ORACLE

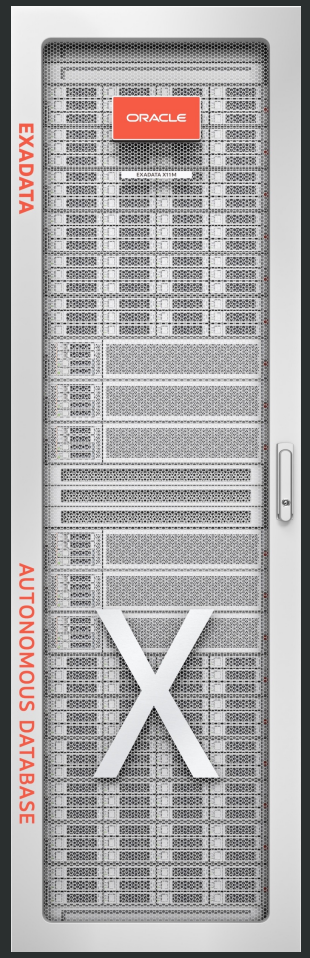
Oracle Exadata Database Machine

Maximum Security Architecture to Protect your Data

August 11, 2026

Exadata Maximum Security Architecture (MSA) Vision

Extreme Performance, Availability, and Security



Database Aware System Software
Unique algorithms vastly improve OLTP, Analytics, Consolidation

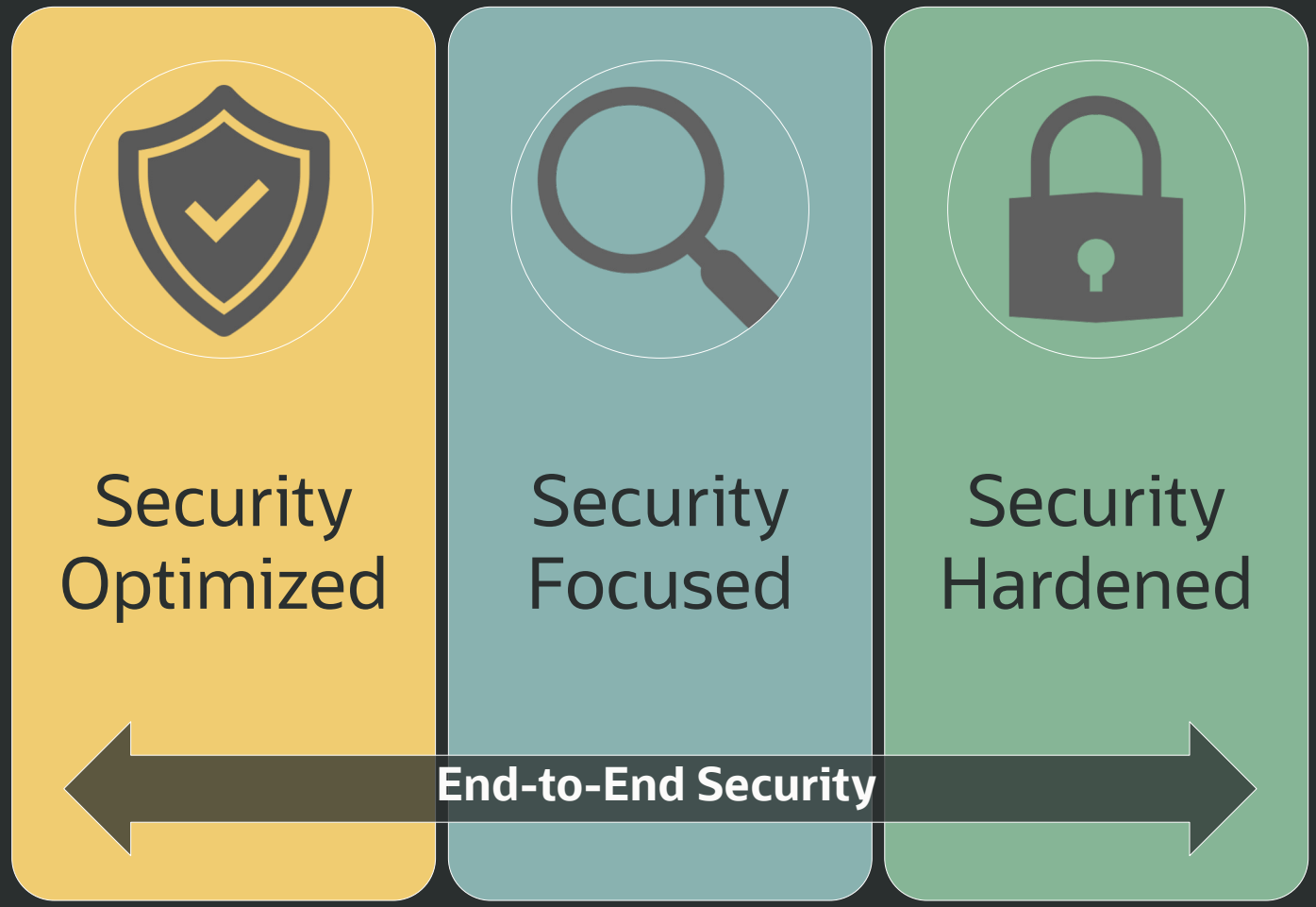
Highly Available Architecture
Oracle MAA Best Practices Built-In

End-to-End Security
Security-optimized, Security-focused, Security-hardened

Copyright © 2026, Oracle and/or its affiliates

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



Copyright © 2026, Oracle and/or its affiliates

Verizon 2026 Data Breach Investigations Report

Attackers are scaling through vulnerability exploitation, ransomware, mobile devices, and generative AI

VULNERABILITY EXPLOITATION

31% Now the most common initial access vector for breaches.

GENERATIVE AI

15 median days Generative AI helps attackers find gaps and build malware faster.

2026 DBIR

Attack surface pressure is rising.

RANSOMWARE

48% Breaches involving ransomware; 69% of victims did not pay.

MOBILE DEVICES

40% Attackers are shifting from email to mobile channels.

Weak passwords and permissions took nearly 8 months to resolve 50% of findings.

Copyright © 2026, Oracle and/or its affiliates

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/

Copyright © 2026, Oracle and/or its affiliates

Smaller Installation Footprint

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

- Fewer device drivers
- Smaller footprint
- Improved upgrade time

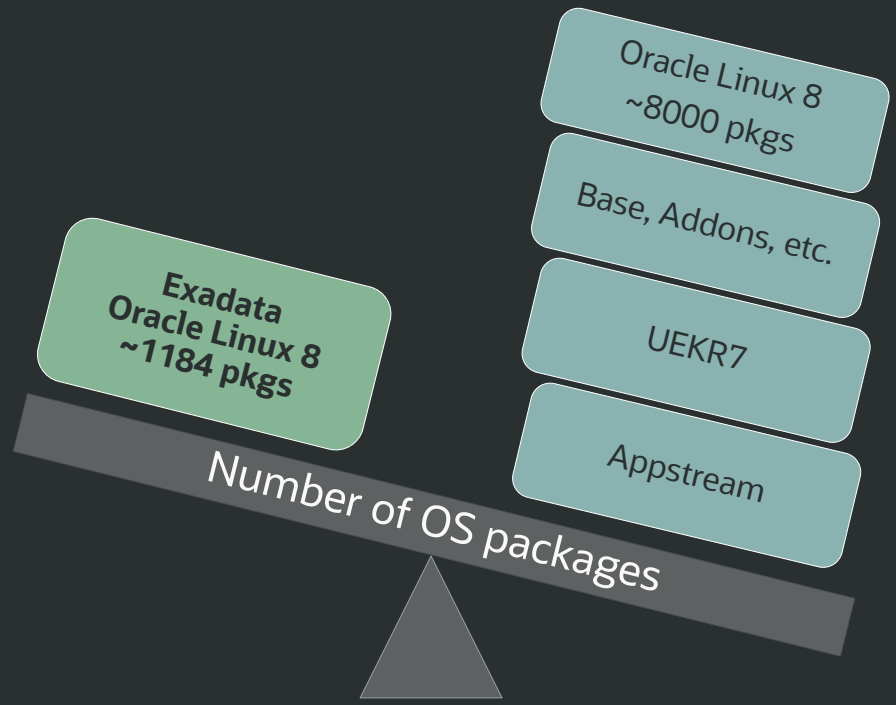
Full Enterprise Oracle Linux 8 UEK7 kernel

- kernel-uek-5.15.<>.el8uek
- Guest kernel size 170MB

Exadata Oracle Linux 8 UEK7 kernel

- kernel-uek-core-5.15.<>.el8uek
- Guest kernel size 103MB

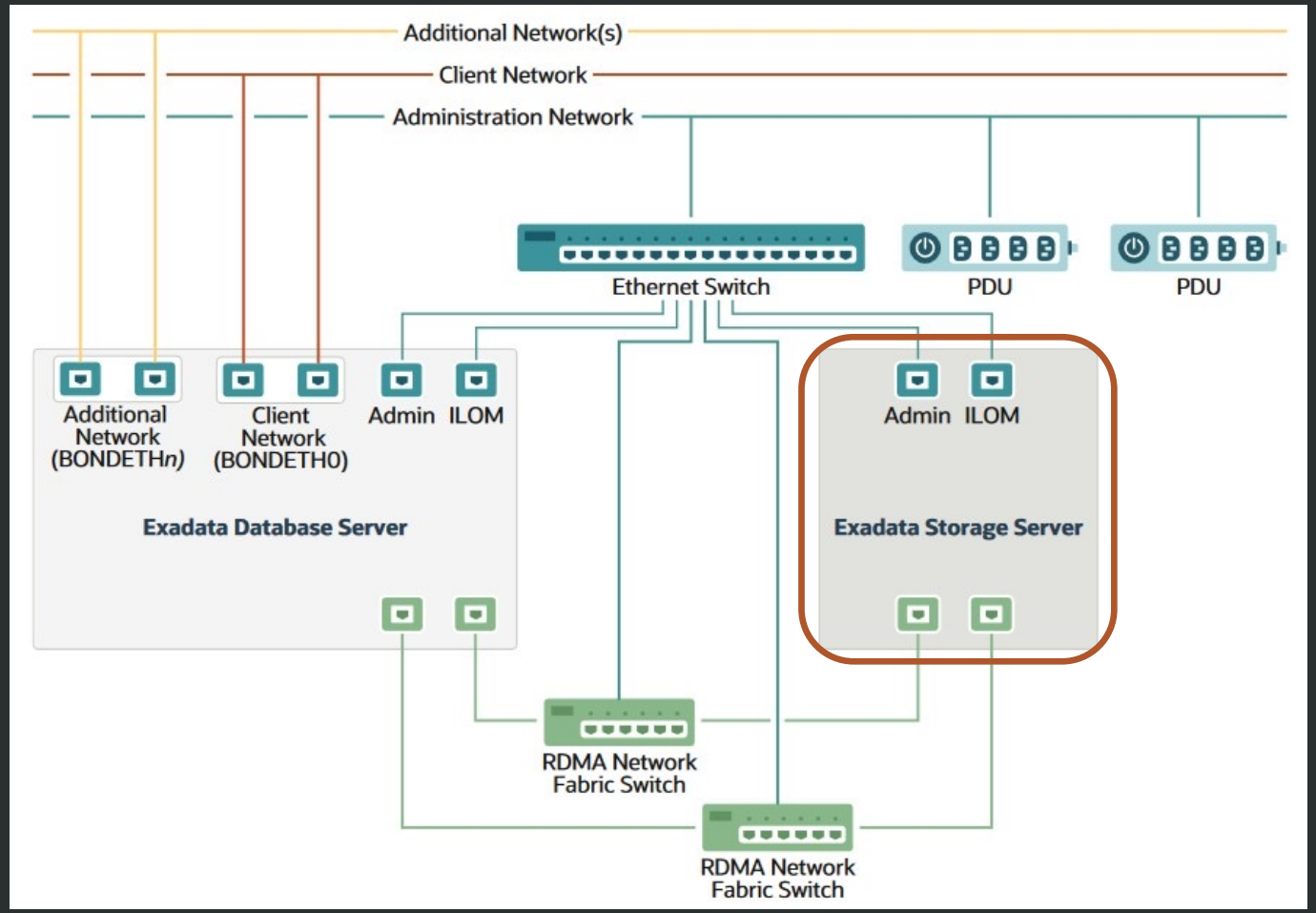
Exadata **reduces the attack surface** by only including the software components required specifically to run the Oracle database.



Copyright © 2026, Oracle and/or its affiliates

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.



Copyright © 2026, Oracle and/or its affiliates

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/AI code analyzing
- Malware scans
- Third-party software checks
- Vulnerability scans
- System hardening reviews (STIG)

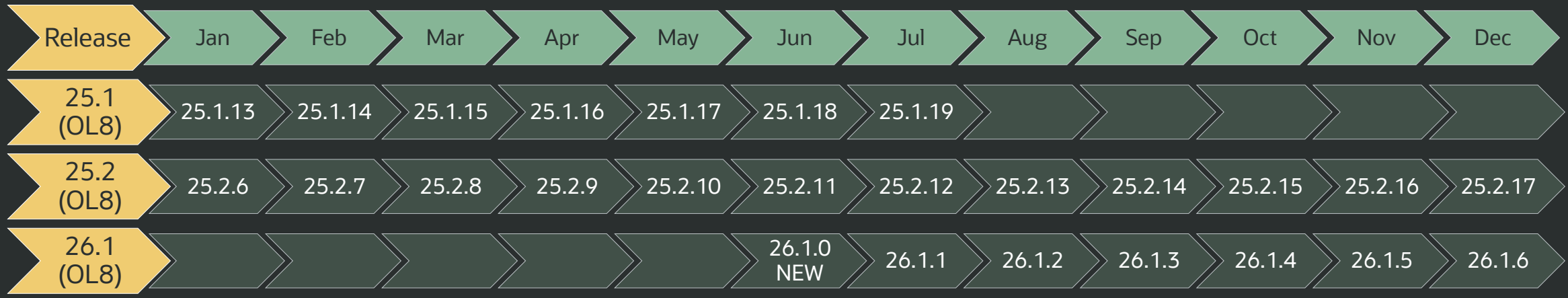
Customers take advantage of these fixes out of the box by just upgrading to the latest release.

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

Copyright © 2026, Oracle and/or its affiliates

Exadata Releases CY2026

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



*Future releases and dates are **estimates** only.*

Copyright © 2026, Oracle and/or its affiliates

Common Vulnerabilities and Exposures (CVE)

49,920



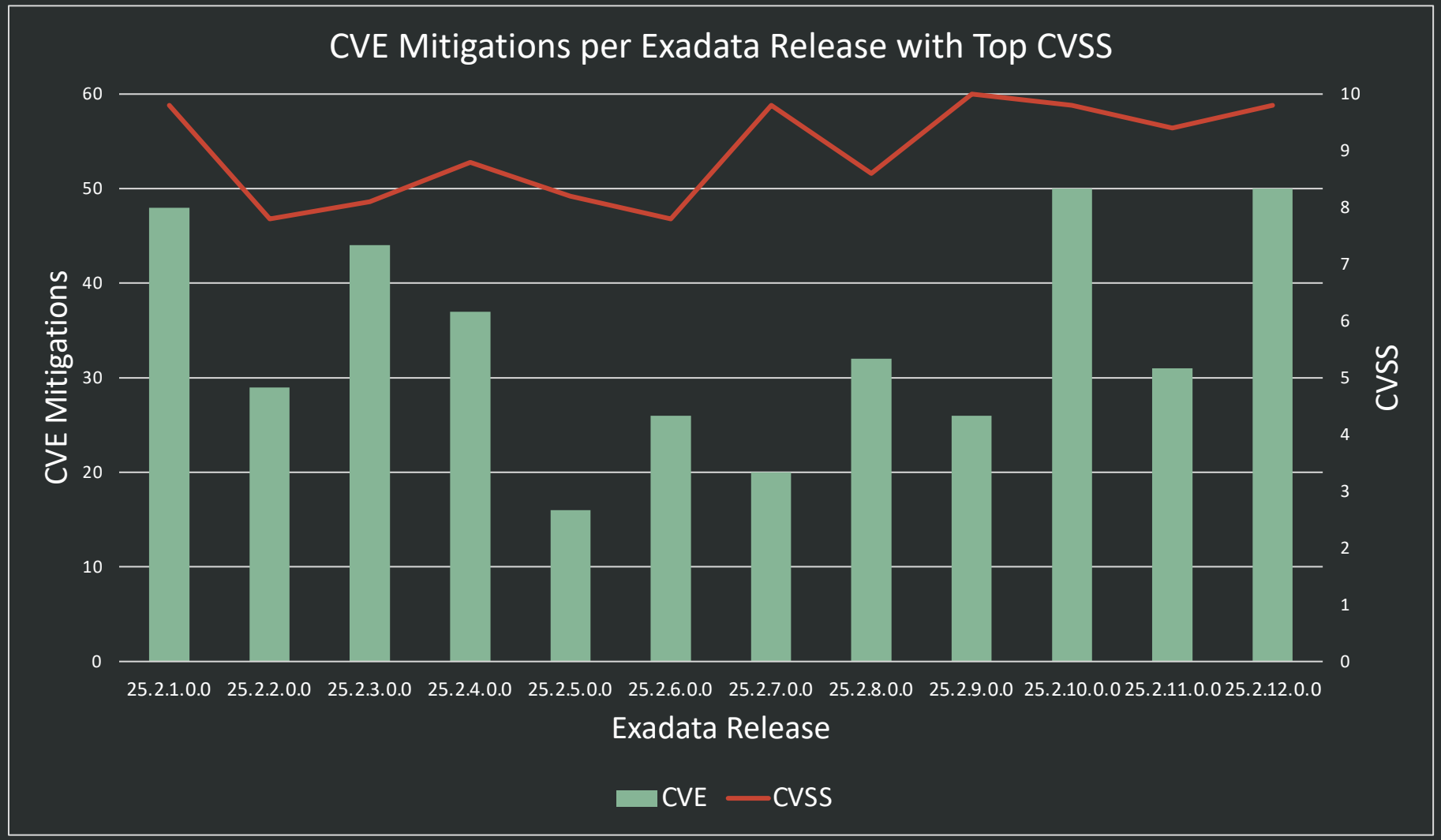
Common Vulnerabilities and Exposures CVE IDs issued in 2025 *across the international IT marketplace.*

Exadata Security Value Add:

- Scanned images
- Monthly releases

Copyright © 2026, Oracle and/or its affiliates

Monthly Oracle Linux CVE Mitigations for Exadata 25.2.x

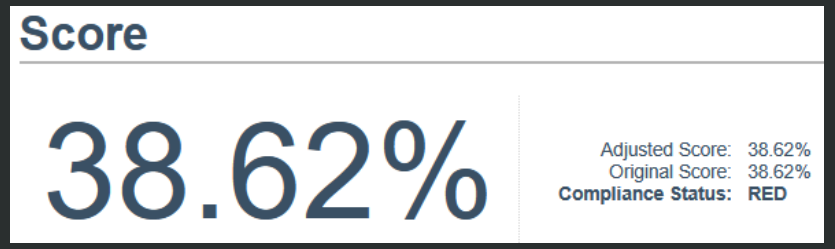


Copyright © 2026, Oracle and/or its affiliates

High STIG SCAP Oracle Linux 8 Benchmark Built-In!

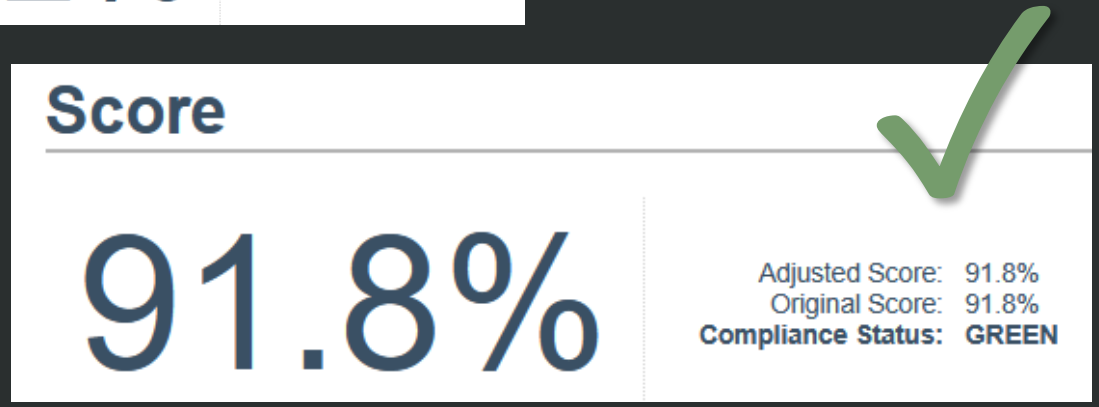
"The Oracle Linux 8 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of the Department of Defense (DoD) information systems."

Standard Linux installation



Exadata KVM Guest running 26.1.1.0.0

- Use host_access_control to finalize selected security features for your compliance goals
- Benchmark: OL8 V2R8 STIG SCAP



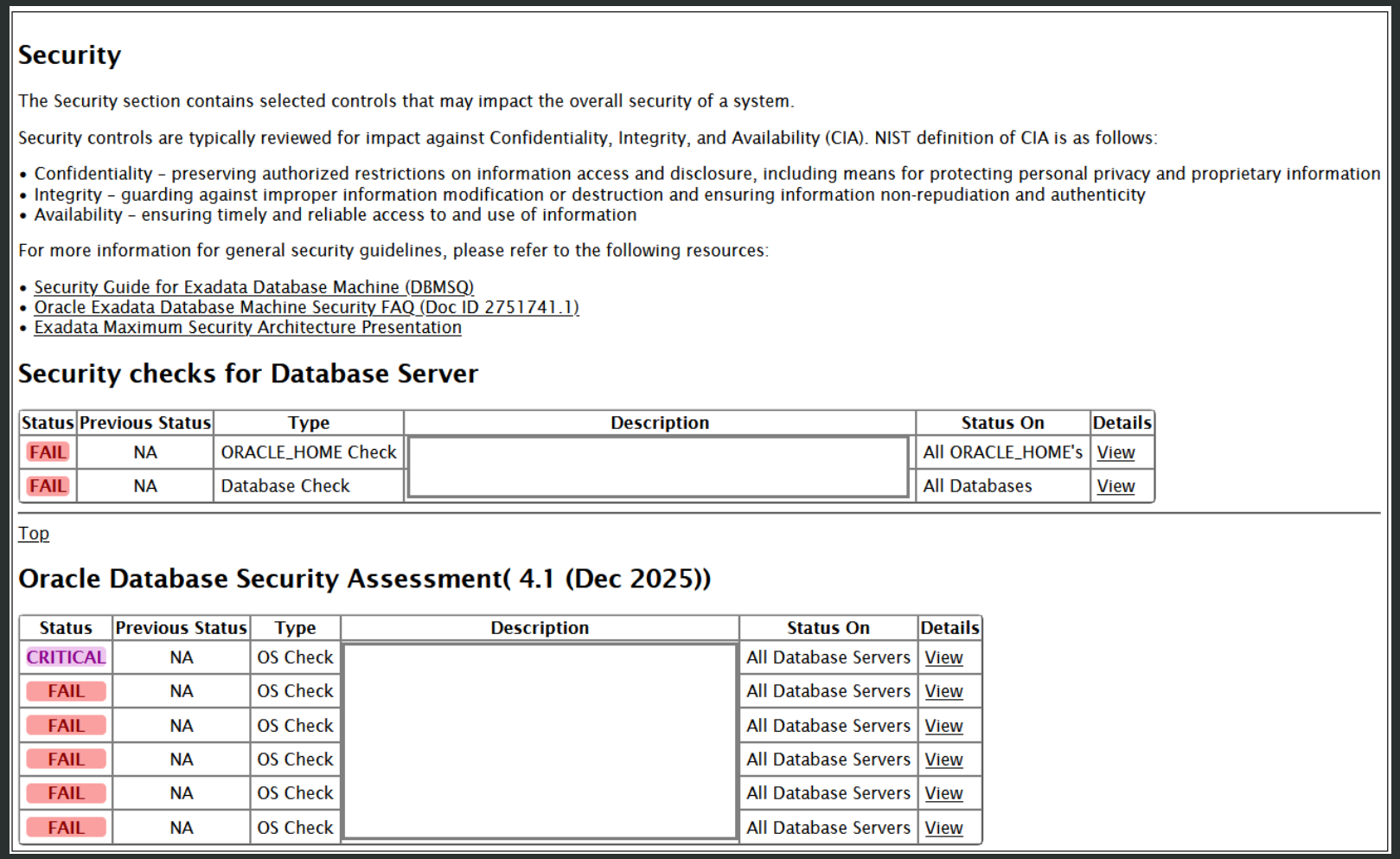
Copyright © 2026, Oracle and/or its affiliates

Exachk Security Scorecard

Default exachk command
./exachk

Exachk with optional security profile
./exachk -includeprofile security

Optional profile includes:
- Default password checks
  - Database server
  - Storage server
  - ILOM
  - Database users
- Validate network configuration file
  - Grid home
  - RDBMS home
- DBSAT report (database)



Security

The Security section contains selected controls that may impact the overall security of a system.

Security controls are typically reviewed for impact against Confidentiality, Integrity, and Availability (CIA). NIST definition of CIA is as follows:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability – ensuring timely and reliable access to and use of information

For more information for general security guidelines, please refer to the following resources:

- Security Guide for Exadata Database Machine (DBMSQ)
- Oracle Exadata Database Machine Security FAQ (Doc ID 2751741.1)
- Exadata Maximum Security Architecture Presentation

Security checks for Database Server

Status	Previous Status	Type	Description	Status On	Details
FAIL	NA	ORACLE_HOME Check		All ORACLE_HOME's	View
FAIL	NA	Database Check		All Databases	View

Top

Oracle Database Security Assessment(4.1 (Dec 2025))

Status	Previous Status	Type	Description	Status On	Details
CRITICAL	NA	OS Check		All Database Servers	View
FAIL	NA	OS Check		All Database Servers	View
FAIL	NA	OS Check		All Database Servers	View
FAIL	NA	OS Check		All Database Servers	View
FAIL	NA	OS Check		All Database Servers	View
FAIL	NA	OS Check		All Database Servers	View

Copyright © 2026, Oracle and/or its affiliates

Exadata Security Capabilities

Maximize Security, Maximize Performance, Maximum Availability

Storage Server Security Hardening

Oracle Exadata System Software release 26.1.0 introduces new capabilities that harden storage server security.

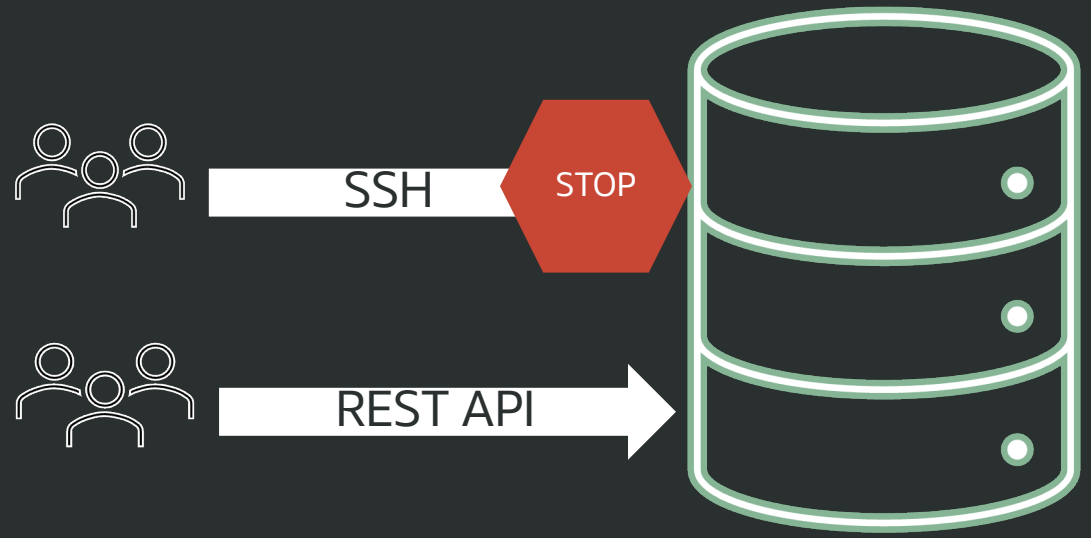
- The Exadata storage server built-in operating system (OS) user accounts (celladmin and cellmonitor) are restricted to run specific Cell Command Line Interface (CellCLI) and Exascale Command Line Interface (ESCLI) commands, along with a limited set of read-only Linux OS commands.
- Additionally, for Exascale environments, each OS user now uses a separate Exascale keystore (wallet) with appropriate corresponding credentials. By default, the wallet associated with celladmin provides Exascale administrator privileges, while the cellmonitor wallet provides read-only access to Exascale objects and metadata.
- Exadata administrators can now manage SSH equivalence for the celladmin and cellmonitor accounts using CellCLI commands to CREATE SSHEQUIVALENCE, LIST SSHEQUIVALENCE, and DROP SSHEQUIVALENCE.
- Oracle Exadata Deployment Assistant (OEDA) supports initial deployments using the celladmin OS user account. During these deployments, celladmin performs the deployment tasks, and root SSH access is disabled on all storage servers.

Copyright © 2026, Oracle and/or its affiliates

Storage Server Lockdown with RESTful Service

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.



Copyright © 2026, Oracle and/or its affiliates

Exascale Immutable Snapshots

Starting with Oracle Exadata System Software release 26.1.0, you can lock an Exascale snapshot (file or volume) to prevent its deletion before a specified future date and time. You can also make the lock immutable, which prevents users from removing the lock or changing it to expire earlier.

Immutable snapshots can help organizations meet financial or legal data retention requirements. They also provide tamper-resistant, time-based retention for Exascale files and volumes, helping customers create trusted point-in-time copies for compliance, ransomware recovery, and testing.

`snapLockExpiryTime`: Specifies the snapshot lock expiry time.

`snapLockImmutable`: Boolean value (true or false) indicating whether the lock is immutable:

- A mutable (variable) lock (snapLockImmutable=false) prevents the snapshot from being deleted before the snapshot lock expiry time (snapLockExpiryTime).
- An immutable lock (snapLockImmutable=true) prevents the snapshot from being deleted before the snapshot lock expiry time (snapLockExpiryTime) and also prevents users from removing the lock or changing it to expire earlier.

Copyright © 2026, Oracle and/or its affiliates

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.

Copyright © 2026, Oracle and/or its affiliates

Simpler Linux Package Dependency Management

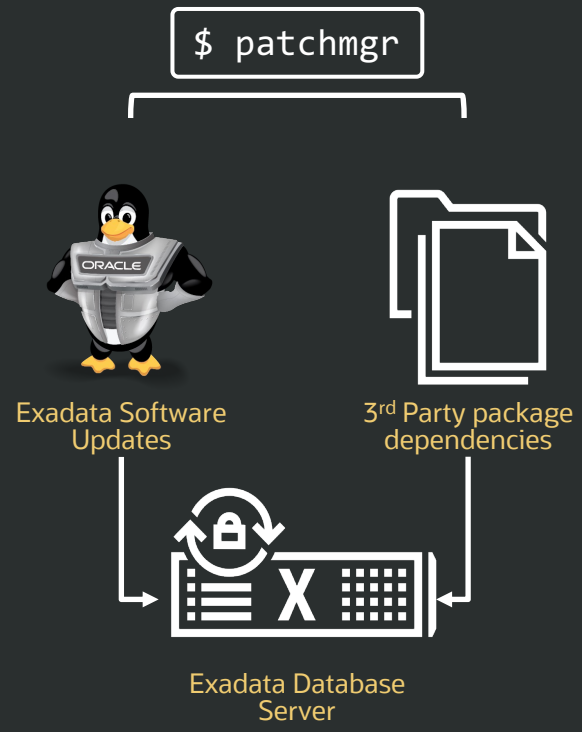
Customers often install 3rd party software on Exadata Database Servers such as security, monitoring, and backup utilities.

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 3rd party software during database server updates

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



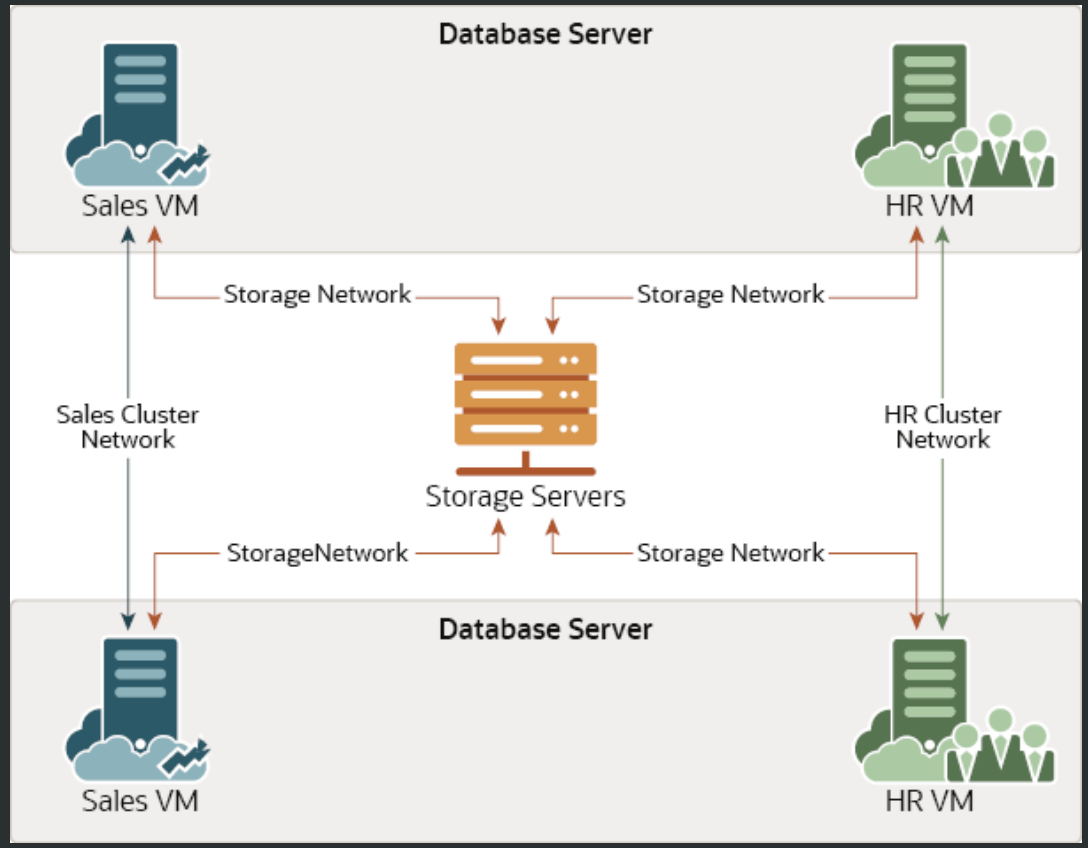

```
$ patchmgr --precheck | --upgrade [ { --additional-rpms } | --additional-rpms-list } [ --additional-rpms-from-repo ]
```


Copyright © 2026, Oracle and/or its affiliates

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.



Copyright © 2026, Oracle and/or its affiliates

Exadata Live Update

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

- 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.

When using Exadata Live Update, you must choose from the following options:

- **highcvss**: All new packages with High or Critical security mitigations
- **allcvss**: All new packages with any security mitigations (Low, Medium, High, Critical)
- **full**: All new packages in the image



98% security mitigation compliance without a reboot*

**testing based on 25.1.1.0.0 – 25.1.12.0.0 with Exadata Live Update using "allcvss"*

Copyright © 2026, Oracle and/or its affiliates

Exadata Live Update Example

Patchmgr command

```
# ./patchmgr --dbnodes dbs_group --upgrade --repo <repo>/exadata_ol8_26.1.1.0.0.260713_Linux-x86-64.zip --target_version 26.1.1.0.0.260713 --log_dir auto --live-update-target allcvss
```

Imagehistory output from Exadata 25.2.x with Exadata Live Update to 26.1.1.0.0

```
Exadata software version: 25.2.10.0.0.260528
Exadata Live Update Type: all (CVSS 1-10)
Exadata Live Update Version: 26.1.1.0.0.260713 (Live Update applied. Reboot at any time to finalize outstanding items.)
Node type: GUEST
```


Copyright © 2026, Oracle and/or its affiliates

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*

Copyright © 2026, Oracle and/or its affiliates

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
```


Copyright © 2026, Oracle and/or its affiliates

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)
```


Copyright © 2026, Oracle and/or its affiliates

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
```


Copyright © 2026, Oracle and/or its affiliates

Oracle Database 26ai and Exadata-Relevant Enhancements

Smart Scan on AES-XTS encrypted data

- Enables Exadata Smart Scan for AES-XTS encrypted tablespaces, improving security while preserving scan performance.

Smart Scan during online encryption operations

- Keeps Exadata Smart Scan enabled during online encryption, decryption, and rekeying operations.

Transportable Binary XML with Exadata pushdown

- Supports Exadata pushdown operations for better XML query performance and scalability.

Automatic In-Memory sizing improves Exadata scans

- Improves Exadata scan performance for partially populated objects in Autonomous AI Database.

Memory Speed Columnar

- Reduces format mismatch across HCC, Exadata flash columnar formats, and Database In-Memory to improve analytic scan efficiency.

Copyright © 2026, Oracle and/or its affiliates

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 (KB281712)
- LDAP configuration example in Exadata compute nodes and storage servers using SSSD (KB680684)

Copyright © 2026, Oracle and/or its affiliates

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

Copyright © 2026, Oracle and/or its affiliates

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
…
```


Copyright © 2026, Oracle and/or its affiliates

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.

Copyright © 2026, Oracle and/or its affiliates

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

Copyright © 2026, Oracle and/or its affiliates

host_access_control (hac) – system settings

```
# /opt/oracle.cellos/host_access_control --help
```

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

Copyright © 2026, Oracle and/or its affiliates

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

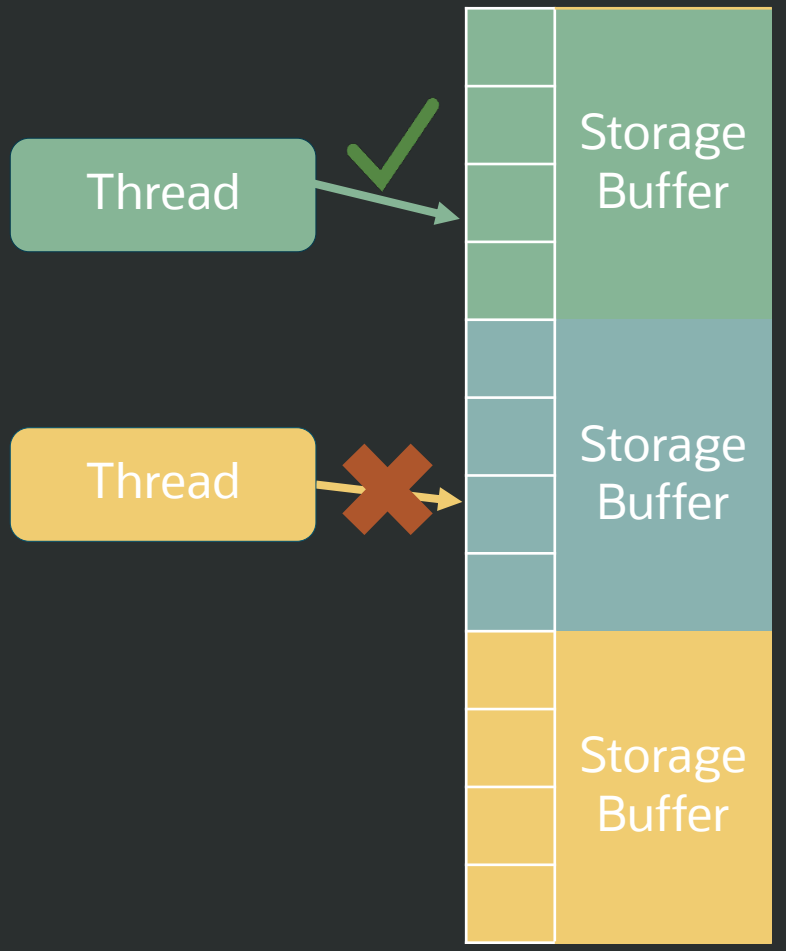
- SSH controls
  - STIG mitigation: The Oracle Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Copyright © 2026, Oracle and/or its affiliates

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.**



Copyright © 2026, Oracle and/or its affiliates

Secure Computing 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 performs additional validation of the arguments.

Copyright © 2026, Oracle and/or its affiliates

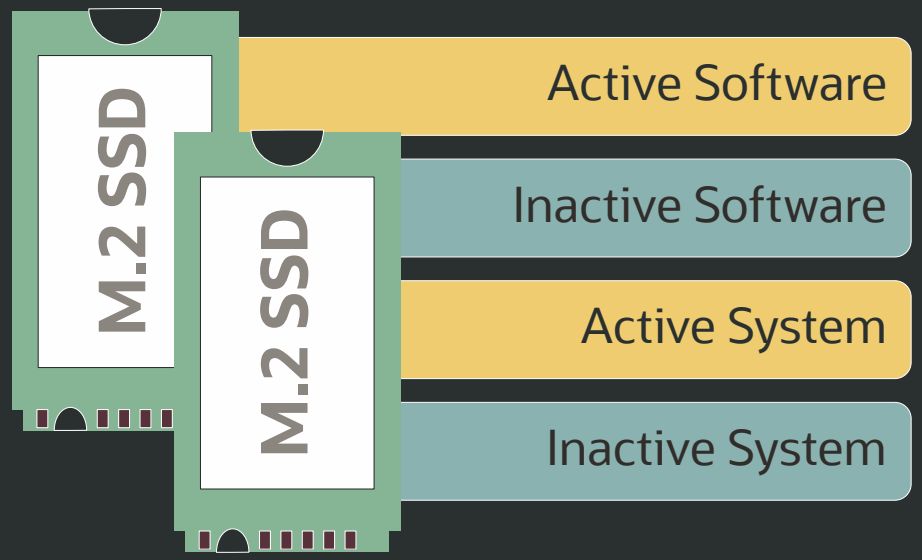
Storage Server Partition Installation

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.

Copyright © 2026, Oracle and/or its affiliates

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.

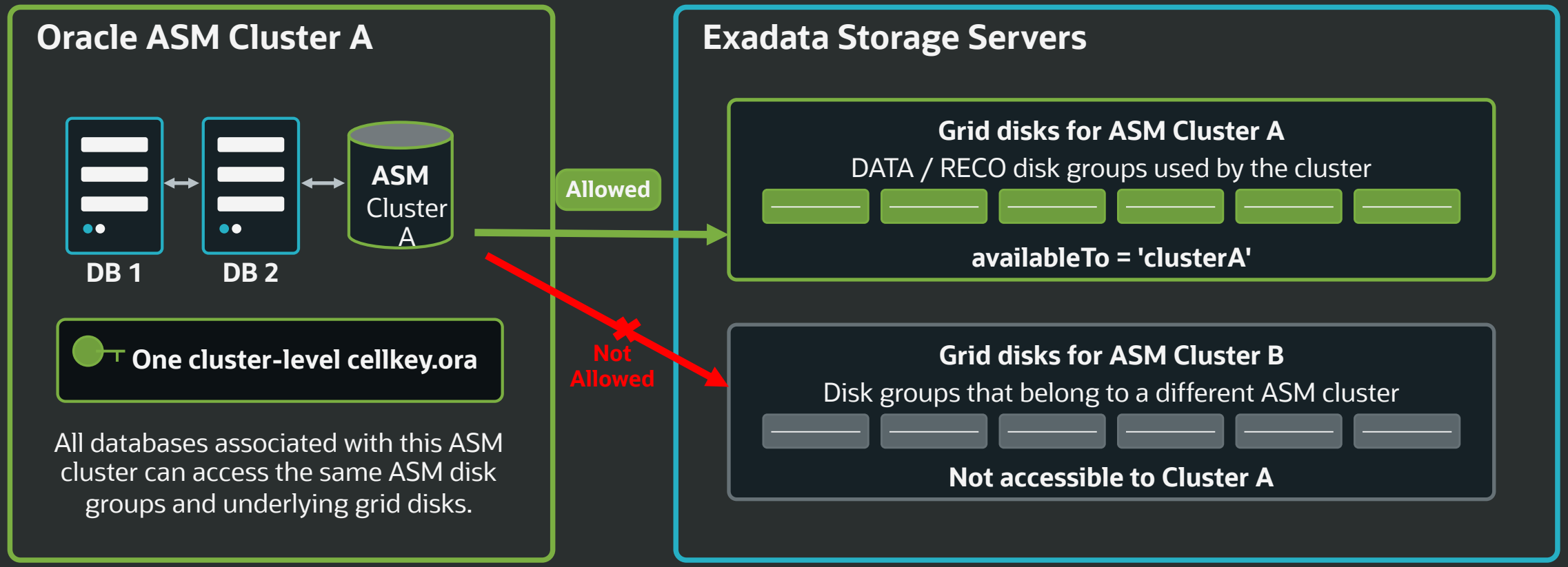
```
# /opt/oracle.SupportTools/exadataAIDE -status
AIDE: daily cron is currently enabled.

To add additional rules:
Edit the file /etc/aide.conf

Update the AIDE database metadata.
# /opt/oracle.SupportTools/exadataAIDE -u
```

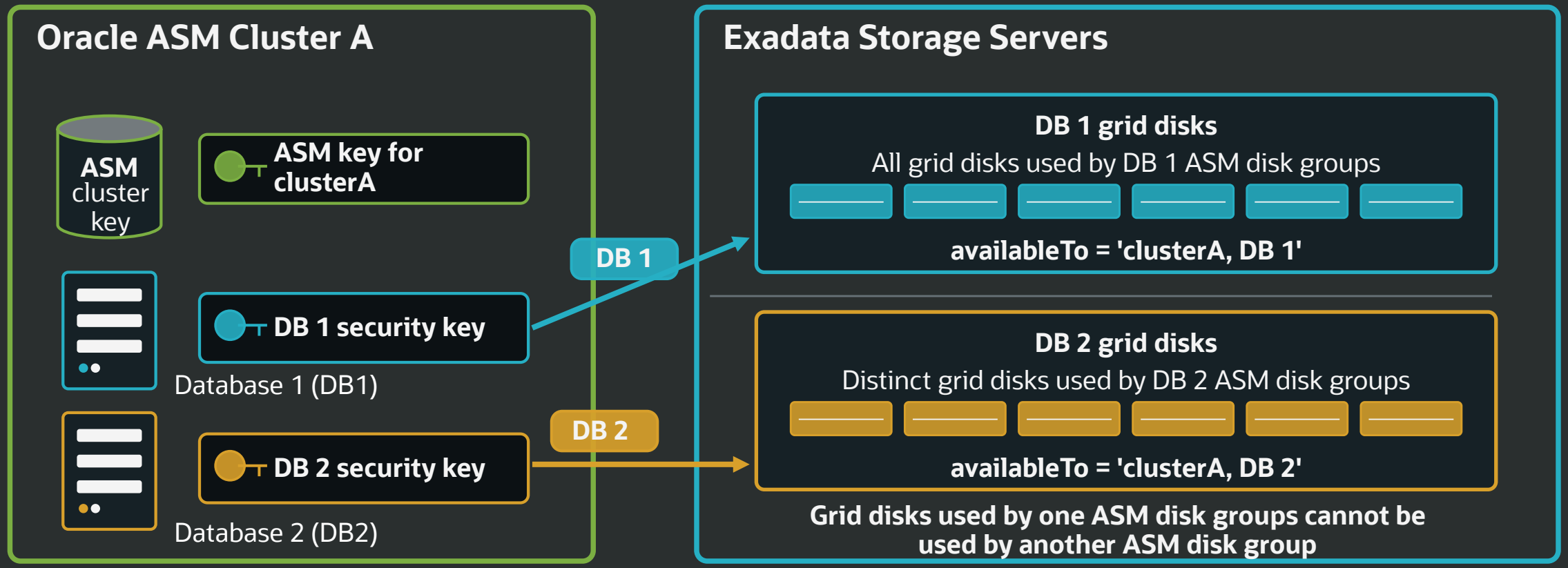

Copyright © 2026, Oracle and/or its affiliates

ASM-scoped security



Copyright © 2026, Oracle and/or its affiliates

DB-scoped security



Copyright © 2026, Oracle and/or its affiliates

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	Erasure Method
Hard drive	• 8 TB hard drives on Oracle Exadata Database Machine X5 • All hard drives on Oracle Exadata Database Machine X6 or later	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

Copyright © 2026, Oracle and/or its affiliates

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!

Copyright © 2026, Oracle and/or its affiliates

References

Maximize Security, Maximize Performance, Maximum Availability

Security References

Exadata Security MOS Notes

- Oracle Exadata Database Machine Security FAQ (FAQ6010)

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/

Copyright © 2026, Oracle and/or its affiliates

Thank you

Any questions?

Copyright © 2026, Oracle and/or its affiliates





Copyright © 2026, Oracle and/or its affiliates