Solaris 11 Zonen in der Praxis

Ulrich Gräf
Oracle Deutschland B.V. & Co. KG
Robert-Bosch Str. 5, D-63303 Dreieich

Schlüsselworte
Solaris, Solaris 11, Solaris 10, Solaris Zonen, Virtualisierung, Branded Zones, IPS

Einleitung

Solaris Zonen sind eine Virtualisierung auf Ebene des Betriebssystems.

Unter Virtualisierung verstehen viele nur die Bereitstellung eines virtuellen Computers wie unter OVM (Oracle Virtual Machine), Virtualbox, QEmu, Parallels, VMware ... (HW/SW Schnittstelle). Darauf wird jeweils ein eigenes Betriebssystem installiert und das Sharen von Ressourcen ist limitiert.

Bei Solaris Zonen ist die Schnittstelle der Virtualisierung zwischen User-Programmen und dem Betriebssystem eingerichtet. Das erfordert die Benutzung des gleichen Kernels, erlaubt aber auch das größtmögliche Sharen von Ressourcen.

Solaris Zonen (Solaris Container) sind seit Solaris 10 (2005) verfügbar und heute bei vielen Kunden im Einsatz. Mit Solaris 11 sind einige Details der Zonen an neue Eigenschaften von Solaris 11 angepasst worden und neue Möglichkeiten von Solaris 11 den Zonen zur Verfügung gestellt worden.

Hier soll die Nutzung von Solaris 11 Zonen in der Praxis erläutert werden.

Was sind Zonen?

Eine spezielle Zone, die auch die Hardware des Rechners managt und so aussieht wie ein Solaris vor Solaris 10 nennt man globale Zone.
Eine Solaris Zone, auch nicht-globale oder non-global Zone genannt, ist eine verkleinerte Betriebssystem-Installation, bei der der Teil fehlt, der sich mit dem Managen der Hardware beschäftigt (u.a. der Kernel und die Treiber).
Systemcalls von globaler und nicht-globaler Zone erreichen den Kernel und die für die Zone konfigurierte Umgebung wird vom Kernel berücksichtigt (Security, vgl. *Mandantenfähigkeit*).

Jede Zone hat einen eigenen Dateibaum. Man kann Verzeichnisse definieren, die in mehreren Zonen sichtbar sind, so dass der Dateiaustausch oder die gemeinsame Nutzung von Programmen möglich ist.
Jede Zone hat eigene Netzwerk-Schnittstellen die in von den anderen Zonen separierte Netzwerke gehen können.
Die Zonen haben eine eigene separierte Einstellung für Name-Services (lokal, NIS, DNS, LDAP,...), worunter die Userids, die Netzwerke, die definierten Hosts, usw fallen. Damit kann jede Zone auch unter anderem unterschiedliche Passwörter für `root` haben.
Die Prozesse der Zonen sind nur in der jeweiligen Zone sichtbar. Lediglich die globale Zone kann alle Prozesse sehen.
Shared Segmente, Inter-Prozess Komunikation, Projekte, sind separat von anderen Zonen.
Obwohl in der Voreinstellung keine Devices wie Platten in den Zonen sichtbar sind ist es doch möglich solche Devices an die Zonen zu übergeben, sofern die Applikation dies erfordert.

Die Zonen können mit Resource Management limitiert werden, z.B. bei CPUs, Memory oder Anzahl der möglichen Prozesse, so dass sie sich nicht gegenseitig beeinflussen können.

Neue Möglichkeiten in Solaris 11

Full root Zonen: In Solaris 10 konnte man die Zonen als full-root Zonen oder als sparse Zonen einrichten. In beiden Typen sind in der nicht-globalen Zone alle Pakete der globalen Zone installiert. In der sparse Zone wurde jedoch Platz eingespart, indem große Verzeichnisse wie z.B. `/usr` der globalen Zone in der lokalen Zone mitbenutzt worden sind.

Solaris 11 erfordert dass jede Zone full-root Zone ist, jedoch entfällt die Notwendigkeit, alle Pakete der globalen Zone zu installieren. Insofern kann man jetzt den Umfang der Pakete in der Zone auf das absolut notwendige senken (Security) auch wenn in der globalen Zone alles installiert ist.

Die Entflechtung der Filesysteme erlaubt auch das IPS Paketsystem für die Zonen zu benutzen was weitere Vorteile bringt (siehe unten).

ZFS Encryption: In Solaris 11 wird für ZFS Dateisysteme ein Verschlüsselungssystem eingeführt. Dieses ist auch in Zonen nutzbar.

Physical to virtual Migration: Die globale Zone eines Solaris 11 Systems kann mit einem p2v-Tool (physical to virtual) in eine Zone migriert werden. Dabei wird auf die notwendigen Veränderungen beim Netzwerk und bei Storage hingewiesen (`zonep2vchk` Tool).

Read-only Zonen: Vielfacher Wunsch bei Virtualisierungs- und Konsolidierungssystemen ist dass die Betriebssystemumgebung nicht korrumpiert werden kann. Mit Solaris 11 ist es möglich eine Zone auf read-only zu konfigurieren, das heisst die Betriebssystem-Installation in der Zone ist unveränderlich. Man kann Teile schreibbar machen (`/etc` oder `/var`) und natürlich können die Applikationsverzeichnisse schreibbar konfiguriert werden.

Die Zone ist somit sicherheitstechnisch gehärtet und in sensitiven Umgebungen einsetzbar. Für Updates oder sonstige Systemarbeiten kann die Zone als schreibbar gestartet werden. Dieses ist aber nur von dem Administrator der Zone aus der globalen Zone heraus möglich. Der Adminstrator, der nur Zugang zur Zone selbst hat, kann die Schreibbarkeit nicht herstellen.

Netzwerk Virtualisierung (Crossbow)

In Solaris 11 gibt es ein System zur Netzwerk-Virtualisierung, das für die Verbindung von Zonen zu Netzwerken ausserhalb, von Zonen untereinander und zu Logical Domains (OVM for SPARC) genutzt werden kann.

Bereits in Solaris 10 gibt es den Modus *exclusive-IP* von Zonen, die dann eine eigene Instanz des IP Stackes besitzen. Man kann dann die IP Interfaces in der Zone konfigurieren. In Solaris 10 benötigt man für diesen Modus jedoch ein eigenes Interface oder VLAN-Interface für jedes Interface der Zone. Diese Limitierung erschwert wegen der Netzwerk-Randbedingungen und der limitierten Zahl der einbaubaren Netzwerk-Karten die Nutzung von exclusive-IP in Solaris 10.

In Solaris 11 beruht die Netzwerk-Virtualisierung (Entwicklungsname: Crossbow) auf der Möglichkeit vnics (virtual network interface card) zu erzeugen (Kommando: `dladm`).
Ein solcher vnic kann auf einer realen Netzwerk-Karte erzeugt werden und ist damit quasi an dem Netzwerk-Kabel angeschlossen, an dem auch der reale Netzwerk-Anschluss angeschlossen ist. Von einem echten Netzwerk-Interface unterscheidet sich ein vnic nicht, er hat ebenfalls eine eigene MAC Adresse, gehört ggf. zu einem Vlan und läßt sich wie eine Netzwerk-Karte administrieren (`ipadm`).

Zusätzlich läßt sich ein vnic auch auf einem virtuellen Switch erzeugen, wodurch man Zonen verbinden kann, indem man für sie jeweils einen vnic auf dem gleichen virtuellen Switch erzeugt.

Weiterhin kann man Bridges zwischen Netzwerk-Interfaces definieren. Damit können vnics verbunden werden, die sonst keine Verbindung haben. Diese Funktionalität kann quasi zum einfachen *Verdrahten* von bestehenden Komponenten verwendet werden.

Zu den vnics kann noch eine Bandbreite konfiguriert werden (`flowadm`), mit der man einfach verhindern kann, dass eine Applikation in einer Zone die Netzwerkbandbreite anderer Applikationen stört.

Solaris 10 Zone in Solaris 11

Solaris 10 Systeme können in Solaris 11 ablaufen (*branded zone*, Zonen Typ: `solaris10`)

Dazu kann man eine native Solaris 10 Zone (Typ: `native`) archivieren und unter Solaris 11 in einer Solaris 10 Zone installieren. Die Zone selber sieht dann eine Solaris 10 Umgebung und kann fast unverändert ablaufen. Zusätzlich kann die Netzwerk-Virtualisierung von Solaris 11 für die Einbindung der Solaris 10 Zone verwendet werden. Unter anderem funktioniert auch das Resource Management für Netzwerke von Solaris 11 (`flowadm`) für die Solaris 10 Zonen, das so unter Solaris 10 nicht existiert.

Zusätzlich ist es möglich eine Solaris 10 globale Zone in eine Solaris 10 Zone unter Solaris 11 zu migrieren.

Diese Funktonalität erlaubt eine leichte Migration von Solaris 10 Umgebungen nach Solaris 11 ohne dass die Anwendungsumgebung sofort migriert werden muss. So kommen die Vorteile von Solaris 11 auch diesen Applikationen zugute, ohne dass ein wesentlicher Migrationsaufwand anfällt.

In der SPARC Version von Solaris 10 gibt es die Zonen-Typen `solaris8` und `solaris9`, die benutzt werden können um Altsysteme auf aktueller Hardware laufen zu lassen. Dieses erleichtert die Umstellung und kann Revisionszwecken dienen. Diese Zonen-Typen stehen unter Solaris 11 nicht zur Verfügung, so dass der Betrieb dieser Zonen auf Solaris 10 bleiben muss. Der Solaris 10 Support bleibt aber noch einige Zeit bestehen, so dass man nur bei langfristig geplanten Betrieb an eine Migration denken muss.

IPS Paketsystem für Zonen

Mit Solaris 11 steht das neue IPS Paketsystem (*Image Packaging System*) zur Verfügung. Es basiert auf einem neuen Format für Pakete, das besser an aktuelle Anforderungen angepasst ist. Das wesentliche Merkmal ist, daß die Installation im Regelfall über das Netzwerk erfolgt. Die Pakete sind dazu auf einem Server abgelegt, der als Package Repository dient. Es kann der Repository Server von Oracle über das Internet verwendet werden oder es kann ein eigener Server aufgebaut werden. Sogar eine Infrastruktur ohne direkte Verbindung zum Internet ist möglich.

Das Paket Utility (`pkg`) erlaubt Pakete zu suchen, zu installieren und zu löschen. Insbesondere werden Abhängigkeiten automatisch aufgelöst, wodurch das manuelle Herstellen von Vorausetzungen entfällt, was noch bei Solaris 10 notwendig war.
Es enthält ebenfalls Funktionen um ganze Gruppen von Paketen bis zum gesamten Betriebssystem zu installieren oder zu aktualisieren.

Die Mechanismen für das Patchen von Solaris 10 werden durch Aktualisierung auf neue Paket-Versionen in Solaris 11 ersetzt. Da nur die zwischen dem Ist-Stand und dem Soll-Stand

unterschiedlichen Dateien transferiert werden, ist dieses System sogar effizienter als die Patches von Solaris 10. Die Solaris 10 Paches müssen immer alle möglichen Dateien enthalten, weil vorher nicht bekannt sein kann, auf welchen Ist-Stand der Patch installiert wird.

Die SVR4 Pakete vor Solaris 11 lassen sich ebenfalls installieren, was besonders für die Nutzer interessant ist, die eigene Pakete erstellt haben.

Werkzeuge zum Erstellen, Kopieren und Updaten von Paket Repositories sind auch enthalten.
Ein wesentlicher Punkt ist, dass die Möglichkeiten von Live Upgrade (Solaris 8 bis Solaris 10) zum Update des Betriebssystems während des Normalbetriebs nun in einer Standard-Installation enthalten sind (Boot Environments, `beadm`). Die besonderen Eigenschaften des ZFS Dateisystems im Bereich Snapshots und Clones werden hier genutzt.

Ein wesentliches Defizit von Solaris 10 bei dem Bewegen von Zonen zwischen Rechnern war, dass die Zonen auf den gleichen Stand installiert werden mussten. Die Erkennung des gleichen Standes wurde durch die Patch Mechanismen erschwert. Das IPS System vereinfacht die Anpassung der Zonen erheblich: Mit Solaris 11 erhalten die Zonen ebenfalls Boot Environments die in einem ZFS Dateisystem liegen und können parallel zu der globalen Zone aktualisiert werden. Eine Zone kann wie unter Solaris 10 an ein Zielsystem angepasst werden (`zoneadm attach -u / -U`). Zusätzlich ist es einfach möglich, eine Zone an das vorige System mit dem älteren Stand zurückzugeben, weil die alte Version des Boot-Environments der Zone dort noch *passt*.

Zusammenfassung

Solaris Zonen haben in Solaris 11 Verbesserungen erfahren, welche den Administrations- und Management-Cycle vereinfacht und die Sicherheit erhöhen. Solaris 10 Systeme können einfach auf Solaris 11 in Zonen migriert werden und die Verschiebung von Zonen zwischen Rechnern wird verbessert und vereinfacht und kann fast immer rückgängig gemacht werden. Über die Möglichkeiten der Solaris 11 Netzwerk-Virtualisierung wird der automatische Aufbau auch komplexer Architekturen und die Konsolidierung mit Zonen stark vereinfacht.

Kontaktadresse:
Ulrich Gräf
Oracle Deutschland B.V. & Co. KG
Robert-Bosch Str. 5
D-63303 Dreieich

Telefon: +49 (0) 6103 397 390
E-Mail ulrich.graef@oracle.de
Internet: http://blogs.oracle.com/solarium http://blogs.oracle.com/blug