

**ORACLE®**




**ORACLE<sup>®</sup>**

## **Sichere SPARC Serverinstallation mittels der Wanboot-Technologie**

Stefan Gärtner, CCF AG

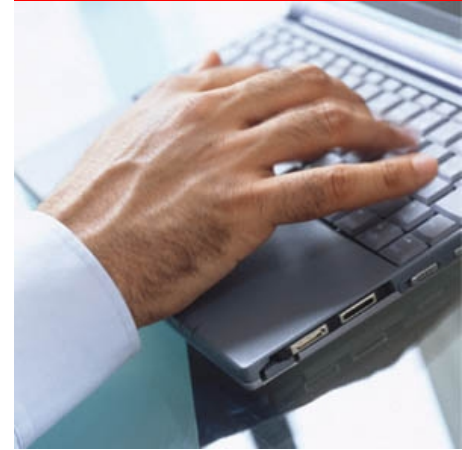
Andreas Auer, ORACLE Deutschland B.V. & Co. KG



The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

# Agenda

- Funktionsweise Wanboot (Sparc)
- Wanboot mit Jumpstart in Solaris 10
- Wanboot mit AI und IPS in Solaris 11 (b175)
- Unterschiede Jumpstart - AI
- Demo Secure Wanboot Solaris 10
- Demo Wanboot Solaris 11 (b175)
  
- Appendix
  - Cookbook Solaris 10
  - Cookbook Solaris 11



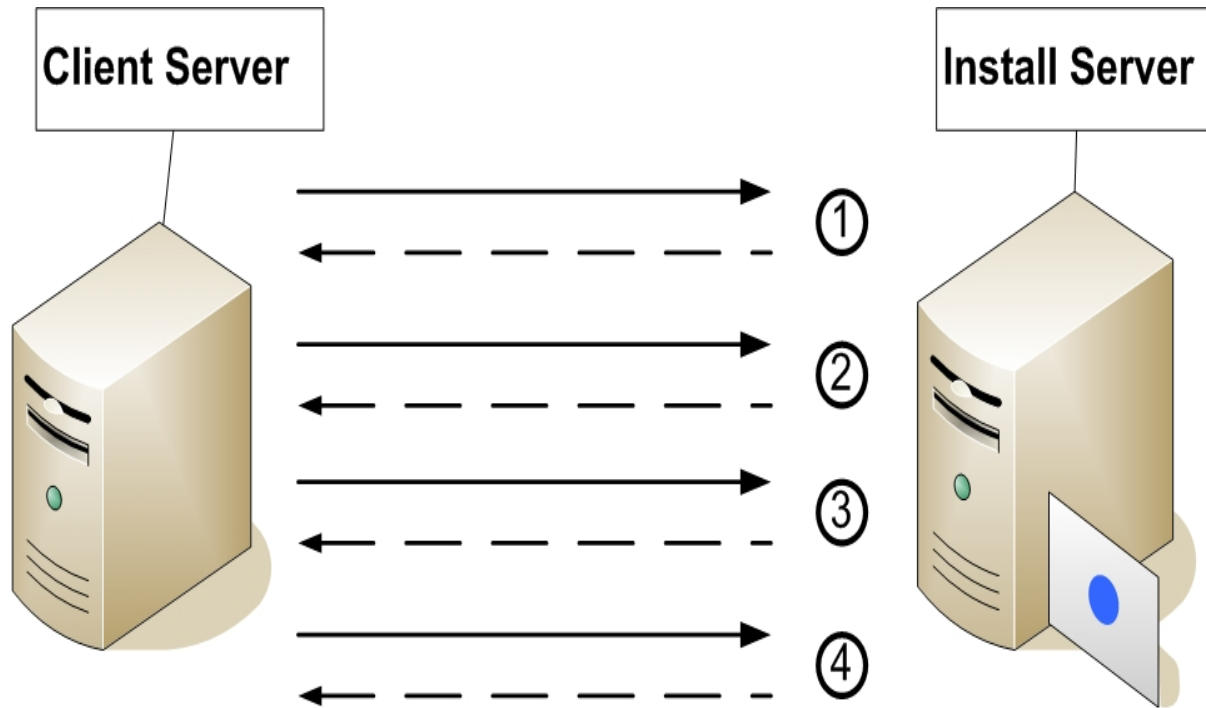
# Funktionsweise Wanboot (Sparc)

- **Peer Authentifikation:**  
Die Identität von Client und Server kann mit Hilfe von digitalen Zertifikaten gewährleistet werden
- **Vertraulichkeit der Daten:**  
Der Datenstrom kann über https (aes128 bit) verschlüsselt werden
- **Datenintegrität:**  
Durch Verwendung von digitalen Signaturen und der sicheren Verbindung wird ein modifizieren der Daten verhindert
- **Gehärtetes Miniroot Bootimage**

# Funktionsweise Wanboot (Sparc)

- Installation über http/https (Apache2)
- Flash-Archive
- Jumpstart Mechanismus
- Unternehmensweite Nutzung eines zentralen Installservers
- Keine zusätzlichen Services notwendig (DHCP,tftp,rarp,bootparamd)

# Funktionsweise Wanboot (Sparc)



# Funktionsweise Wanboot (Sparc)

Charakterisierung einer WAN-Boot Installation

- 1) Netzwerkkonfiguration und Download des Wanboot Programms
- 2) Ausführen des Wanboot Programms und Aufbau einer sicheren https Verbindung
- 3) Download des Solaris Miniroot Boot-Image
- 4) Ausführen des Miniroot Images und ausführen der Jumpstart Installation



# Funktionsweise Wanboot (Sparc)

## Booten des Clientsystems (ok boot net - install)

### 1) Auslesen der OBP Parameter

- Konfiguration des Netzwerkinterfaces
- Aktivierung der Schlüssel
- Laden des Wanboot Binary vom Installserver
- Ausführen des Wanboot Binary

# Funktionsweise Wanboot (Sparc)

## Booten des Clientsystems (cont.)

2) Laden des Clientzertifikats (Authentifizierung am Server)

- Entschlüsseln des Zertifikats mit AES Schlüssel
- Aufbau einer sicheren https Verbindung

3) Laden des Miniroot Boot-Image

- Booten des Miniroot Images

# Funktionsweise Wanboot (Sparc)

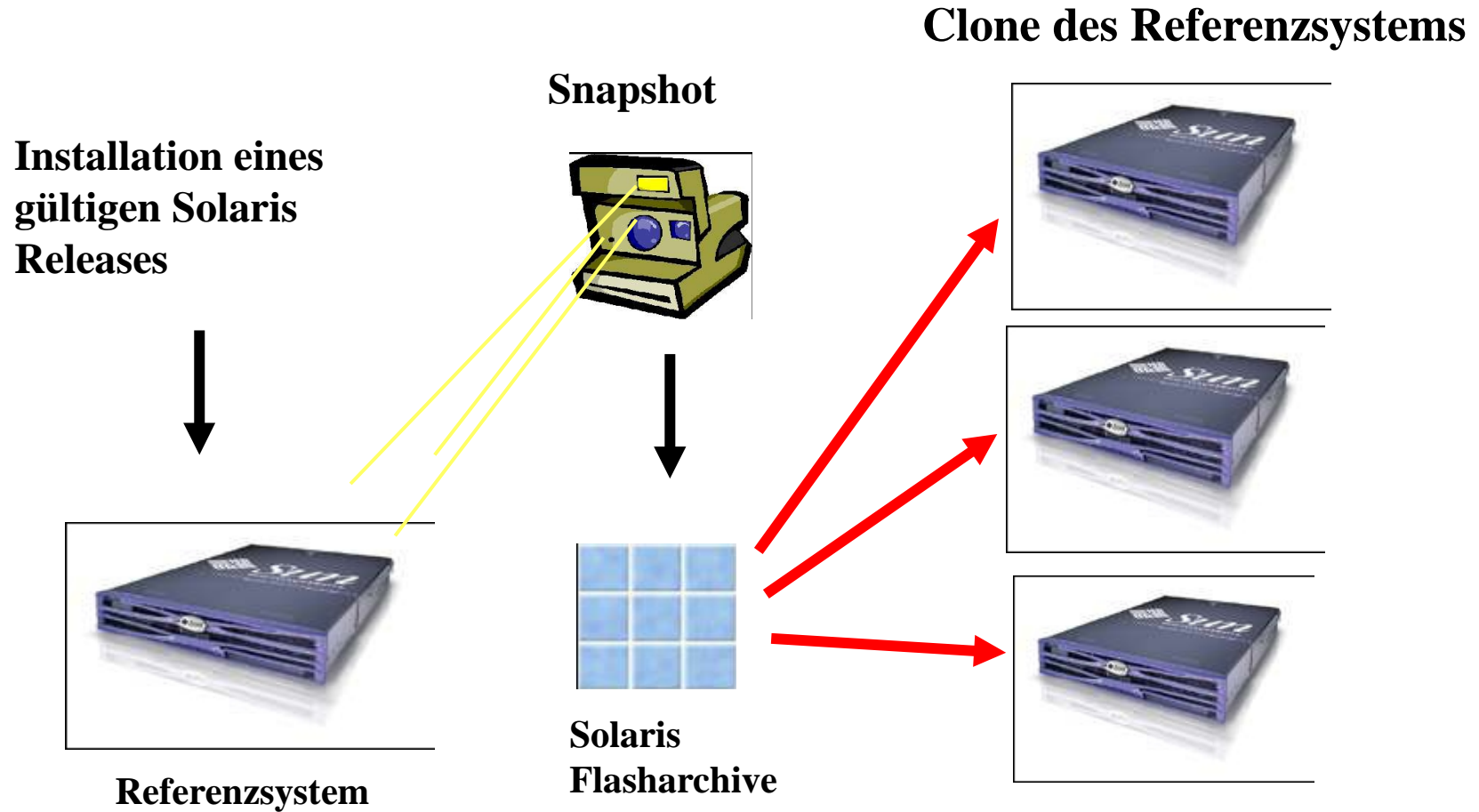
## Booten des Clientsystems (cont.)

### 4) Starten der Jumpstart Installation

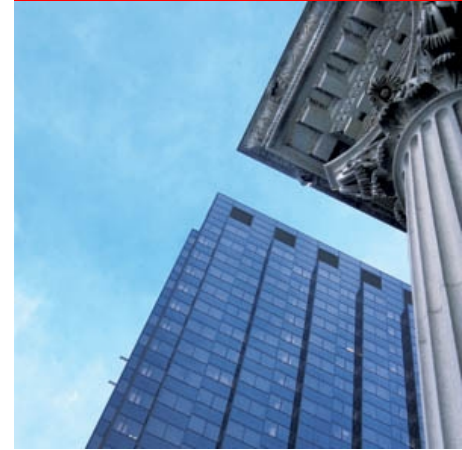
- Laden notwendiger Jumpstart Konfigurationsdateien vom Installserver (rules.ok, profile, begin und finish-Skripte)
- Ausführen eines evtl. begin-Skripts
- Laden und installieren des Flash-Archives
- Ausführen eines evtl. finish-Skripts und Reboot

# Funktionsweise Wanboot (Sparc)

## Solaris Flasharchive



- Funktionsweise Wanboot (Sparc)
- **Wanboot mit Jumpstart in Solaris 10**
- Wanboot mit AI und IPS in Solaris 11 (b175)
- Unterschiede Jumpstart - AI
- Demo Wanboot Solaris 10  
Demo Wanboot Solaris 11
  
- Appendix
  - Cookbook Solaris 10
  - Cookbook Solaris 11



# Wanboot mit Jumpstart in Solaris 10

## Wichtige Verzeichnisse (wanboot)

- /etc/netboot
- /etc/netboot/<Netzwerk-ID>/<Client-ID>/ ← Clientspez.

## Wanboot Konfig

- /etc/netboot/certificates/ ← Zertifikatsordner
- /etc/netboot/certificates/root\_ca/ ← Root-CA,Root-CA(p12)
- /etc/netboot/certificates/webserver/ ← Webserver Zert.
- /etc/netboot/certificates/<Client-ID>/ ← Client Zert.

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (wanboot)

- /etc/netboot/<Netzwerk-ID>/<Client-ID>/wanboot.conf
- /etc/netboot/<Netzwerk-ID>/<Client-ID>/system.conf
- /etc/netboot/<Netzwerk-ID>/<Client-ID>/truststore
- /etc/netboot/<Netzwerk-ID>/<Client-ID>/certstore
- /etc/netboot/<Netzwerk-ID>/<Client-ID>/keystore

# Wanboot mit Jumpstart in Solaris 10

wanboot.conf

*root\_server=https://192.168.10.10:443/cgi-bin/wanboot-cgi*

*boot\_file=/wanboot/wanboot.sun4v.sol10u10*

*root\_file=/miniroot/sparc.miniroot.sol10u10*

*signature\_type=sha1*

*encryption\_type=aes*

*server\_authentication=yes*

*client\_authentication=yes*

*boot\_logger=https://192.168.10.10:443/cgi-bin/bootlog-cgi*

*system\_conf=system.conf*



# Wanboot mit Jumpstart in Solaris 10

Wichtige Dateien (system.conf)

*SsysidCF=https://192.168.10.10:443/config/192.168.10.0/  
0100144F2A8AFC*

*SjumpsCF=https://192.168.10.10:443/config/192.168.10.0/  
0100144F2A8AFC*

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Client Zertifikate/Schlüssel)

- truststore → Identifikation des Servers
- certstore → Identifikation gegenüber dem Server
- keystore → RSA Schlüssel zum Entschlüsseln der Daten

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Verzeichnisse (Apache2)

- /etc/apache2/
- /etc/apache2/ssl.key/ ← Webserver RSA Key
- /etc/apache2/ssl.csr/ ← Webserver Zert.-Requests
- /etc/apache2/ssl.crt/ ← Webserver Zertifikat
- /var/apache/htdocs/ ← Document-Root des Apache
- /var/apache2/log/ ← Log-Verzeichniss
- /var/apache2/cgi-bin/ ← CGI-Skripte

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Apache2)

- /etc/apache2/http.conf ← Apache2 Konfigdatei
- /etc/apache2/ssl.conf ← SSL Konfigdatei
  
- /etc/apache2/ssl.key/server.key ← RSA Key
- /etc/apache2/ssl.csr/server.csr ← Webserver Request
- /etc/apache2/ssl.csr/server.cert ← Webserver Zert.
- /etc/apache2/ssl.csr/ca.crt ← Root Zert. Chain
  
- /var/apache2/log/access\_log ← Zugriffs-Logdatei
- /var/apache2/log/error\_log ← Fehler-Logdatei

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Verzeichnisse (Jumpstart)

- /installsrv/ ← Apache Document Root (ssl)
- /installsrv/config/ ← Client Jumpstart Verzeichnisse
- /installsrv/flash/ ← Flash-Archive
- /installsrv/wanboot/ ← Wanboot Binary
- /installsrv/miniroot/ ← Boot Image
- /installsrv/iso/ ← Solaris 10 ISO Images
- /installsrv/log/ ← Log-Verzeichniss

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Jumpstart)

- /installsrv/config/<Net-ID>/<Client-ID>/rules
- /installsrv/config/<Net-ID>/<Client-ID>/check
- /installsrv/config/<Net-ID>/<Client-ID>/rules.ok
- /installsrv/config/<Net-ID>/<Client-ID>/profile
- /installsrv/config/<Net-ID>/<Client-ID>/sysidcfg

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Jumpstart)

- /installsrv/config/<Net-ID>/<Client-ID>/rules.ok

Inhalt: Standard rules Datei

*any - - any.profile -*

*# version=2 checksum=1760*

# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Jumpstart)

- `/installsrv/config/<Net-ID>/<Client-ID>/any.profile`

*install\_type*            *flash\_install*

*archive\_location*      *https://192.168.10.10:443/flar/solaris\_10u10\_sparc\_T1000.flar*

*partitioning*            *explicit*

*pool rpool auto auto auto rootdisk.s0*

*bootenv installbe bename sol10u10 dataset /var*



# Wanboot mit Jumpstart in Solaris 10

## Wichtige Dateien (Jumpstart)

- `/installsrv/config/<Net-ID>/<Client-ID>/sysidcfg`

*system\_locale=C*

*timezone=CET*

*terminal=vt100*

*timeserver=localhost*

*name\_service=NONE*

*nfs4\_domain=dynamic*

*root\_password=U83x9BD5ldxgo*

*network\_interface=bge0 {hostname=sparc-client default\_route=192.168.10.1  
ip\_address=192.168.10.20 netmask=255.255.255.0 protocol\_ipv6=no}*

*security\_policy=NONE*

*service\_profile=limited\_net*

*auto\_reg=NONE*

# Agenda

- Funktionsweise Wanboot (Sparc)
- Wanboot mit Jumpstart in Solaris 10
- **Wanboot mit AI und IPS in Solaris 11 (b175)**
- Unterschiede Jumpstart - AI
- Demo Wanboot Solaris 10
- Demo Wanboot Solaris 11
  
- Appendix
  - Cookbook Solaris 10
  - Cookbook Solaris 11



# Image Packaging System (IPS)

Einführung mit Solaris 11

- IPS verwaltet Pakete
- Pakete bestehen aus
  - Ordner
  - Dateien
  - Links
  - Treibern
  - Abhängigkeiten!!!
  - Gruppen
  - Benutzer
  - Lizenzinformationen

# Image Packaging System (IPS)

## Pakete

- Unterstützt IPS und SVR4 Pakete
- Pakete werden von „Publishern“ aus „Repositories“ abgerufen
- Erforderliche Pakete kommen aus dem Repository
- Beispiel: Paket „entire“ hat als Abhängigkeit alle Pakete

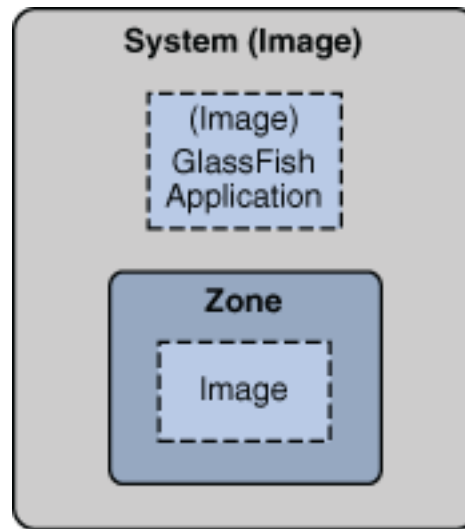
# Image Packaging System (IPS)

## Image

- Hier können Pakete installiert werden
- 3 Imagearten
  - Full Image (Komplettes Abbild eines Systems)
  - Partial Images (verknüpft mit einem Full Image)
  - User Images (vom Gesamtsystem unabhängig)

# Image Packaging System (IPS)

Image



# Solaris 11 AI Installserver

## Hard- & Softwareanforderungen

- CPU-Architektur SPARC oder x86 / 1 GB RAM
- Netzwerkanbindung
- Solaris 11 Installation
- Speicher für Repository / Repositories

# Solaris 11 AI Installserver

## Vorgehensweise

- Solaris 11 Repository in vorgesehenes Verzeichnis
- AI Installation Tools installieren
- AI Install Service erstellen und konfigurieren
- Service- und System Configuration Manifest editieren (XML)



# Solaris 11 AI Installserver

## Empfehlungen

- Eigener Datenpool für Repository
- Aktivierung von DHCP für PXE-Installation notwendig

# Solaris 11 AI Installserver

## Service-Manifest

- Unterschiedliche Client-Konfigurationsanweisungen
- Zieldefinition (hierarchisch)
  - CPU-Architektur *arch* (i86pc || sun4u || sun4v)
  - MAC-Adresse *mac*
  - IP-Adressrange *ipv4*
  - Prozessortyp *cpu* (i386 || sparc)
  - Maschinentyp *platform* (i86pc || SUNW,Sun-Fire-T200 ||...)
  - feste RAM-Größe oder RAM-Bereich *mem* (unbounded = unbegrenzt)

# Solaris 11 AI Installserver

## Service-Manifest

- Gesamtes Manifest umschlossen von `<auto_install>` und darin `<ai_instance>`
- In `<target>` kann das Zielgerät angegeben werden (optional)
- Innerhalb von `<software>` Angabe von Quellinformationen
  - `<source>` Repositoryname, weitere Repo-Server
  - Wichtig: Hier wird das übergeordnete Image für die Installation angegeben!
- `<add_drivers>` (selbsterklärend und optional)

# Solaris 11 AI Installserver

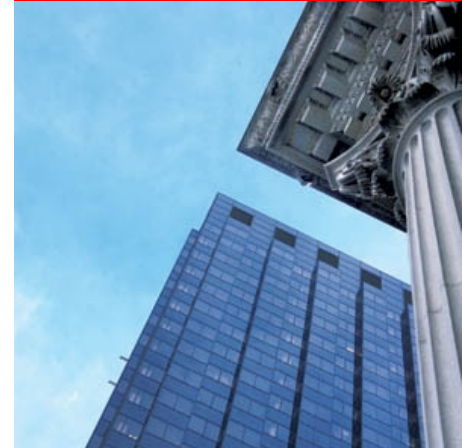
## System Configuration Manifest

- Benutzer-, Gruppen- und Rolleneinstellungen
- Terminal-Typ und Keyboard
- Netzwerkeinstellungen

# Solaris 11 AI SPARC-Client Installation

- Client in OBP booten
- Client auf Installserver erstellen (*installadm create-client ...*)
- *network-boot-arguments* in OBP setzen
- *boot net – install*

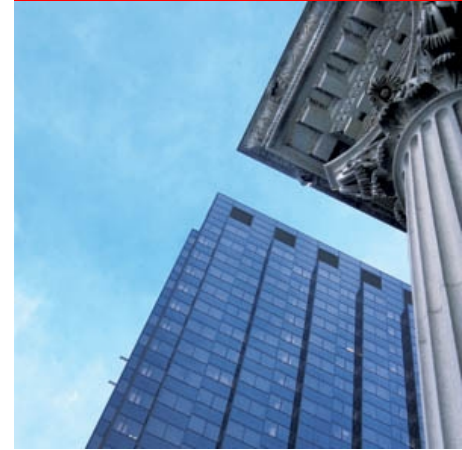
- Funktionsweise Wanboot (Sparc)
- Wanboot mit Jumpstart in Solaris 10
- Wanboot mit AI und IPS in Solaris 11 (b175)
- **Unterschiede Jumpstart - AI**
- Demo Wanboot Solaris 10  
Demo Wanboot Solaris 11
  
- Appendix
  - Cookbook Solaris 10
  - Cookbook Solaris 11



# Vergleich: Jumpstart & AI

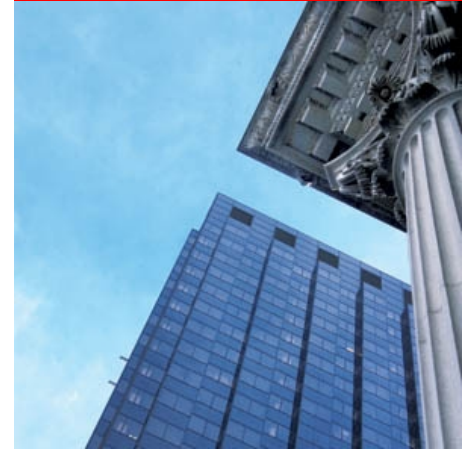
- Jumpstart traditionell (Skripte und ASCII-Dateien)
- AI verfolgt Solaris 10-Schema (Serviceorientiert und Manifests)
  - Befehle wurden an Solaris 11 Konvention angepasst
- Service Manifest ersetzt rules und profile
- SC Manifest ersetzt sysidcfg
- Jumpstart verwendet System V Release 4 Pakete und Flash-Archive
- AI verwendet Image Packaing System

- Funktionsweise Wanboot (Sparc)
- Wanboot mit Jumpstart in Solaris 10
- Wanboot mit AI und IPS in Solaris 11 (b175)
- Unterschiede Jumpstart - AI
- Demo Wanboot Solaris 10
- Demo Wanboot Solaris 11
  
- Appendix
  - Cookbook Solaris 10
  - Cookbook Solaris 11






# Demo



# For More Information

<http://search.oracle.com>



or

[oracle.com](http://oracle.com)

**ORACLE®**



**ORACLE IS THE INFORMATION COMPANY**