OpenWorld 2017
Exadata Security Best Practices

Strategy, Tactics, and Real-World Experience

October 1–5, 2017
SAN FRANCISCO, CA

Jeffrey T. Wright, Oracle Sr. Principal Product Manager
Dan Norris, Oracle Consulting Member Technical Staff
Daniel Munteanu, IT Technical Architect

Oct 4, 2017

Presented with

GROUPE SOCIETE GENERALE

ORACLE

Safe Harbor Statement

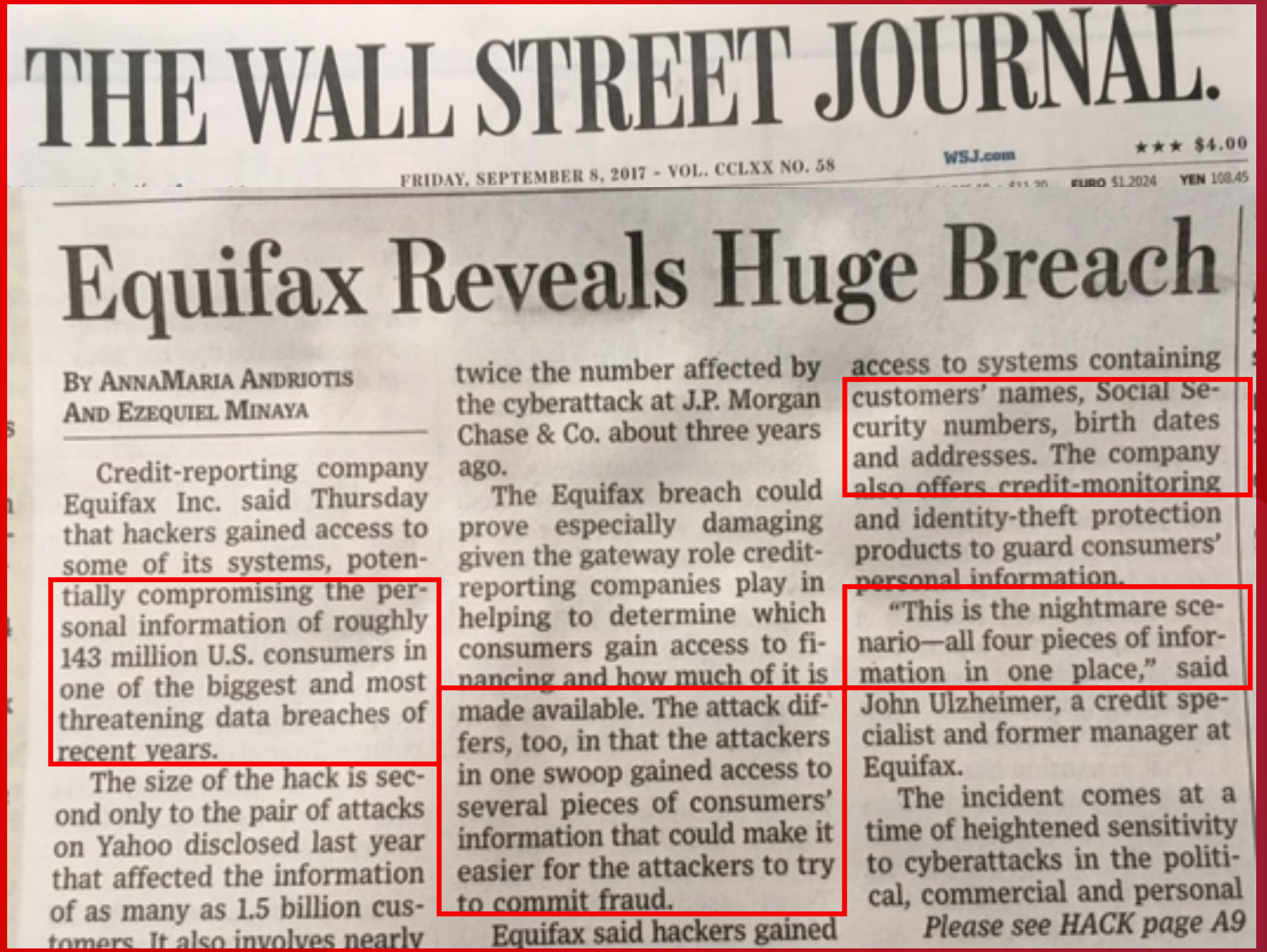
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

How Did This Happen?

Nearly half of the adults in the US were likely affected

Our enemy is evolving

[Cyber]war is upon us



THE WALL STREET JOURNAL.

FRIDAY, SEPTEMBER 8, 2017 - VOL. CCLXX NO. 58 WSJ.com ★★★ $4.00

EURO $1.2024 YEN 108.45

Equifax Reveals Huge Breach

By AnnaMaria Andriotis And Ezequiel Minaya

Credit-reporting company Equifax Inc. said Thursday that hackers gained access to some of its systems, potentially compromising the personal information of roughly 143 million U.S. consumers in one of the biggest and most threatening data breaches of recent years.

The size of the hack is second only to the pair of attacks on Yahoo disclosed last year that affected the information of as many as 1.5 billion customers. It also involves nearly twice the number affected by the cyberattack at J.P. Morgan Chase & Co. about three years ago.

The Equifax breach could prove especially damaging given the gateway role credit-reporting companies play in helping to determine which consumers gain access to financing and how much of it is made available. The attack differs, too, in that the attackers in one swoop gained access to several pieces of consumers' information that could make it easier for the attackers to try to commit fraud.

Equifax said hackers gained access to systems containing customers' names, Social Security numbers, birth dates and addresses. The company also offers credit-monitoring and identity-theft protection products to guard consumers' personal information.

"This is the nightmare scenario—all four pieces of information in one place," said John Ulzheimer, a credit specialist and former manager at Equifax.

The incident comes at a time of heightened sensitivity to cyberattacks in the political, commercial and personal

Please see HACK page A9

Program Agenda

1. Security terminology
2. Thread agents and attack techniques
3. Strategy
4. Tactics - Architecture and implementation with Exadata
5. Real world experience from BRD

Security Terminology

- Attack surface - Code within a computer system that can be run by unauthorized users
- Port - Network term referring to a virtual endpoint
- Service – Operating system term for background process or daemon
- Critical Patch Update (CPU) - Quarterly released security patches for Oracle products
- Authentication – Are you who you say you are?
- Authorization – Are you allowed do to what you have asked to do?

Threat Agents

- Unstructured hacker
- Structured hacker
- Organized crime, industrial espionage
- Insider
- Unfunded terrorist group or hacktivist
- Funded terrorist group
- Nation state

https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf

Attack Techniques

- Penetration
  - Infrastructure
  - Platform
  - Database
  - Application
- Insider placement
- Insider recruitment
- Diversion

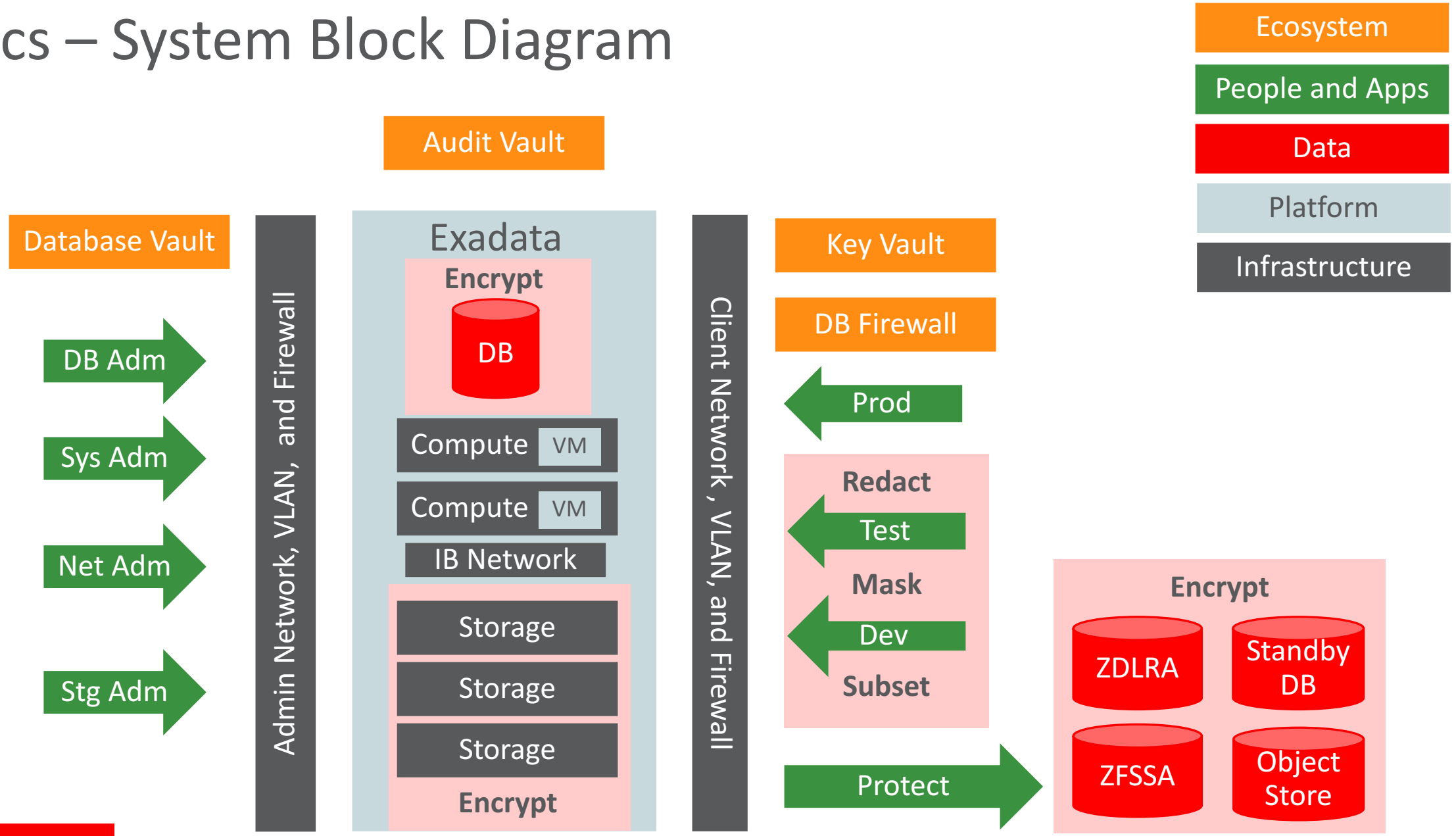
- Denial of service
- Distributed denial of service
- Interception/sniffing
- Spoofing/masquerading
- Substitution/modification
- Direct malicious code
- Indirect malicious code

https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf

Strategy

- Fix vulnerabilities under our control
  - Don’t orient on threats that are out of our control
- Minimize attack surface
  - Code available to execute, ports and services, visible data
- Separate roles and require coordination of disinterested parties
  - Disinterested action and auditing to keep parties honest
- Authentication, authorization, and auditing
  - Make sure people are who they say they are
  - Make sure person is allowed to take the specific action
  - Make sure we are aware of everything that person is doing

Tactics – System Block Diagram



Exadata Infrastructure Security Features

- Signed firmware
  - Ensure pristine code running on chips
  - Eliminate hardware attack surfaces
- Smart storage – Exadata Storage Cell
  - Designed and built by Oracle for database security
  - Integrated with database security, including TDE
- InfiniBand storage network
  - Physical security through dedicated network
  - InfiniBand partitioning

Exadata Cell Lockdown

- Cells can have remote access disabled – no direct SSH access to OS
- Must enable temporarily for maintenance (upgrades)
- New cell attributes: remoteAccessPerm, remoteAccessTemp
- Can temporarily enable access, automatic lock up at a specified time
- Can still access console via ILOM
- Use exacli/exadcli from DB nodes for cell commands

Centralized Cell Syslog

- Cells have syslogconf cell attributes (for quite a while)
- DB nodes have /etc/rsyslog.conf
  - On 12.1.2.1.0 & later, also have syslogconf dbserver attribute

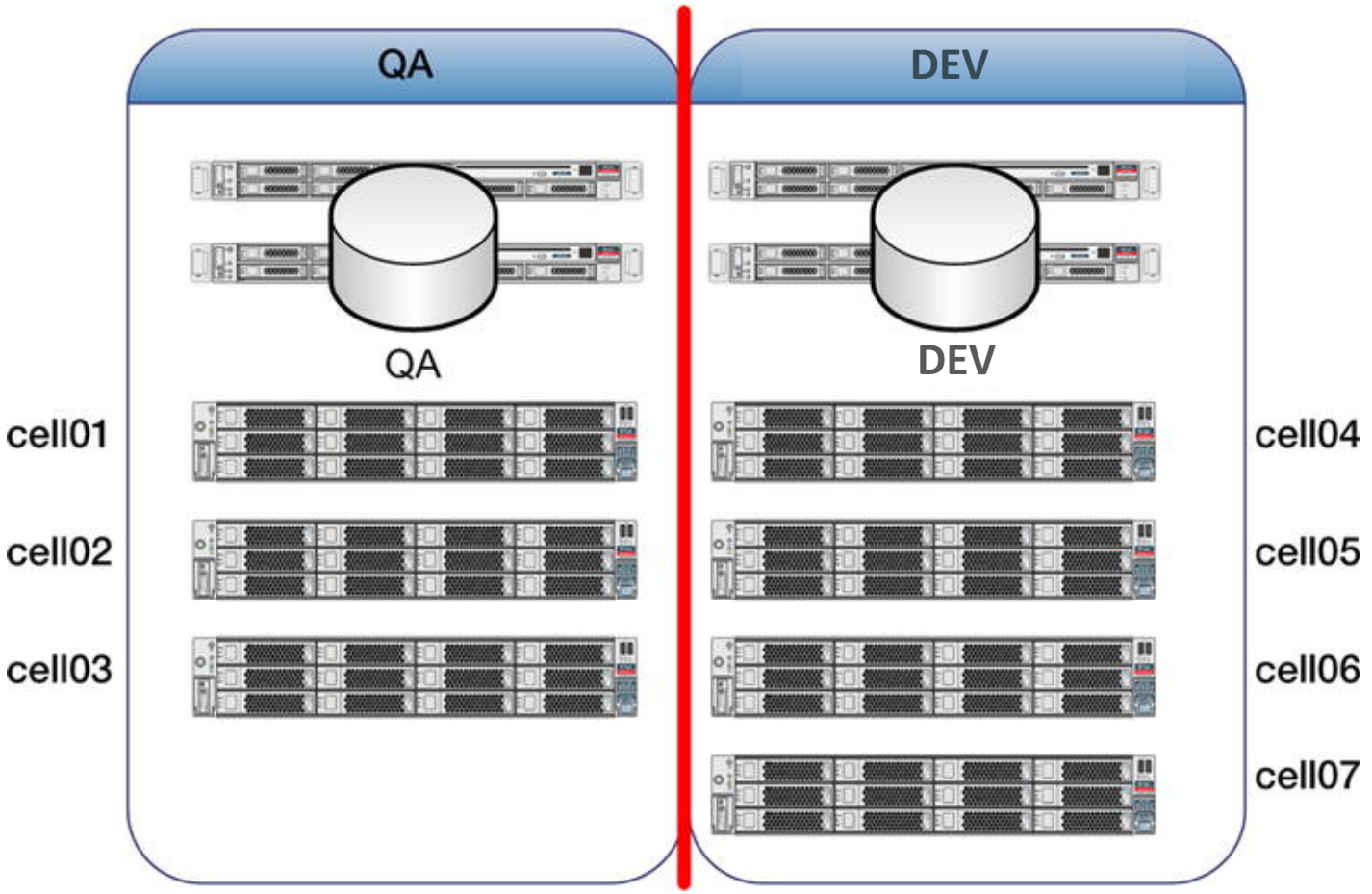
```
cellcli> alter cell syslogconf=('authpriv.* @syslgsrv', 'security.*
@seclogserver');

cellcli> alter cell validate syslogconf 'authpriv.error';

dbmcli> alter dbserver syslogconf=('authpriv.* @syslgsrv', 'security.*
@seclogserver');

dbmcli> alter dbserver validate syslogconf 'authpriv.error';
```

ASM-Scoped Security Mode



Exadata Cloud Service Network Security Features

- Firewall is built into the network
  - Software and hardware firewalls in Oracle Cloud Infrastructure
  - User self service and Oracle SR process
  - Default to deny all traffic, we require explicit opening of any communication
    - Port 22 open by default for SSH, customers may restrict port 22 access as appropriate
- VPN to connect to on-premises networks
- VCN and private network implementations available
- Comprehensive security rules, lists, and policies
  - Ensure only appropriate ports and addresses have access to your services

Exadata Platform Security Features

- Hardened Oracle Enterprise Linux
- Minimal software deployment
- User accounts are secure by default
- Linux firewall
- Exadata Cloud
  - Default configuration per Oracle security best practices
- Exadata Database Machine
  - Resecure Machine install step implements security best practices

Exadata Platform Default Security Implementation

- Short package install list
- Only necessary services enabled
- https management interface
- sshd secure default settings
- Password aging
- Maximum failed login attempts
- auditd monitoring enabled
- cellwall: iptables firewall
- CPUs included in patch bundles, releases synchronized
- System hardening
- Boot loader password protection

Basic Exadata Platform Security Best Practices

- Restrict root's login on DB nodes
  - Protect the console at the infrastructure level
- Disable direct login of privileged users on DB nodes
  - At least disable root, consider disabling oracle and grid
  - Currently, must enable root login during patching/upgrade events
- Use sudo to perform tasks as privileged users on DB nodes
  - Audit such actions, watch for unauthorized or unexpected access
- Use passwordless ssh for authentication
  - Passwords have too many attack surfaces, key management is easier

Post-Deployment Configuration

Address site-specific requirements

- Change all passwords for all default accounts (MOS 1291766.1)
  - Run: `exachk -profile security`
- Exachk: MOS 1070954.1
- Perform validation for local policies or rules
  - See MOS 1405320.1 for commonly identified audit findings

Oracle Database Security Defense in Depth

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key & Wallet Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
DBA Controls & Cyber Security	Auditing and Reporting	Configuration Management

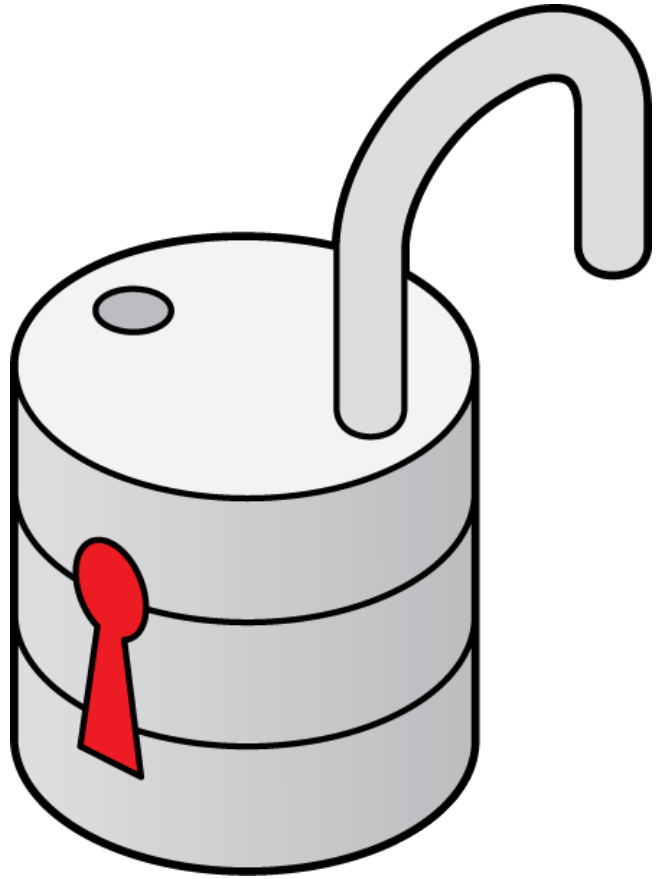
Protect the Data from Unauthorized Access

- Use TDE
  - Hardware offload for high performance
  - Included in Exadata Cloud subscription, enabled by default for database you create
  - You should enable when you migrate to Exadata Cloud
- Use data redaction, masking, and subsetting for non-prod
  - Remove non-prod attack surface for sensitive data
  - Mitigate risks when other security is minimized to make non-prod easier to use
  - Prevent unauthorized developers and testers from seeing sensitive information

Operational Security Considerations

Remain security-minded when patching, upgrading, backing up

- Changes permitted on DB nodes, not cells
- Backups can be encrypted
- Patching or upgrading may “undo” some changes; verify after
- DB node updates use yum commands with excludes (see doc for excludes)



Operational Security Considerations

Remain security-minded when patching, upgrading, backing up

- Periodic reviews to ensure settings remain and vulnerabilities don't
- Secure erase for storage cells is available
- Disk drive retention is available
- Oracle Enterprise Manager Governance, Risk & Compliance Manager continuously reviews the system

Operational Security Considerations

Patching considerations

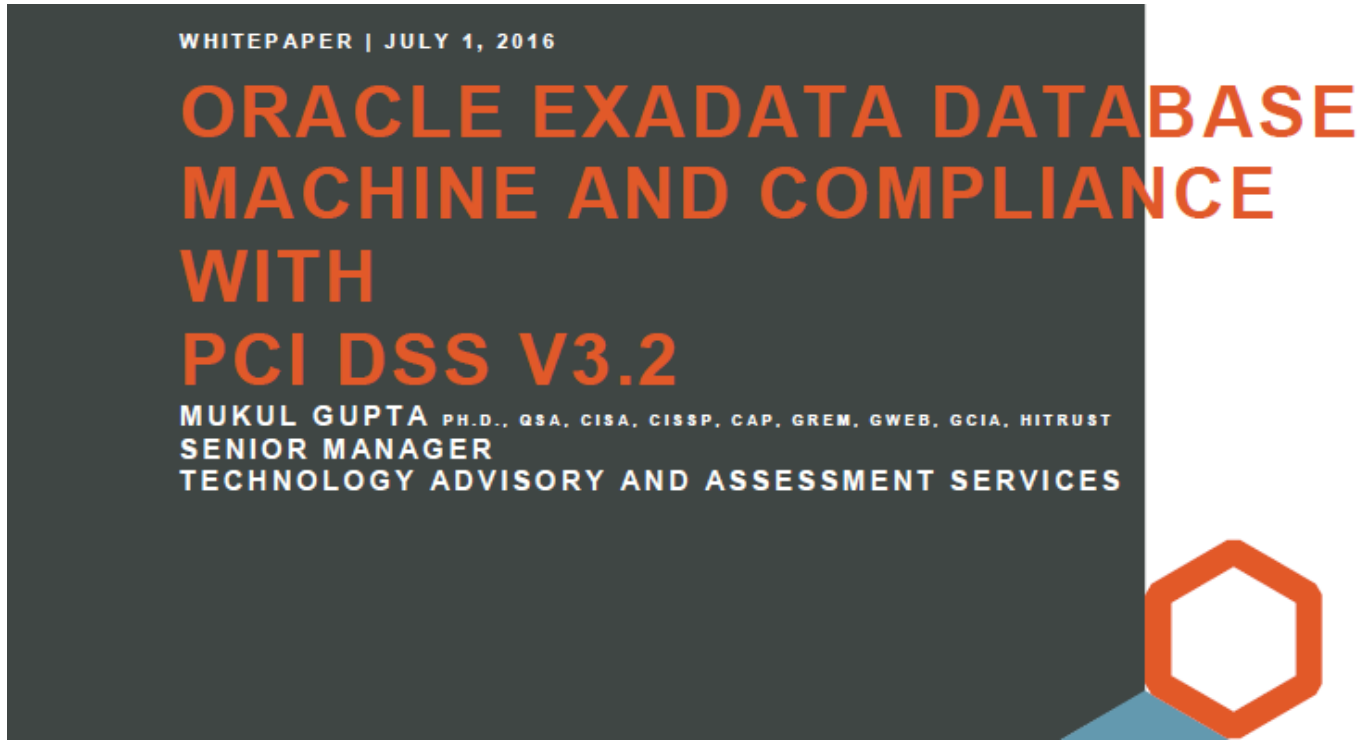
Component	Access Required
Database – Patch set	Database server root, software home owner, passwordless SSH to all software home owners (on other nodes)
Database – Bundle Patch	Database server root, software home owner
Grid Infrastructure	Same as Database
Exadata Database Server (OS)	Database server root, passwordless SSH to database server root
Exadata Storage Server	Database server root, passwordless SSH from database server root to storage server root (temporarily disable lockdown)
InfiniBand Switch	Database server root, InfiniBand switch passwordless SSH to switch root

Secure Technical Implementation Guide - STIG

Especially important to public sector

- ExadataSTIGFix script: How to configure and execute the ExadataStigFix script for Exadata STIG environments (Doc ID 2181944.1)
  - Script to implement additional security hardening for STIG customers
- SCAP: Oracle Exadata Database Machine DoD STIG and SCAP Guidelines (Doc ID 1526868.1)
  - Specific guidance on running SCAP reports, to include false-positive and mitigation

Compliance



- Exadata Database Machine can be used for PCI compliant systems
- Exadata Cloud at Customer PCI certification targeted Jan-2018
- Roadmap for Exadata Cloud at Customer
  - SOC 1 Type II, HIPAA, ISO 27001

http://www.oracle.com/technetwork/database/exadata/exadata-pci-dss-3101847.pdf

Presented with

BRD

GROUPE SOCIETE GENERALE

BRD Next GEN IT Infrastructure

Exadata Cloud at Customer project

Daniel Munteanu
IT Technical Architect
BRD - Information Technology Department

October 04, 2017

BUILDING TOGETHER
TEAM SPIRIT SOCIETE GENERALE

ORACLE

About BRD

BRD, member of Groupe Societe Generale is one of the market leaders in Romania for individual customers.
It counts 2.3 million customers, who are contacting the bank through classic branches, the Internet, the mobile phone and also through a high performance contact centre.

BRD is among the top banks active on the market of loans for individuals and on cards. The bank's sales force operates in a network of approx. 800 branches.
The bank is one of the major financers for the SMEs, as well as one of the most important players on the Romanian corporate banking

Societe Generale is one of the largest European financial services groups.
With more than 145,000 employees, based in 66 countries, accompany 31 million clients throughout the world on a daily basis. Societe Generale's teams offer advice and services to individual, corporate and institutional customers in three core businesses:

- Retail banking in France
- International retail banking, financial services and insurance
- Corporate and investment banking, private banking, asset management and investor services

Cloud transformation builds the essential foundations to digital transformation

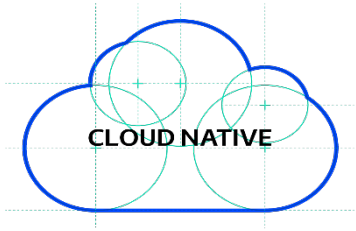
BRD
GROUPE SOCIETE GENERALE

BRD – IT Department strategy

What we propose as actor

We **already shifted** to full virtualized infrastructure

We promote the migration to **private cloud. We are ready**



We adopt **Cloud native architectures**

What we propose as catalyst & contributor

We setup **"Go to Cloud" services** to support application transformation

We contribute to **reduce traditional, heavy applications** footprint and simplification of the BRD's IS architecture

By 2021

Migration of 50% of our virtualized infrastructures to private cloud through self-provisioning, metering and charge-backing.

Cloud and Automation bring significant benefits

BRD
GROUPE SOCIETE GENERALE

Scalability

Cloud services consumption is **dynamic** and **scalable**, including workload peaks

Resilience & Security

Improved **production quality**
Simplified business continuity management

Time-to-market

Autonomy to **continuously deliver** business applications

Savings

Consistent savings,
mainly from **standardisation**

Pay-per-use

On-demand, on-spot
resources @ **effective cost**

Exadata Cloud at Customer implementation in BRD

BRD
GROUPE SOCIETE GENERALE

Project scope

- A solution for BRD's Oracle databases that provide high performance, high availability and scalability for any type of workload: OLTP, DW, mixed
- Flexible growth in a Pay as you Grow model
- Build a platform for IaaS (on OCM) for BRD Test&Dev teams

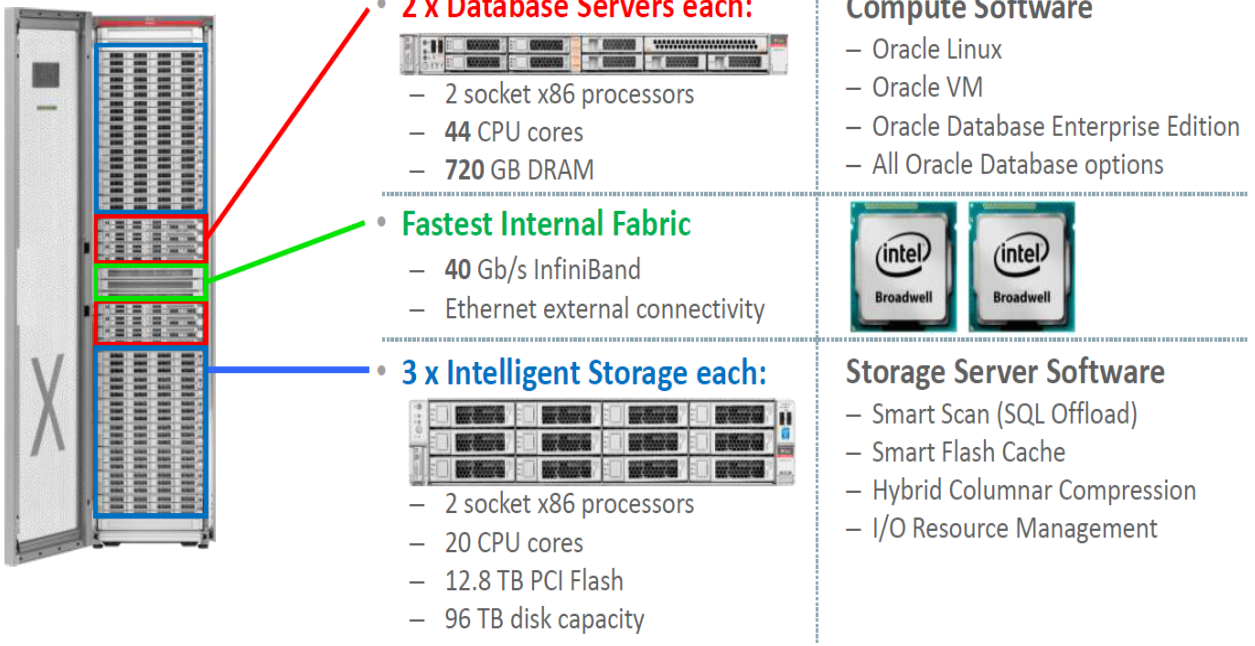
Perimeter

- 180 DBs Oracle on PROD/Test/DRC environment.
- All databases encrypted with AES 256. The encryption performance overhead was <2% due to AES HW acceleration on Intel chips.

Application details:

- Online banking
- Insurance
- Reporting (financial, risk, etc.)

Exadata Cloud at Customer – Hardware Details



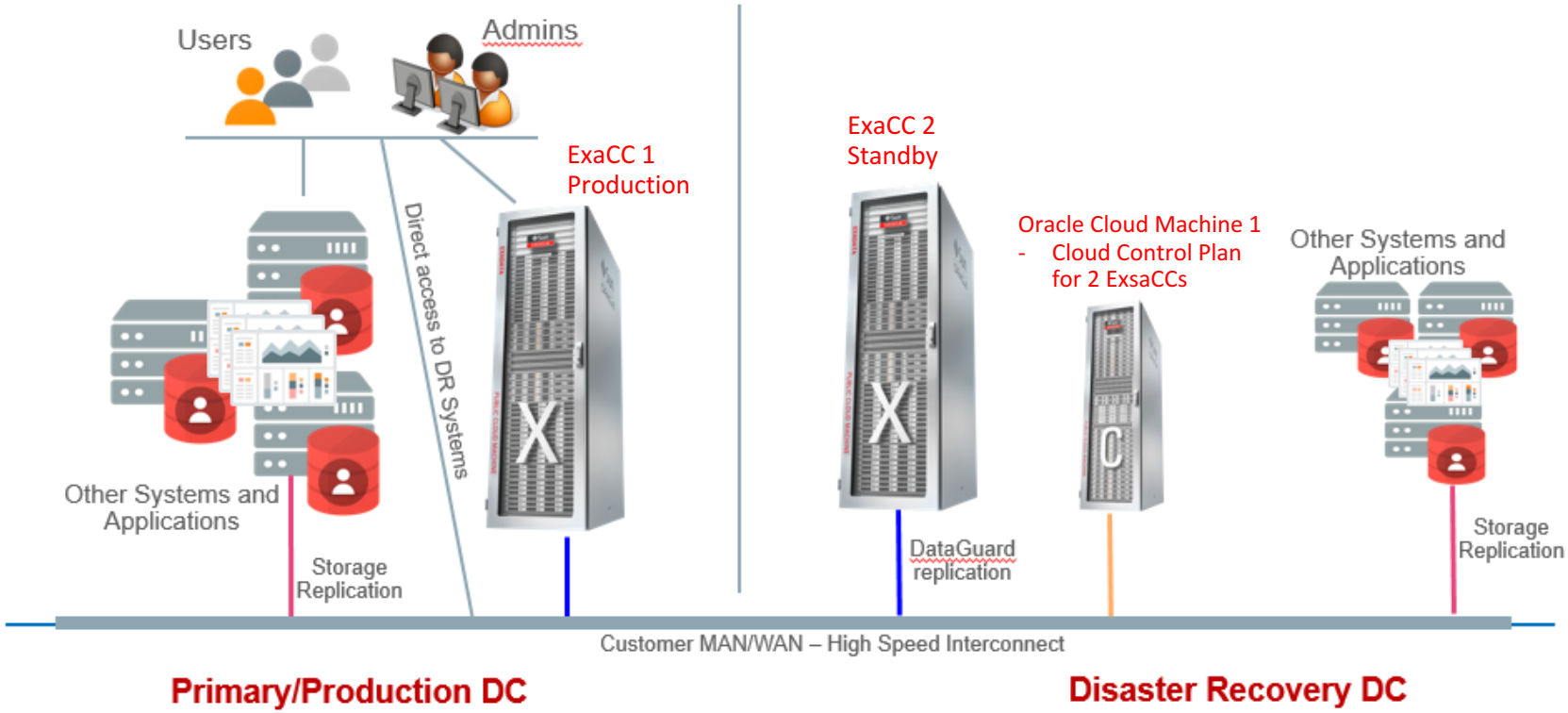
BRD Exadata Cloud at Customer Configuration:

- OCM Model 288
- Exadata Cloud at Customer Prod Quarter Rack
- Exadata Cloud at Customer DRC/Test Quarter Rack

Exadata Cloud at Customer architecture and security considerations

BRD
GROUPE SOCIETE GENERALE

- Firewalls secure internal BRD network using 10Gb throughput / port.
- Oracle Transparent Data Encryption used to encrypt all data tablespaces. Data is encrypted using AES 256 bit keys.
- Master keys stored outside of ExaCC in specialized Hardware Security Module.
- Disaster Recovery Site synchronized with Data Guard on a similar environment, secured with firewalls, AES 256 encryption, external Hardware Security Module.



Exadata Cloud at Customer – solution benefit

BRD
GROUPE SOCIETE GENERALE

Before

- Multiple DB servers with different versions, placed on different server platforms (IBM Power, Intel x86)
- Provisioning new database servers was a time consuming operation
- Hard to manage licensing
- Hard to implement a standard policy for backups
- DB disaster recovery based on storage replication

After

- All Oracle DBs are stored on ExaCC, engineered platform for Oracle Databases
- Provisioning new databases is done automatically using cloud interface
- All databases are stored on ExaCC
- All databases on ExaCC are backed up automatically to VTL using 10Gbps Eth
- Disaster recovery will be based on Oracle DataGuard (DB replication)

Benefit

- Improved performance, reliability and scalability. Pay per Use model with instant boosting.
- Reduced time to market, reduced human errors
- Simple licensing model – pay per use
- Standardization and reduced backup/restore windows for applications
- Reduced bandwidth for database replications, database consistency and simplified DRC procedures

BRD

GROUPE SOCIETE GENERALE

"Powerful Database Cloud Platform, fully licensed, scalable in just one click, in our datacenter."

Dan Lungu
Head of Database and Middleware Platforms
BRD - Information Technology Department

ORACLE

Next Steps – Get Educated

References

Note or URL	Description
http://is.gd/orasec	Oracle Security Alerts subscription
1068804.1	Guidelines for enhancing the security for an Oracle Database Machine deployment
1291766.1	How to change OS user password for Cell Node, Database Node, ILOM, KVM, Infiniband Switch , GigaBit Ethernet Switch and PDU on Exadata
888828.1	Exadata Database Machine and Exadata Storage Server Supported Versions
1405320.1	Responses to common Exadata security scan findings
http://is.gd/exaconsolidation	Oracle Exadata Database Machine Consolidation: Segregating Databases and Roles
http://is.gd/entsecassessment	Enterprise Data Security Assessment

References

MOS Note	Description
2069987.1	HOWTO: Update JDK on Exadata Database Nodes
2075464.1	HOWTO: Update JDK on Exadata Storage Cell Nodes
1070954.1	Oracle Exadata Database Machine exachk or HealthCheck
2207063.1	HOWTO: Install ksplice kernel updates for Exadata Database Nodes
1526868.1	Oracle Exadata Database Machine DoD STIG and SCAP Guidelines
1274318.1	Oracle Sun Database Machine Setup/Configuration Best Practices
1068804.1	Guidelines for enhancing the security for an Oracle Database Machine deployment

Integrated Cloud

Applications & Platform Services


ORACLE®