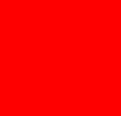
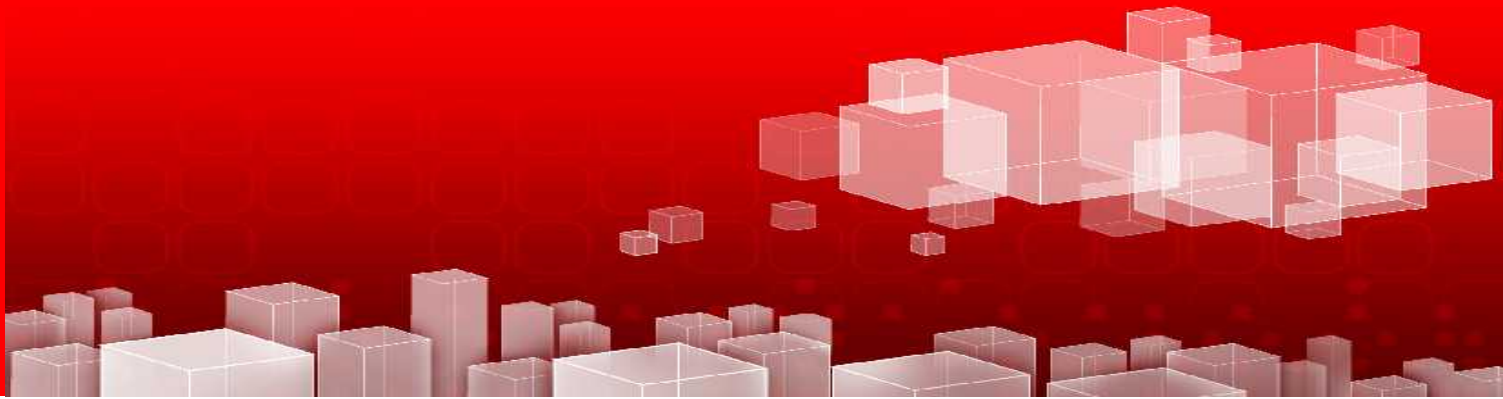


**ORACLE®**



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.



**ORACLE®**

## **Solaris Zones in Oracle Solaris 11**

**Detlef Drewanz**

Principal Sales Consultant, EMEA Server Presales

# Oracle Solaris 11



- Für Clouds
- Das Beste für Enterprise Anwendungen
- Engineered für Oracle

# SPARC Server Ausblick

Maximizing Results

**DELIVERED**

**T-Series**  
1-4 Socket  
+ 2x Throughput

**M-Series**  
1-64 Socket  
+ 20%

**T-Series**  
1-4 Sockets  
+1x Throughput  
+5x Single Strand

**In Test**  
**M-Series**  
16-64 Sockets  
+6x Throughput  
+1.5x Single Strand

**In Test**  
**T-Series**  
1-8 Sockets  
+2.5x Throughput  
>1x Single Strand

**M-Series**  
16-64 Sockets  
+2x Throughput  
>1x Single Strand

**T-Series**  
1-8 Sockets  
+20%

**SPARC**  
1-64 Sockets  
+2x Throughput  
+1.5x Single Strand

## 5 Year Trajectory

Cores	4x
Threads	32x
Memory Capacity	16x
Database TPM	40x
Java Ops Per Second	10x

2010

2011

2012

2013

2014

2015

Solaris 11 Express  
Software Lifecycle  
Scalability  
Networking

Solaris 11  
Software Lifecycle  
Scalability,  
Networking  
Security

Solaris 11 Update  
High-Availability  
Memory Scalability  
Virtualization

Solaris 11 Update  
System Management  
IO Scalability

Solaris 11 Update  
Core Scalability

ORACLE

# Besuchen Sie einen unserer Solaris TechDays und lernen Sie mehr über die neuste Version 11 von Oracle Solaris.



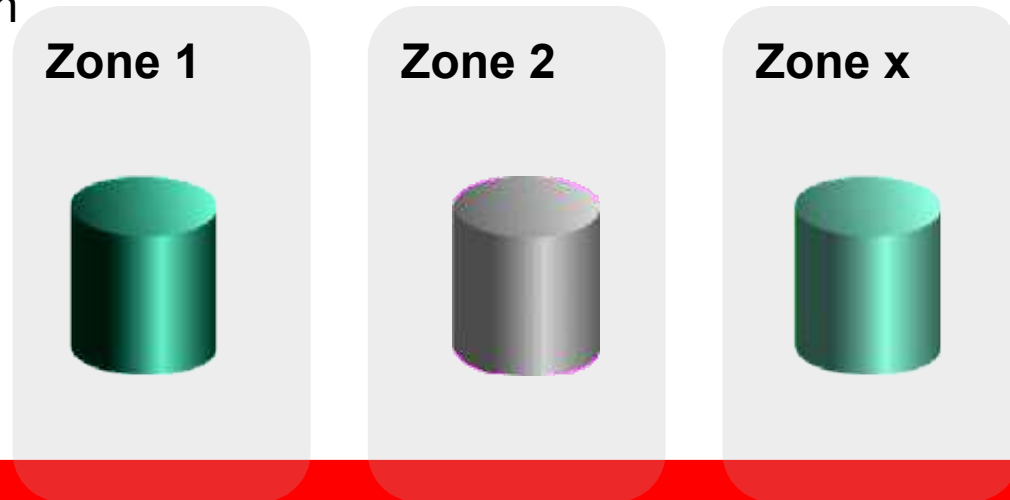
- Düsseldorf 6.2.2012
- Stuttgart 8.2.2012
- Hamburg 9.2.2012
- Potsdam 10.2.2012
- Frankfurt 13.2.2012
- München 14.2.2012

# Oracle Solaris 11: Systemanforderungen

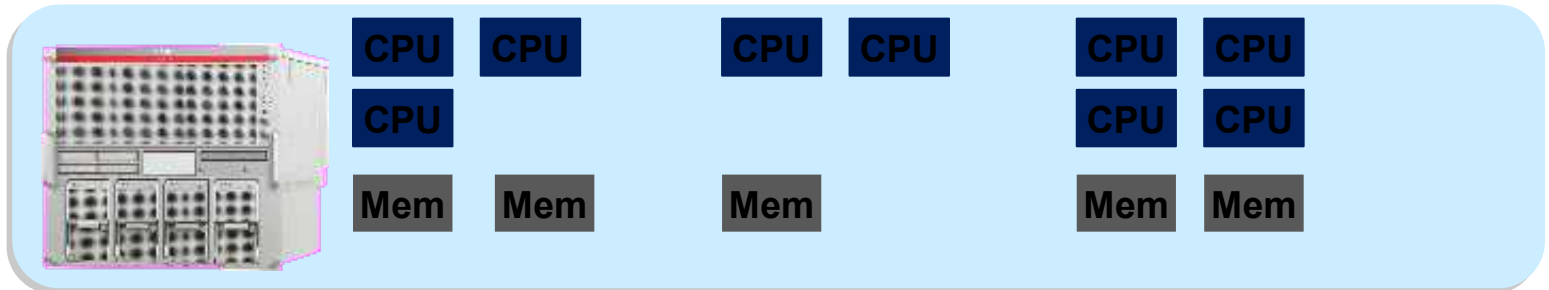
- SPARC
  - Alle T-Serie und M-Serie Systems
- X86 (64bit)
  - <http://www.oracle.com/webfolder/technetwork/hcl/index.html>
- Min. 1 GB Speicher (besser 1.5 GB)
- Plattenplatz
  - Live Media: 5GB (7GB empfohlen)
  - Text Installer: 2.5GB (4.5GB empfohlen)
  - Automated Installer: 2.5GB (13GB empfohlen)

# Oracle Solaris Zones (aka Containers)

- One OS for all zones
- Separate file systems
- Complete software isolation
- Sub-thread granularity
- Dynamic and mobile
- Low overhead
- No cost to end user



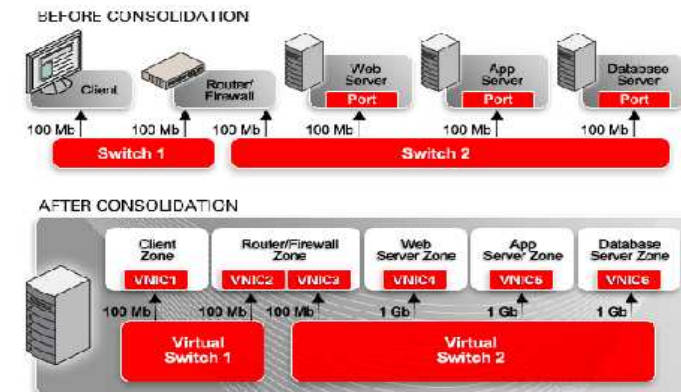
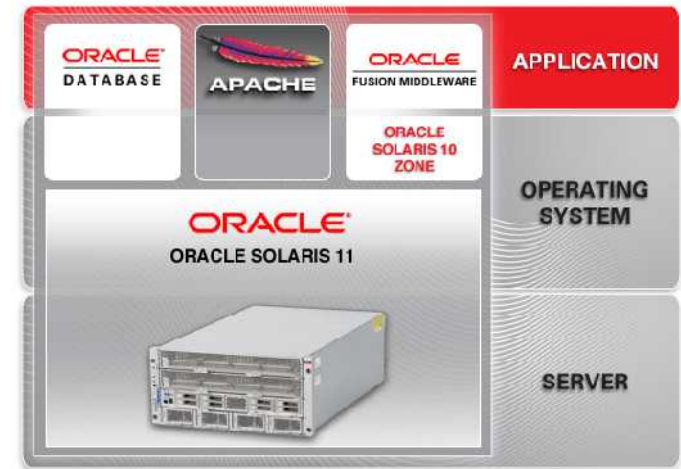
**Solaris**





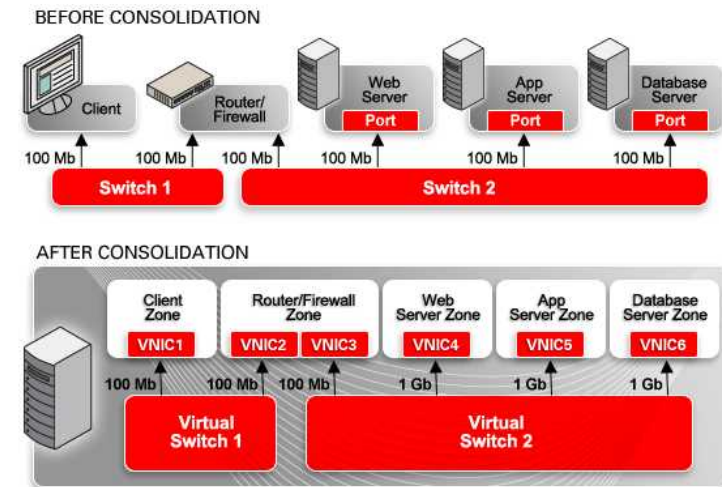
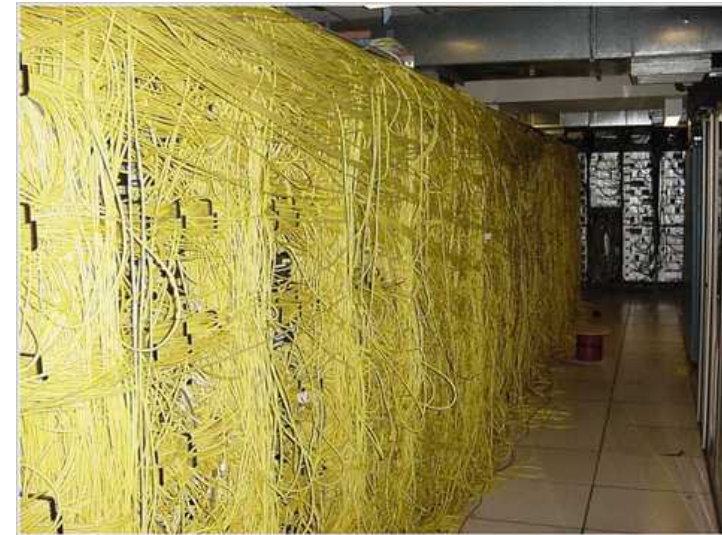
# Oracle Solaris Zones und Netzwerk Virtualisierung

- OS Virtualisierung integriert
  - Native Performance
  - Unabhängig von der Hardware
  - Secure, Rapid Application Deployment
  - Als Hard Partitions nutzbar
- Integrierte Netzwerk Virtualisierung
  - Simulation von Produktionsumgebungen
  - Virtuelle Adapter
  - Virtuelle Switches
- Netzwerk Ressourcenkontrolle
- Die Standard-Umgebung für Anwendungen



# Netzwerk Virtualisierung

- Simulation von Produktionsumgebungen
  - Netzwerk Equipment in Software
  - Weniger Risiko durch mehr Tests
  - Einfache und schnelle Tests unterschiedlicher Umgebungen
- Schnelle produktive Umsetzung
  - Genauere Bestimmung der Produktionsanforderungen



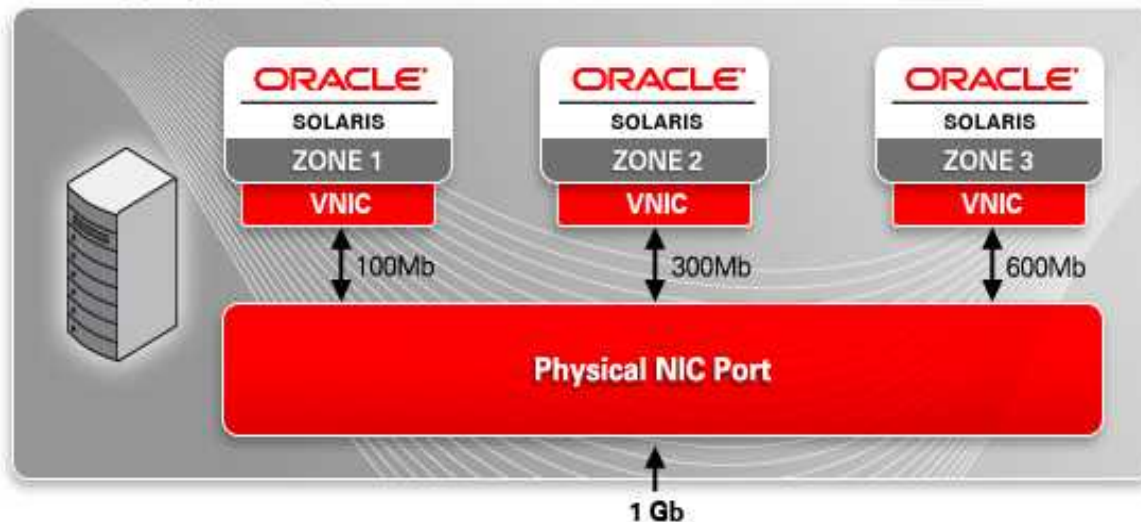
# Netzwerk-Virtualisierung

## Überblick

- VNIC
  - Netzwerk-Virtualisierung mit VNIC auf PNIC
- Etherstub
  - Software-basierte Netzwerkswitches und Bridges
- Flows
  - Klassifikation von Netzverkehr
- Bandbreitenzuweisung
  - Zu VNIC und Flows
- Aktuelle und Aufzeichnung von Statistiken
  - Für VNIC und Flows
- Ein Managementinterface

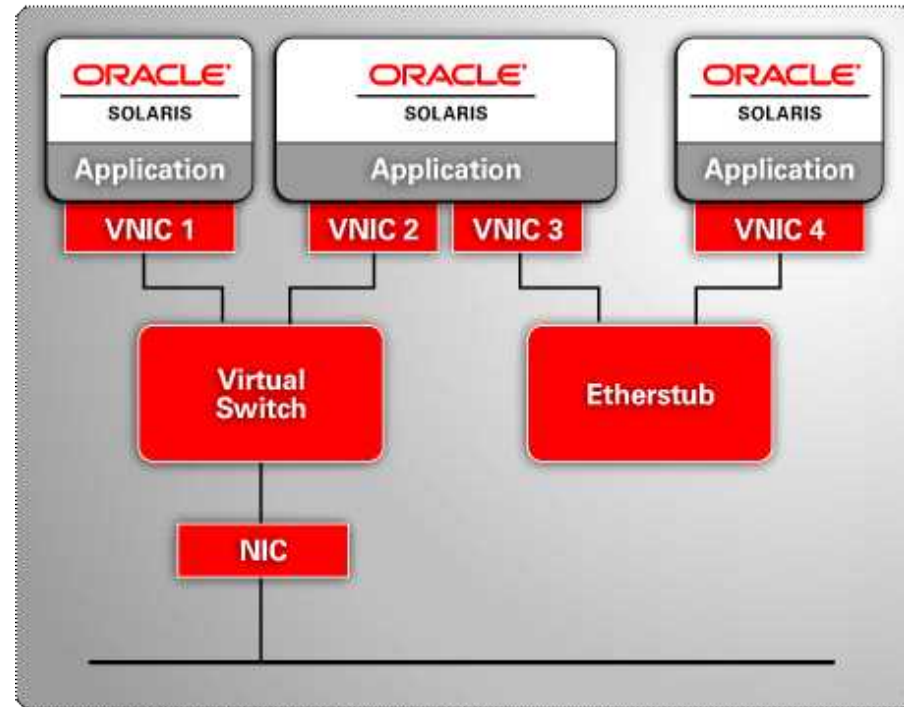
# VNIC

- Virtual network interfaces, vnics
  - Virtuelles Interface auf einem phys. Interface oder Etherstub
  - Eigene MAC Adresse
  - Lokaler Switch bei mehreren VNIC auf einem Interface
  - Ermöglicht viele Zonen mit exclusive-IP Instanzen



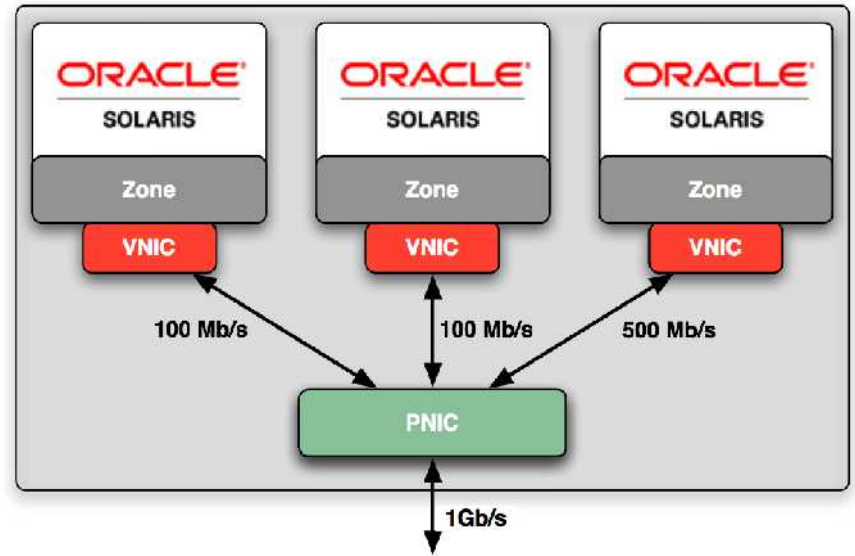
# VNIC und Etherstub

- Interne Netzwerke, Etherstub
  - Virtueller Ankerpunkt für VNIC
  - Für Datacenter-in-a-box
  - Verschiedene Layer einer Architektur in verschiedenen Zonen abbilden

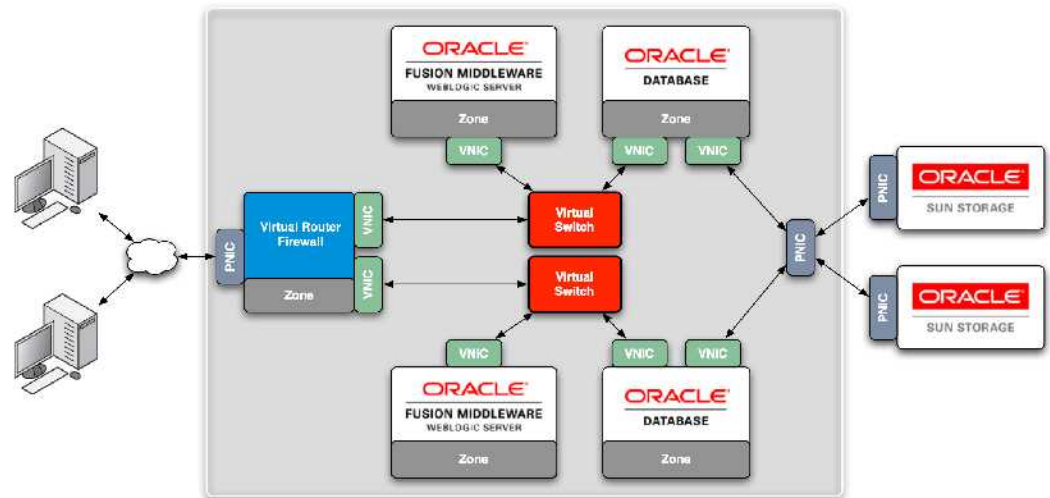
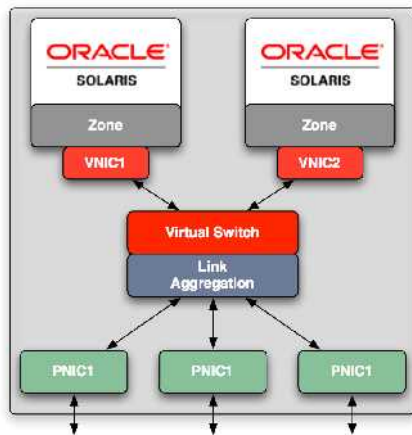


# Virtual Networking

- Network Traffic Limits ---



- Arbitrary networks:



# Flows

- Ressourcen Management
  - Bandbreite für NIC/VNIC
    - `dladm set-linkprop maxbw=50M net0`
  - Bandbreite für Flows
    - `flowadm add-flow -l net0 -a transport=tcp,local_port=80 http`
    - `flowadm set-flowprop -p maxbw=500M http`
    - `flowadm show-flowprop http`

# Zonen: Terminologie

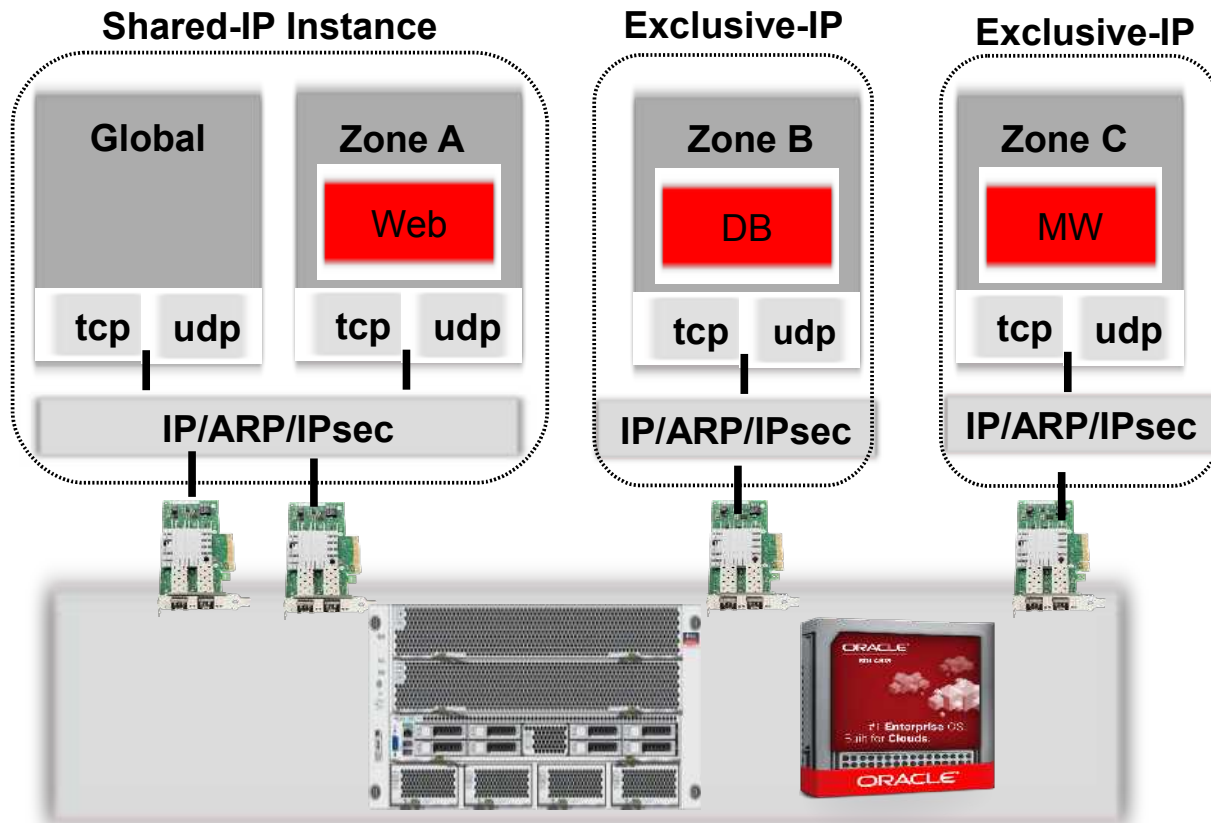
- Global Zone
  - Direkt auf der Hardware oder der VM installiert
  - Genau eine GZ je Installation
- Non-global Zone
  - Virtualisierte Umgebung
  - Mehrere NGZ teilen sich je eine GZ
- Branded Zone
  - Eine Zone bildet eine andere OS-Umgebung ab, als die dazugehörige GZ
- Solaris 10 Zone
  - Eine Branded Zone für Solaris 10 in Solaris 11
- Solaris Legacy Container
  - Eine Branded Zone für Solaris 8 oder Solaris 9 in Solaris 10



# Zonen in Solaris 11

- ZFS compressed Dataset als root Filesystem
- Genau ein Type Solaris 11 Zonen: solaris
  - Ohne Unterscheidung nach Whole root und Sparse root
- Installation und Minimierung durch Group Packages
  - Default: pkg:/group/solaris-small-server
- Automatische und interaktive Installation
  - Siehe: `/usr/share/auto_install/manifest/zone_default.xml`
- Boot Umgebungen in Zonen
- Gemeinsames Update aller Zonen
  - pkg update
- NFS Server in der Solaris 11 Zone nutzbar

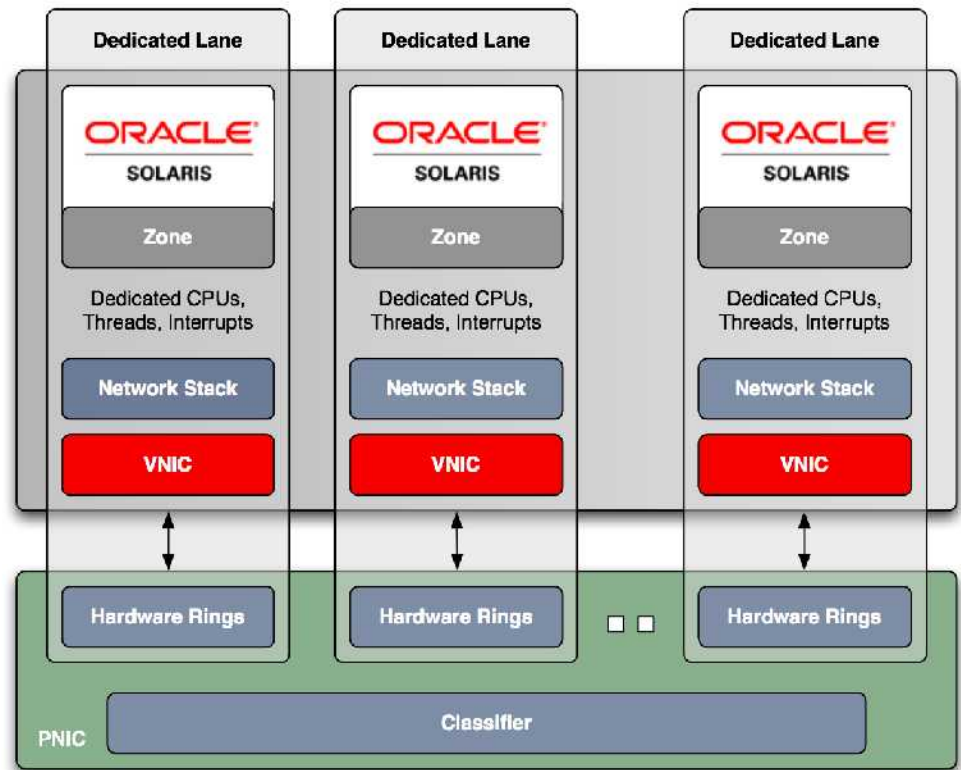
# Shared-IP vs. Exclusive IP-Instances



# Virtual Networking

- Virtual Network Interfaces (vnic)

- On physical interfaces
- Or with virtual switches
- Interfaces for Zones with exclusive-ip
- And:
  - Bridging
  - IPMP
  - Firewalling
  - Load Balancer
  - Private Networks

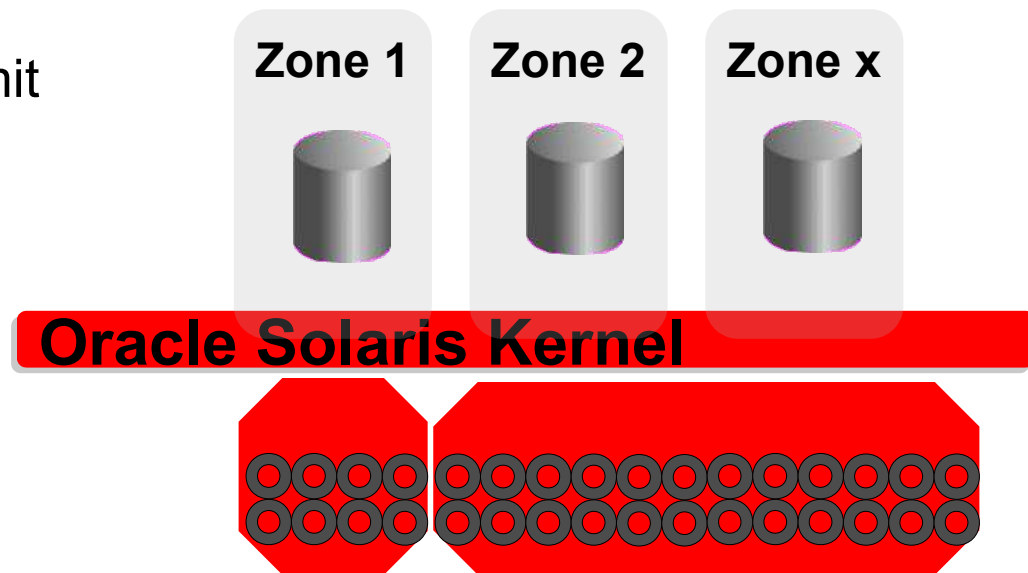


# Netzwerke und Oracle Solaris Zonen

- Ein oder mehrere automatische VNIC per Zone (anet)
  - Automatisch beim Boot erzeugt und einer Zone zugeordnet
  - net0, net1, ... als Namen
- Exclusive-IP Stack ist Default
  - Zur Begrenzung von Adressen
    - zonecfg allowed-address/mac-address
  - Bandbreitensteuerung
    - zonecfg maxbw/priority
  - IPMP auf VNICs in der Zone konfigurieren
- Shared-IP Stack konfigurierbar

# Ressource management

- Balance
  - Faire Share Ressources through rules
  - Assigned based on shares in the event of 100% utilization (no limit below 100%)
- Capping
  - Cap ressources on a limit
- Partitioning
  - Assign and use ressources exclusively



# Ressource management with zones (keep SLAs!)

- CPU
  - CPU Fair Shares
  - CPU Capping
  - CPU Partitioning
- Memory
  - Used phys memory (RSS)
  - Virtual memory (= Swap)
  - Non-Pageable Memory (Locked)
  - Shared Memory, Semaphores
- Processes
  - LWP's
  - Processes (new with S11)
- Networking (new with S11)

zone.max-swap					
system	16.0EB	max	deny	-	
zone.max-locked-memory					
system	16.0EB	max	deny	-	
zone.max-shm-memory					
system	16.0EB	max	deny	-	
zone.max-shm-ids					
system	16.8M	max	deny	-	
zone.max-sem-ids					
system	16.8M	max	deny	-	
zone.max-msg-ids					
system	16.8M	max	deny	-	
zone.max-lwps					
system	2.15G	max	deny	-	
zone.cpu-cap					
system	4.29G	inf	deny	-	
zone.cpu-shares					
privileged	1	-	none	-	
system	65.5K	max	none	-	

# Resource Management

- New max-processes resource control

```
example# zonecfg -z myzone
zonecfg:myzone> set max-processes=300
```

- prctl(1) now shows resource utilization:

```
example# prctl -i zone foo
zone: 4: foo
NAME      PRIVILEGE          VALUE      FLAG      ACTION
zone.max-lofi
          usage              0
          system          18.4E      max      deny
zone.max-swap
          usage            28.3MB
          privileged    3.00GB     -        deny
          system          16.0EB     max      deny
```

# Security und Zonen

- Immutable Zones
  - Root-Filesystem der Zone teilweise oder vollständig readonly
  - zonecfg set file-mac-profile =
    - none:
    - strict: gesamtes Filesystem readonly, logging remote
    - fixed-configuration: /var schreibbar (ohne configs)
    - Flexible-configuration: /var und /etc schreibbar
- Administrationsrechten von bestimmten Nutzern der Globalen Zone für bestimmte Zonen
  - zonecfg add admin
    - set user
    - set auths



# Zones Security Enhancements

- Delegated administration (via RBAC authorizations)
- Authorizations can be configured directly in zonecfg(1m):

```
example# zonecfg -z myzone
zonecfg:myzone> add admin
zonecfg:myzone:admin> set user=jack
zonecfg:myzone:admin> set auths=login,manage
zonecfg:myzone:admin> end
zonecfg:myzone> commit
```

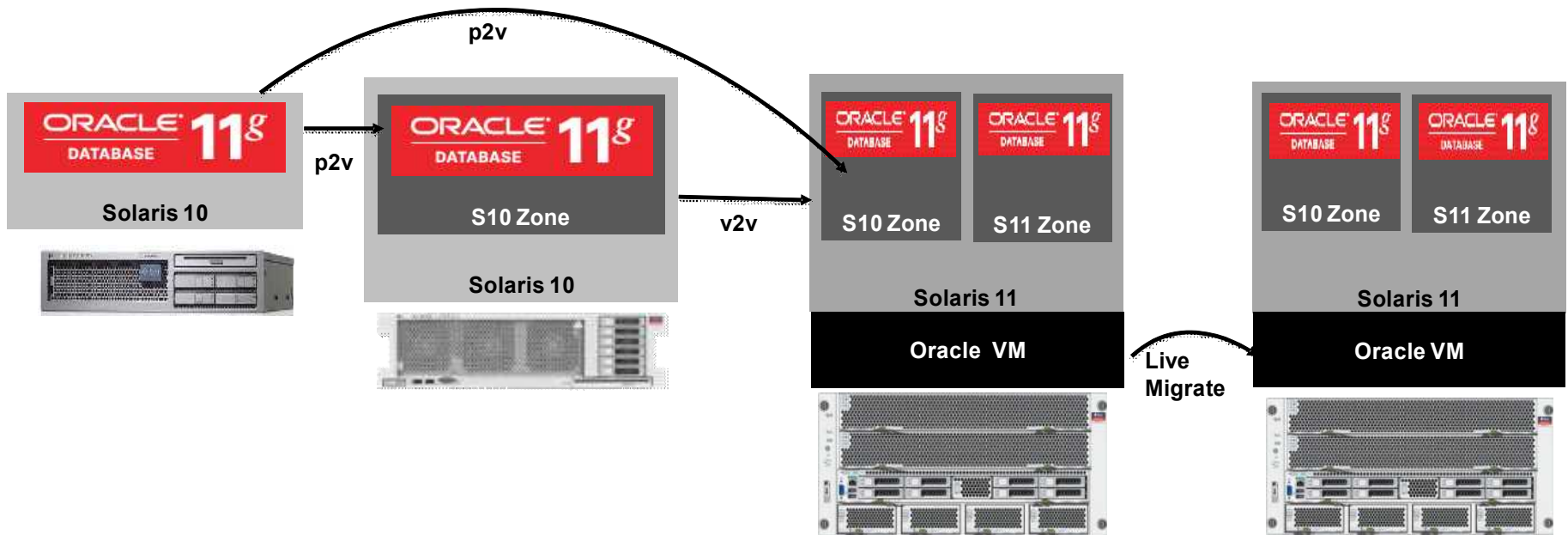
- Authorizations are implemented via `/etc/user_attr` and synced there by zonecfg.

# Solaris 10 Zonen

- Feature von Solaris 11
- Nutzung von VNICs möglich
- Kein NFS-Server Feature in Solaris 10 Zonen
- v2v
  - Solaris 10 Zone von Solaris 10 nach Solaris 11 verlagern
- p2v
  - Solaris 10 System in eine Solaris 10 Zone verlagern
  - Zonen vorher mit v2v separat verlagern
- Solaris 10 10/09 oder neuer
- Keine Solaris 8 oder Solaris 9 Zonen

# Sicherer Pfad für Upgrades

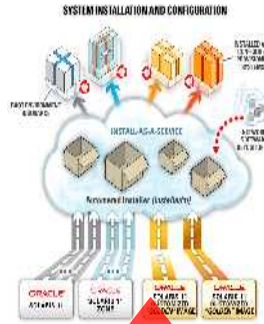
- Upgrades von Oracle Solaris 10
  - Pre-flight Checker verfügbar
- Live Migration mit OVM SPARC und OVM x86



# Integrierte Virtualisierung

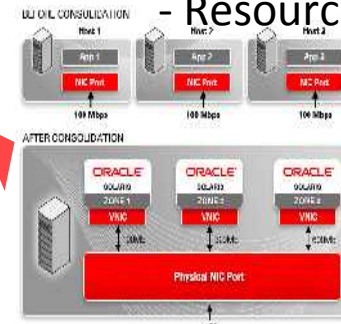
## Provisioning

- Automated Installer
- Distro Constructor



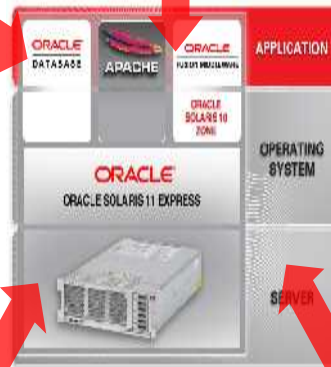
## Netzwerk Virtualisierung

- Network in a Box
- Bandwidth Control
- Resource Management



## Security

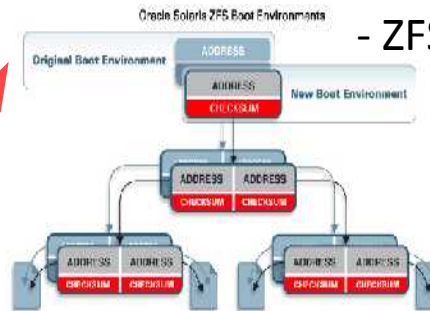
- Immutable Zones
- Delegation



## Zones

## Data Management

- ZFS



## Software Management

- IPS
- Repositories
- Boot Environments



# Zones for Solaris 11: Summary

- Rationalized installation, system configuration, update
  - One default zones model
- NFS server in a Zone, lofi improved
- Networking
  - Exclusive Stack now the default
  - Automatic networking
  - Network resource management in the zones config
- Immutable Zones
- Delegated Administration
- Solaris 10 Zones

**ORACLE®**