

ORACLE

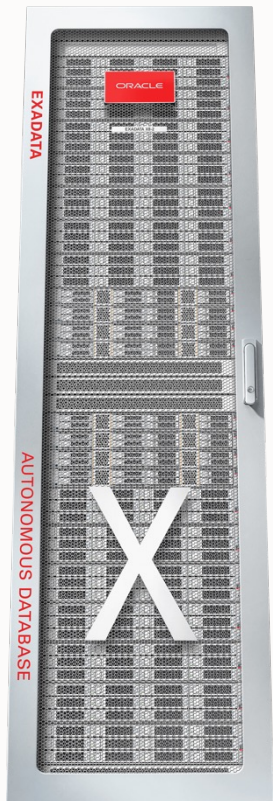


# Oracle Exadata Database Machine

Maximum Security Architecture to Protect your Data

# Exadata Maximum Security Architecture (MSA) Vision

Extreme Performance, Availability, and Security



## Database Aware System Software

Unique algorithms vastly improve OLTP, Analytics, Consolidation

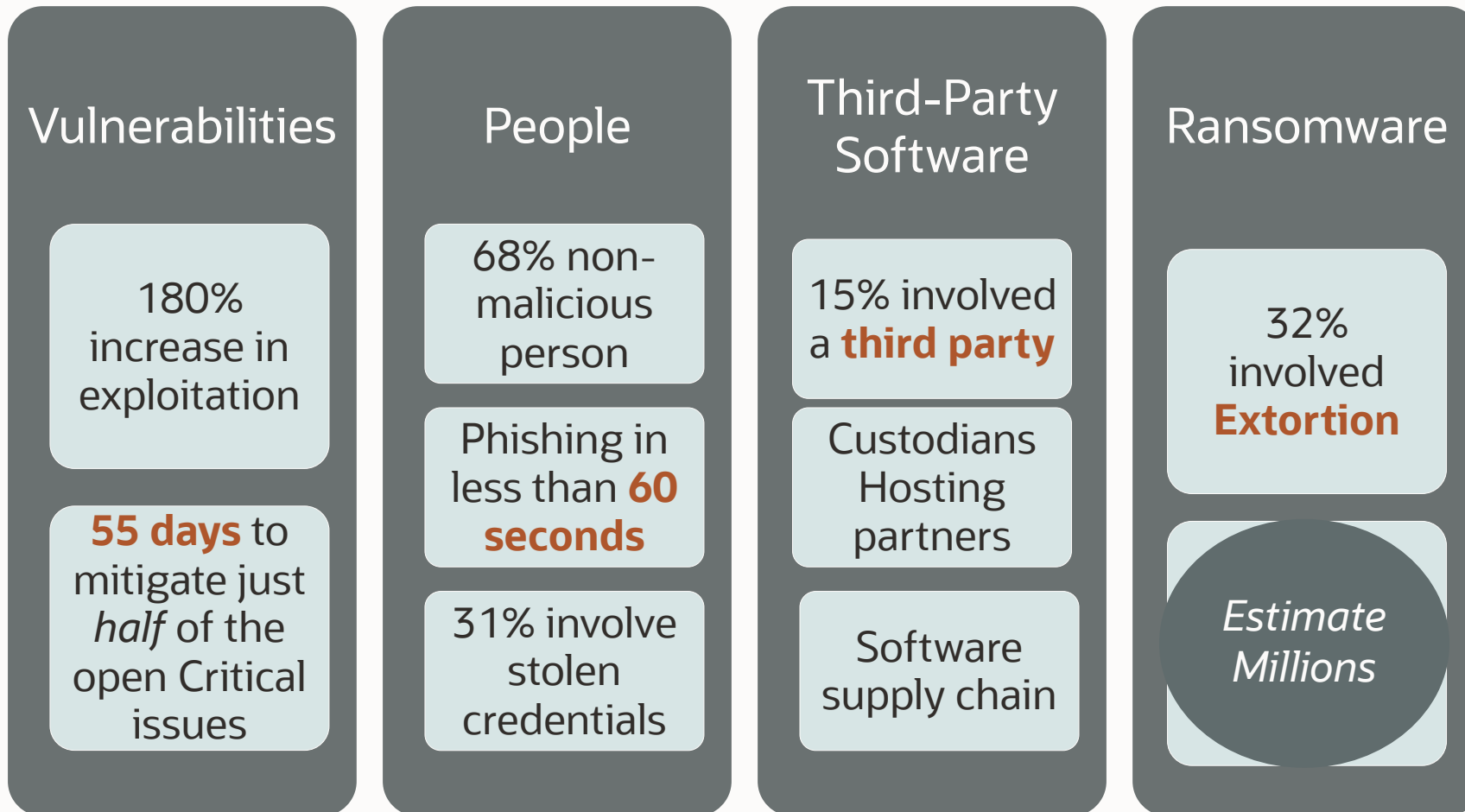
## Highly Available Architecture

Oracle MAA Best Practices Built-In

## End-to-End Security

Security-optimized, Security-focused, Security-hardened

# Verizon 2024 Data Breach Investigations Report



# Oracle Corporate Security Policies

Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.

Aligned with the following standards

- ISO/IEC 27002:2013
- ISO/IEC 27001:2013
- NIST

References

- <https://www.oracle.com/corporate/security-practices/>

# Exadata Security Value-Add Overview

- ✓ Smaller Kernel/Package Footprint
- ✓ Principle of Least Privilege
- ✓ Storage Server Firewall
- ✓ System Calls Restrictions
- ✓ Centralized User Authentication
- ✓ File Integrity Monitoring
- ✓ System Hardening
- ✓ Multi-Tenant Isolation
- ✓ Boot Device Protection
- ✓ Fast Crypto Erase
- ✓ Security Enabled Linux
- ✓ Memory Protection Keys
- ✓ Storage Server SSH Lockdown



“The Oracle Autonomous Database, which completely automates provisioning, management, tuning, and upgrade processes of database instances without any downtime, not just **substantially increases security and compliance of sensitive data stored in Oracle Databases** but makes a compelling argument for moving this data to the Oracle Cloud.”

**KuppingerCole Analysts**

# Smaller Installation Footprint

Exadata uses a minimal Linux kernel with removed dependencies that reduce size.

- Fewer device drivers
- Smaller footprint
- Improved upgrade time

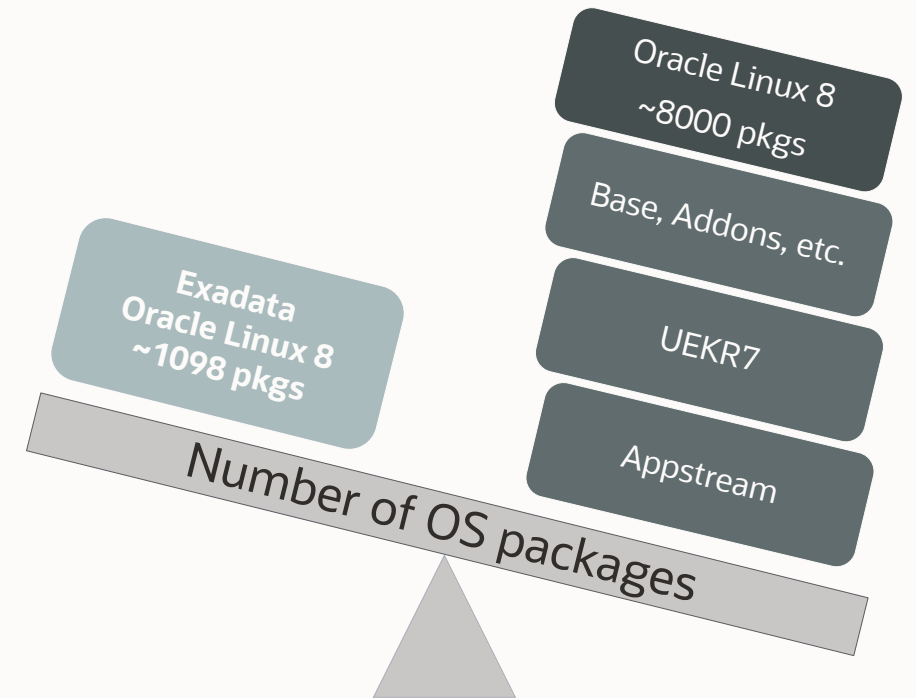
Full Enterprise Oracle Linux 8 UEK7 kernel

- kernel-uek-5.15.<>.el8uek
- Guest kernel size **161MB**

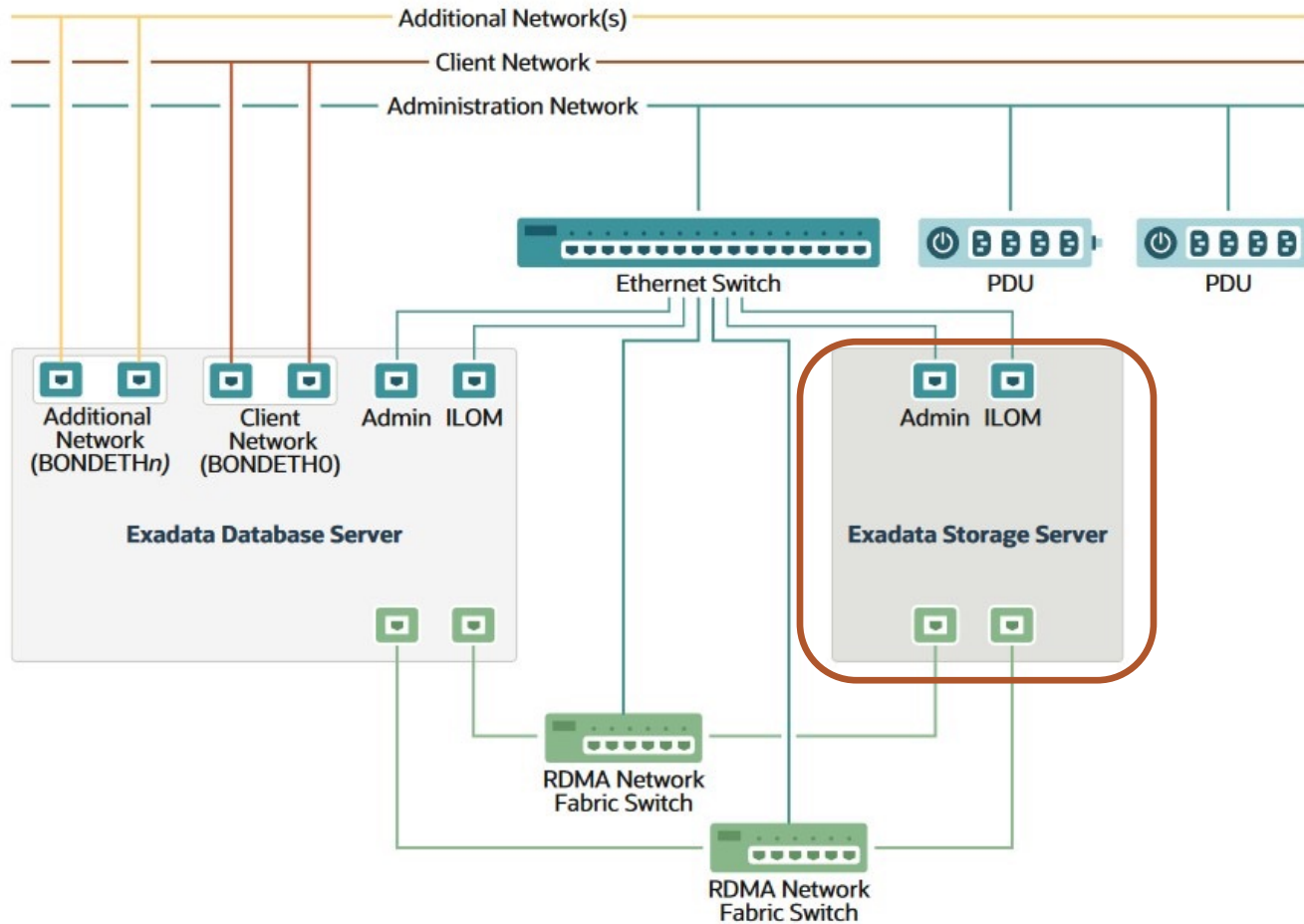
Exadata Oracle Linux 8 UEK7 kernel

- kernel-**uek-core**-5.15.<>.el8uek
- Guest kernel size **77MB**

Exadata **reduces the attack surface** by only including the software components required specifically to run the Oracle database.



# Network Access to Storage Servers



- Oracle Exadata System Software includes the cellwall service that implements a **firewall** on each storage server.
- The SSH server is configured to respond to connection requests only on the management network (NET0) and the RDMA Network Fabric.
- The Exadata Storage Servers have no direct connectivity to the client network.



# Pre-scanned full stack

Every Exadata release includes **security and emergency fixes** to address zero-day vulnerabilities discovered by our internal scanning tools.

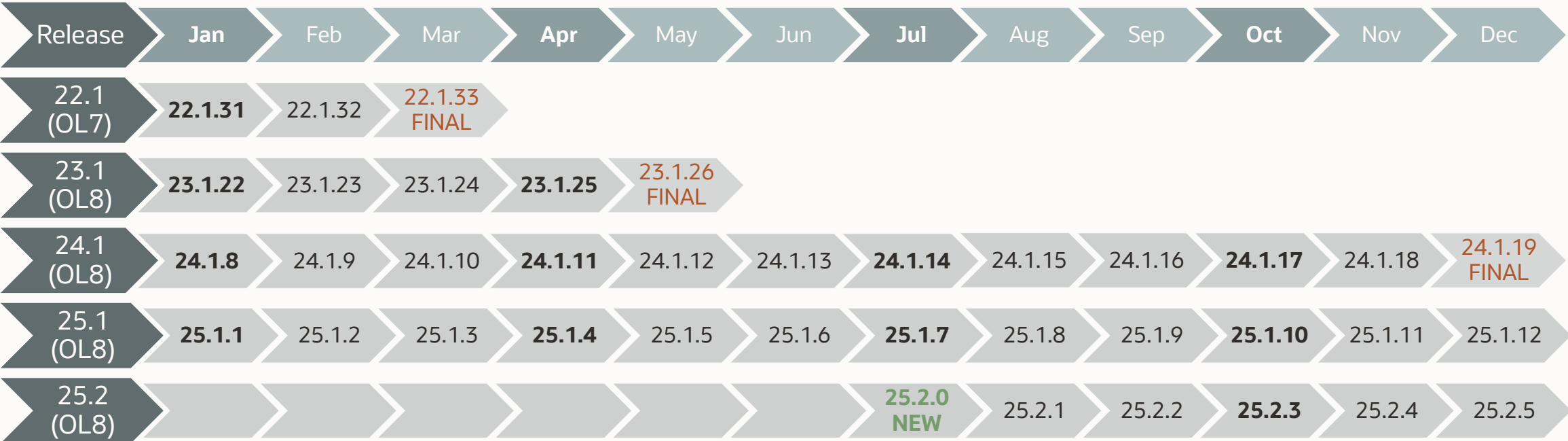
- Static/Dynamic code analyzing
- Malware scans
- Third-party software checks
- Vulnerability scans
  - Responses to common Exadata security scan findings (Doc ID 1405320.1)
- System hardening reviews (STIG)
  - Exadata OL8 System Hardening for STIG Security Compliance (Doc ID 2934166.1)

Customers take advantage of these fixes out of the box by just upgrading to the latest release.

- The number of annual issues reported is significantly less compared to a custom configuration with third party database, network and storage components.

# Exadata Releases CY2025

Monthly Exadata System Software maintenance releases include the latest security updates to protect your data.



*Future releases and dates are estimates only.*



# 40,002

Common Vulnerabilities and Exposures (CVE) IDs issued in 2024 *across the international IT marketplace.*

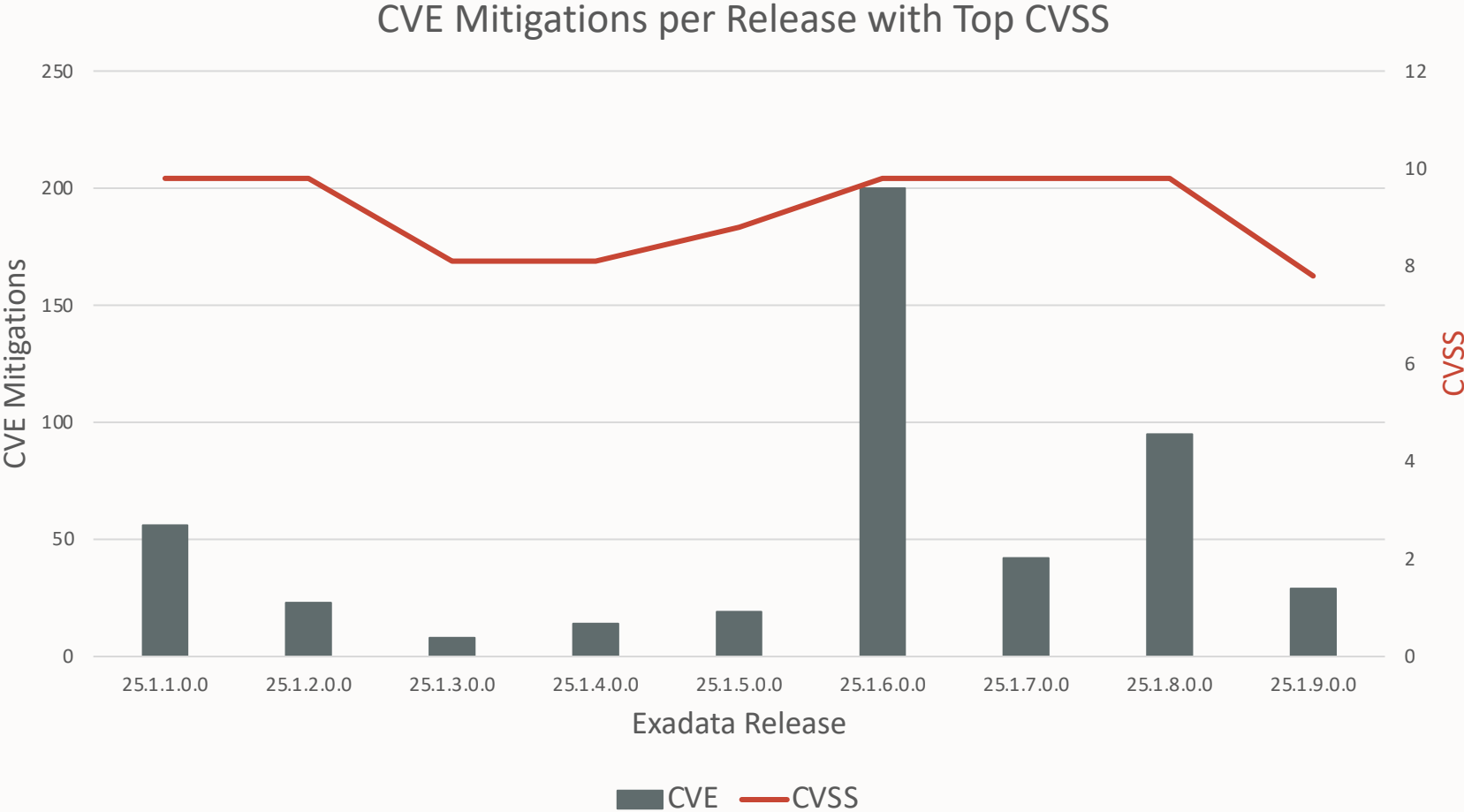
**That's ~110 per day!**

Exadata Security Value Add:

- Scanned images
- Monthly releases



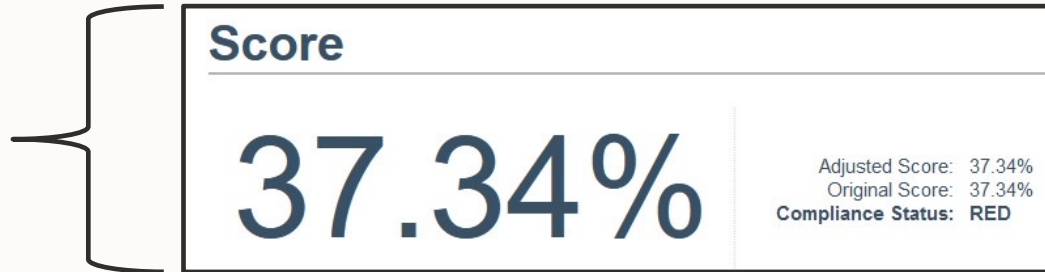
# Monthly Oracle Linux CVE Mitigations for Exadata 25.1.x



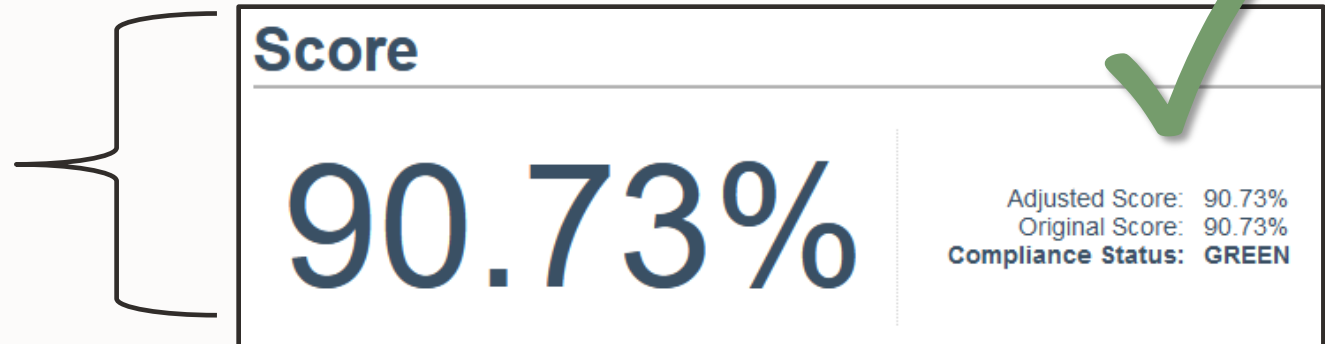
# High STIG SCAP Oracle Linux 8 Benchmark from the Factory!

“The Oracle Linux 8 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of the Department of Defense (DoD) information systems.”

Standard Linux installation



Exadata KVM Guest Deployed



# New Security Features in Exadata

---

**Maximize Security**, Maximize Performance, Maximum Availability

# Security Enabled Linux (SELinux) – Permission Mode Enabled by Default

The SELinux enhancement to the Linux kernel implements the **Mandatory Access Control (MAC) policy**, which allows defining a security policy that provides granular permissions for all users, programs, processes, files, and devices.

- Starting with Oracle Exadata System Software release 25.2.0, all new Exadata implementations use SELinux in permissive mode by default, significantly strengthening the default Exadata security posture.
- The default configuration includes a pre-built SELinux policy that is custom-engineered for Exadata and Oracle Database, enabling seamless adoption. Additional custom policies are also allowed to support 3rd-party or implementation-specific software requirements.
- Monitoring SELinux in permissive mode enables the identification of potential issues, providing the opportunity to take corrective action to ensure the security and integrity of Exadata environments. Starting with permissive mode enables easy adoption and is the ideal preparation before manually moving to a mode that strictly enforces the SELinux security policies.

# Exadata Security Capabilities

---

**Maximize Security**, Maximize Performance, Maximum Availability

# Oracle Linux 8 – Unbreakable Enterprise Kernel 7 (UEK7)

## Oracle Linux 8 Key security features

- Various SELinux improvements
- System-wide cryptographic policies applied by default
- OpenSSH updates
  - RSA min key 1024
  - DH module size 2048
  - DSA keys disabled
- TLS 1.3 cryptographic libraries added
- GPG key length increased to 4096 bits

Platform	Component	O/S	Kernel
RoCE	KVM Host	OL8	<b>UEK7</b>
	KVM Guest	OL8	<b>UEK7</b>
	Bare Metal	OL8	<b>UEK7</b>
	Storage Server	OL8	<b>UEK7</b>
Infiniband	Xen Dom0	OL7	UEK6
	Xen DomU	OL8	UEK6
	Bare Metal	OL8	UEK6
	Storage Server	OL8	UEK6

RDMA over Converged Ethernet (RoCE) server components move to UEK7



# Simpler Linux Package Dependency Management

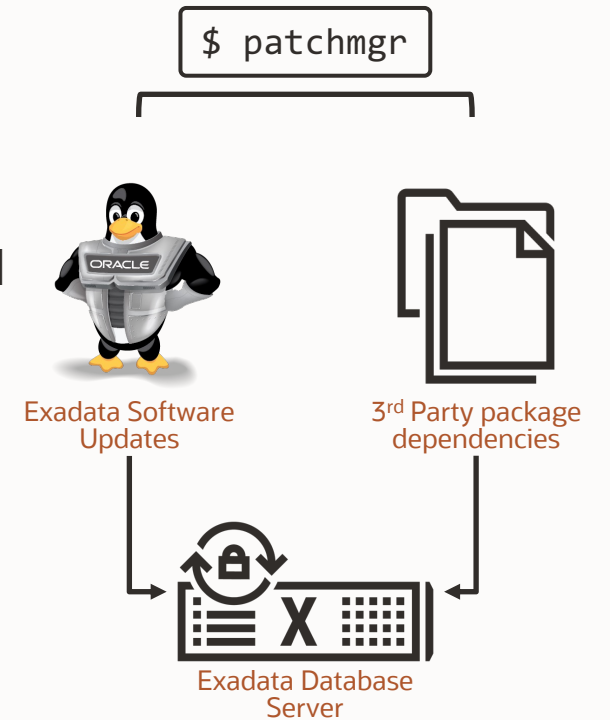
Customers often install 3<sup>rd</sup> party software on Exadata such as security, monitoring, and backup utilities.

These utilities often have additional Linux RPM dependencies over the curated Exadata repository.

Patch Manager enables additional non-Exadata software packages to be installed or updated as part of an Exadata database server update.

## Avoids removal and reinstallation of 3<sup>rd</sup> party software during database server updates

- Validate package dependencies with `patchmgr --precheck`
- Update the Exadata database server software and additional packages simultaneously



```
$ patchmgr --precheck | --upgrade [ { --additional-rpms } | --additional-rpms-list ] [ --additional-rpms-from-repo ]
```

# Simpler Linux Package Dependency Management

Two phases of operation:

1. Precheck – iteratively test required packages are present in additional\_rpms location and dependencies are resolved
2. Upgrade – applies database server update along with update and install of additional rpms

```
$ patchmgr --dbnodes db_group --precheck --iso_repo /u01/exadata_ol8_25.1.0.0.0.241130_linux-x86-64.zip  
--target_version 25.1.0.0.0.241130 --log_dir auto --additional_rpms /u01/additional_rpms/repo/
```

```
$ patchmgr --dbnodes db_group --upgrade --iso_repo /u01/exadata_ol8_25.1.0.0.0.241130_linux-x86-64.zip  
--target_version 25.1.0.0.0.241130 --log_dir auto --additional_rpms /u01/additional_rpms/repo/
```

/u01/additional\_rpms/repo/ (example contents)

- elfutils-debuginfod-client-0.190-2.el8.x86\_64.rpm
- elfutils-libelf-devel-0.190-2.el8.x86\_64.rpm
- keyutils-libs-devel-1.5.10-9.0.1-el8.x86\_64.rpm
- krb5-devel-1.82.2-28.0.1-el8.x86\_64.rpm

# Software Upgrade on Cisco Network Switches

Oracle Exadata System Software includes **NX-OS 10.3.(x)** Cisco system software release for the Cisco Management Network Switch and the Cisco RoCE Network Fabric Switches.

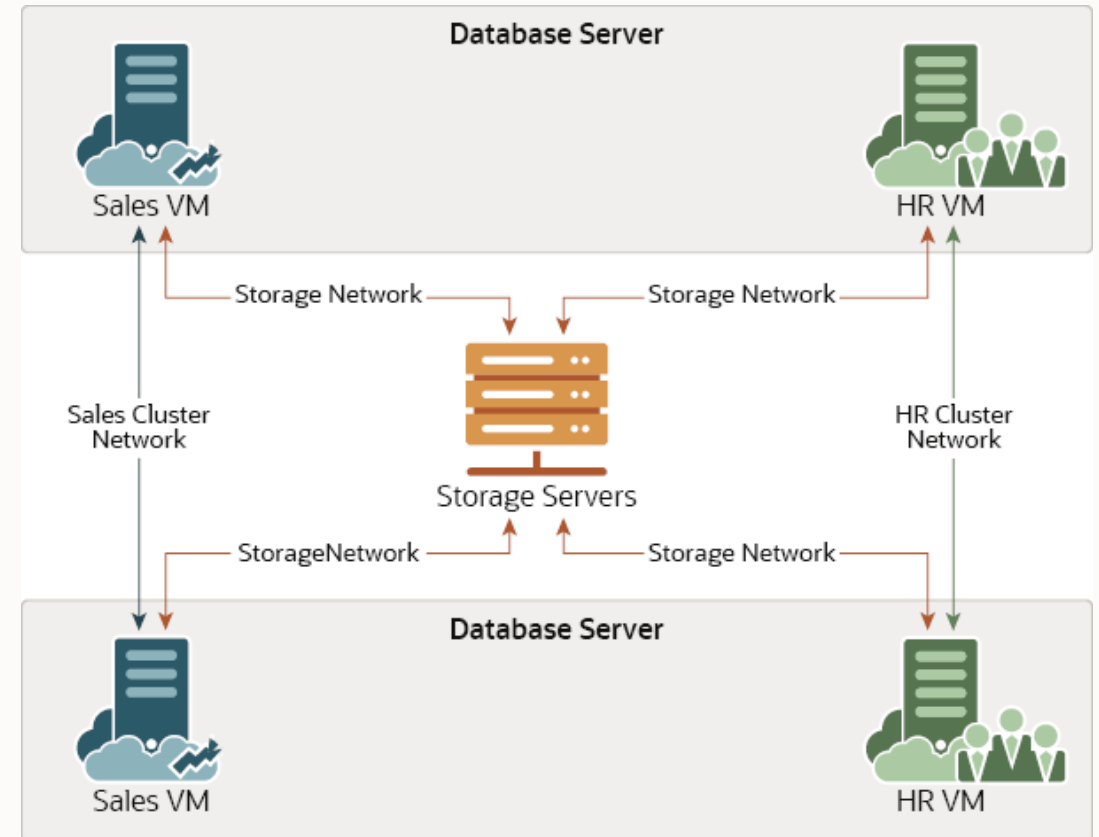
In addition to the general performance and security enhancements contained in NX-OS 10.3.(x), the update procedure for NX-OS has been optimized, resulting in substantially quicker updates.

- Depending on the switch being updated and its configuration, the overall time required to perform the update is reduced by up to 44%.

# Secure Fabric is Recommended and Enabled by Default

Exadata Secure Fabric for RoCE systems implements **network isolation** for Virtual Machines while allowing access to common Exadata Storage Servers.

- Each Exadata VM Cluster is assigned a private network.
- VMs cannot communicate with each other.
- All VMs can communicate to the shared storage infrastructure.
- Security cannot be bypassed.
  - Enforcement done by the network card on every packet.
  - Rules programmed by hypervisor automatically.



# Exadata Live Update

Exadata Live Update is a suite of enhancements to the mechanisms that orchestrate Exadata **software updates** on Exadata database servers.

Exadata Live Update uses online update capabilities based on standard Linux technologies, such as RPM and ksplice.

- Depending on the specific contents of the update, the update operation might occur without interrupting databases or rebooting the server.

Any update items that cannot be completed online are staged for completion during a later server reboot.

- You can schedule the outstanding items to be completed at a specific time or during the next graceful server reboot.
- You can also choose to defer the outstanding items indefinitely.

Exadata Live Update can be controlled using the Exadata patchmgr utility, which provides an easy and familiar experience for existing Exadata users.

# Exadata Live Update

Exadata Live Update enables partial updates to address security issues, based on Common Vulnerability Scoring System (CVSS). When using Exadata Live Update, you must choose from the following options:

- **highcvss:** Performs only critical security updates to address vulnerabilities with a CVSS score of 7 or greater.
  - All new packages with High or Critical security mitigations
- **allcvss:** Performs only security updates to address vulnerabilities with a CVSS score of 1 or greater.
  - All new packages with any security mitigations (Low, Medium, High, Critical)
- **full:** Performs a full update, which includes all security-related updates and all other non-security updates.
  - All new packages in the image

# Exadata Live Update

Patchmgr command

```
# ./patchmgr --dbnodes dbs_group --upgrade --repo <path>exadata_ol8_ 24.1.0.0.0.240517.1  
_Linux-x86-64.zip --target_version 24.1.0.0.0.240517.1 --log_dir auto --live-update-target  
allcvss
```

Imagehistory output from Exadata 23.1.x with Exadata Live Update to 24.1.0.0.0

```
Version : 23.1.1.0.0.230422  
Exadata Live Update Version : 24.1.0.0.0. 240517.1 (all) (CVSS 1-10) (Live Update  
applied. Reboot at any time to finalize outstanding items.)
```

# Database and Storage Server Secure Boot

Oracle Exadata System Software extends Secure Boot to Storage Servers, KVM Host, KVM Guest\*, and Bare Metal.

Secure Boot is a method used to **restrict** which **binaries** can be executed to boot the system.

- With Secure Boot, the system UEFI firmware will only allow the execution of boot loaders that carry the cryptographic signature of trusted entities.
- With each reboot of the server, every executed component is verified.
- This prevents malware from hiding embedded code in the boot chain.
  - Intended to prevent boot-sector malware or kernel code injection
  - Hardware-based code signing
  - Extension of the UEFI firmware architecture
  - Can be enabled or disabled through the UEFI firmware

*\*KVM Guest Secure Boot can be enabled during VM Cluster deployment in OEDA*

# Access Control For RESTful Service

Oracle Exadata System Software includes the capability to **restrict access** to the HTTPs and RESTful interfaces using access controls.

- Specify a list of IP addresses or subnet masks to control access to the RESTful service via HTTPs.
- If not used, RESTful service can be disabled altogether.

```
# lsof -i -P -n | grep LISTEN | grep java
java      <pid> dbmsvc  55u  IPv4  40193      0t0  TCP *:7879 (LISTEN)

# dbmcli -e alter dbserver httpsAccess=none
This command requires restarting MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating HTTPs access control list.
Starting MS services...
The STARTUP of MS services was successful.
DBServer successfully altered

# lsof -i -P -n | grep LISTEN | grep java
```

# Listening Interface For RESTful Service

Oracle Exadata System Software includes the capability to **restrict the network interfaces** that listen for commands using the Exadata RESTful service.

- The following values are allowed for *listeningInterface*: ALL, NONE, or list of network interfaces.
- The listening interface attribute complements the *httpsAccess* attribute.

```
# lsof -i -P -n | grep LISTEN | grep java
java          63902  dbmsvc   34u  IPv6      157781      0t0  TCP *:7879 (LISTEN)

# dbmcli -e alter dbserver listeningInterface=vmeth0
This command will automatically restart and redeploy MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating attribute "listeningInterface" before redeploying MS.
Starting MS services...
The STARTUP of MS services was successful.
DBServer scaqal04adm05 successfully altered

# lsof -i -P -n | grep LISTEN | grep java
java          237672  dbmsvc   34u  IPv6 308318206      0t0  TCP <ipaddress>:7879 (LISTEN)
```

# SNMP Security Enhancements

SNMP V3 provides strong **authentication and encryption** and is highly recommended.

- SNMP V3 subscribers (type=v3 or type=v3ASR) uses SHA2 authentication protocols.
  - SHA-224, SHA-256, SHA-384, and SHA-512.
- SNMP V1 (type=v1 or type=ASR) remain available but are discouraged.
  - The administrator must specify the SNMP community (public and private are discouraged).

```
# cellcli -e alter cell snmpuser='((name=user01,authprotocol=SHA-512,authpassword=*))'  
snmpUser user01 authpassword: *****  
Confirm snmpUser user01 authpassword: *****  
Cell <host> successfully altered  
# cellcli -e alter cell snmpSubscriber='((host=localhost,port=162,type=V3,snmpUser=user01))'  
snmpSubscriber ((<host>,port=162,community=public,type=asr,asrmPort=16161)) has been replaced with  
((host=localhost,port=162,snmpUser=user01,type=V3)).  
Cell <host> successfully altered
```

# Database 23ai Security Enhancements

The following features in Database 23ai are transparently available in Oracle Exadata System Software:

- **Smart Scan on AES-XTS Encrypted Data**
  - In conjunction with Oracle Database 23ai, Oracle Exadata System Software release 24.1.0 transparently enables Exadata Smart Scan on data in tablespaces encrypted using AES-XTS.
  - AES-XTS provides improved security and better performance, especially on Exadata where TDE can take advantage of parallel processing and specialized instructions built into processor hardware.
- **Smart Scan during Online Encryption**
  - Exadata Smart Scan remains fully enabled during long-running online encryption, decryption, and rekeying operations.
  - Previously, Exadata Smart Scan was disabled during such operations.

# Centralized Identification and Authentication of OS Users

Oracle Exadata System Software offers support for infrastructure **centralized identification and authentication** of operating system (OS) users.

- LDAP identity management systems
- Kerberos authentication
- Linux System Security Services Daemon (SSSD)
  - Pre-configured with Exadata-specific custom security profile
  - Customizations preserved across upgrades

Centralizes accounts for enhanced security

- Easier administration provisioning/deprovisioning
- Easier password management
- Enterprise security controls

References:

- How to configure Kerberos and SSSD-KCM in Exadata compute nodes and cells (Doc ID 2948255.1)
- LDAP configuration example in Exadata compute nodes and storage servers using SSSD (Doc ID 3020122.1)

# Implement Principle of Least Privilege

Security best practices require that each process run with the **lowest privileges** needed to perform the task. The following processes now run as non-privileged users:

- **Smart Scan processes:** Performing a smart scan predicate evaluation does not require root privileges.
  - User cellofl and group celltrace
- **Select ExaWatcher processes:** Some of the ExaWatcher commands that collect iostat, netstat, ps, top, and other information have been modified to run without requiring root user privilege.
  - User exawatch and group exawatch

# Operating System Activity Monitoring

Each Exadata server is configured with auditd to **audit system-level activity**.

- Manage audits and generate reports use the auditctl command.
- When the auditd service starts, it runs the augenrules utility. This utility merges all component audit rules files found in the audit rules directory and places the merged results in the /etc/audit/audit.rules file.
  - Exadata specific audit rules are stored in /etc/audit/rules.d/01-exadata\_audit.rules.
  - Customer custom audit rules may be stored in /etc/audit/rules.d/20-customer\_audit.rules.

```
# auditctl -l
-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremove
xattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
...
```

# Encrypting System Log Information (rsyslog)

Management Server (MS) on database and storage servers supports the syslogconf attribute.

- The syslogconf attribute extends syslog rules for a database server.
- The attribute can be used to designate that syslog messages be **forwarded to a specific remote syslogd service.**
- On the MS, the forwarded messages are directed to a file, console, or management application, depending on the syslog configuration on the MS.
- This enables system logs from different servers to be aggregated and mined in a centralized logging server for security auditing, data mining, and so on.

Use certificates and the syslogconf attribute to configure encryption of the syslog information.

# Oracle Exadata Deployment Assistant (OEDA)

Use the deployment assistant for initial configuration, and when modifying or adding to an existing deployment. You can import an existing configuration when adding new components or modifying an existing deployment.

- When you first log in to a host following the **Resecure Machine** deployment step, you are prompted to reset the root password. This still occurs even when SSH key-based authentication is enabled, and password-based authentication is disabled.

Password  
Complexity

Password  
Aging

Password  
Expiration

Permissions



# host\_access\_control – system settings

Implement the available features and security plan post deployment via host\_access\_control.

```
# /opt/oracle.cellos/host_access_control apply-defaults --strict_compliance_only
INACTIVE=0
Deny on login failure count set to 3
Account fail_interval for failed login attempts set to 900
Account unlock_time after {deny} failed login attempts set to 900
Password history set to pam_pwhistory.so 5
Password strength set to pam_pwquality.so minlen=15 minclass=4 dcredit=-1 ucredit=-1 lcredit=-1
ocredit=-1 difok=8 maxrepeat=3 maxclassrepeat=4 local_users_only retry=3 authtok_type=
PermitRootLogin no
hard maxlogins 10
hmac-sha2-256,hmac-sha2-512 for both server and client
Password aging -M 60, -m 1, -W 7
```

# host\_access\_control – system settings

## Subset of commands

- access - User access from hosts, networks, etc.
- auditd-options - Options for auditd
- banner - Login banner management
- fips-mode - FIPS mode for openSSH
- idle-timeout - Shell and SSH client idle timeout control
- pam-auth - PAM authentication settings
- password-aging - Adjust current users' password aging
- rootssh - Root user SSH access control
- ssh-access - Allow or deny user and group SSH access
- sshciphers - SSH cipher support control
- ssh-macs - SSH supported MACs
- sudo - User privilege control through sudo

# FIPS 140-2 for Oracle Linux Kernel/SSH on Exadata Database Nodes

## `/opt/oracle.cellos/host_access_control fips-mode –enable`

- Kernel settings - *Requires a reboot*
  - STIG mitigation: The Oracle Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
  - STIG mitigation: The Oracle Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

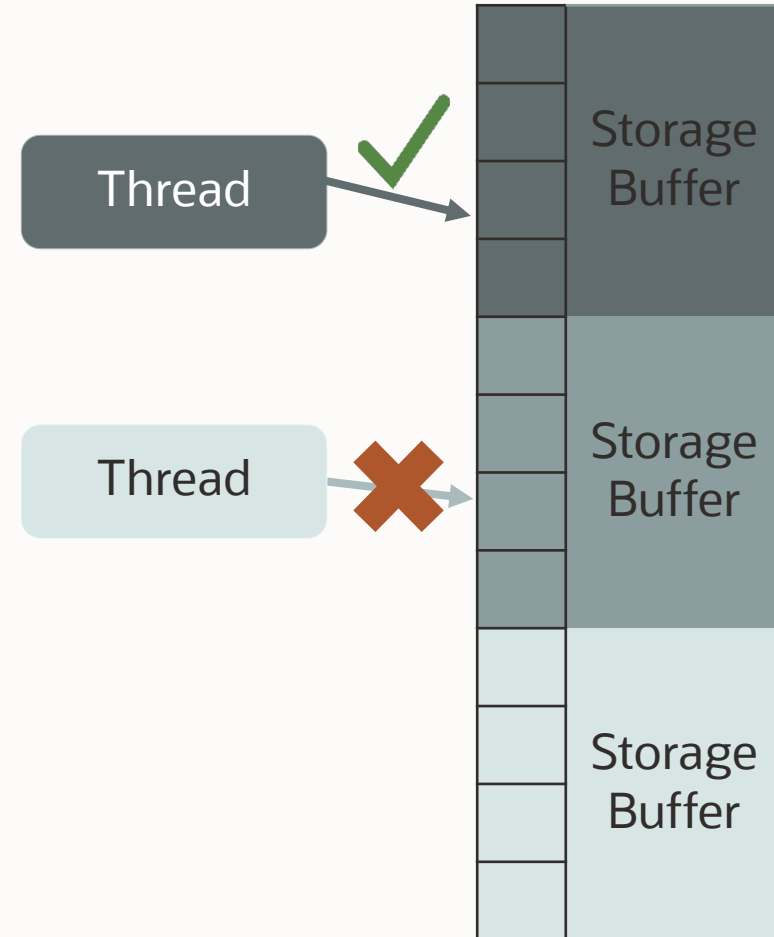
## `/opt/oracle.cellos/host_access_control ssh-macs –secdefaults`

- SSH controls
  - STIG mitigation: The Oracle Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

# Securing Storage Server Processes with Memory Protection Keys

Storage Server Software Memory is partitioned with 16 colors.

- Four bits in each page table entry used to identify the color.
- Each thread is allowed to read/write and enable/disable to its matching color.
- Any access to a piece of memory that does not have the correct color traps the process.
- Protects against inadvertent software defects.
- Enabled out of the box with no tuning needed.
- **Eliminates a class of potential memory corruptions.**



# Other Security Capabilities for Storage Servers

**Secure Computing (seccomp)** feature in Oracle Linux Kernel used to **restrict system calls** that can be made.

- Kernel has hundreds of system calls, most not needed by any given process.
- A seccomp filter defines whether a system call is allowed.
- Seccomp filters installed for cell server and offload processes automatically during upgrade.
- Allow-list set of system calls are allowed to be made from these processes.
- Seccomp performance additional validation of the arguments.

## Disabling SSH

- Storage servers can be **“locked”** from SSH access.
- ExaCLI can still be used to perform operations.
  - Communicates using HTTPS and REST APIs to a web service running on the server.
  - Temporary access can be enabled for operational access if required.

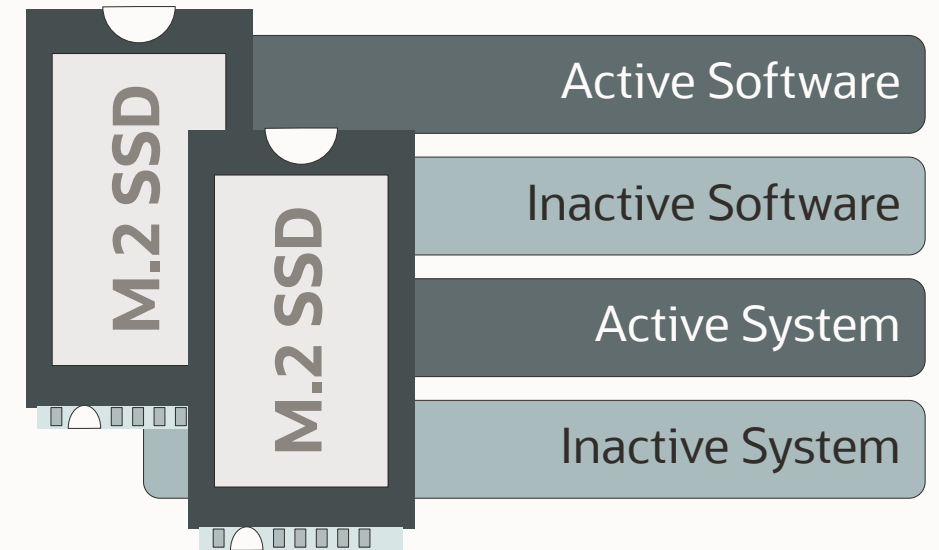
# Storage Server Partition Installation

Exadata installs the system/software on alternating partitions.

- When upgrading to a newer version, the software is installed on the inactive partition and then booted to that partition.

This ensures a complete OS refresh is completed at each upgrade which **minimizes the propagation of infected files**. OS data is separate from database data.

- Database is safe from OS corruption.



Oracle Exadata Rack and Oracle Exadata Storage Servers can remain online and available while replacing an M.2 disk.

# Advanced Intrusion Detection Environment (AIDE)

Help **guard against unauthorized access** to the files on your Exadata system.

- AIDE creates a database of files on the system and then uses that database to ensure file integrity and to detect system intrusions.

```
# /opt/oracle.SupportTools/exadataAIDE -status
```

```
AIDE: daily cron is currently enabled.
```

To add additional rules:

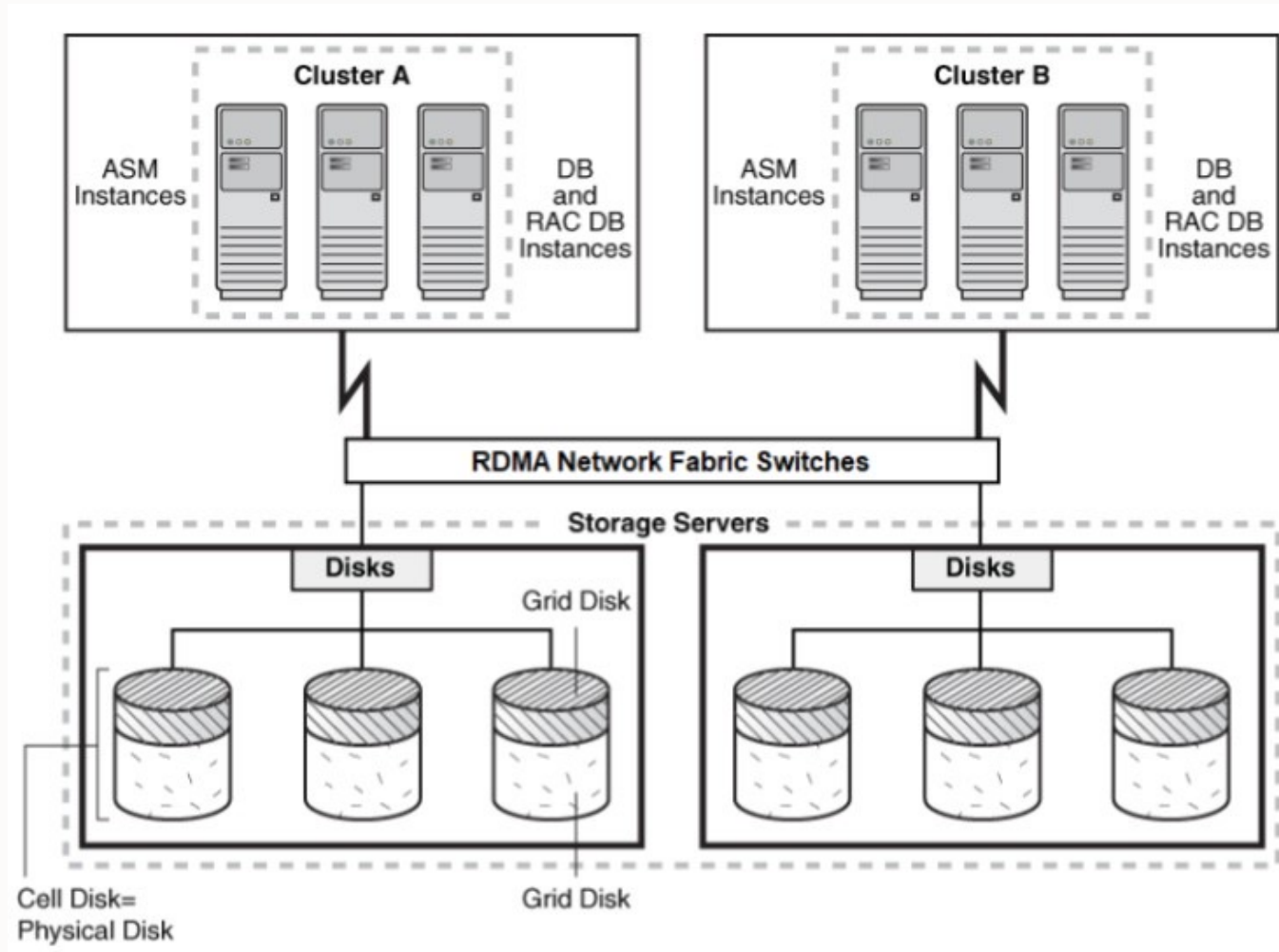
Edit the file /etc/aide.conf

Update the AIDE database metadata.

```
# /opt/oracle.SupportTools/exadataAIDE -u
```

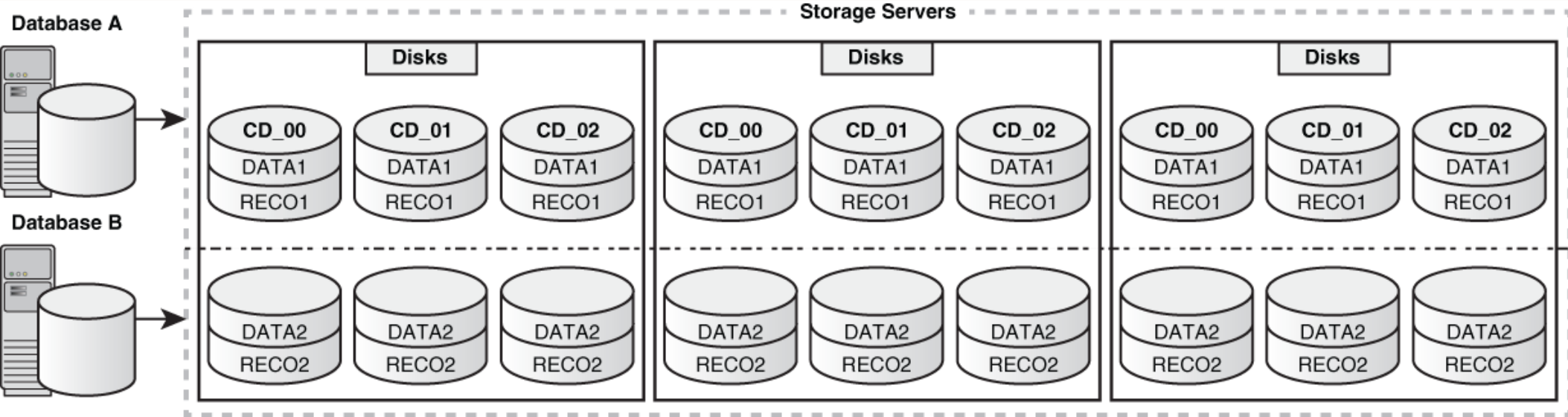
# ASM-Scoped Security

**Restrict access** to only the grid disks used by the Oracle ASM disk groups associated with an Oracle ASM cluster.



# DB-Scoped Security

**Restrict access** for an Oracle Database instance to a specific set of grid disks.



# Secure Erase

Provide a **secure erase solution** for every component within Oracle Exadata Database Machine

- Crypto-erase is used whenever possible and is fully compliant with the NIST SP-800-88r1 standard

Component	Make or Model	Erase Method
Hard drive	<ul style="list-style-type: none"><li>• 8 TB hard drives on Oracle Exadata Database Machine X5</li><li>• All hard drives on Oracle Exadata Database Machine X6 or later</li></ul>	Crypto erase
Hard drive	All other hard drives	1/3/7-Pass erase
Flash device	Flash devices on Oracle Exadata Database Machine X5 or later	Crypto erase
Flash device	All other flash devices	7-pass erase
M.2 device	Oracle Exadata Database Machine X7-2 or later	Crypto erase





“Oracle Exadata Cloud@Customer uses the superior technology of Oracle Database as a cloud service delivered in our own data centers, **meeting all of our data sovereignty and compliance requirements** for the Regional Revitalization Cloud.”

**Norihito Senda**

Nagoya Branch  
Advanced Solution Department  
Corporate Business Headquarters  
Nippon Telegraph and Telephone West Corporation (NTT WEST)

# Security Best Practices

The security of a system is only as good as its weakest link.

- Regular scans should be **run by YOU the owner of the system** to ensure against any deviations from the delivered configurations.
- Maintaining the latest Software Update ensures the latest security vulnerabilities are mitigated.
- Tools and processes are there to assist in creating a secure environment, but they must be used!

# References

---

**Maximize Security**, Maximize Performance, Maximum Availability

# Security References

## Oracle Exadata Database Machine Security FAQ

- My Oracle Support (MOS) note: **Doc ID 2751741.1**

## Oracle Exadata Documentation

- <https://docs.oracle.com/en/engineered-systems/exadata-database-machine/books.html>

## Oracle Corporate Security Practices

- <https://www.oracle.com/corporate/security-practices/>

## Critical Patch Updates, Security Alerts and Bulletins

- <https://www.oracle.com/technetwork/topics/security/alerts-086861.html>

## Oracle Corporate Security Blog

- <https://blogs.oracle.com/security/>

# Thank you

---

ORACLE