Oracle® Database Appliance

Security Guide

Release 19.19
F78637-01
May 2023

Oracle Database Appliance Security Guide, Release 19.19

F78637-01

Contents

Preface

Audience v
Documentation Accessibility v
Related Documents v
Conventions vi

1 Overview of Oracle Database Appliance Security

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

2 Security Features of Oracle Database Appliance

About Oracle Database Appliance Security Features 2-1
About Multi-User Access for Oracle Database Appliance Security 2-2
Using Isolation Policies 2-3
- Isolating Network Traffic 2-3
- Isolating Databases 2-3

Controlling Access to Data 2-4
- Controlling Network Access 2-4
- Controlling Database Access 2-5
- About Managing Privileges and Security with SUDO 2-5
- Configuring a SUDO Security Policy for the DCS Stack 2-6

Using Cryptographic Services 2-7
Monitoring and Auditing of Databases on Oracle Database Appliance 2-8
About FIPS 140-2 Compliance on Oracle Database Appliance 2-9
Checking for STIG Compliance on Oracle Database Appliance 2-9
About Enabling CIS Benchmarks on Oracle Database Appliance 2-14
Using Oracle ILOM for Secure Management 2-16

3 Planning a Secure Environment

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

4 Keeping Oracle Database Appliance Secure

Securing the Hardware 4-1
Securing the Software 4-1
Maintaining a Secure Environment 4-2
- About Secure Environments 4-3
- Maintaining Network Security 4-3
- Updating Software and Firmware 4-4
- Ensuring Data Security Outside of Oracle Database Appliance 4-4

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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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/.

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
boldface	Boldface type indicates graphical user interface elements associated with an action, emphasis, or terms defined in text or the glossary.
italic	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 the `oracle` user.
`#` prompt	The pound (`#`) prompt indicates a command that is run as the `root` 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/execute 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.

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.

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 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.
- 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.
- 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 Enabling CIS Benchmarks on Oracle Database Appliance
  Understand how you can enable Center for Internet Security (CIS) Benchmarks for Oracle Database Appliance.
- 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.

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 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.

> **See Also:**
>
> *Oracle Database Appliance Deployment and User's Guide* for your hardware model.

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.
##
Cmnd_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: oda1001
            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 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.

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 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 provides support for Oracle Linux 7 Security Scripts (OLSS) to assist with documenting and aligning with the DISA Oracle Linux 7 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 the STIG script 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 the STIG script:

1. Log in as `root` user.

2. Run the command from the `/opt/oracle/dcs/stig` directory:

```
[root@oda1 stig]# ./RunSTIG
```

The summary and detailed logs are in the `/opt/oracle/dcs/stig/04_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 execution of 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

```
$ ./RunSTIG

Initializing tests.....

******** WARNING    WARNING    WARNING    WARNING    WARNING *********
```

```
                    Oracle Linux 7 Security Scripts The Oracle Linux
Security Scripts (OLSS) are a tool designed to assist in creation and
deployment of secured Oracle Linux 7 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

  **** Welcome to the Oracle Linux 7 STIG tool ****

This tool has two primary modes: Secure or Verify

Throughout this tool the answers in [] are the expected responses

Did you want to Secure or Verify? [Secure|Verify]:

**********************
When 'Verify' is chosen:
**********************
Did you want to Secure or Verify? [Secure|Verify]: Verify
Responded: Verify

Is "Verify" correct? (y/n): y
Responded: y

Oracle Linux 7 Security Scripts have 4 flavors:

1) SCAP             - The 177 DISA SCAP checks

2) Exadata or ZDLRA - The 177 DISA SCAP checks with the special
                      host_access_control command for them

3) ODA - All 252 STIG checks with ODA exceptions

4) Full - All 252 STIG checks

Did you want to run checks against [1|2|3|4]: 3
Responded: 3

Is "3" correct? (y/n): y
Responded: y
ODA set of STIG checks  will be run
```

```
Did you want to run checks against SEV1, SEV2, SEV3, All [1|2|3|A]:A
Responded: A

Is "A" correct? (y/n): y
Responded: y

   **** Beginning: Verify testing;  ****
```

Example 2-4 Running STIG Scripts in the Secure Mode

The Secure mode assigns severity of the STIG warnings: SEV1 - Severity-1 STIG rules, SEV2 - Severity02 STIG rules, SEV3-Severity-3 STIG rules.

```
$ ./RunSTIG

**** Welcome to the Oracle Linux 7 STIG tool ****

This tool has two primary modes: Secure or Verify

Throughout this tool the answers in [] are the expected responses

Did you want to Secure or Verify? [Secure|Verify]: Secure
Responded: Secure

Is "Secure" correct? (y/n): y
******** WARNING    WARNING    WARNING    WARNING    WARNING *********

   When running this tool to Secure the system, the tool will modify
   the running system - BE SURE to quiet the system during this time
   by shutting down all apps (web servers, databases, etc) first.

   If required, exit this program with a Control-c

   Reversing any of the changes made by the tool is completed manually
   by reading the contents of the log files that should show exactly
   what was changed and undoing the change.

******** WARNING    WARNING    WARNING    WARNING    WARNING *********


Oracle Linux 7 Security Scripts have 4 flavors:

1) SCAP             - The 177 DISA SCAP checks

2) Exadata or ZDLRA - The 177 DISA SCAP checks with the special
                      host_access_control command for them

3) ODA - All 252 STIG checks with ODA exceptions

4) Full - All 252 STIG checks

Did you want to run checks against [1|2|3|4]: 3
Responded: 3
```

```
Is "3" correct? (y/n): y
Responded: y
ODA set of STIG checks  will be run

Did you want to run checks against [1|2|3|4]: 3
Responded: 3

Is "3" correct? (y/n): y
Responded: y
ODA set of STIG checks  will be run

Did you want to run checks against SEV1, SEV2, SEV3, All [1|2|3|A]: A
Responded: A

Is "A" correct? (y/n): y
Responded: y

   **** Beginning: Secure testing;  ****
```

Example 2-5 Location of Logs

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

```
[root@oda1 stig]# ls -la
total 128
drwx------.  8 3878  900  4096 Aug  4 11:55 .
drwxr-xr-x. 22 root root  4096 Aug  4 20:00 ..
drwx------.  2 3878  900  4096 Jul 27 13:24 01_Sev1
drwx------.  2 3878  900 12288 Jul 27 13:24 02_Sev2
drwx------.  2 3878  900  4096 Jul 27 13:24 03_Sev3
drwx------.  2 3878  900  4096 Aug  3 10:25 04_Logs
-rwx------.  1 3878  900 19716 Jul 27 13:24 .auto_answer
-rwx------.  1 3878  900  9288 Jul 27 13:24 .Change_log
-rwx------.  1 3878  900 16745 Jul 27 13:24 .control_01
drwx------.  2 3878  900  4096 Jul 27 13:24 .files
drwx------.  2 3878  900  4096 Jul 27 13:24 .messages
-rwx------.  1 3878  900 13169 Jul 27 13:24 README
-rwx------.  1 3878  900 19871 Jul 27 13:24 RunSTIG
```

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 Enabling CIS Benchmarks on Oracle Database Appliance

Understand how you can enable Center for Internet Security (CIS) Benchmarks for Oracle Database Appliance.

Center for Internet Security (CIS) Benchmarks are best practices for the secure configuration of a target system. They are consensus-based, best-practice security configuration guides developed and accepted by government, business, industry, and academia. The CIS Benchmarks are available for download at https://learn.cisecurity.org/benchmarks.

Oracle Database Appliance bundles the CIS script `cis.py` with the product for both bare metal and Virtualized Platform, in the directory `/opt/oracle/oak/bin/`.

Running the CIS Script

Follow these steps to run the CIS script:

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

   ```
   # ./cis.py
   ```

   On Virtualized Platform, run `cis.py` in `ODA_BASE` on both nodes to ensure that the script can fix any exceptions.

The table lists the command options for the CIS script.

Table 2-1 CIS Options for Oracle Database Appliance

Command Option	Description
`-h`	Specifies command options for Oracle Database Appliance CIS scripts
`-v`	Describes the CIS version information
`enable-SSH`	Enables direct ssh root login on the system
`disable-SSH`	Disables direct ssh root login on the system
`check`	Checks and lists Oracle Database Appliance CIS violations on the system. Use `check -h` to display all parameters for the `check` option.
`fix`	Fixes Oracle Database Appliance CIS violations reported on the system. Use `fix -h` to display all parameters for the `fix` option.

The table lists the parameters for the `check` option in the CIS script.

Table 2-2 Parameters for `check` option for Oracle Database Appliance CIS Script

Command Option	Description
`-h`	Provides help for the `check` option.
`all`	Tests and reports the security vulnerability for all components on the system
`perm`	Tests and reports the security vulnerability for all permissions checks
`conf`	Tests and reports the security vulnerability for all configuration parameters classification checks
`audit`	Tests and reports the security vulnerability for all auditing classification checks
`account`	Tests and reports the security vulnerability for all accounts classification checks
`fs`	Tests and reports the security vulnerability for all file systems classification checks
`grub`	Tests and reports the security vulnerability for enable/disable of grub password checks
`access`	Tests and reports the security vulnerability for access classification checks

The table lists the parameters for the `fix` option in the CIS script.

Table 2-3 Parameters for `fix` option for Oracle Database Appliance CIS Script

Command Option	Description
`-h`	Provides help for the `fix` option.
`all`	Fixes and reports security vulnerability for all components on the system
`perm`	Fixes and reports security vulnerability for permissions classification checks
`conf`	Fixes and reports security vulnerability for all system configuration classification checks
`audit`	Fixes and reports security vulnerability for all system audits classification checks
`account`	Fixes and reports security vulnerability for all system accounts classification checks
`fs`	Fixes and reports security vulnerability for all system file systems classification checks
`grub`	Fixes and reports security vulnerability for all system for enable/disable of grub password to adhere to CIS recommendations
`access`	Fixes and reports security vulnerability for all system access classification checks
`rollback`	Brings the system files at System Imaged state (without CIS modifications). Run this option only with the `fix` option.
`restore_prev`	Brings the system files to the state prior to previous security vulnerability fix. Run this option only with the `fix` option.

Logging of CIS Checks

The logs for CIS checks and fixes are stored in the directory `/opt/oracle/oak/log/oda_1/cis/check_time_stamp.log`. Log files are created for each execution of the check, fix, enable, and disable commands with the time stamp appended to each log file.

Examples for Running the CIS Script

Example 2-7 Checking for CIS Benchmarks Compliance

```
# ./cis.py check
```

Example 2-8 Implementing CIS Changes

```
# ./cis.py fix
```

Fixing Failed CIS Benchmarks

There may be CIS benchmarks that need system administrator assistance for implementing them. These CIS benchmarks have a status of `Failed` after you run the CIS script with the `fix` option.

For example:

```
[CIS_ID : 4.2.1.4] The rsyslog file is not configured for remote log
check,  please contact system administrtor

[CIS_ID : 4.2.3] syslog-ng is not configured, please check with system
administrator
```

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	• `root` • `oracle` • `grid` • `odaadmin`
Oracle Databases	• `sys` • `system` • `dbsnmp` For more information about database users, see the *Oracle Database Security Guide*.

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.
- 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 in Oracle Database Appliance, and keep a record in a secure place. All components in 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.

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.

You can 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, *2-3*
accessing ILOMs, *2-16*
accountability, *1-3*
accounting, *1-1*
auditing, *1-1*
authentication, *1-1*
authorization, *1-1*

C

ciphers, *4-1*
CIS, *2-14*
classification strategies, *2-3*
classifying data, *2-3*
client access
    isolating, *2-3*
cryptographic services, *2-7*

D

default passwords, *3-3*
disposing old hard drives, *4-4*

E

encrypting
    backups, *3-1*
    JDBC traffic, *2-7*
    Oracle Net Services, *2-7*
    traffic, *3-1*
Ethernet security guidelines, *3-1*
event accountability, *1-3*

F

FIPs, *2-9*
FIPS 140-2, *4-1*

H

hardening, *2-1*

I

ILOM, *2-7*
ILOM (Integrated Lights Out Manager), *2-7*
Intel AES-NI, *2-7*
IPMI v2.0, *2-16*
isolating
    client access, *2-3*
    management access, *2-3*
    multiple databases, *2-3*

K

Kerberos, *2-5*
key credentials, *2-5*

L

LDAP repositories, *2-5*
logical realms, *2-3*

M

MAC address, *3-1*
management access
    isolating, *2-3*
monitoring user logins, *1-1*

O

Oracle Advanced Security
    cryptographic services, *2-7*
    encrypting traffic, *3-1*
    using public keys, *2-5*
Oracle Audit Vault
    enablinig proactive detection, *2-8*
Oracle Data Guard, *3-1*
Oracle Database Firewall Remote Monitor, *2-8*
Oracle Database security products, *4-1*
Oracle Database Vault
    managing access, *2-5*
    mandatory access control, *2-3*
Oracle Enterprise User Security, *2-5*

Oracle ILOM (Oracle Integrated Lights Out Manager), 2-16
Oracle Label Security, 2-3
Oracle Recovery Manager (RMAN), 3-1
Oracle Virtual Private Database, 2-3
out-of-band, 3-1

P

password policy, 3-3

R

RADIUS, 2-5
restrictive file permissions, 3-3
RMAN (Oracle Recovery Manager)
  encrypting backups, 3-1
row level isolation, 2-3

S

secure isolation levels, 2-3
securing commnunications, 2-7
security considerations, 3-1
separation of duties, 2-5
serial numbers, 1-1
SNMPv3, 2-16
SSH (Secure Shell), 2-7, 2-16, 4-1
SSH (Secure Shell): default protocol limit, 3-3
SSH protocol 2 (SSH2), 4-1
SSL/TLS, 2-7
STIG, 2-9

T

TDE (Transparent Data Encryption), 2-7, 3-1
tracking hardware assets, 1-1

V

VLANs (virtual local area networks), 2-3, 3-1
VTP (VLAN Trunking Protocol), 3-1