

Database Security

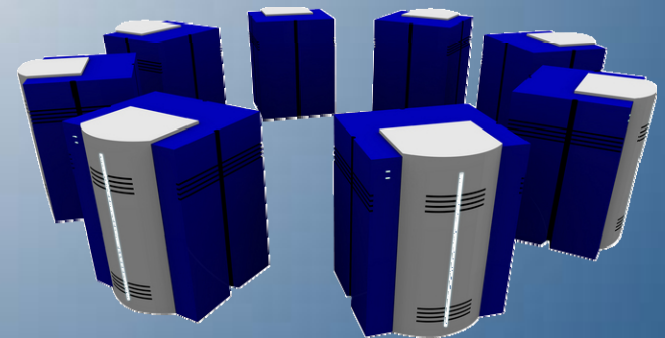
The Last Line of Defense

Ron Shaffer
Ross Group Inc

Solutions For A Data Intensive World

About Me

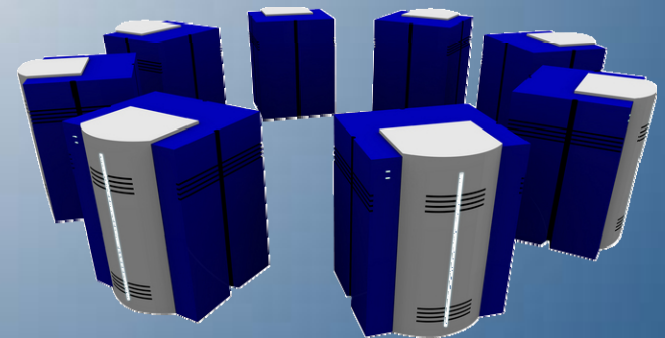
- 17 years working in the IT industry
- 12ish years working with Oracle and SQL Server (I prefer Oracle 😊)
- Performance Tuning and Operational Management of Databases is my Passion
- Security is my new passion
- Practice Manager of the Database Services Group at Ross Group Inc



Ross Group Inc

Overview

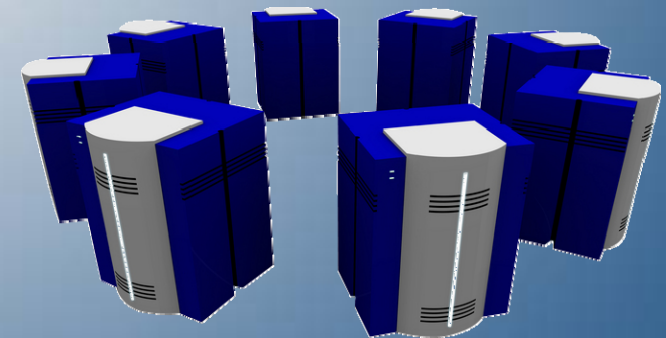
- Regulatory Risk
- Oracle 11G Security Improvements
- 11G Additional Options
- Vulnerabilities
- Where to find more?



Ross Group Inc

Regulatory Risks

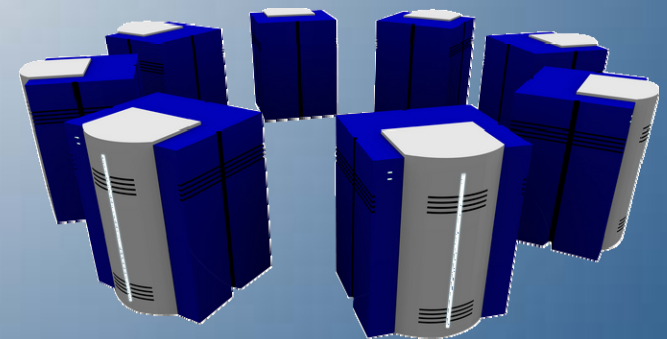
- Sarbanes-Oxley Section 302
 - Unauthorized changes to data
- Sarbanes-Oxley Section 404
 - Modification to data, unauthorized access
- Sarbanes-Oxley Section 409
 - Denial of service, unauthorized access
- Gramm-Leach-Bliley
 - Unauthorized access, modification, or disclosure
- Health Insurance Portability and Accountability Act (HIPAA) 164.306
 - Unauthorized access to data
- HIPAA 164.312
 - Unauthorized access to data
- Basel II – Internal Risk Management
 - Unauthorized access to data
- CFR Part 11
 - Unauthorized access to data



Ross Group Inc

Regulatory Risks

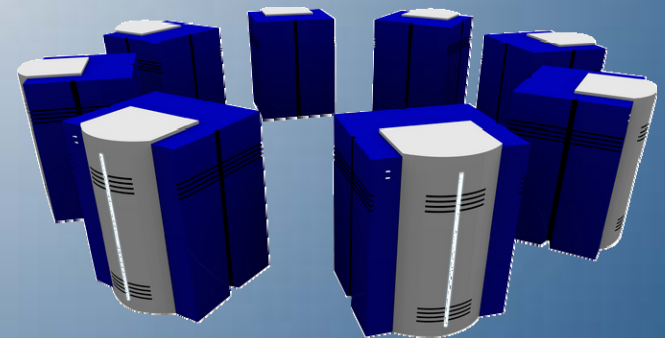
- Japan Privacy Law
 - Unauthorized access to data
- EU Directive on Privacy and Electronic Communications
 - Unauthorized access to data
- Payment Card Industry Data Security Standard (PCI DSS)
 - Unauthorized changes to data



Ross Group Inc

Oracle 11G Security Improvements

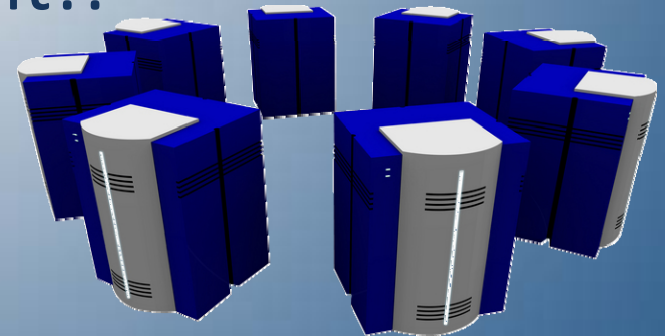
- Automatically Secure Configuration
- Password Enhancements
- SYSDBA and SYSOPER strong Authentication
- SYSASM Privilege
- Encryption
- FGAC on Network Services
- XML DB Enhancements
- Directory Enhancements
- OCI Enhancements



Ross Group Inc

Automatically Secure Configuration

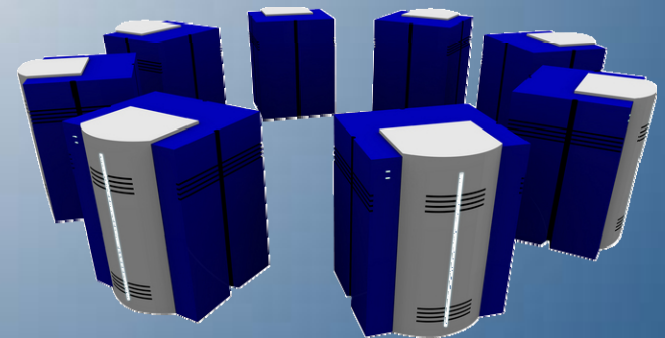
- The default password profile now has settings!!
 - Failed login attempts (10)
 - Password Grace Time (7)
 - Password Lock Time (1)
 - Password Reuse Max (unlimited)
 - Password Reuse Time (unlimited)
- Auditing is turned on by default!!
 - Audit_Trail = DB
 - 26 statements +
 - some security related statements
 - SOX compliance!!



Ross Group Inc

Password Enhancements

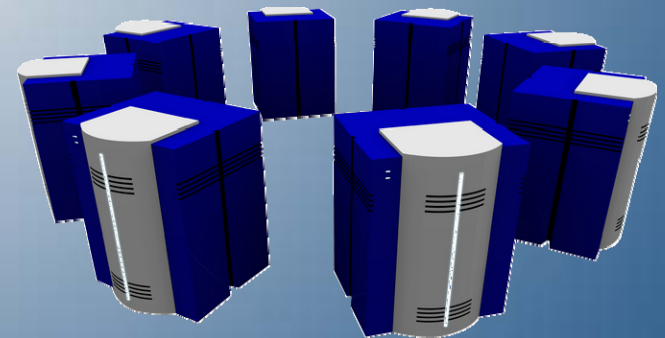
- Easily find users with default passwords
 - DBA_USERS_WITH_DEFPWD
- Password Complexity Verification
 - UTLPWDMG.SQL
 - Between 8 and 30 characters
 - Checks for variations on the username
 - Variations on the servername
 - Checks against a simplistic set of known words
 - Must be alphanumeric
 - 3 letter difference from the prior password
- SHA-1 Hashing with salt!!
 - Bummer – still stores old hash!



Ross Group Inc

SYSDBA and SYSOPER

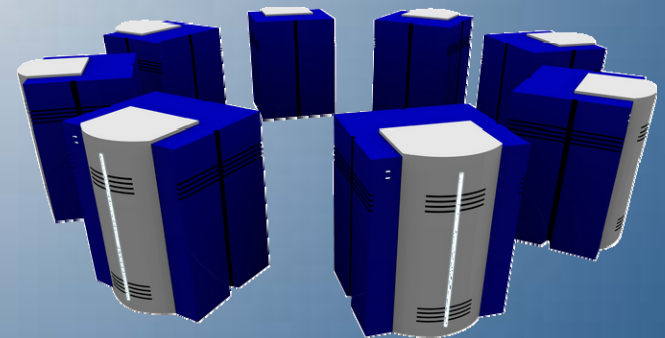
- Kerberos Authentication
- SSL Authentication



Ross Group Inc

SYSASM

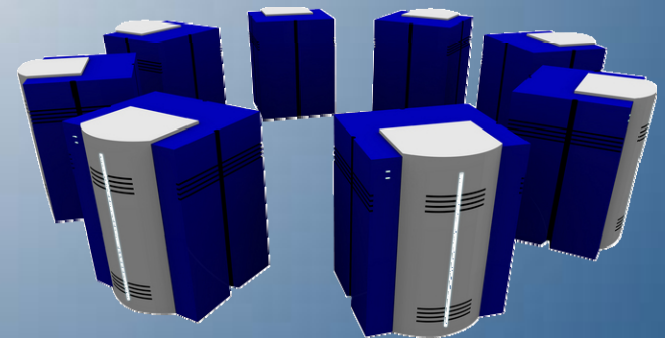
- New privilege for ASM only administration
- Role division between admins



Ross Group Inc

Encryption

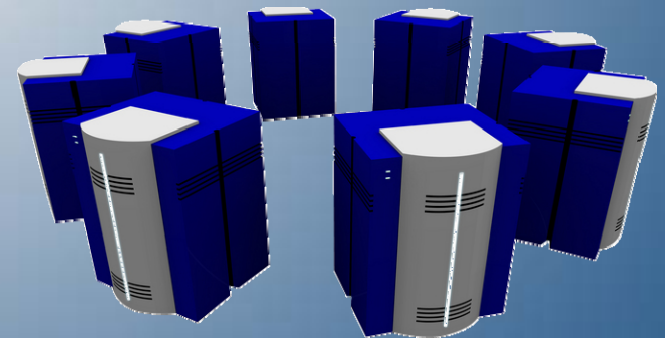
- SecureFiles LOB for encryption
- DataPump can Encrypt and Compress exports
- Hardware Security Module Integration for Transparent Data Encryption
- Transparent Tablespace Encryption



Ross Group Inc

FGAC on Network Services

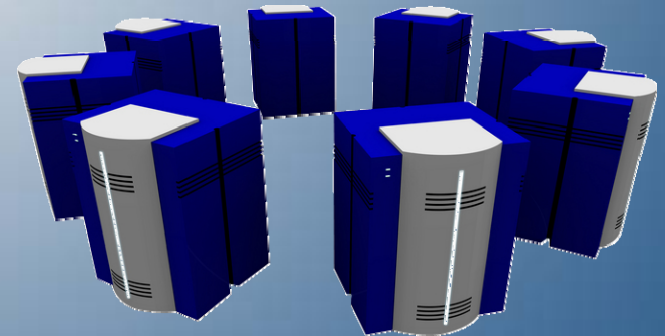
- Creates Access Control Lists in XML DB for services and privileges for the database
- Since this requires XMLDB it creates a larger footprint for defending the install



Ross Group Inc

XML DB

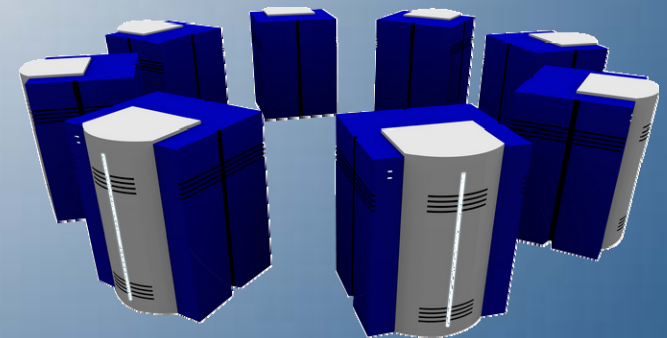
- XML Translation Support builtin
 - Language translation is builtin – no external addons required...
- SOA Web Services support was added
 - How is this more secure?
 - We can manage security and access to the web services in the database.



Ross Group Inc

Directory Enhancements

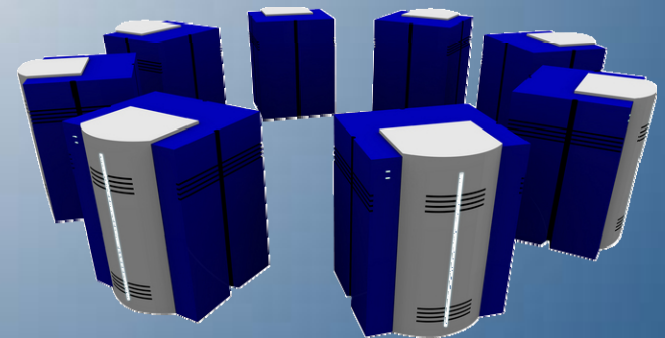
- Administrators may now disallow Anonymous access and require authentication for LDAP lookups – nice...



Ross Group Inc

OCI Enhancements

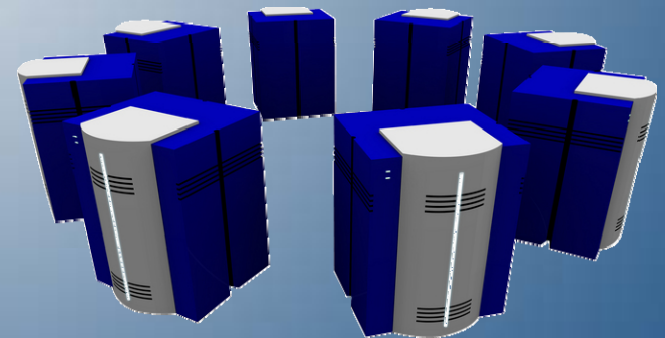
- Report bad packets
- Terminate connections on bad packets
- Set maximum authentication attempts
- Hide the version banner on connect
- Create a custom banner for warnings



Ross Group Inc

Oracle 11G Options

- Data Vault
 - Protect Data from unauthorized users
 - Even DBAs
- Audit Vault
 - Store all Audit data in One Place!
- Secure Backup
 - Encrypt Tape
 - ~\$3K per tape drive



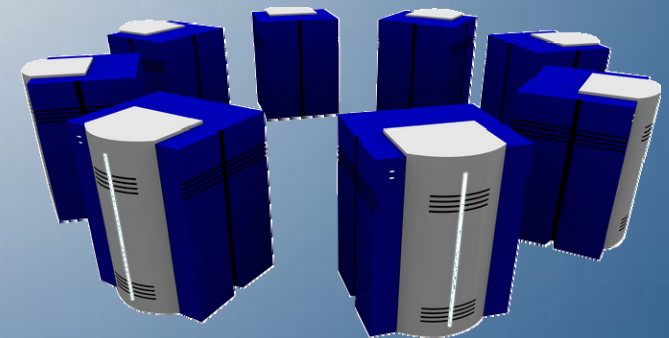
Ross Group Inc

Oracle Vulnerabilities (Addressed?)

- Leaked password hashes (we changed the hash) SHA-1 and added salt
- Weak passwords and default users (we identified the default passwords for the default users)
- Too many features enabled (we still do this)
 - APEX increases the target
- No audit enabled (enabled 11G)
- TNS is an easy target (protected with ACLs and other security features)

Listener

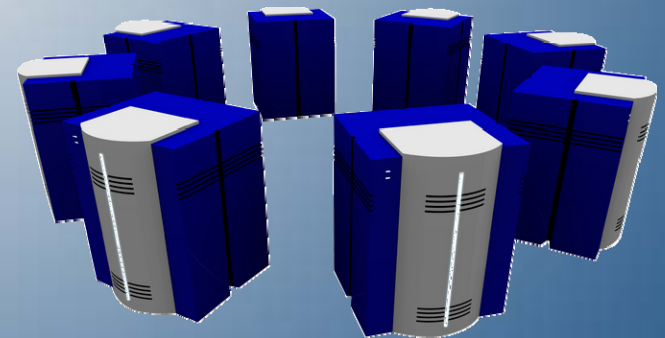
- No password management – still a problem
- No failed login attempts
- No default logging
- Set a password – 10g has local authentication
- Turn on logging
- Check the logs!



Ross Group Inc

Files (installer set permissions?)

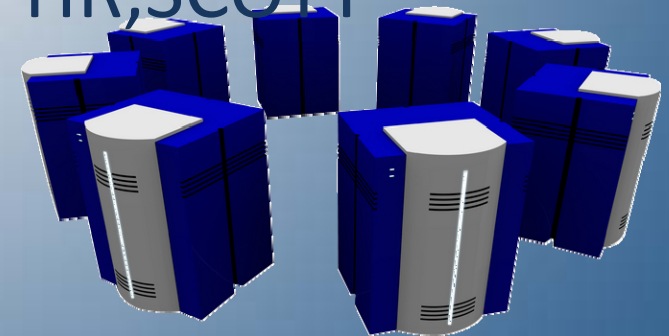
- Set Permissions on Important Files
- Listener.ora
- Tnsnames.ora
- Sqlnet.ora



Ross Group Inc

Internals

- Check for password=username
- Check for default passwords
 - 11G makes it easy
- Check your users' passwords with a brute force or dictionary attack – orabf, checkpwd
- Remove schemas not in use “HR,SCOTT”
- Enable profiles for users



Ross Group Inc

11G Internals

- The DBA_USERS view no longer exposes password hashes
 - But they are still in the base table!!
- Logging is more centralized and most logs are XML
- DDL can be logged to the XML alert log
- _dbms_sql_security_level prevents cursor snarfing and injection
- Cursor numbers are randomly generated now

Where to find more?

- Oracle Documentation - <http://tahiti.oracle.com>
- Default passwords - http://www.petefinnigan.com/default/default_password_checker.htm
- Password cracker (orabf) - <http://www.toolcrypt.org>
- Privilege audit scripts
- CIS Oracle benchmark - http://www.cisecurity.org/ench_oracle.html
- Patrik Karlsson (OAT,OScanner) – <http://www.cqure.net>
- Listener audit tool – <http://www.integrigy.com/downloads/lsnrcheck.exe>
- Backtrack CD - <http://www.remote-exploit.org/index.php/BackTrack>
- White Papers on Forensics and Commercial scanner - <http://www.ngssoftware.com/>

Thanks! Q&A

The Last Slide

Ron Shaffer
Ross Group Inc

Solutions For A Data Intensive World