Sichere SPARC Serverinstallation mittels der Wanboot-Technologie

Stefan Gärtner CCF AG / Griesheim
Andreas Auer Oracle Deutschland / Langen

Schlüsselworte:

Wanboot, Solaris 10, Solaris 11, SPARC, Installation, Automatisierung, Sicherheit, Authentifizierung, Verschlüsselung, Jumpstart, Zertifikate, Automated Installer (AI), Imaging Package System (IPS)

Einleitung

Der Vortrag gibt eine Einführung und technische Übersicht über die verschlüsselte und automatisierte SPARC-Serverinstallation unter Zuhilfenahme der Wanboot-Technologie für Solaris 10 und Solaris 11 (Build 173).
Es wird eine Lösung präsentiert, die einen sehr hohen Zugriffsschutz, kürzere Installationszeiten und eine geringe Komplexität durch Automatisierung bietet. Das im Detail vorgestellte Verfahren ermöglicht unternehmensweite Installationen für sicherheitssensible Bereiche über mehrere Standorte hinweg.

Wanboot Technologie[1]

Die wanboot-Technologie ermöglicht es, Software unter Verwendung von HTTP bzw HTTPS über ein WAN (Wide Area Network) zu booten und zu installieren. Mit wanboot können somit Solaris Systeme über große, öffentliche Netzwerke, deren Infrastruktur nicht vertrauenswürdig ist, auf SPARC-Systemen installiert werden. Die Sicherheitsfunktionen von wanboot schützen die Vertraulichkeit der Daten und stellen die Integrität der Server/Client Verbindung sicher.

Mit der wanboot Installationsmethode können verschlüsselte und unverschlüsselte Solaris Flash-Archive über ein Netzwerk an einen entfernten SPARC-Client übertragen werden. Die wanboot-Programme installieren das Serversystem, wobei das herkömmliche Jumpstart-Verfahren genutzt wird. Die Integrität der Installation lässt sich mit privaten Schlüsseln zur Authentifizierung und Verschlüsselung der Daten schützen. So können die Installationsdaten und -dateien auch über eine sichere HTTP-Verbindung gesendet werden. Hierfür muss allerdings explizit die Verwendung von digitalen Zertifikaten konfiguriert werden.

Während der wanboot Installation werden folgende Informationen von einem Webserver heruntergeladen und installiert:

- wanboot-Programm – Das wanboot-Programm ist das sekundäre Boot-Programm, das die wanboot-Miniroot, die Client-Konfigurationsdateien und die Installationsdateien lädt. Das wanboot-Programm führt ähnliche Vorgänge wie die Boot-Unterprogramme „ufsboot“ oder „inetboot“ durch.

- wanboot-Dateisystem – wanboot 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 wanboot-Dateisystem, an den Client.

- wanboot-Miniroot – Die wanboot-Miniroot ist eine auf die wanboot-Installation ausgerichtete Variante des Solaris-Miniroot. Wie das Solaris-Miniroot enthält das wanboot-Miniroot einen Kernel und gerade so viel Software, wie zur Installation von Solaris erforderlich ist.

- Benutzerdefinierte JumpStart-Konfigurationsdateien – Für die Installation des Systems überträgt wanboot die Dateien „sysidcfg“, „rules.ok“ sowie Profildateien an den Client. Wanboot 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 werden die Clientsysteme installiert. Wanboot 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.

Funktionsweise wanboot

Die Installation eines SPARC Rechners über wanboot läuft in verschiedenen Schritten ab. Die folgende Illustration verdeutlich den genauen Ablauf. Der getrennt dargestellten Web- bzw Installationsserver kann auch jeweils als Dienst auf einem zentralen Server konfiguriert werden.

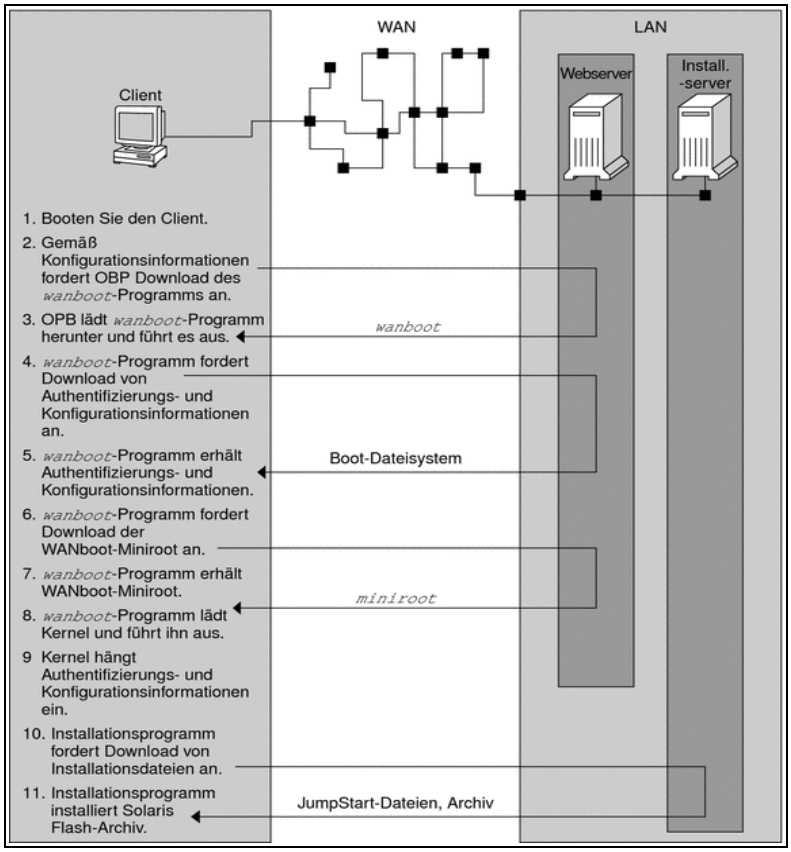

Abbildung 1: Funktionsweise wanboot-Installation[1]

1. Der Client wird auf eine der folgenden Arten installiert:
   - Booten aus dem Netzwerk durch Setzen von Netzwerkschnittstellen-Variablen im Open Boot PROM (OBP).
   - Booten aus dem Netzwerk mit oder ohne 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 dazu das wanboot-Programm von einer der folgenden Quellen herunter:
   - Von einem speziellen Webserver, dem wanboot-Server, unter Verwendung von HTTP.
   - Von einer lokalen CD-ROM (nicht abgebildet). Notwendig, wenn der OBP des Systems wanboot nicht unterstützt

4. Das wanboot-Programm fordert die Client-Konfigurationsinformationen vom wanboot-Server an.
5. Das wanboot-Programm lädt Konfigurationsdateien, die vom Programm wanboot-cgi übertragen werden, vom wanboot-Server herunter. Die Konfigurationsdateien werden als wanboot-Dateisystem an den Client übertragen.
6. Das wanboot-Programm fordert das wanboot-Miniroot vom wanboot-Server an.
7. Das wanboot-Programm lädt das wanboot-Miniroot per HTTP oder HTTPS vom wanboot-Server herunter.
8. Das wanboot-Programm lädt den UNIX-Kernel aus dem wanboot-Miniroot und führt ihn aus.
9. Der UNIX-Kernel sucht das wanboot-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 HTTP- oder HTTPS-Verbindung herunter.
11. Das Installationsprogramm installiert mit dem benutzerdefinierten JumpStart-Verfahren das Solaris Flash-Archiv auf dem Client.

Schutz der Daten während einer wanboot-Installation

Das wanboot-Installationsverfahren erlaubt den Einsatz von Hashing-Schlüsseln und digitalen Zertifikaten zum Schutz der Systemdaten während der Installation. Dazu werden die vom wanboot-Installationsverfahren unterstützten Datenschutzmethoden kurz dargestellt.

Überprüfen der Datenintegrität mit einem Hashing-Schlüssel

Zum Schutz der Daten, die von einem wanboot-Server an den Client übertragen werden, kann ein sogenannter HMAC-Schlüssel (Hashed Message Authentication Code) erstellt werden. Dieser Hashing-Schlüssel wird sowohl auf dem wanboot-Server als auch auf dem Client konfiguriert. Der wanboot-Server signiert mit diesem Schlüssel die an den Client zu übertragenden Daten. Der Client verwendet den Schlüssel dann zum Überprüfen der Integrität der vom wanboot-Server übertragenen Daten. Nach der Installation eines Hashing-Schlüssels auf einem Client steht dieser Schlüssel für einen definierten Zeitraum dem Client für künftige wanboot-Installationen zur Verfügung.

Verschlüsseln von Daten mit Chiffrierschlüsseln

Zusätzlich können die Daten vom Installationsserver beim wanboot-Installationsverfahren verschlüsselt werden. Das wanboot-Dienstprogrammen kann eine 3DES(Triple Data Encryption Standard)- oder AES(Advanced Encryption Standard)-Verschlüsselung durchführen. Der erstellte Schlüssel wird sowohl dem wanboot-Server als auch dem Client zur Verfügung gestellt. Mit diesem Chiffrierschlüssel werden die Daten vom Server zum zu installierenden Client verschlüsselt. Der Client nutzt dann diesen Schlüssel zum Entschlüsseln der Installation, Konfigurations- und Sicherheitsdateien. Nach der Installation eines Chiffrierschlüssels auf einem Client steht dieser Schlüssel dem Client für künftige wanboot-Installationen für einen definierten Zeitraum zur Verfügung.

Schutz von Daten durch HTTPS

Bei der Konfiguration mit digitalen Zertifikaten kann entweder nur der Server oder sowohl der Server als auch der Client während der Installation sicher authentifiziert werden. Durch HTTPS werden, wie

bereits dargestellt die Daten, die bei der Installation vom Server an den Client übertragen werden, verschlüsselt.

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, muss ein digitales Zertifikat auf dem Server installiert werden. Ebenso kann festgelegt werden, dass sich der Client gegenüber dem Server ausweisen muss.

Jumpstart Server²

Die JumpStart Installationsmethode ist ein Profil gesteuertes Verfahren um Serversysteme automatisiert installieren oder aktualisieren zu können. In einer sogenannten Profildatei wird der Softwareumfang sowie das Plattenlayout definiert. Zudem können vor oder nach der Installation eigene Shellskripte ausgeführt werden. In der Datei „sysidcfg“ werden systemspezifische Konfigurationsdaten abgelegt, so dass die Installation bzw. das Betriebssystemupdate komplett automatisiert ablaufen kann. Diese Datei muss bei jedem neuen Solaris Releaseupdate auf neu hinzugekommene Konfigurationsparameter geprüft werden, damit die automatisierte Installation erfolgreich durchläuft.

JumpStart Beispiel

Zuerst wird die sogenannte „rules“ Datei erstellt. In dieser Text-Datei werden die verschiedenen Systemtypen anhand eindeutiger Regeln unterschieden, damit verschiedenen Systemgruppen eigene Profile- Dateien und ggf. Pre- bzw Post-Skripte zugeordnet werden können.Beide Konfigurationsdateien (rules und Profile) werden auf dem JumpStart Server abgelegt.

In folgendem Beispiel wird eine „rules” Datei erstellt, die die Systeme in 3 Gruppen unterteilt. Dann wird jeder Gruppe eine eigene „Profile”-Datei zugewiesen. Zur Validierung der „rules” Datei gibt es ein sog. „check” Skript. Diese wandelt die „rules” Datei in die „rules.ok” Datei. Das JumpStart Verfahren nutzt dann immer die verifizierte Datei.

Ablauf der JumpStart Installation

Nachdem die „rules"-Datei verifiziert ist kann die Installation gestartet werden. Der JumpStart Prozess wird in der Datei von oben nach unten nach einer für das zu installierende System geeigneten Regel suchen und mit der vorgesehenen „Profile"-Datei das System mit Solaris installieren.

In folgender Abbildung wird der Ablauf dargestellt:

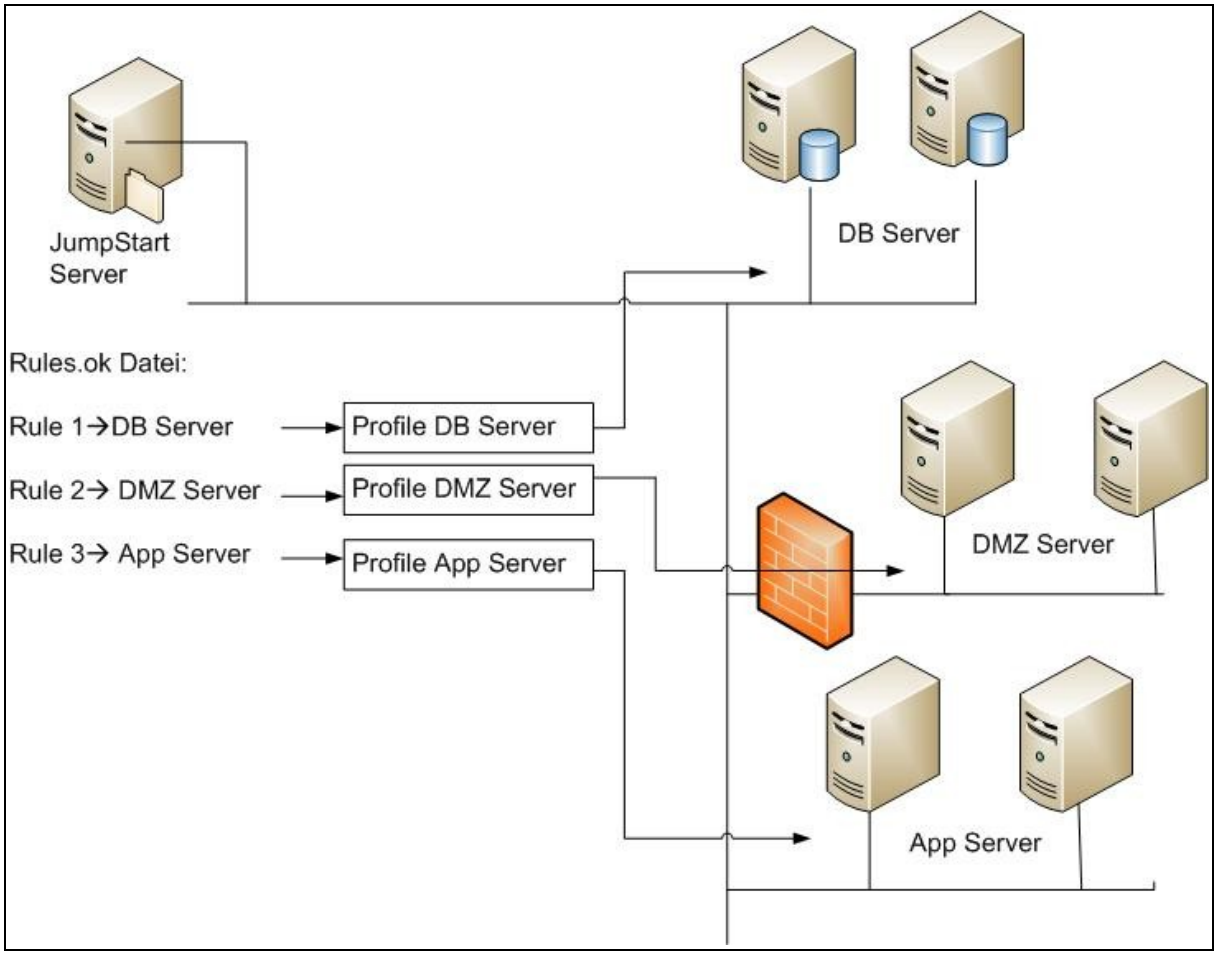

Abbildung 2: Ablauf einer JumpStart Installation

Automated Installer (AI)[3]

Der „Automated Installer (AI)" ist das neue Installationverfahren, um Solaris 11 Systeme automatisiert in einem Netzwerk installieren zu können. Aufgrund der Änderungen in der Paketverwaltung zu Solaris 10 musste ein neuer Mechanismus etabliert werden. Dieser nennt sich „Automated Installer" und gilt sowohl für SPARC als auch x86 Systeme. Bei diesem Mechanismus werden ein oder mehrere Software Repositories benötigt.

Wie läuft die Installation ab ?

Der AI-Mechnismus eignet sich zur automatisierten Installation von Solaris auf SPARC sowie x86 Systemen. Die zu installierenden Clientsysteme können sich wie bei der JumpStart Methode durch

verschiedene Charakteristiken wie Plattenkapazität, Systemarchitektur, Hauptspeicherkapazität usw. unterscheiden. Die Installation kann dadurch sehr systemtypisch z.B. im Softwareumfang oder Plattenlayout angepasst werden.

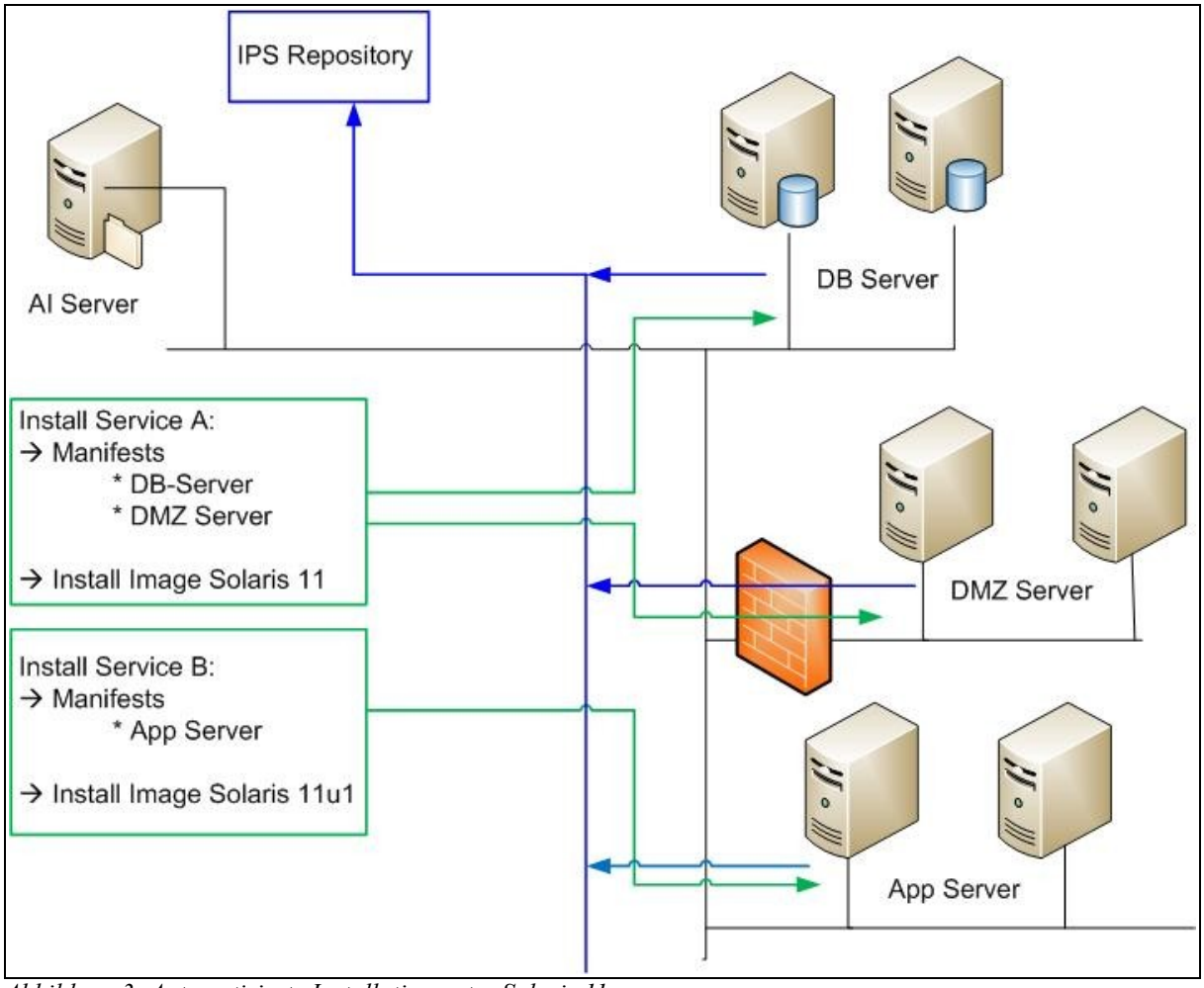

Abbildung 3: Automatisierte Installation unter Solaris 11

Die Installation kann anhand folgender Schritte beschrieben werden:

1. Das Clientsystem bootet und bekommt vom DHCP Server oder den eingegebenen Bootargumenten (network-boot-arguments) die IP und andere notwendige Informationen.

2. Die Charakteristik des Clientsystems bestimmt welche Dienste und Installationsprozeduren durchlaufen werden.

3. Das Solaris Betriebssystem wird anhand eines vom AI Dienst festgelegten Manifests installiert. Die notwendigen Pakete werden vom Repository Server bezogen.

Um mit dem AI Clientsysteme installieren zu können, muss für x86 Systeme ein DHCP Service aufgesetzt werden. Dieser versorgt das System mit den notwendigen IP-Daten. SPARC Systeme benötigen keinen DHCP. Hier kann mit dem wanboot-Verfahren direkt vom OBP auf das Installationsimage des AI-Servers, analog dem wanboot-Verfahren unter Solaris 10, zugegriffen werden.

Das zu installierende Clientsystem muss zudem auf das IPS (Imaging Package System) zugreifen können. Dieser Dienst kann auf dem AI-Server zusätzlich eingerichtet werden.

Funktionsweise Automated Installer (AI)

Der AI-Dienst verweist bei der Installation entsprechend der Architektur des Clientsystem auf ein SPARC oder x86 Installationsimage. Zudem enthält es zusätzliche Anweisungen (Manifests) um die Installation abschließen zu können. Anhand des Installationsimages kann die Installation nicht fertiggestellt werden. Das Clientsystem benötigt immer den Zugriff auf ein oder mehrere IPS-Repositories, die in dem Manifest konfiguriert werden. Desweiteren kann ein Manifest auch zusätzliche Pakete oder Partitionsinformationen enthalten. Zudem können der Installation nachgeschaltete Konfigurationsanpassungen mitgegeben werden.

Falls unterschiedliche Solaris Versionen oder Maschinentypen (SPARC/x86) installiert werden sollen, muss für jedes Solaris Release bzw. jeden Maschinentyp ein eigener AI-Dienst laufen, der ein spezielles AI-image anbietet.

Falls die gleiche Betriebssystemversion auf gleichen Maschinentypen installiert wird, die Systeme aber verschiedene Softwarestände bekommen sollen, benötigt man nur einen AI-Dienst, aber verschiedene Manifeste. In den Manifesten wird dann der zu installierende Softwareumfang definiert.

Unterschiede Paketverwaltung System V und Image Packaging System

Die unter Solaris 10 und den vorherigen Solaris-Versionen (seit Solaris 2.0) verwendete Paketverwaltung stammt von dem System V Release 4 (SVR4) ab. Dieses Release wurde bereits im Jahr 1989 entwickelt und entspricht nicht den heutigen Anforderungen.

Bei der SVR4-Paketverwaltung müssen Pakete auf einem für Solaris zugänglichen Dateisystem liegen, um installiert werden zu können. Im Gegensatz dazu, kann man bei dem Image Packaging System (IPS) auf einen oder mehrere Repository Server zugreifen. Die Vorteile liegen schon jetzt auf der Hand, da Pakete nur einmal an einer vertrauenswürdigen Stelle abgelegt werden müssen.

Das IPS wurde unter Berücksichtigung aktueller Solaris-Features, u.a. Zonen, Live Update uvm. entwickelt, und ist zudem keine Sammlung unterschiedlicher Befehle, sondern ein Frameset „pkg(5)“. Unter Solaris 11 wird es eine neue Namenskonvention geben. Eine Liste der Namensänderung ist unter http://hub.opensolaris.org/bin/view/Project+pkg/Renamed (Stand September 2011) zu finden. So wird beispielsweise das SVR4-Paket „SUNWcakr“ ab Solaris 11 unter dem IPS „system/kernel/platform“ lauten. (Auch unter Solaris 11 werden SVR4-Pakete weiterhin unterstützt.)

SVR4 Pakete

Um Pakete mittels der SVR4-Werkzeuge erstellen, hinzufügen, löschen oder aktualisieren zu können, muss man den Aufbau der SVR4-Paketverwaltung kennen.

Die Informationen (Metadaten) eines Paketes stehen in der pkginfo(-Datei), diese kann folgendermaßen aussehen:

```
PKG=SUNWcadap
NAME=Chip designers need CAD application software to design abc
chips.
Runs only on xyz hardware and is installed in the usr partition.
ARCH=sparc
VERSION=release 1.0
CATEGORY=system
BASEDIR=/opt
```

Der in der ersten Zeile angegebene Paketname (PKG) muss eindeutig sein. Bei der Installation eines gleichnamigen Paketes, wird das alte Paket entfernt.
Wichtige Parameter dieser Datei sind ebenfalls die Prozessor-Architektur (ARCH), Version (VERSION), sowie das Basisverzeichnis (BASEDIR).

Die zu paketierenden Komponenten (alle Dateien und Ordner) werden bei der Paket-Erstellung hierarchisch angeordnet. Um Änderungen während des „pkgadd“ (hinzufügen des Pakets) durchzuführen, können „Class Action Scripts“ und „Standardklassen“ verwendet werden.
Abhängigkeiten können bei SVR4-Paketen unterschiedlich definiert werden. Hier gibt es drei Arten, das „prerequisite package“ (vorausgesetzte Paket), sowie die „reverse dependency“ (eine Abhängigkeit von...) und „incompatible package“ (inkompatible Paket).

IPS (Image Packaging System)

Ab Oracle Solaris 11 wird Software über das IPS installiert. IPS Pakete werden in Repositories (Depots) gespeichert, und von Publishern veröffentlicht.
Zusätzlich hat man die Möglichkeit, Images zu bereitzustellen. Diese werden unterteilt in:

–Full Images: Können ein komplettes System beinhalten
–Partial Images: Sind verknüpft mit einem Full Image, beinhalten jedoch kein Eigenes
–User Images: Verschiebbares Image

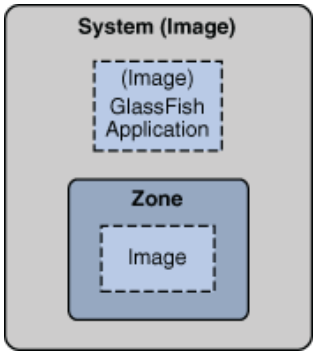

Abbildung 4: Partial Images innerhalb eines System Images[4]

Zur Verwaltung der Pakete auf einem System können zusätzlich zur Kommandozeile auch die graphischen Benutzerschnittstellen „Package Manager“ und „Update Manager“ verwendet werden.

Durch IPS werden folgende Fähigkeiten unterstützt:

- Auflisten, suchen, installieren, aktualisieren und entfernen von Software Paketen
- Auflisten, hinzufügen und entfernen von Paket Publishern. Ändern von Attributen der Publisher, wie die Suchpriorität und Attraktivität
- Systemaktualisierung auf einen neuen Stand.
- Spiegel eines existierenden Paket Depots erstellen.
- Neues Paket Depot erstellen.
- Pakete erstellen und veröffentlichen.
- Auflisten, erstellen, umbenennen, aktivieren und entfernen von Paketen in Bootumgebungen.

Kontaktadresse:

	Stefan Gärtner	**Andreas Auer**
	CCF AG	Oracle Deutschland
	Boschstrasse, 1	Amperestrasse 6
	D-64347 Griesheim	D-63225 Langen
Telefon:	+49 (0) 6155 666832	+49 (0) 6103 752 429
Fax:	+49 (0) 6155 666868	+49 (0) 6103 752 299
E-Mail	stefan.gaertner@ccf.de	andreas.auer@oracle.com
Internet:	www.ccf.de	www.oracle.com

Quellenverzeichnis:

1) *http://download.oracle.com/docs/cd/E19253-01/821-2332/ejurz/index.html*
2) *http://download.oracle.com/docs/cd/E18752_01/html/821-1911/jumpstartoverview-4.html*
3) *http://download.oracle.com/docs/cd/E19963-01/html/820-6566/intro-1.html*
4) *http://download.oracle.com/docs/cd/E19963-01/html/820-6572/figures/concept_img.png*