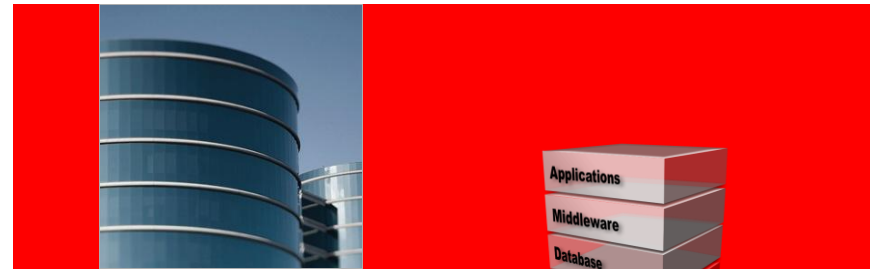


ORACLE®



ORACLE®

## Hardening the Infrastructure

Luc Wijns  
Chief Technologist Systems Benelux, CISSP





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.

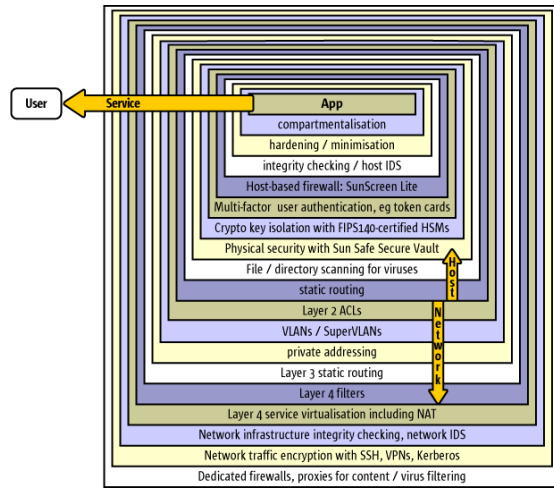


## Agenda

- Defense in Depth – Architecture
- Technologies Available
- Solaris 10+ - Security
- Solaris 10+ - Zones
- ORACLE Database in Zones – Secure Deployment
- Q&A



## Layers of Security: Defense in Depth



ORACLE

© 2011 Oracle Corporation

5

## Agenda

- Defense in Depth – Architecture
- Technologies Available
- Solaris 10+ - Security
- Solaris 10+ - Zones
- ORACLE Database in Zones – Secure Deployment
- Q&A

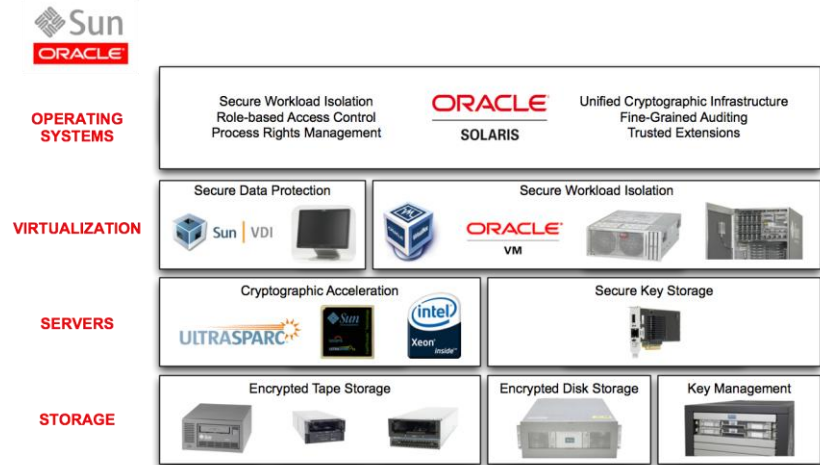


ORACLE

© 2011 Oracle Corporation

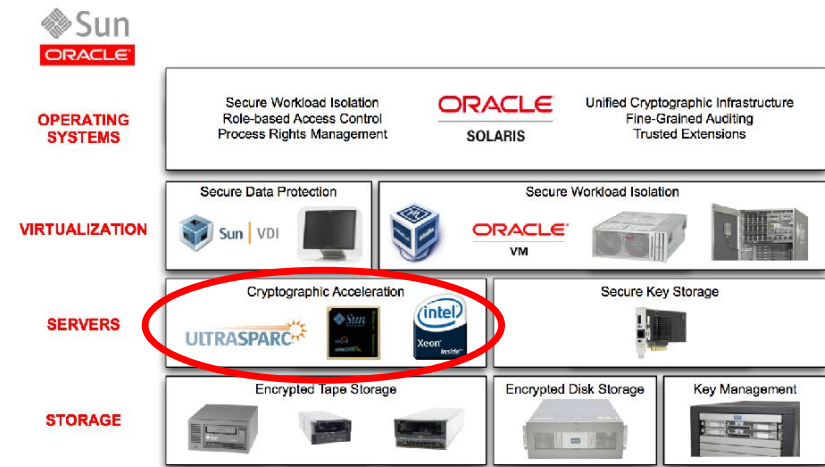
6

## Infrastructure Security Foundation



ORACLE

## Infrastructure and Cryptography



ORACLE

# Infrastructure and Cryptography



**OPERATING SYSTEMS**

Secure Workload Isolation Role-based Access Control Process Rights Management	<b>ORACLE</b> SOLARIS	Unified Cryptographic Infrastructure Fine-Grained Auditing Trusted Extensions
---	--------------------------	---

**VIRTUALIZATION**

Secure Data Protection Sun   VDI	Secure Workload Isolation <b>ORACLE</b> VM	
-------------------------------------	--	--

**SERVERS**

Cryptographic Acceleration ULTRASPARC	Secure Key Storage
--	--------------------

**STORAGE**

Encrypted Tape Storage	Encrypted Disk Storage	Key Management
------------------------	------------------------	----------------

**ORACLE**

# Infrastructure and Cryptography



**OPERATING SYSTEMS**

Secure Workload Isolation Role-based Access Control Process Rights Management	<b>ORACLE</b> SOLARIS	Unified Cryptographic Infrastructure Fine-Grained Auditing Trusted Extensions
---	--------------------------	---

**VIRTUALIZATION**

Secure Data Protection Sun   VDI	Secure Workload Isolation <b>ORACLE</b> VM	
-------------------------------------	--	--

**SERVERS**

Cryptographic Acceleration ULTRASPARC	Secure Key Storage
--	--------------------

**STORAGE**

Encrypted Tape Storage	Encrypted Disk Storage	Key Management
------------------------	------------------------	----------------

**ORACLE**

# Infrastructure and Cryptography



**OPERATING SYSTEMS**

Secure Workload Isolation Role-based Access Control Process Rights Management	<b>ORACLE</b> SOLARIS	Unified Cryptographic Infrastructure Fine-Grained Auditing Trusted Extensions
---	--------------------------	---

**VIRTUALIZATION**

Secure Data Protection Sun   VDI	Secure Workload Isolation <b>ORACLE</b> VM	
-------------------------------------	--	--

**SERVERS**

Cryptographic Acceleration ULTRASPARC	Secure Key Storage intel Xeon
--	----------------------------------

**STORAGE**

Encrypted Tape Storage	Encrypted Disk Storage	Key Management
------------------------	------------------------	----------------

**ORACLE**

# Infrastructure and Cryptography



**OPERATING SYSTEMS**

Secure Workload Isolation Role-based Access Control Process Rights Management	<b>ORACLE</b> SOLARIS	Unified Cryptographic Infrastructure Fine-Grained Auditing Trusted Extensions
---	--------------------------	---

**VIRTUALIZATION**

Secure Data Protection Sun   VDI	Secure Workload Isolation <b>ORACLE</b> VM	
-------------------------------------	--	--

**SERVERS**

Cryptographic Acceleration ULTRASPARC	Secure Key Storage intel Xeon
--	----------------------------------

**STORAGE**

Encrypted Tape Storage	Encrypted Disk Storage	Key Management
------------------------	------------------------	----------------

**ORACLE**

## Multi-Tenancy - Solaris Virtualization Security



## Solaris 10+ Security

**ORACLE**

**SOLARIS**

- Secure Service Containers: Solaris Zones
- Digital Certificates Everywhere
- IP Filter firewall, TCP Wrapper
- Solaris Security Toolkit (JASS)
- Secure Network Install & Minimal Packaging
- Secure Execution (non-executable stack)
- User Rights and Process Rights Management
- Cryptographic infrastructure
- Secure by Default networking
- Solaris Trusted Extensions
- Common Criteria Certification
  - EAL4+
  - Labeled Security, Controlled Access, Role-Based Access Control protection profiles
- BART: Basic Audit and Reporting Tool
- Fingerprint Database
- Etc ...

## Solaris Secure By Default & Minimal Install

- Minimal install: limited set of packages
- Only Secure Shell is reachable by default.
  - root use of Secure Shell is not permitted by default.
- Existing services are configured in SMF to either be:
  - Disabled by default
  - Listening for local (e.g., loopback) connections only
- Configuration can be selected using CLI or JumpStart:
  - netservices: open (traditional) or limited (SBD)
  - service\_profile: open or limited\_net
- Default installation method in Solaris 11:
  - Solaris upgrades are not changed or impacted.
  - Solaris 10 initial (fresh) installations can select SBD mode.

ORACLE

## User Rights Management

**User Rights Management** allows you to distribute rights to management “roles” with finer granularity. Users can then assume these roles.



**Decomposes super user role**



**Roles stored in naming service for centralization**



**Auditing records 'real' user – no anonymous admin!**

ORACLE

## Reduce Application Privileges

**Process Rights Management** allows you to distribute rights among applications with finer granularity:

- ✓ Eliminates need to run applications as super user
- ✓ Reduces customer exposure to security attacks
- ✓ Compatible with existing applications
- ✓ Always turned on

ORACLE

© 2011 Oracle Corporation

18

## Agenda

- Defense in Depth – Architecture
- Technologies Available
- Solaris 10+ - Security
- **Solaris 10+ - Zones**
- ORACLE Database in Zones – Secure Deployment
- Q&A



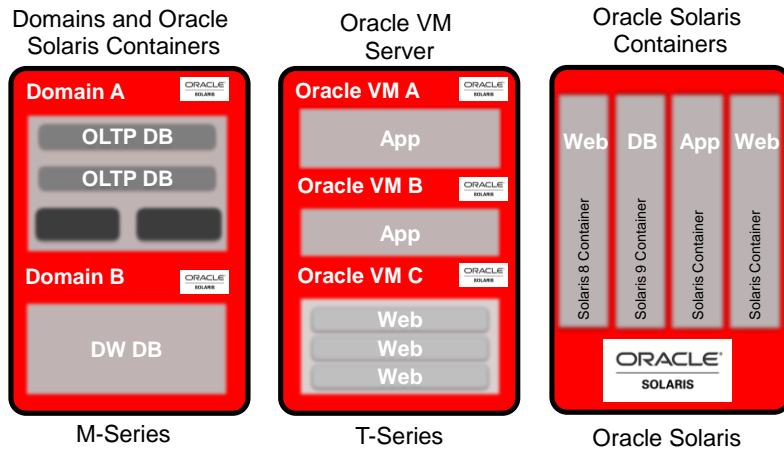
ORACLE

© 2011 Oracle Corporation

19

## Solaris and SPARC Isolation through Virtualization

Better Resource Utilization for a More Efficient Datacenter

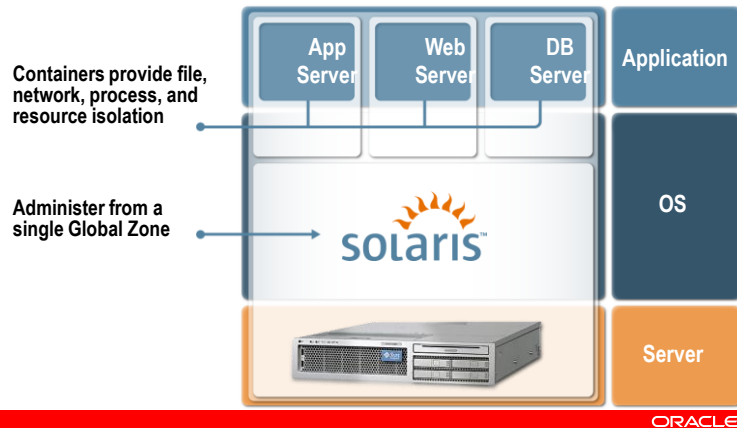


## Solaris Zones

- Zones are virtualized application environments.
  - No direct access to hardware.
- Zones have security boundaries around them.
  - Zones have their own: root directory, naming service configuration, process containment, resource controls, devices, etc.
- Zones communicate via network only (default).
  - shared vs. exclusive IP
- Zones operate with fewer privileges (default).
  - some privileges can be added or removed
  - Root in a zone has less privileges

## Container Security – Solaris Zones

Reduce risk by isolating applications in separate containers – yet administer centrally



## Why Run Services in Zones?

- Restricted Operations for Enhanced Security
  - Individual Solaris OS hardening and RBAC configurations
  - Prohibited from directly accessing the kernel or raw memory
  - Prohibited from manipulating kernel modules
  - Prohibited from manipulating network interfaces (shared IP only)
- Enforcement with Integrity
  - Configurable privileges, sparse root zones, IP Instances, IP Filter
- Resource Control and Management
  - CPU, Memory, Disk, Networking, Devices, etc.
- Observability with Integrity
  - BART, Solaris Auditing, etc.

## Zones are Less Privileged

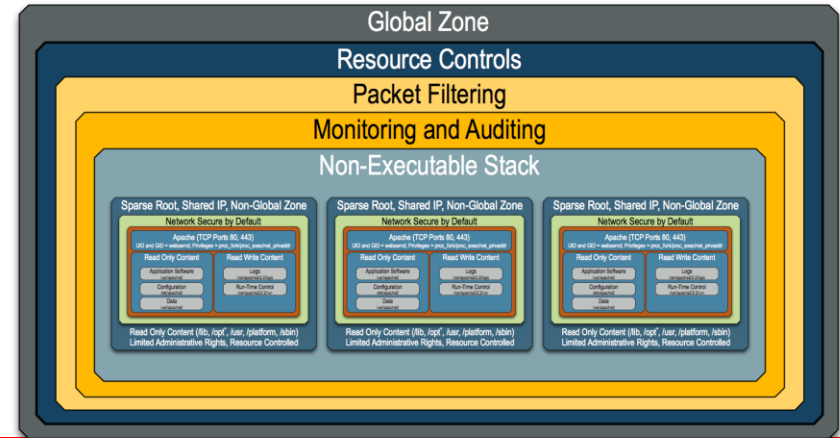
"cpc_cpu"	Access to per-CPU perf counters	"proc_lock_memory"	Lock pages in physical memory
"dtrace_kernel"	DTrace kernel tracing	"proc_owner"	See/modify other process states
"dtrace_proc"	DTrace process-level tracing	"proc_prioctl"	Increase priority/sched class
"dtrace_user"	DTrace user-level tracing	"proc_session"	Signal/trace other session process
"file_chown"	Change file's owner/group IDs	"proc_setid"	Set process UID
"file_chown_self"	Give away (chown) files	"proc_taskid"	Assign new task ID
"file_dac_execute"	Override file's execute perms	"proc_zone"	Signal/trace processes in other zones
"file_dac_read"	Override file's read perms	"sys_acct"	Manage accounting system (acct)
"file_dac_search"	Override dir's search perms	"sys_admin"	System admin tasks (node/domain name)
"file_dac_write"	Override (non-root) file's write perms	"sys_audit"	Control audit system
"file_link_any"	Create hard links to diff uid files	"sys_config"	Manage swap
"file_owner"	Non-owner can do misc owner ops	"sys_devices"	Override device restricts (exclusive)
"file_setidac"	Non-owner can set file perms (no seuid)	"sys_ipc_config"	Increase IPC queue
"file_setid"	Set uid/gid (non-root) to diff id	"sys_linkdir"	Link/unlink directories
"ipc_dac_read"	Override read on IPC, Shared Mem perms	"sys_mount"	Filesystem admin (mount,quota)
"ipc_dac_write"	Override write on IPC, Shared Mem perms	"sys_net_config"	Config net interfaces,routes,stack
"ipc_owner"	Override set perms/owner on IPC	"sys_nfs"	Bind NFS ports and use syscalls
"net_icmpaccess"	Send/Receive ICMP packets	"sys_res_config"	Admin processor sets, res pools
"net_privaddr"	Bind to privilege port (<1023+extras)	"sys_resource"	Modify res limits (rlimit)
"net_rawaccess"	Raw access to IP	"sys_suser_compat"	3rd party modules use of suser
"proc_audit"	Generate audit records	"sys_time"	Change system time
"proc_chroot"	Change root (chroot)		
"proc_clock_highres"	Allow use of hi-res timers		
"proc_exec"	Allow use of execve()		
"proc_fork"	Allow use of fork() calls		
"proc_info"	Examine /proc of other processes		

Interesting  
Basic  
Removed

Some interesting privileges  
Non-root privileges  
Not available in Zones

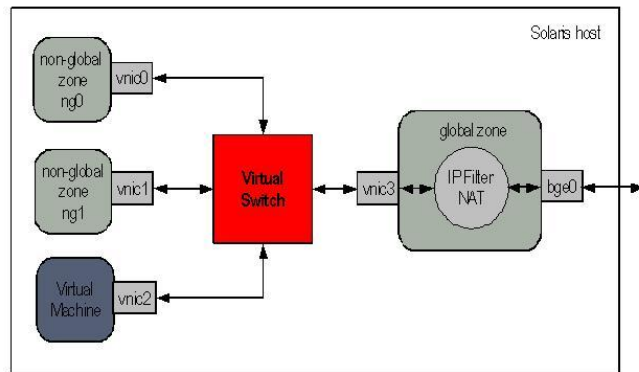
ORACLE

## Multi-Tenant Infrastructure



ORACLE

## Solaris 11 – Host Network Virtualization



ORACLE

© 2011 Oracle Corporation

26

## Agenda

- Defense in Depth – Architecture
- Technologies Available
- Solaris 10+ - Security
- Solaris 10+ - Zones
- **ORACLE Database in Zones – Secure Deployment**
- Q&A



ORACLE

© 2011 Oracle Corporation

27

## The Approach (1/3):

- Zones
  - Encapsulate database in own environment
  - Zone configuration and resources are controlled from “outside”
- Zones Networking inclusive IPF/IPNAT
  - Enforce network traffic
    - Block/Filter Traffic
    - Map external to/from internal traffic
  - Control network traffic
  - Log/Monitor network traffic
- ZFS with Zones
  - Filesystems will be controlled from “outside”
  - Selective read/execute rights per filesystem (dataset)
  - The use of snapshots enables evidence and fast “return”

ORACLE

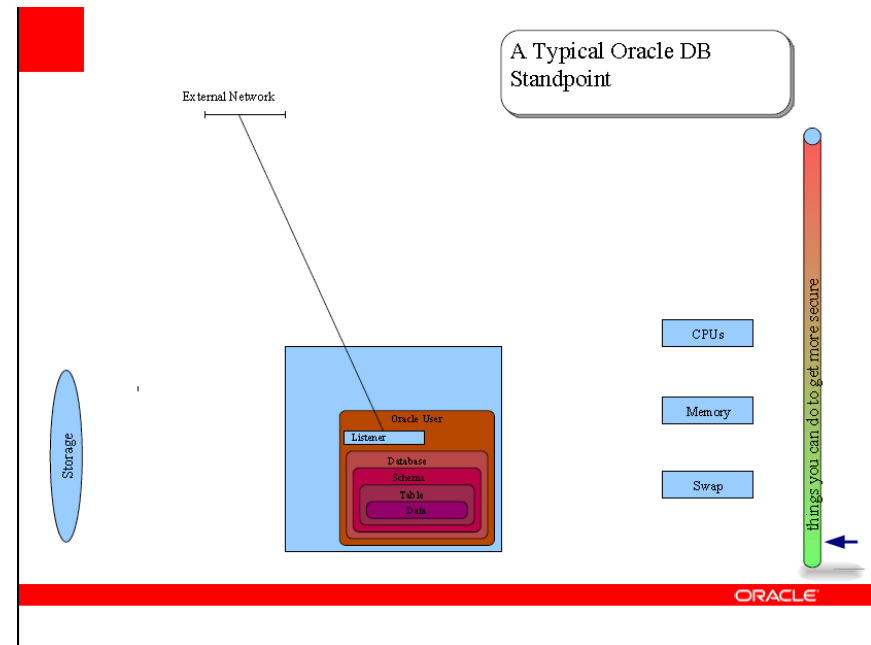
## The Approach (2/3):

- RBAC (role base access control)
  - No root user
  - No oracle user
  - User rights and execute control
  - Enforce correct login
- BSM (base security module, aka OS Audit)
  - Create audit trail
  - Enforces that audit will be written
  - Store access- and execute-path
- BART (basic audit and reporting tool)
  - Double-check OS Installation with Solaris fingerprint database
  - Searches for changes on files and directories
- Zones
  - Encapsulate database in own environment
  - Zone configuration and resources are controlled from “outside”

ORACLE

### The Approach (3/3):

- Projects and Resource-Controls
  - Limited access or usage of Memory/Swap/CPU
- PRM (process right management)
  - Reduces Privileges for processes/users/executable
- SMF (service management facility)
  - Central switchboard for services
  - Access to the switchboard might be granted/restricted
- Dtrace: Observability in the Global Zone
- Others
  - CryptoFramework, Kerberos, IPsec, TrustedExtensions, signed patches, ssh, /dev/random, pam, smartcard framework, java security, ldap connections.....

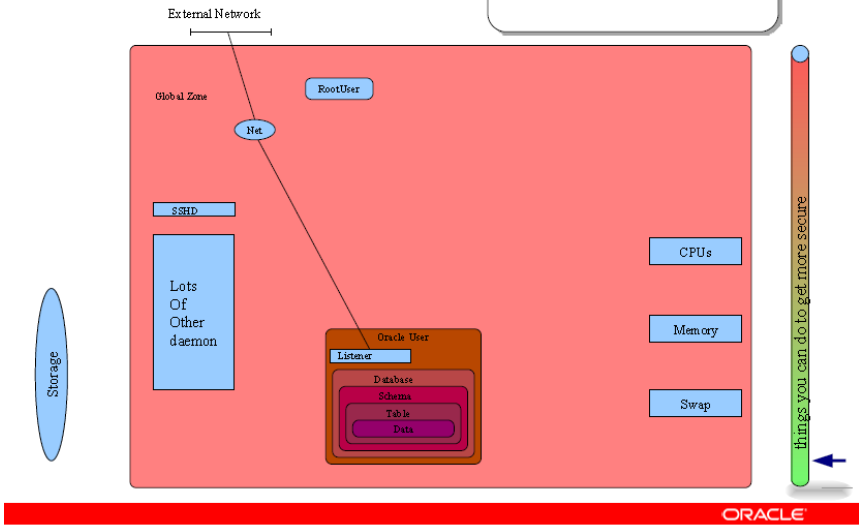


ORACLE

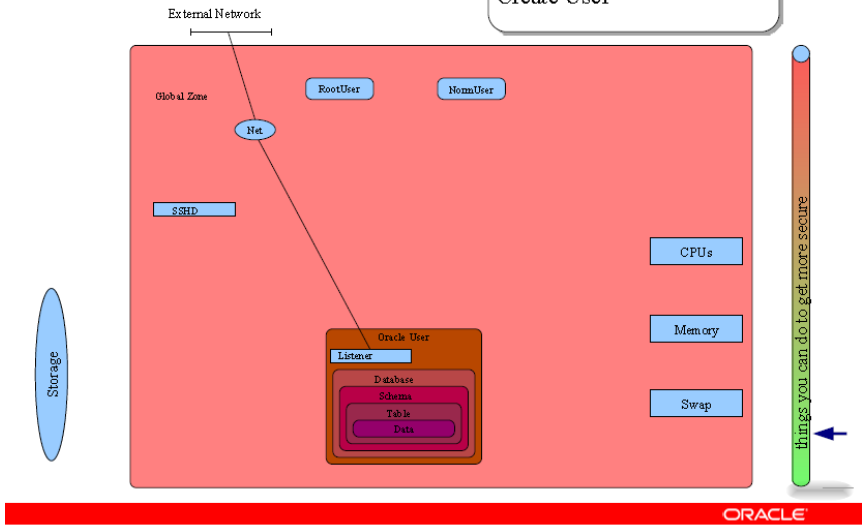
ORACLE



### A Bit More Detailed

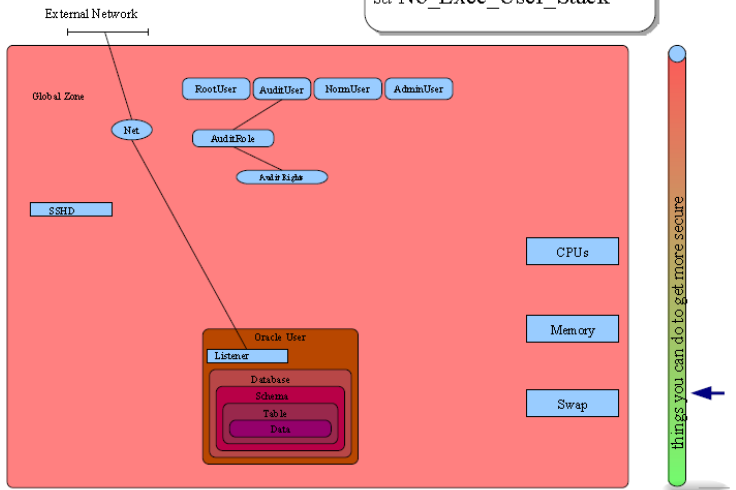


### Netservices „limited“ Create User





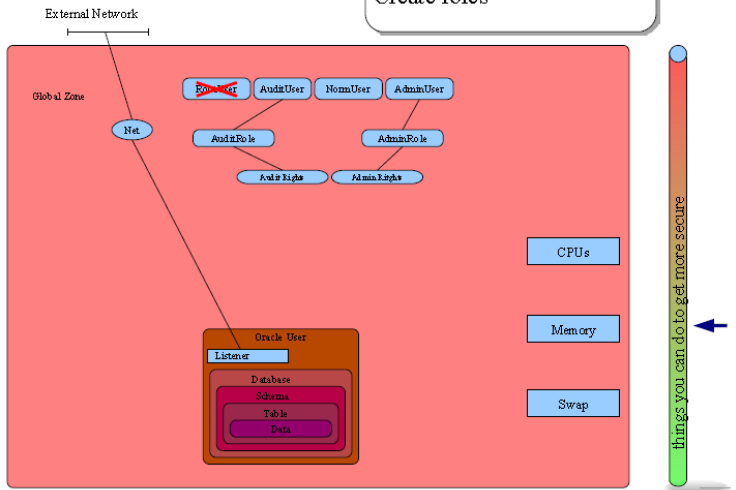
Configure Audit  
set No\_Exec\_User\_Stack



ORACLE



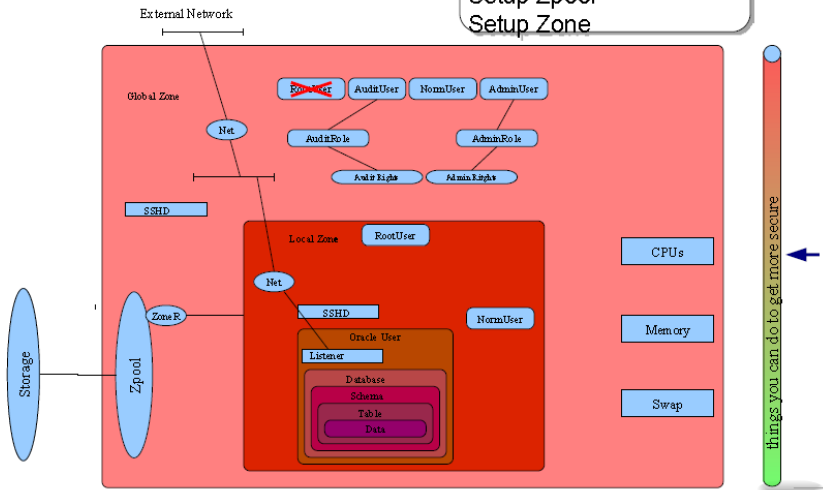
Reconfig root  
Create roles



ORACLE



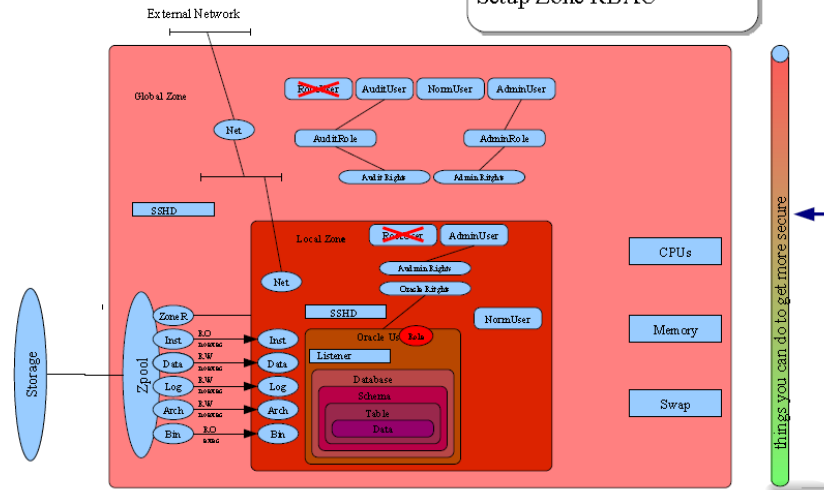
Setup int Net  
Setup Zpool  
Setup Zone



ORACLE



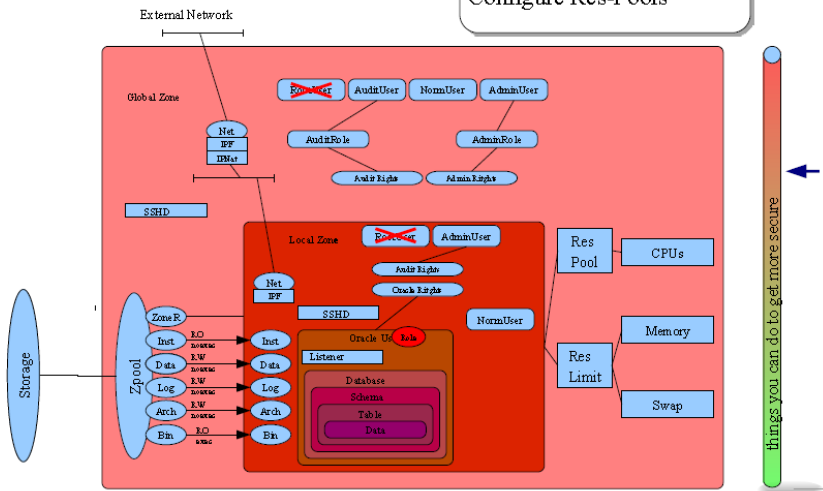
Create Datasets  
Setup Zone RBAC



ORACLE



Configure IPF/IPNAT  
Configure Res-Pools

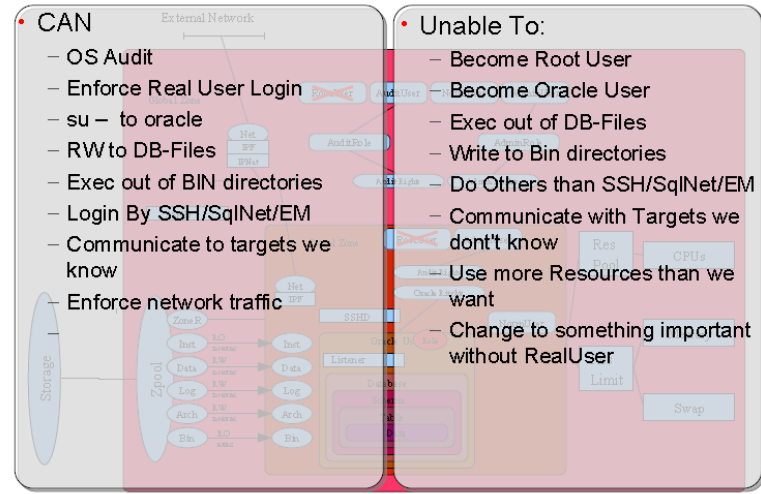


things you can do to get more secure

ORACLE



### Can / Can Not



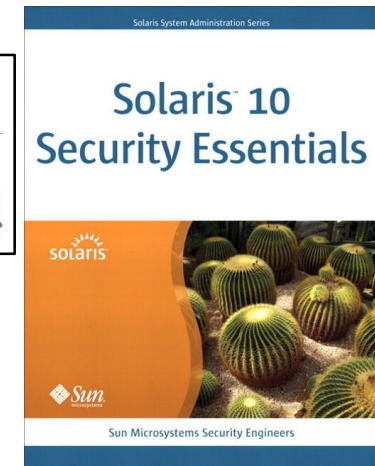
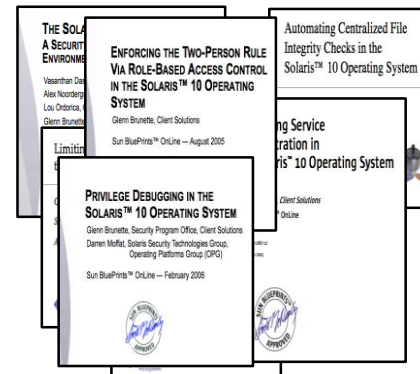
things you can do to get more secure

ORACLE

## Key Takeways

- A Good Security Architecture Matters – Defense in Depth for Application, Systems, Storage & Network
- Oracle Database and Applications to Leverage Oracle Infrastructure Security Technologies
- OS Virtualization – Solaris Zones - Enabler for Multi-Tenancy and Databases Consolidation
- Oracle Database Consolidation with Solaris Zones is Best Practice.

## Solaris Security – More Information





The preceding 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®