
ORACLE®

GRID Computing Dynamics

Geoffrey Brown
Director, Grid Technologies

Advanced Technology Solutions
Technology Business Unit

Oracle Corporation

Bryan Pryce
Director of Architecture

Asia Pacific

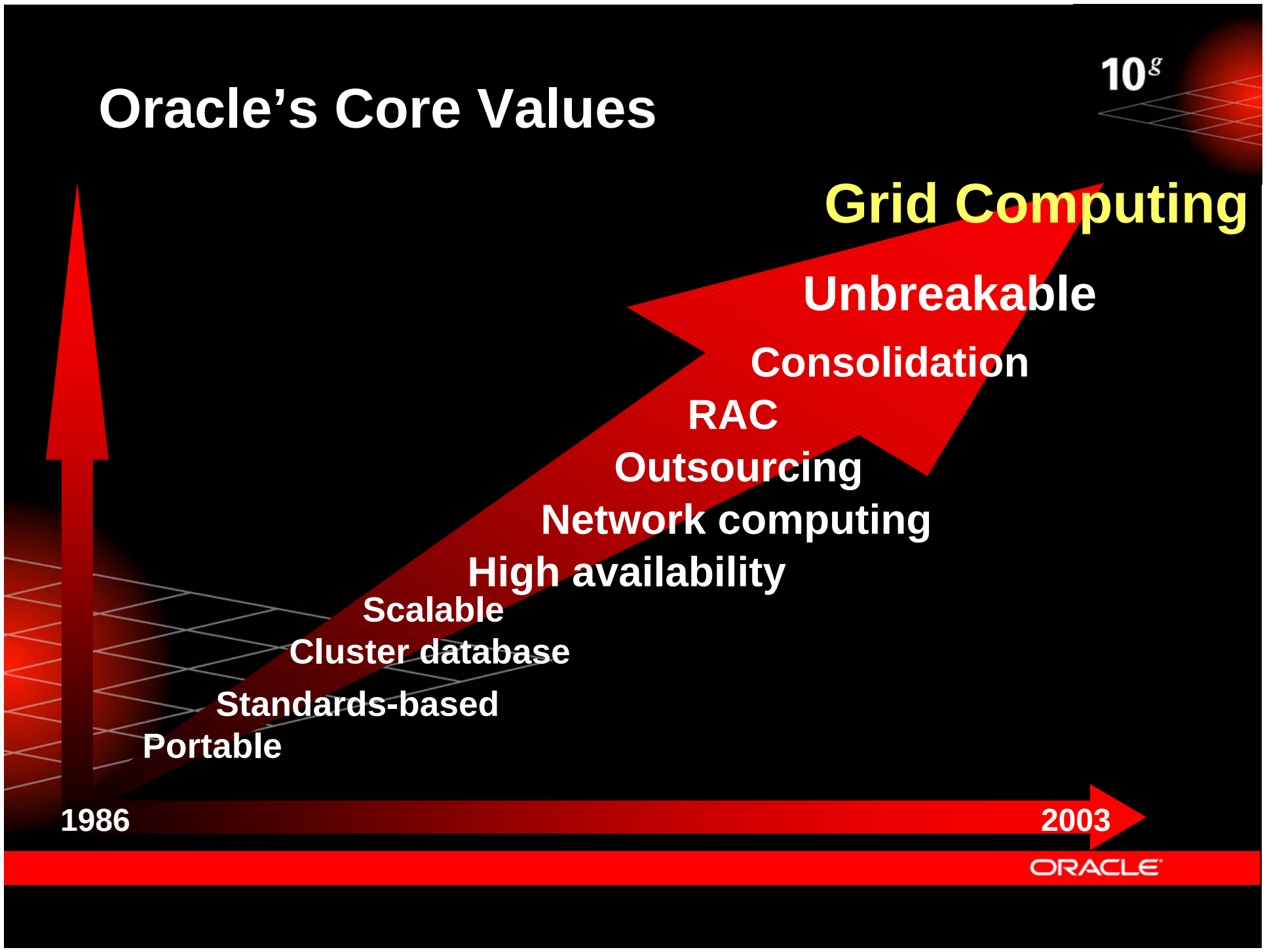
Oracle Corporation

ORACLE

Agenda

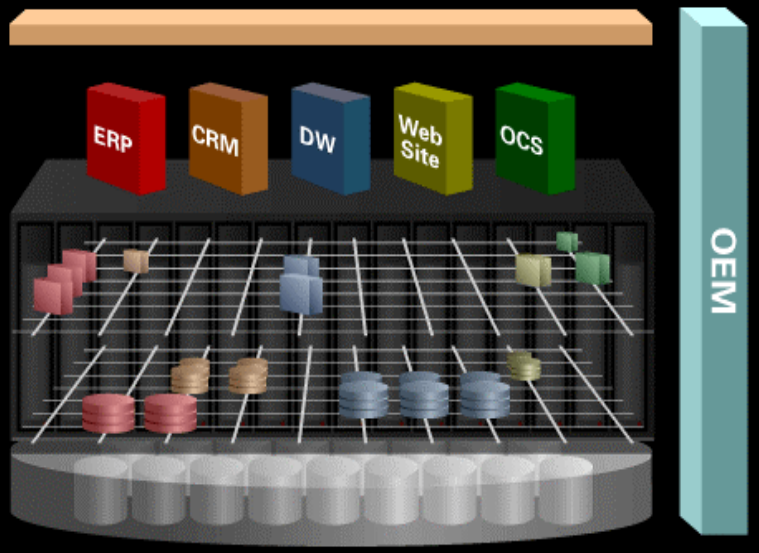
- **Oracle's Core Values**
- **The GRID Environment**
- **What GRID Services are needed**
- **Security**
- **Privacy**

Oracle's Core Values



The GRID Environment

10g



Technology

- Interoperability
- Advancement in efficiency
- Autonomics & Virtualization
- Self management
- Dynamic behaviour

Applications

- HPC Demand
- Business Transaction Management
- Bio Informatics
- Workload Management
- GRID TP vs Batch

Economics

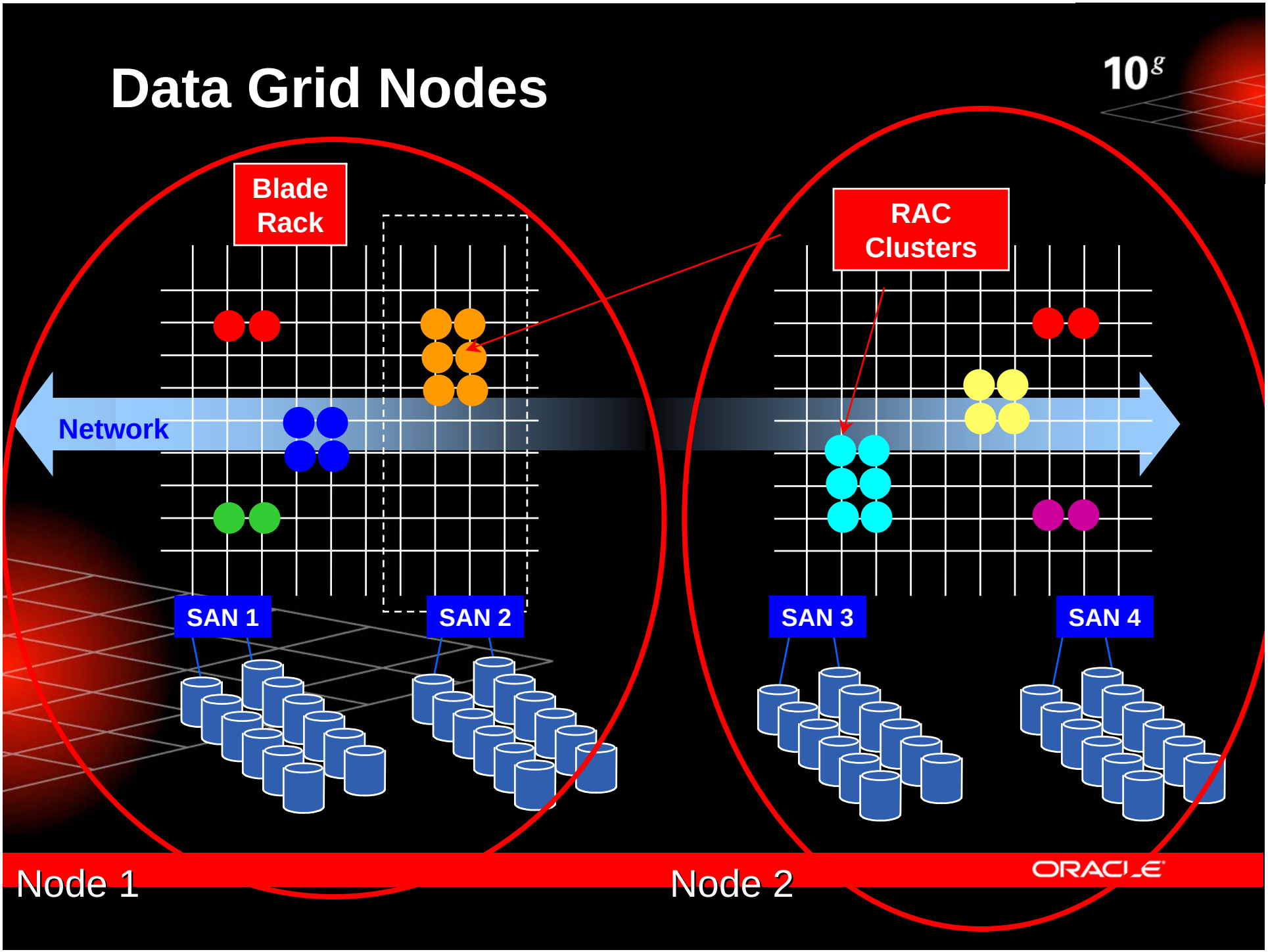
- ROI - Consolidation
- Event acceleration
- Evolutionary investments

Oracle Grid Principles

10g

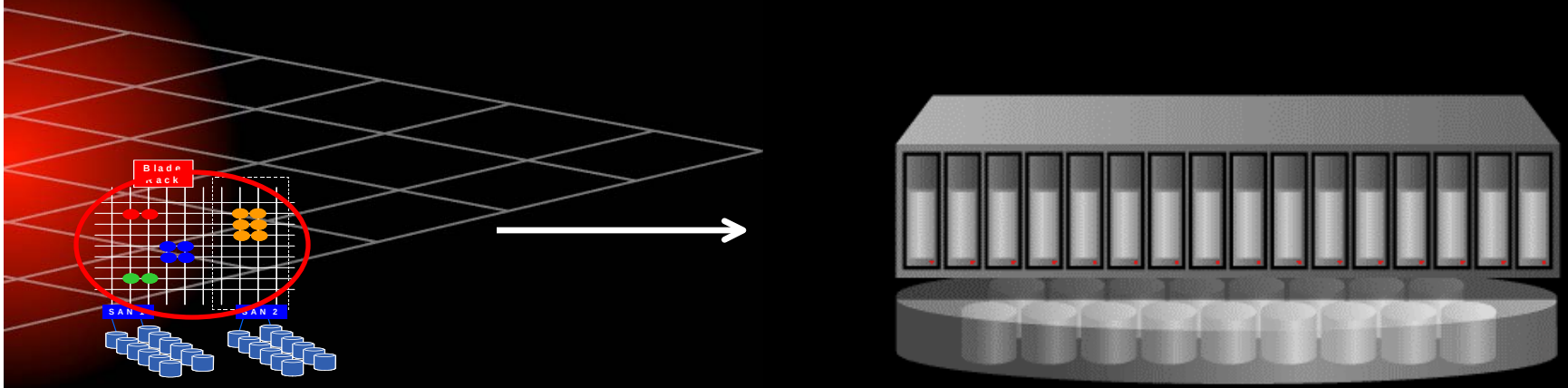
- Commodity Components
- Start with the nodes (consolidate, cluster)
- Evolution not Revolution
- Scale Up and Scale Down
- Batch AND OLTP
- Integrated stack for alternative QoS
- Secure and interoperable

Data Grid Nodes



Processor Virtualisation: Blades

- Flexible add/remove blades
- Operate in presence of blade failure
- Automatically provision blades
- Manage blade farm as single system(Data Grid Node)

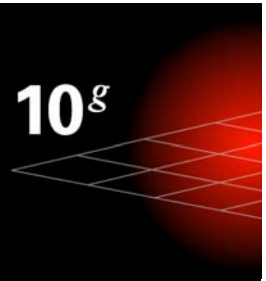


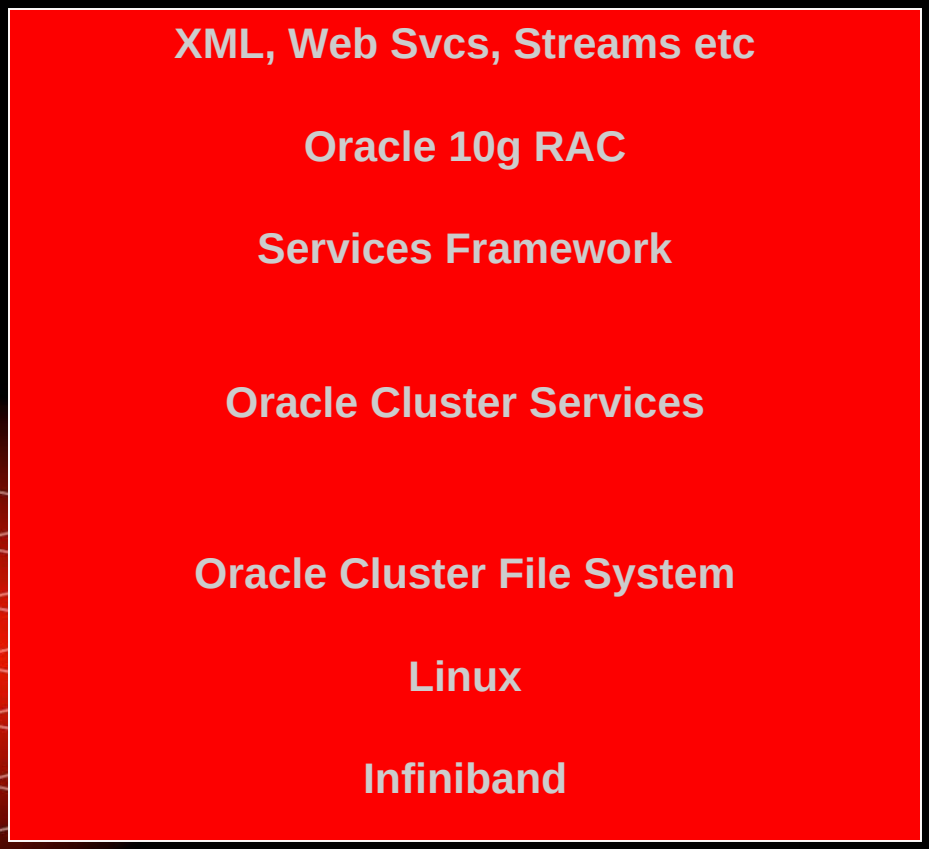
Processor Virtualisation: Blades

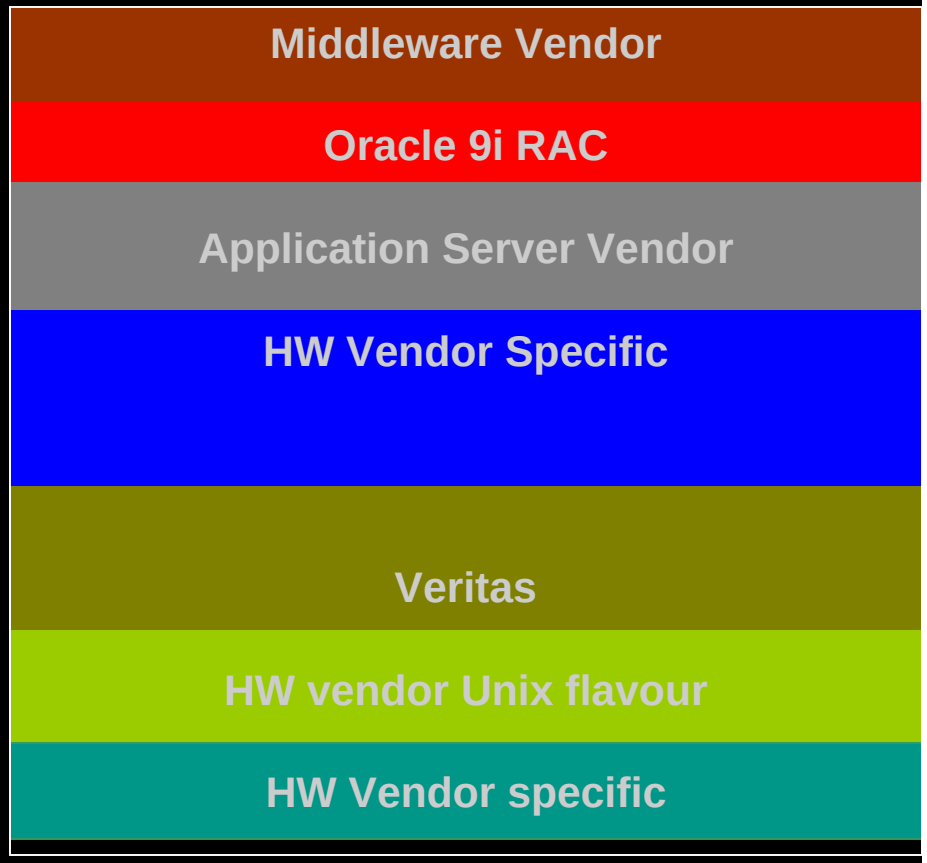
10g

- Add/Drop Node
  - Dynamic Provisioning using DBCA
- Fault tolerance
  - Makes commodity components unbreakable
- Rolling Upgrades
  - Patch with no downtime
- Cluster Workload Management with Resonance
  - Automatically provision CPU across multiple databases to meet workload service objectives
- Automatic Service Provisioning
  - Provision cpu within a database via services

Increasing Availability = Reduced Complexity







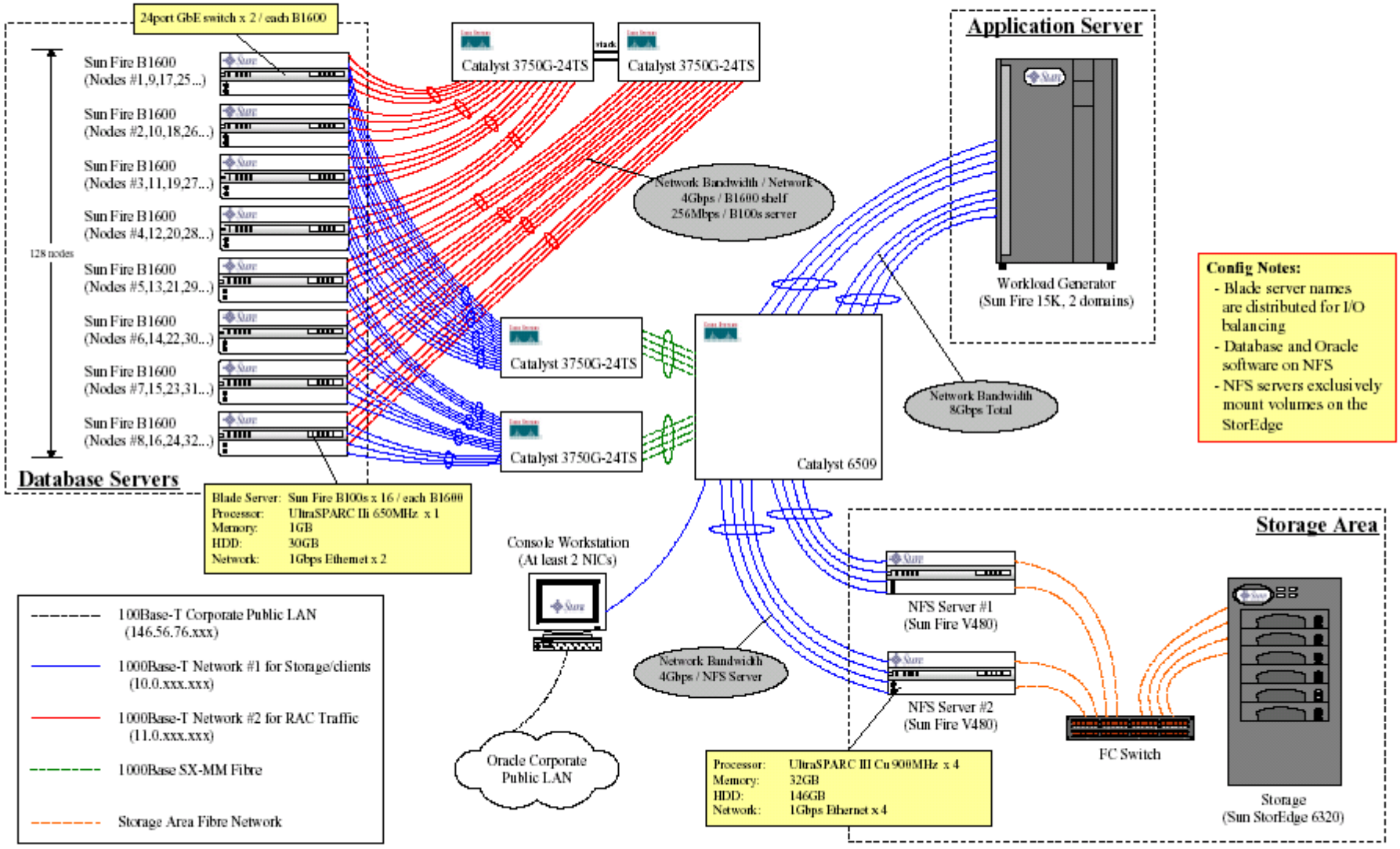
Oracle on Linux at AppsWorld

- 128 “blade servers” for the RAC instances
- Two NFS servers for storage
- Two workload generator servers
- Two network segments
  - #1 for CSS / RAC traffic
  - #2 for NFS / Application traffic

- System overview diagram available at:
  http://files.oraclecorp.com/content/AllPublic/Workspaces/128-Project%20G%20%28World%20Record%20Challenge%29-Public/System%20Configuration.pdf

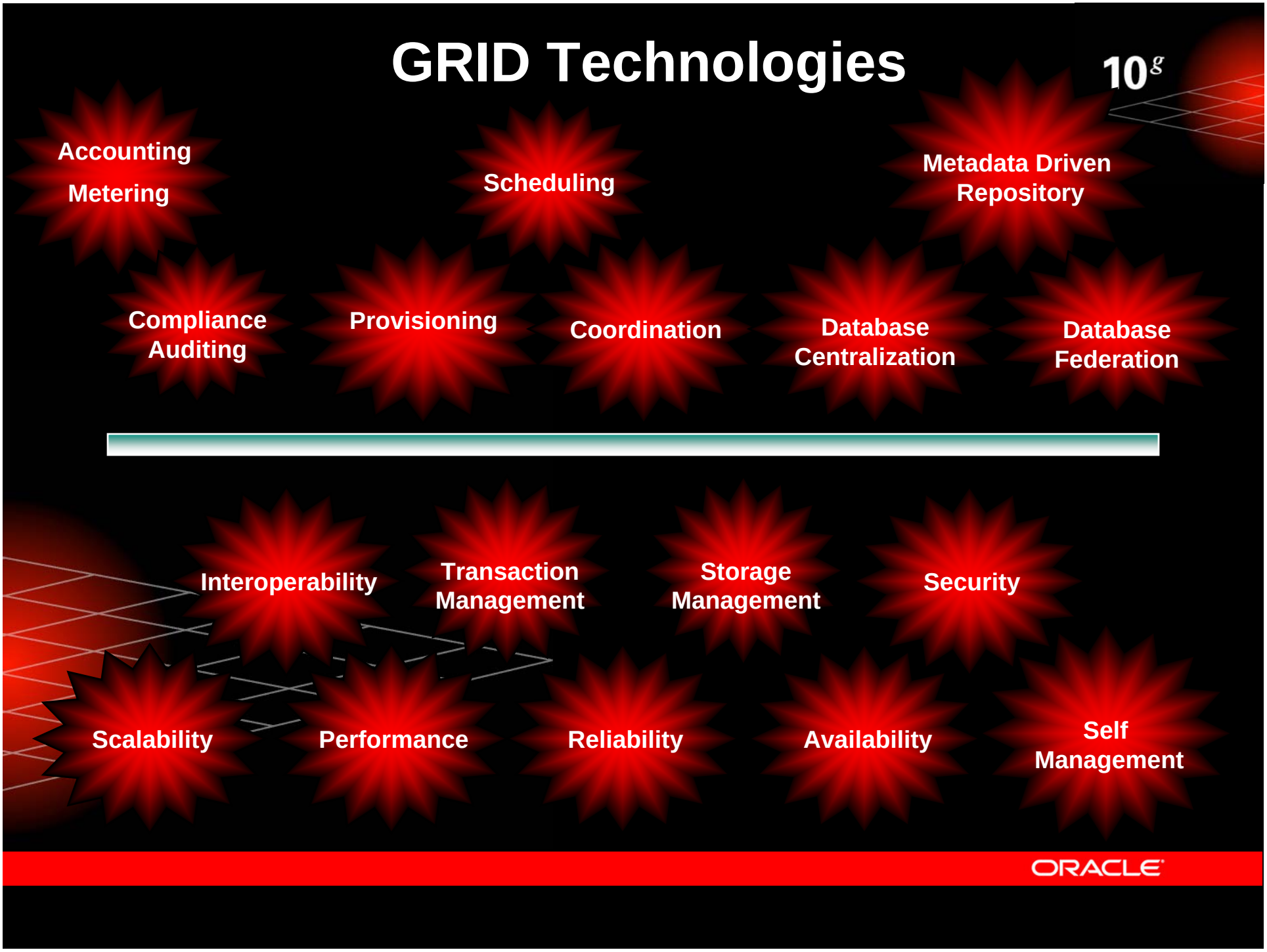
Hardware/Network Configuration for Oracle Database 10g Demo at Oracle World Tokyo

Author: atsushi.morimura@oracle.com Date: Nov-11, 2003 Version: 1.3



GRID Technologies

10g



ORACLE

What Services do Grids need ?

10g

- Authentication – Is the person or process who they say they are ?
- Access Control – Do they have the right to perform the operation or access the data ?
- Data Integrity – Has the data been tampered with ?
- Auditing / non-repudiation
- Public Key Infrastructure – distribute and manage identity and encryption

Manage and Secure GRID Infrastructure

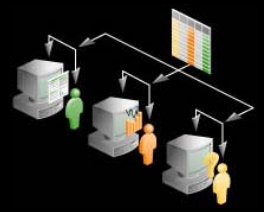
Web Site(s)

J2EE apps &
Web Services

Oracle Internet Directory

Oracle Enterprise Manager

Security



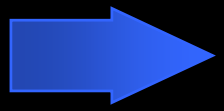
Internet / intranet Users

Oracle Instances and Clusters

- Integrated Management and Security Framework
- One tool for application server and database administration
- One unified, end-to-end security model for App Servers & DB's
- One directory to manage all of your users and privileges

Security Answers

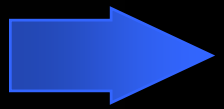
- Privacy of Communications



Is an order read or modified in transit?

Network encryption

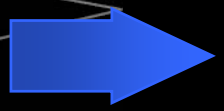
- Sensitive Data Storage



Is your private info in the clear?

Encryption of stored data

- Granular Access Control



Can a customer see only *her own order?*

Virtual Private Database

Grid Security Standards

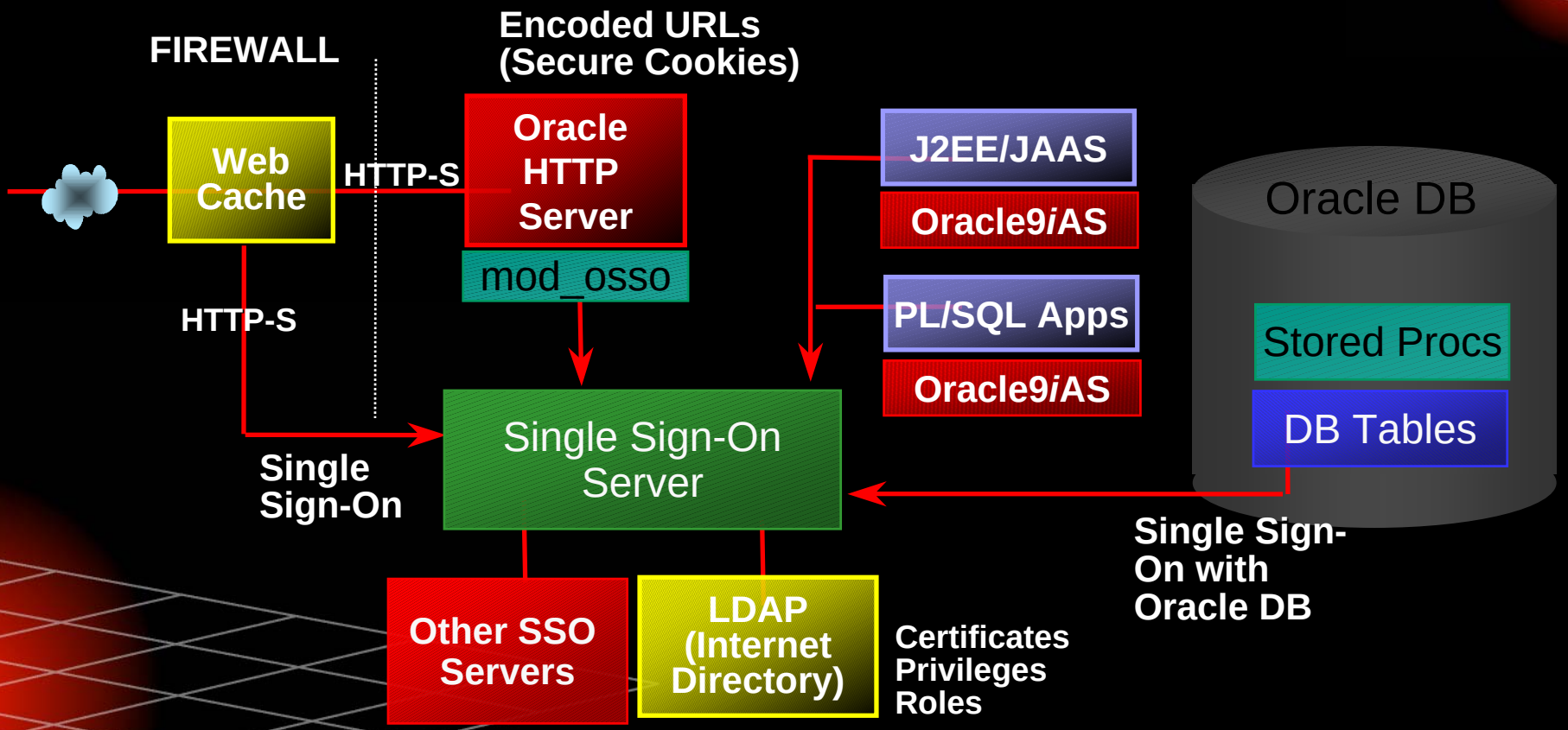
10g

- Open Grid Services Architecture (OGSA) specifications were submitted on 7/19/2002
  - By default, the underlying communication is based on the mutual authentication of digital certificates and SSL/TLS.
  - Makes heavy use of Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL), and Web Service Inspection (WSI).
- Globus add some extensions on Grid Security Infrastructure (GSI). It is based on the Generic Security Service API, which is a standard API promoted by the Internet Engineering Task Force (IETF).

In the meantime, we already have a standards based approach…

Directory and Security Services

10g



- Integrated Standards Based Security Framework
- One unified, end-to-end security model for App Servers & DB's
- One directory to manage all of your users and privileges

Java Security - JAAS

10g

- What is JAAS?
  - Java package that enables services to authenticate users and enforce access controls (authorization)
  - Implements a Java version of the standard Pluggable Authentication Module (PAM) framework
  - Delegation (enabling code to run securely, with privileges of other users)
- What is Available
  - Oracle's JAAS (Java Authentication and Authorization Services) implementation, *plus extensions*

JAAS Authentication Features

- LoginModules
  - Enables customers to add strong authentication for Java-based applications
    - SSO
    - SSL
    - Custom
  - For example, a Java-based banking app could require challenge-response authentication
- Benefits
  - Ability to integrate Java apps with SSO
  - Extensible authentication

JAAS Authorization Features

10g

- JAAS Authorization
  - Support for hierarchical, role-based access control
  - Support for principal (that is, user) and code-based policies
  - Full support for Java2 permission model
- JAAS-LDAP
  - Centrally manage users, access control policies in Oracle Internet Directory
  - Scales to very large user communities
- JAAS-XML
  - Manage users, access control policies in XML files
  - Lighter weight than LDAP
  - Unlike principals.xml, obfuscates passwords

JAAS Delegation Features

10g

- Impersonation
  - support for impersonation of a specified user
  - includes RunAsClient and RunAsID
- Benefits
  - Enforcement of security principle of ‘least privilege’
    - users have *fewest* privileges required to do their jobs
    - users only exercise privilege in context of a well-formed business rule (e.g. an enterprise bean)

Network Encryption

- Secure Sockets Layer (SSL)
  - Internet standard encryption protocol for http
  - a.k.a. HTTPS
  - Provided by mod_OSSL
- Provides
  - Data confidentiality on the network
  - Data integrity on the network
  - Optional user authentication via PKI (X.509v3 certificate)
- Strong crypto for world-wide use
  - RC4/128
  - 3DES

Authentication

- Basic authentication
  - Username/Password
  - Widely used
- SSL
  - Based on “entire” client X.509v3 Cert
- SSO
  - Integrates HTTP Server with Oracle SSO
  - Uses mod_OSSO

Access Control

- Access control enforced on
  - URL patterns
  - Files
  - Directories
- Access protection based on combination of:
  - X.509 Certificate pattern
  - User identity
  - Group membership
  - Host name
  - IP address
  - Other characteristics (e.g., browser type)

Security Evaluations and Assessments

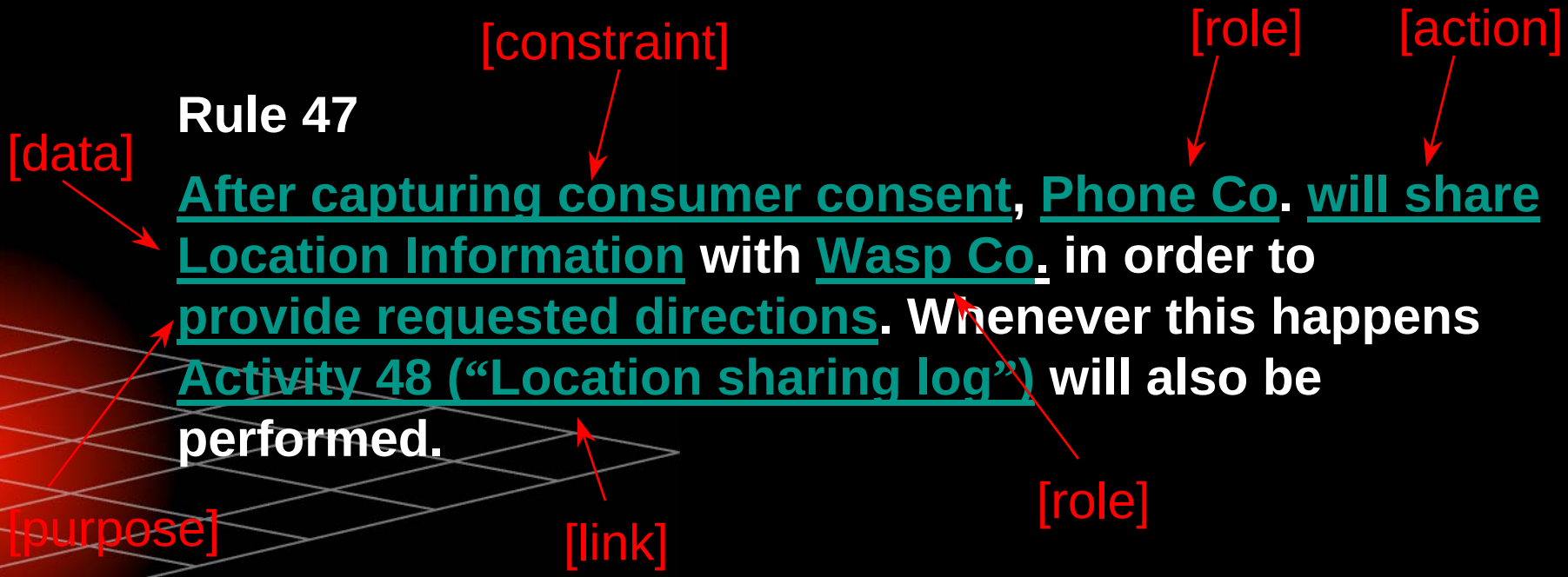
- Only Oracle has multiple independent security evaluations of the server
  - **14** independent security evaluations completed (Common Criteria, Orange Book, ITSEC) & first Common Criteria EAL-4 of any type
  - Standards-compliant (Common Criteria - ISO standard 15048)
  - FIPS-140 Level 2 certification for Oracle Advanced Security
- Independent evaluations provide the only real assurance that vendor's claims are real

Standards: PRML

- Privacy Rights Markup Language (PRML)
  - A privacy policy syntax
  - Focus on enforcement of privacy policies in servers
  - Semantics of policy are dependent on external references
  - PRML proposed to standards body
  - Supported by ZeroKnowledge and IBM

Standards: PRML

- Example



Existing Support

- Many requirements satisfied using existing features
  - Policy and Preference Repository
    - Directory
  - Privacy enforcement and auditing
    - Authentication - SSO
    - Access Control - OLS, FGAC, Views
    - Auditing - Fine Grain Audit, SYS Auditing
    - Application Context
    - Database Encryption
    - Digital Signatures

10g

Enforcement: Oracle Label Security

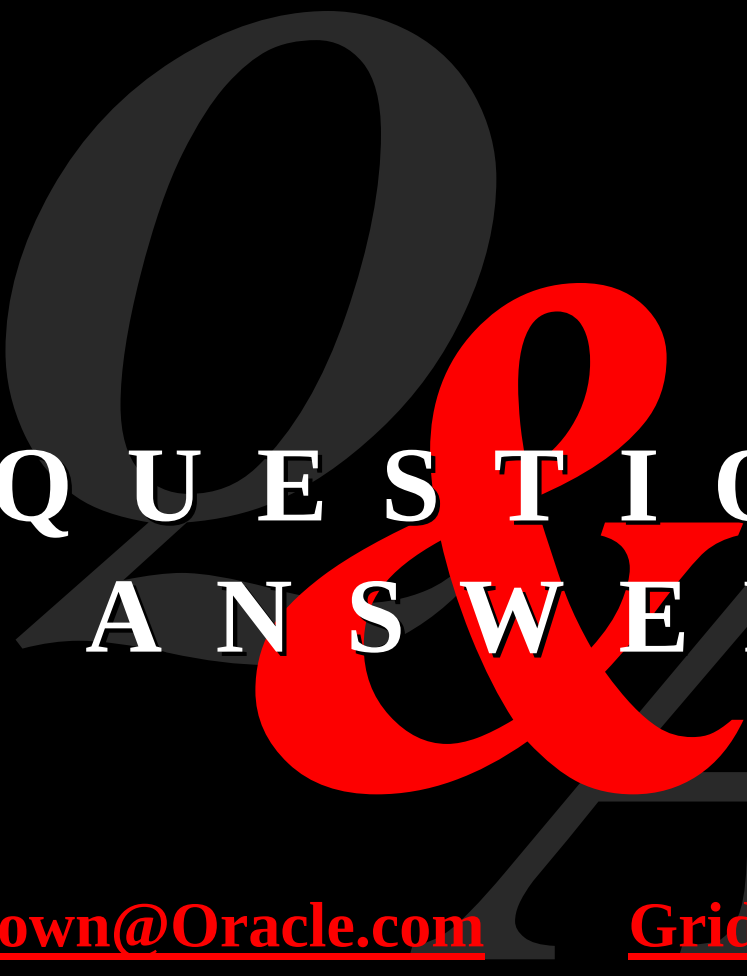
- Oracle Label Security (OLS)
  - Framework for simplifying use of FGAC
  - Shipping since 12/2000
- Labels
  - Level: CONFIDENTIAL, SECRET, TOP SECRET
  - Compartments: FINANCIAL, STRATEGIC, NUCLEAR
  - Groups: HR, PAYROLL, ENGINEERING
- Access Controls
  - Level(User) $\geq$ Level(Data)
  - Compartments(User) $\supseteq$ Compartments(Data)
  - (Groups(User) $\cap$ Groups(Data)) $\neq \varnothing$

Details of the OLS-based Approach

- Data Labels
  - Define Group Identifiers for each Purpose/Recipient pair
    - TELEMARKETING_OURS and DIRECTIONS_WASPCO
  - For each column C_i in a ROW construct a group G_i with:
    - Each mandatory purpose/recipient allowed
    - Each optional purpose/recipient allowed by the user
  - The data label for the row has Groups = $G_1 \cap G_2 \cap \ldots G_n$
  - Row is accessible if user is entitled to access ALL columns in the row
- User Labels
  - User is assigned a label with Groups containing every purpose/recipient pair they are allowed to access.

Enforcement: Relevant Column VPD

- VPD policy is triggered when a set of relevant columns are accessed
- Each type of data can have its own access policy
  - Attach appropriate policy based on data type of each column
- Access policy can depend on: purpose, recipient and user preference
  - Policy references user preference and privacy policy



QUESTIONS ANSWERS

Geoffrey.Brown@Oracle.com GridProjects_us@Oracle.com
Bryan.Pryce@Oracle.com

ORACLE