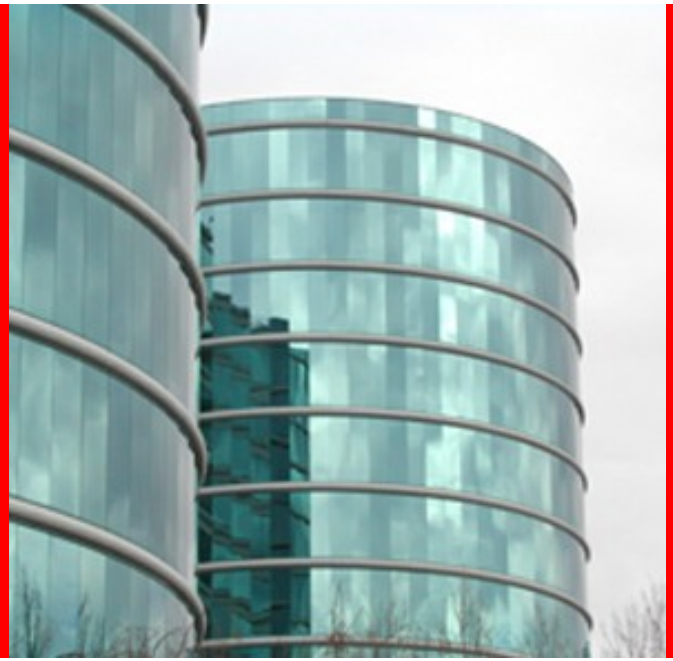

ORACLE®



ORACLE®

Project Alcatraz: Secure Oracle DB on Solaris

Bertram Dorn
Systems Architect
Advanced Customer Service for Systems, Delivery

Disclaimer

Framework:

- We will show features which are today available with Oracle Solaris 10, this does not mean that all possible combinations are valid for support/production
- The only supported combination is Oralce Solairs 10 with the corresponding Oracle Databases
- The base target of the following Information is to demonstrate structures, functionalities and the easy path for setting things up.

Program Agenda

- Background / some Solaris features
- Config-Vision
- What else can we do?

Secure: Solaris + DB

Some Solaris Features and Background

Callenges

- Priviledged Users (root,oracle)
- Easy to use and changeable Filesystems/Devices
- Difficult security related monitoring
- Not used audit features → No evidence for actions
- Thinking: „Security prevents daily work“
- Unclear access path
- “Inside” actions are possible
- Easy walking between accounts and POSSIBILITIES

The Mission of Project Alcatraz

Combine Solaris features with the Oracle-Database, use related security features to deliver:

- a still suitable to manage environment
- a combination witch is at least activating the security features

The Approach (1/3):

- Zones
  - Encapsulate database in own environment
  - Zone configraation 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”

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)
  - Doublecheck OS-Installation with Solaris fingerprint database
  - Searches for changes on files and directoriesZones
  - Encapsulate database in own environment
  - Zone configraation and resources are controlled from “outside”

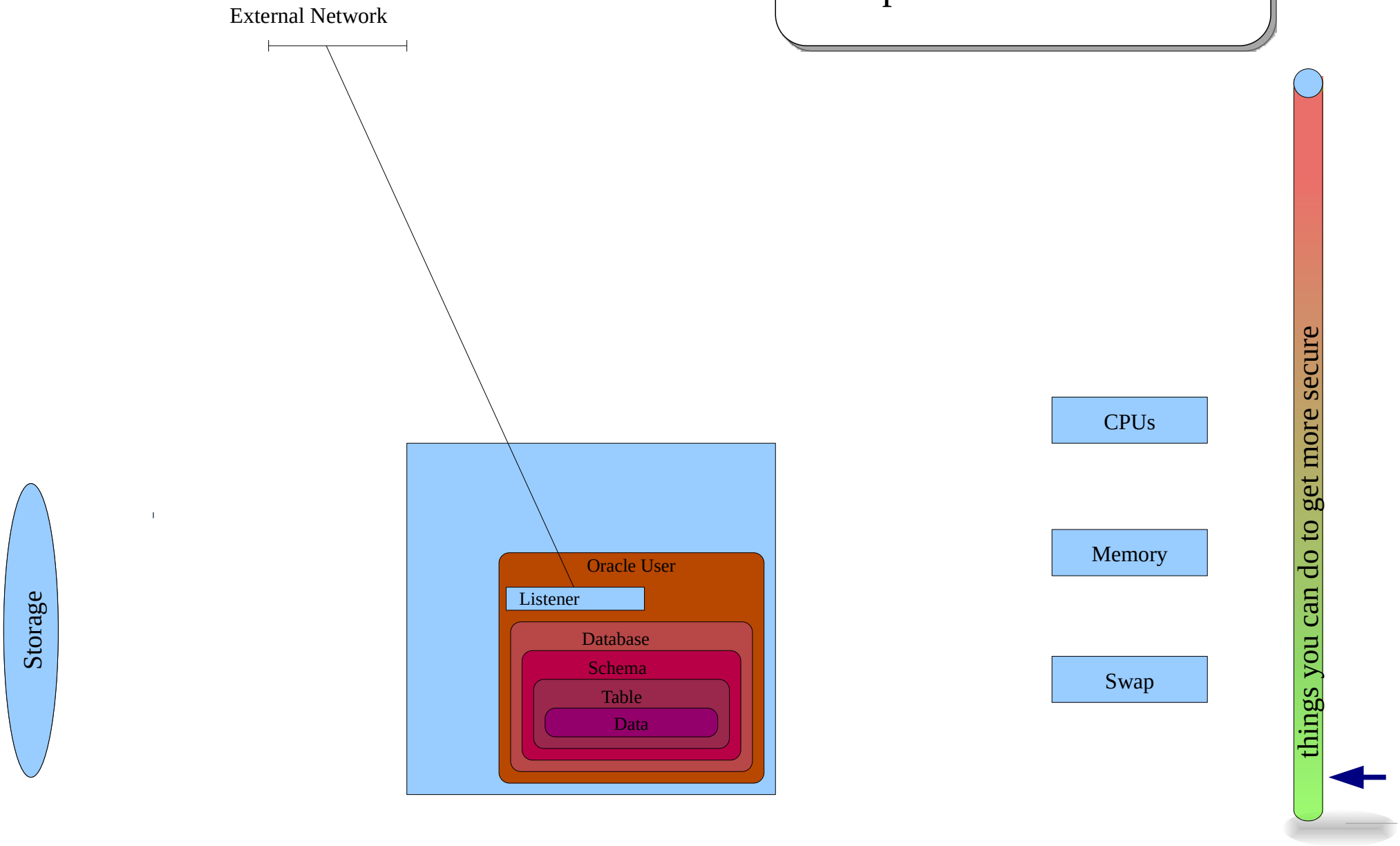
The Approach (3/3):

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

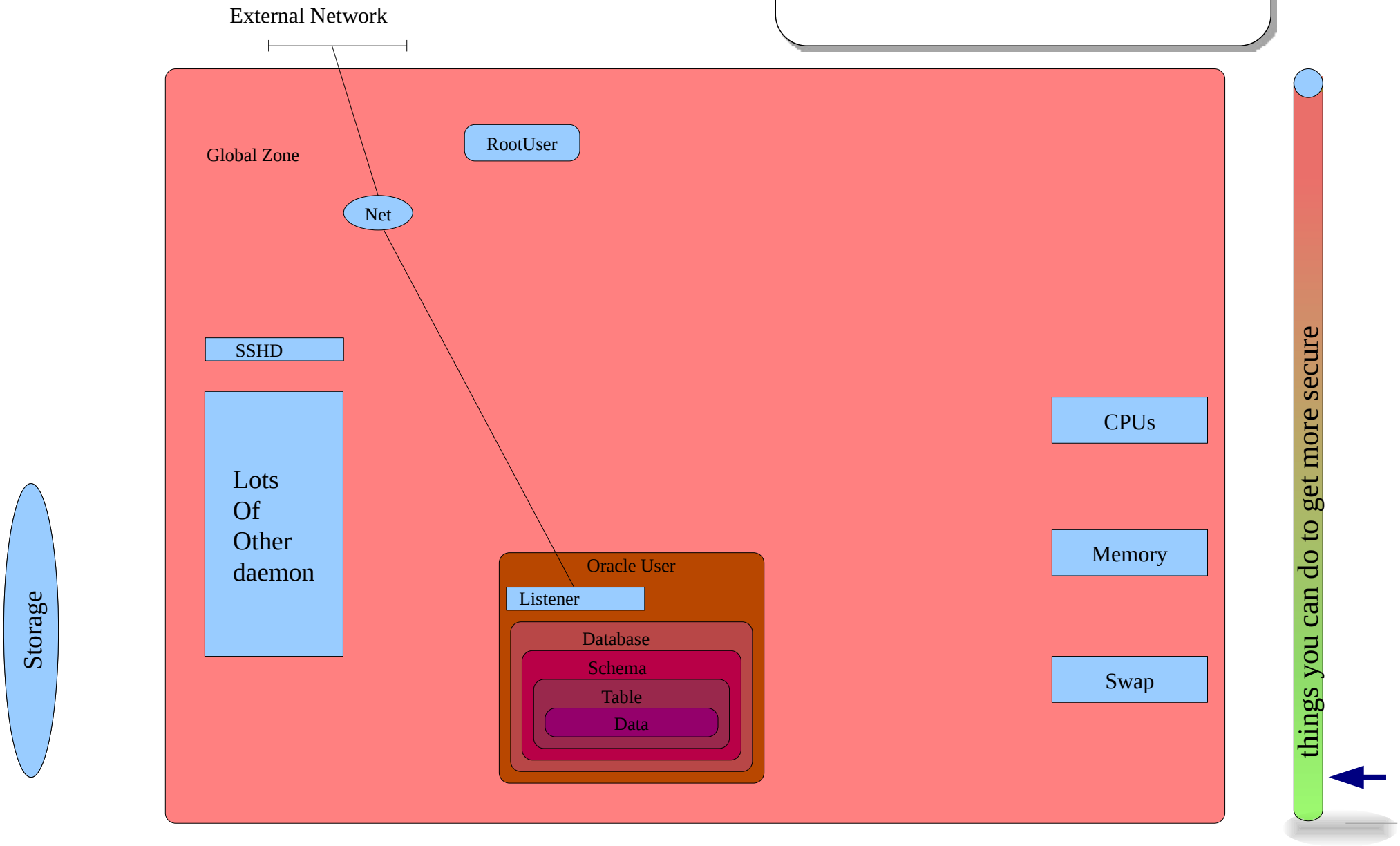
Secure Config

The Vision

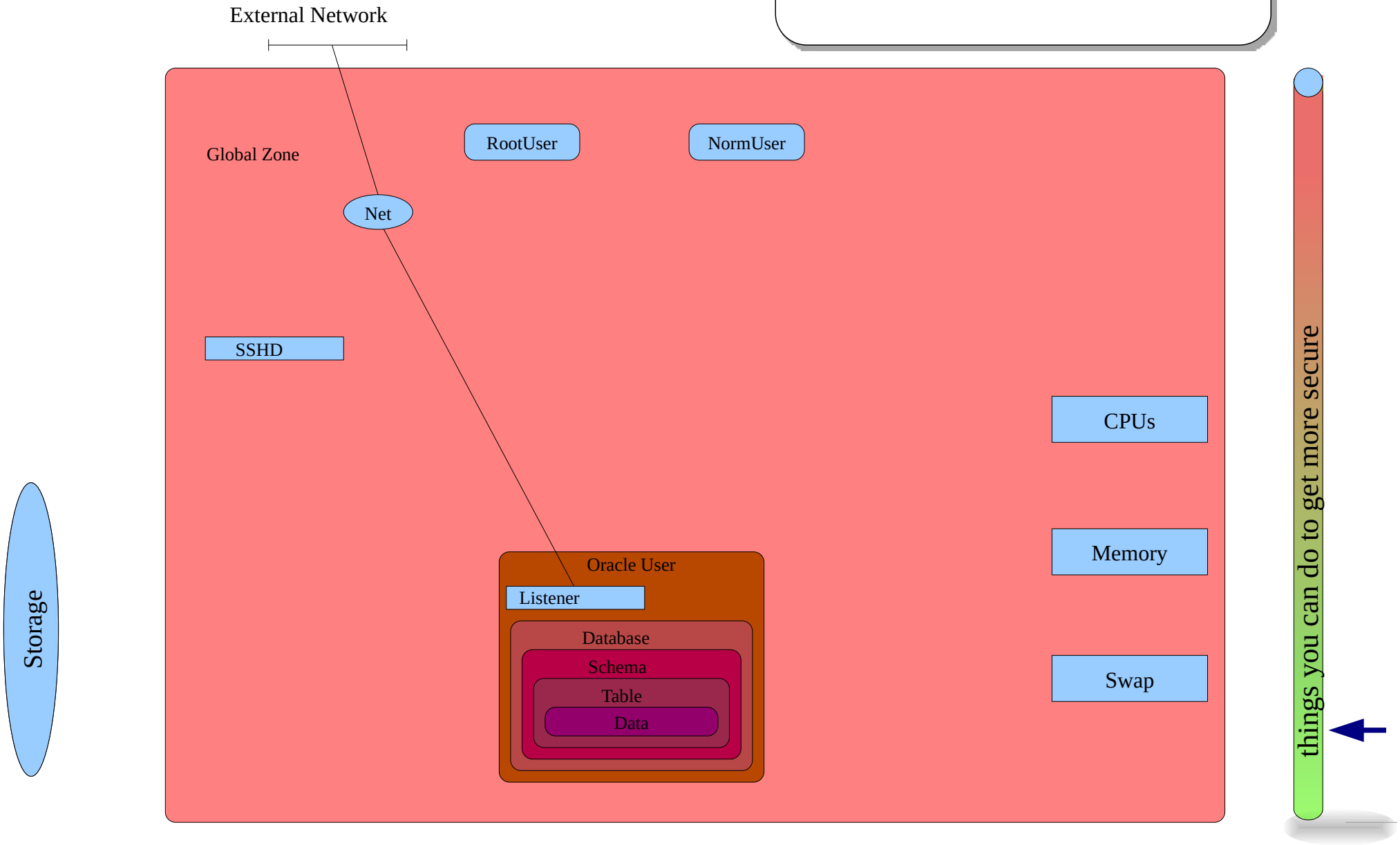
A Typical Oracle DB Standpoint



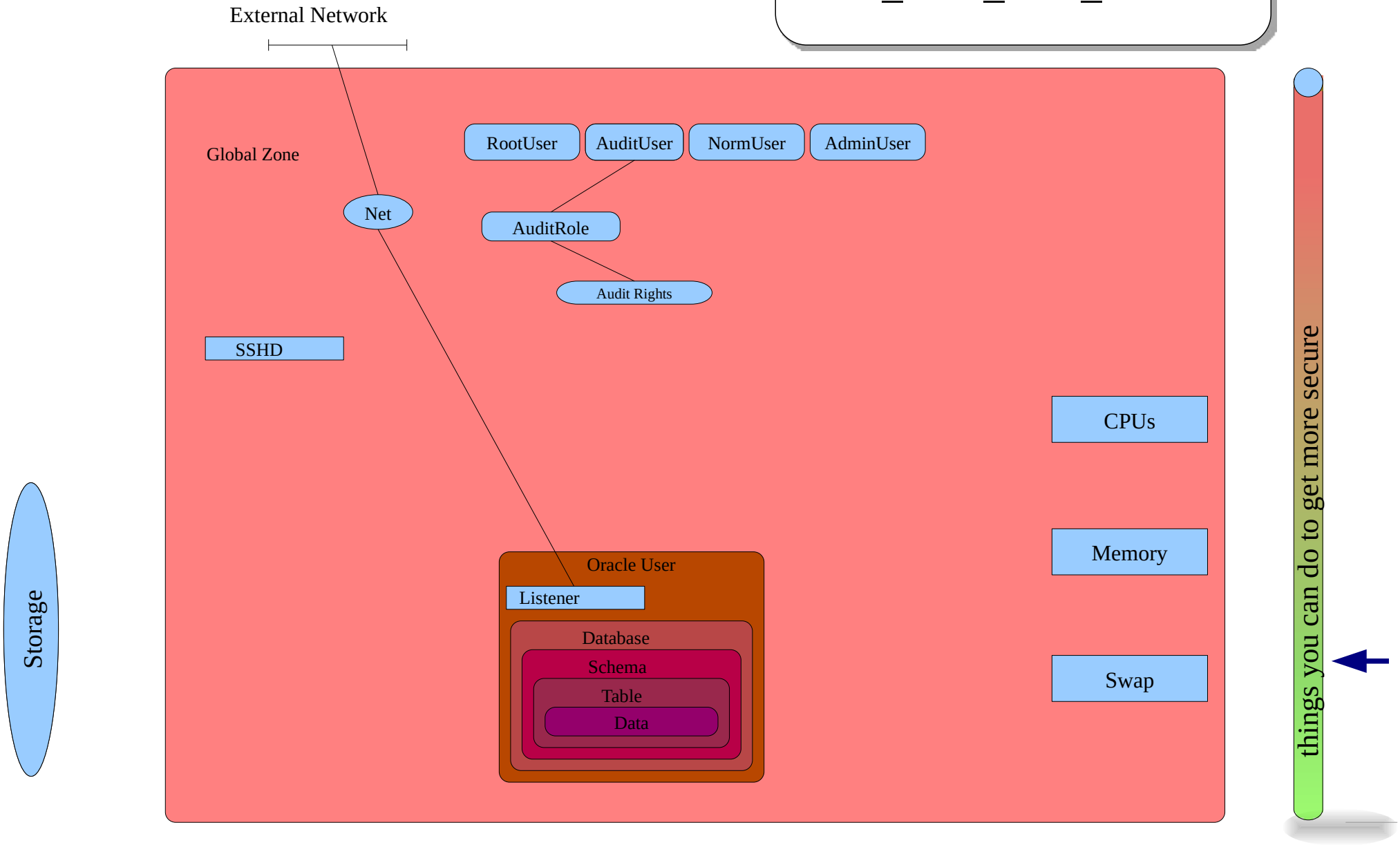
A Bit More Detailed



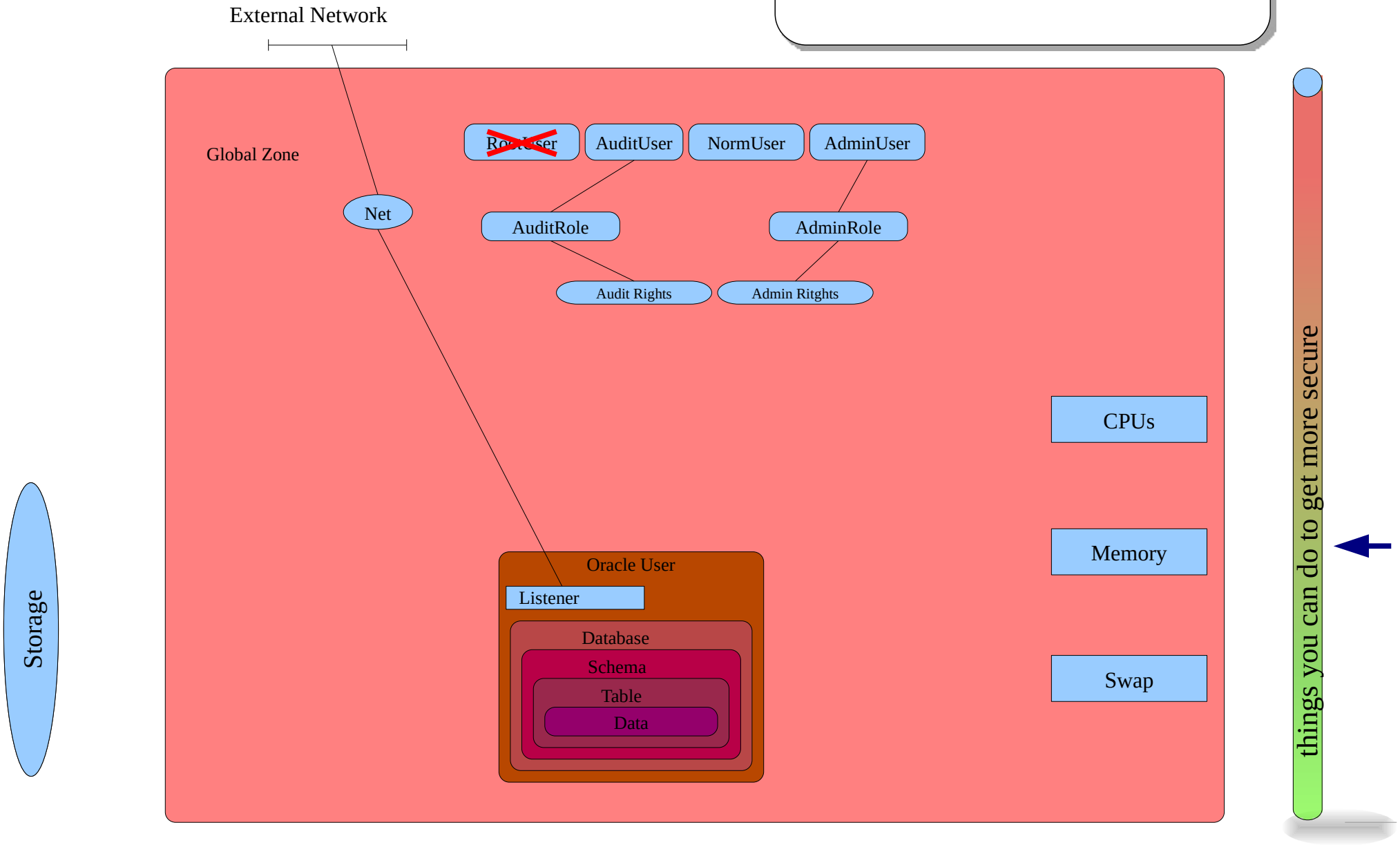
Netserivces „limited“
Create User



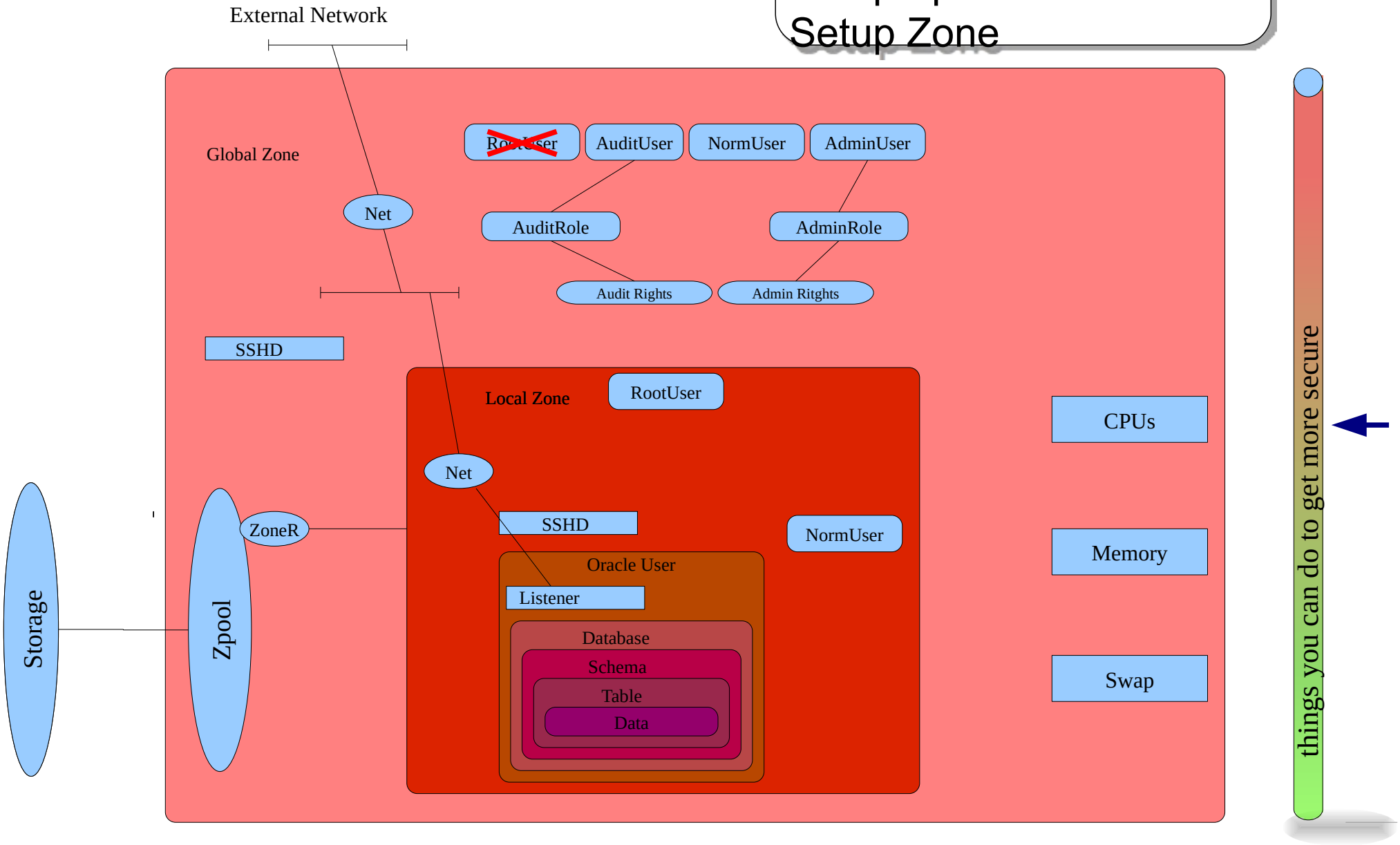
Conf gure Audit
Set No_Exec_User_Stack



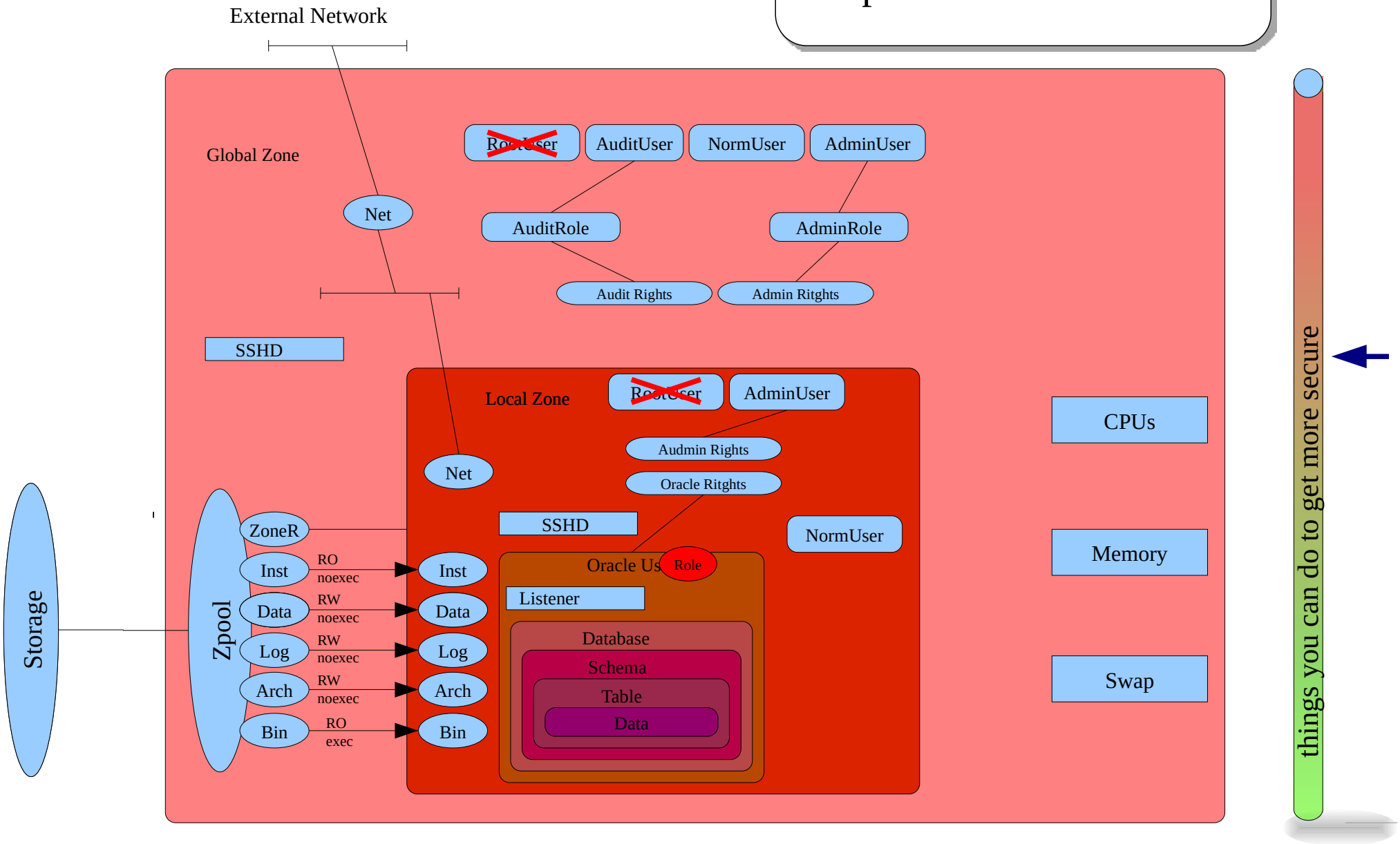
Reconf g root
Create roles



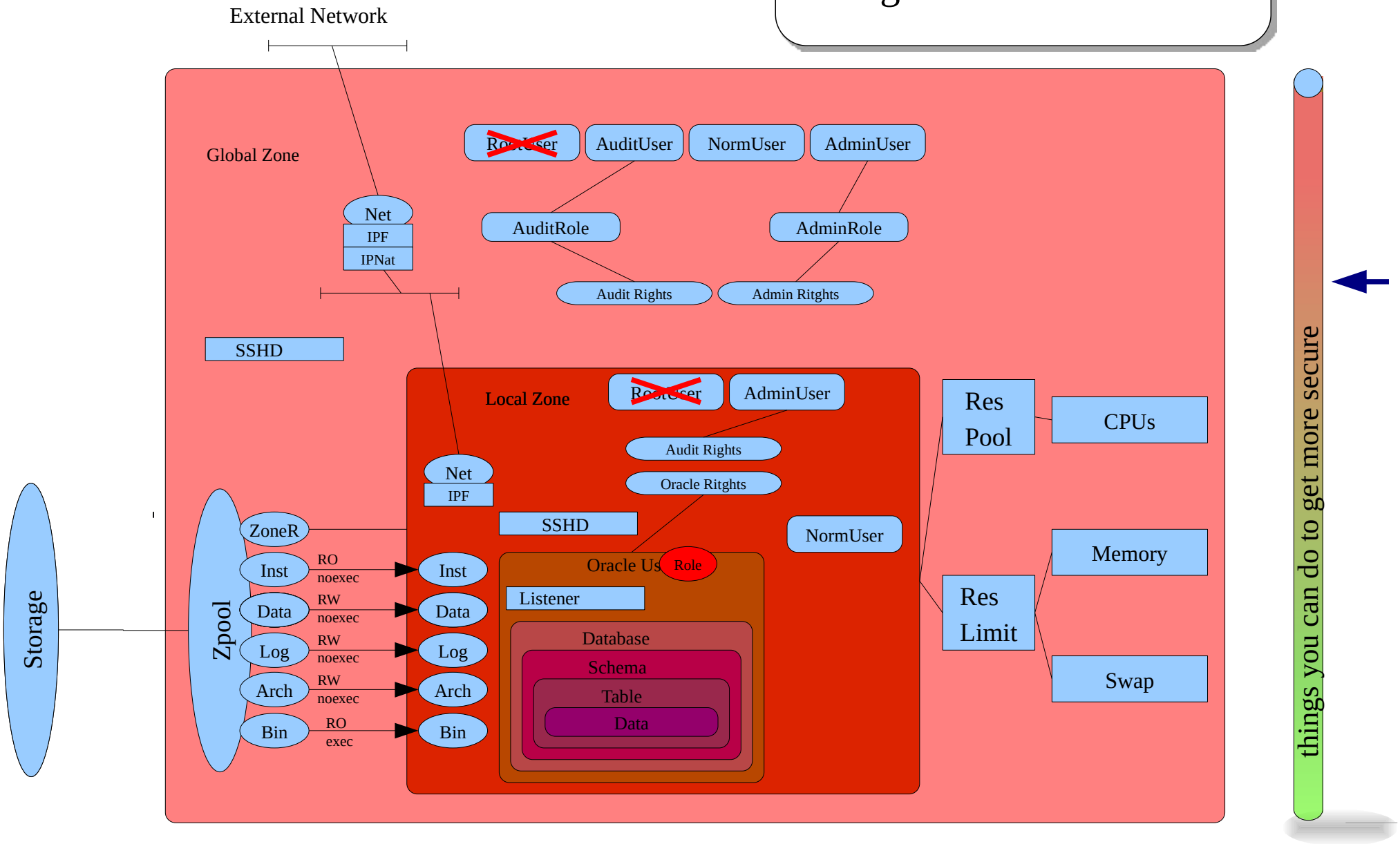
Setup int Net
Setup Zpool
Setup Zone



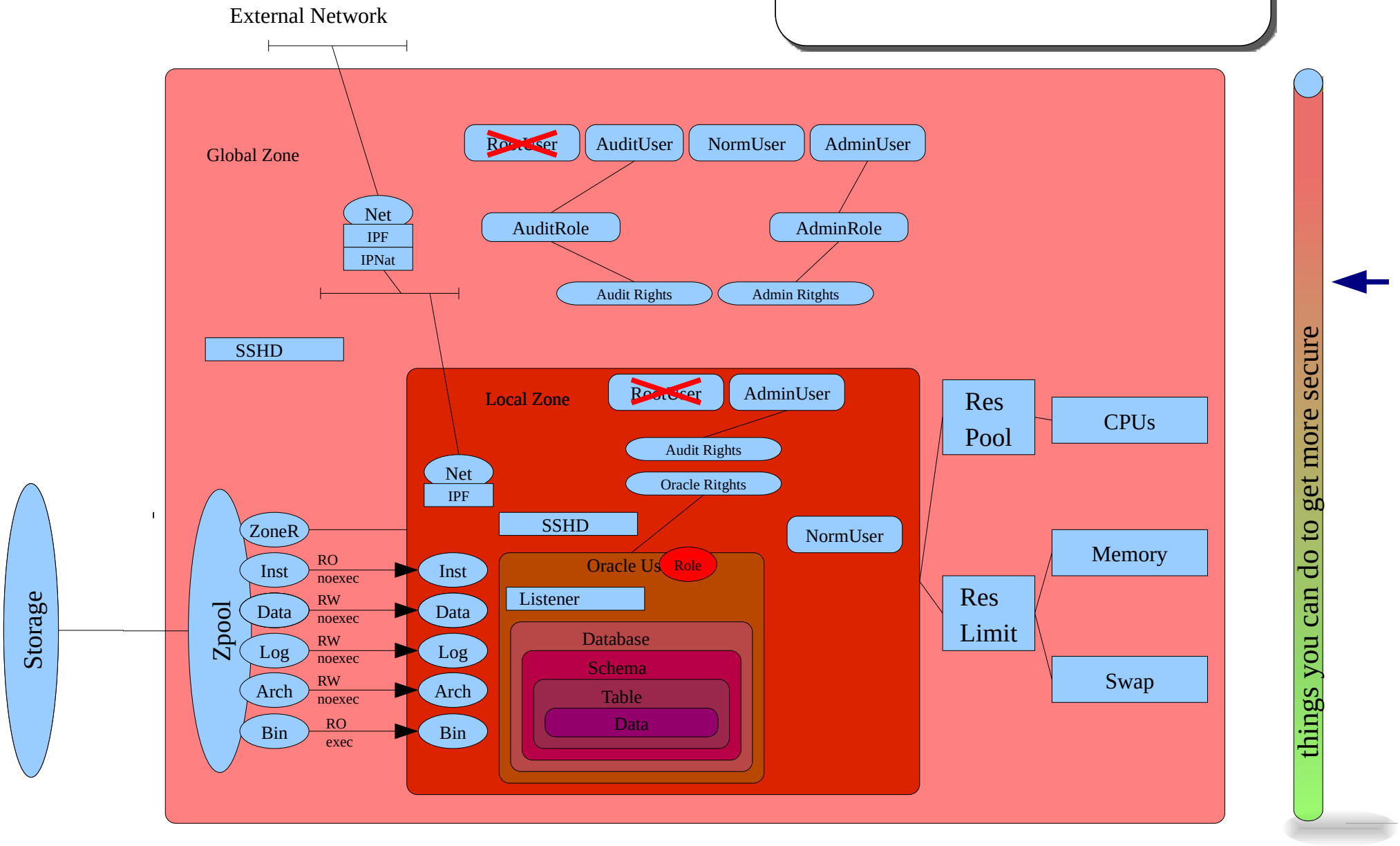
Create Datasets
Setup Zone RBAC



Conf gure IPF/IPNAT
Conf gure Res-Pools



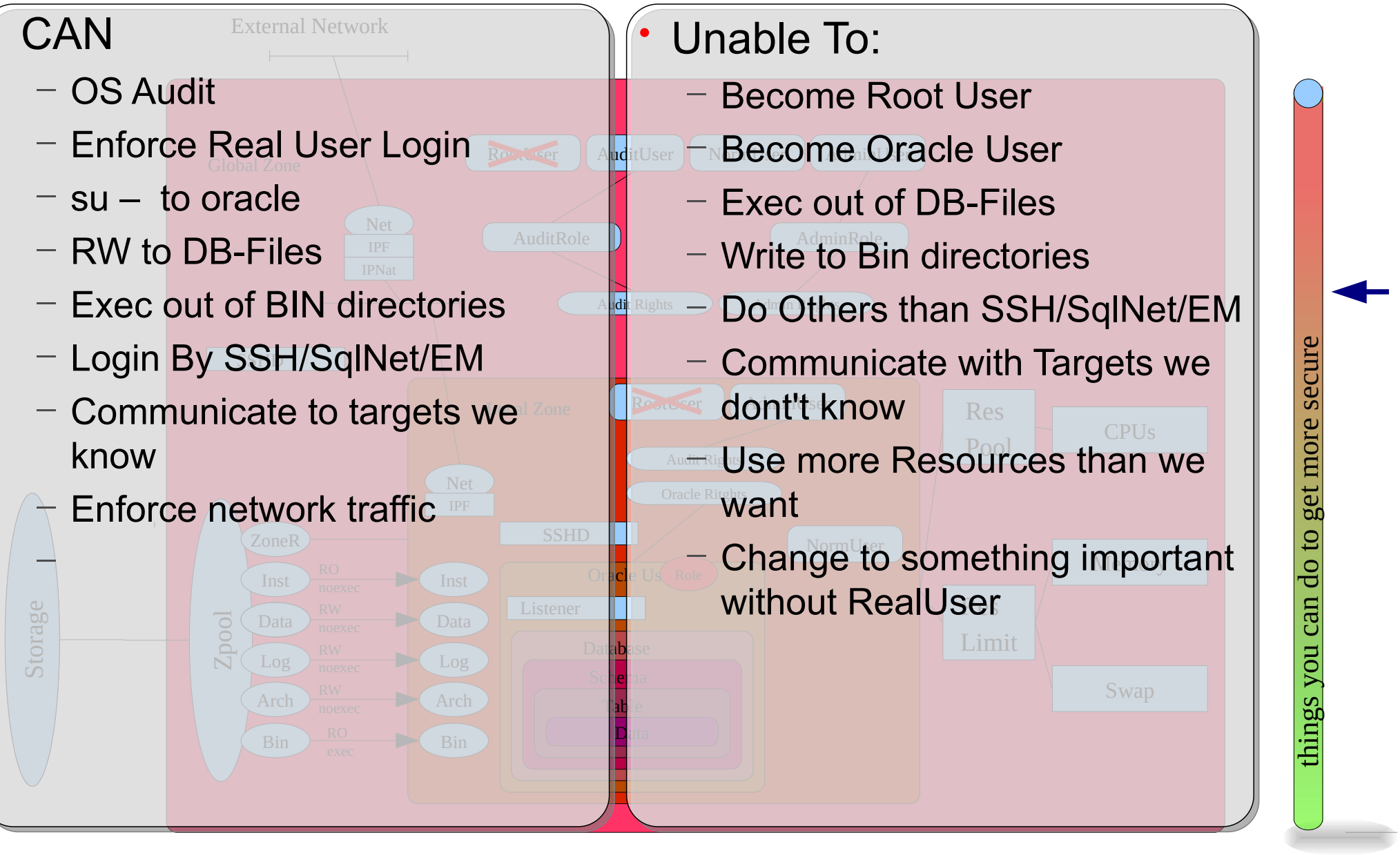
Final Setup for Today



Can / Can Not

- CAN
  - OS Audit
  - Enforce Real User Login
  - su – to oracle
  - RW to DB-Files
  - Exec out of BIN directories
  - Login By SSH/SqlNet/EM
  - Communicate to targets we know
  - Enforce network traffic
  - –

- Unable To:
  - Become Root User
  - Become Oracle User
  - Exec out of DB-Files
  - Write to Bin directories
  - Do Others than SSH/SqlNet/EM
  - Communicate with Targets we dont't know
  - Use more Resources than we want
  - Change to something important without RealUser



Secure: Inside the DBMS

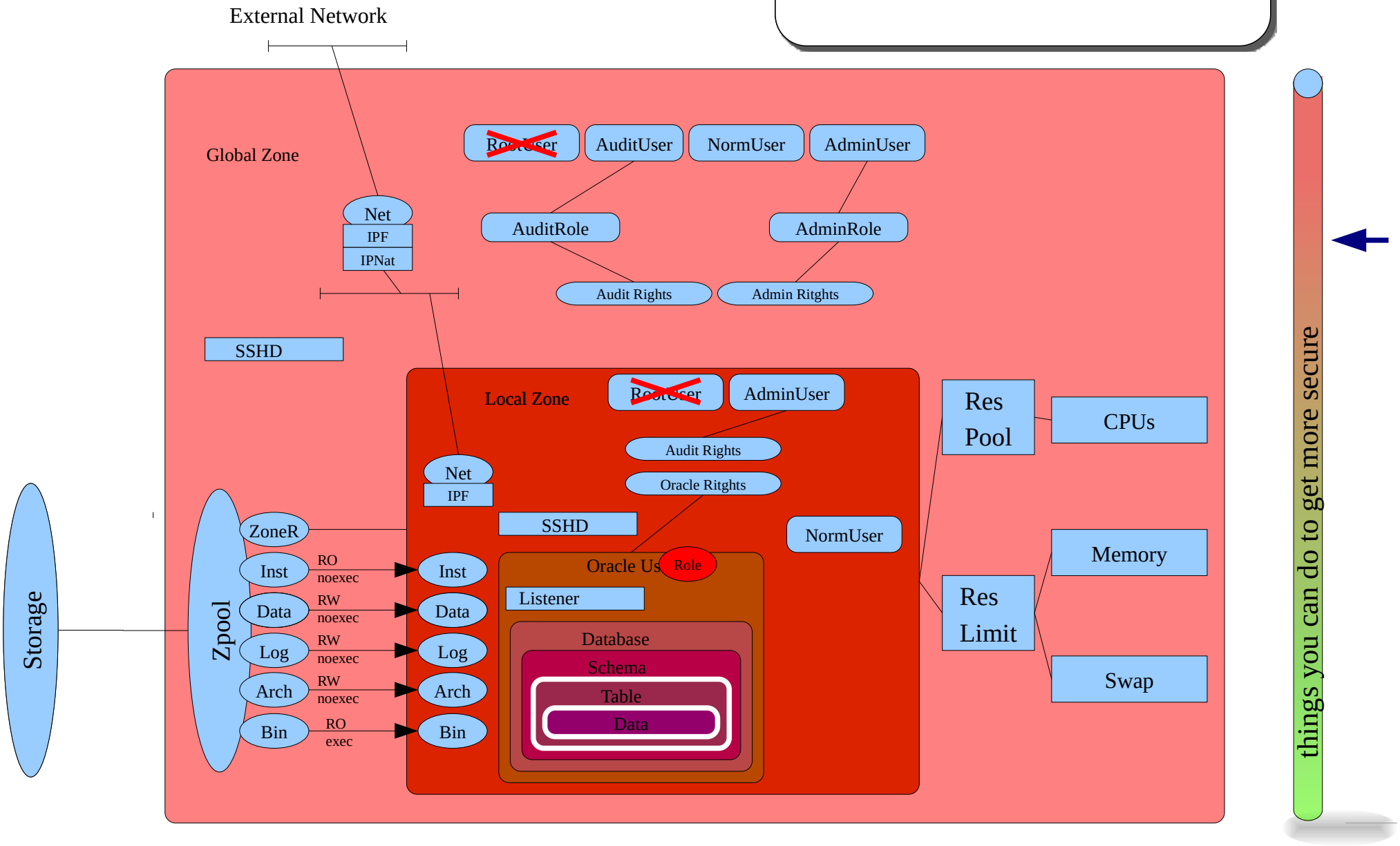
Callenges on the DBMS Side

- Priviledged Users (sys) may see and change everything
- SqlNet ist not encrypted by default
- Data on Disk is not encrypted
- Audit speaks of start and stop, but not a lot of more
- Grand to users might be to generic
- Access to not allowed objects is not logged
- “Inside” actions are possible

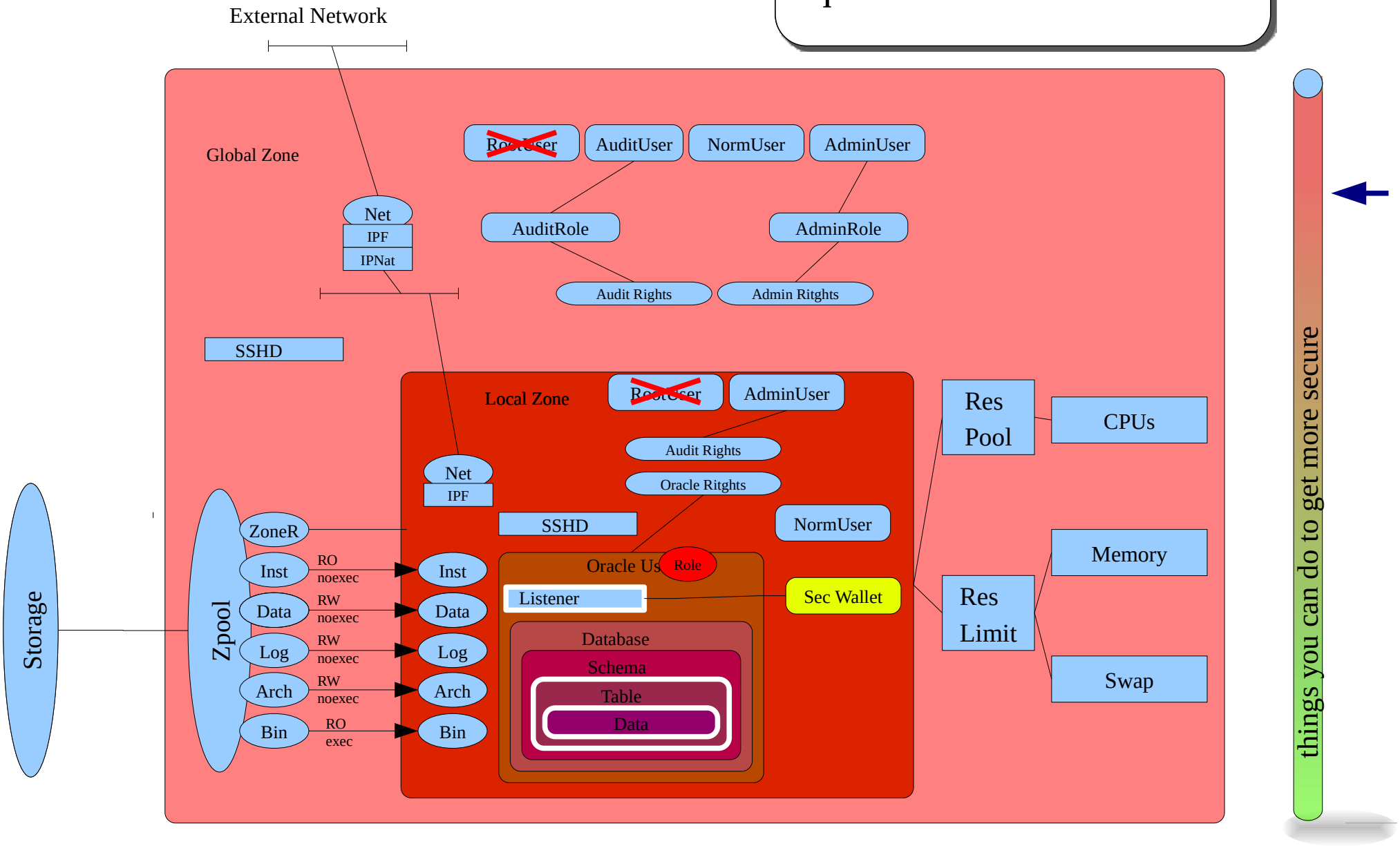
The Approach (1/1):

- DB Audit
  - Use the DB-Build in Audit to get Informations
  - Setup Audit to see
- DB Vault
  - Enforce Access/Deny to DB-Objects
  - Get Informations into the Database
  - Prevent Sys/DBA to access critical Objects
- Advances Securit Options
  - Setup Wallet
  - Listener Security
    - Setup ACL
    - Setup Logging
    - Setup SqlNet Encryption
  - Data Encryption
    - Encrypt a Tablespace

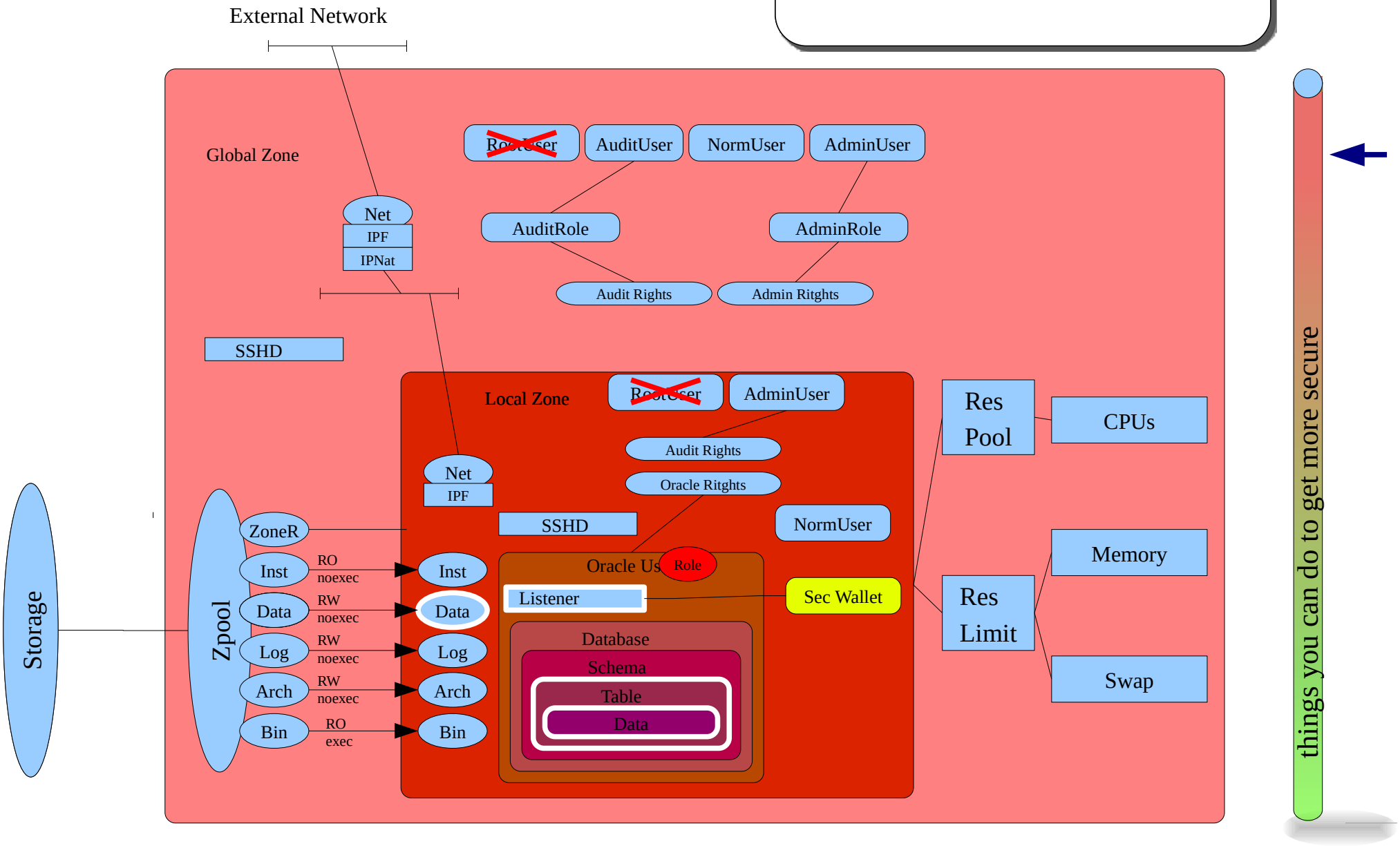
Secure Objects with DB Vault



Encrypt and Secure SqlNET

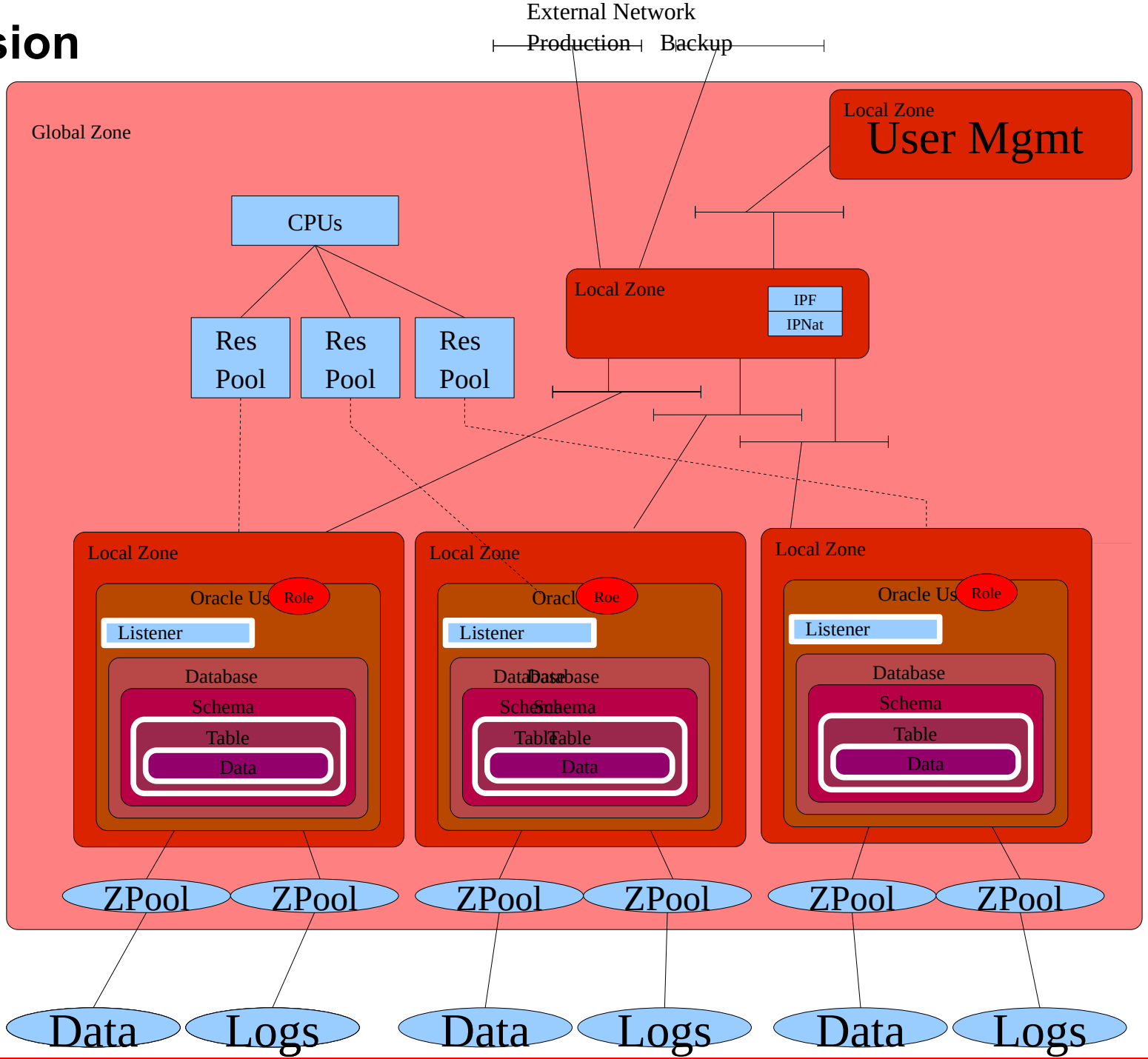


Encrypt Tablespace



Vision

Vision



things you can do to get more secure

Q&A

Ask us, and get in contact if you need help

bertram.dorn@oracle.com

Credits

This Information/Demo Is Based On:

- Lots of Customer Projects and Discussions
- Immutable Service Container Blueprint

  (Glenn Brunette)
- Influenced by several presentations

  (e.g Protecting Networked Services with (Open)Solaris Security Features by Dr. Christoph Schuba, Solaris 10 Security Deep Dive)
- Solaris Security Toolkit

SOFTWARE. HARDWARE. COMPLETE.

We encourage you to use the newly minted corporate tagline
“Software. Hardware. Complete.” at the end of all your presentations.
This message should replace any reference to our previous corporate tagline
“Oracle Is the Information Company.”

Some more Information on local Zones

Local Zones Are:

- Lighwight representation of a Solaris-OS
- A GlobalZone (a normal Solaris install) might run one ore more LocalZones
- LocalZones are
  - guests on a Type 4 Hypervisor
  - participating on resources from the GlobalZone
    - Kernel
    - Networking
    - Memory
    - Scheduling
    - Device Access
  - do have own user databases
  - communicating via network only
  - operating with fewer privileges
  - having their own root directory
  - either inherit binaries ore are working on a copy of the original binaries
- Special rights and device access is controlled by the GlobalZone

Some more Information on local Zones Networking

- GlobalZone sets network possibilities for local Zones
- LocalZones only communicate over the network
- GlobalZone might run IPF/IPNAT for access/traffic management from and to local Zone
- LocalZones might have own IP-Stack, and therefor might run own IPF Instances
- LocalZones might have own routing
- LocalZones might have their own set of services
- LocalZones must be maintained similar to any other Solaris Install

Some more Information on ZFS

- ZFS (from a security standpoint and very condensed)
  - Works with “Copy on Write”
  - Checksumming of data
  - Easy to use snapshots
    - Will create read only copy of dataset
    - Might be used for forensic and fast recovery
  - ZFS Pools
    - Are a summary (and description) of single “Disks” (or lunes)
    - Defines RaidLevel
  - ZFS Dataset (filesystem)
    - Does have own quota and access rights
    - Will be delegate to zone
    - Will be controlled from the globalzone → from outside

Some more Information on RBAC and BSM

- RBAC
  - Defines Roles
  - Roles must be assigned to users
  - A direct login to a role is not possible
  - Enforces a user login
  - Might eliminate privilegded users like root or “oracle”
  - A role might have less or more rights than the user
  - We might define effective or real user id for each binary a role/user will start
  - Is deeply integrated with the Solaris-Audit to log the access pathes
  - Roles can not delegate what they don't have
- BSM
  - Checkes files against a fingerprint which has been created before
  - Might check Installation against the Solaris-Fingerprint-Database

Some more Information on “others”

- Netservices Limited
- No exec user stack
  - Prevents code to start code out of the stack
- SMF
  - Integrade with right management and RBAC
  - Will not deeply discussed because this is “dayly work”