

# Misconfigured By Default

## Installing the Oracle Database for Expert Oracle DBAs

Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: damorgan11g  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)



# Introduction



# Daniel Morgan

 Oracle ACE Director

- Oracle Educator

-  Curriculum author and primary program instructor at University of Washington

-  Consultant: Harvard University

- University Guest Lecturers

- APAC: University of Canterbury (NZ)

- EMEA: University of Oslo (Norway)

- Latin America: Universidad Latina de Panama and Technologico de Costa Rica

- IT Professional

- First computer: IBM 360/40 in 1969: Fortran IV

- Oracle Database since 1988-9

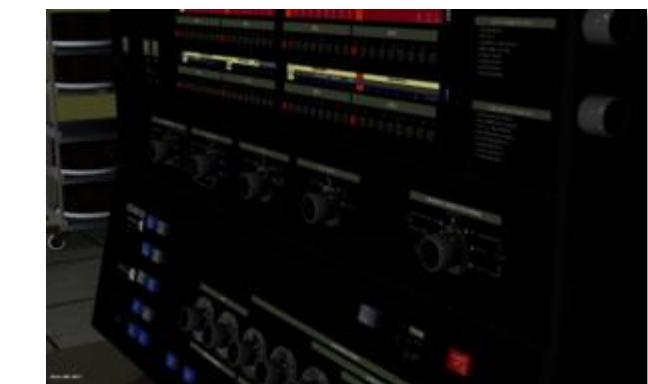
- Beta Tester 10g, 11g, 12c, TimesTen, GoldenGate

- The Morgan behind [www.morganslibrary.org](http://www.morganslibrary.org)

- Member Oracle Data Integration Solutions Partner Advisory Council

- Co-Founder International GoldenGate Oracle Users Group

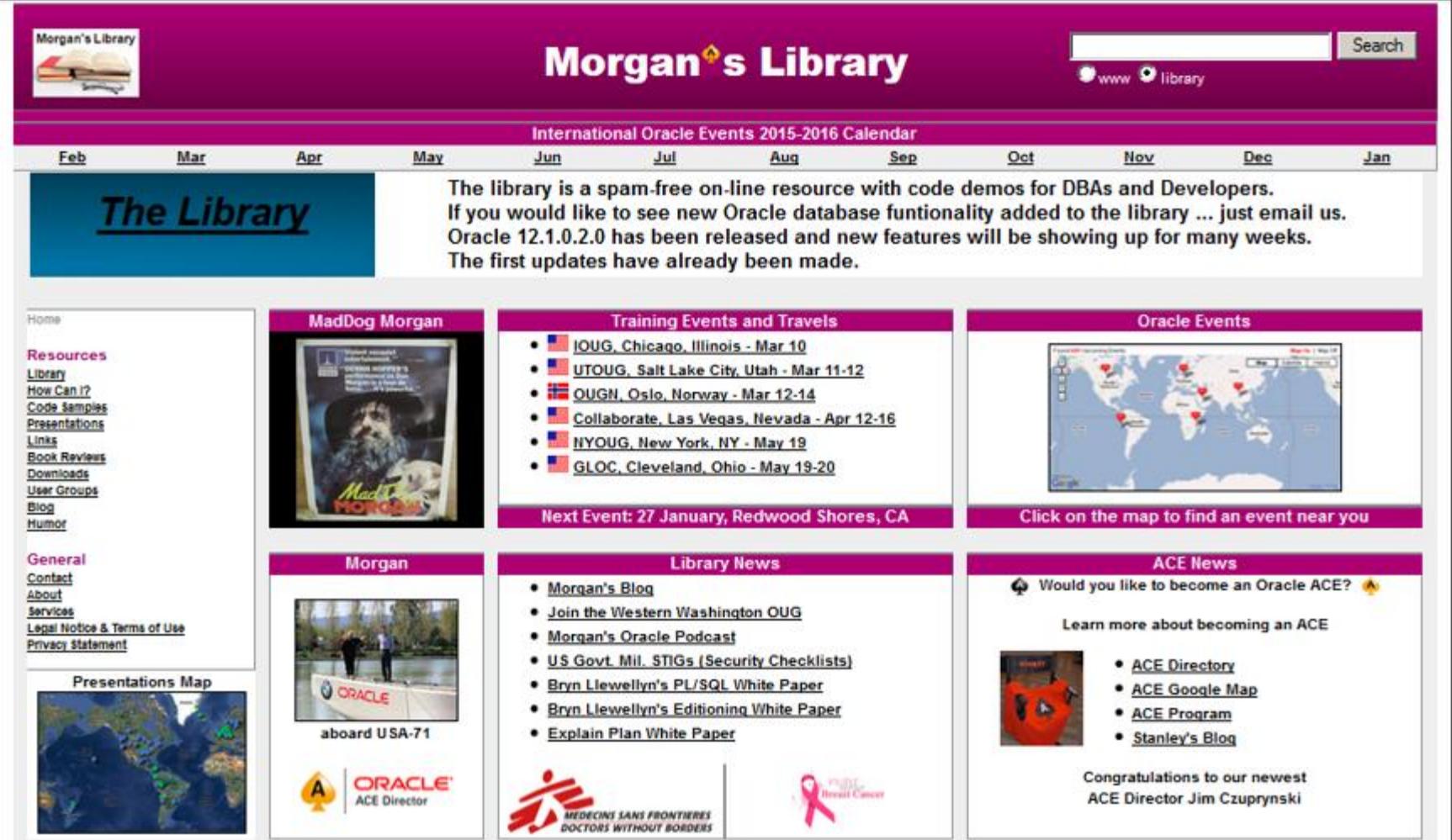
- Principal Adviser: Forsythe **Meta7**



System/370-145 system console



# My Websites: Morgan's Library



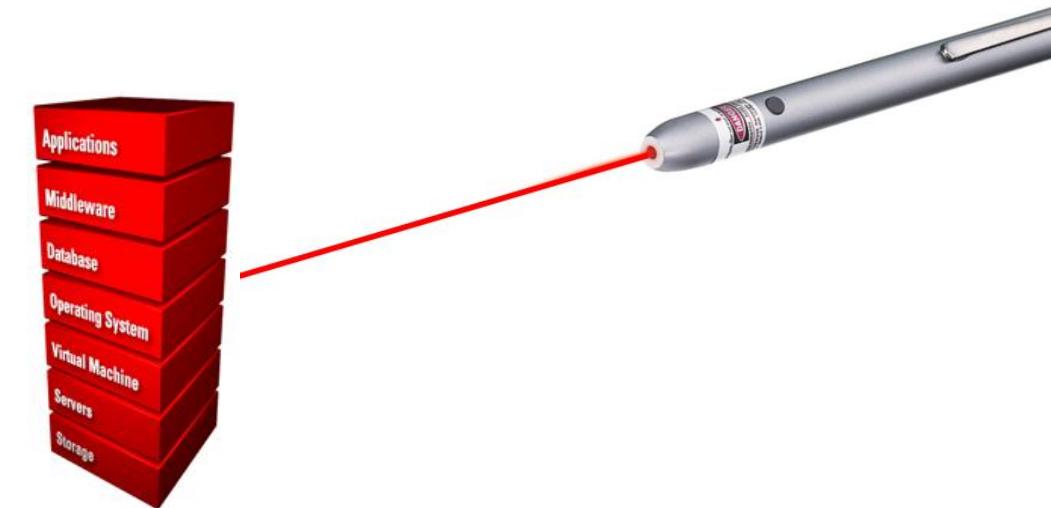
The screenshot shows the homepage of Morgan's Library. The header features a logo with books and the text "Morgan's Library". A search bar and a link to "www.library" are also in the header. Below the header is a navigation bar with links for Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec, and Jan. A large blue banner on the left says "The Library". The main content area includes a section for "International Oracle Events 2015-2016 Calendar" with a list of events and a map of the world showing event locations. There are also sections for "MadDog Morgan" (with a photo of a dog), "Training Events and Travels" (listing events like IOUG, UTOUG, OUGN, Collaborate, NYOUG, and GLOC), "Oracle Events" (with a map), "Morgan" (with a photo of a person on a boat), "Library News" (listing various Oracle-related links), and "ACE News" (with a video player and a list of ACE-related links). A sidebar on the left contains links for Home, Resources (Library, How Can I?, Code Samples, Presentations, Links, Book Reviews, Downloads, User Groups, Blog, Humor), and General (Contact, About, Services, Legal Notice & Terms of Use, Privacy Statement). A "Presentations Map" is also shown in the sidebar.

[www.morganslibrary.org](http://www.morganslibrary.org)



# What Meta7 Brings To The Party

- The "Oracle Only" division of Forsythe focused on only the Red Stack
- A team of skilled professionals with
  - Extensive experience across multiple industries
  - Deep specialization in core Oracle technologies
    - Hardware
    - Licensing
    - Professional Services
  - 0% off-shoring: All work performed by US residents
- Reliable on-time and on-budget delivery
- Corporate headquarters in Chicago, Illinois
- New, State-of-the-Art Technology Evaluation Center
- Secure hosting and Managed Services in our own Tier 3 data center on the same power grid and fibre as O'Hare airport
- Flexible financial support



# What Meta7 Brings To The Party (2:2)

Product Area	Strategy
Cloud Solutions	Oracle Optimized Solution for Enterprise Cloud Infrastructure
Database	Oracle Database 11g
Database	Oracle Database 11g Data Warehousing
Database	Oracle Database 12c
Database	Oracle Enterprise Manager 12c
Database	Oracle Real Application Clusters 11g
Engineered Systems	Oracle Database Appliance Specialization
Engineered Systems	Oracle Exadata Database Machine
Industries	Professional Services
Middleware	GoldenGate 12.2
Servers and Storage Systems	Oracle Linux 5
Servers and Storage Systems	Oracle Solaris 10
Servers and Storage Systems	Oracle Solaris 11
Servers and Storage Systems	Oracle VM 3
Servers and Storage Systems	Oracle ZFS Storage
Servers and Storage Systems	SPARC Enterprise Entry-Midrange M-Series Servers
Servers and Storage Systems	SPARC T2 and T3-Based Servers
Servers and Storage Systems	SPARC T4-Based Servers
Servers and Storage Systems	SPARC T5-Based Servers
Servers and Storage Systems	Sun ZFS Storage Appliance





# *Zero Downtime Database Migrations with GoldenGate*

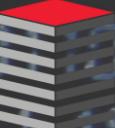
Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: [damorgan11g](skype:damorgan11g)  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)

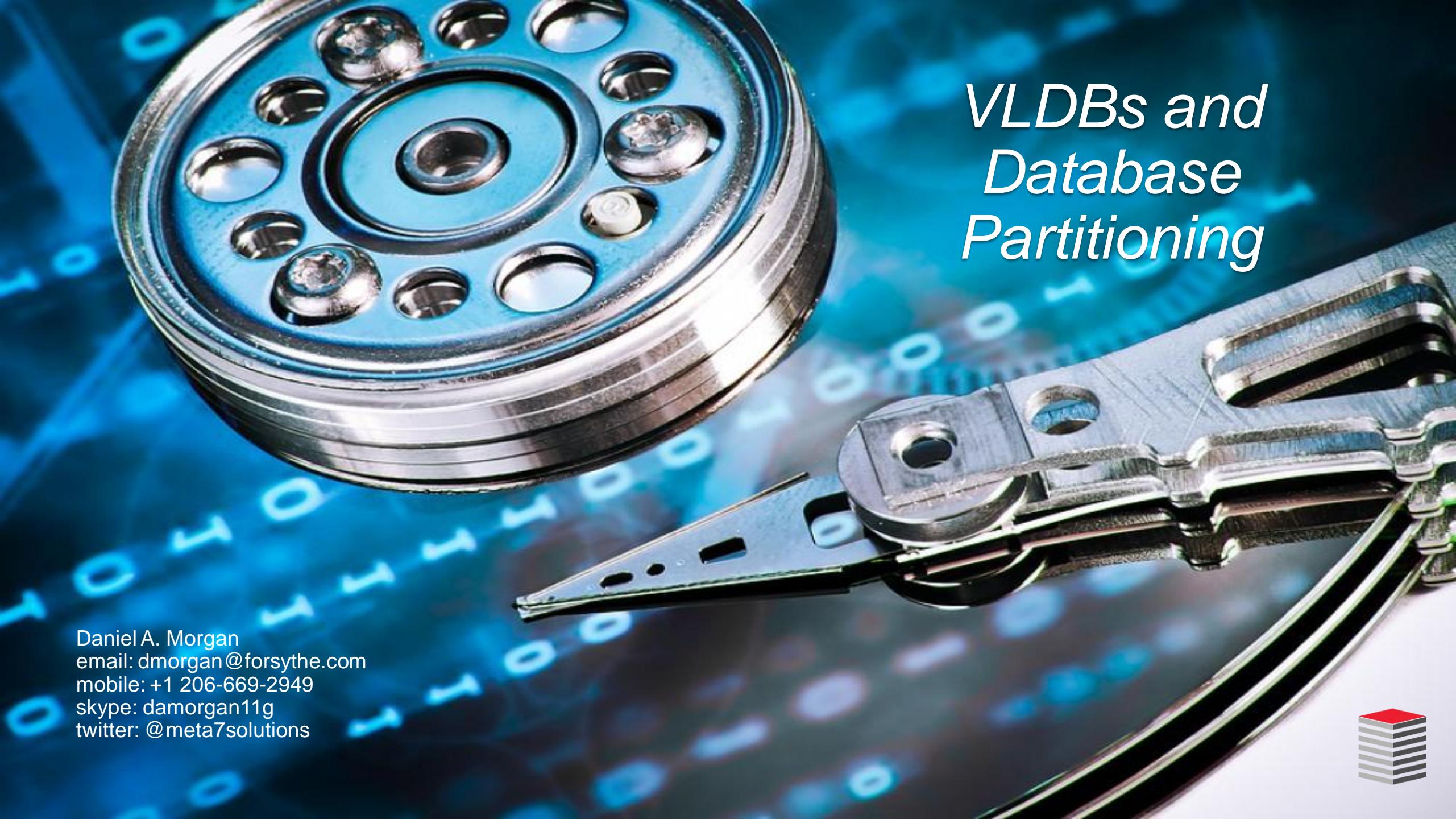




# *How Do You Safeguard the Database Against Today's Cyber Threats?*

Daniel A. Morgan  
email: dmorgan@forsythe.com  
mobile: +1 206-669-2949  
skype: damorgan11g  
twitter: @meta7solutions





# *VLDBs and Database Partitioning*

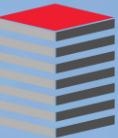
Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: [damorgan11g](skype:damorgan11g)  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)



# *Database Performance*



Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: damorgan11g  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)



# *IT Fire Fighting*

Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: [damorgan11g](skype:damorgan11g)  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)



# *Oracle DBaaS Migration Road Map*



Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: damorgan11g  
twitter: [@meta7solutions](https://twitter.com/meta7solutions)



# Content Density Warning



Take Notes ... Ask Questions

# Rhetorical Question

- Would you want your surgeon to practice medicine like he did in the 1990s?



- Then why are you installing the Oracle Database the way we did in the 90's?

# Why Am I Focusing On Oracle Database Installation?

- Because no one else is
- Because Oracle University doesn't teach this material
- Because essentially no-one does a good job of Oracle Database installation
- Because almost no one knows the full syntax of CREATE DATABASE
- Because we have now spent 37 years installing it and we still have issues with the three S's
  - Stability
  - Scalability
  - Security
- Because OUI and DBCA do a mediocre job of database installation
- Because we, as an industry, need to stop implementing and accepting mediocrity and rise to the standard of being professionals



# The Concept

- Simply put ... do it right during initial installation ... not incrementally over subsequent days, weeks, months, and years
- Getting it right during initial installation will eliminate years of fighting fires, security breaches, audit failures, and performance issues
- This means
  - Buy the right infrastructure
  - Properly configure the networks
  - Properly configure the storage
  - Properly configure the servers
  - Properly configure the operating system and any virtualization layer
  - Properly configure every aspect of the database
- And it means educating our network, storage, and system administrators on what constitutes "best practices"
  - I hope this won't frighten them too much but they have to read the docs



- The biggest single difference between an OUI + DBCA installation and what is recommended here is addressing the inherent risk in using SQL\*Plus in the \$ORACLE\_BASE file system which is an unacceptable security compromise
- Other than an extremely limited set of tasks there is no regular monitoring or maintenance job that requires operating system access as the owner of the Oracle binaries and the \$ORACLE\_BASE file system
- Anyone that can log in as the \*NIX user oracle
  - Has the ability to own your database using "/ as sysdba"
  - Has access to the alert log
  - Has access to \$ADR\_HOME and can read diagnostics
  - Has access to the FRA
  - Has access to the listener and its configuration files
  - Has access to every script in /rdbms/admin
  - Likely also can read RMAN, Export, Import, and shell scripts
- If people have this level of access security is essentially impossible to achieve



- Thus, it is strongly recommended, that an Oracle Database installation
- Unless it will store nothing more important than my mother's cookie recipes
- Involve creation of two separate owner's for Oracle binaries
  - \$ORACLE\_BASE for installation of the Oracle Database
  - \$ORACLI\_BASE for installation of the Oracle Client
- And a third owner if Oracle Clusterware and ASM are utilized
  - \$GRID\_BASE for installation of Oracle Clusterware and ASM



# Database Installation Roadmap

1. Gather Requirements
2. Plan Networks, Storage, Servers & Operating Environment
3. Deploy VM and Operating System
4. Configure Operating System
5. Shell Configuration
6. Operating System Lockdown
7. **Clusterware & DB Binary Installation**
8. Listener Configuration
9. Database Installation
10. SPFILE Modification
11. GLOGIN Modification
12. Secure Database
13. Privilege Revocation
14. Get Optimizer Statistics
15. Get Processing Rates
16. Set AWR Collection
17. Create Tablespaces
18. Create Users



# Database Client Installation Roadmap

1. Gather Requirements
2. Plan Networks, Storage, Servers & Operating Environment
3. Deploy VM and Operating System
4. Configure Operating System
5. **Shell Configuration**
6. Operating System Lockdown
7. **Client Installation**
8. Listener Configuration
9. Database Installation
10. SPFILE Modification
11. **GLOGIN Modification**
12. Secure Database
13. Privilege Revocation
14. Get Optimizer Statistics
15. Get Processing Rates
16. Set AWR Collection
17. Create Tablespaces
18. Create Users



# The Basics



# In The Beginning

- Before you purchase servers
- Before you purchase software licenses
- Before anything is racked-and-stacked
- Before downloading the installation zip files
- There are things that you must know to have any chance of getting it right
- This section addresses essential background information that you must possess and understand



# Requirements

- You cannot make good decisions without knowing the answers to these questions
  - Service Level Agreement (SLA)
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
  - Cost, per minute/hour, of unplanned outage
  - Anticipated number of simultaneous connections and 3-5 year growth projection
  - Anticipated number of simultaneous transactions and 3-5 year growth projection
  - Anticipated storage footprint and 3-5 year growth projection
  - Anticipated interfaces by software, protocol, bandwidth, and latency
  - Internal governance requirements and how they will be achieved
  - External compliance requirements and how they will be achieved



# Requirements

- If you cannot answer the preceding questions you cannot
  - Determine whether you need
    - One data center or three
    - x86-64 or z-Series frame ... ODA or Exadata ... T7 or SuperCluster or M10
    - Express, SE2, Standard or Enterprise Edition
    - High Availability options such as RAC and Data Guard
    - Active Data Guard licensing
    - Advanced Compression Option
    - Security Options such as Database Vault, Advanced Security, Label Security
    - Multitenant Option
    - In-Memory Option
    - Diagnostic and Tuning Pack
  - Whether licensing should be based on cpu cores or named users
  - Whether licensing should be perpetual or time limited



# Networks (1:2)

- Every Oracle Database deployment may require multiple network connections: Here is a full listing

Name	Protocol	Utilization
Management	TCP/IP	System Admin connection to the server's light's-out management card
Public	TCP/IP	Access for applications, DBAs, exports, imports, backups: No keep-alive if RAC
SAN Storage	Fibre Channel	Server connection to a Storage Area Network (SAN)
NAS Storage	TCP/IP or IB	Connection to an NFS or DNFS mounted storage array
RAC Cache Fusion interconnect	UDP or IB	Jumbo Frames, no keep-alive, with custom configured read and write caching
Replication	TCP/IP	Data Guard and GoldenGate
Backup and Import/Export	TCP/IP	

- If you wish to avoid single points of failure while deploying RAC and Data Guard in accordance with "best practice" guidelines ... there is a lot of network planning that needs to take place
- And no conversation of networking is complete without considering Firewalls DNS, and NTP (time) Servers



- NIC cards should support
  - For both stand-alone and RAC
    - TCP Segmentation Offloading (TSO)
    - Allows the system to do TCP segmentation in the NIC driver instead of main CPU via the kernel
- RAC
  - Configurable "keep-alive"
    - If a connection won't die immediately and cleanly it will never perform a transparent failover
  - Jumbo Frames (for the Cache Fusion Interconnect if 10gEth)
    - The normal frame size is 1518 bytes which must include the Layer 2 header and frame check sequence
    - To pass an 8K block without Jumbo Frames requires breaking the packet up into 5 pieces at the source and reassembling them at the target
    - As UDP packets are not sent in sequence additional read and write buffering is also required
    - Lost or flushed packets can result in a RAC node shooting itself in the head

## Keepalive Configuration Mode Commands

Downloads: [This chapter](#) (PDF - 148.0 KB) [The complete book](#) (PDF - 5.06 MB) | [Feedback](#)



### Table Of Contents

[Keepalive Configuration Mode Commands](#)  
[\(config-keepalive\) active](#)  
[\(config-keepalive\) description](#)  
[\(config-keepalive\) frequency](#)  
[\(config-keepalive\) hash](#)  
[\(config-keepalive\) ip address](#)  
[\(config-keepalive\) maxfailure](#)  
[\(config-keepalive\) method](#)  
[\(config-keepalive\) no](#)  
[\(config-keepalive\) port](#)  
[\(config-keepalive\) retryperiod](#)  
[\(config-keepalive\) suspend](#)  
[\(config-keepalive\) tcp-close](#)  
[\(config-keepalive\) type](#)  
[\(config-keepalive\) uri](#)

### Keepalive Configuration Mode Commands

Keepalive configuration mode allows you to configure keepalive properties and apply them to any service. Global keepalives reduce the amount of configuration required for each service. You can apply the keepalive configuration to multiple services. Global keepalives are independent of service mode.



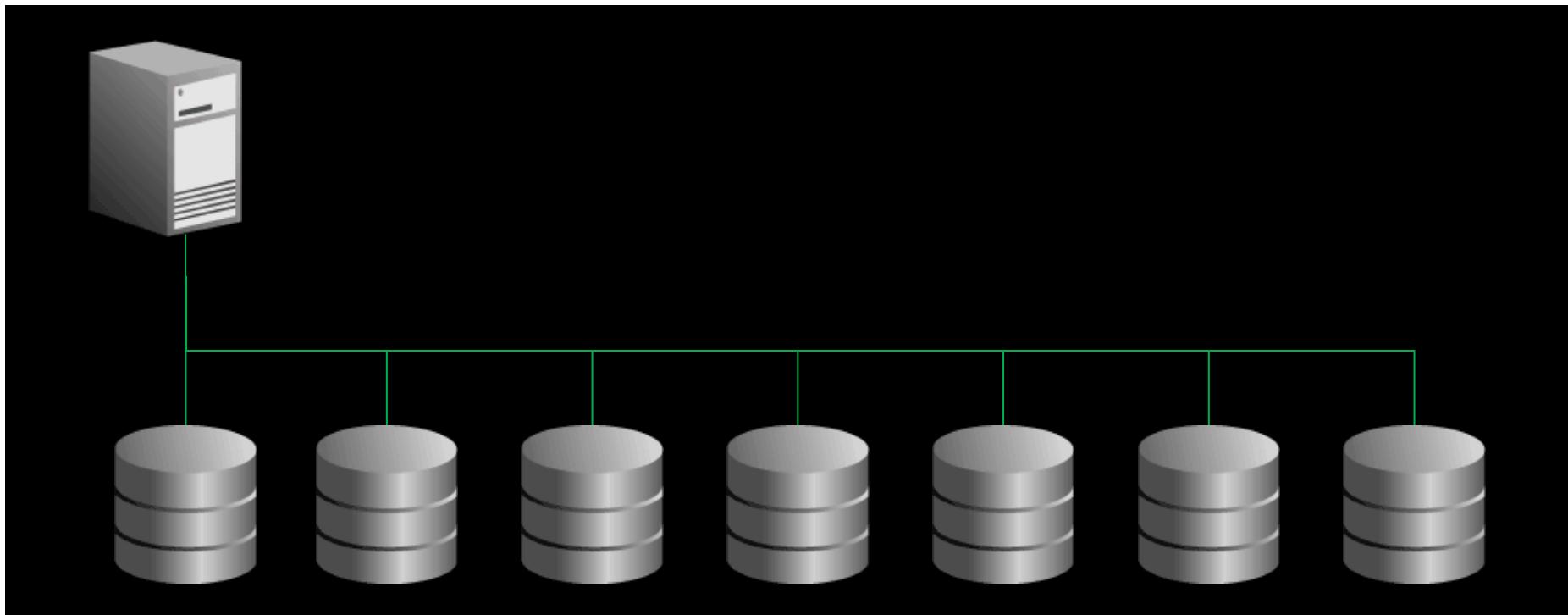
# Storage (1:2)

- Every Oracle Database deployment requires far more thought than just assigning a specified number of GB or TB to a LUN or Disk Group
- Let's explore some of those considerations
  - Amount of physical space that must be allocated at the time of deployment
  - The anticipated growth/shrinkage of the space requirement over time
  - The type of storage to be used: DASD, SAN, NAS
  - The speed and type of storage media
  - If shared storage the other storage tenants and their load profiles
  - File system or ASM
    - If a file system ... which one?
  - Will thin or thick provisioning be used?
  - Will "Snap & Clone" capabilities be in use?
  - Will storage device be encryption utilized?
  - Will storage device compression be utilized?
  - Will Direct and/or Asynch I/O be used?
  - The tool(s) that will be used to allocate and manage database storage



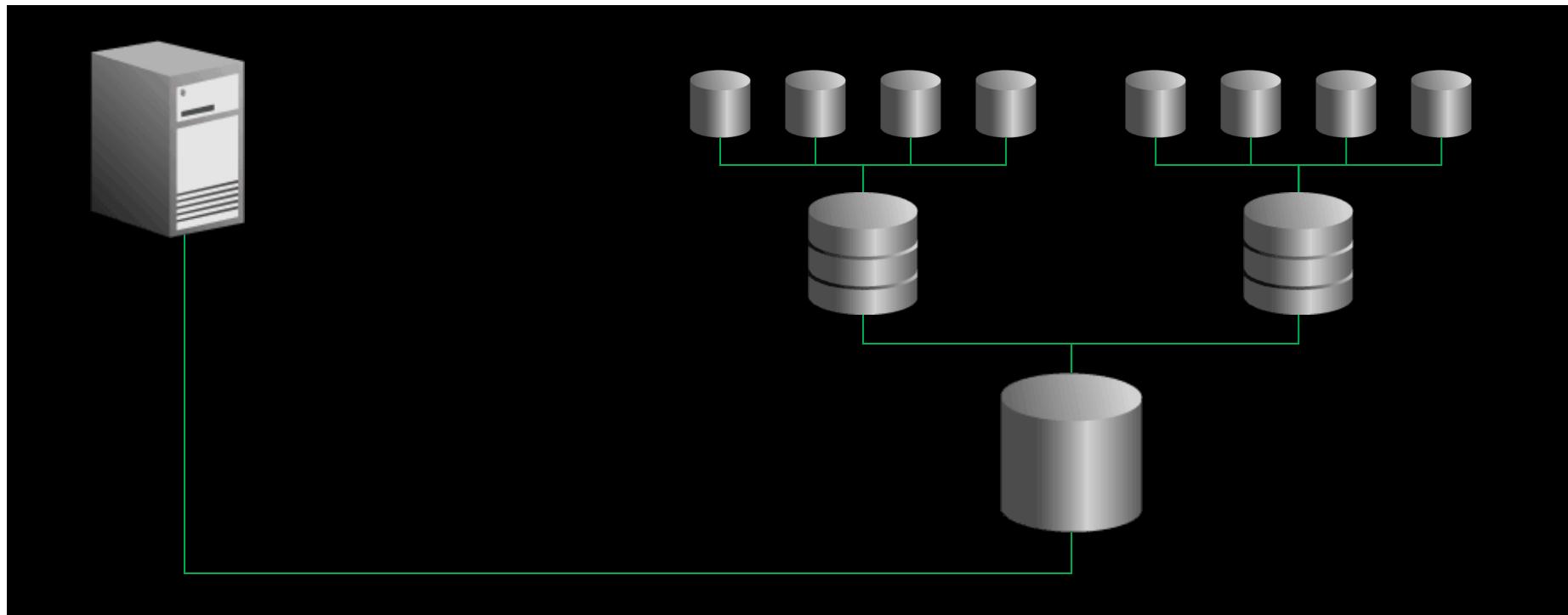
# Direct Attached Storage (DASD / JBOD)

- Drive directly attached via copper SCSI, Fibre SCSI, or infiniBand
- Least expensive and least flexible storage



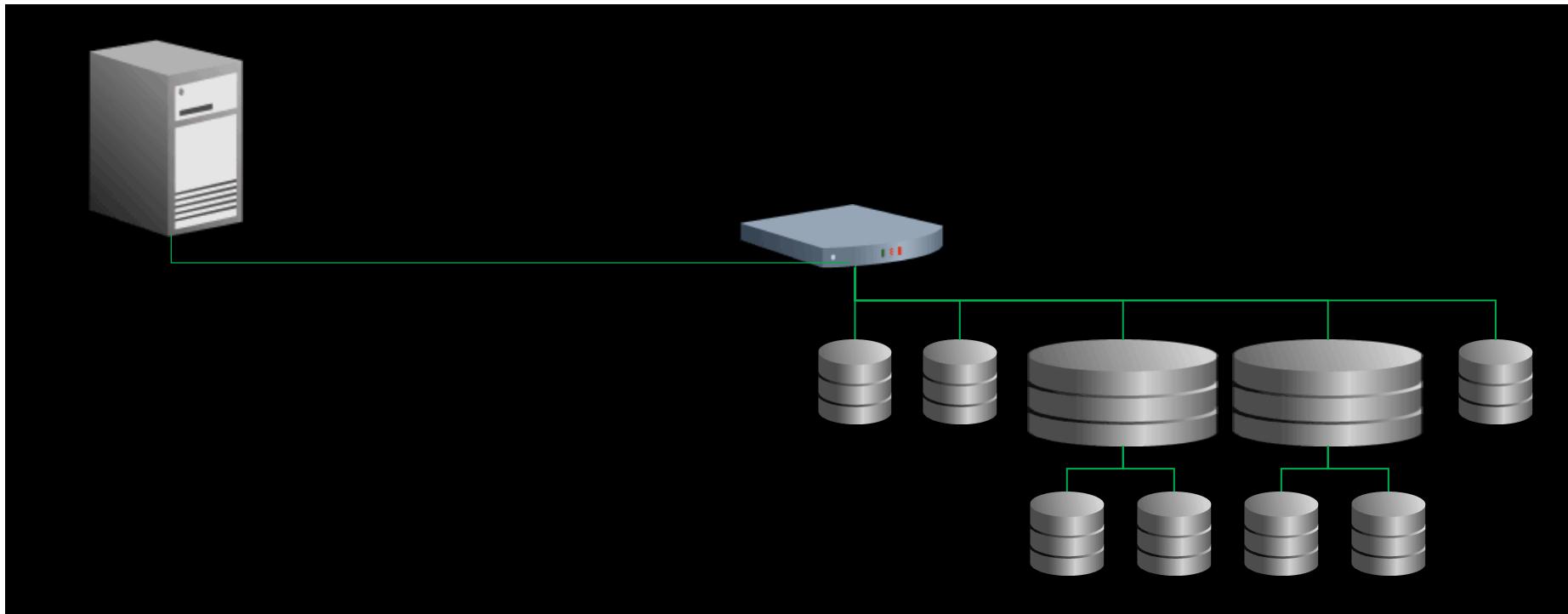
# Network Attached Storage (NAS)

- Separate devices attached to servers by TCP/IP Network or infiniBand
- Simple and Flexible



# Storage Area Network (SAN)

- Requires HBA (Host Bus Adapters) in each server
- Requires fabric switches
- Most expensive approach



# Storage (2:2)

- The following is strongly recommended
  - DASD ... this is what all high-performance engineered systems choose ...it is fastest and least expensive
  - Do not share storage with non-Oracle database loads
  - Purchase a mixture of drive types: Solid State, High Performance, and High Capacity with storage tiering so that the fastest and most expensive storage is allocated where required and the least expensive storage is utilized for legacy data
    - Be sure you understand how to utilize Oracle Automatic Data Optimization (ADO), Heap Maps, and Partitioning
  - Use thin provisioning ONLY it will be utilized to allow for dynamic space allocation
    - Never use thin provisioning for the purpose of allocating a single volume of space in a way that, in effect, pretends more space exists than is real
  - Use ASM
  - Do not use Snap & Clone ... replicates valid or corrupt blocks at the same high speed
  - Do not utilize hardware-based storage compression
  - Carefully test all scenarios before utilizing hardware-based storage encryption



# Servers

- Blades are not an appropriate infrastructure for Oracle Databases
- Blades are an unstable infrastructure for Oracle RAC
- What matters most in choosing servers
  - Component quality
  - Bus speed
  - Sufficient cpu cores and threads
  - A chipset that includes Oracle Database routines burned into the silicon
  - Sufficient memory
  - SNMP vs NUMA architecture
  - Slots sufficient to allow for redundant communications to all networks
  - Redundant power supplies
  - Hot-swappable components
  - A support organization that has a solid track-record supporting Oracle databases



# Virtualized Environments & Operating Systems



- Reasons for VMs
  - Create protected environments
  - Run multiple operating system environments on the same physical server
  - Leverage hardware models such as "Capacity on Demand" and "Pay as you Grow"
  - Control resource allocation
    - Manage processor allocation between platforms and users
  - Control licensing costs
    - Two types of partitioning
      - Soft Partitioning
        - Virtually segments a server
        - Not recognized by Oracle Database licensing
      - Hard Partitioning
        - Physically segments a server
        - Recognized by Oracle Database licensing



# Virtualized Environments (2:3)

OEM	Product	Description	License Recognition
Apache	Docker	Container ... both IBM and Oracle are making big investments into this technology	Not Determined
Fujitsu	PPAR		Yes
IBM	DLPAR	Container	Yes
IBM	Integrity Virtual Machine		Yes
IBM	LPAR		Yes
IBM	Micro-partitions	Capped Partitions only	Yes
IBM	nPar		Yes
IBM	Power VM Live		No
IBM	Secure Resource Partitions	Capped Partitions only	Yes
IBM	vPar	Container	Yes
Microsoft	Virtual PC	Hosted Virtualization	No
Oracle	Solaris Containers	Container	Yes
Oracle	Solaris LDOM	Container	Yes
Oracle	Solaris Zones	Container: Hard Partitions only	Yes
Oracle	Virtual Machine	Bare Metal Virtualization: Soft Partitioned	No
Oracle	Virtual Machine	Bare Metal Virtualization: Hard Partitions only	Yes
VMWare	ESX	Bare Metal Virtualization	No
VMWare	Workstation	Hosted Virtualization	No



- Reasons to NOT use VMs
- Oracle always recognizes hard partitioning
- Oracle never recognizes soft partitioning
  - Even when the soft partitioning is done with its own products like OVM and Solaris
- It is not Oracle's problem that VMware does not provide hard partitioning
- It is not Oracle's problem that some people selling soft partitioning either don't understand the difference or don't have an issue misrepresenting their products to their customers
- All partitioning
  - Reduce available memory
  - Reduces available cpu
  - Increases complexity
  - May remove Oracle optimizations that talk directly to hardware such as ASM, Asynch I/O, Direct I/O, Compression on Silicon, and Encryption on Silicon



# Friends don't let friends run Oracle Production Databases in VMware

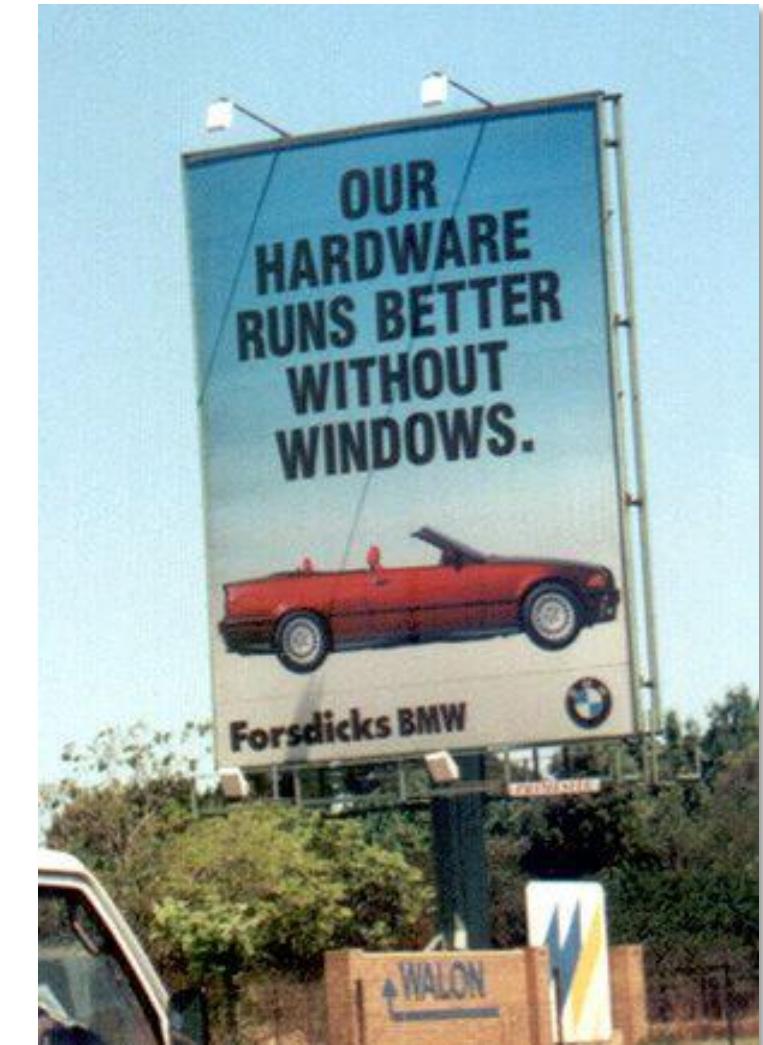


- What you lose with VMware
  - Optimizations wherein Oracle bypasses the O/S and talks directly to hardware
  - Oracle database code written into silicon
  - cpu resources
  - ASM
  - \$



# Operating Systems

- AIX
  - Vendor lock-in to IBM P-Series servers and IBM support
  - Best traditional virtualization architecture: LPAR
  - Solid memory management
- Linux
  - No vendor lock-in
  - Solid memory management
- Solaris
  - Vendor lock-in to Oracle Sun Sparc servers and Oracle support (not a bad thing)
  - Extremely good virtualization architecture: LDOM, Containers
  - Solid memory management
- Windows
  - Seriously?



# Operating Systems Environment

- The remaining slides in this section cover the details of properly configuring your environment and will not be covered in this presentation
- HugePages
- Name Resolution and DNS Caching
  - /etc/nscd.conf
  - /etc/resolv.conf
- TCP/IP network optimizations
- NUMA architecture
- swappiness
- /etc/hosts
- /etc/profile
- /etc/sysctl.conf
- /etc/security/limits
- STIGs
- Creating GROUPS and USERS
- bash environment
- installation directory structure
  - GRID\_BASE
  - ORACLE\_BASE
  - ORACLI\_BASE



- For Oracle Databases, using HugePages reduces the operating system maintenance of page states, and increases the Translation Lookaside Buffer (TLB) hit ratio
- Enabling HugePages makes it possible for the operating system to support memory pages greater than the default (usually 4KB)
- Using very large page sizes can improve system performance by reducing the amount of system resources required to access page table entries

## Advantages of configuring HugePages

- Page size is set to 2MB: substantially larger than 4K
- Memory is locked and cannot be paged out
- When using HugePages the entire SGA must fit within the HugePage allocation

```
cat /proc/meminfo |grep HugePages
HugePages_Total:      0
HugePages_Free:       0
HugePages_Rsvd:       0
HugePages_Surp:       0
Hugepagesize:        2048 kB
```



## HugePages (2:3)

- The first step in allocating HugePages to use the following formula to calculate the `vm.nr_hugepages` kernel parameter which is a value large enough to hold all SGAs

`[Desired HugePage Allocation/2,048,000 = [Number of Pages to Allocate]]`

- So, for example on an ODA Oracle allocates 96GB to HugePages

`16 * 1,024,000,000 = 98,304,000,000 bytes`  
`98,304,000,000 / 2,048,000 = 48,000 pages`

- To set 48,000 pages edit `/etc/sysctl.conf` so it includes the following line

`vm.nr_hugepages=48000`

then reboot the operating system and verify configuration (see next slide)

- If using Oracle 11g AMM must be disabled (which you should do anyway)
- If SGA sizing is dynamic the number of HugePages must reflect that maximum size to which the SGA, or a total of all SGAs, can grow

Note: Oracle provides code for performing the calculation at: [https://docs.oracle.com/cd/E37670\\_01/E37355/html/o1\\_config\\_hugepages.html](https://docs.oracle.com/cd/E37670_01/E37355/html/o1_config_hugepages.html)



## HugePages (3:3)

- The oracle userid needs to be reconfigured to enable it to lock a greater amount of memory which is done in /etc/security/limits.conf

```
oracle soft memlock 12582912
oracle hard memlock 12582912
```

- Verifying HugePage allocation on an ODA can return the following and you should see something similar on your system

```
cat /proc/meminfo |grep HugePages
HugePages_Total: 26000
HugePages_Free: 24183
HugePages_Rsvd: 6376
HugePages_Surp: 0
Hugepagesize: 2048 kB
```



# Name Resolution and DNS Caching

- When DNS caching is enabled DNS look-up results are cached in the operating system so that future requests can leverage the cached information and do not have to hit DNS resources, with the attendant delay to resolve names
- On Linux (and probably most Unix), there is no OS-level DNS caching unless `nscd` is installed and running
- `nscd` is a daemon that provides a cache for the most common name service requests and watch for changes in configuration files appropriate including `/etc/passwd`, `/etc/hosts`, and `/etc/resolv.conf`
- There are two caches
  - a positive one for items found
  - a negative one for items not found
- Each cache has a separate TTL (time-to-live) period for its data
- The default configuration file, `/etc/nscd.conf`, determines cache daemon behavior



- Out of the box

```
$ grep hosts /etc/nscd.conf
  enable-cache hosts yes
  positive-time-to-live hosts 0
  negative-time-to-live hosts 0
  keep-hot-count hosts 20
  check-files hosts yes
```

```
$ nscd -g
CACHE: hosts

CONFIG:
  enabled: yes
  per user cache: no
  avoid name service: no
  check file: yes
  check file interval: 0
  positive ttl: 0
  negative ttl: 0
  keep hot count: 20
  hint size: 2048
  max entries: 0 (unlimited)

STATISTICS:
  positive hits: 0
  negative hits: 0
  positive misses: 0
  negative misses: 0
  total entries: 0
  queries queued: 0
  queries dropped: 0
  cache invalidations: 0
  cache hit rate: 0.0
```



- After cache configuration

```
$ grep hosts /etc/nscd.conf
  enable-cache hosts yes
  positive-time-to-live hosts 60
  negative-time-to-live hosts 60
  keep-hot-count hosts 20
  check-files hosts yes
```

```
$ nscd -g
CACHE: hosts

CONFIG:
  enabled: yes
  per user cache: no
  avoid name service: no
  check file: yes
  check file interval: 0
  positive ttl: 60
  negative ttl: 0
  keep hot count: 20
  hint size: 2048
  max entries: 0 (unlimited)

STATISTICS:
  positive hits: 143
  negative hits: 1
  positive misses: 20
  negative misses: 41
  total entries: 20
  queries queued: 0
  queries dropped: 0
  cache invalidations: 0
  cache hit rate: 70.2
```

- Enabling a 60 sec. cache reduced DNS lookup by 70%



# /etc/resolv.conf

- An improperly configured resolv.conf file can result in everything from poor performance to an inability to connect making the database inaccessible
- The first resolv.conf example created a near outage condition at a SaaS Cloud provider

```
search morgan.priv
nameserver 10.24.244.200
nameserver 10.24.244.21 (Bind server 01)
nameserver 10.24.244.25 (Bind server 02)
nameserver 10.24.244.29 (Bind server 03)
```

- What belongs in every resolv.conf file

Parameter	Description
attempts	The number of times the resolver will send a query to its name servers before returning an error
rotate	Forces round-robin selection of name servers to spread the query load among all listed servers,
timeout	The number of seconds the resolver will wait for a response from a remote name server before retrying the query via a different name server

- Performance optimized

```
search morgan.priv
nameserver 10.24.244.21 (Bind server 01)
nameserver 10.24.244.25 (Bind server 02)
nameserver 10.24.244.29 (Bind server 03)
option attempts:2
option rotate
option timeout:1
```



# Networks: TCP/IP

- The following do not appear to be critical in Linux 6 or above but in Linux 5 are clearly part of a discussion that should be had with your network and system admins

```
--enable TCP kernel auto-tuning
/proc/sys/net/ipv4/tcp_moderate_rcvbuf (1=on)

-- tune TCP max memory: tune to 2xBDP (Bandwidth x Delay Product)
-- For example, with 40 Mbits/sec bandwidth, 25 msec delay,
-- BDP = (40 x 1000 / 8 Kbytes/sec) x (0.025 sec) ~ 128 Kbytes
/proc/sys/net/ipv4/tcp_rmem 4096 87380 174760
/proc/sys/net/ipv4/tcp_wmem 4096 87380 174760

-- tune the socket buffer sizes by setting to 2xBDP
/proc/sys/net/core/rmem_max
/proc/sys/net/core/wmem_max

-- ensure that TCP Performance features are enabled (set to 1)
/proc/sys/net/ipv4/tcp_sack (to set sysctl -w net.ipv4.tcp_sack=1)
/proc/sys/net/ipv4/tcp_window_scaling
/proc/sys/net/ipv4/tcp_timestamps
```



# Networks: UDP

- Bandwidth-delay product is the product of network bandwidth and the round trip time of data going over the network
- To determine the round trip time, is to use a command such as ping from one host to another and use the response times returned by ping
- For example, if a network has a bandwidth of 100 Mbps and a round trip time of 5ms, then the send and receive buffers should be at least  $(100*10^6) * (5/10^3)$  bits or approximately 62.5 Kilobytes
- The following equation shows the relationships between the units and factors involved

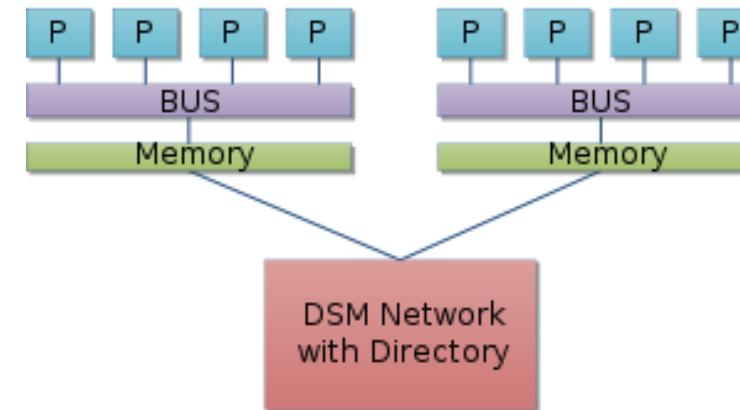
$$\frac{100,000,000 \text{ bits}}{1 \text{ second}} \times \frac{1 \text{ byte}}{8 \text{ bits}} \times \frac{5 \text{ seconds}}{1000} = 62,500 \text{ bytes}$$



# NUMA Memory Allocation

## ■ Non-Uniform Memory Access

- A memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor
- A processor can access its own local memory faster than non-local memory
- The benefits of NUMA are limited to particular workloads, notably on servers where the data are often associated strongly with certain tasks or users



- Oracle recommends disabling NUMA at the hardware level: System Admins don't
- If VM's are in use they too must be NUMA aware

Diagram Source: Wikipedia



# NUMA Usage Detection

```
[root@hclpl-oda01 etc]# numactl --hardware
available: 1 nodes (0)
node 0 size: 262086 MB
node 0 free: 113558 MB
node distances:
node 0
 0: 10
```

```
[root@hclpl-oda01 etc]# numactl --show
policy: default
preferred node: current
physcpubind: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41
42 43 44 45 46 47
cpubind: 0
nodebind: 0
membind: 0
```

NUMA Not Configured on an ODA

```
[dmorgan@lxorap1n5 ~]$ numactl --hardware
available: 2 nodes (0-1)
node 0 size: 48457 MB
node 0 free: 269 MB
node 1 size: 48480 MB
node 1 free: 47 MB
node distances:
node 0 1
 0: 10 20
 1: 20 10
```

```
[dmorgan@lxorap1n5 ~]$ numactl --show
policy: default
preferred node: current
physcpubind: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
cpubind: 0 1
nodebind: 0 1
membind: 0 1
```

NUMA Configured



# Swappiness

- Specifies a bias value for the kernel to swap out memory pages used by processes in the cgroup rather than reclaim pages from the page cache
- A value smaller than the default value of 60 reduces the kernel's preference for swapping out
- A value greater than 60 increases the preference for swapping out
- A value greater than 100 allows the system to swap out pages that fall within the address space of the cgroup's tasks

Value	Swapping Strategy
0	The kernel will swap only to avoid an out of memory condition
60	The default value
100	The kernel will swap aggressively



# /etc/hosts

- As a server boots it needs to know the mapping of some hostnames to IP addresses before DNS can be referenced
- The mapping is kept in the **/etc/hosts** file
- In the absence of a name server, a network program on your system consults this file to determine the IP address that corresponds to a host name
- Be sure that the file does not contain any mappings that are not essential ... unnecessary mappings compromise security

```
# Do not remove the following line, or various programs that require network functionality will fail.
::1 localhost6.localdomain6 localhost6

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.16 orclsys-scan.example.com orclsys-scan

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan

# Following added by OneCommand
127.0.0.1 localhost.localdomain localhost

# PUBLIC HOSTNAMES

# PRIVATE HOSTNAMES
192.168.16.24 orclsys1-priv0.example.com orclsys1-priv0
192.168.16.25 orclsys2-priv0.example.com orclsys2-priv0
192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

# VIP HOSTNAMES
192.0.2.20 orclsys1-vip.example.com orclsys1-vip
192.0.2.21 orclsys2-vip.example.com orclsys2-vip

# NET(0-3) HOSTNAMES
192.0.2.18 orclsys1.example.com orclsys1
192.0.2.19 orclsys2.example.com orclsys2

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan
```



## /etc/profile

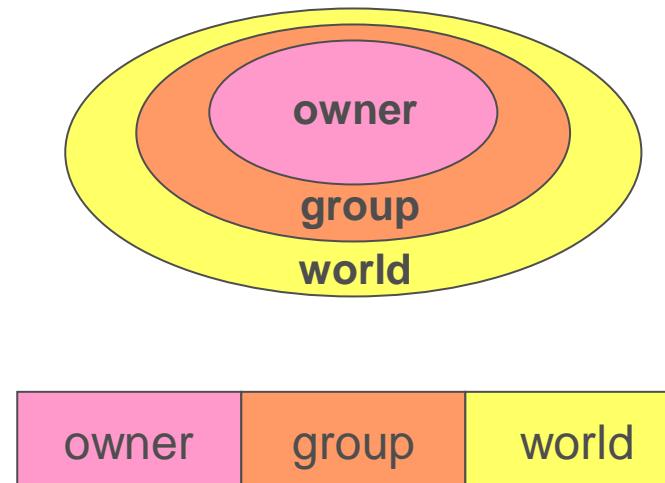
- The shell program `/bin/bash` uses a collection of startup files to help create the environment
- Each file has a specific use and may affect login and interactive environments differently
- The files in the `/etc` directory generally provide global settings
- If an equivalent file exists in a home directory it may override the global settings
- An interactive login shell is started after a successful login, using `/bin/login`, by reading the `/etc/passwd` file
- This bash shell invocation normally reads `/etc/profile` and its private equivalent `~/.bash_profile` upon startup
- `ulimit` controls the maximum number of processes a user is authorized to have
- `umask` controls the permission on newly created files and is the inverse of `chmod (133 = 644)`

```
cat >> /etc/profile <<EOF
if [ $USER = "oracle" ] ; then
  ulimit -u 16384 -n 65536
  umask 133
fi
EOF
```



# umask

- Clearly the greatest security comes from using the lowest possible permission value and for an optimized installation that means no more permissive than 644
- There is literally no excuse for anything in the oracle file system being executable by "world"



Value	Result
111	- - - x - x - x
222	- - w - w - w
333	- - w x - w x - w x
444	- r - r - r - -
555	- r - x r - x r - x
666	- r w - r w - r w -
777	- r w x r w x r w x -
124	- - - x - w - r - -
644	- - - w r - - r - -
755	- r w x r - x r - x



- The overwhelming majority of Oracle Database's are not configured in accordance with documented recommendations
- Here are those recommendations for version 12.1 with common errors in red

Parameter	Value
semmsl	250
semmns	32000
semopm	100
semmni	128
shmall	50 percent of the size of physical memory in pages
shmmmax	Half the size of physical memory in bytes. See My Oracle Support Note 567506.1 for additional information about configuring
shmmni	4096
panic-on-oops	1
file-max	(512 * processes) + open O/S file handles but not less than 6815744
aio-max-nr	fs.aio-max-nr = 1048576
ip_local_port_range	net.ipv4.ip_local_port_range = 9000 65500
rmem_default	262144
rmem_max	4194304
wmem_default	262144
wmem_max	1048576



- FS.FILE-MAX

- Far too often I see this configured as follows:

```
fs.file-max = 6815744
```

- But here's what the docs actually say:

- "Oracle recommends that for each Oracle database instance found within a system, allocate **512\*PROCESSES** in addition to the open file handles already assigned to the operating system"
    - "Oracle recommends a value no smaller than 6815744"
    - "PROCESSES within a database instance refers to the maximum number of processes that can be concurrently connected to the Oracle database by the oracle user"
      - The default value for processes is 300 but is not an indication that processes in your production rdbms will require no optimizations that could change this value
      - Thus if more than one database is installed on your server the number may need to be adjusted
      - If you have deployed 12c RAC, by definition, you have the ASM instance and \_MGMTDB management database too so minimum processes going to be substantially higher than 300



- FS.FILE-MAX
  - The configuration from my Windows laptop deployment of 12.1.0.2

```
--the output from my Windows laptop
SQL> show parameter processes
```

NAME	TYPE	VALUE
aq_tm_processes	integer	1
db_writer_processes	integer	1
gcs_server_processes	integer	0
global_txn_processes	integer	1
job_queue_processes	integer	1000
log_archive_max_processes	integer	4
processes	integer	300



- So let's do the math for the following
  - Oracle Database with 800 processes
  - RAC management database with 300 processes
  - ASM instances with 600 processes
  - Linux with a reasonable number of Default Linux Processes: 173

$$(512 * (800+300+600) + 173 = 870573)$$

- 870,573 is a small fraction of 6,814,744 so unless you are running a very large number of databases, or other applications, the default value should be acceptable
- But if you are consolidating multiple instances onto a single platform the default number may be inadequate ... do the math



- SHMALL
  - By definition SHMALL specifies "... the total amount of shared memory, in pages, that the system can use at one time."
  - And should be set as follows " half the size of physical memory in pages"
  - On a system 96GB RAM and HugePages defined the correct value should be 24000
    - Substantially smaller than the number often used which is 2097152 for far less RAM
- SHMMAX
  - Essentially everyone puts in what Oracle calls the maximum possible value which is 4294967295 ignoring the documentation: Do the calculation and put in the correct value
  - Here is what Oracle advises in MOS Document "**Maximum SHMMAX values for Linux x86 and x86-64**" (**Doc ID 567506.1**)

In an Oracle RDBMS application, **this "physical limit" still leaves inadequate system memory for other necessary functions**. Therefore, the common "Oracle maximum" for SHMMAX that you will often see is "1/2 of physical RAM".

- PANIC-ON-OOPS
  - This is a new parameter with Database 12cR1 ... be sure it is set

```
kernel.panic_on_oops = 1
```



- **limits.conf** is the configuration file for the pam\_limits module
- The pam\_limit module applies ulimits limits, nice priority, and number of simultaneous login session limits to user login sessions
- Entries with "hard" enforce hard resource limits which are limits set by the superuser and enforced by the Kernel
  - The user cannot raise his requirement of system resources above such values
- Entries with "soft" enforce soft resource limits which are limits that the user can move up or down within the range permitted by any pre-existing hard limits



- The following limits parameters are new with Database 12c
  - ORACLE SOFT STACK  
At least 10240
  - ORACLE HARD STACK  
At least 10240 but not more than 32768KB
  - MEMLOCK SOFT  
At least 90% of the current memory RAM when HugePages memory is enabled but less than the amount of installed memory: Oracle demos use 92%
  - MEMLOCK HARD  
At least 90% of the current memory RAM when HugePages memory is enabled but less than the amount of installed memory: Oracle demos use 92%
  - Assuming 96GB RAM

```
oracle soft nofile 1024
oracle hard nofile 65536
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft stack 10240
oracle hard stack 10240
oracle soft memlock 90439680
oracle hard memlock 90439680
```



- A STIG is a **Security Technical Implementation Guide** produced or approved by the US Department of Defense
- Oracle Support provides downloadable scripts that can be used to check an for STIG compliance and report three levels of violations
- We strongly recommend running the most appropriate STIG script with the **-check** option and recommend having your security and admin teams identify issues to be corrected and that modifications be made manually rather than running with the **-fix** option: The **-fix** option's "fix" may be more extreme than you expect



The screenshot shows a web browser window for Oracle My Oracle Support. The URL is [https://support.oracle.com/epmos/faces/SearchDocDisplay?\\_adf.ctrl-state=8gv63d6pu\\_98\\_afrLoop=44873298819788](https://support.oracle.com/epmos/faces/SearchDocDisplay?_adf.ctrl-state=8gv63d6pu_98_afrLoop=44873298819788). The page title is "Document Display". The main content is about the "STIG Implementation Script for Oracle Database Appliance (Doc ID 1461102.1)".

**APPLIES TO:**

Oracle Database Appliance - Version All Versions and later  
Oracle Database Appliance Software - Version 2.2.0.0 to 12.1.2.4 [Release 2.2 to 12.1]  
Linux x86-64

**GOAL**

The ODA STIG script provides prescriptive steps that can be used to both assess and improve the security configuration of the Oracle Database Appliance. This script is based on the Oracle Linux 5 Security Technical Implementation Guide (STIG) that can be found at <http://iae.disa.mil>.

For more information Please contact [tammy.bednar@oracle.com](mailto:tammy.bednar@oracle.com)

**SOLUTION**

Download the latest STIG script>

**Document Details**

- Type: HOWTO
- Status: REVIEWED
- Last Major Update: Sep 11, 2015
- Update: Sep 11, 2015
- Last Update:

**Related Products**

- Oracle Database Appliance Software
- Oracle Database Appliance

**Information Centers**

- Information Center: Oracle Database Appliance [1417713.2]



## Features

- Works on Oracle Database Appliance Bare Metal and Virtualized platform(Execution of the script from ODA\_BASE only)
- Works on X5-2, X4-2, X3-2 & V1 platforms

## Usage

- Download the script and execute it as root. Sample usage scenarios are documented below
- The script logs its actions in the "/opt/oracle/oak/log/<hostname>/stig/stig.log" file
- The option -check is used to check the system for any violation of the guidelines
- The option -force is used to re-run the script even if there are no violations
- The option -fix is used to implement the guidelines
- The enable and disable option can be used to enable or disable direct ssh logging as root. Direct ssh login as root is required for Patching and therefore before patching, the unlock needs to be executed.
- Once a violation has been fixed, it cannot be automatically rolled back to a previous state.

## Sample usage

```
./stig.py -h
```

Usage for STIG (Security Technical Implementation Guide):



STIG checks and corrects violations within Oracle Database Appliance

<First Parameter> : -h | -? | -help | -v | -V | -version | check | fix | enable | disable

<Second Parameter> : all | force | perm | conf | account | access | grub | audit

Example : ./stig.py <First Parameter> <Second Parameter>

STIG script Parameter Information:

---

-h : Provides information regarding STIG scripts

-v : Provides STIG script version information

enable : Enables direct ssh root login on the system

disable : Disables direct ssh root login on the system

check : Checks and lists the STIG violations on the system

check -h : Provides options help available with check

fix : Fixes or Corrects the STIG violations reported on the system

fix -h : Provides options help available with fix

---



- Typical Level 1 Violations
  - Ctrl-Alt-Del combination to shutdown system is enabled
  - Password for grub not enabled
  - Privilege account 'halt' is present
  - Privilege account 'shutdown' is present
  - RealVNC rpm is installed on system
  - sendmail decode command is not commented in /etc/aliases
  - Support for USB device found in kernel



- Typical Level 2 Violations
  - Access to cron is not through cron.allow and cron.deny
  - ekshell supported by the pam.rhost
  - Force of at least one lower case character is not set for password
  - FAIL\_DELAY is not present in /etc/login.defs
  - Login delay is not enabled in /etc/pam.d/system-auth
  - Maximum age for a password change is more than 60 days
  - Non privileged account oprofile found on system
  - Non privileged account avahi-autoipd found on system
  - pam\_tally not used to lock account after 3 consecutive failed logins
  - Password can be changed more than once in 24 hours
  - Remember not used in PAM configuration files
  - Permission of directory /root is more permissive than octal 700
  - Files in directory '/etc/xinetd.d/' have permission which are more permissive than octal 440
  - Unnecessary account games found on system



- Typical Level 3 Violations
  - 9330 manual pages in directory '/usr/share/man/' have permission which are more permissive than octal 640
  - Permission of directory /home/grid/.mozilla/extensions is more permissive than octal 750
  - Permission of directory /home/grid/.mozilla/plugins is more permissive than octal 750
  - Permission of directory /home/oracle/.mozilla/extensions is more permissive than octal 750
  - Permission of directory /home/oracle/.mozilla/plugins is more permissive than octal 750
  - sendmail version is not hidden



# Groups and Users (1:2)

- Essentially 100% of all database installations get this wrong
- Why?
- Because they follow the Oracle docs
- So let's get it right
- Here's what Oracle recommends

```
/usr/sbin/groupadd -g 490 oinstall (54321 default with validated OEL package)
/usr/sbin/groupadd -g 491 dba
/usr/sbin/groupadd -g 492 oper
/usr/sbin/groupadd -g 493 backupdba
/usr/sbin/groupadd -g 494 dgdba
/usr/sbin/groupadd -g 495 kmdba

/usr/sbin/useradd -u 500 -m -g oinstall -G dba,oper oracle
id oracle

-- set the password to oracle1
passwd oracle
```



# Groups and Users (2:2)

- What's wrong with Oracle's recommendation?
- It enables a gross violation of basic security principles ... separation of duties
- If someone logs into the server as the user `oracle` they own everything under `$ORACLE_BASE`
- Create a separate group and user that will allow you to manage the database, and provide vendor access, without compromising the `$ORACLE_BASE` file system

```
/usr/sbin/groupadd -g 490 oinstall (54321 default with validated OEL package)
/usr/sbin/groupadd -g 491 dba
/usr/sbin/groupadd -g 492 oper
/usr/sbin/groupadd -g 493 backupdba
/usr/sbin/groupadd -g 494 dgdba
/usr/sbin/groupadd -g 495 kmdba
/usr/sbin/groupadd -g 496 cinstall

/usr/sbin/useradd -u 500 -m -g oinstall -G dba,oper oracle
id oracle
/usr/sbin/useradd -u 501 -m -g cinstall oracli
id oracli

-- set the passwords ... make them complex and different
passwd oracle
passwd oracli
```



# oracle BASH Environment (1:2)

- Unless you have multiple databases defined within a single operating system environment define as much of the bash shell as you can in one of two files located at `/home/oracle`
  - `.bash_profile`
    - executed for login shells
    - executed once for all terminal windows
  - `.bashrc`
    - executed for interactive non-login shells
    - executed every time you open a new terminal window
- Avoid duplicating shell information you can call `.bashrc` from `.bash_profile` as demonstrated

```
-- add the following lines to .bash_profile

if [ -f ~/.bashrc ]; then
  source ~/.bashrc
fi

-- .bashrc is called when you login to your machine from a console
```



# Directory Structure Creation

- Oracle Database Directories
  - If ASM and Oracle Clusterware will be installed create one additional file system owned by root for the installation
  - The \$GRID\_BASE directory structure can be built following Oracle's documented recommendations without compromising security
- Oracle Client Directories
  - Note that in addition to creating an entirely separate installation file system a separate staging directory is also created

```
mkdir -p /app/oracle
chown -R oracle:dba /app/oracle
chmod -R 775 /app/oracle
```

```
mkdir /stageo
chown -R oracle:dba /stageo
```

```
mkdir -p /cli/oracle
chown -R oracli:cinstall /cli/oracle
chmod -R 775 /cli/oracle
```

```
mkdir /stagec
chown -R oracli:cinstall /stagec
```

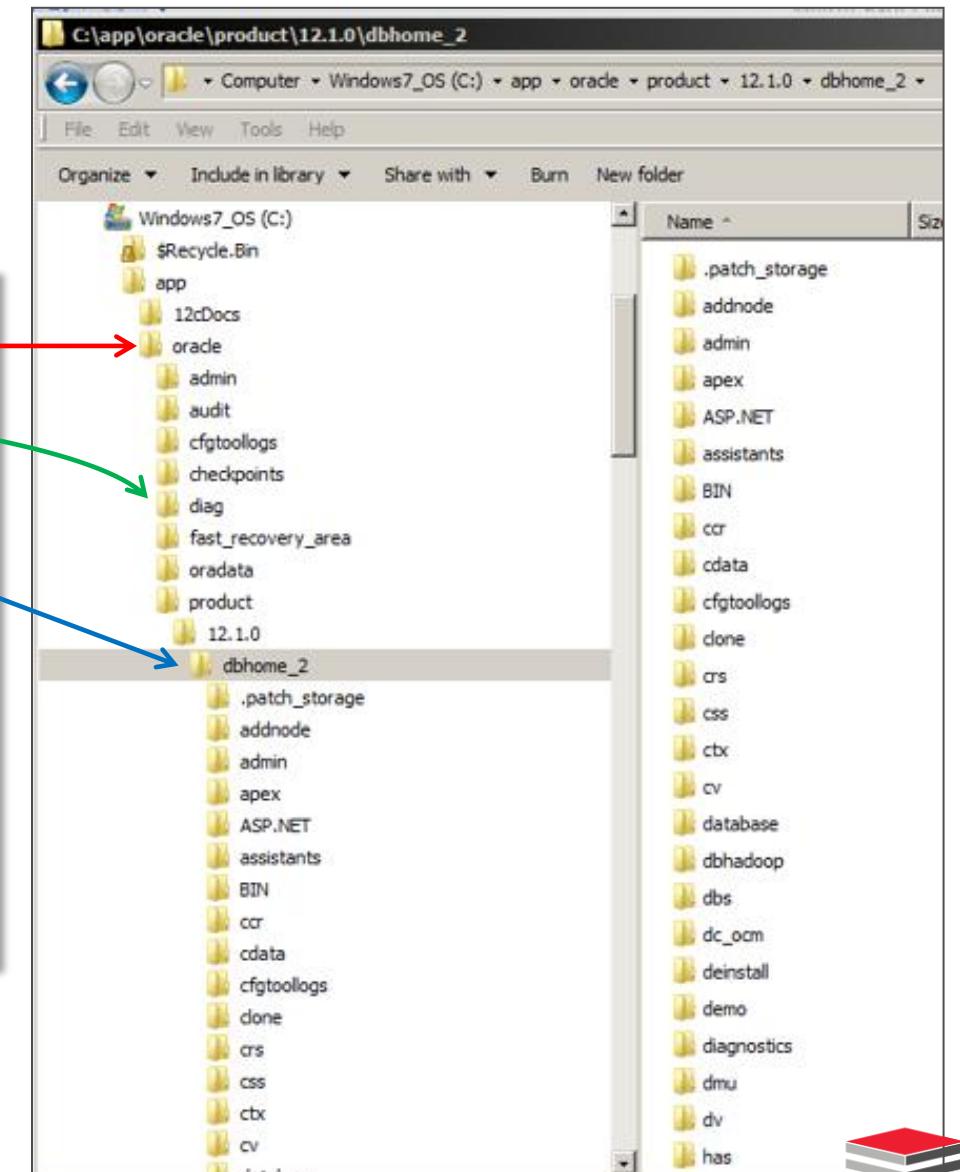


# oracle BASH Environment (2:2)

- The following is a typical .bashrc or .bash\_profile file for an Oracle 12c Database

```
ORACLE_HOSTNAME=alpha1.mlib.org
ORACLE_BASE=/app/oracle/product
ADR_HOME=/app/oracle/diag
ORACLE_HOME=/app/oracle/product/12.1.0/db_1
ORACLE_SID=orabase
LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
TMP=/tmp
TEMP=/tmp
TMPDIR=/tmp
PATH=$ORACLE_HOME/bin:$PATH
export PATH ORACLE_BASE ORACLE_HOME ADR_HOME
export ORACLE_SID LD_LIBRARY_PATH
export TMP TEMP TMPDIR

alias oh='cd $ORACLE_HOME'
```



# oracli BASH Environment

- The same rules apply to the owner of the Oracle Client software ... define the environment in either .bash\_profile or .bashrc being careful to create no overlaps that would compromise file system security

```
ORACLE_HOSTNAME=alpha1.mlib.org
ORACLI_BASE=/cli/oracle/product
ORACLI_HOME=/cli/oracle/product/12.1.0/db_1
ORACLE_SID=orabase
LD_LIBRARY_PATH=$ORACLI_HOME/lib:$LD_LIBRARY_PATH
TMP=/tmp
TEMP=/tmp
TMPDIR=/tmp
PATH=$ORACLI_HOME/bin:$PATH
export PATH ORACLI_BASE ORACLI_HOME
export ORACLE_SID LD_LIBRARY_PATH
export TMP TEMP TMPDIR

alias oh='cd $ORACLI_HOME'
```



# Database Installation



# OUI + DBCA

- Install Oracle Binaries
- FRA
  - Determine what is going to be written to the FRA
    - Redo log multiplexing
    - Archived redo logs
    - Backups
  - Does it need to have its own file system or ASM Disk Group?
- Control File multiplexing
  - By default OUI+DBCA puts all control file copies into the same location
- Redo log sizing and multiplexing
  - By default OUI+DBCA does not multiplex redo logs
  - Be sure that you create a second member in separate physical and logical locations
  - Be sure that you properly size your redo logs to perform a log switch every 5-15 minutes



# Redo Logs (1:4)

- The Oracle installer has not been informed of another critically important configuration issue: Redo logs need to be multiplexed and appropriately sized
- By default the installer creates three redo groups but with only one member each
  - Lose the CURRENT redo log and your database is toast
  - Lose the ACTIVE redo log and your database is toast
  - In both cases you will have an unrecoverable loss of data
  - Lose the INACTIVE redo log and your database will halt
- Does any of the above sound like "best practice?"
- Does any of the above sound like "unbreakable?"
- Does any of the above sound like an outage lurking in the data center?



# Redo Logs (2:4)

- Multiplex redo logs to separate physical disk

```
SQL> SELECT member FROM v$logfile;

MEMBER
-----
/app/oracle/fast_recovery_area_orabase/redo01A.log
/app/oracle/fast_recovery_area_orabase/redo02A.log
/app/oracle/fast_recovery_area_orabase/redo03A.log

6 rows selected.

SQL> ALTER DATABASE ADD LOGFILE MEMBER '/app/oracle/dbs/log1b.log' TO GROUP 1;

SQL> ALTER DATABASE ADD LOGFILE MEMBER '/app/oracle/dbs/log2b.log' TO GROUP 2;

SQL> ALTER DATABASE ADD LOGFILE MEMBER '/app/oracle/dbs/log3b.log' TO GROUP 3;

SQL> SELECT member FROM v$logfile;

MEMBER
-----
/app/oracle/fast_recovery_area_orabase/redo01A.log
/app/oracle/fast_recovery_area_orabase/redo02A.log
/app/oracle/fast_recovery_area_orabase/redo03A.log
/app/oracle/oradata/orabase/redo01B.log
/app/oracle/oradata/orabase/redo02B.log
/app/oracle/oradata/orabase/redo03B.log
```



# Redo Logs (3:4)

- Monitor redo log switch frequency to identify high-risk activities

```
SELECT TO_CHAR(first_time, 'MMDD') MMDD,
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '00', 1, 0)), '99') "00",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '01', 1, 0)), '99') "01",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '02', 1, 0)), '99') "02",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '03', 1, 0)), '99') "03",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '04', 1, 0)), '99') "04",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '05', 1, 0)), '99') "05",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '06', 1, 0)), '99') "06",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '07', 1, 0)), '99') "07",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '08', 1, 0)), '99') "08",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '09', 1, 0)), '99') "09",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '10', 1, 0)), '99') "10",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '11', 1, 0)), '99') "11",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '12', 1, 0)), '99') "12",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '13', 1, 0)), '99') "13",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '14', 1, 0)), '99') "14",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '15', 1, 0)), '99') "15",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '16', 1, 0)), '99') "16",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '17', 1, 0)), '99') "17",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '18', 1, 0)), '99') "18",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '19', 1, 0)), '99') "19",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '20', 1, 0)), '99') "20",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '21', 1, 0)), '99') "21",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '22', 1, 0)), '99') "22",
       TO_CHAR(SUM(DECODE(TO_CHAR(first_time, 'HH24'), '23', 1, 0)), '99') "23"
  FROM v$log_history
 GROUP BY TO_CHAR(first_time, 'MMDD') ORDER BY 1;
```



# Redo Logs (4:4)

- Monitor redo log switch frequency to identify high-risk activities

MMDD	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0609	16	11	9	8	8	10	12	8	8	10	8	10	14	10	11	15	15	8	12	8	7	6	9	7
0610	13	12	8	9	7	6	11	9	6	8	7	8	12	6	7	6	8	7	10	7	4	4	4	5
0611	12	8	5	9	9	7	11	7	6	7	8	5	12	9	10	8	9	12	12	10	6	6	9	8
0612	13	12	7	9	7	9	10	10	7	7	9	8	11	7	7	8	7	7	11	9	5	6	8	7
0613	12	11	7	8	8	7	13	7	9	7	8	7	13	10	9	8	8	8	11	8	7	5	7	6
0614	15	10	9	9	8	9	13	9	9	7	11	13	11	9	8	9	13	9	12	9	7	9	7	7
0615	15	10	10	8	10	9	12	8	9	8	9	7	13	6	8	7	7	7	15	10	7	7	7	5
0616	13	8	8	7	7	6	10	8	11	7	8	6	11	7	12	13	13	14	13	9	9	9	7	8
0617	15	13	10	9	8	9	16	8	8	10	9	10	16	11	10	10	8	11	13	8	9	9	7	9
0618	12	13	15	15	13	13	15	13	9	12	8	11	14	9	10	9	9	8	14	9	8	8	9	8
0619	16	11	10	11	9	9	13	12	10	9	12	12	17	8	9	9	11	11	14	9	9	11	10	12
0620	19	15	11	10	10	10	19	11	9	9	9	9	13	7	15	10	11	11	12	10	9	11	11	10
0621	13	16	11	9	10	13	16	8	14	9	11	12	17	10	10	11	8	11	14	8	11	14	8	11
0622	16	13	13	11	11	9	16	9	9	11	10	11	17	10	9	10	10	10	13	14	9	10	10	8
0623	19	13	12	13	13	11	16	12	11	11	11	11	16	9	10	13	2	14	14	8	9	8	8	8
0624	14	9	9	9	7	9	11	8	8	7	8	8	14	7	8	7	9	3	6	0	0	0	0	0
...																								
0630	7	4	23	19	9	10	5	6	7	17	19	17	15	17	15	43	40	32	17	15	14	20	13	15
0701	15	12	14	12	13	12	13	17	15	17	20	20	18	18	17	15	14	13	10	10	15	15	13	19
0702	21	22	20	18	14	14	12	13	11	11	14	14	14	10	9	10	9	10	11	9	11	9	10	12
0703	9	13	10	17	14	17	15	17	23	20	19	20	17	19	16	17	15	17	15	15	15	16	16	18
0704	22	19	19	18	16	15	13	13	14	11	13	10	12	14	10	12	14	11	9	11	12	13	12	9
0705	14	13	9	11	10	12	13	11	11	8	10	10	11	11	11	12	10	10	9	10	8	9	12	7
0706	14	15	11	12	9	15	13	12	12	9	12	14	12	12	12	12	13	11	8	9	12	13	2	0
0707	0	0	1	0	3	15	10	10	7	8	10	11	12	8	6	9	13	12	9	8	9	8	10	10
0708	16	9	8	15	10	11	9	8	8	14	9	10	10	8	8	14	15	10	9	9	8	9	10	10
0709	13	12	9	10	10	9	9	10	11	11	8	9	9	8	9	13	8	9	6	9	9	11	10	9
0710	12	10	9	10	9	12	9	8	8	11	7	10	11	9	9	13	10	9	8	9	11	12	10	10



# Listener Configuration



# Oracle Listeners

- The first question with respect to listeners you must address is the number of listeners: Here are some of the important considerations
- Stand-alone database requires one local listener per O/S environment
- RAC databases require one Grid listener per O/S environment
- Data Guard best practices dictate two listeners per O/S environment
  - Public Listener: Often configured using port 1521 routed to a public switch for applications
  - Private Listener: Often using port 1526 routed to a private switch for replication
- Additional listeners may be best practice depending upon a number of factors including
  - Database version and patch level
  - Granular traffic control
  - Network pathing
  - ORACLE\_HOMEs configuration supporting versions
  - Security isolation



ORACLE® Help Center [Sign In](#)

Home / Database / Oracle Database Online Documentation 12c Release 1 (12.1) / Database Administration

## Database Net Services Administrator's Guide

Table of Contents

- Oracle Database Net Services Administrator's Guide
  - Preface
  - Changes in This Release for Oracle Database Net Services Administrator's Guide
  - Introducing Oracle Net Services
  - Identifying and Accessing the Database
  - Managing Network Address Information
  - Understanding the Communication Layers
  - Understanding Oracle Net Architecture
  - Quick Start to Oracle Net Services
  - Managing Oracle Net Services
  - Configuring Naming Methods

## 14 Optimizing Performance

This chapter describes how to optimize connection performance. This chapter contains the following topics:

- Understanding the Benefits of Network Data Compression
- Configuring Session Data Unit
- Determining the Bandwidth-Delay Product
- Configuring I/O Buffer Space
- Configuring SDP Support for InfiniBand Connections
- Limiting Resource Consumption by Unauthorized Users



# Session Data Unit (SDU)

- The amount of data provided to Oracle Net to send at any one time is referred to as the message size
- Oracle Net assumes by default that the message size will normally vary between 0 and 8192 bytes, and infrequently, be larger than 8192 bytes
- If this assumption is true, then most of the time, the data is sent using one SDU buffer



# SQLNET.ORA

- What goes into SQLNET.ORA affects all listeners and all tnsnames aliases
- If you have multiple listeners, "best practice" for Data Guard, perform listener specific configuration in the listener.ora file or parameters listed in sqlnet.ora will apply to both

```
NAMES.DIRECTORY_PATH=(TNSNAMES, EZCONNECT)

DEFAULT_SDU_SIZE=32767

ENCRYPTION_WALLET_LOCATION = (
    SOURCE=(METHOD=FILE) (METHOD_DATA=(DIRECTORY=/app/oracle/admin/orabase/wallet)))

SQLNET.ALLOWED_LOGON_VERSION=12a

valid_node_checking_registration_listener=on
tcp.invited_nodes=(sales.meta7.com, hr.us.mlib.com, 144.185.5.73)
tcp.excluded_nodes=(blackhat.hacker.com, mktg.us.acme.com, 144.25.5.25)
```



- Stand-Alone

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = CLRExtProc)
      (ORACLE_HOME = c:\app\oracle\product\12.1.0\dbhome_1)
      (PROGRAM = extproc)
      (ENVS = "EXTPROC_DLLS=ONLY:c:\app\oracle\product\12.1.0\dbhome_1\bin\oraclr12.dll")
    )
    (SID_DESC =
      (SID_NAME = PDBDEV)
      (ORACLE_HOME = c:\app\oracle\product\12.1.0\dbhome_1)
    )
    (SID_DESC =
      (SID_NAME = PDBTEST)
      (ORACLE_HOME = c:\app\oracle\product\12.1.0\dbhome_1)
    )
    (SID_DESC =
      (SID_NAME = PDBPROD)
      (ORACLE_HOME = c:\app\oracle\product\12.1.0\dbhome_1)
    )
  )
)

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = PERRITO4)(PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )
)

ADR_BASE_LISTENER = C:\app\oracle
```



- RAC Grid Listener

```
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER))))  
LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER_SCAN1))))  
ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER_SCAN1=ON  
ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER=ON
```



## ■ Data Guard

```
# /sbin/ifconfig
# listener.ora Network Configuration File: /app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
# Generated by Oracle configuration tools.

DG_LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = 10.0.4.1) (PORT = 1526))
      (SEND_BUF_SIZE=9375000)
      (RECV_BUF_SIZE=9375000)
    )
  )

SID_LIST_DG_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SDU = 32767)
      (GLOBAL_DBNAME = proda)
      (ORACLE_HOME = /app/oracle/product/11.2.0/dbhome_1)
      (SID_NAME = proda)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = omega1.mlib.org) (PORT = 1521))
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /app/oracle/product/11.2.0/dbhome_1)
      (PROGRAM = extproc)
    )
  )
```



# TNSNAMES.ORA

- With 12c you must manually add an entry for CDB\$ROOT and for every PDB

```
# tnsnames.ora Network Configuration File: C:\app\oracle\product\12.1.0\dbhome_1\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

ORACLR_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521)))
    (CONNECT_DATA = (SID = CLRExtProc) (PRESENTATION = RO)))

ORABASE =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orabase)))

PDBDEV =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521)))
    (CONNECT_DATA = (SERVICE_NAME = pdbdev)))

PDBTEST =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = pdbtest)))

PDBPROD =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = pdbprod)))
```



# SPFILE

- As with other aspects of the Oracle Database default installation you will find that a number of initialization parameters are configured for backward compatibility ... not for maximizing stability, scalability, and security

```
ALTER SYSTEM SET global_names = TRUE CONTAINER = CURRENT SCOPE = BOTH;  
ALTER SYSTEM SET remote_login_passwordfile = NONE CONTAINER = ALL SCOPE = SPFILE;  
ALTER SYSTEM SET sec_max_failed_login_attempts = 3 CONTAINER = ALL SCOPE = SPFILE;  
ALTER SYSTEM SET sec_protocol_error_further_action = 1 CONTAINER = ALL SCOPE = SPFILE;  
ALTER SYSTEM SET sec_protocol_error_trace_action = log CONTAINER = CURRENT SCOPE = BOTH;  
ALTER SYSTEM SET use_large_pages = TRUE CONTAINER = ALL SCOPE = SPFILE;
```

-- shutdown the database and restart it so that these parameter changes take effect



# Database Configuration: General



# GLOGIN.SQL (1:2)

- Modify glogin.sql will not directly affect stability, scalability, or security but will greatly enhance your sanity and reduce the amount of time you spend doing the same job over-and-over-and-over again
- Find the file `{ORACLE_HOME}/sqlplus/admin/glogin.sql` and rename it to `glogin.bak`. Create a new file in the same directory named glogin.sql with the as follows contents
- You will likely want to add additional column (col) arguments as you work with the new database and find all of the places where Oracle's column widths have expanded, in many cases, to 128 bytes

```
set arraysize 250
set define off
set linesize 121
set long 1000000
set pagesize 45
set serveroutput on
set trim on
set trimspool on

col column_name format a30
col constraint_name format a30
col container_name format a30
col grantee format a30
col index_name format a30
col object_name format a30
```

```
col package_name format a30
col partition_name format a30
col pdb format a20
col synonym_name format a30
col table_name format a30
col type_name format a30
col type_owner format a30
col username format a30
col value format a30
```



## GLOGIN.SQL (2:2)

- In addition it is recommended that you add the following two lines at the end of your glogin.sql file
- The first makes vi the default editor within SQL\*Plus
- The second changes the default date column display format so that you can see time
- The third change guarantees that when you compile, or recompile, PL/SQL objects in SQL\*Plus you will be able to see any generated compiler warnings

```
define _editor = vi
ALTER SESSION SET NLS_DATE_FORMAT='DD-MON-YYYY HH24:MI:SS';
ALTER SESSION SET PLSQL_WARNINGS='ENABLE:ALL';
```



# Database Configuration: Scalability



# SPFILE

- The spfile is configured, primarily, with ALTER SYSTEM statements
- The syntax should be always recognize the instance and container
- And always contain a comment

In 12c you can specify specific containers or all containers

MEMORY, SPFILE, or BOTH

In RAC you can specify a specific instance or all

```
ALTER SYSTEM SET "_enable_NUMA_support" = TRUE
COMMENT= 'NUMA Support Enabled 15-Mar-2015'
CONTAINER=ALL
SCOPE=SPFILE
SID='*' ;
```



# Database Configuration: Security



- Oracle default installations include Profile configurations which are a combination of 16 resource names assigned to two different resource types

RESOURCE NAME	RESOURCE TYPE
KERNEL	COMPOSITE_LIMIT
KERNEL	CONNECT_TIME
KERNEL	CPU_PER_CALL
KERNEL	CPU_PER_SESSION
KERNEL	IDLE_TIME
KERNEL	LOGICAL_READS_PER_CALL
KERNEL	LOGICAL_READS_PER_SESSION
KERNEL	PRIVATE_SGA
KERNEL	SESSIONS_PER_USER

RESOURCE NAME	RESOURCE TYPE
PASSWORD	FAILED_LOGIN_ATTEMPTS
PASSWORD	PASSWORD_GRACE_TIME
PASSWORD	PASSWORD_LIFE_TIME
PASSWORD	PASSWORD_LOCK_TIME
PASSWORD	PASSWORD_REUSE_MAX
PASSWORD	PASSWORD_REUSE_TIME
PASSWORD	PASSWORD_VERIFY_FUNCTION

- At installation in 12c a single profile named DEFAULT is created
- Two actions are recommended at installation
  - The default profile should be modified as described on the following slide
  - A second profile should be created specifically for assignment to mech\_ids (described later in this presentation)



# Profiles (2:3)

- The DEFAULT profile provided by Oracle is the appearance of security without the substance
- The create substance perform the following steps
  - Open the file `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql`
  - Scroll to the bottom of the file and extract the following SQL

```
ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_REUSE_TIME 365
PASSWORD_REUSE_MAX 5
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_VERIFY_FUNCTION ora12c_strong_verify_function;
```

- Modify it so that it looks like the following and run it as SYSDBA (in the root Container)

```
ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_REUSE_TIME 365
PASSWORD_REUSE_MAX 1
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_VERIFY_FUNCTION ora12c_strong_verify_function;
```



- The following profile is a good starting point for a mech\_id profile

```
CREATE PROFILE c##mech_profile LIMIT
FAILED_LOGIN_ATTEMPTS 1
PASSWORD_LOCK_TIME 365
PASSWORD_GRACE_TIME 1
PASSWORD_LIFE_TIME 180
PASSWORD_REUSE_MAX 1
PASSWORD_REUSE_TIME 9999
IDLE_TIME 1440;
```

- If developers or auditors are allowed to connect to a production database they should not be allowed to use the default profile but rather have a profile written specifically for them with a much shorter PASSWORD\_LIFE\_TIME, IDLE\_TIME, and a limit of no more than 2 SESSIONS\_PER\_USER



# Password Verification

- The password verify function in database version 12c is substantially altered from previous versions
- Read `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql` to document the changes
  - Review the CIS (Computer Internet Security) and DOD STIG profile modifications commented out
  - Read too catpf.sql



# Security Parameters

- There are a number of init.ora/spfile parameters that can contribute to creating a more secure environment
  - O7\_DICTIONARY\_ACCESSIBILITY
  - LDAP\_DIRECTORY\_ACCESS
  - LDAP\_DIRECTORY\_SYSAUTH
  - OS\_ROLES
  - REMOTE\_LISTENER
  - REMOTE\_LOGIN\_PASSWORDFILE
  - REMOTE\_OS\_ROLES
  - SEC\_CASE\_SENSITIVE\_LOGON
  - SEC\_MAX\_FAILED\_LOGIN\_ATTEMPTS
  - SEC\_PROTOCOL\_ERROR\_FURTHER\_ACTION
  - SEC\_PROTOCOL\_ERROR\_TRACE\_ACTION
  - SEC\_RETURN\_SERVER\_RELEASE\_BANNER
  - SQL92\_SECURITY



# Secure Configuration

- In Database 12.c Oracle has added a new file `$ORACLE_HOME/rdbms/admin/secconf.sql` that you must read and learn
- SECCONF stands for Secure Configuration
- Here's the file's header

```
Rem      NAME
Rem      secconf.sql - SECure CONFiguration script
Rem
Rem      DESCRIPTION
Rem      Secure configuration settings for the database include a reasonable
Rem      default password profile, password complexity checks, audit settings
Rem      (enabled, with admin actions audited), and as many revokes from PUBLIC
Rem      as possible. In the first phase, only the default password profile is
Rem      included.
Rem
Rem
Rem      NOTES
Rem      Only invoked for newly created databases, not for upgraded databases
```

- This file affects the default profile and prompts for audit configuration
- If you don't enable `ORA_SECURECONFIG` expect your auditors to ask why



# Privilege Revocation (1:2)

- There are a lot of objects for which Oracle's default installation grants access to PUBLIC and for which PUBLIC access is unnecessary and inappropriate for most deployments

Would you grant PUBLIC access to ALL\_SOURCE?

```
REVOKE execute ON dbms_job FROM PUBLIC;
REVOKE execute ON dbms_obfuscation_toolkit FROM PUBLIC;
REVOKE execute ON dbms_random FROM PUBLIC;
REVOKE select ON all_source FROM PUBLIC;
REVOKE select ON role_role_privs FROM PUBLIC;
REVOKE select ON user_role_privs FROM PUBLIC;
REVOKE select ON user_sys_privs FROM PUBLIC;
REVOKE select ON user_tab_privs FROM PUBLIC;
```

- And if your database contains the user scott consider this

SQL> SELECT * FROM user_sys_privs;				
USERNAME	PRIVILEGE	ADM	COM	
SCOTT	UNLIMITED TABLESPACE	NO	NO	
SCOTT	CREATE CLUSTER	NO	NO	
SCOTT	CREATE TABLE	NO	NO	

- Does scott really need unlimited tablespace?



# Privilege Revocation (2:2)

```
REVOKE select ON dba_auto_segadv_ctl FROM PUBLIC;
REVOKE select ON dba_auto_segadv_summary FROM PUBLIC;
REVOKE select ON dba_col_pending_stats FROM PUBLIC;
REVOKE select ON dba_dbfs_hs_fixed_properties FROM PUBLIC;
REVOKE select ON dba_editioning_view_cols FROM PUBLIC;
REVOKE select ON dba_editioning_view_cols_ae FROM PUBLIC;
REVOKE select ON dba_flashback_archive FROM PUBLIC;
REVOKE select ON dba_flashback_archive_tables FROM PUBLIC;
REVOKE select ON dba_flashback_archive_ts FROM PUBLIC;
REVOKE select ON dba_heat_map_segment FROM PUBLIC;
REVOKE select ON dba_heat_map_seg_histogram FROM PUBLIC;
REVOKE select ON dba_ind_pending_stats FROM PUBLIC;
REVOKE select ON dba_java_classes FROM PUBLIC;
REVOKE select ON dba_scheduler_remote_databases FROM PUBLIC;
REVOKE select ON dba_sdo_maps FROM PUBLIC;
REVOKE select ON dba_sdo_styles FROM PUBLIC;
REVOKE select ON dba_sdo_themes FROM PUBLIC;
REVOKE select ON dba_sr_partn_ops FROM PUBLIC;
REVOKE select ON dba_sr_stlog_stats FROM PUBLIC;
REVOKE select ON dba_sync_capture_tables FROM PUBLIC;
REVOKE select ON dba_tab_histgrm_pending_stats FROM PUBLIC;
REVOKE select ON dba_tab_pending_stats FROM PUBLIC;
REVOKE select ON dba_tab_stat_prefs FROM PUBLIC;
REVOKE select ON dba_tstz_tables FROM PUBLIC;
REVOKE select ON dba_xmlschema_level_view FROM PUBLIC;
```



# Network Communications (1:3)

- The Oracle database contains built-in components that can be utilized to enable communications to the intranet and internet
- They can also be used to hack both internal and external networks
  - DBMS\_NETWORK\_ACL\_ADMIN
  - DBMS\_NETWORK\_ACL.Utility
  - UTL\_HTTP
  - UTL\_INADDR
  - UTL\_MAIL
  - UTL\_SMTP
  - UTL\_TCP
- Unfortunately many of them are, by default, exposed to PUBLIC

```
SQL> SELECT grantee, table_name
  2  FROM cdb_tab_privs
  3  WHERE table_name IN ('DBMS_NETWORK_ACL_ADMIN',
  'DBMS_NETWORK_ACL.Utility',
  'UTL_HTTP',
  'UTL_INADDR',
  'UTL_MAIL',
  'UTL_SMTP',
  'UTL_TCP')
  4  ORDER BY 2,1;
```

GRANTEE	TABLE_NAME
APEX_040200	UTL_HTTP
DBA	DBMS_NETWORK_ACL_ADMIN
EXECUTE_CATALOG_ROLE	DBMS_NETWORK_ACL_ADMIN
PUBLIC	DBMS_NETWORK_ACL.Utility
ORDPLUGINS	UTL_HTTP
PUBLIC	UTL_HTTP
ORACLE_OCM	UTL_INADDR
PUBLIC	UTL_INADDR
APEX_040200	UTL_SMTP
PUBLIC	UTL_SMTP
PUBLIC	UTL_TCP



# Network Communications (2:3)

## ■ UTL\_INADDR Demo

```
SQL> SELECT utl_inaddr.get_host_address ('www.oracle.com') FROM dual;

UTL_INADDR.GET_HOST_ADDRESS ('WWW.ORACLE.COM')
-----
2600:1404:a:394::2d3e

SQL> SELECT utl_inaddr.get_host_address ('umn.edu') FROM dual;

UTL_INADDR.GET_HOST_ADDRESS ('UMN.EDU')
-----
134.84.119.107

SQL> SELECT utl_inaddr.get_host_name ('134.84.119.7') FROM dual;

UTL_INADDR.GET_HOST_NAME ('134.84.119.7')
-----
isrv-w.tc.umn.edu

SQL> SELECT utl_inaddr.get_host_name ('134.84.119.22') FROM dual;

UTL_INADDR.GET_HOST_NAME ('134.84.119.22')
-----
isrv-w.tc.umn.edu

SQL> SELECT utl_inaddr.get_host_name ('134.84.119.31') FROM dual;

UTL_INADDR.GET_HOST_NAME ('134.84.119.31')
-----
isrv-w.tc.umn.edu
```



- DBMS\_NETWORK\_ACL\_ADMIN/UTILITY

```
SQL> SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual;
      SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual
      *
ERROR at line 1:
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```



# Database Link Communications (1:2)

- Database Links can be a valuable productivity tool
- They can also be an attack vector
- Regularly audit existing links and creation of new links

Explanation	Database links are objects that allow creation of an almost transparent connection between databases that can be used to select, insert, update, and/or delete data.				
Validation	<pre>SELECT * FROM dba_db_links ORDER BY 1,2;</pre>				
Finding	OWNER	DB_LINK	USERNAME	HOST	CREATED
	-----	-----	-----	-----	-----
	PUBLIC	EPMPRD.???.EDU	SYSADM	EPMPRD	19-APR-12
	PUBLIC	FINPRD.???.EDU	SYSADM	FINPRD	10-NOV-11
	PUBLIC	HRRPT.???.EDU	SYSADM	HRRPT	10-NOV-11
	PUBLIC	HRTRN.???.EDU	SYSADM	HRTRN	10-NOV-11
	PUBLIC	OEPRD.???.EDU	PS_READ	oeprd	07-DEC-11
	PUBLIC	OUDWH.???.EDU	PS_READ	??DWH	10-NOV-11
	PUBLIC	OUPRD.???.EDU	PS_READ	??PRD	10-NOV-11
	PUBLIC	PROD.???.EDU	PS_READ	PROD	10-NOV-11
	SPOTLIGHT	QUEST_SO0_HRPRD1.???.EDU		hrprd1	02-DEC-11
	SPOTLIGHT	QUEST_SO0_HRPRD2.???.EDU		hrprd2	02-DEC-11
	SPOTLIGHT	QUEST_SO0_HRPRD3.???.EDU		hrprd3	02-DEC-11



# Database Link Communications (2:2)

- DBMS\_DISTRIBUTED\_TRUST\_ADMIN

- First released with in 2001, contains procedures to maintain the Trusted Servers List
- Use the package to define whether a server is trusted. If a database is not trusted, Oracle refuses current user database links from the database
  - Cannot stop PDB to PDB links in the same CDB

```
SQL> exec dbms_distributed_trust_admin.deny_all;

PL/SQL procedure successfully completed.

SQL> SELECT * FROM ku$_trlink_view;

V V NAME          FUNCTION          TYPE
--- --- ---          --- --- ---          ---
1 0 -*           DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL      0

SQL> exec dbms_distributed_trust_admin.allow_server('BIGDOG.MLIB.ORG');

PL/SQL procedure successfully completed.

SQL> SELECT * FROM ku$_trlink_view;

V V NAME          FUNCTION          TYPE
--- --- ---          --- --- ---          ---
1 0 -*           DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL      0
1 0 BIGDOG.MLIB.ORG          DBMS_DISTRIBUTED_TRUST_ADMIN.ALLOW_SERVER 1
```



# Optimizer Settings

- ALL\_ROWS and FIRST\_ROWS define the default behavior of the instance's optimization approach
- Syntax

```
Range of values: {first_rows_[1 | 10 | 100 | 1000] | first_rows | all_rows}
```

- Altering the default value

```
ALTER SYSTEM SET optimizer_mode = FIRST_ROWS_10 SCOPE = BOTH SID='*' ;
```



# System Event Triggers (1:2)

- DDL Event Triggers can prevent bad things from happening

```
CREATE OR REPLACE TRIGGER save_our_db
BEFORE DROP OR TRUNCATE
ON SCHEMA
DECLARE
  oper ddl_log.operation%TYPE;
BEGIN
  oper := ora_sysevent;
  log_proc(ora_sysevent, ora_dict_obj_owner, ora_dict_obj_name);

  IF oper = 'DROP' THEN
    RAISE_APPLICATION_ERROR(-20998, 'Attempt To Drop In Production Has Been Logged');
  ELSIF oper = 'TRUNCATE' THEN
    RAISE_APPLICATION_ERROR(-20999, 'Attempt To Truncate A Production Table Has Been Logged');
  END IF;
END save_our_db;
/
```



# System Event Triggers (2:2)

- System Event Triggers can detect bad things you cannot detect any other way

```
CREATE OR REPLACE TRIGGER logon_failures
AFTER SERVERERROR
ON DATABASE
BEGIN
    IF (IS_SERVERERROR(1017)) THEN
        INSERT INTO connection_audit
        (login_date, user_name)
        VALUES
        (SYSDATE, 'ORA-1017');
        COMMIT;
    END IF;
END logon_failures;
/
```



# User Authentication and Permissions

- No user should be created using the default profile ... more about profiles next
- Check for default password usage
  - If you find default passwords being used either change the passwords or lock and expire the account
- Do not use externally authenticated users such as OPS\$ unless you can prove that O/S access is secure and will stay that way: Never with Windows

```
SQL> SELECT d.con_id, d.username, u.account_status
  2  FROM cdb_users_with_defpwd d, cdb_users u
  3  WHERE d.username = u.username
  4  AND u.account_status = 'OPEN'
  5  ORDER BY 3,1, 2;
```

CON_ID	USERNAME	ACCOUNT_STATUS
1	SYS	OPEN
1	SYS	OPEN
1	SYSTEM	OPEN
1	SYSTEM	OPEN
3	HR	OPEN
3	OE	OPEN
3	PM	OPEN
3	SCOTT	OPEN
3	SH	OPEN
3	SYS	OPEN
3	SYS	OPEN
3	SYSTEM	OPEN
3	SYSTEM	OPEN



# Oracle Default Roles

- There is literally no excuse for anyone having the CONNECT or RESOURCE roles
- Similarly no human should have the DBA role either
- Create your own DBA role with only the privileges actually required to manage the database

```
SQL> SELECT con_id, grantee, granted_role
  2  FROM cdb_role_privs
  3  WHERE granted_role IN ('CONNECT', 'RESOURCE')
  4  AND grantee NOT LIKE '%SYS%'
  5  AND grantee NOT LIKE '%GSM%'
  6  AND grantee NOT LIKE '%SPATIAL%'
  7  AND grantee NOT LIKE 'DV%'
  8  AND grantee NOT IN ('MDDATA', 'XDB')
 9* ORDER BY 2,3,1;
```

CON_ID	GRANTEE	GRANTED_ROLE
1	APEX_040200	CONNECT
3	APEX_040200	CONNECT
1	APEX_040200	RESOURCE
3	APEX_040200	RESOURCE
3	BI	RESOURCE
3	HR	RESOURCE
3	IX	CONNECT
3	IX	RESOURCE
1	LOGSTDBY_ADMINISTRATOR	RESOURCE
3	LOGSTDBY_ADMINISTRATOR	RESOURCE
3	OE	RESOURCE
1	OUTLN	RESOURCE
3	OUTLN	RESOURCE
3	PDB_DBA	CONNECT
3	PM	CONNECT
3	PM	RESOURCE
3	SCOTT	CONNECT
3	SCOTT	RESOURCE
3	SH	RESOURCE

19 rows selected.



# Who Needs The DBA Role?

```
SQL> select privilege
  2  FROM dba_sys_privs
  3  WHERE grantee = 'DBA'
  4  ORDER BY 1;
```

PRIVILEGE

-----  
ADMINISTER ANY SQL TUNING SET  
ADMINISTER DATABASE TRIGGER  
ADMINISTER RESOURCE MANAGER  
ADMINISTER SQL MANAGEMENT OBJECT  
ADMINISTER SQL TUNING SET  
ADVISOR  
ALTER ANY ASSEMBLY  
ALTER ANY CLUSTER  
ALTER ANY CUBE  
ALTER ANY CUBE BUILD PROCESS  
ALTER ANY CUBE DIMENSION  
ALTER ANY DIMENSION  
ALTER ANY EDITION  
ALTER ANY EVALUATION CONTEXT  
ALTER ANY INDEX  
ALTER ANY INDEXTYPE  
ALTER ANY LIBRARY  
ALTER ANY MATERIALIZED VIEW  
ALTER ANY MEASURE FOLDER  
ALTER ANY MINING MODEL  
ALTER ANY OPERATOR  
ALTER ANY OUTLINE  
ALTER ANY PROCEDURE  
ALTER ANY ROLE  
ALTER ANY RULE  
ALTER ANY RULE SET  
ALTER ANY SEQUENCE  
ALTER ANY SQL PROFILE  
ALTER ANY SQL TRANSLATION PROFILE  
ALTER ANY TABLE  
ALTER ANY TRIGGER  
ALTER ANY TYPE  
ALTER DATABASE  
ALTER PROFILE  
ALTER RESOURCE COST  
ALTER ROLLBACK SEGMENT  
ALTER SESSION  
ALTER SYSTEM  
ALTER TABLESPACE  
ALTER USER  
ANALYZE ANY  
ANALYZE ANY DICTIONARY  
AUDIT ANY  
AUDIT SYSTEM

BACKUP ANY TABLE  
BECOME USER  
CHANGE NOTIFICATION  
COMMENT ANY MINING MODEL  
COMMENT ANY TABLE  
CREATE ANY ASSEMBLY  
CREATE ANY CLUSTER  
CREATE ANY CONTEXT  
CREATE ANY CREDENTIAL  
CREATE ANY CUBE  
CREATE ANY CUBE BUILD PROCESS  
CREATE ANY CUBE DIMENSION  
CREATE ANY DIMENSION  
CREATE ANY DIRECTORY  
CREATE ANY EDITION  
CREATE ANY EVALUATION CONTEXT  
CREATE ANY INDEX  
CREATE ANY INDEXTYPE  
CREATE ANY JOB  
CREATE ANY LIBRARY  
CREATE ANY MATERIALIZED VIEW  
CREATE ANY MEASURE FOLDER  
CREATE ANY MINING MODEL  
CREATE ANY OPERATOR  
CREATE ANY OUTLINE  
CREATE ANY PROCEDURE  
CREATE ANY RULE  
CREATE ANY RULE SET  
CREATE ANY SEQUENCE  
CREATE ANY SQL PROFILE  
CREATE ANY SQL TRANSLATION PROFILE  
CREATE ANY SYNONYM  
CREATE ANY TABLE  
CREATE ANY TRIGGER  
CREATE ANY TYPE  
CREATE ANY VIEW  
CREATE ASSEMBLY  
CREATE CLUSTER  
CREATE CREDENTIAL  
CREATE CUBE  
CREATE CUBE BUILD PROCESS  
CREATE CUBE DIMENSION  
CREATE DATABASE LINK  
CREATE DIMENSION  
CREATE EVALUATION CONTEXT  
CREATE EXTERNAL JOB  
CREATE INDEXTYPE  
CREATE JOB  
CREATE LIBRARY  
CREATE MATERIALIZED VIEW  
CREATE MEASURE FOLDER

CREATE MINING MODEL  
CREATE OPERATOR  
CREATE PLUGGABLE DATABASE  
CREATE PROCEDURE  
CREATE PROFILE  
CREATE PUBLIC DATABASE LINK  
CREATE PUBLIC SYNONYM  
CREATE ROLE  
CREATE ROLLBACK SEGMENT  
CREATE RULE  
CREATE RULE SET  
CREATE SEQUENCE  
CREATE SESSION  
CREATE SQL TRANSLATION PROFILE  
CREATE SYNONYM  
CREATE TABLE  
CREATE TABLESPACE  
CREATE TRIGGER  
CREATE TYPE  
CREATE USER  
CREATE VIEW  
DEBUG ANY PROCEDURE  
DEBUG CONNECT SESSION  
DELETE ANY CUBE DIMENSION  
DELETE ANY MEASURE FOLDER  
DELETE ANY TABLE  
DEQUEUE ANY QUEUE  
DROP ANY ASSEMBLY  
DROP ANY CLUSTER  
DROP ANY CONTEXT  
DROP ANY CUBE  
DROP ANY CUBE BUILD PROCESS  
DROP ANY CUBE DIMENSION  
DROP ANY DIMENSION  
DROP ANY DIRECTORY  
DROP ANY EDITION  
DROP ANY EVALUATION CONTEXT  
DROP ANY INDEX  
DROP ANY INDEXTYPE  
DROP ANY LIBRARY  
DROP ANY MATERIALIZED VIEW  
DROP ANY MEASURE FOLDER  
DROP ANY MINING MODEL  
DROP ANY OPERATOR  
DROP ANY OUTLINE  
DROP ANY PROCEDURE  
DROP ANY ROLE  
DROP ANY RULE  
DROP ANY RULE SET  
DROP ANY SEQUENCE  
DROP ANY SQL PROFILE  
DROP ANY SQL TRANSLATION PROFILE

DROP ANY SYNONYM  
DROP ANY TABLE  
DROP ANY TRIGGER  
DROP ANY TYPE  
DROP ANY VIEW  
DROP PROFILE  
DROP PUBLIC DATABASE LINK  
DROP PUBLIC SYNONYM  
DROP ROLLBACK SEGMENT  
DROP TABLESPACE  
DROP USER  
EN EXPRESS CONNECT  
ENQUEUE ANY QUEUE  
EXECUTE ANY ASSEMBLY  
EXECUTE ANY CLASS  
EXECUTE ANY EVALUATION CONTEXT  
EXECUTE ANY INDEXTYPE  
EXECUTE ANY LIBRARY  
EXECUTE ANY OPERATOR  
EXECUTE ANY PROCEDURE  
EXECUTE ANY PROGRAM  
EXECUTE ANY RULE  
EXECUTE ANY RULE SET  
EXECUTE ANY TYPE  
EXECUTE ASSEMBLY  
EXEMPT DDL REDACTION POLICY  
EXEMPT DML REDACTION POLICY  
EXPORT FULL DATABASE  
FLASHBACK ANY TABLE  
FLASHBACK ARCHIVE ADMINISTER  
FORCE ANY TRANSACTION  
FORCE TRANSACTION  
GLOBAL QUERY REWRITE  
GRANT ANY OBJECT PRIVILEGE  
GRANT ANY PRIVILEGE  
GRANT ANY ROLE  
IMPORT FULL DATABASE  
INSERT ANY CUBE DIMENSION  
INSERT ANY MEASURE FOLDER  
INSERT ANY TABLE  
LOCK ANY TABLE  
LOGMINING  
MANAGE ANY FILE GROUP  
MANAGE ANY QUEUE  
MANAGE FILE GROUP  
MANAGE SCHEDULER  
MANAGE TABLESPACE  
MERGE ANY VIEW  
ON COMMIT REFRESH  
QUERY REWRITE  
READ ANY FILE GROUP  
READ ANY TABLE

READ ANY TABLE  
REFRESH ANY TABLE  
RESTRICTED SESSION  
RESUMABLE  
SELECT ANY CUBE  
SELECT ANY CUBE BUILD PROCESS  
SELECT ANY CUBE DIMENSION  
SELECT ANY DICTIONARY  
SELECT ANY MEASURE FOLDER  
SELECT ANY MINING MODEL  
SELECT ANY SEQUENCE  
SELECT ANY TABLE  
SELECT ANY TRANSACTION  
SET CONTAINER  
UNDER ANY TABLE  
UNDER ANY TYPE  
UNDER ANY VIEW  
UPDATE ANY CUBE  
UPDATE ANY CUBE BUILD PROCESS  
UPDATE ANY CUBE DIMENSION  
UPDATE ANY TABLE  
USE ANY SQL TRANSLATION PROFILE

220 rows selected.

**FEEL FREE TO EXPLAIN  
WHY YOU NEED THE  
READ ANY TABLE  
PRIVILEGE**

**IF YOU CANNOT EXPLAIN  
IT ... YOU DON'T NEED IT**



# Excessive Privileges (1:2)

- Does every user connecting to an Oracle Database need EXECUTE privilege on these 187 packages?
- The answer is clearly no

```
SQL> SELECT DISTINCT table_name AS PACKAGE_NAME
  2  FROM cdb_tab_privs
  3  WHERE grantee = 'PUBLIC'
  4  AND table_name LIKE 'DBMS%'
  5  AND owner IN ('SYS', 'XDB')
  6* ORDER BY 1;
```

```
PACKAGE_NAME
-----
DBMSOUTPUT_LINESARRAY
DBMS_ADDM
DBMS_ADVISOR
DBMS_APPLICATION_INFO
DBMS_APP_CONT_PRVT
DBMS_AQJMS
DBMS_AQ_EXP_CMT_TIME_TABLES
DBMS_AQ_EXP_DEQUEUELOG_TABLES
DBMS_AQ_EXP_HISTORY_TABLES
DBMS_AQ_EXP_INDEX_TABLES
DBMS_AQ_EXP_QUEUES
DBMS_AQ_EXP_QUEUE_TABLES
DBMS_AQ_EXP_SIGNATURE_TABLES
DBMS_AQ_EXP_SUBSCRIBER_TABLES
DBMS_AQ_EXP_TIMEMGR_TABLES
DBMS_AQ_IMP_INTERNAL
DBMS_AQ_INV
```

PACKAGE_NAME
DBMS_ASSERT
DBMS_AUTO_REPORT
DBMS_AUTO_TASK
DBMS_AW
DBMS_AW\$COLUMNLIST_T
DBMS_AW\$DIMENSION_SOURCES_T
DBMS_AW\$DIMENSION_SOURCE_T
DBMS_AW_EXP
DBMS_AW_STATS
DBMS_AW_XML
DBMS_CDC_DPUTIL
DBMS_CDC_EXPDP
DBMS_CDC_EXPVDP
DBMS_CDC_IMPDP
DBMS_CDC_ISUBSCRIBE
DBMS_CDC_SUBSCRIBE
DBMS_COMPRESSION
DBMS_CREDENTIAL
DBMS_CRYPTO_TOOLKIT
DBMS_CUBE
DBMS_CUBE_ADVISE
DBMS_CUBE_ADVISE_SEC
DBMS_CUBE_EXP
DBMS_CUBE_LOG
DBMS_CUBE_UTIL
DBMS_CUBE_UTIL_DFLT_MSR_R
DBMS_CUBE_UTIL_DFLT_MSR_T
DBMS_CUBE_UTIL_EXT_MD_R
DBMS_CUBE_UTIL_EXT_MD_T
DBMS_DATAPUMP
DBMS_DATA_MINING
DBMS_DATA_MINING_TRANSFORM
DBMS_DB_VERSION

PACKAGE_NAME
DBMS_DDL
DBMS_DEBUG
DBMS_DEBUG_JDWP
DBMS_DEBUG_JDWP_CUSTOM
DBMS_DEBUG_VC2COLL
DBMS_DESCRIBE
DBMS_DIMENSION
DBMS_DM_MODEL_EXP
DBMS_DM_MODEL_IMP
DBMS_EDITIONS_UTILITIES
DBMS_EPG
DBMS_ERRLOG
DBMS_EXPORT_EXTENSION
DBMS_FBT
DBMS_FILE_GROUP_EXP
DBMS_FILE_GROUP_IMP
DBMS_FREQUENT_ITEMSET
DBMS_HEAT_MAP
DBMS_HS_PARALLEL
DBMS_IIM
DBMS_IIM_ADMIN
DBMS_INDEX_UTL
DBMS_IOT
DBMS_ITRIGGER_UTL
DBMS_JAVA
DBMS_JOB
DBMS_JOB\$
DBMS_LCR
DBMS_LDAP
DBMS_LDAP_UTL
DBMS_LOB
DBMS_LOBUTIL
DBMS_LOBUTIL_DEDUPSET_T



# Excessive Privileges (2:2)

PACKAGE\_NAME

---

DBMS\_LOBUTIL\_INODE\_T  
DBMS\_LOBUTIL\_LOBEXTENTS\_T  
DBMS\_LOBUTIL\_LOBEXTENT\_T  
DBMS\_LOBUTIL\_LOBMAP\_T  
DBMS\_LOGREP\_EXP  
DBMS\_LOGREP\_IMP  
DBMS\_LOGSTDBY\_CONTEXT  
**DBMS\_METADATA**  
**DBMS\_METADATA\_DIFF**  
**DBMS\_NETWORK\_ACL.Utility**  
DBMS\_OBFUSCATION\_TOOLKIT  
DBMS\_OBJECTS\_UTILS  
DBMS\_ODCI  
DBMS\_OUTPUT  
DBMS\_PARALLEL\_EXECUTE  
DBMS\_PART  
DBMS\_PCLXUTIL  
DBMS\_PICKLER  
DBMS\_PREDICTIVE\_ANALYTICS  
DBMS\_PREPROCESSOR  
DBMS\_PROFILER  
DBMS\_PSP  
DBMS\_RANDOM  
DBMS\_REFRESH  
DBMS\_REFRESH\_EXP\_LWM  
DBMS\_REFRESH\_EXP\_SITES  
DBMS\_REPCAT\_EXP  
DBMS\_REPCAT\_INSTANTIATE  
DBMS\_REPCAT\_RGT\_EXP  
DBMS\_REPORT  
DBMS\_RESOURCE\_MANAGER  
DBMS\_RESOURCE\_MANAGER\_PRIVS  
DBMS\_RESULT\_CACHE\_API

PACKAGE\_NAME

---

DBMS\_RMGR\_GROUP\_EXPORT  
DBMS\_RMGR\_PACT\_EXPORT  
DBMS\_RMGR\_PLAN\_EXPORT  
DBMS\_RMIN  
DBMS\_ROWID  
DBMS\_RULE  
DBMS\_RULEADM\_INTERNAL  
DBMS\_RULE\_ADMIN  
DBMS\_RULE\_EXP\_EV\_CTXS  
DBMS\_RULE\_EXP\_RULES  
DBMS\_RULE\_EXP\_RULE\_SETS  
DBMS\_RULE\_EXP\_UTLI  
DBMS\_RULE\_IMP\_OBJ  
DBMS\_SCHEDULER  
DBMS\_SCHED\_ATTRIBUTE\_EXPORT  
DBMS\_SCHED\_CHAIN\_EXPORT  
DBMS\_SCHED\_CLASS\_EXPORT  
**DBMS\_SCHED\_CREDENTIAL\_EXPORT**  
**DBMS\_SCHED\_EXPORT\_CALLOUTS**  
**DBMS\_SCHED\_FILE\_WATCHER\_EXPORT**  
**DBMS\_SCHED\_JOB\_EXPORT**  
**DBMS\_SCHED\_PROGRAM\_EXPORT**  
**DBMS\_SCHED\_SCHEDULE\_EXPORT**  
**DBMS\_SCHED\_WINDOW\_EXPORT**  
**DBMS\_SCHED\_WINGRP\_EXPORT**  
DBMS\_SCN  
DBMS\_SESSION  
DBMS\_SNAPSHOT  
DBMS\_SNAPSHOT\_UTL  
DBMS\_SPACE  
DBMS\_SPD  
DBMS\_SPM  
**DBMS\_SQL**

PACKAGE\_NAME

---

DBMS\_SQLDIAG  
DBMS\_SQLPA  
DBMS\_SQLTUNE  
DBMS\_SQLTUNE\_UTIL2  
DBMS\_SQL\_MONITOR  
DBMS\_SQL\_TRANSLATOR  
DBMS\_SQL\_TRANSLATOR\_EXPORT  
DBMS\_STANDARD  
DBMS\_STATS  
DBMS\_STAT\_FUNCS  
DBMS\_STAT\_FUNCS\_AUX  
DBMS\_STREAMS  
DBMS\_STREAMS\_PUB\_RPC  
DBMS\_SUMMARY  
DBMS\_SUM\_RWEQ\_EXPORT  
DBMS\_SYNC\_REFRESH  
**DBMS\_TRACE**  
DBMS\_TRANSACTION  
DBMS\_TRANSFORM\_EXIMP  
DBMS\_TYPES  
DBMS.Utility  
DBMS\_WARNING  
DBMS\_XA  
DBMS\_XA\_XID  
DBMS\_XA\_XID\_ARRAY  
DBMS\_XMLGEN  
DBMS\_XMLQUERY  
DBMS\_XMLSAVE  
DBMS\_XMLSTORE  
DBMS\_XPLAN  
DBMS\_XPLAN\_TYPE  
DBMS\_XPLAN\_TYPE\_TABLE  
DBMS\_XQUERY

PACKAGE\_NAME

---

DBMS\_XQUERYINT  
**DBMS\_XSLPROCESSOR**  
DBMS\_XS\_NSATTR  
DBMS\_XS\_NSATTRLIST  
DBMS\_XS\_SESSIONS  
DBMS\_ZHELP\_IR  
UTL\_ALL\_IND\_COMPS  
UTL\_BINARYINPUTSTREAM  
UTL\_BINARYOUTPUTSTREAM  
**UTL\_CALL\_STACK**  
UTL\_CHARACTERINPUTSTREAM  
UTL\_CHARACTEROUTPUTSTREAM  
UTL\_COLL  
UTL\_COMPRESS  
UTL\_ENCODE  
**UTL\_FILE**  
UTL\_GDK  
**UTL\_HTTP**  
UTL\_I18N  
UTL\_IDENT  
**UTL\_INADDR**  
UTL\_LMS  
UTL\_MAIL\_INTERNAL  
UTL\_MATCH  
UTL\_NLA  
UTL\_NLA\_ARRAY\_DBL  
UTL\_NLA\_ARRAY\_FLT  
UTL\_NLA\_ARRAY\_INT  
UTL\_PG  
UTL\_RAW  
UTL\_REF  
**UTL\_SMTP**  
**UTL\_TCP**  
UTL\_URL



# Statistics Collection



# Statistics Collection

- Some of the stats collected by use of the DBMS\_STATS package are collected automatically
- The ones most important at installation time are only collected when you manually initiate collection
- The stats we are focusing on here are
  - System Statistics
  - Fixed Object Statistics
  - Data Dictionary Statistics
  - Processing Rates
- Other statistics should be addressed on an ongoing basis with a production system through manual collection or through the use of DBMS\_SCHEDULER jobs
  - Copying or setting table statistics immediately following partition creation
  - Copying or setting index statistics immediately following partition creation



# System Statistics

- The Oracle Database, by default, does not collect system stats

```
SQL> exec dbms_stats.gather_system_stats('INTERVAL', 15);
```

```
SQL> SELECT * FROM sys.aux_stats$;
```

SNAME	PNAME	PVAL1	PVAL2
SYSSTATS_INFO	STATUS		COMPLETED
SYSSTATS_INFO	DSTART		05-27-2015 09:45
SYSSTATS_INFO	DSTOP		05-27-2015 09:51
SYSSTATS_INFO	FLAGS	0	
SYSSTATS_MAIN	CPUSPEEDNW	3010	
SYSSTATS_MAIN	IOSEEKTIM	10	
SYSSTATS_MAIN	IOTFRSPEED	4096	
SYSSTATS_MAIN	SREADTIM	3.862	
SYSSTATS_MAIN	MREADTIM	1.362	
SYSSTATS_MAIN	CPUSPEED	2854	
SYSSTATS_MAIN	MBRC	17	
SYSSTATS_MAIN	MAXTHR		
SYSSTATS_MAIN	SLAVETHR		

- Or Fixed Object Stats
- Or Dictionary Stats



# Processing Rate (1:2)

- Processing Rate collection is new as of version 12cR1
- Besides the amount of work the optimizer also needs to know the HW characteristics of the system to understand how much time is needed to complete that amount of work
- Consequently, the HW characteristics describe how much work a single process can perform on that system, these are expressed as bytes per second and rows per second and are called processing rates
- As they indicate a system's capability it means you will need fewer processes (which means less DOP) for the same amount of work as these rates go higher; the more powerful a system is, the less resources you need to process the same statement in the same amount of time
- Processing rates are collected manually

```
SQL> exec dbms_stats.gather_processing_rate('START', 20);

SQL> SELECT operation_name, manual_value, calibration_value, default_value
  2  FROM v$optimizer_processing_rate
  3  ORDER BY 1;
```



# DBMS\_STATS: Processing Rate (2:2)

OPERATION_NAME	MANUAL_VAL	CALIBRATION	DEFAULT_VAL
AGGR			1000.00000
ALL			200.00000
CPU			200.00000
CPU_ACCESS			200.00000
CPU_AGGR			200.00000
CPU_BYTES_PER_SEC			1000.00000
CPU_FILTER			200.00000
CPU_GBY			200.00000
CPU_HASH_JOIN			200.00000
CPU_IMC_BYTES_PER_SEC			2000.00000
CPU_IMC_ROWS_PER_SEC			2000000.00
CPU_JOIN			200.00000
CPU_NL_JOIN			200.00000
CPU_RANDOM_ACCESS			200.00000
CPU_ROWS_PER_SEC			1000000.00000
CPU_SEQUENTIAL_ACCESS			200.00000
CPU_SM_JOIN			200.00000
CPU_SORT			200.00000
HASH			200.00000
IO			200.00000
IO_ACCESS			200.00000
IO_BYTES_PER_SEC			200.00000
IO_IMC_ACCESS			1000.00000
IO_RANDOM_ACCESS			200.00000
IO_ROWS_PER_SEC			1000000.00000
IO_SEQUENTIAL_ACCESS			200.00000
MEMCMP			500.00000
MEMCPY			1000.00000

SQL> exec dbms\_stats.set\_processing\_rate('IO', 100);



# Automatic Workload Repository Enhancement

- Automatic Workload Repository (AWR), by default, collects statistics once each hour and retains them for 7 days
- This is totally inadequate for almost any real-world requirement to use an AWR Report
  - An Oracle Database customer should be able to compare periods with the current period and the prior period is often the previous week or month
- Tom Kyte, years ago with StatsPack wrote that collection should be every **15-20** minutes and retention to **31** days
- The following code alters collection to match this recommendation and well as altering the "top n SQL" collection to **50,000**
- The last value in the following code demo is the database's **DBID**

```
exec dbms_workload_repository.modify_snapshot_settings( (24*60*31) , 20 , 50000 , 428676178) ;
```



# Automatic Workload Repository Enhancement

- Automatic Workload Repository (AWR), by default, collects statistics once each hour and retains them for 7 days
- This is totally inadequate for almost any real-world requirement to use an AWR Report
  - An Oracle Database customer should be able to compare periods with the current period and the prior period is often the previous week or month
- Tom Kyte, years ago with StatsPack wrote that collection should be every **15-20** minutes and retention to **31** days
- The following code alters collection to match this recommendation and well as altering the "top n SQL" collection to **50,000**
- The last value in the following code demo is the database's **DBID**

```
exec dbms_workload_repository.modify_snapshot_settings( (24*60*31) , 20 , 50000 , 428676178) ;
```



# User Creation



# Proxy Users (3:3)

```
-- create a non-human database user
SQL> CREATE USER mechid
  2 IDENTIFIED BY "A1Ac9C81292FC1CF0b8A40#5F04C0A"
  3 DEFAULT TABLESPACE uwdata
  4 TEMPORARY TABLESPACE temp
  5 QUOTA 100M ON uwdata;
```

User created.

```
SQL> AUDIT CONNECT BY scott ON BEHALF OF mechid;
```

Audit succeeded.

```
-- create proxy for mechid
```

```
SQL> ALTER USER mechid GRANT CONNECT THROUGH scott;
```

User altered.

```
SQL> SELECT * FROM sys.proxy_info$;
```

CLIENT#	PROXY#	CREDENTIAL_TYPE#	FLAGS
142	109	0	5

```
SQL> conn scott[MECHID]/tiger@pdbdev
Connected.
```

```
SQL> sho user
USER is "MECHID"
```

```
SQL> SELECT sys_context('USERENV', 'CURRENT_SCHEMA')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'CURRENT_SCHEMA')
-----
```

```
MECHID
```

```
SQL> SELECT sys_context('USERENV', 'CURRENT_USER')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'CURRENT_USER')
-----
```

```
MECHID
```

```
SQL> SELECT sys_context('USERENV', 'PROXY_USER')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'PROXY_USER')
-----
```

```
SCOTT
```



Wrap Up



# Conclusion

- The presentation covers a subset of the Oracle Database's default configurations that will not give you the optimum
  - Stability
  - Security
  - Scalability
- you need for your environment and for your applications
- You can invest a large number of hours, each week, trying to fix things one-at-a-time or you can invest some time, up-front, during installation configuring your environment correctly before you make it available for customers



\*

**ERROR at line 1:**

**ORA-00028: your session has been killed**

# Thank You From Meta7

Daniel A. Morgan  
email: [dmorgan@forsythe.com](mailto:dmorgan@forsythe.com)  
mobile: +1 206-669-2949  
skype: damorgan11g  
twitter: @meta7solutions

