# cd /
wanserver-1# mkdir /etc/netboot/
wanserver-1# chmod 700 /etc/netboot
wanserver-1# chown nobody:admin /etc/netboot
wanserver-1# exit
wanserver-1# su nobody
Password:
nobody# mkdir -p /etc/netboot/192.168.198.0/010003BA152A42
nobody# chmod 700 /etc/netboot/192.168.198.0/
nobody# chmod 700 /etc/netboot/192.168.198.0/
```

Kopieren des Programms wanboot-cgi auf den WAN-Boot-Server

Bei Systemen, die aktuelle Solaris-Release ausführen, befindet sich das wanboot-cgi-Programm im Verzeichnis/usr/lib/inet/wanboot/. Damit der WAN-Boot-Server die Installationsdaten übertragen kann, müssen Sie das Programm wanboot-cgi in das Verzeichnis cgi-bin unter dem Webserver-Software-Verzeichnis kopieren.

```
wanserver-1# cp /usr/lib/inet/wanboot/wanboot-cgi \
/opt/apache/cgi-bin/wanboot-cgi
wanserver-1# chmod 755 /opt/apache/cgi-bin/wanboot-cgi
```

(Optional) Konfigurieren des WAN-Boot-Servers als Anmeldeserver

Standardmäßig werden alle Protokollmeldungen beim WAN-Boot auf dem Clientsystem angezeigt, um eine schnelle Fehlerdiagnose bei Installationsproblemen zu ermöglichen.

Wenn Sie Boot- und Installationsmeldungen auf dem WAN-Boot-Server sehen möchten, kopieren Sie das Skript bootlog-cgi in das Verzeichnis cgi-bin auf wanserver-1.

wanserver-1# cp /usr/lib/inet/wanboot/bootlog-cgi /opt/apache/cgi-bin/ wanserver-1# chmod 755 /opt/apache/cgi-bin/bootlog-cgi

Konfiguration des WAN-Boot-Servers für die Verwendung von HTTPS

Wenn Sie bei den WAN-Boot-Installationen mit HTTPS arbeiten möchten, müssen Sie in der Webserver-Software die SSL-Unterstützung aktivieren. Außerdem müssen Sie auf dem WAN-Boot-Server ein digitales Zertifikat installieren. In diesem Beispiel wird angenommen, dass der Apache-Webserver auf wanserver-1 für die Arbeit mit SSL konfiguriert ist. Des Weiteren wird davon ausgegangen, dass ein digitales Zertifikat und eine Zertifizierungsstelle (CA) zur Bestimmung der Identität von wanserver-1 bereits auf wanserver-1 installiert sind.

Beispiele für die Einstellung der SSL-Unterstützung in der Webserver-Software entnehmen Sie bitte der Dokumentation Ihres Webservers.

Liefern des vertrauenswürdigen Zertifikats an den Client

Indem Sie festlegen, dass sich der Server gegenüber dem Client ausweisen muss, erzielen Sie einen Schutz der Daten, die über HTTPS vom Server an den Client übertragen werden. Zur Server-Authentifizierung liefern Sie dem Client ein vertrauenswürdiges Zertifikat. Auf Grundlage des vertrauenswürdigen Zertifikats kann der Client bei der Installation die Identität des Servers überprüfen.

Um dem Client das vertrauenswürdige Zertifikat zur Verfügung zu stellen, nehmen Sie die Benutzerrolle des Webserver-Benutzers an. Dann teilen Sie das Zertifikat auf und erhalten so das vertrauenswürdige Zertifikat. Fügen Sie dann das vertrauenswürdige Zertifikat in die Datei truststore des Clients in der /etc/netboot-Hierarchie ein.

In diesem Beispiel nehmen Sie die Benutzerrolle nobody an, da dies die Rolle des Webserver-Benutzers ist. Dann teilen Sie das PKCS#12-Serverzertifikat namens cert.p12 auf und fügen das vertrauenswürdige Zertifikat in das Verzeichnis /etc/netboot für wanclient-1 ein.

```
wanserver-1# su nobody
Password:
wanserver-1# wanbootutil p12split -i cert.p12 -t \
/etc/netboot/192.168.198.0/010003BA152A42/truststore
```

(Optional) Einsatz von privatem Schlüssel und Zertifikat zur Client-Authentifizierung

Zum weiteren Schutz Ihrer Daten während der Installation können Sie festlegen, dass sich wanclient-1 gegenüber wanserver-1 authentifizieren muss. Zur Aktivierung der Client-Authentifizierung in der WAN-Boot-Installation fügen Sie ein Client-Zertifikat und einen privaten Schlüssel (private key) in das Client-Unterverzeichnis der /etc/netboot-Hierarchie ein.

Gehen Sie wie folgt vor, um dem Client einen privaten Schlüssel und ein Zertifikat zur Verfügung zu stellen.

- Nehmen Sie die Benutzerrolle des Webserver-Benutzers an.
- Teilen Sie die PKCS#12-Datei in einen privaten Schlüssel und ein Client-Zertifikat auf.
- Fügen Sie das Zertifikat in die Datei certstore des Clients ein.
- Fügen Sie den privaten Schlüssel in die keystore-Datei des Clients ein.

In diesem Beispiel nehmen Sie die Benutzerrolle nobody an, da dies die Rolle des Webserver-Benutzers ist. Dann teilen Sie das PKCS#12-Serverzertifikat namens cert.p12 auf. Sie fügen das Zertifikat in die /etc/netboot-Hierarchie für wanclient-1 ein. Anschließend fügen Sie den als wanclient.key benannten privaten Schlüssel in die keystore-Datei des Clients ein.

```
wanserver-1# su nobody
Password:
wanserver-1# wanbootutil p12split -i cert.p12 -c \
/etc/netboot/192.168.198.0/010003BA152A42/certstore -k wanclient.key
wanserver-1# wanbootutil keymgmt -i -k wanclient.key \
-s /etc/netboot/192.168.198.0/010003BA152A42/keystore \
-o type=rsa
```

Erzeugen der Schlüssel für Server und Client

Zum Schutz der Daten, die zwischen Server und Client übertragen werden, erzeugen Sie einen Hashing-Schlüssel und eine Verschlüsselung (d. h. einen Chiffrierschlüssel). Mit dem Hashing-Schlüssel schützt der Server die Integrität des Programms wanboot. Den Chiffrierschlüssel verwendet der Server zum Verschlüsseln der Konfigurations- und Installationsdaten. Mit dem Hashing-Schlüssel prüft der Client die Integrität des heruntergeladenen wanboot-Programms. Der Chiffrierschlüssel dient außerdem dem Client zum Entschlüsseln der Daten bei der Installation.

Nehmen Sie zunächst die Benutzerrolle des Webserver-Benutzers an. In diesem Beispiel die Benutzerrolle nobody.

wanserver-1# **su nobody** Password:

Generieren Sie dann mit dem Befehl wanbootutil keygen einen HMAC SHA1-Hauptschlüssel für wanserver-1.

wanserver-1# wanbootutil keygen -m

Erzeugen Sie dann einen Hashing-Schlüssel und eine Verschlüsselung für wanclient-1.

wanserver-1# wanbootutil keygen -c -o net=192.168.198.0,cid=010003BA152A42,type=sha1
wanserver-1# wanbootutil keygen -c -o net=192.168.198.0,cid=010003BA152A42,type=3des

Der vorige Befehl generiert einen HMAC SHA1-Hashing-Schlüssel und eine 3DES-Verschlüsselung für wanclient-1. 192.168.198.0 ist das Teilnetz von wanclient-1, 010003BA152A42 die Client-ID von wanclient-1.

Erzeugen des Solaris Flash-Archivs

In diesem Beispiel erzeugen Sie ein Solaris Flash-Archiv, indem Sie das wanserver-1-Master-System klonen. Das Archiv erhält den Namen sol_10_sparc und wird 1:1 vom Master-System kopiert. Es stellt ein exaktes Duplikat des Master-Systems dar. Das fertige Archiv wird in sol_10_sparc.flar gespeichert. Sie speichern das Archiv im Unterverzeichnis flash/archives des Dokument-Root-Verzeichnisses auf dem WAN-Boot-Server.

```
wanserver-1# flarcreate -n sol_10_sparc \
/opt/apache/htdocs/flash/archives/sol_10_sparc.flar
```

Erzeugen der Datei sysidcfg

Für die Vorkonfiguration des Systems wanclient-1 geben Sie in der Datei sysidcfg Schlüsselwörter und Werte an. Speichern Sie diese Datei im passenden Unterverzeichnis des Dokument-Root-Verzeichnisses auf wanserver-1.

BEISPIEL 14-1 sysidcfg-Datei für das System client-1

Das folgende Beispiel zeigt eine mögliche sysidcfg-Datei für wanclient-1. Host-Name, IP-Adresse und Netzmaske dieser Systeme wurden durch Bearbeitung des Naming Service vorkonfiguriert. Diese Datei befindet sich im Verzeichnis /opt/apache/htdocs/flash/.

Erstellen des Client-Profils

Erstellen Sie für das System wanclient-1 ein Profil namens wanclient_1_prof. Die Datei wanclient_1_prof enthält die folgenden Einträge, die definieren, wie die 10 9/10-Software auf dem System wanclient-1 installiert werden soll.

profile values
flash_install
https://192.168.198.2/flash/archives/cdrom0.flar
explicit
c0t1d0s0 4000 /
c0t1d0s1 512 swap
c0t1d0s7 free /export/home

In der folgenden Liste sind einige Schlüsselwörter und Werte aus diesem Beispiel beschrieben.

install_type	Das Profil installiert ein Solaris Flash-Archiv auf dem Klonsystem. Wie bei einer Erst- bzw. Neuinstallation werden alle Dateien überschrieben.
archive_location	Das komprimierte Solaris Flash-Archiv wird von wanserver-1 abgerufen.

partitioning Mit dem Wert explicit legen Sie fest, dass die Dateisystem-Slices von den filesys-Schlüsselwörtern definiert werden. Die Größe von Root (/) ist von der Größe des Solaris Flash-Archivs abhängig. Der swap-Bereich wird auf c0tld0s1 angelegt und seine Größe nach Bedarf automatisch festgelegt. /export/home ist vom verbleibenden Speicherplatz abhängig. /export/home wird auf c0tld0s7 angelegt.

Erzeugen und Überprüfen der Datei rules

Aus der Datei rules wählen die Programme für die benutzerdefinierte JumpStart-Installation das richtige Profil für das System wanclient-1 aus. Erzeugen Sie eine Textdatei namens rules. Fügen Sie dann Schlüsselwörter und Werte in diese Datei ein.

Die IP-Adresse von wanclient - 1 lautet 192.168.198.210, die Netzmaske 255.255.255.0. Mit dem Schlüsselwort network geben Sie an, welches Profil die Programme für die benutzerdefinierte JumpStart-Installation zur Installation von wanclient - 1 verwenden sollen.

network 192.168.198.0 - wanclient_1_prof -

Die rules-Datei legt damit fest, dass die Programme für die benutzerdefinierte JumpStart-Installation das Profil wanclient_1_prof verwenden sollen, um die aktuelle Solaris-Release-Software auf wanclient-1 zu installieren.

Nennen Sie diese Datei wanclient_rule.

Wenn Sie das Profil und die rules-Datei erzeugt haben, führen Sie das check-Skript aus, um die Gültigkeit der Dateien zu überprüfen.

wanserver-1# ./check -r wanclient_rule

Wenn das Skript check keine Fehler findet, erstellt es die Datei rules.ok.

Speichern Sie die Datei rules.ok im Verzeichnis/opt/apache/htdocs/flash/.

Erzeugen der Systemkonfigurationsdatei

Erzeugen Sie eine Systemkonfigurationsdatei, in der die Adresse der Datei sysidcfg und der JumpStart-Dateien auf dem Installationsserver angegeben sind. Speichern Sie diese Datei in einem für den WAN-Boot-Server zugänglichen Verzeichnis.

In folgendem Beispiel sucht das Programm wanboot - cgi die Datei sysidcfg und die JumpStart-Dateien im Dokument-Root-Verzeichnis des WAN-Boot-Servers. Der

Domain-Name des WAN-Boot-Servers lautet https://www.Beispiel.com.Der WAN-Boot-Server ist für die Verwendung von sicherem HTTP konfiguriert, so dass die Daten und Dateien bei der Installation geschützt sind.

In diesem Beispiel lautet der Name der Systemkonfigurationsdatei sys-conf.s10–sparc, und die Datei wurde in der /etc/netboot-Hierarchie des WAN-Boot-Servers gespeichert. Die Datei sysidcfg und die JumpStart-Dateien befinden sich im Unterverzeichnis flash des Dokument-Root-Verzeichnisses.

SsysidCF=https://www.example.com/flash/ SjumpsCF=https://www.example.com/flash/

Erzeugen der Datei wanboot.conf

Bei der Installation des Clientsystems greift WAN-Boot auf die Konfigurationsinformationen in der Datei wanboot.conf zurück. Erzeugen Sie die Datei wanboot.conf in einem Texteditor. Speichern Sie die Datei im entsprechenden Client-Unterverzeichnis der /etc/netboot-Hierarchie auf dem WAN-Boot-Server.

Die folgende wanboot.conf-Datei für wanclient-1 enthält Konfigurationsinformationen für eine WAN-Installation, die sicheres HTTP verwendet. Die Datei bestimmt außerdem, dass die Daten bei der WAN-Boot-Installation mit einem HMAC SHA1-Hashing-Schlüssel und einer 3DES-Verschlüsselung zu schützen sind.

```
boot_file=/wanboot/wanboot.s10_sparc
root_server=https://www.example.com/cgi-bin/wanboot-cgi
root_file=/miniroot/miniroot.s10_sparc
signature_type=sha1
encryption_type=3des
server_authentication=yes
client_authentication=no
resolve_hosts=
boot_logger=
system_conf=sys-conf.s10-sparc
```

Aus dieser wanboot.conf-Datei ergibt sich die folgende Konfiguration:

boot_file=/wanboot/wanboot.s10_sparc

Das wanboot-Programm heißt wanboot.s10_sparc. Dieses Programm befindet sich im Verzeichnis wanboot des Dokument-Root-Verzeichnisses auf wanserver-1.

root_server=https://www.example.com/cgi-bin/wanboot-cgi

Die Adresse des Programms wanboot-cgi auf wanserver-1 lautet https://www.Beispiel.com/cgi-bin/wanboot-cgi. Der https-Teil der URL gibt an, dass diese WAN-Boot-Installation mit sicherem HTTP vorgenommen wird. root_file=/miniroot/miniroot.s10_sparc

Die WAN-Boot-Miniroot heißt miniroot.s10_sparc. Die Miniroot befindet sich im Verzeichnis miniroot des Dokument-Root-Verzeichnisses auf wanserver-1.

signature_type=sha1

Das wanboot-Programm und das WAN-Boot-Dateisystem werden mit einem HMAC SHA1-Hashing-Schlüssel signiert.

encryption_type=3des

Das wanboot-Programm und das WAN-Boot-Dateisystem werden mit einem 3DES-Schlüssel chiffriert.

server_authentication=yes

Der Server wird bei der Installation authentifiziert.

client_authentication=no

Der Client wird bei der Installation nicht authentifiziert.

Hinweis – Wenn Sie die unter "(Optional) Einsatz von privatem Schlüssel und Zertifikat zur Client-Authentifizierung" auf Seite 244 beschriebenen Schritte ausgeführt haben, setzen Sie diesen Parameter auf client_authentication=yes.

resolve_hosts=

Es werden keine zusätzlichen Host-Namen für die WAN-Boot-Installation benötigt. Alle Host-Namen, die das Programm wanboot - cgi benötigt, sind in der Datei wanboot . conf und im Client-Zertifikat angegeben.

boot_logger=

Boot- und Installations-Protokollmeldungen werden auf der Systemkonsole angezeigt. Wenn Sie den Protokollserver in "(Optional) Konfigurieren des WAN-Boot-Servers als Anmeldeserver" auf Seite 243 konfiguriert haben und die WAN-Boot-Meldungen auch auf dem WAN-Boot-Server angezeigt werden sollen, setzen Sie diesen Parameter auf boot_logger=https://www.Beispiel.com/cgi-bin/bootlog-cgi.

system_conf=sys-conf.s10-sparc

Die Systemkonfigurationsdatei, in der die Speicherorte der sysidcfg- und JumpStart-Dateien angegeben werden, befindet sich in der Datei sys-conf.s10–sparc in der /etc/netboot-Hierarchie auf wanserver-1.

In diesem Beispiel wurde die Datei wanboot.conf im Verzeichnis /etc/netboot/192.168.198.0/010003BA152A42 auf wanserver-1 gespeichert.

Überprüfen des Gerätealias net im OBP

Zum Booten des Clients aus dem WAN mit dem Befehl boot net muss der Gerätealias net auf das primäre Netzwerkgerät des Clients gesetzt werden. Geben Sie an der Eingabeaufforderung ok des Clients den Befehl devalias ein, und prüfen Sie, ob der Aliasname net auf das primäre Netzwerkgerät/pci@lf,0/pci@l,1/network@c,1 gesetzt ist.

/pci@lf,0/pci@l,1/SUNW,m64B@2
/pci@lf,0/pci@l,1/network@c,1
/pci@lf,0/pci@l,1/network@5,1
/pci@lf,0/pci@l/scsi@8/disk@0,0
/pci@lf,0/pci@l,1/ide@d/cdrom@0,0:f
/pci@lf,0/pci@l,1/ebus@l/su@l4,3083f8
/pci@lf,0/pci@l,1/ebus@l/su@l4,3062f8

In dieser Beispielausgabe ist dem Alias net das primäre Netzwerkgerät /pci@lf,0/pci@l,1/network@c,1zugewiesen. Sie müssen ihn also nicht ändern.

Installation von Schlüsseln auf dem Client

In "Erzeugen der Schlüssel für Server und Client" auf Seite 245 haben Sie einen Hashing-Schlüssel und eine Verschlüsselung (den Chiffrierschlüssel) zum Schutz der Daten während der Installation erzeugt. Diese Schlüssel müssen auf wanclient-1 installiert werden, damit der Client die von wanclient-1 übertragenen Daten entschlüsseln kann.

Zeigen Sie auf wanserver-1 die Schlüsselwerte an.

```
wanserver-1# wanbootutil keygen -d -c -o net=192.168.198.0, cid=010003BA152A42, type=sha1
b482aaab82cb8d5631e16d51478c90079cc1d463
wanserver-1# wanbootutil keygen -d -c -o net=192.168.198.0, cid=010003BA152A42, type=3des
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
```

Dieses Beispiel enthält folgende Informationen:

net=192.168.198.0 Die IP-Adresse des Teilnetzes, in dem sich der Client befindet.

```
cid=010003BA152A42
Die Client-ID.
```

```
b482aaab82cb8d5631e16d51478c90079cc1d463
Den Wert des HMAC SHA1-Hashing-Schlüssels des Clients.
```

```
9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
Den Wert der 3DES-Verschlüsselung des Clients.
```

Wenn Sie in Ihrer Installation einen AES-Schlüssel verwenden, müssen Sie type=3des in type=aes ändern, damit der Schlüsselwert angezeigt wird.

Installieren Sie die Schlüssel an der Befehlseingabe ok auf wanclient-1.

```
ok set-security-key wanboot-hmac-sha1 b482aaab82cb8d5631e16d51478c90079cc1d463
ok set-security-key wanboot-3des 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04
```

Diese Befehle führen folgende Aktionen durch:

- Installation des HMAC SHA1-Hashing-Schlüssels mit dem Wert b482aaab82cb8d5631e16d51478c90079cc1d463 auf wanclient-1
- Installation der 3DES-Verschlüsselung mit dem Wert 9ebc7a57f240e97c9b9401e9d3ae9b292943d3c143d07f04 auf wanclient-1

Installation des Clients

Sie können eine ungeführte Installation durchführen, indem Sie an der Eingabeaufforderung ok die Netzwerk-Boot-Variablen für wanclient-1 setzen und den Client dann booten.

```
ok setenv network-boot-arguments host-ip=192.168.198.210,
router-ip=192.168.198.1,subnet-mask=255.255.255.0,hostname=wanclient-1,
file=http://192.168.198.2/cgi-bin/wanboot-cgi
ok boot net - install
Resetting ...
```

```
Sun Blade 100 (UltraSPARC-IIe), No Keyboard
Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved.
OpenBoot 4.x.build_28, 512 MB memory installed, Serial #50335475.
Ethernet address 0:3:ba:e:f3:75, Host ID: 83000ef3.
```

```
Rebooting with command: boot net - install
Boot device: /pci@lf,0/network@c,1 File and args: - install
```

```
<time unavailable> wanboot progress: wanbootfs: Read 68 of 68 kB (100%)
<time unavailable> wanboot info: wanbootfs: Download complete
Fri Jun 20 09:16:06 wanboot progress: miniroot: Read 166067 of 166067 kB (100%)
Fri Jun 20Tue Apr 15 09:16:06 wanboot info: miniroot: Download complete
SunOS Release 5.10 Version WANbootl0:04/11/03 64-bit
Copyright 1983-2003 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
Configuring devices.
```

Es werden die folgenden Variablen gesetzt:

- Die IP-Adresse des Clients wird auf 192.168.198.210 gesetzt.
- Die IP-Adresse des Client-Routers wird auf 192.168.198.1 gesetzt.
- Die Teilnetzmaske des Clients wird auf 255.255.255.0 gesetzt.

- Der Host-Name des Clients wird auf wanclient 1 gesetzt.
- Das Programm wanboot-cgi befindet sich unter http://192.168.198.2/cgi-bin/wanboot-cgi.

Der Client wird über das WAN installiert. Wenn das wanboot-Programm nicht alle erforderlichen Installationsinformationen findet, werden Sie möglicherweise dazu aufgefordert, die fehlenden Informationen an der Befehlszeile einzugeben.
• • • KAPITEL 15

WAN-Boot (Referenz)

Dieses Kapitel bietet eine kurze Darstellung der Befehle und Dateien, die bei einer WAN-Installation eingesetzt werden.

- "Befehle f
 ür die WAN-Boot-Installation" auf Seite 253
- "OBP-Befehle" auf Seite 256
- Einstellungen und Syntax der Systemkonfigurationsdatei" auf Seite 257
- "Parameter der Datei wanboot.conf und Syntax" auf Seite 258

Befehle für die WAN-Boot-Installation

In den folgenden Tabellen sind die Befehle beschrieben, die Sie bei einer WAN-Boot-Installation verwenden.

- Tabelle 15–1
- Tabelle 15–2

TABELLE 15–1 Vorbereitung der WAN-Boot-Installations- und Konfigurationsdateien

Schritt und Beschreibung	Befehl
Solaris-Installationsabbild nach <i>Inst_verz_pfad</i> und die WAN-Boot-Miniroot nach <i>WAN_verz_pfad</i> auf der Festplatte des Installationsservers kopieren	setup_install_server —w WAN_verz_pfad Inst_verz_pfad

Schritt und Beschreibung	Befehl
Ein Solaris Flash-Archiv mit dem Namen <i>Name</i> . flar erzeugen <i>Name</i> ist der Name des Archivs.	flarcreate – n Name [optionale-Parameter] Dokument-Root/flash/Dateiname
 optionale_Parameter sind optionale Parameter f ür die Anpassung des Archivs. 	
 Dokument-Root ist der Pfad zum Dokument-Root-Verzeichnis auf dem Installationsserver. 	
 Dateiname ist der Name des Archivs. 	
Gültigkeit der rules-Datei mit dem Namen <i>Regeln</i> für die benutzerdefinierte JumpStart-Installation überprüfen	./check -r <i>Regeln</i>
 Gültigkeit der Datei wanboot.conf überprüfen <i>Netz-IP</i> ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	<pre>bootconfchk /etc/netboot/Netz-IP/Client-ID/wanboot.conf</pre>
 Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	
Unterstützung für WAN-Boot im Client-OBP überprüfen	eeprom grep network-boot-arguments

 TABELLE 15-1
 Vorbereitung der WAN-Boot-Installations- und Konfigurationsdateien
 (Fortsetzung)

 TABELLE 15-2
 Vorbereitung der WAN-Boot-Sicherheitsdateien

Schritt und Beschreibung	Befehl
HMAC SHA1-Masterschlüssel für den WAN-Boot-Server erzeugen	wanbootutil keygen -m
 HMAC SHA1-Hashing-Schlüssel für den Client erzeugen <i>Netz-IP</i> ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	wanbootutil keygen -c -o net= <i>Netz-IP</i> ,cid= <i>Client-ID</i> ,type=sha1
 Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	

Schritt und Beschreibung	Befehl
 Chiffrierschlüssel für den Client erzeugen Netz-IP ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	wanbootutil keygen -c -o net= <i>Netz-IP</i> ,cid= <i>Client-ID</i> ,type= <i>Schlüsseltyp</i>
 Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	
 Schlüsseltyp ist entweder 3des oder aes. 	
Eine PKCS#12-Zertifikatdatei aufteilen und das Zertifikat in die truststore-Datei des Clients einfügen	<pre>wanbootutil p12split -i P12Zert -t /etc/netboot/Netz-IP/Client-ID/truststore</pre>
 <i>p12cert</i> ist der Name der PKCS#12-Zertifikatdatei. 	
 Netz-IP ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	
• <i>Client-ID</i> kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein.	
Eine PKCS#12-Zertifikatdatei aufteilen und das Client-Zertifikat in die certstore-Datei des Clients einfügen <i>pl2cert</i> ist der Name der	wanbootutil p12split -i <i>p12cert</i> -c /etc/netboot/ <i>Netz-IP/Client-ID</i> /certstore -k <i>Schlüsseldatei</i>
PKCS#12-Zertifikatdatei.	
 Netz-IP ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	
 <i>Client-ID</i> kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	
 Schlüsseldatei ist der Name des privaten Schlüssels des Clients. 	
 Den privaten Schlüssel des Clients aus einer aufgeteilten PKCS#12-Datei in die keystore-Datei des Clients einfügen Schlüsseldatei ist der Name des privaten Schlüssels des Clients. 	wanbootutil keymgmt -i -k <i>Schlüsseldatei</i> -s /etc/netboot/ <i>Netz-IP/Client-ID</i> /keystore -o type=rsa
 Netz-IP ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	
 Client-ID kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	

Schritt und Beschreibung	Befehl
 Den Wert eines HMAC SHA1-Hashing-Schlüssels anzeigen <i>Netz-IP</i> ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	wanbootutil keygen -d -c -o net= <i>Netz-IP</i> ,cid= <i>Client-ID</i> ,type=shal
 <i>Client-ID</i> kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	
 Einen Verschlüsselungswert anzeigen <i>Netz-IP</i> ist die IP-Adresse des Teilnetzes, in dem sich der Client befindet. 	<pre>wanbootutil keygen -d -c -o net=Netz-IP,cid= Client-ID,type=Schlüsseltyp</pre>
 <i>Client-ID</i> kann eine benutzerdefinierte oder die per DHCP zugewiesene Client-ID sein. 	
• <i>Schlüsseltyp</i> ist entweder 3des oder aes.	
Einen Hashing-Schlüssel oder eine Verschlüsselung auf einem laufenden System einfügen. <i>Schlüsseltyp</i> kann einen der Werte sha1, 3des und aes aufweisen.	/usr/lib/inet/wanboot/ickey -o type= <i>Schlüsseltyp</i>

- . - a. 1 . <u>___</u>

OBP-Befehle

In der folgenden Tabelle sind die OBP-Befehle aufgeführt, die Sie für eine WAN-Boot-Installation an der Eingabeaufforderung ok auf dem Client eingeben können.

Schritt und Beschreibung	OBP-Befehl
Eine ungeführte WAN-Boot-Installation beginnen	boot net – install
Eine interaktive WAN-Boot-Installation beginnen	boot net —o prompt - install
Eine WAN-Boot-Installation von einer lokalen CD beginnen	boot cdrom –F wanboot - install
Installieren Sie vor dem Beginn der WAN-Boot-Installation einen Hashing-Schlüssel. <i>Schlüsselwert</i> ist der hexadezimale Wert des Hashing-Schlüssels.	set-security-key wanboot-hmac-sha1 <i>Schlüsselwert</i>

Schritt und Beschreibung	OBP-Befehl
 Vor Beginn einer WAN-Boot-Installation eine Verschlüsselung installieren Schlüsseltyp ist entweder wanboot - 3des oder wanboot - aes. Schlüsselwert ist der Hexadezimalwert der Verschlüsselung. 	set-security-key Schlüsseltyp Schlüsselwert
Überprüfen, ob Schlüsselwerte im OBP gesetzt sind	list-security-keys
 Vor Beginn der WAN-Boot-Installation Client-Konfigurationsvariablen setzen <i>Client-IP</i> ist die IP-Adresse des Clients. <i>Router-IP</i> ist die IP-Adresse des Netzwerk-Routers. <i>Maskenwert</i> ist der Wert der Teilnetzmaske. <i>Client-Name</i> ist der Host-Name des Clients. <i>Proxy-IP</i> ist die IP-Adresse des Proxy-Servers im Netzwerk. <i>wanbootCGI-Pfad</i> ist der Pfad zu den wanbootCGI-Programmen auf dem Webserver. 	<pre>setenv network-boot-arguments host-ip= Client-IP,router-ip=Router-IP,subnet-mask= Maskenwert,hostname=Clientname ,http-proxy=Proxy-IP,file=WanbootCGI-Pfad</pre>
Netzwerkgerät-Alias überprüfen	devalias
Den Netzwerkgerät-Alias festlegen, wobei <i>Gerätepfad</i> der Pfad zum primären Netzwerkgerät ist.	 Um den Alias nur für die aktuelle Installation zu setzen, geben Sie devalias net <i>Gerätepfad</i> ein. Um den Alias dauerhaft zu setzen, geben Sie nyvalias net <i>Gerätepfad</i> ein.

... c 1 1 c ...

Einstellungen und Syntax der Systemkonfigurationsdatei

Mit der Systemkonfigurationsdatei leiten Sie die WAN-Boot-Installationsprogramme zu den folgenden Dateien:

- sysidcfg
- rules.ok
- Profil für die benutzerdefinierte JumpStart-Installation

Bei der Systemkonfigurationsdatei handelt es sich um eine Normaltextdatei, die nach diesem Muster formatiert sein muss:

setting=value

Die Datei system. conf muss die folgenden Einstellungen enthalten:

SsysidCF=sysidcfg-Datei-URL

Diese Einstellung verweist auf das Verzeichnis auf dem Installationsserver, in dem sich die Datei sysidcfg befindet. Für WAN-Installationen per HTTPS ist der Wert auf eine gültige HTTPS-URL zu setzen.

SjumpsCF=jumpstart-Dateien-URL

Diese Einstellung verweist auf das JumpStart-Verzeichnis, das die Datei rules.ok und die Profildateien enthält. Für WAN-Installationen per HTTPS ist der Wert auf eine gültige HTTPS-URL zu setzen.

Die Datei system. conf kann in jedem für den WAN-Boot-Server zugänglichen Verzeichnis gespeichert werden.

Parameter der Datei wanboot.conf und Syntax

Die Datei wanboot.conf ist eine Konfigurationsdatei im Textformat, auf welche die WAN-Boot-Installationsprogramme für die Durchführung einer WAN-Installation zugreifen. Bei der Installation des Clientsystems greifen die folgenden Programme und Dateien auf die Informationen in der Datei wanboot.conf zurück:

- Programm wanboot cgi
- WAN-Boot-Dateisystem
- WAN-Boot-Miniroot

Speichern Sie die Datei wanboot. conf im entsprechenden Client-Unterverzeichnis der /etc/netboot-Hierarchie auf dem WAN-Boot-Server. Wie Sie den Aktionsbereich für Ihre WAN-Boot-Installation in der /etc/netboot-Hierarchie festlegen, erfahren Sie in "Erstellen der /etc/netboot-Hierarchie auf dem WAN-Boot-Server" auf Seite 186.

Zur Angabe von Informationen in der Datei wanboot . conf führen Sie Parameter und die dazugehörigen Werte in folgendem Format auf:

parameter=value

Parametereinträge dürfen sich nicht über mehrere Zeilen erstrecken. Durch Voranstellen des Zeichens # können Sie Kommentare in die Datei einfügen.

Ausführliche Informationen über die Datei wanboot.conf finden Sie in der Manpage wanboot.conf(4).

In der Datei wanboot.conf müssen die folgenden Parameter gesetzt werden:

boot_file=Wanboot-Pfad

Mit diesem Parameter geben Sie den Pfad zum wanboot-Programm an. Der Wert besteht in einem Pfad, der relativ zum Dokument-Root-Verzeichnis auf dem WAN-Boot-Server ist.

boot_file=/wanboot/wanboot.s10_sparc

root_server=WanbootCGI-URL/wanboot-cgi

Mit diesem Parameter geben Sie die URL des Programms wanboot-cgi auf dem WAN-Boot-Server an.

• Für eine WAN-Boot-Installation ohne Client- oder Server-Authentifizierung geben Sie eine HTTP-URL an.

root_server=http://www.example.com/cgi-bin/wanboot-cgi

 Verwenden Sie eine HTTPS-URL, wenn Sie eine WAN-Boot-Installation mit Serveroder mit Server- und Client-Authentifizierung durchführen.

root_server=https://www.example.com/cgi-bin/wanboot-cgi

root_file=Miniroot-Pfad

Mit diesem Parameter geben Sie den Pfad zur WAN-Boot-Miniroot auf dem WAN-Boot-Server an. Der Wert besteht in einem Pfad, der relativ zum Dokument-Root-Verzeichnis auf dem WAN-Boot-Server ist.

root_file=/miniroot/miniroot.sl0_sparc

signature_type=sha1 | leer

Mit diesem Parameter geben Sie den Typ des für die Integritätsprüfung der übertragenen Daten und Dateien einzusetzenden Hashing-Schlüssels an.

 Für WAN-Boot-Installationen, bei welchen das wanboot-Programm durch einen Hashing-Schlüssel geschützt werden soll, setzen Sie diesen Wert auf sha1.

signature_type=sha1

Für unsichere WAN-Installationen ohne Hashing-Schlüssel lassen Sie diesen Wert leer.

signature_type=

encryption_type=3des | aes | leer

Mit diesem Parameter geben Sie den gewünschten Chiffrierschlüsseltyp für die Verschlüsselung des wanboot-Programms und des WAN-Boot-Dateisystems an.

 Für WAN-Boot-Installationen per HTTPS setzen Sie diesen Wert auf 3des oder aes, je nachdem, welches Schlüsselformat Sie verwenden. Außerdem muss der Wert des Schlüsselworts signature type auf shal gesetzt werden.

encryption_type=3des

oder

encryption_type=aes

 Wenn Sie eine unsichere WAN-Boot-Installation ohne Verschlüsselung durchführen möchten, lassen Sie diesen Wert leer.

encryption_type=

server_authentication=yes | no

Mit diesem Parameter geben Sie an, ob bei der WAN-Boot-Installation eine Server-Authentifizierung stattfinden soll.

 Für WAN-Boot-Installationen mit Server- oder mit Server- und Client-Authentifizierung setzen Sie diesen Wert auf yes. Außerdem müssen Sie den Wert von signature_type auf sha1, von encryption_type auf 3des oder aes und die URL von root_server auf einen HTTPS-Wert setzen.

server_authentication=yes

 Für unsichere WAN-Boot-Installationen ohne Server- oder Server- und Client-Authentifizierung setzen Sie diesen Wert auf no. Sie können den Wert auch leer lassen.

server_authentication=no

client_authentication=yes | no

Mit diesem Parameter geben Sie an, ob bei der WAN-Boot-Installation eine Client-Authentifizierung stattfinden soll.

 Für WAN-Boot-Installationen mit Server- und Client-Authentifizierung setzen Sie diesen Wert auf yes. Außerdem müssen Sie den Wert von signature_type auf sha1, von encryption_type auf 3des oder aes und die URL von root_server auf einen HTTPS-Wert setzen.

client_authentication=yes

• Für WAN-Boot-Installationen ohne Client-Authentifizierung setzen Sie diesen Wert auf no. Sie können den Wert auch leer lassen.

client_authentication=no

resolve_hosts=Hostname | leer

Mit diesem Parameter geben Sie weitere Host-Namen an, die während der Installation für das Programm wanboot-cgi aufgelöst werden müssen.

Setzen Sie diesen Wert auf die Host-Namen der Systeme, die in der Datei wanboot . conf oder einem etwaigen Client-Zertifikat noch nicht angegeben wurden.

 Wenn alle erforderlichen Hosts bereits in der Datei wanboot.conf oder dem Client-Zertifikat aufgeführt sind, lassen Sie diesen Wert leer.

resolve_hosts=

 Wenn bestimmte Systeme in der Datei wanboot. conf oder dem Client-Zertifikat nicht aufgeführt sind, setzen Sie diesen Wert auf die Host-Namen dieser Systeme.

```
resolve_hosts=seahag,matters
```

boot_logger=bootlog-cgi-Pfad | leer

Mit diesem Parameter geben Sie die URL des Skripts bootlog-cgi auf dem Protokollserver an.

 Um Boot- oder Installationsprotokollmeldungen auf einem speziellen Protokollserver aufzeichnen zu lassen, setzen Sie den Wert auf die URL des Skripts bootlog-cgi auf dem Protokollserver.

boot_logger=http://www.example.com/cgi-bin/bootlog-cgi

• Wenn die Boot- und Installationsmeldungen auf der Client-Konsole angezeigt werden sollen, lassen Sie diesen Wert leer.

boot_logger=

system_conf=system.conf | benutzerspezif-Systemkonf

Mit diesem Parameter geben Sie den Pfad zu der Systemkonfigurationsdatei an, in der die Adressen der Datei sysidcfg und der JumpStart-Dateien zu finden sind.

Setzen Sie den Wert dieses Pfads auf die Datei sysidofg und die JumpStart-Dateien auf dem Webserver.

system_conf=sys.conf

TEIL IV

Anhänge

Dieser Teil enthält Referenzinformationen.

◆ ◆ ◆ ANHANG /

Fehlerbehebung (Vorgehen)

Dieses Kapitel enthält eine Liste spezifischer Fehlermeldungen und allgemeiner Probleme, die beim Installieren der Solaris 10 9/10-Software auftreten könnten. In diesem Kapitel wird außerdem erläutert, wie Sie Probleme beheben können. Die Erläuterungen in diesem Kapitel sind in die folgenden Abschnitte eingeteilt, je nachdem, wo im Installationsprozess das Problem auftrat.

- Probleme beim Einrichten von Netzwerkinstallationen" auf Seite 265
- "Probleme beim Booten eines Systems" auf Seite 266
- "Neuinstallation von Solaris" auf Seite 272
- "Upgrade von Solaris" auf Seite 274

Hinweis – Der Text "bootable media" bezieht sich auf das Solaris-Installationsprogramm und die JumpStart-Installationsmethode.

Probleme beim Einrichten von Netzwerkinstallationen

Unbekannter Client "Host-Name"

Grund: Das Argument *Host-Name* im Befehl add_install_client bezieht sich nicht auf einen Host in diesem Naming Service.

Lösung: Fügen Sie den Host *Host-Name* zum Naming Service hinzu und führen Sie den Befehl add_install_client erneut aus.

Fehler: <system name> ist in der NIS ethers Map nicht vorhanden

Fügen Sie ihn hinzu, und führen Sie den Befehl add_install_client erneut aus. Beschreibung: Beim Ausführen von add_install_client schlägt der Befehl mit der oben aufgeführten Fehlermeldung fehl.

Grund: Der Client, den Sie zum Installationsserver hinzufügen, ist in der Datei /etc/ethers des Servers nicht vorhanden.

Lösung: Fügen Sie die erforderlichen Informationen zur Datei /etc/ethers auf dem Installationsserver hinzu, und führen Sie den Befehl add install client erneut aus.

1. Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. Suchen Sie die ethers-Adresse auf dem Client.

```
# ifconfig -a grep ethers
ether 8:0:20:b3:39:1d
```

- 3. Öffnen Sie die /etc/ethers-Datei in einem Editor auf dem Installationsserver. Fügen Sie die Adresse der Liste hinzu.
- 4. Führen Sie erneut den Befehl add_install_client auf dem Client aus.
 - # ./add_install_client bluegill sun4u

Probleme beim Booten eines Systems

Booten von Medien, Fehlermeldungen

le0: No carrier - transceiver cable problem
Grund: Das System ist nicht mit dem Netzwerk verbunden.

Lösung: Handelt es sich hierbei um ein nicht vernetztes System, ignorieren Sie diese Meldung. Handelt es sich um ein vernetztes System, vergewissern Sie sich, dass die Ethernet-Verkabelung stimmt.

Die gerade geladene Datei scheint nicht ausführbar zu sein Grund: Das System findet das richtige Medium zum Booten nicht.

Lösung: Überprüfen Sie, ob das System ordnungsgemäß für die Installation der Solaris 10 9/10-Software über das Netzwerk von einem Installationsserver aus eingerichtet wurde. Sie können beispielsweise folgende Überprüfungen durchführen:

- Wenn Sie die Abbilder der Solaris-DVD oder der Solaris Software-CDs auf den Installationsserver kopiert haben, vergewissern Sie sich, dass Sie bei der Einrichtung die richtige Plattformgruppe des Systems angegeben haben.
- Wenn Sie mit DVD oder CD vorgehen, vergewissern Sie sich, dass die Solaris-DVD bzw. Solaris Software-1 CD eingehängt und auf dem Installationsserver zugänglich ist.

boot: cannot open <Dateiname> (nur SPARC-Systeme)

Grund: Dieser Fehler tritt auf, wenn Sie den Speicherort von boot - file für das Booten überschreiben, indem Sie diesen explizit angeben.

Hinweis - Dateiname ist eine Variable für den Namen der betreffenden Datei.

Lösung: Gehen Sie wie folgt vor:

- Setzen Sie boot file im PROM auf "" (leer).
- Stellen Sie sicher, dass "diag-switch" auf "off" und auf "true" gesetzt ist.

Kann von Datei/Gerät nicht booten

Grund: Das Installationsmedium findet das Boot-Medium nicht.

Lösung: Stellen Sie sicher, dass folgende Bedingungen erfüllt sind:

- Das DVD-ROM- oder CD-ROM-Laufwerk muss ordnungsgemäß installiert und eingeschaltet sein.
- Die Solaris-DVD oder die Solaris Software-1 CD muss ins Laufwerk eingelegt sein.
- Der Datenträger ist unbeschädigt und nicht verschmutzt.

WARNING: clock gained xxx days -- CHECK AND RESET DATE! (**nur SPARC-basierte** Systeme)

Beschreibung: Diese Meldung dient zu Ihrer Information.

Lösung: Ignorieren Sie die Meldung und fahren Sie mit der Installation fort.

Kein UFS-Dateisystem (nur x86-basierte Systeme)

Grund: Bei der Installation von aktuelle Solaris-Release (mit dem Solaris-Installationsprogramm oder benutzerdefiniertem JumpStart) wurde keine Boot-Diskette ausgewählt. Sie müssen jetzt das BIOS bearbeiten, um das System zu booten.

Lösung: Wählen Sie das BIOS, das gebootet werden soll. Erläuterungen dazu finden Sie in der BIOS-Dokumentation.

Booten von Medien, allgemeine Probleme

Das System wird nicht gebootet.

Beschreibung: Wenn Sie zum ersten Mal einen benutzerdefinierten JumpStart-Server einrichten, kann es beim Booten zu Problemen kommen, bei denen keine Fehlermeldung ausgegeben wird. Verwenden Sie den Boot-Befehl mit der Option -v, um Informationen über das System und den Boot-Vorgang abzurufen. Wenn Sie die Option -v verwenden, gibt der Boot-Befehl Fehlerbehebungsinformationen am Bildschirm aus. Hinweis – Wenn diese Option nicht angegeben wird, werden die Meldungen zwar ausgegeben, aber die Ausgabe wird in die Systemprotokolldatei umgeleitet. Weitere Informationen entnehmen Sie bitte der Manpage syslogd(1M).

Lösung: Für SPARC-Systeme geben Sie an der Eingabeaufforderung ok folgenden Befehl ein.

```
ok boot net -v - install
```

Das Booten von DVD schlägt bei Systemen mit einem DVD-ROM-Laufwerk SD-M 1401 von Toshiba fehl.

Beschreibung: Wenn das System mit einem DVD-ROM-Laufwerk SD-M1401 von Toshiba mit Firmware-Revision 1007 ausgestattet ist, kann das System nicht von der Solaris-DVD booten.

Lösung: Wenden Sie Patch 111649–03 oder später an, um die Firmware des Toshiba SD-M1401 DVD-ROM-Laufwerks zu aktualisieren. Das Patch 111649–03 ist auf sunsolve.sun.com verfügbar.

Das System hängt sich auf oder eine Panik tritt auf, wenn

Nicht-Speicher-PC-Karten eingelegt werden. (Nur x86-basierte Systeme) Grund: Nicht-Speicher-PC-Karten können nicht die gleichen Speicherressourcen verwenden wie andere Geräte.

Lösung: Um das Problem zu beheben, schlagen Sie in den Anweisungen zu Ihrer PC-Karte nach und überprüfen Sie den Adressbereich.

Das System hängt sich auf, bevor die Systemeingabeaufforderung angezeigt wird. (Nur x86-basierte Systeme)

Lösung: Es ist Hardware vorhanden, die nicht unterstützt wird. Lesen Sie hierzu in der Dokumentation des Hardware-Herstellers nach.

Booten vom Netzwerk, Fehlermeldungen

WARNING: getfile: RPC failed: error 5 (RPC Timed out).

Beschreibung: Dieser Fehler tritt auf, wenn zwei oder mehr Server in einem Netzwerk auf die Boot-Anforderung eines Installations-Clients reagieren. Der Installations-Client stellt eine Verbindung zum falschen Boot-Server her und die Installation hängt. Zu diesem Fehler kann es aus folgenden Gründen kommen:

Grund: *Grund*&;1:Möglicherweise sind auf verschiedenen Servern /etc/bootparams-Dateien mit einem Eintrag für diesen Installationsclient vorhanden. Lösung: *Grund 1:* Stellen Sie sicher, dass die Server im Netzwerk nicht mehrere /etc/bootparams-Einträge für den Installations-Client haben. Haben sie jedoch mehrere Einträge, entfernen Sie alle doppelten Client-Einträge in der Datei /etc/bootparams auf allen Installations- und Boot-Servern außer dem, den der Installationsclient verwenden soll.

Grund: *Grund* 2: Für den Installations-Client liegen möglicherweise mehrere /tftpbootoder /rplboot-Verzeichniseinträge vor.

Lösung: *Grund 2*: Stellen Sie sicher, dass für den Installations-Client nicht mehrere /tftpboot- oder /rplboot-Verzeichniseinträge auf den Servern im Netzwerk vorliegen. Ist dies jedoch der Fall, entfernen Sie doppelte Client-Einträge aus den Verzeichnissen /tftpboot oder /rplboot auf allen Installations- und Boot-Servern außer auf dem, den der Installationsclient verwenden soll.

Grund 3: Möglicherweise liegt ein Installations-Client-Eintrag in der Datei /etc/bootparams auf einem Server und ein Eintrag in einer anderen Datei /etc/bootparams vor, der es allen Systemen ermöglicht, auf den Profilserver zuzugreifen. Ein solcher Eintrag sieht ungefähr folgendermaßen aus:

* install_config=profile_server:path

Dieser Fehler kann auch durch eine Zeile wie die oben genannte in der bootparams-Tabelle von NIS oder NIS+ verursacht werden.

Lösung: *Grund 3:* If a wildcard entry is in the naming service bootparams map or table (for example, * install_config=), delete it and add it to the /etc/bootparams file on the boot server.

No network boot server. Unable to install the system. See installation instructions. (nur SPARC-basierte Systeme)

Grund: Dieser Fehler tritt auf einem System auf, das Sie über das Netzwerk zu installieren versuchen. Das System ist nicht korrekt konfiguriert.

Lösung: Sorgen Sie dafür, dass das System korrekt für eine Installation über das Netzwerk eingerichtet wird. Siehe hierzu "Hinzufügen der über das Netzwerk zu installierenden Systeme mit einem CD-Abbild" auf Seite 110.

prom_panic: Could not mount file system (nur SPARC-basierte Systeme) Grund: Dieser Fehler tritt auf, wenn Sie Solaris über ein Netzwerk installieren, aber die Boot-Software Folgendes nicht finden kann:

- Solaris-DVD, entweder die DVD oder eine Kopie des DVD-Abbildes auf dem Installationsserver
- Abbild der Solaris Software-1 CD, entweder die Solaris Software-1 CD oder eine Kopie des CD-Abbildes auf dem Installationsserver.

Lösung: Vergewissern Sie sich, dass die Installationssoftware eingehängt und freigegeben ist.

- Bei der Installation von Solaris vom DVD-ROM- oder CD-ROM-Laufwerk des Installationsservers aus müssen Sie sicherstellen, dass die Solaris-DVD oder die Solaris Software-1 CD ins CD-ROM-Laufwerk eingelegt, eingehängt und in der Datei /etc/dfs/dfstab freigegeben ist.
- Bei der Installation von einer Kopie des Solaris-DVD-Abbildes oder des Solaris Software-1 CD-Abbildes auf der Festplatte des Installationsservers aus stellen Sie sicher, dass der Verzeichnispfad zu der Kopie in der Datei /etc/dfs/dfstab freigegeben ist.

Timeout waiting for ARP/RARP packet...(nur SPARC-basierte Systeme) Grund: Grund 1: Der Client versucht, vom Netzwerk zu booten, kann aber kein System finden, das den Client kennt.

Lösung: *Grund 1*: Überprüfen Sie den Host-Namen des Systems im Naming Service NIS oder NIS+. Überprüfen Sie auch die bootparams-Suchreihenfolge in der Datei /etc/nsswitch.conf des Boot-Servers.

Beispielsweise bedeutet die folgende Zeile in der Datei /etc/nsswitch.conf, dass JumpStart oder das Solaris-Installationsprogramm zuerst in den NIS-Maps nach bootparams-Informationen sucht. Wenn das Programm keine Informationen findet, erfolgt eine Suche in der Datei /etc/bootparams auf dem Boot-Server.

bootparams: nis files

Grund: Grund 2: Die Ethernet-Adresse des Clients ist nicht korrekt.

Lösung: *Grund 2*: Stellen Sie sicher, dass die Ethernet-Adresse des Clients in der Datei /etc/ethers des Installationsservers korrekt angegeben ist.

Grund 3: In einer benutzerdefinierten JumpStart-Installation gibt der Befehl add_install_client die Plattformgruppe an, die einen bestimmten Server als Installationsserver verwendet. Wenn der falsche Architekturwert mit dem Befehl add_install_client verwendet wird, tritt dieses Problem auf. Beispiel: Der Rechner, der installiert werden soll, ist ein sun4u-Rechner, aber Sie haben i86pc verwendet.

Lösung: *Grund 3*: Führen Sie den Befehl add_install_client nochmals mit dem korrekten Architekturwert aus.

IP: joining multicasts failed on tr0 - will use link layer broadcasts for multicast (nur x86-basierte Systeme)

Grund: Diese Fehlermeldung erscheint beim Booten eines Systems mit einer Token Ring-Karte. Ethernet-Multicast und Token Ring-Multicast funktionieren nicht auf die gleiche Weise. Der Treiber gibt diese Fehlermeldung zurück, weil ihm eine ungültige Multicast-Adresse zur Verfügung gestellt wurde.

Lösung: Ignorieren Sie diese Fehlermeldung. Wenn Multicast nicht funktioniert, verwendet IP stattdessen Layer-Broadcasts, und die Installation schlägt deswegen nicht fehl.

Requesting Internet address for *Ethernet_Address* (**nur x86-basierte Systeme**) Grund: Der Client versucht, vom Netzwerk zu booten, kann aber kein System finden, das den Client kennt.

Lösung: Überprüfen Sie, ob der Systemname im Naming Service enthalten ist. Wenn der Host-Name des Systems im Naming-Service NIS oder NIS+ aufgelistet ist und das System weiterhin diese Fehlermeldung ausgibt, versuchen Sie es mit einem Neustart.

RPC: Timed out No bootparams (whoami) server responding; still trying... (nur
x86-basierte Systeme)

Grund: Der Client versucht, über das Netzwerk zu booten, aber er findet kein System mit einem Eintrag in der Datei /etc/bootparams auf dem Installationsserver.

Lösung: Geben Sie den Befehl add_install_client auf dem Installationsserver ein. Dieser Befehl fügt den entsprechenden Eintrag in die Datei /etc/bootparams ein und ermöglicht dem Client damit das Booten vom Netzwerk.

Still trying to find a RPL server... (nur x86-basierte Systeme)
Grund: Das System versucht, vom Netzwerk zu booten, aber der Server ist nicht so
konfiguriert, dass er dieses System booten kann.

Lösung: Führen Sie auf dem Installationsserver für das zu installierende System add_install_client aus. Der Befehl add_install_client richtet ein Verzeichnis /rplboot ein, das das nötige Netzwerk-Boot-Programm enthält.

CLIENT MAC ADDR: FF FF FF FF FF FF (nur Netzwerkinstallationen per DHCP) Grund: Der DHCP-Server ist nicht richtig konfiguriert. Dieser Fehler kann auftreten, wenn die Optionen oder Makros in der DHCP-Manager-Software nicht richtig definiert sind.

Lösung: Überprüfen Sie die Definition der Optionen und Makros in der DHCP-Manager-Software. Vergewissern Sie sich, dass die Router-Option definiert ist und den Wert für das Teilnetz aufweist, das bei der Netzwerkinstallation verwendet wird.

Booten vom Netzwerk, allgemeine Probleme

Das System bootet über das Netzwerk, aber von einem anderen als dem angegebenen Installationsserver.

Grund: Auf einem anderen System ist ein Eintrag in /etc/bootparams und eventuell auch in /etc/ethers für den Client enthalten.

Lösung: Aktualisieren Sie den Eintrag /etc/bootparams für das zu installierende System auf dem Namensserver. Der Eintrag muss folgende Syntax haben:

install_system root=boot_server:path install=install_server:path

Stellen Sie außerdem sicher, dass für den Installationsclient nur ein bootparams-Eintrag im Teilnetz vorliegt.

Das System bootet nicht über das Netzwerk (**gilt nur für Installationen über das** Netzwerk mit DHCP).

Grund: Der DHCP-Server ist nicht richtig konfiguriert. Dieser Fehler kann auftreten, wenn das System auf dem DHCP-Server nicht als Installationsclient konfiguriert wurde.

Lösung: Überprüfen Sie im DHCP Manager, dass für das betreffende Client-System Installationsoptionen und Makros definiert sind. Weitere Informationen finden Sie in "Vorkonfiguration der Systemkonfigurationsinformationen mit dem DHCP-Service (Vorgehen)" auf Seite 52.

Neuinstallation von Solaris

Die Neuinstallation schlägt fehl.

Lösung: Wenn die Solaris-Installation fehlschlägt, müssen Sie sie neu starten. Um die Installation neu zu starten, booten Sie das System von der Solaris-DVD, der Solaris Software-1 CD oder über das Netzwerk.

Sie können die Solaris-Software nicht deinstallieren, wenn sie teilweise installiert wurde. Sie müssen das System von einer Sicherungskopie wiederherstellen oder den Solaris-Installationsprozess erneut ausführen.

/cdrom/sol_Solaris_10/SUNW xxxx/reloc.cpio: Gebrochene Pipe Beschreibung: Diese Fehlermeldung ist informativer Natur und hat keine Auswirkung auf die Installation. Die Bedingung tritt ein, wenn für einen Schreibzugriff auf ein Pipe kein Leseprozess vorhanden ist.

Lösung: Ignorieren Sie die Meldung und fahren Sie mit der Installation fort.

WARNING: STANDARD-BOOT-GERÄT WECHSELN (nur x86-basierte Systeme) Grund: Diese Meldung dient zu Ihrer Information. Als Standard-Boot-Gerät ist im BIOS des Systems möglicherweise ein Gerät eingestellt, das zum Booten des Systems die Solaris Device Configuration Assistant erfordert.

Lösung: Fahren Sie mit der Installation fort und ändern Sie gegebenenfalls das Standard-Boot-Gerät des Systems, das im BIOS angegeben ist, nachdem Sie die Solaris-Software auf einem Gerät installiert haben, für das die Solaris Device Configuration Assistant nicht erforderlich ist. x86 nur – Wenn Sie zum Testen eines benutzerdefinierten JumpStart-Profils für eine Erstinstallation das Schlüsselwort locale verwenden, schlägt der Test des Profils mithilfe des Befehls pfinstall -D fehl. Die Beschreibung einer Abhilfe finden Sie in der Erläuterung zur Fehlermeldung "could not select locale," im Abschnitt "Upgrade von Solaris" auf Seite 274.

x86: So überprüfen Sie eine IDE-Festplatte auf fehlerhafte Blöcke

IDE-Festplatten weisen fehlerhaften Blöcke nicht automatisch aus, wie andere von Solaris-Software unterstützte Festplatten. Bevor Sie Solaris auf einer IDE-Festplatte installieren, sollten Sie unter Umständen eine Oberflächenanalyse der Festplatte durchführen. Gehen Sie dazu folgendermaßen vor.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services.*

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

- 2 Booten Sie vom Installationsdatenträger.
- 3 Wählen Sie Option 6 (Single User Shell), wenn Sie zur Auswahl einer Installationsart aufgefordert werden.
- 4 Siehe hierzu die Manpage format(1M).

format

5 Geben Sie das IDE-Laufwerk an, für das die Oberflächenanalyse durchgeführt werden soll.

cx**d**y

- cx ist die Controller-Nummer
- dy ist die Gerätenummer
- 6 Ermitteln Sie, ob eine fdisk-Partition vorhanden ist.
 - Wenn bereits eine Solaris-Partition fdisk vorhanden ist, fahren Sie mit Schritt 7 fort.
 - Wenn noch keine Solaris-fdisk-Partition existiert, legen Sie mit dem Befehl fdisk eine Solaris-Partition auf der Festplatte an.

format> fdisk

- 7 Um die Oberflächenanalyse zu starten, geben Sie folgenden Befehl ein: format> analyze
- 8 Um die aktuellen Einstellungen zu ermitteln, geben Sie folgenden Befehl ein: analyze> config
- 9 (Optional) Wenn Sie die Einstellungen ändern wollen, geben Sie Folgendes ein: analyze> setup
- 10 Um nach fehlerhaften Blöcken zu suchen, geben Sie Folgendes ein: analyze> type_of_surface_analysis Typ_der_Oberflächenanalyse kann "read", "write" oder "compare" sein Wenn format fehlerhafte Blöcke findet, weist es diese neu zu.
- 11 Um die Analyse zu beenden, geben Sie Folgendes ein: analyze> quit
- 12 Wollen Sie Blöcke zum erneuten Zuweisen angeben?
 - Wenn nicht, fahren Sie mit Schritt 13 fort.
 - Wenn ja, geben Sie Folgendes ein:

format> **repair**

- 13 Um das Programm format zu beenden, geben Sie folgendes ein: quit
- 14 Booten Sie vom Datenträger im Mehrfachbenutzermodus durch Eingeben des folgenden Befehls.

exit

Upgrade von Solaris

Durchführen eines Upgrade, Fehlermeldungen

No upgradable disks

Grund: Ein Swap-Eintrag in der Datei /etc/vfstab verursacht das Fehlschlagen der Aktualisierung.

Lösung: Setzen Sie die folgenden Zeilen in der Datei /etc/vfstab auf Kommentar:

- Alle Swap-Dateien und -Slices auf Platten, die nicht aufgerüstet werden
- Swap-Dateien, die nicht mehr vorhanden sind
- Nicht verwendete Swap-Slices

usr/bin/bzcat not found

Grund: Solaris Live Upgrade schlägt fehl, da ein benötigtes Patch-Cluster fehlt.

Lösung: Für die Installation von Solaris Live Upgrade ist ein Patch erforderlich. Eine stets aktuelle Patchliste finden Sie auf http://sunsolve.sun.com. Suchen Sie auf der SunSolve-Website nach dem Informationsdokument 72099.

Es wurden aktualisierbare Solaris-Root-Geräte, jedoch keine geeigneten Partitionen für das Solaris-Installationsprogramm gefunden. Ein Upgrade mit dem Solaris-Installationsprogramm ist nicht möglich. Unter Umständen kann ein Upgrade mit der Solaris Software 1-CD durchgeführt werden. (Nur x86-basierte Systeme)

Grund: Ein Upgrade mit der Solaris Software-1 ist nicht möglich, da nicht genug Platz vorhanden ist.

Lösung: Um ein Upgrade durchzuführen, können Sie entweder ein Swap-Slice erstellen, das größer oder gleich 512 MB ist, oder ein anderes Upgrade-Verfahren verwenden, zum Beispiel das Solaris-Installationsprogramm von der Solaris-DVD, ein Netzwerk-Installationsabbild oder JumpStart.

ERROR: Could not select locale (nur x86-basierte Systeme)

Grund: Wenn Sie ein JumpStart-Profil mithilfe des Befehls pfinstall -D testen, schlägt der Dry Run-Test in den folgenden Situationen fehl:

- Das Profil enthält das Schlüsselwort "locale".
- Sie testen ein Release, das GRUB-Software enthält Ab Solaris-Release 10 1/06 erleichtert der GRUB-Bootloader das Booten unterschiedlicher Betriebssysteme mithilfe des GRUB-Menüs.

Mit der Einführung der GRUB-Software wurde die Miniroot komprimiert. Die Software findet deswegen in der komprimierten Miniroot nicht mehr die Liste der Gebietsschemata. Die Miniroot ist das kleinstmögliche Solaris root-Dateisystem (/). Sie befindet sich auf dem Solaris-Installationsdatenträger.

Lösung: Führen Sie die folgenden Schritte aus. Geben Sie die folgenden Werte ein:

- MEDIA_DIR is /cdrom/cdrom0/
- MINIROOT_DIR is \$MEDIA_DIR /Solaris_10/Tools/Boot
- MINIROOT_ARCHIVE is \$MEDIA_DIR /boot/x86.miniroot
- TEMP_FILE_NAME is /tmp/test

1. Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. Entpacken Sie das Miniroot-Archiv.

```
# /usr/bin/gzcat $MINIROOT_ARCHIVE > $TEMP_FILE_NAME
```

3. Erstellen Sie mithilfe des Befehls lofiadm das Miniroot-Gerät.

```
# LOFI_DEVICE=/usr/sbin/lofiadm -a $TEMP_FILE_NAME
# echo $LOFI_DEVICE
/dev/lofi/1
```

4. Hängen Sie die Miniroot mithilfe des Befehls lofi unter dem Miniroot-Verzeichnis ein.

/usr/sbin/mount -F ufs \$LOFI_DEVICE \$MINIROOT_DIR

5. Testen Sie das Profil.

```
# /usr/sbin/install.d/pfinstall -D -c $MEDIA_DIR $path-to-jumpstart_profile
```

6. Hängen Sie nach dem Abschluss des Tests das lofi-Gerät wieder aus.he lofi device.

```
# umount $LOFI_DEVICE
```

- 7. Löschen Sie das lofi-Gerät.
 - # lofiadm -d \$TEMP_FILE_NAME

Durchführen eines Upgrade, allgemeine Probleme

Die Upgrade-Option wird nicht angeboten, obwohl auf dem System eine Upgrade-Version der Solaris-Software vorhanden ist.

Grund 1: Das Verzeichnis /var/sadm ist ein symbolischer Link oder wurde von einem anderen Dateisystem aus eingehängt.

Lösung: *Grund 1*: Verschieben Sie das Verzeichnis /var/sadm in das Root-Dateisystem (/) oder in das Dateisystem /var.

Grund: Grund 2: Die Datei /var/sadm/softinfo/INST_RELEASE fehlt.

Lösung: *Grund 2*: Erstellen Sie eine neue Datei INST_RELEASE. Verwenden Sie dazu folgende Vorlage:

```
OS=Solaris
VERSION=x
REV=0
```

x ist die Version der Solaris-Software auf dem System

Grund: Grund 3: SUNWusr ist in /var/sadm/softinfo nicht vorhanden.

Lösung: *Lösung 3:* Sie müssen eine Neuinstallation durchführen. Ein Upgrade der Solaris-Software ist nicht möglich.

- Der md-Treiber lässt sich nicht herunterfahren oder initialisieren. Lösung: Gehen Sie wie folgt vor:
 - Handelt es sich bei dem Dateisystem nicht um ein RAID-1-Volume, so setzen Sie den entsprechenden Teil der Datei vsftab auf Kommentar.
 - Handelt es sich um ein RAID-1-Volume, brechen Sie den Mirror-Verbund auf und führen Sie die Installation erneut durch. Informationen zum Aufbrechen des Mirror-Verbunds finden Sie in "Removing RAID-1 Volumes (Unmirroring)" in Solaris Volume Manager Administration Guide.

Das Upgrade schlägt fehl, weil das Solaris-Installationsprogramm ein Dateisystem nicht einhängen kann.

Grund: Bei einem Upgrade wird durch das Skript versucht, alle in der Datei /etc/vfstab des Systems aufgeführten Dateisysteme in das Root-Dateisystem (/) einzuhängen, an dem das Upgrade durchgeführt wird. Wenn das Installationsskript ein Dateisystem nicht einhängen kann, schlägt es fehl und wird abgebrochen.

Lösung: Stellen Sie sicher, dass alle Dateisysteme in der Datei /etc/vfstab des Systems eingehängt werden können. Setzen Sie alle Dateisysteme in der Datei /etc/vfstab auf Kommentar, die nicht eingehängt werden können oder die das Problem anderweitig verursachen könnten, so dass das Solaris-Installationsprogramm beim Upgrade nicht versucht, sie einzuhängen. Systembasierte Dateisysteme jedoch, die zu aktualisierende Software enthalten (beispielsweise /usr), können nicht auf Kommentar gesetzt werden.

Das Upgrade schlägt fehl.

Beschreibung: Das System verfügt nicht über genügend Speicherplatz für das Upgrade.

Grund: Suchen Sie unter "Upgrade mit Neuzuweisung von Festplattenspeicher" in Oracle Solaris 10 9/10 Installationshandbuch: Planung von Installationen und Upgrades nach Informationen zum Speicherplatzproblem und versuchen Sie, ob Sie es ohne ein Auto-Layout zum Neuzuweisen des Speicherplatzes beseitigen können.

Probleme beim Aktualisieren von RAID-1-Volumes als Root-Dateisysteme (/) Lösung: Sollten sich beim Upgrade mit Solaris Volume Manager RAID-1-Volumes als Root-Dateisystem (/) Probleme ergeben, schlagen Sie in Kapitel 25, "Troubleshooting Solaris Volume Manager (Tasks)" in *Solaris Volume Manager Administration Guide* nach.

So setzen Sie ein Upgrade nach einem Fehlschlag fort

Das Upgrade ist fehlgeschlagen und das System lässt sich nicht über die Software booten. Der Grund für den Fehlschlag liegt außerhalb Ihres Einflussbereichs, zum Beispiel ein Stromausfall oder der Ausfall einer Netzwerkverbindung.

- 1 Starten Sie das System von der Solaris-DVD, der Solaris Software-1 CD oder über das Netzwerk neu.
- 2 Wählen Sie die Upgrade-Option für die Installation.

Das Solaris-Installationsprogramm ermittelt, ob das System teilweise aufgerüstet wurde, und setzt das Upgrade fort.

x86: Probleme mit Solaris Live Upgrade bei der Verwendung von GRUB

Bei Verwendung von Solaris Live Upgrade und dem GRUB-Bootloader auf x86-basierten Systemen können die folgenden Fehler auftreten.

ERROR: Das Tools-Installationsverzeichnis *Installationsverzeichnis* ist auf dem Produktmedium nicht vorhanden.

ERROR: The media *dirctory* does not contain an operating system upgrade image. Beschreibung: Dieser Fehlermeldungen werden angezeigt, wenn mithilfe des Befehls luupgrade ein Upgrade auf eine neue Boot-Umgebung durchgeführt wird.

Grund: Es wird eine ältere Version Solaris Live Upgrade verwendet. Die auf Ihrem System installierten Packages von Solaris Live Upgrade sind mit dem Datenträger und dessen Softwareversion nicht kompatibel.

Lösung: Sie müssen stets die Solaris Live Upgrade-Packages des Releases verwenden, auf den Sie upgraden möchten.

Beispiel: Im folgenden Beispiel zeigt die Fehlermeldung an, dass die auf dem System installierten Packages von Solaris Live Upgrade nicht der auf dem Datenträger befindlichen Version entsprechen.

```
# luupgrade -u -n sl0ul -s /mnt
Validating the contents of the media </mnt>.
The media is a standard Solaris media.
ERROR: The media product tools installation directory
</mnt/Solaris_10/Tools/Boot/usr/sbin/install.d/install_config> does
not exist.
ERROR: The media </mnt> does not contain an operating system upgrade
image.
```

ERROR: Cannot find or is not executable: </sbin/biosdev>.

ERROR: One or more patches required by Solaris Live Upgrade has not been installed.

Grund: Eines oder mehrere, für Solaris Live Upgrade erforderliche Patches sind nicht auf Ihrem System installiert. Bitte beachten Sie, dass mit dieser Fehlermeldung nicht alle fehlenden Patches erkannt werden.

Lösung: Vor dem Arbeiten mit Solaris Live Upgrade müssen Sie erst alle erforderlichen Patches installieren. Eine stets aktuelle Patchliste finden Sie auf <u>http://sunsolve.sun.com</u>. Suchen Sie auf der SunSolve-Website nach dem Informationsdokument 72099.

ERROR: Device mapping command </sbin/biosdev> failed. Please reboot and try again.

Grund *1:* Solaris Live Upgrade kann aufgrund vorheriger administrativer Aufgaben keine Geräte zuweisen.

Lösung: Grund 1: Booten Sie das System neu und starten Sie Solaris Live Upgrade erneut.

Grund: *Grund 2*: Wenn nach einem erneuten Booten des Systems diese Fehlermeldung wieder angezeigt wird, heißt das, dass sich im System zwei identische Festplatten befinden. Der Befehl zum Zuweisen von Geräten kann diese beiden Platten nicht unterscheiden.

Lösung: *Grund 2:* Erstellen Sie auf einer der beiden Festplatten eine fdisk-Dummypartition. Weitere Informationen entnehmen Sie bitte der Manpage fdisk(1M) Booten Sie dann das System neu.

Cannot delete the boot environment that contains the GRUB menu Grund: Solaris Live Upgrade besitzt die Einschränkung, dass Boot-Umgebungen, die das GRUB-Menü enthalten, nicht gelöscht werden können.

Lösung: Mit den Befehlen lumake(1M) oder luupgrade(1M) können Sie diese Boot-Umgebung wiederverwenden.

The file system containing the GRUB menu was accidentally remade. However, the disk has the same slices as before. For example, the disk was not re-sliced. Grund: Das Dateisystem, das das GRUB-Menü enthält, wird zum Booten des Systems benötigt. Solaris Live Upgrade-Befehle zerstören das GRUB-Menü nicht. Wenn das GRUB-Menü jedoch mit anderen, nicht zu Solaris Live Upgrade gehörenden Befehlen versehentlich oder aus anderen Gründen überschrieben bzw. zerstört wird, versucht die Software zur Wiederherstellung des Systems, das GRUB-Menü neu zu installieren. Diese Software kopiert das GRUB-Menü beim nächsten Booten des Systems in das gleiche Dateisystem. Es kann zum Beispiel sein, dass Sie mit den Befehlen newfs oder mkfs das GRUB-Menü versehentlich zerstört haben. Damit das GRUB.Menü ordnungsgemäß wiederhergestellt werden kann, muss das Slice die folgenden Bedingungen erfüllen:

- Es muss ein einhängbares Dateisystem besitzen.
- Es muss zur gleichen Boot-Umgebung von Solaris Live Upgrade wie vorher gehören.

Nehmen Sie vor einem Systemneustart am Slice die erforderlichen Korrekturen vor.

Lösung: Starten Sie das System neu. Es wird automatisch eine Sicherungskopie des GRUB-Menüs installiert.

The GRUB menu's menu.lst file was accidentally deleted.

Lösung: Starten Sie das System neu. Es wird automatisch eine Sicherungskopie des GRUB-Menüs installiert.

Systempanik bei einem Upgrade mit Solaris Live Upgrade und Veritas VxVm

Wenn Sie bei einem Upgrade Solaris Live Upgrade benutzen und Veritas VxVM läuft, kommt es beim Neustart zu einer Systempanik. Um diese zu vermeiden, müssen Sie das Upgrade mit dem folgenden Verfahren durchführen. Das Problem tritt auf, wenn Packages nicht den neuen Solaris-Richtlinien für Packages entsprechen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Hinweis – Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

- 2 Erstellen Sie eine inaktive Boot-Umgebung. Siehe "Erstellen einer neuen Boot-Umgebung" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades.
- 3 Vor dem Upgrade der inaktiven Boot-Umgebung müssen Sie in der inaktiven Boot-Umgebung die vorhandene Veritas-Software deaktivieren.
 - a. Hängen Sie die inaktive Boot-Umgebung ein.

lumount inactive_boot_environment_name mount_point
Beispiel:

lumount solaris8 /mnt

b. Wechseln Sie in das Verzeichnis, das die vfstab enthält. Beispiel:

cd /mnt/etc

- c. Erstellen Sie eine Kopie der Datei vfstab der inaktiven Boot-Umgebung. Beispiel:
 # cp vfstab vfstab.501
- d. Setzen Sie in der kopierten Datei vfstab alle Veritas-Dateisystemeinträge auf Kommentar. Beispiel:

sed '/vx\/dsk/s/^/#/g' < vfstab > vfstab.novxfs

Als erstes Zeichen erscheint in den entsprechenden Zeilen ein #. Dadurch gelten diese Zeilen als Kommentarzeilen. Beachten Sie, dass diese Kommentarzeilen sich von den Kommentarzeilen in der Systemdatei unterscheiden.

e. Kopieren Sie die geänderte Datei vfstab. Beispiel:

```
# cp vfstab.novxfs vfstab
```

- f. Wechseln Sie in das Verzeichnis mit der Systemdatei der inaktiven Boot-Umgebung. Beispiel:
 - # cd /mnt/etc
- g. Erstellen Sie eine Kopie der Systemdatei der inaktiven Boot-Umgebung. Beispiel:
 - # cp system system.501
- h. Kennzeichnen Sie alle Einträge des Typs "forceload:" als Kommentare, die drv/vx enthalten.

```
# sed '/forceload: drv\/vx/s/^/*/' <system> system.novxfs
```

Als erstes Zeichen erscheint in den entsprechenden Zeilen ein *. Dadurch gelten diese Zeilen als Befehlszeilen. Beachten Sie, dass diese Kommentarzeilen sich von den Kommentarzeilen in der Datei vfstab unterscheiden.

- i. Erstellen Sie die Veritas-Datei install-db. Beispiel:
 - # touch vx/reconfig.d/state.d/install-db
- j. Hängen Sie die inaktive Boot-Umgebung aus.
 - # luumount inactive_boot_environment_name
- 4 Führen Sie das Upgrade der inaktiven Boot-Umgebung durch. Siehe Kapitel 5, "Ausführen eines Upgrades mit Solaris Live Upgrade (Vorgehen)" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades.
- 5 Aktivieren Sie die inaktive Boot-Umgebung. Siehe "Aktivieren einer Boot-Umgebung" in Oracle Solaris 10 9/10 Installationshandbuch: Solaris Live Upgrade und Planung von Upgrades.

6 Fahren Sie das System herunter.

init 0

7 Booten Sie die inaktive Boot-Umgebung im Einzelbenutzermodus:

OK boot -s

Mehrere Meldungen und Fehlermeldungen, die "vxvm" oder "VXVM" enthalten, werden angezeigt. Ignorieren Sie diese. Die inaktive Boot-Umgebung wird aktiv.

- 8 Führen Sie ein Upgrade von Veritas durch.
 - a. Entfernen Sie das Package Veritas VRTSvmsa vom System. Beispiel: # pkgrm VRTSvmsa
 - b. Wechseln Sie in das Verzeichnis mit den Veritas-Packages.

cd /location_of_Veritas_software

- c. Fügen Sie die neuesten Veritas-Packages zum System hinzu:
 - # pkgadd -d 'pwd' VRTSvxvm VRTSvmsa VRTSvmdoc VRTSvmman VRTSvmdev
- 9 Stellen Sie die ursprüngliche Datei vfstab und die ursprünglichen Systemdateien wieder her:

cp /etc/vfstab.original /etc/vfstab
cp /etc/system.original /etc/system

10 Starten Sie das System neu.

init 6

x86: Service-Partition wird auf Systemen ohne bereits vorhandene Service-Partition nicht standardmäßig erzeugt

Wenn Sie die aktuelle Solaris-Release auf einem System installieren, das noch keine Servicebzw. Diagnosepartition enthält, wird eine solche unter Umständen nicht automatisch vom Installationsprogramm erzeugt. Wenn Sie eine Service-Partition auf der gleichen Festplatte wie die Solaris-Partition einrichten möchten, müssen in Sie die Service-Partition neu erstellen, bevor Sie die aktuelle Solaris-Release installieren.

Bei der Installation von Solaris 8 2/02 auf einem System mit Service-Partition behält das Installationsprogramm die Service-Partition u. U. nicht bei. Sofern Sie das Layout der Boot-Partition fdisk nicht manuell bearbeiten, um die Service-Partition beizubehalten, wird die Service-Partition vom Installationsprogramm gelöscht. Hinweis – Wenn Sie die Service-Partition bei der Installation von Solaris 8 2/02 nicht ausdrücklich beibehalten haben, ist es u. U. nicht möglich, die Service-Partition wiederherzustellen und ein Upgrade auf die aktuelle Solaris-Release durchzuführen.

Um auf der Festplatte mit der Solaris-Partition auch eine Service-Partition einzurichten, wählen Sie eine der nachfolgenden Problemlösungen.

So installieren Sie die Software von einem Netzwerk-Installationsabbild oder der Solaris-DVD

Zur Installation von einem Netzwerk-Installationsabbild oder von der Solaris-DVD über das Netzwerk gehen Sie wie folgt vor:

- 1 Löschen Sie den Inhalt der Festplatte.
- 2 Legen Sie vor der Installation die Service-Partition an. Verwenden Sie hierzu die Diagnose-CD für Ihr System.

Wie Sie die Service-Partition erzeugen, entnehmen Sie bitte der Dokumentation zur jeweiligen Hardware.

3 Booten Sie das System über das Netzwerk.

Der Bildschirm für die Anpassung der fdisk-Partitionen wird angezeigt.

4 Um das Standard-Layout für die Bootplatten-Partitionen zu laden, klicken Sie auf "Default". Das Installationsprogramm behält die Service-Partition bei und erzeugt die Solaris-Partition.

So installieren Sie von der Solaris Software-1 CD oder einem Netzwerk-Installationsabbild

Zur Installation von der Solaris Software-1 CD oder von einem Netzwerkinstallationsabbild auf einem Boot-Server mithilfe des Solaris-Installationsprogramms gehen Sie wie folgt vor:

1 Löschen Sie den Inhalt der Festplatte.

2 Legen Sie vor der Installation die Service-Partition an. Verwenden Sie hierzu die Diagnose-CD für Ihr System.

Wie Sie die Service-Partition erzeugen, entnehmen Sie bitte der Dokumentation zur jeweiligen Hardware.

- 3 Das Installationsprogramm fordert Sie dazu auf, eine Methode zur Erstellung der Solaris-Partition auszuwählen.
- 4 Booten Sie das System.
- 5 Wählen Sie die Option Use rest of disk for Solaris partition.
 Das Installationsprogramm behält die Service-Partition bei und erzeugt die Solaris-Partition.
- 6 Schließen Sie die Installation ab.

Ausführen einer Installation oder eines Upgrades von einem entfernten System (Vorgehen)

In diesem Anhang wird die Installation von bzw. das Upgrade auf Solaris BS auf einem Rechner oder einer Domäne ohne direkt angeschlossenes DVD-ROM- oder CD-ROM-Laufwerk mithilfe des Solaris-Installationsprogramms erläutert.

Hinweis – Wenn Sie das Solaris BS auf einem Mehrdomänenserver installieren oder aktualisieren möchten, lesen Sie vor dem Installationsprozess bitte die Dokumentation zum Systemcontroller oder zum Systemserviceprozesser.

SPARC: Ausführen einer Installation oder eines Upgrade von einer entfernten DVD-ROM oder CD-ROM mithilfe des Solaris-Installationsprogramms

Wenn Solaris auf einem Rechner oder in einer Domäne ohne direkt angeschlossenes DVD-ROM- oder CD-ROM-Laufwerk installiert werden soll, können Sie ein Laufwerk verwenden, das an einen anderen Rechner angeschlossen ist. Beide Rechner müssen sich in demselben Teilnetz befinden. Anhand der folgenden Anweisungen können Sie eine solche Installation ausführen.

SPARC: So führen Sie eine Installation oder ein Upgrade von einer entfernten DVD-ROM oder CD-ROM aus

Hinweis – Bei diesem Verfahren wird davon ausgegangen, dass Volume Manager auf dem System ausgeführt wird. Wenn Sie den Volume Manager nicht zum Verwalten von Medien verwenden, lesen Sie bitte *System Administration Guide: Devices and File Systems*.

Im folgenden Verfahren wird das entfernte System mit dem DVD-ROM- oder CD-ROM-Laufwerk als *entferntes System* bezeichnet. Das zu installierende Clientsystem wird als das *Clientsystem* bezeichnet.

- 1 Wählen Sie ein System, auf dem Solaris ausgeführt wird und das über ein DVD-ROM- oder CD-ROM-Laufwerk verfügt.
- 2 Legen Sie auf dem *entfernten System* mit dem DVD-ROM- oder CD-ROM-Laufwerk die Solaris-DVD oder die Solaris Software for SPARC Platforms - 1-CD in das Laufwerk ein.

Der Datenträger wird von Volume Manager eingehängt.

- 3 Wechseln Sie auf dem entfernten System in das Verzeichnis auf der DVD oder CD, in dem sich der Befehl add_install_client befindet.
 - Bei einer DVD geben Sie Folgendes ein:

remote system# cd /cdrom/cdrom0/Solaris_10/Tools

Bei einer CD geben Sie Folgendes ein:

remote system# cd /cdrom/cdrom0

- 4 Fügen Sie auf dem entfernten System das zu installierende System als Client hinzu.
 - Bei einer DVD geben Sie Folgendes ein:

remote system# ./add_install_client \
client_system_name arch

Bei einer CD geben Sie Folgendes ein:

```
remote system# ./add_install_client -s remote_system_name: \
/cdrom/cdrom0 client_system_name arch
```

Name_entferntes_SystemDer Name des Systems mit dem DVD-ROM- oder
CD-ROM-Laufwerk

Name_des_Clientsystems Der Name des Rechners, auf dem installiert werden soll

Arch

Die Plattformgruppe des Rechners, auf dem installiert werden soll, zum Beispiel sun4u Auf dem System, auf dem installiert werden soll, können Sie die Plattformgruppe mit dem Befehl uname -m ermitteln.

5 Booten Sie das zu installierende Clientsystem.

client system: ok **boot net** Die Installation beginnt.

6 Befolgen Sie die Anweisungen und geben Sie bei Bedarf die Systemkonfigurationsinformationen ein.

- Wenn Sie eine DVD verwenden, befolgen Sie die Anweisungen am Bildschirm, um die Installation abzuschließen. Sie sind jetzt fertig.
- Wenn Sie CDs verwenden, wird das System neu gestartet, und das Solaris-Installationsprogramm beginnt. Nach dem Willkommensbildschirm wird das Dialogfeld "Medien angeben" angezeigt, in dem die Option "Entferntes Dateisystem (NFS)" bereits gewählt ist. Fahren Sie mit Schritt 7 fort.
- 7 Klicken Sie im Dialogfeld "Medien angeben" auf "Weiter".

Das Dialogfeld "Pfad für Netzwerkdateisystem angeben" mit dem Installationspfad im Texteingabefeld erscheint.

IP-Adresse_Clientsystem: / cdrom/cdrom0

8 Wechseln Sie auf dem entfernten System, auf dem die DVD oder CD eingehängt ist, in das Verzeichnis root.

remote system# cd /

9 Suchen Sie auf dem entfernten System den Pfad zu dem Slice, das zur gemeinsamen Nutzung freigegeben wurde.

remote system# share

10 Heben Sie auf dem entfernten System die Freigabe der Solaris-DVD bzw. der Solaris Software for SPARC Platforms - 1-CD auf. Verwenden Sie dazu den Pfad, den Sie in Schritt 9 ermittelt haben. Wenn der Pfad auf zwei Slices verweist, heben Sie die Freigabe beider Slices mit unshare auf.

remote system# unshare absolute_path

absoluter_Pfad Der vom Befehl share zurückgegebene absolute Pfad

In diesem Beispiel wird die Freigabe von Slice 0 und Slice 1 aufgehoben.

remote system# unshare /cdrom/cdrom0
remote system# unshare /cdrom/cdrom0

- 11 Setzen Sie die Solaris-Installation fort, indem Sie auf dem zu installierenden Clientsystem auf "Weiter" klicken.
- 12 Wenn Sie das Solaris-Installationsprogramm auffordert, die Solaris Software 2-CD einzulegen, gehen Sie wie unter Schritt 9 bis Schritt 11 erläutert vor, um die Freigabe der Solaris Software-1 CD aufzuheben und die Solaris Software - 2-CD zu exportieren und zu installieren.
- 13 Wenn Sie das Solaris-Installationsprogramm auffordert, weitere Solaris Software-CDs einzulegen, gehen Sie wie unter Schritt 9 bis Schritt 11 erläutert vor, um die Freigabe der Solaris Software-CDs aufzuheben und die betreffenden CDs zu exportieren und zu installieren.
- 14 Wenn Sie das Solaris-Installationsprogramm auffordert, die Solaris Languages-CD einzulegen, gehen Sie wie unter Schritt 9 bis Schritt 11 erläutert vor, um die Freigabe der Solaris Software-CDs aufzuheben und die Solaris Languages-CD zu exportieren und zu installieren.

Wenn Sie eine Solaris Languages-CD exportieren, erscheint auf dem Rechner mit der eingehängten CD-ROM ein Installationsfenster. Ignorieren Sie das Installationsfenster, während Sie die Solaris Languages-CD installieren. Schließen Sie nach der Installation der Solaris Languages-CDs das Installationsfenster.
Glossar

3DES	([Dreifach-DES] Triple-Data Encryption Standard, Standard für die dreifache Datenverschlüsselung). Eine symmetrische Verschlüsselungsmethode, die eine Schlüssellänge von 168 Bit bietet.
Abgeleitetes Profil	Ein Profil, das bei einer benutzerdefinierten JumpStart-Installation dynamisch von einem Begin-Skript erstellt wird.
Abgesichertes Boot-Archiv	Nur x86: Ein Boot-Archiv, das zur Wiederherstellung verwendet wird, falls das primäre Boot-Archiv beschädigt ist. Dieses Boot-Archiv startet das System, ohne das Root-Dateisystem (/) einzuhängen. Im GRUB-Menü wird dieses Boot-Archiv als "abgesichert" bezeichnet. Es dient hauptsächlich dazu, das primäre Boot-Archiv neu zu erzeugen (also das Boot-Archiv, mit dem das System normalerweise gestartet wird). Siehe <i>Boot-Archiv</i> .
AES	(Advanced Encryption Standard) Eine symmetrische 128-Bit-Blockdaten-Verschlüsselungstechnik. Die U.SRegierung hat die Rijndael-Variante des Algorithmus im Oktober 2000 als Verschlüsselungsstandard angenommen. AES ersetzt die DES-Verschlüsselung als Regierungsstandard.
Aktualisierung	Eine Installation, bei der bereits auf dem System vorhandene Software desselben Typs geändert wird. Im Gegensatz zu einem Upgrade (einer Aufstufung) kann eine Aktualisierung (engl. Update) auch eine Herabstufung des Systems bewirken. Anders als bei einer Erst- bzw. Neuinstallation, muss Software desselben Typs wie die zu installierende Software bereits auf dem System vorhanden sein, damit eine Aktualisierung vorgenommen werden kann.
Archiv	Eine Datei, die einen Satz von Dateien enthält, die von einem Mastersystem kopiert wurden. Die Datei enthält auch Identifikationsinformationen über das Archiv, zum Beispiel einen Namen und das Datum der Archiverstellung. Nach der Installation eines Archivs auf einem System verfügt dieses System über genau dieselbe Konfiguration wie das Mastersystem.
	Dabei kann es sich auch um ein Differenzarchiv handeln, d. h. ein Solaris Flash-Archiv, das nur die Unterschiede zwischen zwei Systemabbildern (einem unveränderten und einem aktualisierten Master-Abbild) enthält. Ein Differenzarchiv enthält die auf dem Klonsystem beizubehaltenden, zu ändernden oder zu löschenden Dateien. Eine solche differentielle Aktualisierung ändert nur die angegebenen Dateien und kann nur auf Systeme angewendet werden, deren Software mit derjenigen des unveränderten Master-Abbilds übereinstimmt.
Aufgabe	Eine benutzerdefinierte Aufgabe, die ein Computersystem ausführen soll.

Aushängen	Das Beenden des Zugriffs auf ein Verzeichnis auf einer Festplatte, die mit einem lokalen Rechner oder mit einem entfernten Rechner in einem Netzwerk verbunden ist.
Bedienfeld	Ein 'Behälter', in dem der Inhalt eines Fensters, Dialogfeldes oder Applets angeordnet ist. In einem Bedienfeld werden möglicherweise Benutzereingaben aufgenommen und bestätigt. Häufig wird in Assistenten eine Folge mehrere Bedienfelder angezeigt, die den Benutzer durch einen bestimmten Vorgang leiten.
Befehlszeile	Eine Zeichenkette, die mit einem Befehl beginnt, oft gefolgt von Argumenten einschließlich Optionen, Dateinamen und anderen Ausdrücken, und mit einem Zeilenendezeichen endet.
Begin-Skript	Ein benutzerdefiniertes Bourne-Shell-Skript, spezifiziert innerhalb der Datei rules, das bestimmte Aufgaben ausführt, bevor die Solaris-Software auf dem System installiert wird. Begin-Skripte können ausschließlich bei benutzerdefinierten JumpStart-Installationen eingesetzt werden.
Benutzerdefinierte JumpStart-Installation	Ein Installationstyp, bei dem die Solaris-Software auf der Basis eines benutzerdefinierten Profils automatisch auf einem System installiert wird. Man kann benutzerdefinierte Profile von Benutzern und Systemen erstellen. Eine benutzerdefinierte JumpStart-Installation ist eine JumpStart-Installation, die Sie erstellen.
Benutzerdefinierte probes-Datei	Eine Datei, die sich im gleichen JumpStart-Verzeichnis befinden muss wie die rules-Datei. Es handelt sich dabei um ein Bourne-Shell-Skript, das zwei Typen von Funktionen enthält: Probe-Funktionen (Sondierfunktionen) und Comparison-Funktionen (Vergleichsfunktionen). Probe-Funktionen sammeln die Informationen, die benötigt werden, oder setzen eine entsprechende SIUmgebungsvariable, die Sie definieren. Probe-Funktionen werden zu Probe-Schlüsselwörtern. Comparison-Funktionen rufen die entsprechende Probe-Funktion auf, vergleichen die Ausgabe der Probe-Funktion und geben 0 zurück, wenn das Schlüsselwort übereinstimmt, bzw. 1, wenn das Schlüsselwort nicht übereinstimmt. Comparison-Funktionen werden zu Rule-Schlüsselwörtern. Siehe auch <i>rules-Datei.</i>
Betriebssystemserver	Ein System, das den Systemen in einem Netzwerk Dienste zur Verfügung stellt. Um Diskless Clients bedienen zu können, benötigt ein Betriebssystemserver Festplattenkapazitäten, die für die Root-Dateisysteme (/) und Swap-Bereiche der einzelnen Diskless Clients vorgesehen sind (/export/root, /export/swap).
Boot-Archiv	 Nur x86: Ein Boot-Archiv ist ein Satz grundlegender Systemdateien, die zum Booten von Solaris dienen. Diese Dateien werden beim Systemstart benötigt, bevor das Root-Dateisystem (/) eingehängt wird. Auf jedem System werden zwei Boot-Archive vorgehalten: Das Boot-Archiv, das zum Booten von Solaris verwendet wird. Dieses Archiv wird auch als "primäres" Boot-Archiv bezeichnet.
	 Das Boot-Archiv, das zur Wiederherstellung verwendet wird, falls das primäre Boot-Archiv beschädigt ist. Dieses Boot-Archiv startet das System, ohne das Root-Dateisystem (/) einzuhängen. Im GRUB-Menü wird dieses Boot-Archiv als "abgesichert" bezeichnet. Es dient hauptsächlich dazu, das primäre Boot-Archiv neu zu erzeugen (also das Boot-Archiv, mit dem das System normalerweise gestartet wird).

Boot-Loader	Nur x86 : Der Boot-Loader ist das erste Programm, das nach dem Einschalten eines Systems ausgeführt wird. Dieses Programm leitet den Boot-Vorgang ein.
Boot-Server	Ein Serversystem, das den Clientsystemen in Teilnetzen des gleichen Netzwerks die Programme und Daten zur Verfügung stellt, die diese zum Starten benötigen. Ein Boot-Server ist bei einer Installation über das Netzwerk erforderlich, wenn sich der Installationsserver in einem anderen Teilnetz befindet als die Systeme, auf denen die Solaris-Software installiert werden soll.
Boot-Umgebung	Eine Sammlung obligatorischer Dateisysteme (Festplatten-Slices und Einhängepunkte), die Voraussetzung für die Ausführung des Betriebssystems Solaris sind. Diese Festplatten-Slices können sich auf einer Festplatte befinden oder über mehrere Festplatten verteilt sein.
	Die aktive Boot-Umgebung ist die zum jeweiligen Zeitpunkt gebootete. Es kann immer nur eine aktive Boot-Umgebung gebootet sein. Eine inaktive Boot-Umgebung ist zum jeweiligen Zeitpunkt nicht gebootet, kann sich aber in einem Wartezustand befinden und auf Aktivierung beim nächsten Systemneustart warten.
Booten	Laden der Systemsoftware in den Hauptspeicher und starten dieser Software.
bootlog-cgi- Programm	Das CGI-Programm, das es einem Webserver ermöglicht, während einer WAN-Boot-Installation die Meldungen zum Booten entfernter Clients sowie die Installationskonsolen-Meldungen aufzunehmen und zu speichern.
CD	Optischer Datenträger (im Gegensatz zu einem magnetischen Datenträger), der die auf dem CD-Markt übliche Schreibung erkennt. Bei CD-ROMs und DVD-ROMs handelt es sich z. B. um optische Datenträger.
certificate authority (Zertifizierungsstelle)	(ZA, auch Zertifizierungsstelle) Eine vertrauenswürdige Fremdorganisation oder -firma, die digitale Zertifikate zum Zweck der Erstellung von digitalen Signaturen und Paaren öffentlicher und privater Schlüssel ausstellt. Der ZA garantiert, dass der Benutzer, für den ein eindeutiges Zertifikat ausgestellt wurde, wirklich ist, wer er/sie zu sein behauptet.
certstore- Datei	Eine Datei, die ein digitales Zertifikat für ein spezifisches Clientsystem enthält. Während einer SSL-Aushandlung wird der Client möglicherweise aufgefordert, dem Server diese Zertifikatdatei vorzulegen. Anhand dieser Datei verifiziert der Server die Client-Identität.
CGI	(Common Gateway Interface) Eine Schnittstelle, über die externe Programme mit dem HTTP-Server kommunizieren. Programme, die auf die Verwendung der CGI ausgerichtet sind, werden als CGI-Programme oder CGI-Skripten bezeichnet. CGI-Programme verarbeiten Formulare oder parsen Ausgaben, die der Server normalerweise nicht verarbeitet oder parst.
checksum	Das Ergebnis der Addition einer Gruppe von Datenelementen. Der Vorgang dient zum Überprüfen der Gruppe. Bei den Datenelementen kann es sich um Zahlen oder um andere Zeichenfolgen handeln. Auch diese werden bei der Prüfsummenberechnung wie Zahlen behandelt. Anhand des Prüfsummenwertes kann sichergestellt werden, dass die Kommunikation zwischen zwei Geräten erfolgreich war.

Client	Im Client-Server-Kommunikationsmodell ist der Client ein Prozess, der von fern auf Ressourcen auf einem Rechenserver zugreift, zum Beispiel auf Verarbeitungsleistung oder auf eine große Hauptspeicherkapazität.
Cluster	Eine logische Sammlung von Packages (Softwaremodulen). Die Solaris-Software ist in mehrere <i>Softwaregruppen</i> eingeteilt, die jeweils aus Clustern und <i>Packages</i> bestehen.
Dataset	Ein allgemeiner Name für die folgenden ZFS-Entitäten: Klone, Dateisysteme, Snapshots oder Volumes (Datenträger).
Datei rules.ok	Eine generierte Version der rules-Datei. Die Datei rules.ok wird von der benutzerdefinierten JumpStart-Installationssoftware dazu benötigt, ein System einem Profil zuzuordnen. Zum Erstellen der Datei rules.ok <i>muss</i> das Skript check verwendet werden.
Dateiserver	Ein Server, der als Speicher für die Software und die Dateien für die Systeme in einem Netzwerk dient.
decryption (Entschlüsselung)	Der Vorgang, bei dem kodierte Daten in Normaltext konvertiert werden. Siehe auch encryption (Verschlüsselung).
DES	(Data Encryption Standard) Eine 1981 entwickelte und 3 als ANSI X.92.56 von ANSI standardisierte symmetrische Verschlüsselungsmethode. DES verwendet einen 56-Bit-Schlüssel.
DHCP	(Dynamic Host Configuration Protocol) Ein Protokoll der Anwendungsschicht (Application Layer). Ermöglicht es einzelnen Computern bzw. Clients in einem TCP/IP-Netzwerk, eine IP-Adresse oder andere Netzwerkkonfigurationsinformationen von einem oder mehreren designierten und zentral gepflegten DHCP-Servern zu extrahieren. Die verringert den Aufwand für die Pflege und Verwaltung großer IP-Netzwerke.
Dienstprogramm	Ein Standardprogramm, das beim Kauf eines Computers in der Regel im Preis inbegriffen ist und für verschiedene interne Funktionen des Computers zuständig ist.
Differenzarchiv	Ein Solaris Flash-Archiv, das nur die Unterschiede zwischen zwei Systemabbildern, einem unveränderten und einem aktualisierten Master-Abbild, enthält. Ein Differenzarchiv enthält die auf dem Klonsystem beizubehaltenden, zu ändernden oder zu löschenden Dateien. Eine solche differentielle Aktualisierung ändert nur die angegebenen Dateien und kann nur auf Systeme angewendet werden, deren Software mit derjenigen des unveränderten Master-Abbilds übereinstimmt.
Digitales Zertifikat	Eine nicht übertragbare, unfälschbare digitale Datei, die von einer Stelle ausgestellt wurde, die für beide Kommunikationspartner bereits als vertrauenswürdig gilt.
Diskless Client	Ein Client in einem Netzwerk, der als Festplattenspeicher einen Server benötigt.
Dokument-Root-Verzeichnis	Der Ursprung einer Hierarchie auf einem Webserver, auf dem sich die Dateien, Grafiken und Daten befinden, die Sie den auf den Webserver zugreifenden Benutzern zur Verfügung stellen möchten.
Domäne	Ein Teil der Namenshierarchie im Internet. Eine Domäne ist eine Gruppe von Systemen in einem lokalen Netzwerk, die Administrationsdateien gemeinsam nutzen.

Domänenname	Der Name einer Gruppe von Systemen in einem lokalen Netzwerk, die Administrationsdateien gemeinsam nutzen. Der Domänenname ist erforderlich, damit der Network Information Service (NIS) ordnungsgemäß funktioniert. Ein Domain-Name besteht aus einer Folge von Komponentennamen, die durch Punkte getrennt sind (Beispiel: tundra.mpk.ca.us). Der Domänenname wird von links nach rechts gelesen. Weiter links stehen also die Komponentennamen von übergeordneten (und in der Regel weiter entfernten) administrativen Bereichen.
Einhängen	Der Zugriff auf ein Verzeichnis von einer Festplatte aus, die mit einem Rechner verbunden ist, welcher die Einhängeanforderung absetzt, oder von einer entfernten Festplatte in einem Netzwerk aus. Zum Einhängen eines Dateisystems ist ein Einhängepunkt auf dem lokalen System erforderlich und der Name des einzuhängenden Dateisystems muss bekannt sein (zum Beispiel /usr).
Einhängepunkt	Ein Workstation-Verzeichnis, in das ein Dateisystem eingehängt wird, das auf einem entfernten Rechner residiert.
encryption (Verschlüsselung)	Der Vorgang, bei dem Daten unverständlich gemacht werden, um sie vor unberechtigten Zugriffen zu schützen. Die Verschlüsselung basiert auf einem Code, dem Schlüssel (key), mit dem die Daten wieder entschlüsselt werden. Siehe auch decryption (Entschlüsselung).
Erstinstallation / Neuinstallation	Eine Installation, bei der die aktuell installierte Software überschrieben oder eine leere Festplatte initialisiert wird.
	Mit einer Neu- bzw. Erstinstallation des Solaris-BS wird die Festplatte (bzw. mehrere) des Systems mit der neuen Version des Solaris-BS überschrieben. Wenn das Solaris-BS nicht auf dem System läuft, müssen Sie eine Neuinstallation ausführen. Wenn eine upgrade-fähige Version des Solaris-BS auf dem System läuft, wird bei einer Neuinstallation die Festplatte überschrieben und weder das BS noch lokale Änderungen werden beibehalten.
/etc/netboot- Verzeichnis	Das Verzeichnis auf einem WAN-Boot-Server, in dem sich die für eine WAN-Boot-Installation erforderlichen Client-Konfigurationsinformationen und Sicherheitsdaten befinden.
/etc-Verzeichnis	Ein Verzeichnis mit wichtigen Systemkonfigurationsdateien und Wartungsbefehlen.
/export- Dateisystem	Ein Dateisystem auf einem Betriebssystemserver, das mit anderen Systemen im Netzwerk gemeinsam genutzt wird. Das Dateisystem /export zum Beispiel kann das Root-Dateisystem (/) und den Swap-Bereich für Diskless Clients sowie die Home-Verzeichnisse für Benutzer im Netzwerk enthalten. Diskless Clients benötigen das Dateisystem /export auf einem Betriebssystemserver, damit sie booten und laufen können.
Fallback	Das System greift auf die Umgebung zurück, die zuvor ausgeführt wurde. Ein Fallback ist erforderlich, wenn Sie eine Boot-Umgebung aktivieren und die Boot-Umgebung, mit der gebootet werden soll, fehlschlägt oder ein unerwünschtes Verhalten zeigt.

fdisk- Partition	Eine logische Partition auf einem Festplattenlaufwerk bei x86-basierten Systemen, die für ein bestimmtes Betriebssystem vorgesehen ist. Zum Installieren der Solaris-Software muss auf einem x86-basierten System mindestens eine fdisk-Partition eingerichtet werden. Bei x86-basierten Systemen sind bis zu vier verschiedene fdisk-Partitionen pro Festplatte zulässig. Diese Partitionen können einzelne Betriebssysteme aufnehmen. Jedes Betriebssystem muss sich in einer eindeutigen fdisk-Partition befinden. Ein System kann nur eine Solaris fdisk-Partition pro Festplatte aufnehmen.
Festplatte	Magnetischer Datenträger, bestehend aus einer runden Platte oder Gruppe von Platten, eingeteilt in konzentrische Spuren und Sektoren. Dient zum Speichern von Daten, zum Beispiel in Dateien. Siehe auch CD (optischer Datenträger).
Festplatten- konfigurationsdatei	Eine Datei, die die Struktur einer Festplatte angibt (z. B. Byte/Sektor, Flags, Slices). Festplattenkonfigurationsdateien ermöglichen die Verwendung des Befehls pfinstall, um von einem einzelnen System aus Profile auf Festplatten unterschiedlicher Größe zu testen.
Dateisystem	Im Betriebssystem SunOS ein Netzwerk von Dateien und Verzeichnissen in einer Baumstruktur, auf die zugegriffen werden kann.
Finish-Skript	Ein benutzerdefiniertes Bourne-Shell-Skript, angegeben in der rules-Datei, das Aufgaben ausführt, nachdem die Solaris-Software auf dem System installiert wurde, aber bevor das System neu gestartet wird. Finish-Skripten werden bei benutzerdefinierten JumpStart-Installationen eingesetzt.
format	Daten in eine bestimmte Struktur bringen oder eine Festplatte in Sektoren aufteilen, so dass darauf Daten gespeichert werden können.
Funktionstasten	Die mindestens 10 Tasten auf der Tastatur mit der Bezeichnung F1, F2, F3 usw., denen bestimmte Funktionen zugeordnet sind.
Gemeinsam genutzte Dateisysteme	Dateisysteme, bei denen es sich um benutzerdefinierte Dateien handelt, zum Beispiel /export/home und /swap. Diese Dateisysteme werden von der aktiven und der inaktiven Boot-Umgebung gemeinsam genutzt, wenn Sie Solaris Live Upgrade verwenden. Gemeinsam genutzte Dateisysteme enthalten in der aktiven und der inaktiven Boot-Umgebung den gleichen Einhängepunkt in der Datei vfstab. Eine Aktualisierung der gemeinsam genutzten Dateien in der aktiven Boot-Umgebung bewirkt gleichzeitig auch eine Aktualisierung der Daten in der inaktiven Boot-Umgebung. Gemeinsame genutzte Dateisysteme werden standardmäßig gemeinsam genutzt. Sie können jedoch ein Ziel-Slice angeben. Daraufhin werden die Dateisysteme kopiert.
Gesamte Solaris-Softwaregruppe	Eine Softwaregruppe, die die vollständige Solaris-Version enthält.
Gesamte Solaris-Softwaregruppe plus OEM-Unterstützung	Eine Softwaregruppe, die das vollständige Solaris-Version plus zusätzliche Hardwareunterstützung für OEMs enthält. Diese Softwaregruppe ist zu empfehlen, wenn die Solaris-Software auf SPARC-Servern installiert werden soll.

Globale Zone	In Solaris Zones gilt die globale Zone sowohl als Standardzone des Systems als auch als Zone für die systemweite Administrationssteuerung. Die globale Zone ist die einzige Zone, von der aus eine nicht-globale Zone konfiguriert, installiert, verwaltet oder deinstalliert werden kann. Die Verwaltung der Systeminfrastruktur, wie beispielsweise physische Geräte, das Routing oder die dynamische Rekonfiguration (DR), ist nur in der globalen Zone möglich. Entsprechend privilegierte Prozesse, die in der globalen Zone ausgeführt werden, können auf Objekte zugreifen, die anderen Zonen zugewiesen sind. Siehe auch <i>Solaris Zones</i> und <i>Nicht-globale Zone</i> .
GRUB	Nur x86 : Der GNU GRand Unified Bootloader (GRUB) ist ein Open-Source-Boot-Loader mit einer einfachen Menüoberfläche. Das Menü zeigt eine Liste mit den Betriebssystemen, die auf dem betreffenden System installiert sind. Über GRUB lassen sich diese unterschiedlichen Betriebssysteme (z. B. Solaris, Linux oder Microsoft Windows) komfortabel starten.
GRUB-Bearbeitungsmenü	Nur x86 : Ein Boot-Menü, das dem GRUB-Hauptmenü untergeordnet ist. Es enthält verschiedene GRUB-Befehle. Mit diesem Befehlen lässt sich das Boot-Verhalten anpassen.
GRUB-Hauptmenü	Nur x86: Ein Boot-Menü mit der Liste der Betriebssysteme, die auf dem betreffenden System installiert sind. Über dieses Menü können Sie komfortabel ein bestimmtes Betriebssystem starten, ohne dafür die fdisk-Partitionseinstellungen oder die BIOS-Konfiguration ändern zu müssen.
Hard Link	Ein Verzeichniseintrag, der auf eine Datei auf einer Festplatte verweist. Mehrere dieser Verzeichniseinträge können auf die gleiche physische Datei verweisen.
hash	Eine Zahl, die aus einer Eingabe generiert wird und wesentlich kürzer ist als diese Eingabe. Für identische Eingaben wird stets derselbe Ausgabewert generiert. Hash-Funktionen lassen sich in Tabellensuchalgorithmen, bei der Fehlersuche und Manipulationserkennung einsetzen. Für die Manipulationserkennung werden die Hash-Funktionen so gewählt, dass es unwahrscheinlich ist, dasselbe Hash-Ergebnis für zwei Eingaben zu erhalten. MD5 und SHA-1 sind Beispiele für Einweg-Hash-Funktionen. Beispielsweise reduziert ein Meldungs-Digest eine Eingabe variabler Länge auf einen kleinen Wert.
Hashing	Der Vorgang, bei dem eine aus Buchstaben bestehende Zeichenkette in einen Wert oder Schlüssel umgeformt wird, der die ursprüngliche Zeichenkette darstellt.
HMAC	Verschlüsselte Hashing-Methode zur Nachrichtenauthentifizierung. HMAC wird mit einer iterativen kryptografischen Hash-Funktion wie MD5 oder SHA-1 zusammen mit einem geheimen gemeinsam genutzten Schlüssel verwendet. Die kryptografischen Stärke von HMAC hängt von den Eigenschaften der zu Grunde liegenden Hash-Funktion ab.
Host-Name	Der Name, unter dem ein System den anderen Systemen im Netzwerk bekannt ist. Dieser Name muss unter den Systemen in einer Domain (in der Regel bedeutet das innerhalb einer Organisation) eindeutig sein. Ein Host-Name kann aus einer beliebigen Kombination von Buchstaben, Ziffern und Minuszeichen (-) bestehen, kann aber nicht mit einem Minuszeichen beginnen oder enden.
НТТР	(Hypertext Transfer Protocol) (n.) Das Internet-Protokoll, das Hypertext-Objekte von Remote-Hosts abruft. Dieses Protokoll basiert auf TCP/IP.

HTTPS	Eine sichere Version von HTTP, die unter Verwendung von SSL (Secure Sockets Layer) implementiert wird.
Installationsserver	Ein Server, der die Solaris-DVD- oder -CD-Abbilder zur Verfügung stellt, von denen andere Systeme in einem Netzwerk Solaris installieren können (auch bekannt als <i>Medienserver</i>). Sie können einen Installationsserver erstellen, indem Sie die Solaris-DVD- bzwCD-Abbilder auf die Serverfestplatte kopieren.
IPv6	IPv6 ist eine Version (Version 6) des Internet Protocol (IP), die einen Entwicklungsschritt über die aktuelle Version IPv4 (Version 4) hinaus darstellt. Die Bereitstellung von IPv6 mithilfe definierter Umsetzungsmechanismen unterbricht den aktuellen Systembetrieb nicht. Darüber hinaus liefert IPv6 eine Plattform für eine neue Internet-Funktionalität.
JumpStart-Installation	Ein Installationstyp, bei dem die Solaris-Software automatisch auf einem System installiert wird, und zwar mithilfe der werkseitig installierten JumpStart-Software.
JumpStart-Verzeichnis	Bei benutzerdefinierten JumpStart-Installationen von einer Profildiskette entspricht das JumpStart-Verzeichnis dem Root-Verzeichnis auf der Diskette, das alle wichtigen, benutzerdefinierten JumpStart-Dateien enthält. Bei benutzerdefinierten JumpStart-Installationen von einem Profilserver entspricht das JumpStart-Verzeichnis dem Verzeichnis auf dem Server, das alle wichtigen, benutzerdefinierten JumpStart-Dateien enthält.
Kerberos	Ein Netzwerkauthentisierungsprotokoll, das es mithilfe einer leistungsstarken Kryptographie mit geheimen Schlüsseln Clients und Servern ermöglicht, einander über eine nicht abgesicherte Netzwerkverbindung zuverlässig zu identifizieren.
keystore- Datei	Eine Datei, in der sich die von Client und Server gemeinsam verwendeten Schlüssel befinden. Bei einer WAN-Boot-Installation dienen die Schlüssel dem Clientsystem zur Überprüfung der Integrität der vom Server übertragenen Daten und Dateien oder zum Entschlüsseln dieser.
Klonsystem	Ein System, das mithilfe eines Solaris Flash-Archivs installiert wurde. Das Klonsystem hat dieselbe Installationskonfiguration wie das Mastersystem.
Kritische Dateisysteme	Für das Solaris-BS unabdingbare Dateisysteme. Wenn Sie Solaris Live Upgrade verwenden, sind diese Dateisysteme separate Einhängepunkte in der Datei vfstab der aktiven und der inaktiven Boot-Umgebung. Dateisysteme sind beispielsweise root (/), /usr, /var und /opt. Diese Dateisysteme werden immer von der Quelle in die inaktive Boot-Umgebung kopiert.
LAN	(Local Area Network) Eine Gruppe von nahe beieinander installierten Computersystemen, die über Verbindungshardware und -software miteinander kommunizieren können.
LDAP	(Lightweight Directory Access Protocol) Ein erweiterbares Standardprotokoll für den Zugriff auf Verzeichnisse, das bei der Kommunikation zwischen Clients und Servern des LDAP-Namen-Services zum Einsatz kommt.
locate (Gebietsschema)	Ein Gebiet in geografischen oder politischen Grenzen, in dem die gleiche Sprache, die gleichen Sitten und die gleichen kulturellen Konventionen gelten. Die englische Sprachumgebung für die USA heißt zum Beispiel en_US, die für Großbritannien heißt en_UK.

Logisches Gerät	Eine Gruppe physischer Slices auf einer oder mehreren Festplatten, die im System als ein einziges logisches Gerät erscheinen. In Solaris Volume Manager wird ein logisches Gerät Volume genannt. Für eine Anwendung oder ein Dateisystem sind Volumes, was ihre Funktionsweise angeht, mit einer physischen Festplatte identisch.
Manifest-Teil	Ein Teil eines Solaris Flash-Archivs, der zur Überprüfung des Klonsystems dient. Im Manifest-Teil sind die Dateien eines Systems aufgeführt, die auf dem Klonsystem beibehalten, ergänzt oder gelöscht werden sollen. Dieser Teil ist rein informativ. Die Dateien sind in einem internen Format aufgeführt, sodass dieser Teil nicht zum Skripting verwendet werden kann.
Mastersystem	Ein System, mit dem ein Solaris Flash-Archiv erstellt wird. Die Systemkonfiguration wird in dem Archiv gespeichert.
MD5	(Message Digest 5) Eine iterative kryptographische Hash-Funktion für die Meldungs-Authentifizierung, einschließlich digitaler Signaturen. Diese Funktion wurde 1991 von Rivest entwickelt.
Medienserver	Siehe Installationsserver.
menu.lst (Datei)	Nur x86: Eine Datei mit einer Liste aller Betriebssysteme, die auf dem betreffenden System installiert sind. Der Inhalt dieser Datei legt fest, welche Betriebssysteme im GRUB-Hauptmenü erscheinen. Über das GRUB-Hauptmenü können Sie komfortabel ein bestimmtes Betriebssystem starten, ohne dafür die fdisk-Partitionseinstellungen oder die BIOS-Konfiguration ändern zu müssen.
Metagerät	Siehe Volume.
Miniroot	Ein minimales root-Dateisystem mit Bootfähigkeit (/), das auf dem Solaris-Installationsdatenträger enthalten ist. Eine Miniroot besteht aus der Solaris-Software, mit der Systeme installiert und aktualisiert werden können. Auf x86-basierten Systemen wird die Miniroot in das System kopiert, damit es dort als Failsafe-Bootarchiv verfügbar ist. Siehe <i>Failsafe-Bootarchiv</i> .
Mirror	Siehe RAID-1-Volume.
Namen-Server	Ein Server, der den Systemen in einem Netzwerk einen Namen-Service zur Verfügung stellt.
Namen-Service	Eine verteilte Netzwerkdatenbank, die grundlegende Systeminformationen über alle Systeme im Netzwerk enthält, so dass die Systeme miteinander kommunizieren können. Ist ein Namen-Service vorhanden, können die Systeminformationen netzwerkweit gepflegt und verwaltet und es kann netzwerkweit darauf zugegriffen werden. Ohne Namen-Service muss auf jedem System eine eigene Kopie der Systeminformationen gepflegt werden (in den lokalen /etc-Dateien). Sun unterstützt die folgenden Namen-Services: LDAP, NIS und NIS+.
Netzwerkinstallation	Eine Möglichkeit, Software über das Netzwerk zu installieren, und zwar von einem System mit CD-ROM- oder DVD-ROM-Laufwerk auf einem System ohne CD-ROM- oder DVD-ROM-Laufwerk. Für Netzwerkinstallationen sind ein <i>Namen-Server</i> und ein <i>Installationsserver</i> erforderlich.

Nicht-globale Zone	Eine virtuelle Betriebssystemumgebung, die in einer bestimmten Instanz des Betriebssystems Solaris erstellt wurde. In einer nicht-globalen Zone können Anwendungen ausgeführt werden, ohne dass sie in irgendeiner Form mit dem Rest des Systems interagieren. Nicht-globale Zonen werden auch kurz als Zonen bezeichnet. Siehe auch <i>Solaris Zones</i> und <i>globale Zone</i> .
Nicht vernetzte Systeme	Systeme, die nicht an ein Netzwerk angeschlossen sind und keine anderen Systeme benötigen.
NIS	Der Netzwerkinformationsservice von SunOS 4.0 (Minimum). Eine verteilte Netzwerkdatenbank mit grundlegenden Informationen über die Systeme und die Benutzer im Netzwerk. Die NIS-Datenbank wird auf dem Master-Server und allen Slave-Servern gespeichert.
NIS+	Der Netzwerkinformationsservice von SunOS 5.0 (Minimum). NIS+ ersetzt NIS, den Netzwerkinformationsservice SunOS 4.0 (Minimum).
/opt-Dateisystem	Ein Dateisystem, das die Einhängepunkte für Software von Drittanbietern und nicht in einem Package enthaltene Software enthält.
Package	Eine Sammlung von Software, die für die modulare Installation zu einer Einheit zusammengefasst wurde. Die Solaris-Software ist in mehrere <i>Softwaregruppen</i> eingeteilt, die jeweils aus Clustern und <i>Packages</i> bestehen.
Patch Analyzer	Ein Skript, das Sie von Hand oder als Teil des Solaris-Installationsprogramms ausführen können. Patch Analyzer analysiert das System und ermittelt, welche Patches gegebenenfalls bei einem Upgrade auf ein aktualisiertes Solaris-Release entfernt werden.
Pfeiltasten	Die vier Richtungstasten auf dem numerischen Tastenblock.
Plattformgruppe	Eine vom Anbieter definierte Gruppe von Hardwareplattformen für die Distribution einer bestimmten Software. Beispiele für gültige Plattformgruppen sind i86pc und sun4u.
Plattformname	Die Ausgabe des Befehls uname -i. Der Plattformname der Ultra 60 lautet beispielsweise SUNW,Ultra-60.
Pool	Eine logische Gruppe von Geräten, die das Layout und die physischen Merkmale des verfügbaren ZFS-Speichers beschreibt. Datensätzen wird Speicher aus einem Pool zugewiesen.
Power Management	Software, die den Status eines Systems automatisch speichert und dieses System nach 30 Minuten Inaktivität herunterfährt. Wenn Sie die Solaris-Software auf einem System installieren, das der Version 2 der Energy Star-Richtlinien der amerikanischen Umweltbehörde entspricht, wird die Power Management-Software standardmäßig installiert. Ein Beispiel für ein System, bei dem die Power Management-Software standardmäßig installiert ist, ist ein sun4u SPARC-basiertes System. Nach einem Neustart werden Sie dann dazu aufgefordert, Power Management zu aktivieren bzw. zu deaktivieren. Die Energy Star-Richtlinien erfordern, dass Systeme bzw. Monitore automatisch in einen "Sleep-Modus" (Verbrauch von 30 Watt oder weniger) wechseln, in welchem System oder

Primäres Boot-Archiv	Ein Boot-Archiv, das zum Booten von Solaris verwendet wird. Dieses Archiv wird auch als "primäres" Boot-Archiv bezeichnet. Siehe <i>Boot-Archiv</i> .
Privater Schlüssel	Auch private key. Der Entschlüsselungs-Code für die Verschlüsselung mit öffentlichen Schlüsseln (public-key).
Probe-Schlüsselwort	Ein syntaktisches Element, das bei der benutzerdefinierten JumpStart-Installation Attributinformationen über ein System abruft. Im Gegensatz zu Regeln ist es bei Probe-Schlüsselwörtern nicht erforderlich, Übereinstimmungskriterien einzurichten und Profile auszuführen. Siehe auch <i>Regel</i> .
Profil	Eine Textdatei, in der festgelegt ist, wie die Solaris-Software bei einem benutzerdefinierten JumpStart-Verfahren installiert werden soll. So ist in einem Profil beispielsweise die zu installierende Softwaregruppe definiert. Jede Regel spezifiziert ein Profil, das definiert, wie ein System installiert werden soll, wenn es der Regel entspricht. Sie können für jede Regel ein eigenes Profil erstellen. Sie können ein Profil jedoch auch in mehreren Regeln verwenden. Siehe auch <i>rules-Datei</i> .
Profildiskette	Eine Diskette mit allen wichtigen, benutzerdefinierten JumpStart-Dateien im Root-Verzeichnis (JumpStart-Verzeichnis).
Profilserver	Ein Server mit allen wichtigen, benutzerdefinierten JumpStart-Dateien in einem JumpStart-Verzeichnis.
public key (Öffentlicher Schlüssel)	Der Verschlüsselungsschlüssel, der bei der Verschlüsselung mit öffentlichen Schlüsseln zum Einsatz kommt.
public-key cryptography (Verschlüsselung mit öffentlichen Schlüsseln)	Ein Kryptographiesystem, bei dem zwei Schlüssel verwendet werden: ein öffentlicher, allen bekannter Schlüssel und ein privater Schlüssel, den nur der Nachrichtenempfänger kennt.
RAID-0-Volume	Eine Volumenart, bei der es sich um einen Streifen (Stripe) oder eine Verkettung handeln kann. Diese Komponenten werden auch Submirrors genannt. Ein Stripe oder eine Verkettung stellt den Grundbaustein für einen Mirror dar.
RAID-1-Volume	Eine Volume-Art, bei der Daten durch die Vorhaltung mehrerer Kopien repliziert werden. Ein RAID-1-Volume besteht aus einem oder mehreren RAID-0-Volumes; diese werden <i>Submirrors</i> genannt. RAID-1-Volumes werden manchmal auch als <i>Mirrors</i> bezeichnet.
RAID-Z Storage Pool	Ein virtuelles Gerät, das Daten und Parität auf mehreren Platten speichert, die als ein ZFS-Speicherpool verwendet werden können. RAID-Z ähnelt RAID-5.
Regel	Eine Folge von Werten, die einem Profil eine oder mehrere Systemattribute zuordnet. Bei benutzerdefinierten JumpStart-Installationen werden Regeln eingesetzt.
Root	Als Stamm- oder "Root"-Ebene bezeichnet man die oberste Ebene in einer Elementhierarchie. Alle anderen Elemente sind vom Stamm- bzw. Root-Element abhängig. Siehe <i>Rootverzeichnis</i> oder <i>root (/) Dateisystem</i> .

Root-Dateisystem (/)	Das oberste Dateisystem, das alle anderen Dateisysteme unter sich enthält. Alle anderen Dateisysteme sind im Root-Dateisystem (/) eingehängt, und dieses wird niemals ausgehängt. Das Root-Dateisystem (/) enthält die Verzeichnisse und Dateien, die für den Systembetrieb unverzichtbar sind, zum Beispiel den Kernel, die Gerätetreiber und die Programme, die zum Starten (Booten) eines Systems verwendet werden.
Root-Verzeichnis	Die oberste Verzeichnisebene, die alle anderen Verzeichnisse unter sich enthält.
rules- Datei	Eine Textdatei, die eine Regel für jede Gruppe von Systemen oder für Einzelsysteme enthält, die automatisch installiert werden sollen. Jede Regel charakterisiert eine Gruppe von Systemen auf der Grundlage von einem oder mehreren Systemattributen. Die Datei rules verknüpft jede Gruppe mit einem Profil, einer Textdatei, die definiert, wie die Solaris-Software auf allen Systemen in der Gruppe installiert wird. Eine rules-Datei kommt bei benutzerdefinierten JumpStart-Installationen zum Einsatz. Siehe auch <i>Profil</i> .
Schlüssel	Der Code zum Ver- oder Entschlüsseln von Daten (auch als "Key" bezeichnet). Siehe auch encryption (Verschlüsselung).
server	$Ein Netzwerkger \"at, das Ressourcen verwaltet und einem Client Dienste zur Verf \" gung stellt.$
SHA1	(Secure Hashing Algorithm) Dieser Algorithmus erzeugt Meldungs-Digests für Eingaben mit einer Länge von weniger als 2^{64} .
Slice	Auch Bereich. Die Einheiten, in die der Platz auf der Festplatte von der Software unterteilt wird.
snapshot	Ein schreibgeschütztes Abbild eines ZFS-Dateisystems oder eines Volumens einem bestimmten Zeitpunkt.
Softwaregruppe	Eine logische Zusammenstellung der Solaris-Software (bestehend aus Clustern und Packages). Bei einer Solaris-Installation können Sie eine der folgenden Softwaregruppen installieren: die Softwaregruppen für die Hauptsystemunterstützung, Endbenutzer, Entwickler, die gesamte Solaris-Softwaregruppe und, nur auf SPARC-Systemen, die gesamte Solaris-Softwaregruppe plus OEM-Unterstützung.
Softwaregruppe für zentrales System (Core)	Eine Softwaregruppe, die die zum Booten und zum Ausführen des Solaris-BS auf einem System erforderliche Minimalsoftware enthält. Core enthält etwas Netzwerksoftware sowie die Treiber zum Ausführen des CDE-Desktop (Common Desktop Environment-Desktop). Die CDE-Software selbst enthält sie nicht.
Softwaregruppe mit eingeschränkter Netzwerkunterstützung	Eine Softwaregruppe, die den zum Booten und Ausführen eines Solaris-Systems mit eingeschränkter Netzwerkunterstützung mindestens erforderlichen Code enthält. Die Softwaregruppe mit eingeschränkter Netzwerkunterstützung bietet eine textbasierte Mehrbenutzerkonsole und Dienstprogramme für die Systemverwaltung. Mit dieser Softwaregruppe kann ein System Netzwerkschnittstellen erkennen, aktiviert aber keine Netzwerkdienste.
Solaris-DVD- oder -CD-Abbilder	Die Solaris-Software, die auf einem System installiert wird und die auf Solaris-DVDs, -CDs oder der Festplatte eines Installationsservers zur Verfügung steht, auf die die Solaris-DVD- oder -CD-Abbilder kopiert wurden.

Solaris Flash	Eine Solaris-Installationsfunktion, mit deren Hilfe Sie ein Archiv der Dateien auf einem System erstellen können <i>Mastersystem</i> genannt). Mithilfe dieses Archivs können dann weitere Systeme installiert werden. Diese sind in ihrer Konfiguration mit dem Mastersystem identisch. Siehe auch <i>-Archiv</i> .
Solaris-Installationsprogramm	Ein Installationsprogramm mit einer grafischen Benutzeroberfläche (GUI) oder Befehlszeilenschnittstelle (CLI), das den Benutzer mithilfe von Assistentenfenstern Schritt für Schritt durch die Installation der Solaris-Software und die Software von Drittanbietern führt.
Solaris Live Upgrade	Eine Upgrade-Methode, bei welcher das Upgrade in einer zuvor duplizierten Boot-Umgebung ausgeführt wird, während die aktive Boot-Umgebung weiter in Betrieb ist, so dass es nicht zu Ausfällen der Produktionsumgebung kommt.
Solaris-Softwaregruppe für Endbenutzer	Eine Softwaregruppe, die die Softwaregruppe für zentrales System (Core) plus die empfohlene Software für einen Endbenutzer enthält, einschließlich Common Desktop Environment (CDE) und DeskSet-Software.
Solaris-Softwaregruppe für Entwickler	Eine Softwaregruppe, die die Solaris-Softwaregruppe für Endanwender und zusätzlich die Bibliotheken, Include-Dateien, Manpages und Programmiertools für die Entwicklung von Software enthält.
Solaris Zones	Eine Software-Partitionierungstechnologie, die zum Virtualisieren von Betriebssystemdiensten und Bereitstellen einer isolierten, sicheren Umgebung zum Ausführen von Anwendungen dient. Indem Sie eine nicht-globale Zone erstellen, erzeugen Sie eine Umgebung für die Ausführung von Anwendungen, in der Prozesse von allen anderen Zonen isoliert sind. Durch diese Isolierung wird verhindert, dass Prozesse, die in einer Zone laufen, Prozesse in anderen Zonen überwachen oder in sie eingreifen. Siehe auch <i>Globale Zone</i> und <i>Nicht-globale Zone</i> .
SSL (Secure Sockets Layer)	Eine Softwarebibliothek, die eine sichere Verbindung zwischen zwei Seiten (Client und Server) ermöglicht und zur Implementierung von HTTPS, der sicheren Version von HTTP, verwendet wird.
Standalone	Ein Computer, der als eigenständiges Gerät läuft und keine Unterstützung durch andere Rechner benötigt.
State Database	Eine Statusdatenbank oder State Database speichert Informationen zum Status Ihrer Solaris Volume Manager-Konfiguration auf einer Festplatte ab. Die State Database ist eine Sammlung aus mehreren replizierten Kopien der Datenbank. Jede dieser Kopien wird als <i>Statusdatenbankreplikation</i> bezeichnet. Die Statusdatenbank überwacht und speichert Angaben zu Speicherort und Status aller bekannten Statusdatenbankreplikationen.
State Database Replica	Eine Kopie einer Statusdatenbank. Die Replica garantiert die Integrität der Datenbankdaten.
Submirror	Siehe RAID-0-Volume.
Subnetz	Ein Schema, bei dem ein logisches Netzwerk in kleinere physische Netzwerke zerlegt wird, um das Routing zu vereinfachen.

Superuser	Ein besonderer Benutzer, der berechtigt ist, alle Administrationsvorgänge auf dem System auszuführen. Der Superuser kann lesend und schreibend auf alle Dateien zugreifen, er kann alle Programme ausführen und die Beendigung beliebiger Prozesse erzwingen.
Swap-Bereich	Ein Slice oder eine Datei zur temporären Aufnahme von Hauptspeicherinhalten, bis diese Inhalte wieder in den Hauptspeicher zurückgeladen werden können. Auch bekannt als Dateisystem / swap oder swap.
sysidcfg	Eine Datei, in der eine Reihe spezieller Systemkonfigurationsschlüsselwörter angegeben werden können, die ein System vorkonfigurieren.
Systemkonfigurations- datei	(system.conf) Eine Textdatei, in der Sie angeben, wo die Datei sysidcfg und die Dateien für die benutzerdefinierte JumpStart-Installation gespeichert sind, die Sie für eine WAN-Boot-Installation verwenden möchten.
Teilnetzmaske	Eine Bit-Maske zur Auswahl von Bits aus einer IP-Adresse für die Adressierung eines Teilnetzes. Die Maske ist 32 Bit lang und wählt den Netzwerkanteil der IP-Adresse sowie 1 oder mehrere Bits des lokalen Adressanteils aus.
time zone (Zeitzone)	Die 24 nach Längengraden eingeteilten Abschnitte der Erdoberfläche, für die eine bestimmte Standardzeit gilt.
truststore- Datei	Eine Datei, die ein oder mehrere digitale Zertifikate enthält. Bei einer WAN-Boot-Installation überprüft das Clientsystem auf Grundlage der Daten in der Datei truststore die Identität des Servers, der die Installation durchzuführen versucht.
Upgrade, Aufstufung, Aufrüstung	Eine Installation, bei der neue Dateien mit vorhandenen vereint und Änderungen soweit wie möglich beibehalten werden.
	Ein Upgrade des Solaris-BS vereint die neue Solaris-Version mit den auf der Systemfestplatte (bzw. Festplatten) vorhandenen Dateien. Dabei werden möglichst viele der Änderungen gespeichert, die Sie an der vorherigen Version des Solaris-BS vorgenommen haben.
Upgrade-Option	Eine Option des Programms Solaris-Installationsprogramm. Bei einem Upgrade wird die neue Version von Solaris mit den vorhandenen Dateien auf der Festplatte bzw. den Festplatten zusammengeführt. Bei einem Upgrade werden möglichst viele der lokalen Modifikationen beibehalten, die seit der letzten Installation von Solaris vorgenommen wurden.
URL	(Uniform Resource Locator) Das Adressiersystem, mit dessen Hilfe Client und Server Dokumente abrufen. Ein URL wird auch häufig als Position bezeichnet. URLs haben das Format <i>Protokoll://Rechner:Port/Dokument</i> .
	Ein Beispiel ist http://www.Beispiel.com/index.html.
/usr- Dateisystem	Ein Dateisystem auf einem Standalone-System oder Server, das viele der Standard-UNIX-Programme enthält. Die gemeinsame Nutzung des großen Dateisystems /usr auf einem Server statt der Pflege einer lokalen Kopie dieses Dateisystems verringert den Gesamtbedarf an Festplattenplatz zum Installieren und Ausführen der Solaris-Software auf einem System.

/var-Dateisystem	Ein Dateisystem oder Verzeichnis (auf Standalone-Systemen) mit Systemdateien, die sich im Zuge der Systemnutzung in der Regel ändern oder wachsen. Zu diesen Dateien gehören Systemprotokolle, vi-Dateien, Mail-Dateien und UUCP-Dateien.
Verkettung	Ein RAID-0-Volume. Bei der Verkettung von Slices werden Daten so lange auf das erste verfügbare Slice geschrieben, bis dieses voll ist. Sobald ein Slice voll ist, werden die Daten auf das jeweils folgende Slice geschrieben. Verkettungen bieten keine Datenredundanz, es sei denn, sie sind Bestandteil eines Mirrors. Siehe auch: RAID-0-Volume.
Vernetzte Systeme	Eine Gruppe von Systemen ("Hosts" genannt), die über Hardware und Software verbunden sind, so dass sie miteinander kommunizieren und Informationen austauschen können. Ein solches System wird als Local Area Network (lokales Netzwerk - LAN) bezeichnet. In vernetzten Systemen sind in der Regel ein oder mehrere Server erforderlich.
Virtuelles Gerät	Ein logisches Gerät in einem ZFS-Pool, bei dem es sich um eine physikalisches Gerät, eine Datei oder eine Sammlung von Geräten handeln kann.
volume	Eine Gruppe physischer Slices oder anderer Volumes, die im System als ein einziges logisches Gerät erscheinen. Für eine Anwendung oder ein Dateisystem sind Volumes, was ihre Funktionsweise angeht, mit einer physischen Festplatte identisch.
	In manchen Befehlszeilen-Dienstprogrammen werden Volumes auch Metageräte genannt. Für Volumes werden auch die Standard-UNIX-Begriffe <i>Pseudogerät</i> oder <i>virtuelles Gerät</i> verwendet.
Volume Manager	Ein Programm, das einen Mechanismus zum Verwalten und Zugreifen auf die Daten auf DVD-ROMs, CD-ROMs und Disketten zur Verfügung stellt.
WAN	(Wide Area Network) Ein Netzwerk, das mehrere LANs (Local Area Networks) oder Systeme an verschiedenen geografischen Standorten über Telefon-, Glasfaserleitung oder Satellit miteinander verbindet.
WAN-Boot-Installation	Eine Installationsart, die es ermöglicht, Software mithilfe von HTTP oder HTTPS über ein WAN (Wide Area Network) zu booten und zu installieren. Mit dem WAN-Boot-Installationsverfahren können Sie ein verschlüsseltes Solaris Flash-Archiv über ein öffentliches Netzwerk senden und auf einem entfernten Client eine benutzerdefinierte JumpStart-Installation durchführen.
WAN-Boot-Miniroot	Eine Miniroot, die im Hinblick auf die Durchführung einer WAN-Boot-Installation verändert wurde. Die WAN-Boot-Miniroot enthält einen Teilsatz der Software in der Solaris-Miniroot. Siehe auch Miniroot.
WAN-Boot-Server	Ein Webserver, der die für eine WAN-Boot-Installation benötigten Konfigurations- und Sicherheitsdateien bereitstellt.
wanboot-cgi- Programm	Das CGI-Programm, das die für eine WAN-Boot-Installation benötigten Daten und Dateien abruft und überträgt.
wanboot.conf- Datei	Eine Textdatei, in der Sie die Konfigurationsinformationen und Sicherheitseinstellungen angeben, die für die Durchführung einer WAN-Boot-Installation benötigt werden.

wanboot- Programm	Das sekundäre Boot-Programm, das die WAN-Boot-Miniroot, die Client-Konfigurationsdateien und die für eine WAN-Boot-Installation erforderlichen Installationsdateien lädt. Bei WAN-Boot-Installationen führt das Binärprogramm wanboot ähnliche Vorgänge wie die sekundären Boot-Programme ufsboot oder inetboot durch.
ZFS	Ein Dateisystem, das Speicherpools zum Verwalten des physischen Speichers verwendet.
Zone	Siehe Nicht-globale Zone

Index

Zahlen und Symbole

>WAN-Boot-Installation
Voraussetzungen
web server, 161-162
Webserver-Voraussetzungen, 161-162
>WAN-Boot-Miniroot, erstellen, 178-181
3DES (Chiffrierschlüssel), Verschlüsseln von Daten für die WAN-Boot-Installation, 156
3DES-Verschlüsselung, installieren, mit wanboot-Programm, 229

A

add install client, Beschreibung, 143 add_install_client-Befehl Beispiel Boot-Server, für CDs, 114 Boot-Server, für DVDs, 86 gleiches Teilnetz, für CDs, 114 mit DHCP für CDs, 113, 114 mit DHCP für DVDs, 86 serielle Konsole angeben, 87, 115 Beispiel zum Angeben einer seriellen Konsole, 87, 115 add to install server, Beschreibung, 143 AES (Chiffrierschlüssel), Daten für die WAN-Boot-Installation verschlüsseln, 156 **AES-Verschlüsselung** installieren mitwanboot-Programm, 229

Anmeldeserver, zur WAN-Boot-Installation konfigurieren, 243 Anzeige und Terminal nach I/O-Interrupts zurücksetzen, 144 Anzeigen eingehängte Dateisysteme, 144 gemeinsam genutzte Dateisysteme, 144 Plattformname, 144 Systeminformationen, 144 Arbeitsspeicher, WAN-Boot-Installationsvoraussetzungen, 160 Archiv Beispiel für WAN-Boot-Profil, 203 Erstellen eines Archivs, WAN-Boot-Installation, 198 in Dokument-Root-Verzeichnis für die WAN-Boot-Installation speichern, 163 installieren, mit WAN-Boot, 224-237 Ausgabedateien, bootlog-Datei für WAN-Boot-Installation, 190

B

banner-Befehl, 144
Befehle zum Starten einer Installation, x86-basierte Systeme, 95, 122
Benennung, Systemkonfigurationsdatei für WAN-Boot-Installationen, 207
Benutzerdefinierte JumpStart-Installation Beispiele, Profil für WAN-Boot-Installation, 203 mit WAN-Boot-Installation, 197-206 Berechtigungen, /etc/netboot-Verzeichnis, 188 Beschädigte Binärdateien, bei WAN-Boot-Installationen, 169 Bildschirmauflösung, Vorkonfiguration, 47 Bildschirmformat, Vorkonfiguration, 47 boot: cannot open /kernel/unix, Meldung, 266 boot-Befehlssyntax für WAN-Boot-Installationen, 256 boot file(Parameter), 258 boot logger(Parameter), 260 **Boot-Server** Beschreibung, 68 im Teilnetz erstellen mit DVDs, 80 in einem Teilnetz mithilfe von CDs erstellen, 107 mit DVDs erstellen, Beispiel, 81 Voraussetzung für Netzwerkinstallation, 68 bootconfchk, Befehl, Syntax, 254 bootlog-cgi(Programm), in wanboot.conf festlegen, 260 bootlog-Datei, auf Protokollserver umleiten, 190 bootparams, Datei, aktualisieren, 271 bootserver, Variable, 228

C

-c, Option, add_install_client-Befehl, 112 Can't boot from file/device, Meldung, 266 certstore, Datei, Beschreibung, 165 certstore-Datei, Client-Zertifikat einfügen, 244-245 check script, Syntax für WAN-Boot-Installationen, 254 Chiffrierschlüssel Beschreibung, 156 Daten während der WAN-Boot-Installation verschlüsseln, 156 erstellen, 245 in wanboot.conf festlegen, 259 installieren Beispiel, 220, 223, 250-251 Installationsmethoden, 218-224 mit wanboot-Programm, 229 Client, Voraussetzungen für die WAN-Boot-Installation, 160 client authentication, Parameter, 260

CLIENT MAC ADDR, Fehlermeldung, 271 client_name, Beschreibung, 113 Client-und Server-Authentifizierung, für WAN-Boot-Installation konfigurieren, 244-245 clock gained xxx days, Meldung, 266 CPUs (Prozessoren), WAN-Boot-Installationsvoraussetzungen, 160

D

-d, Option, add_install_client-Befehl, 112 Dateien und Dateisysteme eingehängte Dateisystem anzeigen, 144 gemeinsam genutzte Dateisystem anzeigen, 144 Systemkonfiguration, Syntax, 257-258 WAN-Boot-Dateisystem, 152 wanboot.conf Beschreibung, 258-261 Syntax, 258-261 Daten während der WAN-Boot-Installation verschlüsseln mit digitalen Zertifikat, 244-245 mit privatem Schlüssel, 244-245 Daten während WAN-Boot-Installation verschlüsseln, mit digitalem Zertifikat, 244 Datenschutz bei WAN-Boot-Installationen, 169 Datum und Uhrzeit, Vorkonfiguration, 46 Denial-of-Service-Angriffe, bei WAN-Boot-Installationen, 169 devalias(Befehl), Syntax, 257 DHCP (Dynamic Host Configuration Protocol), Vorkonfiguration, 46 DHCP-Dienst Beschreibung, 52 für WAN-Boot-Installation konfigurieren, 214 Makros für die Solaris-Installation erstellen, 57 Solaris, Booten und Installieren über das Netzwerk, 52 Sun-Vendor-Optionen für WAN-Boot-Installation, 214 **DHCP-Service** Beispielskript zum Hinzufügen von Optionen und Makros, 61

DHCP-Service (Fortsetzung) Erzeugen von Optionen für die Solaris-Installation, 53 WAN-Boot-Installationsvoraussetzungen, 160 dhtadm(Befehl), in Skripten verwenden, 61 Digitale Zertifikate Beschreibung, 157 digitale Zertifikate Beschreibung, 168 Digitale Zertifikate Daten bei der WAN-Boot-Installation schützen, 157 für WAN-Boot-Installationen vorbereiten, 244 digitale Zertifikate Voraussetzungen für die WAN-Boot-Installation, 168 Dokument-Root-Verzeichnis Beispiel, 163, 241 Beschreibung, 162 erstellen, 178 Domain-Name, Vorkonfiguration, 46

E

eeprom, Befehl, OBP-Unterstützung für WAN-Boot-Installationen überprüfen, 254 Einhängen, eingehängte Dateisysteme anzeigen, 144 encryption type, Parameter, 259 Erstellen Boot-Server im Teilnetz (mit CDs), 101 Boot-Server im Teilnetz (mit DVDs), 75 Boot-Server in einem Teilnetz mit DVDs, 80 Boot-Server in einem Teilnetz mithilfe von CDs, 107 /etc/locale-Datei, 49 Installationsserver (mit CDs), 101 Installationsserver (mit DVDs), 75 Installationsserver mit CDs, 103, 135, 139 Installationsserver mit DVDs, 76, 134, 136 WAN-Boot benutzerdefinierte JumpStart-Dateien, 197-206 Dokument-Root-Verzeichnis, 178 /etc/netboot-Verzeichnis, 186-189 Installationsdateien, 197-206

Erstellen, WAN-Boot (Fortsetzung) Solaris Flash-Archiv, 198 WAN-Boot-Miniroot, 178-181 /etc/bootparams, Datei, JumpStart-Verzeichniszugriff aktivieren, 271 /etc/locale-Datei, 49 /etc/netboot, Verzeichnis Beschreibung, 164-167 Konfigurations- und Sicherheitsdateien, Beschreibung, 165 Konfigurations- und Sicherheitsdateien zur gemeinsamen Client-Nutzung freigeben, 164-165, 166-167 /etc/netboot-Verzeichnis Beispiel, 166 Berechtigungen, 186-189 Client-und Server-Authentifizierung konfigurieren, 244-245 einfügen digitales Zertifikat, 244-245 Einfügen Vertrauenswürdige Zertifikate, 244 einführen privater Client-Schlüssel, 244-245 erstellen, 186-189, 242 Konfigurations- und Sicherheitendateien speichern Single-Client-Installationen, 165, 186 Konfigurations- und Sicherheitsdateien speichern gesamte Netzwerkinstallationen, 164, 186 gesamte Teilnetz-Installationen, 164, 186

F

Farbtiefe, Vorkonfiguration, 47
Fehlerbehebung

allgemeine Installationsprobleme
Booten des Systems, 271
Booten über das Netzwerk mit DHCP, 271
Booten über das Netzwerk mit DHCP, 271
Booten vom falschen Server, 271

Festplatten, Größe, verfügbarer Speicherplatz, 77
file, Variable, 226
flarcreate, Befehl, Syntax für

WAN-Boot-Installationen, 254

Freigabe,

WAN-Boot-Konfigurationsinformationen, 166-167

G

Gerätetreiber, Installation, 95, 122
Grafikkarte, Vorkonfiguration, 47
Grafische Benutzeroberfläche (GUI), Befehl zum Starten (x86-basierte Systeme), 95, 122
Größe, Festplatten, verfügbarer Speicherplatz, 77
GRUB-basiertes Booten Befehlsreferenz, 145-148
x86-Clients über das Netzwerk mit DVD installieren, 91, 119

Η

Hashing-Schlüssel Beschreibung, 156 Daten während der WAN-Boot-Installation schützen, 156 erstellen, 245 in wanboot.conf festlegen, 259 installieren Beispiel, 250-251 Installationsmethoden, 218-224 mit wanboot-Programm, 229 Hinzufügen Dataless-Clients mit CDs, 110 mit DVDs, 82 Einträge zur locale.org_dir-Tabelle, 51 Systeme aus Netzwerk, 75, 101 HMAC SHA1 Hashing-Schlüssel, Siehe Hashing-Schlüssel host-ip, Variable, 226 Host-Name, Vorkonfiguration, 46 hostname, Variable, 226 HTTP im Vgl. mit Secure Sockets Layer, Siehe HTTPS http-proxy, Variable, 226 HTTPS Beschreibung, 157

HTTPS (Fortsetzung) Schutz von Daten während der WAN-Boot-Installation, 157 Voraussetzungen für WAN-Boot, 191-197

Т

Install Time Updates (ITUs), Installation, 95, 122 Installation Gerätetreiber, 95, 122 Install Time Updates (ITUs), 95, 122 WAN-Boot, Beschreibung, 151-152 Installation starten, x86-basierte Systeme, 95, 122 Installation vorbereiten Systeminformationen vorkonfigurieren Methoden, 45-47 Vorteile, 17-18 Installationsserver in Teilnetz, 79, 129, 132 mit CDs erstellen, 103 mit CDs erstellen, Beispiel, 106, 135, 139 mit DVDs erstellen, 76 mit DVDs erstellen, Beispiel, 79, 134, 136 relevante Systemtypen, 67-69 WAN-Boot-Installationsvoraussetzungen, 160 **IP-Adressen** Standardroute vorkonfigurieren, 46 Vorkonfiguration, 46 IPv6, Vorkonfiguration, 46 IRQ-Ebene, Vorkonfiguration, 47

Κ

Kerberos, Vorkonfiguration, 46
keystore, Datei, Beschreibung, 165
keystore-Datei, privaten Client-Schlüssel einfügen, 244-245
Kommentare, in der Datei wanboot.conf, 258
Konfiguration DHCP-Server zur Unterstützung der Installation Schritte, DVDs, 75, 102
Konfigurieren DHCP-Dienst für WAN-Boot-Installation, 214 Konfigurieren (Fortsetzung) WAN-Boot-Server, 177-191

L

le0: No carrier - transceiver cable problem, Meldung, 266
list-security-keys, Befehl, Syntax, 257
locale-Datei, 49
locale.org_dir-Tabelle, Einträge hinzufügen, 51

Μ

Makefile-Datei, 48 Monitortyp, Vorkonfiguration, 47 mount-Befehl, 144

Ν

Namen/Benennung Hostname, 113 Systemplattformnamensermittlung, 144 Namen-Server, Vorkonfiguration, 46 Naming Service, Vorkonfigurieren, 46 net Gerätealias, prüfen und ändern, 250 net-Gerätealias, überprüfen und zurücksetzen, 217 network-boot-arguments, OBP-Variablen, in WAN-Boot-Installationen setzen, 228 network-boot-arguments OBP-Variablen, Syntax, 257 Netzmaske, Vorkonfiguration, 46 Netzwerk, Installation Beschreibung, 67-69 vorbereiten, 67-69 Netzwerkinstallation Siehe auch WAN-Boot-Installation mit CDs, 102, 108 mit DVDs, 76,80 mithilfe von PXE, 70-71 Voraussetzungen, 67-69 WAN-Boot-Installation, Beispiel, 239-252 Netzwerkschnittstelle, Vorkonfiguration, 46

nistbladm, Befehl, 51 nistbladm-Befehl, 51 No carrier - transceiver cable problem, Meldung, 266 Not a UFS filesystem, Meldung message, 266 nvalias(Befehl), Syntax, 257

0

OBP auf WAN-Boot-Unterstützung überprüfen, 241 Gerätealias netprüfen, 250 net-Gerätealias setzen, 217 net-Gerätealias überprüfen, 217 Variablen in WAN-Boot-Installationen setzen, 228 WAN-Boot-Installationsvoraussetzungen, 160 WAN-Boot-Unterstützung prüfen, 182 OpenBoot-PROM, *Siehe* OBP

Ρ

-p (Option des Prüfskripts), 204 PKCS#12 (Datei), Voraussetzungen für die WAN-Boot-Installation, 168 PKCS#12-Datei, für WAN-Boot-Installation vorbereiten, 244-245 Planung WAN-Boot-Installation für die Installation erforderliche Informationen, 169-171 Konfigurations- und Sicherheitsdateien freigeben, 166-167 Konfigurations- und Sicherheitsdateien speichern, 164-167 Server-Organisation, 162 Speichern des Programms wanboot-cgi, 168 Speichern von Installationsdateien, 162 Systemvoraussetzungen, 159 Webserver-Voraussetzungen, 161-162 Plattformen Installationsserver-Einrichtung, 113 Namensermittlung, 144 Power Management, 42-43

Preboot Execution Environment (PXE) Beschreibung, 70 BIOS-Setup, Voraussetzungen, 91, 119 Richtlinien, 71 Primäres Dokumentverzeichnis, Siehe Dokument-Root-Verzeichnis printenv-Befehl, auf WAN-Baud-Unterstützung überprüfen, 241 Profile Beispiele WAN-Boot-Installation, 203 benennen, 202 Protokolldateien, für WAN-Boot-Installation, 190 Protokollserver Beschreibung, 161 Speicherort der Protokollmeldungen, 190 WAN-Boot-Installation (Voraussetzungen), 161 Protokollserver, in wanboot.conf festlegen, 260 Prozessoren, WAN-Boot-Installationsvoraussetzungen, 160 Prüfskript, Regeln testen, 204 PXE (Preboot Execution Environment) Beschreibung, 70 BIOS-Setup, Voraussetzungen, 91, 119 Richtlinien, 71

R

Regeln, Validierung für die WAN-Boot-Installation, 204 reset-Befehl, 144 resolve_hosts, Parameter, 260 root_file, Parameter, 259 Root-Passwort, Vorkonfiguration, 46 root_server, Parameter, 258 router-ip, Variable, 226 RPC-Fehler mit Zeitüberschreitung, 271 RPC Timed out, Meldung, 271 rules-Datei, Validierung für die WAN-Boot-Installation, 204

S

SbootURI DHCP-Option Beschreibung, 56 mit WAN-Boot-Installationen verwenden, 214 Schlüssel, Siehe Chiffrierschlüssel, Hashing-Schlüssel Schlüsselwörter, sysidcfg-Datei, 22-42 Schutz von Daten während der WAN-Boot-Installation mit Hashing-Schlüssel, 156 mit HTTPS, 157 mit Verschlüsselung, 156 Secure Sockets Layer, mit WAN-Boot-Installation verwenden, 191-197 Serielle Konsole, 93, 121 serielle Konsole mitadd install clientangeben, 87,115 Serielle Konsole einrichten, 93, 121 Server Netzwerkinstallation mit CDs einrichten Standalone-Installation, 110 Netzwerkinstallation mit DVDs einrichten Standalone-Installation, 82 Voraussetzungen für die Netzwerkinstallation, 67-69 WAN-Boot-Installation Beschreibungen, 159 Konfigurationsoptionen, 162 Voraussetzungen, 159 >WAN-Boot-Installation Webserver-Softwarevoraussetzungen, 161-162 server authentication, Parameter, 259 set-security-key, Befehl, Syntax, 257 set-security-key-Befehl Schlüssel auf WAN-Boot-Client installieren, 250-251 Syntax, 256 setenv, Befehl, Syntax, 257 setup install server Beschreibung, 143 für WAN-Boot-Installation, 178-181 Syntax für WAN-Boot-Installationen, 253 showmount-Befehl, 144 SHTTPproxy DHCP-Option Beschreibung, 57 mit WAN-Boot-Installationen verwenden, 214

sicheres HTTP, Siehe HTTPS Sicherheit WAN-Boot-Installation Beschreibung, 156-157 Sicherheitslücken bei WAN-Boot-Installationen, 169 Sicherheitsrichtlinie, Vorkonfiguration, 46 signature type, Parameter, 259 SjumpsCF, Parameter, 258 SjumpsCF Parameter, 208 Solaris-Installationsprogramm Grafische Benutzeroberfläche (GUI), Befehl zum Starten (x86-basierte Systeme), 95, 122 textbasiertes Installationsprogramm Befehl zum Starten in einer Desktop-Sitzung (x86-basierte Systeme), 95,122 Befehl zum Starten in einer Konsolensitzung (x86-basierte Systeme), 95, 122 Speicherplatz, 160 Speicherplatz. Voraussetzungen für die WAN-Boot-Installation, 160 SSL, bei einer WAN-Boot-Installation verwenden, 191-197 SsysidCF, Parameter, 257 SsysidCF-Parameter, 207 STANDARD-BOOT-GERÄT WECHSELN, Meldung, 272 subnet-mask, Variable, 226 sysidcfg (Datei), Schlüsselwort auto reg, Beschreibung, 23-28 sysidcfq-Datei name service-Schlüsselwort, Beschreibung, 29-32 network interface-Schlüsselwort, Beschreibung, 32-38 Richtlinien und Voraussetzungen, 18-42 root password-Schlüsselwort, Beschreibung, 39 Schlüsselwörter, 22-42 security policy-Schlüsselwort, Beschreibung, 39-40 service profile-Schlüsselwort, Beschreibung, 40-41 Syntax, 22 system_locale-Schlüsselwort, Beschreibung, 41 Tastatur Schlüsselwort, Beschreibung, 28-29 terminal-Schlüsselwort, Beschreibung, 41

sysidcfq-Datei (Fortsetzung) timeserver-Schlüsselwort, Beschreibung, 42 timezone-Schlüsselwort, Beschreibung, 41-42 WAN-Boot, Beispiel, 201 System booten, Terminals und Anzeige zuerst zurücksetzen, 144 system.conf (Datei), Siehe Systemkonfigurationsdatei system conf, Parameter, 261 Systeminformationen, anzeigen, 144 Systemkonfigurationsdatei Beispiele sichere WAN-Boot-Installation, 208, 247-248 unsichere WAN-Boot-Installation, 208 Beschreibung, 165 für WAN-Boot-Installation erstellen, 247-248 in wanboot.conf festlegen, 261 SjumpsCF(Einstellung), 257-258 SsysidCF(Einstellung), 257-258 Syntax, 257-258

Т

Tastatursprache und -layout, Vorkonfiguration, 47 Teilnetz Boot-Server-Erstellung in, mithilfe von CDs, 107 Boot-Servererstellung im, mit DVDs, 80 Terminaltyp, Vorkonfiguration, 46 Testen WAN-Boot rules-Datei, 204 wanboot.conf-Datei, 211 Textbasiertes Installationsprogramm Befehl zum Starten in einer Desktop-Sitzung (x86-basierte Systeme), 95, 122 Befehl zum Starten in einer Konsolensitzung (x86-basierte Systeme), 95,122 Token-Ring-Karte, Fehler beim Booten, 270 transceiver cable problem, Meldung, 266 Triple DES (Chiffrierschlüssel), Siehe 3DES (Chiffrierschlüssel) trust-Anker, Siehe Vertrauenswürdiges Zertifikat truststore, Datei, Beschreibung, 165 truststore-Datei, vertrauenswürdiges Zertifikat einfügen, 244

U

Uhrzeit und Datum, Vorkonfiguration, 46 uname-Befehl, 144 Unbekannter Client (Fehlermeldung), 265 Upgrade, Upgrade fehlgeschlagen, 277 Upgrade fehlgeschlagen, Probleme beim Neustart, 277

V

Validieren, wanboot.conf-Datei, 211 Validierung, rules-Dateien, für die WAN-Boot-Installation, 204 /var/yp/make-Befehl, 50 /var/yp/Makefile, 48 Verschlüsseln von Daten mit HTTPS, WAN-Boot-Installation, 157 Verschlüsseln von Daten während der WAN-Boot-Installation, mit HTTPS, 191-197 Vertrauenswürdiges Zertifikat, in truststore-Datei einfügen, 244 Verzeichnisse Dokument-Root Beispiel, 163, 241 Beschreibung, 162 erstellen, 178 Erstellen, 241 /etc/netboot Beispiel, 166 Beschreibung, 164-167 Konfigurations- und Sicherheitsdateien, Beschreibung, 165 Konfigurations- und Sicherheitsdateien freigeben, 166-167 Konfigurations- und Sicherheitsdateien speichern, 164-165 Konfigurations- und Sicherheitsdateien zur gemeinsamen Client-Nutzung freigeben, 164-165 /etc/netboot-Verzeichnis, 186-189 Voraussetzungen Netzwerkinstallation, Server, 67-69 WAN-Boot-Installation, 159 Vorbereitung der Installation, WAN-Boot-Installation, 173-214

Vorbereitung für die Installation, Client für die WAN-Boot-Installation, 216-224
Vorkonfigurieren der Power Management-Informationen, Power Management, 42-43
Vorkonfigurieren der Systemkonfigurationsinformationen mit DHCP, 52 Methode auswählen, 45-47 Vorteile, 17-18
Vorkonfigurieren von Systemkonfigurationsinformationen mit dem Naming Service, 47 mit einem Naming Service, 47-51 mit sysidcfg-Datei, 47

W

WAN-Boot-Dateisystem, Beschreibung, 152 WAN-Boot-Installation Abfolge der Ereignisse, 153-155 Befehle, 253-256 Beispiele Anmeldeserver konfigurieren, 243 automatische Installation, 226 benutzerdefiniertes JumpStart-Profil, 203 Chiffrierschlüssel auf einem laufenden Client installieren, 223 Chiffrierschlüssel erstellen, 197, 245 Chiffrierschlüssel in OBP installieren, 220, 250-251 Client-Authentifizierung ermöglichen, 244-245 Client-OBP-Unterstützung prüfen, 182 Client-OBP-Unterstützung überprüfen, 241 Client-Zertifikat einfügen, 194, 244-245 Datei rules erzeugen, 247 digitale Zertifikate vorbereiten, 244-245 Dokument-Root-Verzeichnis, 241 Erstellen des /etc/netboot-Verzeichnisses, 188 /etc/netboot-Verzeichnis, 166 /etc/netboot-Verzeichnis erstellen, 242 Gerätealias net prüfen, 250 Hashing-Schlüssel auf einem laufenden Client installieren, 223

WAN-Boot-Installation, Beispiele (Fortsetzung) Hashing-Schlüssel erstellen, 197, 245 Hashing-Schlüssel in OBP installieren, 220, 250-251 Installation mit DHCP-Service, 232 Installation mit lokalen CDs, 235 interaktive Installation, 229 JumpStart-Profil erstellen, 246-247 Konfiguration des Protokollservers, 190 mit Verschlüsselung, 245 net-Gerätealias setzen, 217 net-Gerätealias überprüfen, 217 Netzwerkeinrichtung, 240 nicht-interaktive Installation, 251-252 privaten Client-Schlüssel einfügen, 194 privater Client-Schlüssel einfügen, 244-245 Server-Authentifizierung aktivieren, 194 Server-Authentifizierung ermöglichen, 244-245 Solaris Flash-Archiv erzeugen, 245-246 sysidcfg-Datei, 201 sysidcfg-Datei erzeugen, 246 Systemkonfigurationsdatei, 208 Systemkonfigurationsdatei erstellen, 247-248 ungeführte Installation, 226, 251-252 vertrauenswürdiges Zertifikat einfügen, 194, 244 WAN-Boot-Miniroot erstellen, 241 wanboot-cgi-Programm kopieren, 243 wanboot.conf-Datei, 211, 212, 248-249 wanboot-Programm installieren, 242 beschädigte Binärdateien, 169 Beschreibung, 151-152 bootlog-cgi(Programm), in wanboot.conf festlegen, 260 Chiffrierschlüssel in wanboot.conf festlegen, 259 installing, 218-224 WAN boot installation Chiffrierschlüssel Wert anzeigen, 218-224 WAN-Boot-Installation Chiffrierschlüssel, Datenschutz, 169 Chiffrierschlüssel installieren, 218-224 Client-Voraussetzungen, 160

WAN-Boot-Installation (Fortsetzung) Client-Authentifizierung in wanboot.conf festlegen, 260 Voraussetzungen, 158 Client installieren Installationsverfahren, 224 Daten schützen, 156, 157 Daten verschlüsseln mit Chiffrierschlüssel, 156 mit HTTPS, 191-197 Denial of Service, 169 digitale Zertifikate, Voraussetzungen, 168 Dokument-Root-Verzeichnis Beispiel, 163 Beschreibung, 162 Dateien, 162 erstellen Begin-Skripten, 206 Finish-Skripten, 206 Erstellen Solaris Flash-Archiv, 198 /etc/netboot, Verzeichnis Beschreibung, 164-167 /etc/netboot-Verzeichnis Beispiel, 166 Berechtigungen festlegen, 187 erstellen, 186-189 für die Installation erforderliche Informationen, 169-171 Hashing-Schlüssel in wanboot.conf festlegen, 259 installieren, 218-224 Wert anzeigen, 218-224 Hashing-Schlüssel, Datenschutz, 169 Hashing-Schlüssel installieren, 218-224 Installation eines Clients erforderliche Schritte, 215 Installieren des wanboot-Programms, 183-186 Konfigurations- und Sicherheitsdateien, Beschreibung, 165 Konfigurations- und Sicherheitsdateien gemeinsam nutzen gesamtes Teilnetz, 164, 186

WAN-Boot-Installation (Fortsetzung) Konfigurations- und Sicherheitsdateien gemeinsamen nutzen Client-spezifisch, 165, 186 gesamtes Netzwerk, 164, 186 konfigurieren Client-und Server-Authentifizierung, 244-245 Konfigurieren DHCP-Dienstunterstützung, 214 konfigurieren WAN-Boot-Server, 177-191 nicht-interaktive Installation, 251-252 Planung Dokument-Root-Verzeichnis, 162 /etc/netboot, Verzeichnis, 164-167 Konfigurations- und Sicherheitsdateien freigeben, 164-165 Konfigurations- und Sicherheitsdateien speichern, 164-167 Server-Organisation, 162 Speichern von Installationsdateien, 162 Systemvoraussetzungen, 159 Protokollserver, in wanboot.conf festlegen, 260 Server-Authentifizierung in wanboot.conf festlegen, 259 Voraussetzungen, 158 Serverkonfigurationen, Beschreibung, 162 sichere Konfiguration Beschreibung, 158 Schritte zur Installation, 173 Voraussetzungen, 158 Sicherheitskonfigurationen, Beschreibung, 157-158 Sicherheitslücken, 169 Speichern des Programms wanboot-cgi, 168 Systemvoraussetzungen, 159 Systemkonfigurationsdatei in wanboot.conf festlegen, 261 Syntax, 257-258 Überprüfen der rules-Datei, 204 ungeführte Installation, 251-252 unsichere Konfiguration, 158 Verschlüsseln von Daten mit HTTPS, 157

WAN-Boot-Installation (Fortsetzung) Voraussetzungen Arbeitsspeicher auf Client, 160 Betriebssystem für Webserver, 161 Client-CPU, 160 DHCP-Service, 160 digitale Zertifikate, 168 OBP für Client, 160 Protokollserver, 161 Speicherplatz auf Client, 160 Speicherplatz auf Installationsserver, 160 SSL-Versionsunterstützung, 162 WAN-Boot-Server, 159 Web-Proxy, 161 WAN-Boot-Miniroot Beschreibung, 152 erstellen, 178-181 im Dokument-Root-Verzeichnis speichern, 163 in wanboot.conf festlegen, 259 wanboot (Programm) in wanboot.conf festlegen, 258 wanboot-cgi-Programm, 189-190 auf WAN-Boot-Server kopieren, 189-190 in wanboot.conf festlegen, 258 wanboot-cgi-Programm kopieren, 189-190 wanboot.conf, Datei Parameter, 258-261 Syntax, 258-261 wanboot.conf-Datei validieren, 211 wanboot-Programm Beschreibung, 151 im Dokument-Root-Verzeichnis speichern, 163 installieren, 183-186 wanbootutil-Befehl Chiffrierschlüssel erstellen, 245 Hashing-Schlüssel erstellen, 245 privaten Schlüssel erstellen, 193 vertrauenswürdiges Zertifikat erstellen, 193 wann sinnvoll?, 153 WAN-Boot-Miniroot Beschreibung, 152 erstellen, 241 im Dokument-Root-Verzeichnis speichern, 163

WAN-Boot-Miniroot (Fortsetzung) in wanboot.conf festlegen, 259 WAN-Boot-Server Beschreibung, 159 konfigurieren, 177-191 Voraussetzungen, 159 wanboot-cgi-Programm kopieren, 189-190 Webserver-Voraussetzungen, 161-162 wanboot-cgi, Programm Auswahl von Client-Konfigurationsinformationen, 166 Beschreibung, 164 speichern, 168 Suchreihenfolge in /etc/netboot, 166 wanboot-cgi-Programm auf WAN-Boot-Server kopieren, 189-190, 243 in wanboot.conf festlegen, 258 wanboot.conf, Datei Beschreibung, 258-261 für WAN-Boot-Installation erstellen, 258-261 Syntax, 258-261 wanboot.conf (Datei), Beschreibung, 165 wanboot.conf-Datei Beispiele sichere WAN-Boot-Installation, 211, 248 unsichere WAN-Boot-Installation, 212 für WAN-Boot-Installation, 248-249 für WAN-Boot-Installation validieren, 211, 248-249 wanboot-Programm auf WAN-Boot-Server installieren, 183-186, 242 Beschreibung, 151 im Dokument-Root-Verzeichnis speichern, 163 Schlüssel für WAN-Boot-Installation installieren, 229 Vorgänge bei der WAN-Boot-Installation, 155 wanboot(Programm), in wanboot.conf festlegen, 258 wanbootutil-Befehl Chiffrierschlüssel erstellen, 245 Chiffrierschlüssel-Wert anzeigen, 250-251 Client- und Server-Authentifizierung konfigurieren, 193 Client-und Server-Authentifizierung konfigurieren, 244-245, 245

wanbootutil-Befehl (Fortsetzung)
digitales Client-Zertifikat einfügen, 193, 244-245
Hashing-Schlüssel erstellen, 245
Hashing-Schlüssel-Wert anzeigen, 250-251
PKCS#12-Datei aufteilen, 193, 244
privaten Client-Schlüssel einfügen, 193, 244-245
vertrauenswürdiges Zertifikat einfügen, 193, 244
WARNING: clock gained xxx days, Meldung, 266
WARNUNG: BOOT-GERÄT WECHSELN, 272
Web-Proxy,
WAN-Boot-Installationsvoraussetzungen, 161

Web-Proxy, Vorkonfiguration, 47

Ζ

Zeigegerät, Vorkonfiguration, 47 Zeitzone, Vorkonfiguration, 46 Zertifikate, *Siehe* Digitale Zertifikate