

# Oracle® Database Appliance

## Security Guide



Release 19.29  
G42410-01  
November 2025

ORACLE®

Copyright © 2014, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Audience	i
Documentation Accessibility	i
Related Documents	i
Conventions	i

## 1 Overview of Oracle Database Appliance Security

---

Basic Security Principles	1
Survivability of Mission-Critical Workloads	2
Defense in Depth to Secure the Operating Environment	3
Least Privilege for Services and Users	3
Accountability of Events and Actions	4

## 2 Security Features of Oracle Database Appliance

---

About Oracle Database Appliance Security Features	2
About SELinux on Oracle Database Appliance	2
Oracle Database Appliance and Common Vulnerabilities and Exposures (CVEs)	3
Identifying Security Issues and Picking up Security Updates	3
About Multi-User Access for Oracle Database Appliance Security	4
Restricting the Binaries for Starting the System	4
Understanding Secure Boot	4
Enabling and Disabling Secure Boot	5
Using Isolation Policies	6
Isolating Network Traffic	6
Isolating Databases	7
Controlling Access to Data	7
Controlling Network Access	8
Controlling Database Access	8
About Managing Privileges and Security with SUDO	8
Configuring a SUDO Security Policy for the DCS Stack	9
Using Cryptographic Services	10
Monitoring and Auditing of Databases on Oracle Database Appliance	11

About FIPS 140-2 Compliance on Oracle Database Appliance	12
About STIG Compliance on Oracle Database Appliance	12
Checking for STIG Compliance on Oracle Database Appliance	12
About Oracle Linux Security Scripts auto_answer File	16
About STIG Exceptions on Oracle Database Appliance	18
About Security Content Automation Protocol (SCAP) Findings	24
Using Oracle ILOM for Secure Management	26

## 3 Planning a Secure Environment

---

Considerations for a Secure Environment	1
Understanding User Accounts	3
Understanding the Default Security Settings	3

## 4 Keeping Oracle Database Appliance Secure

---

Securing the Hardware	1
Securing the Software	2
Configuring a Third-Party Certificate for Oracle Database Appliance	3
Creating a Key and Java Keystore and Importing a Trusted Certificate	3
Configuring the DCS Server to Use Custom Keystore	5
Configuring the DCS Agent To Use a Custom Certificate	6
Maintaining a Secure Environment	7
About Secure Environments	7
Maintaining Network Security	7
Updating Software and Firmware	8
Ensuring Data Security Outside of Oracle Database Appliance	8

## Index

---

# Preface

This guide describes security for Oracle Database Appliance. It includes information about the components, the recommended password policies, and best practices for securing the Oracle Database Appliance environment.

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

## Audience

This document is intended for system, database, and network administrators responsible for securing Oracle Database Appliance.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

## Related Documents

For more information about Oracle Database Appliance, go to <http://www.oracle.com/goto/oda/docs> and click the appropriate release.

For more information about using Oracle Database, go to <http://docs.oracle.com/database/> and select the database release from the menu.

For more information about Oracle Integrated Lights Out Manager 3.2, see [https://docs.oracle.com/cd/E37444\\_01/](https://docs.oracle.com/cd/E37444_01/).

For more details about other Oracle products that are mentioned in Oracle Database Appliance documentation, see the Oracle Documentation home page at <http://docs.oracle.com>.

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, emphasis, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
\$ prompt	The dollar sign (\$) prompt indicates a command run as any user other than the <code>root</code> user.
# prompt	The pound (#) prompt indicates a command that is run as the <code>root</code> user.

# 1

## Overview of Oracle Database Appliance Security

Oracle Database Appliance provides a complete package of integrated security capabilities to complement its integrated hardware and software system design.

In addition to basic security principles, Oracle Database Appliance addresses survivability, defense in depth, least privilege, and accountability. Oracle Database Appliance delivers a well-integrated set of security capabilities that help organizations address their most-pressing security requirements and concerns.

Topics:

- [Basic Security Principles](#)  
Oracle Database Appliance is configured with common basic security principles for software and hardware.
- [Survivability of Mission-Critical Workloads](#)  
Oracle Database Appliance follows Oracle Maximum Availability Architecture best practices, which can prevent or minimize the damage caused from accidental and malicious actions taken by internal users or external parties.
- [Defense in Depth to Secure the Operating Environment](#)  
Oracle Database Appliance employs multiple, independent, and mutually-reinforcing security controls to help organizations create a secure operating environment for their workloads and data.
- [Least Privilege for Services and Users](#)  
The Least-Privilege principle includes more than ensuring that applications, services and users have access to the capabilities that they need to perform their tasks. It is equally important to limit access to unnecessary capabilities, services, and interfaces.
- [Accountability of Events and Actions](#)  
When an incident occurs, a system must be able to detect and report the incident. Similarly, when an event cannot be prevented, it is imperative that an organization be able to detect that the event occurred so that proper responses can be taken.

## Basic Security Principles

Oracle Database Appliance is configured with common basic security principles for software and hardware.

Basic security includes the following methods:

- Authentication.  
All components in Oracle Database Appliance use authentication to ensure that users are who they say they are. By default, Oracle Database Appliance authenticates users with local user names and passwords.
- Authorization.  
Authorization enables administrators to control what tasks or privileges a user may perform or use. Oracle Database Appliance system administrators can configure resources with

read/write/run permissions. These permissions are used to control user access to commands, disk space, devices, and applications. In addition, system administrators can use SUDO to grant non-root users the ability to run DCS and OAK commands.

- Accounting and Auditing.

Accounting and auditing enables you to maintain a record of users' activity on the system. Oracle Database Appliance software and hardware features enable administrators to monitor login activity, and to maintain hardware inventories. Accounting and auditing are implemented with the following methods:

- Hardware assets are tracked through serial numbers. Oracle part numbers are electronically recorded on all cards, modules, and motherboards. You can use these serial numbers to maintain inventory records.
- User logins are monitored through system logs. System administrators and service accounts have access to commands that, if used incorrectly, could cause harm and data loss. Use system logs to monitor access and commands.

Oracle Database Appliance uses identity and access management principles including least privilege implementation to control access to key components, services and data. System administration requires root access. Oracle Grid Infrastructure and database management is performed with a combination of root and unprivileged users such as database and grid.

Role separation of database and grid operating system users is supported and recommended. By default, Oracle Database Appliance has one database user. All administration through ODACLI commands requires root access. However, the multi-user access feature allows a non-root, or unprivileged user to administer using ODACLI commands and more than one database user to be present on the system, each owning and managing their database homes and databases. Virtualization support allows isolation of database resources.

For data protection, Oracle Database security features such as Transparent Data Encryption (TDE) and Oracle Database Vault are available. Oracle Audit Vault and Database Firewall (Oracle AVDF) can be used for auditing and network monitoring respectively.

## Survivability of Mission-Critical Workloads

Oracle Database Appliance follows Oracle Maximum Availability Architecture best practices, which can prevent or minimize the damage caused from accidental and malicious actions taken by internal users or external parties.

Oracle Maximum Availability Architecture best practices help to provide organizations with hardware and software platforms for mission-critical workloads. These best practices increase survivability by using the following methods:

- Ensuring that the components used in Oracle Database Appliance are designed, engineered, and tested to work well together in support of secure deployment architectures.

Oracle Database Appliance supports secure isolation, access control, cryptographic services, monitoring and auditing, quality of service, and secure management.

- Reducing the default attack surface of its constituent products to help minimize the overall exposure of the machine.

You can customize Oracle Database Appliance security settings, based on your organization's policies and needs.

- Protecting the machine, including its operational and management interfaces.



Oracle Database Appliance is protected using a complement of open and vetted protocols, and APIs capable of supporting traditional security goals of strong authentication, access control, confidentiality, integrity, and availability.

- Verifying that software and hardware contain features that keep the service available, even when failures occur.

These hardware and software redundancy capabilities help in cases where attackers attempt to disable one or more individual components in the system.

## Defense in Depth to Secure the Operating Environment

Oracle Database Appliance employs multiple, independent, and mutually-reinforcing security controls to help organizations create a secure operating environment for their workloads and data.

Oracle Database Appliance supports the principle of defense in depth by:

- Offering a strong complement of protections, which secure information in transit, in use, and at rest. Security controls are available at the server, storage, network, database, and application layers. You can integrate each layer's unique security controls with the others to enable the creation of strong, layered security architectures.
- Supporting the use of well-defined and open standards, protocols, and interfaces. You can integrate Oracle Database Appliance into your organization's existing security policies, architectures, practices and standards. Integration is critical, because applications and devices do not exist in isolation. IT security architectures is only as strong as its weakest component.
- Conducting multiple security scans using industry-leading security analyzers, which implement all high-priority security items before each new Oracle Database Appliance software version release.
- Other features include:
  - FIPS 140-2 compliant Oracle Linux kernel.
  - TLS 1.2 for all services running as a part of the Oracle Database Appliance software stack.
  - No default passwords, with the only exception being Oracle ILOM.
  - All secrets are stored using Oracle-supported mechanism – wallets.
  - Secure erasure that conforms to the NIST 800-88 standard, also called NIST Special Publication 800-88 (NIST SP 800-88).
  - Availability of STIG benchmark for system hardening.
  - UEFI Secure Boot is enabled on Oracle Database Appliance X10.

## Least Privilege for Services and Users

The Least-Privilege principle includes more than ensuring that applications, services and users have access to the capabilities that they need to perform their tasks. It is equally important to limit access to unnecessary capabilities, services, and interfaces.

Oracle Database Appliance promotes the principle of least-privilege by:

- Granting access to individual servers, storage, operating system, databases, and other components based on the role of each user and administrator. Using role-based and multi-

factor access control models with fine-grained privileges enables you to limit access only to the privileges needed to perform assigned roles.

- Restricting application access to information, underlying resources, network communications, and local or remote service access only to what is needed for the application.

Whether caused by accident or by malicious attack, applications can misbehave. Enforcing Least Privilege practices helps to prevent applications from causing harm beyond their intended use.

## Accountability of Events and Actions

When an incident occurs, a system must be able to detect and report the incident. Similarly, when an event cannot be prevented, it is imperative that an organization be able to detect that the event occurred so that proper responses can be taken.

Oracle Database Appliance uses the following methods to support the principle of accountability:

- Ensuring each of the components used in Oracle Database Appliance supports activity auditing and monitoring, including the ability to record login and logout events, administrative actions, and other events specific to each component.
- Leveraging features in Oracle Database to support fine-grained, auditing configurations. These configurations enables organizations to tune audit configurations in response to their standards and goals. Administrators can ensure that critical information is captured, while minimizing the amount of unnecessary audit events.

# 2

## Security Features of Oracle Database Appliance

Oracle Database Appliance uses hardware and software hardening processes to secure the system, and that assist in deploying a layered security strategy.

Topics:

- [About Oracle Database Appliance Security Features](#)  
Oracle Database Appliance includes hardening configuration and security capabilities to core components.
- [About SELinux on Oracle Database Appliance](#)  
Understand how SELinux enhances security on Oracle Database Appliance
- [Oracle Database Appliance and Common Vulnerabilities and Exposures \(CVEs\)](#)  
Oracle Database Appliance software for each release contains only necessary Oracle Linux RPMs, that is, approximately 20% of the total available Oracle Linux RPMs to minimize potential vulnerabilities and exposures.
- [Identifying Security Issues and Picking up Security Updates](#)  
Oracle Database Appliance conducts regular, extensive security scans across the entire stack using industry leading security scanners.
- [About Multi-User Access for Oracle Database Appliance Security](#)  
Multi-user access can enhance security of the Oracle Database Appliance system and provide an efficient mechanism for role separation.
- [Restricting the Binaries for Starting the System](#)  
Secure Boot is enabled by default on Oracle Database Appliance X10.
- [Using Isolation Policies](#)  
Isolation policies provide more secure multitenant services.
- [Controlling Access to Data](#)  
Controlling access to data, workloads and infrastructure helps to provide greater security.
- [Using Cryptographic Services](#)  
Cryptographic services can help to protect and validate information at rest, in transit, and in use.
- [Monitoring and Auditing of Databases on Oracle Database Appliance](#)  
Oracle Database Appliance includes Oracle Database Fine Grained Auditing (FGA), Oracle Audit Vault, and Oracle Database Firewall Remote Monitor, which provide comprehensive monitoring and auditing features.
- [About FIPS 140-2 Compliance on Oracle Database Appliance](#)  
Understand how FIPS 140-2 is implemented on Oracle Database Appliance.
- [About STIG Compliance on Oracle Database Appliance](#)  
Understand Security Technical Implementation Guidelines (STIG) and how to check Oracle Database Appliance for compliance with STIG.
- [Using Oracle ILOM for Secure Management](#)  
Oracle Integrated Lights-Out Management (Oracle ILOM) enables full out-of-band management, providing remote management capability for Oracle Database Appliance.

# About Oracle Database Appliance Security Features

Oracle Database Appliance includes hardening configuration and security capabilities to core components.

Your organization can use the security features of Oracle Database Appliance as part of a layered security strategy.

## Hardening Configuration

Oracle Database Appliance includes the following recommended hardening configuration procedures:

- Installed packages are trimmed to a minimum, so that unnecessary packages are not installed on the servers.
- Essential services only are enabled on the Oracle Database Appliance nodes.
- Operating system users are audited.
- Secure configurations for chrony, SSH, and other services.

Oracle Database Appliance only enables essential and secure services that are required for system functionality. Among the set of RPMs that Oracle Database Appliance installs, the dependent services that are enabled by default during installation are disabled, if not required. Oracle Database Appliance runs regular security scans, identifies services that are not required, and shuts down these services during installation. For example, systemd services such as rhnsd, smartd, hwmgmt, ibacm rpcidmapd, hmp-interconnect, hmp-ipmi, sssd, and abrt-vmcore. Services that are delivered with a default configuration, can be modified to be more secure. For example, disabling SNMPv1, SNMPv2, and public community on SNMP, or disabling weak ciphers for the sshd service, or disabling the ILOM interconnect network.

## Security Capabilities

Oracle Database Appliance architecture provides security capabilities to the core components. The capabilities are grouped into the following categories:

- Isolation policies
- Controlled access to data
- Cryptographic services
- Monitoring and auditing
- Oracle Integrated Lights Out Manager (ILOM)

# About SELinux on Oracle Database Appliance

Understand how SELinux enhances security on Oracle Database Appliance

SELinux is enabled by default in permissive mode on Oracle Database Appliance. There is an audit of certain targeted operating system services, such as Apache HTTPD (httpd), SSH Daemon (sshd), BIND DNS (named), and others when configured for SELinux. Any denial that appears in the audit log file is informational and does not have any functional impact on the performance of the appliance. A sample list of the violations in categories obtained from Oracle Database Appliance is described in the following table.

**Table 2-1 SELinux violations**

Audit Category	Description	Audit Log Instances (approximate)
ssh	SSH equivalence set up during job runs	32
agetty	Console login by user	6 (depending on the number of logins)
oda-image-first	Runs during startup	4
plymouthd	Runs during startup	4
dmiencode	Hardware information collection during the start process	4
ssh-keygen	Pertain to ssh equivalence setup during job runs	4
rsync	Pertain to Oracle Grid Infrastructure operations after SSH equivalence	2
virsh	Pertain to DB system creation and KVM management	2
unknown	related to file not labelled for SELinux purposes. Some of these violations may not occur after restart and relabel.	230

## Oracle Database Appliance and Common Vulnerabilities and Exposures (CVEs)

Oracle Database Appliance software for each release contains only necessary Oracle Linux RPMs, that is, approximately 20% of the total available Oracle Linux RPMs to minimize potential vulnerabilities and exposures.

Oracle Database Appliance also protects its RPMs through version lock so that you do not accidentally override these RPMs. To check if a specific CVE affects Oracle Database Appliance or when the CVE may be fixed, contact Oracle Support.

## Identifying Security Issues and Picking up Security Updates

Oracle Database Appliance conducts regular, extensive security scans across the entire stack using industry leading security scanners.

Oracle Database Appliance runs the following scans to detect vulnerabilities in the software stack, in compliance with Oracle security standards.

- The proprietary scans called Open Source Compliance Service (OSCS) scan and AppDep Vulnerability scan that Oracle owns, scans open source software that Oracle Database Appliance software uses, for open vulnerabilities. This scan also includes malware scan in open source software Oracle Database Appliance uses. All open-source and third-party software is built internally within Oracle.
- Tenable Nessus vulnerability scan runs on bare metal and DB system to determine vulnerabilities.
- Microfocus Webinspect scan is run against DCS software to determine REST API security.

- Fortify is used for static code analysis.

## About Multi-User Access for Oracle Database Appliance Security

Multi-user access can enhance security of the Oracle Database Appliance system and provide an efficient mechanism for role separation.

When multi-user access is not enabled, a single Oracle Database Appliance account with user name and password is used to connect to the appliance, run ODACLI commands, or log into the Browser User Interface (BUI). The `root` user performs all administration on an Oracle Database Appliance. When multi-user access is enabled, you have the option of providing separate access to database administrators to manage databases. Display of resources within the Browser User Interface is also filtered as per user role. Root access is restricted to the Oracle Database Appliance system administrator to access system logs or debug issues that require root access.

When you enable multi-user access, you create multiple users with different roles that restrict them from accessing resources created by other users and also restrict the set of operations they can perform using ODACLI commands or the BUI. The same user credentials that you set up, can be used for logging into the BUI and running ODACLI commands. The BUI also displays resources and information based on access to the set of resources. A separate **Multi-User Access Management** tab is available only to the `odaadmin` user to administer the users and resources in the system.

Enabling multi-user access requires that you specify the password to run ODACLI commands. A successful authentication generates a token with a validity of 120 minutes. Any ODACLI command that you run within that duration does not require a password and each successful run renews the token, extending its validity. If the token expires due to inactivity, then you are prompted for the password when you run an ODACLI command.

### ① See Also

*Oracle Database Appliance Deployment and User's Guide* for your hardware model.

## Restricting the Binaries for Starting the System

Secure Boot is enabled by default on Oracle Database Appliance X10.

- [Understanding Secure Boot](#)  
Secure Boot is a method used to restrict which binaries can boot the system.
- [Enabling and Disabling Secure Boot](#)  
You can change the Secure Boot setting by entering the Setup during the boot process.

## Understanding Secure Boot

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

With Secure Boot, the system UEFI firmware allows boot loaders that carry the cryptographic signature of trusted entities. All processes that run in the UEFI firmware must be signed with a key that the system recognizes as trustworthy. With each restart of the server, every component in the boot sequence is verified. This prevents malware from hiding embedded code in the boot sequence.

Loadable kernel modules must be signed with a trusted key or they cannot be loaded into the kernel. The following trusted keys are stored in UEFI NVRAM variables:

- **UEFI Secure Boot Database Key (DB):** Signature database that contains well-known keys. Only binaries that can be verified against the DB are run by the BIOS.
- **Forbidden Signature Database Key (DBX):** Keys that are blocked. Attempting to load an object with a key that matches an entry in the DBX will be denied. This is a list of keys that are bad.
- **Machine Owner Key (MOK):** User-added keys for kernel modules that you want to install.
- **Platform Key (PK):** The key installed by the hardware vendor. This key is installed by the vendor and is in the Oracle ILOM firmware. This key is not accessible from the host.
- **Key Exchange Key (KEK):** The key required to update the signature database. The user must have physical access to the system console to add keys, modify keys, or enable and disable Secure Boot through the UEFI configuration menu. The default boot loader on most UEFI-enabled servers running Linux is grub2. With Secure Boot enabled, an additional shim boot loader is needed. When booting in Secure Boot mode, the shimloader is called first because it contains a trusted signature. The shimloader then loads grub2, which then loads the operating system kernel, which is also signed.

#### 📘 See Also

*Overview of Secure Boot in Oracle Linux Working With UEFI Secure Boot* at <https://docs.oracle.com/en/operating-systems/oracle-linux/secure-boot/#Oracle-Linux>

### Restrictions for Secure Boot Availability

Currently, Secure Boot is available with Oracle Database Appliance release 19.20.0.1 on Oracle Database Appliance X10 hardware model on bare metal database servers and KVM host systems. Secure Boot is not supported on DB systems and KVM guest machines.

## Enabling and Disabling Secure Boot

You can change the Secure Boot setting by entering the Setup during the boot process.

#### 📘 See Also

*"Overview of Secure Boot" in Oracle Linux Working With UEFI Secure Boot* at <https://docs.oracle.com/en/operating-systems/oracle-linux/secure-boot/#Oracle-Linux>

### Disabling Secure Boot

Follow these steps:

1. During the boot, Press **F2** to run setup.
2. Select **Security**, then select **Secure Boot**.
3. Select **Attempt Secure Boot**.
4. Select **Disabled**.
5. Press **F10** to save and exit.

### Enabling Secure Boot

Follow these steps:

1. During the boot, Press **F2** to run setup.
2. Select **Security**, then select **Secure Boot**.
3. Select **Attempt Secure Boot**.
4. Select **Enabled**.
5. Press **F10** to save and exit.

### Verifying the Status of the Secure Boot Option

To verify the status of the secure boot option, run the command:

```
# mokutil --sb-state
SecureBoot enabled
```

### Managing Keys and Certificates Used with Secure Boot

For information about managing keys and certificates used with secure boot, refer to the topic *Signing Kernel Images and Kernel Modules for Use With Secure Boot in Oracle Linux Working With UEFI Secure Boot* at <https://docs.oracle.com/en/operating-systems/oracle-linux/secure-boot/#Oracle-Linux>

## Using Isolation Policies

Isolation policies provide more secure multitenant services.

If your organization wants to consolidate IT infrastructure, implement shared service architectures, and deliver secure multitenant services, then you should isolate services, users, data, communications, and storage. Oracle Database Appliance provides organizations the flexibility to implement the isolation policies and strategies, based on their needs.

Topics:

- [Isolating Network Traffic](#)  
Oracle Database Appliance isolates client access from device management and inter-device communication at the physical network level.
- [Isolating Databases](#)  
All Oracle Database security options are available for Oracle Database Appliance.

## Isolating Network Traffic

Oracle Database Appliance isolates client access from device management and inter-device communication at the physical network level.

Oracle Database Appliance isolates client and management network traffic on separate networks. Clients access services on a redundant 10 Gbps Ethernet network that ensures reliable, high-speed access to services running on the system. Cluster management access is provided over a physically separate 1 Gbps Ethernet network. Providing physically separate networks ensures separation between operational and management network traffic.

Your organization can choose to further segregate network traffic over the client access Ethernet network by configuring virtual local area networks (VLANs). VLANs segregate



network traffic based on your organization's requirements. Oracle recommends the use of encrypted protocols over VLANs to assure the confidentiality and integrity of communications.

## Isolating Databases

All Oracle Database security options are available for Oracle Database Appliance.

If your organization requires finer-grained database isolation, then you can use software such as Oracle Database Vault, Oracle Virtual Private Database, and Oracle Label Security. One of the best isolation methods is to create physical separation is to dedicate an entire environment to a single application or database. However, servers dedicated to one application or one database are expensive. A more cost-effective isolation strategy uses multiple databases within the same operating system image. You can obtain multiple database isolation through a combination of database and operating system-level controls, such as dedicated credentials for users, groups, and resource controls.

Oracle Database Vault includes a mandatory access control model, which enforces isolation by using logical realms within a single database. Logical realms form a protective boundary around existing application tables by blocking administrative accounts from having ad-hoc access to application data. Oracle Database Vault command rules enable policy-based controls that limit who, when, where, and how the database and application data is accessed. This creates a trusted path to application data. Oracle Database Vault can also be employed to restrict access based upon time, source IP address, and other criteria.

Oracle Virtual Private Database enables the creation of policies that enforce fine-grained access to database tables and views at the row and column levels. Oracle Virtual Private Database provides security portability because the policies are associated with database objects, and are automatically applied no matter how the data is accessed. Oracle Virtual Private Database can be used for fine-grained isolation within the database.

Oracle Label Security classifies data, and mediates access to that data based upon its classification. Your organization can define classification strategies, such as hierarchical or disjoint, that best support their needs. This capability allows information stored at different classification levels to be isolated at the row level within a single tablespace.

## Controlling Access to Data

Controlling access to data, workloads and infrastructure helps to provide greater security.

To protect application data, workloads, and the underlying infrastructure on which it runs, Oracle Database Appliance offers comprehensive yet flexible access control capabilities for both users and administrators. The control capabilities include network access and database access.

Topics:

- [Controlling Network Access](#)  
Configure Network access to provide fine-grained access control.
- [Controlling Database Access](#)  
Help to reduce the risk of collusive behavior and inadvertent errors by using separation of duties at every layer of database architecture using role-allocated operating system users and group system privileges.
- [About Managing Privileges and Security with SUDO](#)  
A SUDO policy helps to provide system auditing and access control for superuser (root) privileges on the operating system. Use these examples to help to implement a SUDO policy.

- [Configuring a SUDO Security Policy for the DCS Stack](#)  
Use these examples to help to implement a SUDO policy for Oracle Database Appliance models that are using the DCS stack (odacli).

## Controlling Network Access

Configure Network access to provide fine-grained access control.

Beyond simple network-level isolation, fine-grained access control policies can be instituted at the device level. All components in Oracle Database Appliance include the ability to limit network access to services either using architectural methods, such as network isolation, or using packet filtering and access control lists to limit communication to, from, and between components and services.

## Controlling Database Access

Help to reduce the risk of collusive behavior and inadvertent errors by using separation of duties at every layer of database architecture using role-allocated operating system users and group system privileges.

For example, use different operating system user accounts and designate different physical groups to grant Oracle Database and Oracle Automatic Storage Management (Oracle ASM) system privileges to ensure role separation for database and storage administrators. Within Oracle Database, you can assign specific privileges and roles to ensure that users have access to only those data objects that they are authorized to access. Data cannot be shared unless it is explicitly permitted.

In addition to the password-based authentication available in Oracle Database, Oracle Advanced Security enables organizations to implement strong authentication using public key credentials, RADIUS, or a Kerberos infrastructure. Using Oracle Enterprise User Security, the database can be integrated with existing LDAP repositories for authentication and authorization. These capabilities provide higher assurance of the identity of users connecting to the database.

You can use Oracle Database Vault to manage administrative and privileged user access, controlling how, when and where application data can be accessed. Oracle Database Vault protects against misuse of stolen login credentials, application bypass, and unauthorized changes to applications and data, including attempts to make copies of application data. Oracle Database Vault is transparent to most applications, and day-to-day tasks. It supports multi-factor authorization policies, allowing for secure enforcement of policy without disrupting business operations.

Oracle Database Vault can enforce separation of duties to ensure that account management, security administration, resource management, and other functions are granted only to those users authorized to have those privileges.

## About Managing Privileges and Security with SUDO

A SUDO policy helps to provide system auditing and access control for superuser (root) privileges on the operating system. Use these examples to help to implement a SUDO policy.

The Oracle Appliance Manager command-line utility requires `root` system privileges for most administrative actions. If you are not logged in as `root`, then you cannot carry out most actions on the appliance. For example, if you are not logged in as `root`, then you can view storage information, but you cannot modify the storage.

You should use SUDO, instead of `su`, to grant root privilege to administrative users. SUDO enables system administrators to grant certain users (or groups of users) the ability to run commands as root without the need for the root password, unlike `su`. It also logs all commands and arguments as part of your security and compliance protocol.

A SUDO security policy is configured by using the file `/etc/sudoers`. Within the `sudoers` file, you can configure groups of users and sets of commands to simplify and audit server administration with SUDO commands.

## Configuring a SUDO Security Policy for the DCS Stack

Use these examples to help to implement a SUDO policy for Oracle Database Appliance models that are using the DCS stack (`odacli`).

A SUDO policy helps to provide system auditing and access control for superuser (root) privileges on the operating system.

### **Caution**

Configuring SUDO to allow a user to perform any operation is equivalent to giving that user `root` privileges. Consider carefully if this is appropriate for your security needs.

### Example 2-1 SUDO Example 1: Allow a User to Perform Any ODACLI Operation

This example shows how to configure SUDO to enable a user to perform any ODACLI operation. You do this by adding lines to the commands section in the `/etc/sudoers` file:

```
## The commands section may have other options added to it.
##
Cmdnd_Alias ODACLI_CMDS=/opt/oracle/oak/bin/odacli *
jdoe ALL = ODACLI_CMDS
```

In this example, the user name is `jdoe`. The file parameter setting `ALL= ODACLI_CMDS` grants the user `jdoe` permission to run all `odacli` commands that are defined by the command alias `ODACLI_CMDS`. After configuration, you can copy one `sudoers` file to multiple hosts. You can also create different rules on each host.

### **Note**

Before database creation, you must set up user equivalency with SSH for the root user on each server. If you do not set up user equivalency and configure SSH on each server, then you are prompted to provide the root password for each server during database creation.

After you configure the `sudoer` file with the user, the user `jdoe` can run the set of `odacli` commands configured with the command alias `ODACLI_CMDS`. For example:

```
$ sudo odacli create database -db newdb
```

**Example 2-2 SUDO Example 2: Allow a User to Perform Only Selected ODACLI Operations**

To configure SUDO to allow a user to perform only selected ODACLI operations, add lines to the commands section in the `/etc/sudoers` file as follows:

```
## DCS commands for oracle user
Cmnd_Alias DCSCMDS = /opt/oracle/dcs/bin/odacli describe-appliance
oracle ALL=          DCSCMDS
```

```
$ sudo /opt/oracle/dcs/bin/odacli describe-appliance
```

## Appliance Information

```
-----
ID: a977bb04-6cf0-4c07-8e0c-91a8c7e7ebb8
Platform:
Data Disk Count: 6
CPU Core Count: 20
Created: June 24, 2022 6:51:52 AM HDT
```

## System Information

```
-----
Name: odal001
Domain Name: example.com
Time Zone: America/Adak
DB Edition: EE
DNS Servers: 10.200.76.198 10.200.76.199 192.0.2.254
NTP Servers: 10.200.0.1 10.200.0.2
```

## Disk Group Information

```
-----
DG Name          Redundancy          Percentage
-----
Data              Normal              90
Reco              Normal              10
```

In this example, the user `jdoe2` tries to run the `sudo odacli list-databases` command, which is not part of the set of commands that is configured for that user. SUDO prevents `jdoe2` from running the command.

```
[jdoe2@servernode1 ~]$ sudo /opt/oracle/dcs/bin/odacli list-databases
```

```
Sorry, user jdoe2 is not allowed to execute '/opt/oracle/dcs/bin/odacli list-
databases' as root on servernode1.
```

## Using Cryptographic Services

Cryptographic services can help to protect and validate information at rest, in transit, and in use.

From encryption and decryption to digital fingerprint and certificate validation, cryptography is one of the most-widely deployed security controls in IT organizations.

Whenever possible, Oracle Database Appliance makes use of cryptographic engines provided by the hardware processors. Using hardware for cryptographic operations provides significant performance improvement over performing the operations in software.

Network cryptographic services protect the confidentiality and integrity of communications by using a cryptographically-secure protocol. For example, Secure Shell (SSH) access provides secure administrative access to systems and Oracle Integrated Lights Out Manager (Oracle ILOM). TLS enables secure communications between applications and other services.

Database cryptographic services are available from Oracle Advanced Security. Oracle Advanced Security encrypts information in the database using the transparent data encryption (TDE) functionality. TDE supports encryption of application table spaces, and encryption of individual columns within a table. Data stored in temporary table spaces, and redo logs are also encrypted. When the database is backed up, the data remains encrypted on destination media. This protects information at rest no matter where it is physically stored. Oracle Advanced Security should be considered for organizations concerned about the confidentiality of stored database content or database encryption, either at the table space level or column-level.

In addition, Oracle Advanced Security encrypts Oracle Net Services and JDBC traffic using either native encryption or TLS to protect information while in transit over a network. Both administrative and application connections can be protected to ensure that data in transit is protected. The TLS implementation supports the standard set of authentication methods including server-only authentication using X.509 certificates and mutual (client-server) authentication with X.509.

## Monitoring and Auditing of Databases on Oracle Database Appliance

Oracle Database Appliance includes Oracle Database Fine Grained Auditing (FGA), Oracle Audit Vault, and Oracle Database Firewall Remote Monitor, which provide comprehensive monitoring and auditing features.

Whether for compliance reporting or incident response, monitoring and auditing are critical functions that organizations must use to gain increased visibility into their IT environment. The degree to which monitoring and auditing is employed is often based upon the risk or criticality of the environment. Oracle Database Appliance has been designed to offer comprehensive monitoring and auditing functionality at the server, network, database, and storage layers ensuring that information can be made available to organizations in support of their audit and compliance requirements.

Oracle Database Fine Grained Auditing (FGA) can help you to create audit records at the level of individual tables and columns, reducing audit overhead. FGA enables organizations to establish policies that selectively determine when audit records are generated. This helps organizations to focus on other database activities, and to reduce the overhead that is often associated with audit activities.

Oracle Audit Vault centralizes the management of database audit settings and automates the consolidation of audit data into a secure repository. Oracle Audit Vault includes built-in reporting to monitor a wide range of activities including privileged user activity and changes to database structures. The reports generated by Oracle Audit Vault enable visibility into various application and administrative database activities, and provide detailed information to support accountability of actions.

Oracle Audit Vault enables the proactive detection and alerting of activities that may be indicative of unauthorized access attempts or abuse of system privileges. These alerts can

include both system and user-defined events and conditions, such as the creation of privileged user accounts or the modification of tables containing sensitive information.

Oracle Database Firewall Remote Monitor can provide real-time database security monitoring. Oracle Database Firewall Remote Monitor queries database connections to detect malicious traffic, such as application bypass, unauthorized activity, SQL injection and other threats. Using an accurate SQL grammar-based approach, Oracle Database Firewall helps organizations quickly identify suspicious database activity.

## About FIPS 140-2 Compliance on Oracle Database Appliance

Understand how FIPS 140-2 is implemented on Oracle Database Appliance.

Starting with Oracle Database Appliance release 19.11, the Linux kernel used by Oracle Database Appliance running on bare metal and KVM Database Systems is compliant with the United States Federal Information Processing Standard 140-2 (FIPS 140-2) Level 1. In accordance with the FIPS standard, the algorithms used by the secure shell (SSH) are limited to those permitted by the standard. FIPS 140-2 is supported in both newly provisioned systems and patched systems. When a system is updated, FIPS support is automatically enabled. No user intervention is needed.

## About STIG Compliance on Oracle Database Appliance

Understand Security Technical Implementation Guidelines (STIG) and how to check Oracle Database Appliance for compliance with STIG.

### Note

With this release of Oracle Database Appliance, Security Technical Implementation Guidelines (STIG) support is deprecated and may be desupported in a later release.

- [Checking for STIG Compliance on Oracle Database Appliance](#)  
Understand how to check the Oracle Database Appliance for compliance with the Security Technical Implementation Guidelines (STIG).
- [About Oracle Linux Security Scripts auto\\_answer File](#)  
Understand how you can use the `auto_answer` file at `/opt/oracle/dcs/stig/auto_answer` to store responses to queries when you run Oracle Linux Security Scripts (OLSS).
- [About STIG Exceptions on Oracle Database Appliance](#)  
Understand the reasons for Security Technical Implementation Guidelines (STIG) exceptions.
- [About Security Content Automation Protocol \(SCAP\) Findings](#)  
Security Content Automation Protocol (SCAP) describes the STIG checks which can be performed in automated manner. To ensure compliance with STIG, a scan is performed periodically on Oracle Database Appliance to determine how compliant it is with the protocol. The current compliance rate is 91%.

## Checking for STIG Compliance on Oracle Database Appliance

Understand how to check the Oracle Database Appliance for compliance with the Security Technical Implementation Guidelines (STIG).

The United States Defense Information Systems Agency (DISA) recommends (or requires in some cases) the Security Technical Implementation Guidelines (STIG) for deployment and management of software, hardware, and system components. For more information about STIG standards, see <https://public.cyber.mil/stigs/downloads/>.

Oracle Database Appliance installs Oracle Linux Security Scripts (OLSS) scripts for Oracle Linux 8 to assist with documenting and aligning with the DISA Oracle Linux 8 STIG. OLSS enables you to verify your existing environment for STIG standards and secure your system against STIG settings that are not set to DISA standards.

Oracle Database Appliance bundles OLSS with the product for Oracle Database Appliance in the directory `/opt/oracle/dcs/stig`.

OLSS has two modes of operation: Verify and Secure. When you run OLSS, the information is displayed on the screen and also saved to a log file. In the Verify mode, the script examines the current compliance status of your system, but it does not change any settings. In the Secure mode, the script examines the current compliance status of your system, and makes changes to the system when the settings or compliance are not adequate, or flags the item as Manual, so that the administrators can make the change.

### Running the STIG Command

Follow these steps to run OLSS:

1. Log in as root user.
2. Run the command from the `/opt/oracle/dcs/stig` directory:

```
[root@odal stig]# ./RunSTIG
```

The summary and detailed logs are in the `/opt/oracle/dcs/stig/logs` directory. When you run the STIG command in the secure or verify mode, the log files are `STIG.Secure.timestamp` or `STIG.Verify.timestamp` respectively.

An example log when running the STIG command in secure mode is as follows. The log contains the order of running the script, documents the user inputs, the rule description, what was seen on the system, and the changes made.

The file has description of whether a rule PASSED/Manual/FAILED : file name is : `Summary.Secure.08_06_2021_05:21`

```
=====
Tests run: 252: CAT1 = 27, CAT2 = 213, CAT3 = 12
CAT1      results: Pass: 24      Fail: 0      Manual: 3
           results: Pass: 88.88% Fail: 0%      Manual: 11.11%
CAT2      results: Pass: 182     Fail: 3      Manual: 28
           results: Pass: 85.44% Fail: 1.40%   Manual: 13.14%
CAT3      results: Pass: 6       Fail: 0      Manual: 6
           results: Pass: 50.00% Fail: 0%      Manual: 50.00%
Total by  results: Pass: 212     Fail: 3      Manual: 37
Weighted  results: Pass: 84.12%  Fail: 1.19%  Manual: 14.68%
=====
```

Both secure and verify modes of STIG classify the severity of the STIG rules as follows:

- SEV1 - Severity-1 STIG rules
- SEV2 - Severity-2 STIG rules
- SEV3 - Severity-3 STIG rules



To verify and secure your Oracle Database Appliance system with STIG-compliant rules based on severity, specify the options as follows:

- Option 1 for verifying SEV1 - Severity-1 STIG rules
- Option 2 for verifying SEV2 - Severity-2 STIG rules
- Option 3 for verifying SEV3 - Severity-3 STIG rules
- Option A for verifying STIG rules of all severities

Following are examples of running the STIG scripts in the Verify and Secure modes. To verify and secure your Oracle Database Appliance system or a KVM DB system with STIG compliance, select the option 3 when you run the STIG command in both Verify and Secure modes.

### Example 2-3 Running STIG Scripts in the Verify Mode

```
[root@host]# /opt/oracle/dcs/stig/RunSTIG -v
```

#### Oracle Linux 8 Security Scripts

The Oracle Linux Security Scripts (OLSS) are a tool designed to assist in creation and deployment of secured Oracle Linux 8 Operating Environment systems.

The OLSS is comprised of a set of scripts and directories.

DISCLAIMER OF WARRANTIES: THE OLSS IS OFFERED "AS IS" AND "WITH ALL FAULTS" AND WITHOUT WARRANTY OF ANY KIND WHATSOEVER. ORACLE DISCLAIMS, AND USERS OF THE OLSS WAIVE, ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND REPRESENTATIONS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE OLSS IS TO BE USED AT YOUR OWN RISK.

NO LIABILITY: IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE IN CONNECTION WITH OR ARISING OUT OF THE USE OF THE OLSS (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA, OR OTHER ECONOMIC ADVANTAGE) HOWEVER IT ARISES, WHETHER FOR BREACH OR IN TORT, EVEN IF ORACLE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I Have read and agree with the above Warning [y n] y  
Are you sure (y/n)? y

\*\*\*\* Welcome to the Oracle Linux 8 STIG tool \*\*\*\*

This tool has two primary modes: Secure and Verify  
Throughout this tool the answers in [] are the expected responses

OLSS will be running in Verify mode - via command line switch

We are running in this environment: oda



**Example 2-4 Running STIG Scripts without specifying any option**

```
[root@host]# /opt/oracle/dcs/stig/RunSTIG
```

### Oracle Linux 8 Security Scripts

The Oracle Linux Security Scripts (OLSS) are a tool designed to assist in creation and deployment of secured Oracle Linux 8 Operating Environment systems.

The OLSS is comprised of a set of scripts and directories.

DISCLAIMER OF WARRANTIES: THE OLSS IS OFFERED "AS IS" AND "WITH ALL FAULTS" AND WITHOUT WARRANTY OF ANY KIND WHATSOEVER. ORACLE DISCLAIMS, AND USERS OF THE OLSS WAIVE, ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND REPRESENTATIONS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE OLSS IS TO BE USED AT YOUR OWN RISK.

NO LIABILITY: IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE IN CONNECTION WITH OR ARISING OUT OF THE USE OF THE OLSS (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA, OR OTHER ECONOMIC ADVANTAGE) HOWEVER IT ARISES, WHETHER FOR BREACH OR IN TORT, EVEN IF ORACLE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I Have read and agree with the above Warning [y n] y  
Are you sure (y/n)? y

\*\*\*\* Welcome to the Oracle Linux 8 STIG tool \*\*\*\*

This tool has two primary modes: Secure and Verify  
Throughout this tool the answers in [] are the expected responses

Do you want to Secure or Verify? [Secure Verify] Verify  
Are you sure (y/n)?

**Example 2-5 Location of Logs**

The list of files in the /opt/oracle/dcs/stig/ directory are as follows:

```
[root@host stig]# pwd
/opt/oracle/dcs/stig

[root@scaoda10ha02c1n1 stig]# ls -l
total 88
-rw----- 1 root root 34300 Sep 13 10:27 auto_answer
-rw----- 1 root root 1794 Sep 13 10:27 LICENSE
drwx----- 2 root root 4096 Oct 3 11:31 logs
drwx----- 3 root root 4096 Sep 13 10:27 meta
-rwx----- 1 root root 25498 Sep 13 10:27 RunSTIG
drwx----- 2 root root 12288 Sep 13 10:27 scripts
```

## Example 2-6 Secure and Verify Logs Summary

The file names for secure, verify, and the corresponding summary file names are given below. The `Summary.Secure.timestamp` file provides the status of compliance after hardening. The `Summary.Verify.timestamp` file provides the status of compliance before hardening.

```
[root@oda1 stig]# pwd
/opt/oracle/dcs/stig/04_Logs
[root@scaoda813c1n2 04_Logs]# ls -la
total 48
drwx-----. 2 3878 900 4096 Aug 31 07:47 .
drwx-----. 9 3878 900 4096 Aug 31 07:47 ..
-rw----- 1 root root 14716 Aug 31 07:47 STIG.Secure.08_31_2021_07:47
-rw----- 1 root root 12884 Aug 31 07:47 STIG.Verify.08_31_2021_07:46
-rw----- 1 root root 1186 Aug 31 07:47 Summary.Secure.08_31_2021_07:47
-rw----- 1 root root 1186 Aug 31 07:47 Summary.Verify.08_31_2021_07:47
```

## About Oracle Linux Security Scripts `auto_answer` File

Understand how you can use the `auto_answer` file at `/opt/oracle/dcs/stig/auto_answer` to store responses to queries when you run Oracle Linux Security Scripts (OLSS).

There are some STIG rules that cannot be evaluated programmatically and require you to provide values.

When you run OLSS, either in the verify or secure mode, the main script prompts for a response for these STIG rules. You can store answers for the questions and acknowledgements encountered when you run OLSS in the `auto_answer` file at `/opt/oracle/dcs/stig/auto_answer`. A NULL answer in this file means that OLSS will prompt for an answer.

For example, when you run the main OLSS script (`RunSTIG`), you are prompted with the following two questions, that require `y` to be specified for each question, to continue the process.

```
[root@oak0 stig]# ./RunSTIG -v
```

### Oracle Linux 8 Security Scripts

The Oracle Linux Security Scripts (OLSS) are a tool designed to assist in creation and deployment of secured Oracle Linux 8 Operating Environment systems.

The OLSS is comprised of a set of scripts and directories.

DISCLAIMER OF WARRANTIES: THE OLSS IS OFFERED "AS IS" AND "WITH ALL FAULTS" AND WITHOUT WARRANTY OF ANY KIND WHATSOEVER. ORACLE DISCLAIMS, AND USERS OF THE OLSS WAIVE, ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND REPRESENTATIONS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE OLSS IS TO BE USED AT YOUR OWN RISK.

NO LIABILITY: IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE IN CONNECTION WITH OR ARISING OUT OF THE USE OF THE OLSS (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA, OR OTHER ECONOMIC ADVANTAGE) HOWEVER IT ARISES, WHETHER FOR BREACH OR IN TORT, EVEN IF ORACLE HAS BEEN

PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I Have read and agree with the above Warning [y n] y

Are you sure (y/n)? y

You have the option to complete the `auto_answer` file and update the following entry with the name of the user who modified the file.

Replace:

`AA_ACK="NULL"`

with:

`AA_ACK="Jane Doe"`

When you run the OLSS script, you are not prompted with the above questions.

```
[root@oak0 stig]# ./RunSTIG -v
```

#### Oracle Linux 8 Security Scripts

The Oracle Linux Security Scripts (OLSS) are a tool designed to assist in creation and deployment of secured Oracle Linux 8 Operating Environment systems.

The OLSS is comprised of a set of scripts and directories.

DISCLAIMER OF WARRANTIES: THE OLSS IS OFFERED "AS IS" AND "WITH ALL FAULTS" AND WITHOUT WARRANTY OF ANY KIND WHATSOEVER. ORACLE DISCLAIMS, AND USERS OF THE OLSS WAIVE, ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND REPRESENTATIONS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE OLSS IS TO BE USED AT YOUR OWN RISK.

NO LIABILITY: IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE IN CONNECTION WITH OR ARISING OUT OF THE USE OF THE OLSS (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA, OR OTHER ECONOMIC ADVANTAGE) HOWEVER IT ARISES, WHETHER FOR BREACH OR IN TORT, EVEN IF ORACLE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Acknowledged by Jane Doe

\*\*\*\* Welcome to the Oracle Linux 8 STIG tool \*\*\*\*

This tool has two primary modes: Secure and Verify  
Throughout this tool the answers in [] are the expected responses

OLSS will be running in Verify mode - via command line switch

We are running in this environment: oda

## About STIG Exceptions on Oracle Database Appliance

Understand the reasons for Security Technical Implementation Guidelines (STIG) exceptions.

Some failures found by OLSS cannot be fixed. Some of the reasons are:

- The requested fix may remove required functionality.
- Fixing the issue may lead to system errors.
- The architecture of Oracle Database Appliance may not support the requested change.

These types of failures are called exceptions.

Following are the Security Technical Implementation Guidelines (STIG) exceptions in this release and the reason for the specific Oracle Linux 8 STIG ID not being fixed on Oracle Database Appliance:

**Table 2-2 STIG exceptions**

STIG ID	Severity	Reason for Exception
OL8-00-010030	High	Oracle Database Appliance architecture does not support Linux Unified Key Setup (LUKS) encryption. In addition, supporting encryption would require an encryption key to be provided at system start-up which would prevent the system from restarting automatically.
OL8-00-010010	Medium	Oracle Database Appliance is an appliance and Oracle releases updates every quarter for the Oracle Database Appliance software. This includes the latest security updates. The server patches that Oracle Database Appliance provides ensures smooth patching of the appliance. Any additional RPMs installed or RPMs updated out of order can cause an error in the Oracle Database Appliance patching process.
OL8-00-010010	Medium	The users created, when an Oracle Database Appliance system is configured, do not use certificate-based authentication. These accounts must not be configured so. If they are modified as such, it may result in failures on the system.

Table 2-2 (Cont.) STIG exceptions

STIG ID	Severity	Reason for Exception
OL8-00-010340	Medium	Directories under /usr/lib64/.build-id are links to shared libraries of installed software. The application of this rule can cause Oracle Database Appliance-installed software to fail, for example, MySQL. The correct working of this component is crucial for the Oracle Database Appliance stack.
OL8-00-040134	Medium	Oracle Database Appliance architecture does not support mounting the /var/tmp directory as a separate file system.
OL8-00-040133	Medium	Oracle Database Appliance architecture does not support mounting the /var/tmp directory as a separate file system.
OL8-00-010590	Medium	Oracle Database Appliance architecture does not support mounting the /home directory as a separate file system.
OL8-00-030660	Medium	Oracle Database Appliance architecture does not support mounting the /var/audit directory as a separate file system.
OL8-00-010570	Medium	Oracle Database Appliance architecture does not support mounting the /home directory as a separate file system.
OL8-00-040132	Medium	Oracle Database Appliance architecture does not support mounting the /var/tmp directory as a separate file system.
OL8-00-040128	Medium	Oracle Database Appliance architecture does not support mounting the /var/log directory as a separate file system.
OL8-00-040125	Medium	Oracle Database Appliance architecture does not support mounting the /tmp directory as a separate file system.
OL8-00-010380	Medium	The application of this rule can cause failures on the appliance. One example is Oracle HAMI which runs commands through privilege escalation.

Table 2-2 (Cont.) STIG exceptions

STIG ID	Severity	Reason for Exception
OL8-00-010472	Low	The RPM <code>rng-tools</code> package is not installed on Oracle Database Appliance, as it is not required. If you install the RPM, you must uninstall it before patching Oracle Database Appliance to a later release because it can cause an error in the Oracle Database Appliance patching process.
OL8-00-010541	Low	Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-010543	Medium	Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-010550	Medium	Oracle Database Appliance systems are configured for direct login as root. If this is not allowed, it can cause the system to function incorrectly.
OL8-00-010700	Medium	Modifying the ownership of any Oracle Database Appliance installed software directory results in one or more software components to stop working.
OL8-00-010731	Medium	The Oracle Database Appliance user <code>hamictl_oda_dcs</code> may fail if this rule is applied and can be ignored.
OL8-00-010800	Medium	Any change in any current file system size may result in an out-of-space error on the Oracle Database Appliance.
OL8-00-020320	Medium	The system administrator must check the Oracle Database Appliance system for any accounts that were created manually. They must not delete any of the accounts created when the Oracle Database Appliance system is setup.
OL8-00-020351	Medium	It can cause the Oracle Grid Infrastructure and Oracle Database software to be installed with incorrect permissions, which can result in patching failures.
OL8-00-020352	Medium	It can cause the Oracle Grid Infrastructure and Oracle Database software to be installed with incorrect permissions, which can result in patching failures.

Table 2-2 (Cont.) STIG exceptions

STIG ID	Severity	Reason for Exception
OL8-00-020353	Medium	It can cause the Oracle Grid Infrastructure and Oracle Database software to be installed with incorrect permissions, which can result in patching failures.
OL8-00-040030	Medium	firewalld is installed on Oracle Database Appliance but has not been configured. Configuring the same may result in the malfunction of Oracle Database Appliance. If the system administrator remediates this STIG, they must be ready to roll back any changes made.
OL8-00-040124	Medium	Creating a separate file system may result in an error because of lack of space on Oracle Database Appliance. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040127	Medium	Creating a separate file system may result in an error because of lack of space on Oracle Database Appliance. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040130	Medium	Creating a separate file system may result in an error because of lack of space on Oracle Database Appliance. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040135	Medium	The RPM <code>fapolicy</code> package is not installed on Oracle Database Appliance, as it is not required. If you install the RPM, you must uninstall it before patching Oracle Database Appliance to a later release.
OL8-00-040370	Medium	Removal of the <code>gssproxy</code> package deletes dependant packages such as NFS which are required for the working of the Oracle Database Appliance software.

Table 2-2 (Cont.) STIG exceptions

STIG ID	Severity	Reason for Exception
OL8-00-010020	High	Earlier releases of the Oracle Database Appliance software did not create a required Linux configuration parameter when creating or patching a DB system.  This is being tracked by Oracle Database Appliance bugs 36999977 and 37058085.
OL8-00-010170	Medium	It is not recommended to remediate this STIG. Enabling SELinux on Oracle Database Appliance system results in performance degradation of the system.
OL8-00-010358	Medium	The RPM mailx package is not installed on Oracle Database Appliance, as it was not required. If the customer installs the rpm, they will be required to uninstall it, before patching the Oracle Database Appliance to a higher version,
OL8-00-010410	Medium	The RPM opensc package is not installed on Oracle Database Appliance, as it was not required. If the customer installs the rpm, they will be required to uninstall it, before patching the Oracle Database Appliance to a higher version,
OL8-00-010450	Medium	It is not recommended to remediate this STIG. Enabling selinux on an Oracle Database Appliance system will result in performance degradation of the system.
OL8-00-010540	Low	You must not try to create a separate file system. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-010542	Low	You must not try to create a separate file system. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.



Table 2-2 (Cont.) STIG exceptions

STIG ID	Severity	Reason for Exception
OL8-00-010544	Medium	You must not try to create a separate file system. Any change in any current file system size may result in an out-of-space error on Oracle Database Appliance.
OL8-00-010690	Medium	The Oracle Database Appliance created users on the system have few setting in the bash profiles setup. Remediating this STIG can result in the PATH variable to be modified. To run commands, you must then provide the full path to the script.
OL8-00-010710	Medium	Modifying the ownership of any Oracle Database Appliance installed software directory, will result in one or more software components to stop working.
OL8-00-010770	Medium	The Oracle Database Appliance user hamictl_oda_dcs may fail for this STIG and can be ignored.
OL8-00-020039	Medium	The RPM <code>tmux</code> package is not installed on Oracle Database Appliance, as it was not required. If you install the RPM, you must uninstall it before patching Oracle Database Appliance to a later release.
OL8-00-040123	Medium	You must not try to create a separate file system. Any change in any current file system size, may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040126	Medium	You must not try to create a separate file system. Any change in any current file system size, may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040129	Medium	You must not try to create a separate file system. Any change in any current file system size, may result in an out-of-space error on Oracle Database Appliance.
OL8-00-040131	Medium	You must not try to create a separate file system. Any change in any current file system size, may result in an out-of-space error on Oracle Database Appliance.

**Table 2-2 (Cont.) STIG exceptions**

STIG ID	Severity	Reason for Exception
OL8-00-040320	Medium	The system administrator must not uninstall the graphical display manager software/RPMs. This is required for the correct functioning of Oracle Database Appliance.
OL8-00-040400	Medium	The system administrator must not prevent Oracle Database Appliance created users from running privileged functions. This is required for the correct functioning of Oracle Database Appliance.

## About Security Content Automation Protocol (SCAP) Findings

Security Content Automation Protocol (SCAP) describes the STIG checks which can be performed in automated manner. To ensure compliance with STIG, a scan is performed periodically on Oracle Database Appliance to determine how compliant it is with the protocol. The current compliance rate is 91%.

For various reasons, it is not possible to comply with all of the STIG requirements. The following table lists the requirements with which the Oracle Database Appliance is not in compliance and the reason for each.

**Table 2-3 SCAP findings**

Finding	Severity	Oracle Linux ID	Explanation
V-248537	High	OL08-00-010140	Not supported for unattended operation.
V-248548	Medium	OL08-00-010170	Oracle Database Appliance does not support SELinux in enforcing mode.
V-248581	Medium	OL08-00-010380	Oracle Database Appliance requires this functionality for proper operation.
V-248611	Medium	OL08-00-010543	Oracle Database Appliance architecture does not support using a separate file system.
V-248612	Medium	OL08-00-010544	Oracle Database Appliance architecture does not support using a separate file system.
V-248613	Medium	OL08-00-010550	SSH logins as root are required for Oracle Database Appliance functionality.

Table 2-3 (Cont.) SCAP findings

Finding	Severity	Oracle Linux ID	Explanation
V-248616	Medium	OL08-00-010570	Required for database operation.
V-248645	Medium	OL08-00-010770	Oracle Database Appliance requires this functionality for proper operation.
V-248648	Medium	OL08-00-010800	The Oracle Database Appliance architecture does not support using a separate file system.
V-248697	Medium	OL08-00-020210	Oracle Database Appliance does not currently support this functionality.
V-248719	Medium	OL08-00-020351	umask 077 is not recommended for Oracle use.
V-248841	Medium	OL08-00-040101	A firewall using iptables between nodes is not permitted. A network filter between nodes using virsh is enabled. A firewall for connections outside of the appliance may be configured by the user.
V-248859	Medium	OL08-00-040135	This facility is not currently supported by Oracle Database Appliance.
V-248860	Medium	OL08-00-040136	This facility is not currently supported by Oracle Database Appliance.
V-248862	Medium	OL08-00-040139	Not supported by Oracle Database Appliance architecture.
V-248864	Medium	OL08-00-040141	Not supported by Oracle Database Appliance architecture.
V-248890	Medium	OL08-00-040282	Oracle Database Appliance requires this functionality for proper operation.
V-248898	Medium	OL08-00-040320	Not supported by the Oracle Database Appliance architecture.
V-248904	Medium	OL08-00-040370	Oracle Database Appliance requires this functionality for proper operation.

Table 2-3 (Cont.) SCAP findings

Finding	Severity	Oracle Linux ID	Explanation
V-257259	Medium	OL08-00-020035	Oracle Database Appliance requires this functionality for proper operation.
V-248608	Medium	OL08-00-010540	Oracle Database Appliance architecture does not support using a separate file system.
V-248609	Medium	OL08-00-010541	Oracle Database Appliance architecture does not support using a separate file system.
V-248610	Medium	OL08-00-010542	Oracle Database Appliance architecture does not support using a separate file system.

## Using Oracle ILOM for Secure Management

Oracle Integrated Lights-Out Management (Oracle ILOM) enables full out-of-band management, providing remote management capability for Oracle Database Appliance.

IPMI v2.0 and Collections of security controls and capabilities are necessary to properly secure individual applications and services. It is equally important to have comprehensive management capabilities to sustain the security of the deployed services and systems. Oracle Database Appliance uses the security management capabilities of Oracle ILOM.

Oracle ILOM is a service processor embedded in many Oracle Database Appliance components to perform out-of-band management activities. Oracle ILOM provides the following features:

- Secure access to perform secure lights-out management of the database and storage servers. Access includes web-based access protected by Transport Layer Security (TLS), command-line access using Secure Shell, and SNMPv3 protocols.
- Separate duty requirements using a role-based access control model. Individual users are assigned to specific roles that limit the functions that can be performed.
- An audit record of all logins and configuration changes. Each audit log entry lists the user performing the action, and a timestamp. This allows organizations to detect unauthorized activity or changes, and attribute those actions back to specific users.

# 3

## Planning a Secure Environment

Determine security practices that you want to deploy before your Oracle Database Appliance is delivered.

After deployment, review your security practices periodically, and adjust them as needed to stay current with the security requirements of your organization.

Topics:

- [Considerations for a Secure Environment](#)  
Plan to integrate Oracle Database Appliance identity and access management security features with your existing organization security protocols.
- [Understanding User Accounts](#)  
Review the information in this topic to understand default user account information for Oracle Database Appliance deployments.
- [Understanding the Default Security Settings](#)  
Oracle Database Appliance is installed with many default security settings and methods.

## Considerations for a Secure Environment

Plan to integrate Oracle Database Appliance identity and access management security features with your existing organization security protocols.

Oracle Database Appliance includes many layered security controls that can be tailored to meet an organization's specific policies and requirements. Organizations must evaluate how to best utilize these capabilities and integrate them into their existing IT security architecture. Effective IT security must consider the people, processes, and technology in order to provide solid risk management and governance practices. Practices and policies should be designed and reviewed during the planning, installation, and deployment stages of Oracle Database Appliance.

A unified approach to identity and access management should be used when integrating Oracle Database Appliance components, and deployed services with an organization's existing identity and access management architecture. Oracle Database supports many open and standard protocols that allow it to be integrated with existing identity and access management deployments. To ensure application availability, unified identity and access management systems must be available, or the availability of Oracle Database Appliance may be compromised.

Before Oracle Database Appliance arrives, the following security considerations should be discussed. These considerations are based on Oracle best practices for Oracle Database Appliance.

- The use of intrusion prevention systems on database servers to monitor network traffic flowing to and from Oracle Database Appliance. Such systems enable the identification of suspicious communications, potential attack patterns, and unauthorized access attempts.
- The use of host-based intrusion detection and prevention systems for increased visibility within Oracle Database Appliance. By using the fine-grained auditing capabilities of Oracle Database, host-based systems have a greater likelihood of detecting inappropriate actions and unauthorized activity.

- The use of application and network-layer firewalls to protect information flowing to and from Oracle Database Appliance. Filtering network ports provides the first line of defense in preventing unauthorized access to systems and services.

Network-level segmentation using Ethernet virtual local area networks (VLANs) and host-based firewalls enforce inbound and outbound network policy at the host level. Using segmentation allows fine-grained control of communications between components of Oracle Database Appliance. Oracle Database Appliance can be configured with a software firewall.

- The use of encryption features such as Transparent Data Encryption (TDE), Oracle Recovery Manager (RMAN) encryption for backups, and Oracle Advanced Security to encrypt traffic to Oracle Data Guard standby databases.

While many of the features integrated into Oracle Database Appliance are configured by default for secure deployment, organizations have their own security configuration standards. It is important to review Oracle security information before testing any security setting changes to Oracle Database Appliance components. In particular, it is important to identify where existing standards can be improved, and where support issues may limit what changes can be made to a given component.

The security of the data and system is diminished by weak network security. Oracle recommends the following guidelines to maximize your Ethernet network security:

- Configure administrative and operational services to use encryption protocols and key lengths that align with current policies. Cryptographic services provided by Oracle Database Appliance benefit from hardware acceleration, which improves security without impacting performance.
- Manage and separate switches in Oracle Database Appliance from data traffic on the network. This separation is also referred to as "out-of-band."
- Separate sensitive clusters of the system from the rest of the network when using virtual local area networks (VLANs). This decreases the likelihood that users can gain access to information on these clients and servers.
- Use a static VLAN configuration.
- Disable unused switch ports, and assign an unused VLAN number.
- Assign a unique native VLAN number to trunk ports.
- Limit the VLANs that can be transported over a trunk to only those that are strictly required.
- Disable VLAN Trunking Protocol (VTP), if possible. If it is not possible, then set the management domain, password and pruning for VTP. In addition, set VTP to transparent mode.
- Disable unnecessary network services, such as TCP small servers or HTTP. Enable only necessary network services, and configure these services securely.
- Network switches offer different levels of port security features. Use these port security features if they are available:
- Lock the Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If a switch port is locked to a particular MAC address, then super users cannot create back doors into the network with rogue access points.
- Disable a specified MAC address from connecting to a switch.
- Use each switch port's direct connections so the switch can set security based on its current connections.

## Understanding User Accounts

Review the information in this topic to understand default user account information for Oracle Database Appliance deployments.

The following table lists the default users for the Oracle Database Appliance components.

### **Caution**

You must change all default passwords after deploying Oracle Database Appliance.

**Table 3-1 Default User Names for User Accounts**

Component	User Name
Oracle Database Appliance servers	<ul style="list-style-type: none"><li>• root</li><li>• oracle</li><li>• grid</li><li>• odaadmin</li></ul>
Oracle Databases	<ul style="list-style-type: none"><li>• sys</li><li>• system</li><li>• dbstmp</li></ul> <p>For more information about database users, see the <i>Oracle Database Security Guide</i>.</p>

## Understanding the Default Security Settings

Oracle Database Appliance is installed with many default security settings and methods.

Whenever possible and practical, you should select secure default settings.

### Security Settings Deployed by Default on Oracle Database Appliance

Default security methods and settings include the following:

- A minimal software installation to reduce attack surface.
- Oracle Database secure settings developed and implemented using Oracle best practices.
- A password policy that enforces a minimum password complexity.
- Failed log in attempts cause a lockout after a set number of failed attempts.
- All default system accounts in the operating system are locked and prohibited from logging in.
- Restrictive file permissions on key security-related configuration files and executable files.
- SSH listening ports restricted to management and private networks.
- SSH limited to v2 protocol.
- Disabled insecure SSH authentication mechanisms.
- Configured specific cryptographic ciphers.
- Unnecessary protocols and modules are disabled from the operating system kernel.





# 4

## Keeping Oracle Database Appliance Secure

Use the policies and procedures described in this chapter to keep Oracle Database Appliance secure.

Topics:

- [Securing the Hardware](#)  
Oracle recommends that you implement the security policies described here to restrict access to the hardware.
- [Securing the Software](#)  
Review and implement security features and policies for your appliance software.
- [Configuring a Third-Party Certificate for Oracle Database Appliance](#)  
The Browser User Interface and DCS Controller use SSL-based HTTPS protocol for secure communication. Understand the implications of this added security and the options to configure SSL certificates.
- [Maintaining a Secure Environment](#)  
After you implement security policies and methods on your appliance, review these topics to understand how to maintain a secure environment.

### Securing the Hardware

Oracle recommends that you implement the security policies described here to restrict access to the hardware.

After installation of Oracle Database Appliance, secure the hardware.

#### Hardware Security Methods and Procedures

- Install Oracle Database Appliance and related equipment in a locked, restricted-access room.
- Restrict access to hot-pluggable or hot-swappable devices because the components can be easily removed by design.
- Limit SSH listener ports to the management and private networks.
- Limit allowed SSH authentication mechanisms. By default, inherently insecure SSH authentication methods are disabled.
- Mark all significant items of computer hardware, such as FRUs.
- Record the serial numbers of the components of Oracle Database Appliance, and keep a record in a secure place. All components of Oracle Database Appliance have a serial number.

# Securing the Software

Review and implement security features and policies for your appliance software.

## Oracle Database Appliance Operating System and Server Security Policies

- Change all default passwords when the system is installed at the site.  
Oracle Database Appliance uses default passwords for initial installation and deployment that are widely known. A default password that is still in effect could allow unauthorized access to the equipment. Devices such as the network switches have multiple user accounts. Be sure to change all account passwords on the components in the rack.
- Create and use Oracle Integrated Lights Out Manager (ILOM) user accounts for individual users  
Using ILOM user accounts ensures a positive identification in audit trails, and results in less maintenance when administrators leave the team or company.
- Restrict physical access to USB ports, network ports, and system consoles.  
Servers and network switches have ports and console connections, which provide direct access to the system.
- Restrict the capability to restart the system over the network.
- Enable available database security features, as described in *Oracle Database Security Guide*.

## Oracle Database Security Features

Oracle Database Appliance can leverage all the security features available with Oracle Databases installed on legacy platforms. Oracle Database security products and features include the following:

- Oracle Advanced Security
- Data Masking
- Oracle Database Firewall
- Oracle Database Vault
- Oracle Label Security
- Oracle Secure Backup
- Oracle Total Recall
- Oracle Audit Vault. Note that Oracle Audit Vault may not be configured to run on Oracle Database Appliance directly. Instead, Oracle Database Appliance may be configured to use an instance of Oracle Audit Vault that runs on a separate server.

Using the Oracle privileged user and multi-factor access control, data classification, transparent data encryption, auditing, monitoring, and data masking, customers can deploy reliable data security solutions that do not require any changes to existing applications.

Oracle Database Appliance supports creation of TDE-enabled databases, with TDE keys stored on Oracle Database Appliance or on Oracle Key Vault. For more information, see the topic *About Transparent Database Encryption (TDE) in Oracle Database Appliance* in the *Oracle Database Appliance Deployment and User's Guide* for your hardware model.

**Related Topics**

- About Transparent Database Encryption (TDE) in Oracle Database Appliance

## Configuring a Third-Party Certificate for Oracle Database Appliance

The Browser User Interface and DCS Controller use SSL-based HTTPS protocol for secure communication. Understand the implications of this added security and the options to configure SSL certificates.

The Browser User Interface provides an added layer of security using certificates and encryption, when an administrator interacts with the appliance. The use of certificates and encryption ensures that:

- Data is sent to the intended recipient, and not to any malicious third-party.
- When data is exchanged between the server and the browser, data interception cannot occur nor can the data be edited.

When you connect to the Browser User Interface through HTTPS, the DCS Controller presents your browser with a certificate to verify the identity of appliance. If the web browser finds that the certificate is not from a trusted Certificate Authority (CA), then the browser assumes it has encountered an untrusted source, and generates a security alert message. The security alert dialog boxes display because Browser User Interface security is enabled through HTTPS and SSL, but you have not secured your Web tier properly with a trusted matching certificate from a Certificate Authority. To avoid this warning, you can purchase a trusted certificate from a Certificate Authority.

To configure your certificate, create your own key and Java keystore, ensure it is signed by a Certificate Authority (CA) and then import it for use.

**Note**

For Oracle Database Appliance High-Availability hardware models, run the configuration steps on **both** nodes.

- [Creating a Key and Java Keystore and Importing a Trusted Certificate](#)  
Use `keytool`, a key and certificate management utility, to create a keystore and a signing request.
- [Configuring the DCS Server to Use Custom Keystore](#)  
After packaging or converting your keystore into Java keystore, configure the DCS server to use your keystore.
- [Configuring the DCS Agent To Use a Custom Certificate](#)  
After you import the certificate into the keystore, configure the DCS agent to use the same certificate.

## Creating a Key and Java Keystore and Importing a Trusted Certificate

Use `keytool`, a key and certificate management utility, to create a keystore and a signing request.

**1. Create the keystore:**

```
keytool -genkeypair -alias your.domain.com -storetype jks -keystore  
your.domain.com.jks -validity 366 -keyalg RSA -keysize 4096
```

**2. The command prompts you for identifying data:**

1. What is your first and last name? *your.domain.com*
2. What is the name of your organizational unit? *yourunit*
3. What is the name of your organization? *yourorg*
4. What is the name of your City or Locality? *yourcity*
5. What is the name of your State or Province? *yourstate*
6. What is the two-letter country code for this unit? *US*

**3. Create the certificate signing request (CSR):**

```
keytool -certreq -alias your.domain.com -file your.domain.com.csr  
-keystore your.domain.com.jks -ext san=dns:your.domain.com
```

**4. Request a Certificate Authority (CA) signed certificate:**

- a. In the directory where you ran Step 1 above, locate the file *your.domain.com.csr*.
- b. Submit the file to your Certificate Authority (CA).

Details vary from one CA to another. Typically, you submit your request through a website. Then the CA contacts you to verify your identity. CAs can send signed reply files in a variety of formats, and CAs use a variety of names for those formats. The CA's reply must be in PEM, PKCS#7, or P7B format.

- c. There may be a waiting period for the CA's reply.

**5. Import the CA's reply. The CA's reply will provide one PKCS file, or P7B file, or multiple PEM files.**

- a. Copy the CA's files into the directory where you created the keystore in Step 1 above.
- b. Use `keytool` to import the keystore certificate and the CA reply files:
  - i. To import the P7B file, run the command:

```
keytool -importcert -alias your.domain.com -file CAreply.p7b -  
keystore your.domain.name.jks -trustcacerts
```

- ii. Migrate to PKCS12 (P7B), an industry standard format:

```
keytool -importkeystore -srckeystore your.domain.name.jks -  
destkeystore your.domain.name.jks -deststoretype pkcs12
```

- iii. To import the PKCS12 (P7B) signed certificate file, that is stored in JKS file, to `dcs-ca-certs` file, run the command:

```
keytool -importkeystore -srckeystore your.domain.name.jks -  
destkeystore /opt/oracle/dcs/conf/dcs-ca-certs -deststoretype pkcs12
```

- c. To import the PKCS file, run the command:

```
keytool -importcert -trustcacerts -alias your.domain.com -file  
CAreply.pkcs -keystore /opt/oracle/dcs/conf/dcs-ca-certs
```

*CAreply.pkcs* is the name of the PKCS file provided by the CA and *your.domain.com* is the complete domain name of your server.

If the CA sent PEM files, then there may be one file, but most often there are two or three. Import the files to your keystore with commands in the order shown below, after substituting your values:

```
keytool -importcert -alias root -file root.cert.pem -keystore /opt/oracle/dcs/conf/dcs-ca-certs -trustcacerts
keytool -importcert -alias intermediate -file intermediate.cert.pem -keystore /opt/oracle/dcs/conf/dcs-ca-certs -trustcacerts
keytool -importcert -alias intermediat2 -file intermediat2.cert.pem -keystore /opt/oracle/dcs/conf/dcs-ca-certs -trustcacerts
keytool -importcert -alias your.domain.com -file server.cert.pem -keystore /opt/oracle/dcs/conf/dcs-ca-certs -trustcacerts
```

*root.cert.pem* is the name of the root certificate file and *intermediate.cert.pem* is the name of the intermediate certificate file. The root and intermediate files link the CA's signature to a widely trusted root certificate that is known to web browsers. Most, but not all, CA replies include roots and intermediates. *server.cert.pem* is the name of the server certificate file. The file links your domain name with your public key and the CA's signature.

## Configuring the DCS Server to Use Custom Keystore

After packaging or converting your keystore into Java keystore, configure the DCS server to use your keystore.

1. Login to the appliance.

```
ssh -l root oda-host-name
```

2. Generate the obfuscated keystore password:

```
/opt/oracle/dcs/java/java_version/bin/java -cp /opt/oracle/dcs/bin/dcs-controller-n.n.n.n.jar com.oracle.oda.dcs.password.utils.OBFCredentials keystore-password
```

For example:

```
# /opt/oracle/dcs/java/java_version/bin/java -cp /opt/oracle/dcs/bin/dcs-controller-19.28.0.0.jar
com.oracle.oda.dcs.password.utils.OBFCredentials test
OBF:"1z0f1vu91vv11z0f"
```

Copy the obfuscated password that starts with OBF:.

3. Update the following in */opt/oracle/dcs/conf/dcs-controller.yml*:

```
ssl:
  key-store:
    path: file:/opt/oracle/dcs/conf/your.domain.com.jks
    type: "JKS"
    password: "obfuscated keystorepassword"
```

```
trust-store:
  path: file:/opt/oracle/dcs/conf/dcs-ca-certs
key:
  alias: "your.domain.com"
```

4. Restart the DCS controller.

```
systemctl stop initdcscontroller
systemctl start initdcscontroller
```

The DCS controller log file `/opt/oracle/dcs/log/dcs-controller.log` displays the following lines:

```
2022-05-13 04:23:37,266 INFO [main] [] c.o.o.c.DCSControllerSSLConfig:
Custom keystore password is set
2022-05-13 04:23:37,266 INFO [main] [] c.o.o.c.DCSControllerSSLConfig:
Custom truststore password is set
```

5. Access the Browser User Interface at `https://oda-host-name:7093/mgmt/index.html`.

## Configuring the DCS Agent To Use a Custom Certificate

After you import the certificate into the keystore, configure the DCS agent to use the same certificate.

1. Update the DCS agent configuration file:

```
cd /opt/oracle/dcs/conf
```

Update the following parameters in the `dcs-agent.yml` file:

```
dcs:
  config:
    secondary-server:
      ssl:
        key-store: file:/opt/oracle/dcs/conf/your.domain.com.jks
        type: "JKS"
        trust-store: file:/opt/oracle/dcs/conf/dcs-ca-cacerts
        alias: "your.domain.com"
        password: "obfuscated keystorepassword"
```

2. Restart the DCS agent:

```
systemctl stop initdcsagent
systemctl start initdcsagent
```

3. Access the agent at `https://oda-host-name:7070`.
4. Update the CLI certificates.

```
cp -f /opt/oracle/dcs/conf/dcs-ca-certs /opt/oracle/dcs/dcscli/dcs-ca-certs
```

5. Update the DCS command-line configuration files:

```
[root@]# cd /opt/oracle/dcs/dcscli
```

Update the following parameters in `dcsccli-adm.conf` and `dcsccli.conf`:

```
TrustStorePath=/opt/oracle/dcs/dcscli/dcs-ca-certs
TrustStorePassword=keystore_password
```

## Maintaining a Secure Environment

After you implement security policies and methods on your appliance, review these topics to understand how to maintain a secure environment.

Topics:

- [About Secure Environments](#)  
Oracle recommends that you review and update your operational and administrative access policies regularly to maintain a secure environment.
- [Maintaining Network Security](#)  
After the networks are configured based on the security guidelines, carry out regular review and maintenance to ensure that secure host and ILOM settings remain intact and in effect.
- [Updating Software and Firmware](#)  
Oracle regularly introduces security enhancements in new releases and patch sets.
- [Ensuring Data Security Outside of Oracle Database Appliance](#)  
Follow security practices when you back up your data to external storage.

## About Secure Environments

Oracle recommends that you review and update your operational and administrative access policies regularly to maintain a secure environment.

After you implement security policies and features for your system, Oracle recommends that your organization establishes a security review policy. As part of your security policy, periodically update and review your software, hardware, and user access.

For example, check all users and administrators granted access to Oracle Database Appliance, and to its deployed services. Verify if the levels of access and privilege that you have granted to users and administrators remains appropriate.

Without regular security reviews, the level of access granted to individuals could increase unintentionally, due to role changes, or due to changes to default settings. Oracle recommends that you review access rights for operational and administrative tasks regularly. Regular reviews can help to ensure that user level of access remains aligned to the roles and responsibilities for each user.

## Maintaining Network Security

After the networks are configured based on the security guidelines, carry out regular review and maintenance to ensure that secure host and ILOM settings remain intact and in effect.

Follow these guidelines to ensure the security of local and remote access to the system:

- Manage the management network switch configuration file offline, and limit access to the file to only authorized administrators.
- Add descriptive comments for each setting in the configuration file. Consider keeping a static copy of the configuration file in a source code control system.
- Use access control lists to apply restrictions where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use authentication, authorization, and accounting (AAA) features for local and remote access to a switch.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports for any switch connected to Oracle Database Appliance.
- Limit remote configuration to specific IP addresses using SSH.
- Require users to use strong passwords by setting minimum password complexity rules and password expiration policies.
- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Review logs for possible incidents and archive them in accordance with the organization's security policy.

## Updating Software and Firmware

Oracle regularly introduces security enhancements in new releases and patch sets.

Effective proactive patch management is a critical part of system security. Oracle recommends that you install the latest release of the software, and install all necessary security patches on the equipment.

To establish baseline security, Oracle recommends that you apply only Oracle-recommended software and security patches

## Ensuring Data Security Outside of Oracle Database Appliance

Follow security practices when you back up your data to external storage.

Ensure that you back up your data to external storage. Oracle recommends that you store backups in an off-site, secure location. Retain the backups according to your organizational policies and requirements.

When you dispose of old disk drives, physically destroy the drive, or completely erase all the data on the drive. Deleting the files or reformatting the disk drive removes only the address tables on the drive. The information can still be recovered from a disk drive after deleting files or reformatting the drive. If you want to retain replaced disk drives and flash drives, instead of returning them to Oracle, then you can use the Oracle Database Appliance disk retention support option.



# Index

## A

---

access policies, [7](#)  
accessing ILOMs, [26](#)  
accountability, [4](#)  
accounting, [1](#)  
auditing, [1](#)  
authentication, [1](#)  
authorization, [1](#)

## C

---

ciphers, [1](#)  
classification strategies, [7](#)  
classifying data, [7](#)  
client access  
    isolating, [6](#)  
Common Vulnerabilities and Exposures (CVEs), [3](#)  
cryptographic services, [10](#)

## D

---

default passwords, [3](#)  
disposing old hard drives, [8](#)

## E

---

encrypting  
    backups, [1](#)  
    JDBC traffic, [10](#)  
    Oracle Net Services, [10](#)  
    traffic, [1](#)  
Ethernet security guidelines, [1](#)  
event accountability, [4](#)

## F

---

FIPs, [12](#)  
FIPS 140-2, [1](#)

## H

---

hardening, [1](#)

## I

---

ILOM, [10](#)  
ILOM (Integrated Lights Out Manager), [10](#)  
Intel AES-NI, [10](#)  
IPMI v2.0, [26](#)  
isolating  
    client access, [6](#)  
    management access, [6](#)  
    multiple databases, [7](#)

## K

---

Kerberos, [8](#)  
key credentials, [8](#)

## L

---

LDAP repositories, [8](#)  
logical realms, [7](#)

## M

---

MAC address, [1](#)  
management access  
    isolating, [6](#)  
monitoring user logins, [1](#)

## O

---

Oracle Advanced Security  
    cryptographic services, [10](#)  
    encrypting traffic, [1](#)  
    using public keys, [8](#)  
Oracle Audit Vault  
    enabling proactive detection, [11](#)  
Oracle Data Guard, [1](#)  
Oracle Database Firewall Remote Monitor, [11](#)  
Oracle Database security products, [2](#)  
Oracle Database Vault  
    managing access, [8](#)  
    mandatory access control, [7](#)  
Oracle Enterprise User Security, [8](#)  
Oracle ILOM (Oracle Integrated Lights Out Manager), [26](#)

Oracle Label Security, [7](#)  
Oracle Recovery Manager (RMAN), [1](#)  
Oracle Virtual Private Database, [7](#)  
out-of-band, [1](#)

## P

---

password policy, [3](#)

## R

---

RADIUS, [8](#)  
restrict binaries, [4](#)  
restrictive file permissions, [3](#)  
RMAN (Oracle Recovery Manager)  
    encrypting backups, [1](#)  
row level isolation, [7](#)

## S

---

secure boot, [4](#), [5](#)  
secure isolation levels, [6](#)

securing communications, [10](#)  
security considerations, [1](#)  
SELinux, [2](#)  
separation of duties, [8](#)  
serial numbers, [1](#)  
SNMPv3, [26](#)  
SSH (Secure Shell), [10](#), [26](#), [1](#)  
SSH (Secure Shell): default protocol limit, [3](#)  
SSH protocol 2 (SSH2), [1](#)  
SSL/TLS, [10](#)  
STIG, [12](#), [16](#), [18](#), [24](#)

## T

---

TDE (Transparent Data Encryption), [10](#), [1](#)  
tracking hardware assets, [1](#)

## V

---

VLANs (virtual local area networks), [6](#), [1](#)  
VTP (VLAN Trunking Protocol), [1](#)