Solaris 10 Zones

Sebastian Pasewaldt,
Martin Koeleman,
Robert Reicherdt

Solaris 10 Zones

- **Teil I - Einführung in das Zones-Konzept**
  - **Was sind Solaris Zones?**
  - **Anwendungsgebiete**
  - **Features**
  - **Funktionsweise**
  - **Paketverwaltung und Zones**
- **Teil II – Befehle zum Einrichten einer Zone**

Was sind Solaris Zones?

- Mittel zur Virtualisierung und Partitionierung von Betriebssystemdiensten
  - Betriebssystemdienste: Dateisysteme, Geräte, Speicher, CPU-Zeit
- Bietet eine isolierte Umgebung zur Anwendungsausführung
  - Prozesse können auf keinerlei BS-Ressourcen außerhalb ihrer Zone zugreifen
- Vergleichbar mit BSD Jails / Xen
- Auf allen von Solaris 10 unterstützten Rechnerarchitekturen verfügbar
  - Zones benötigen keinerlei besondere Hardware

Anwendungsgebiete

- Zusammenfassung mehrerer Serveranwendungen auf einer Maschine
  - Bessere Ausnutzung leistungsfähiger Hardware
  - Verringerung von Administrationsaufwand und dadurch –kosten
  - Dynamische Umverteilung von Ressourcen
- Verwendung unterschiedlicher Versionen desselben Programms auf einer Maschine
- Kapselung von sicherheitskritischen oder instabilen Anwendungen
  - Es wird keine dedizierte Maschine für solche Anwendungen benötigt
- Delegation von Administrationsaufgaben

Features (1/2)

- Gewährleistung von erhöhter Sicherheit
  - Ein Prozess hat keine Möglichkeit, eine *Non-Global Zone* zu verlassen
  - Auch bei Ausnutzung von Sicherheitslücken bleibt der anrichtbare Schaden auf die jeweilige Zone begrenzt
- Isolation von Anwendungen
  - Benutzung von Anwendungen aus verschiedenen *Trust Domains* auf derselben Maschine
  - Trennung der Netzwerkverkehrs, auch wenn verschiedene Zones dasselbe physikalische Interface verwenden

Features (2/2)

- Virtualisierung
  - Jede Zone bietet eine vollständig virtualisierte Ausführungsumgebung für Anwendungen an
  - Eigenschaften des Hostrechners, wie z.B. IP-Adresse und Geräte-pfade können versteckt werden
- Granularität
  - Betriebssystemressourcen wie Prozessor, Speicher und weitere Geräte können in fast beliebiger Feinheit eingeteilt werden
- Standardkonformität
  - Es werden keine neuen APIs eingeführt
  - Einschränkungen bei Programmbetrieb in einer *Non-Global Zone* beziehen sich fast ausschließlich auf privilegierte Instruktionen

Funktionsweise (1/2)

- Ein gemeinsamer Betriebssystemkern für alle Zones
  - Keine Virtual Machine, wenig Overhead
- Es wird unterschieden zwischen der *Global Zone* und *Non-Global Zones*
- Gemeinsame Verwendung von Paketen aus der G*lobal Zone* in *Non-Global Zones* möglich
  - *Sparse Root Zones* vs. *Whole Root Zones*
- Jede Zone hat ein Wurzelverzeichnis im Dateisystem des Hostrechners
- Einbindung weiterer Dateisysteme ist ohne Einschränkung möglich

Funktionsweise (2/2)

- Gerätedateien können ebenso eingebunden werden
  - Dadurch: Abstraktion von physikalischen Details des Hostrechners, z.B. Pfaden zu Gerätedateien
- Zur Netzwerkanbindung erhält jede Zone ihre eigenen IP-Adressen an den gewünschten Netzwerk-Interfaces
  - Dies ist die einzige Möglichkeit, mit Prozessen in anderen Zones zu kommunizieren
- Der Ressourcenverbrauch von Prozessen in einer Zone kann eingeschränkt werden
  - CPU-Zeit, Speicherplatz, Anzahl von Prozessen

Paketverwaltung und Zones

- Nur eine Teilmenge der Pakete aus der Global Zone wird in eine Non-Global Zone kopiert
- Installation weiterer Pakete in der Non-Global Zone ist möglich
- Pakete und Patches können automatisch in allen oder nur in gewählten Zones (de)installiert werden
- Steuerung des Paketverhaltens im Zusammenspiel mit Zones durch die folgenden pkginfo-Parameter:
  - `SUNW_PKGTYPE` (`root` oder andere)
  - `SUNW_PKG_ALLZONES` (`true` oder `false`)
  - `SUNW_PKG_HOLLOW` (`true` oder `false`)

Solaris 10 Zones

- **Teil I - Einführung in das Zones-Konzept**
- **Teil II – Befehle zum Einrichten einer Zone**
  - **zonecfg**
    - **Erklärung des Befehls**
    - **Subcommands**
    - **Ressourcen**
    - **Beispiel**
  - **Non Global State Model**
  - **zoneadm**
    - **Erklärung des Befehls**
    - **Subcommands**
  - **zlogin**

zonecfg

- Dient der Konfiguration der einzelnen Zonen
- Drei Modi:
  - Interactive: `zonecfg –z zonename` → `zonecfg:zonename>`
  - command-line: `zonecfg –z zonename cmd1; cmd2; ...`
  - command-file: `zonecfg –z zonename –f command_file`
- Aufgaben:
  - Erstellen/Löschen von Konfigurationen
  - Hinzufügen/Entfernen von Ressourcen
  - Ändern von Ressourcen
  - Verifizierung einer Konfiguration

zonecfg – Subcommands (1/3)

`help [subcommand]` – zeigt Hilfsinformationen an

`create [-f –b –t]` – erstellt eine Zonekonfiguration (in-memory)

`export [outputfile]` – Ausgabe der Konfiguration

`info` – gibt Informatioen über die Konfiguration
`zonecfg –z` ***zonename*** **`info`** `<subcommand>`

`set` – ordnet einem Attribut einem Wert zu
`zonecfg:my-zone>` **`set`** ***`zonepath=/export/home/my-zone`***

`select` – wählt Attribut-Wert-Paare von Ressourcen zur Änderung aus

`zonecfg:my-zone>` **`select`** ***`rctl name=zone.cpu-shares`***

zonecfg – Subcommands (2/3)

`add` – fügt Ressourcen hinzu

`end` – beendet Konfiguration einer Ressource und verifiziert sie

```
zonecfg:my-zone> add net
zonecfg:my-zone:net> set address=192.168.0.1
zonecfg:my-zone:net> set physical=hme0
zonecfg:my-zone:net> end
zonecfg:my-zone>
```

`remove` – entfernt Attribut-Werte-Paare

```
zonecfg:my-zone:net> remove address=192.168.0.1
```

`cancel` – beendet Konfiguration, ohne Änderungen zu speichern

zonecfg – Subcommands (3/3)

`verify` – verifiziert die aktuelle Konfiguration

`revert` – setzt die Konfiguration zum letzten per `commit` gespeicherten Punkt zurück

`commit` – verifiziert Konfiguration und schreibt sie auf den Datenträger

`delete` – löscht Konfig. aus Speicher und vom Datenträger

`exit` – beendet *zonecfg* und führt `commit` durch falls nötig

zonecfg – Ressourcen (1/2)

Typ	Properties	Erklärung
zonename	Keine	Identifiziert die Zone für zonecfg
zonepath	Keine	Gibt Pfad der Zone an
fs	dir, special, raw, type, options	Dateisysteme, welche eingebunden wird
inherit-pkg-dir	dir	read-only packaged Software aus Global-Zone
net	adress, physical	virtuelle Netzwerkschnittstelle

zonecfg – Ressourcen (2/2)

Typ	Properties	Erklärung
device	match	Gerätetreiber
rctl	name, value (zone.cpu-shares zone.max-lwps)	Ressource Kontrolle
attr	name, type, value	Kommentare

zonecfg – Beispiel

```
global# zonecfg -z my-zone
zonecfg:my-zone> create
zonecfg:my-zone> set zonepath=/export/home/my-zone
zonecfg:my-zone> add fs
zonecfg:my-zone:fs> set dir=/mnt
zonecfg:my-zone:fs> set special=/dev/dsk/c0t0d0s2
zonecfg:my-zone:fs> set raw=/dev/rdsk/c0t0d0s2
zonecfg:my-zone:fs> set type=ufs
zonecfg:my-zone:fs> add options [nodevices,logging]
zonecfg:my-zone:fs> end
```

Non-Global State Model

- **Configured:** Zonekonfiguration ist abgeschlossen und wurde verifiziert
- **Incomplete:** Zone wird gerade (de)installiert
- **Installed:** Zone wurde mit der verifizierten Konfiguration installiert. Files wurden kopiert und Zone ist nun bootbar.
- **Ready:** Virtuelle Plattform für die Zone wird erschaffen:
  - zsched wird durch Kernel gestartet
  - Festsetzung der Netzwerkeinstellungen
  - Einbinden des Dateisystems
  - Konfiguration der Geräte
  - Zuordnung der Zone ID
- **Running:** Ready-Zone in der min. ein Userprozess läuft
- **Down:** Zone ist angehalten

zoneadm

- dient der Erstellung und Administration von Zones nur in der Global Zone anwendbar
- Aufgaben:
  - Verifizierung der Zonekonfiguration
  - (De)Installation
  - (Re)Boot
  - Anhalten
  - Löschen
  - Anzeigen von Zoneinformationen
- Anwendung:

  `zoneadm –z` *`zonename`* `<subcommand>`

zoneadm - Subcommands

verify – überprüft eine bestehende Konfiguration

```
global# zoneadm -z zonename verify
```

list – gibt nähere Informationen zum Status der Zone

```
global# zoneadm -z [zonename] list [-c,-i,-v,-p]
```

(un)install – (de)installiert eine vorhandene Konfiguration

```
global# zoneadm -z zonename (un)install
```

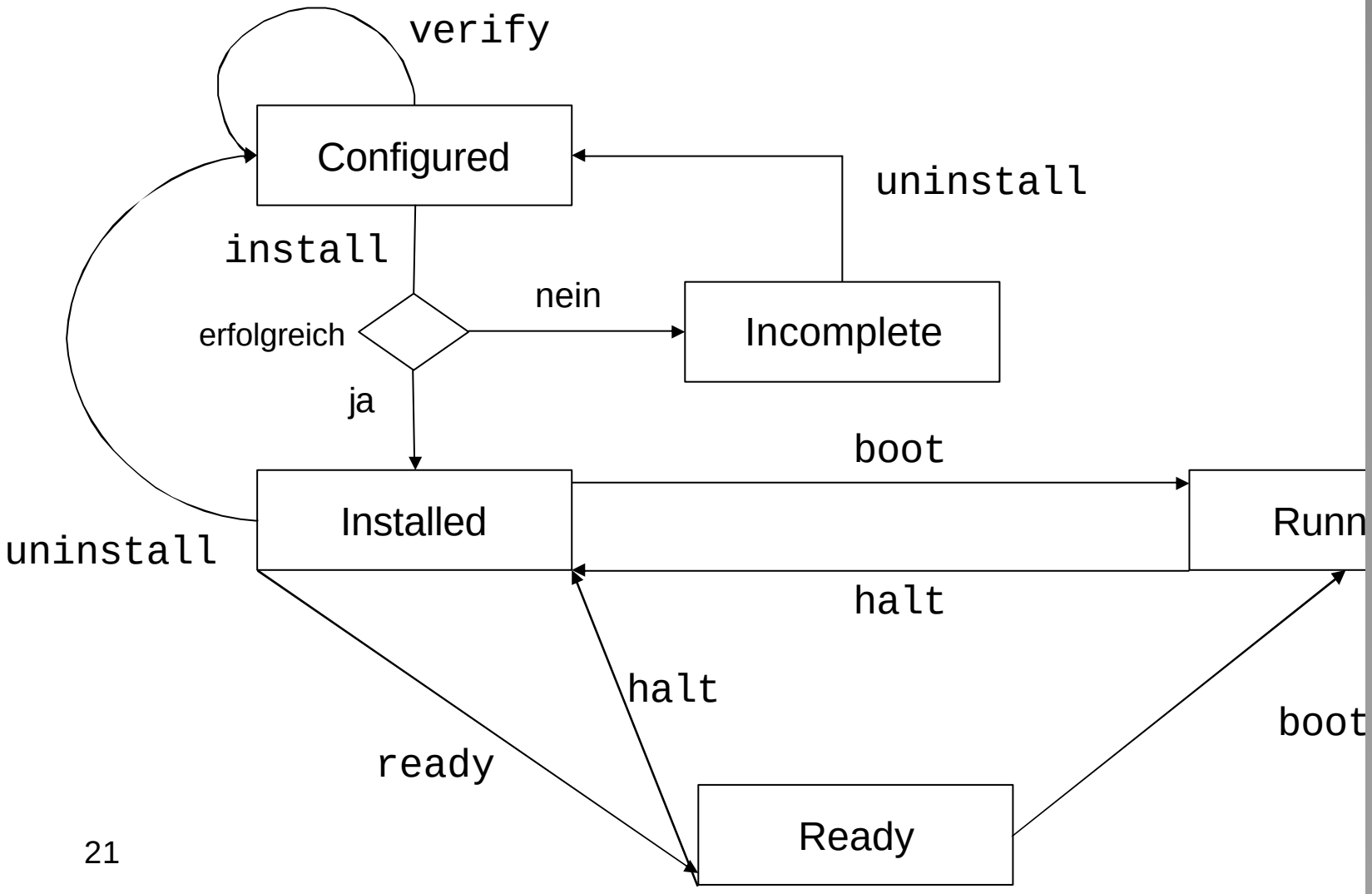
(re)boot – (re)bootet die vorhandene Zone

```
global# zoneadm -z zonename (re)boot
```

halt – hält die Zone an

```
global# zoneadm -z zonename halt
```

zoneadm


verify
Configured
uninstall
install
nein
erfolgreich
Incomplete
ja
boot
Installed
Runn
uninstall
halt
halt
boot
ready
Ready

Zlogin

- Ermöglicht das einloggen in eine Non Global Zone
- Drei Modi: interactive, console, failsafe
- Anwendung:

`zlogin [–c,-s] `*`zonename`*` [shutdown]`

`exit`

Quellen

1. Sun: „**System Administration Guide: Solaris Containers-Resource Management and Solaris Zones**“ http://docs.sun.com/app/docs/doc/817-1592
2. Sun: „**Big Admin: Solaris Zones**“ http://www.sun.com/bigadmin/content/zones/
3. Brendan Gregg: „**Zone Examples**“ http://users.tpg.com.au/adsln4yb/zones.html