Oracle® Database Appliance

Security Guide

Release 12.1.2.4.0

E64202-01

August 2015

ORACLE®

Oracle Database Appliance Security Guide, Release 12.1.2.4.0

E64202-01

Contents

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

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, see the following documents:

- *Oracle Database Appliance Getting Started Guide*
- *Oracle Database Appliance Owner's Guide*
- *Oracle Database Appliance Service Manual*
- *Oracle Database Appliance Administration and Reference Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*
- *Plug-in for Oracle Database Appliance User's Guide*

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 is an optimized, prebuilt and ready-to-use clustered database system that is easy to deploy, operate, and manage. By integrating hardware and software, Oracle Database Appliance eliminates the complexities of nonintegrated, manually assembled solutions. Oracle Database Appliance reduces deployment time from weeks or months to just a few hours, while preventing configuration and setup errors that often result in suboptimal, hard-to-manage database environments.

Within this framework, there are basic security principles that should be adhered to for all software and hardware. The following are the principles:

- Authentication: Authentication is how a user is identified, typically through confidential information such as user name and password, or shared keys. All components in Oracle Database Appliance use authentication to ensure that users are who they say they are. By default, local user names and passwords are used for authentication. Shared key-based authentication is also available.
- Authorization: Authorization allows administrators to control what tasks or privileges a user may perform or use. Personnel can only access the tasks and privileges that have been given to them. Oracle Database Appliance system administrators can configure resources with read/write/execute permissions to control user access to commands, disk space, devices, and applications.
- Accounting and Auditing: Accounting and auditing maintain a record of a user's activity on the system. Oracle Database Appliance software and hardware features allow administrators to monitor login activity, and maintain hardware inventories.
    - 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. Access and commands should be carefully monitored through system logs.
    - Hardware assets are tracked through serial numbers. Oracle part numbers are electronically recorded on all cards, modules, and mother boards, and can be used for inventory purposes.

In addition to the 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. The following sections describe these principles:

- Survivability of Mission-Critical Workloads
- Defense in Depth to Secure the Operating Environment

1.1 Survivability of Mission-Critical Workloads

Organizations selecting hardware and software platforms for their mission-critical workloads can be assured that Oracle Database Appliance can prevent or minimize the damage caused from accidental and malicious actions taken by internal users or external parties. As part of the Oracle Maximum Availability Architecture best practices, survivability is increased by the following:

- Ensuring that the components used have been 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. Organizations can customize the security settings of Oracle Database Appliance based upon the organization's policies and needs.
- Protecting the machine, including its operational and management interfaces, 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 capabilities help in cases where attackers attempt to disable one or more individual components in the system.

1.2 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 as follows:

- Offering a strong complement of protections to secure information in transit, in use, and at rest. Security controls are available at the server, storage, network, database, and application layers. Each layer's unique security controls can be integrated with the others to enable the creation of strong, layered security architectures.
- Supporting the use of well-defined and open standards, protocols, and interfaces. Oracle Database Appliance can be integrated into an organization's existing security policies, architectures, practices and standards. Integration is critical as applications and devices do not exist in isolation. The security of IT architectures is only as strong as its weakest component.
- Conducting multiple security scans using industry-leading security analyzers to implement all high-priority security items prior to the release of each new Oracle Database Appliance software version.

1.3 Least Privilege for Services and Users

Ensuring that applications, services and users have access to the capabilities that they need to perform their tasks is only one side of the least-privilege principle. It is equally

important to ensure that access to unnecessary capabilities, services, and interfaces are limited. Oracle Database Appliance promotes the principle of least-privilege as follows:

- Ensuring that access to individual servers, storage, operating system, databases, and other components can be granted based upon the role of each user and administrator. The use of role-based and multi-factor access control models with fine-grained privileges ensures that access can be limited to only what is needed.
- Constraining applications so that their access to information, underlying resources, network communications, and local or remote service access is restricted based upon need.

Whether caused by an accident or malicious attack, applications can misbehave, and without enforcement of least privilege, those applications may be able to cause harm beyond their intended use.

1.4 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 supports the principle of accountability as follows:

- 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. This allows 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 hardware and software are hardened. The following steps have been done to harden Oracle Database Appliance:

- Trimmed the list of installed packages so that unnecessary packages are not installed on the servers.
- Turned on only essential services on the Oracle Database Appliance nodes.
- Enabled auditing of the operating system user.

Oracle also provides recommended secure configurations for services such as NTP and SSH. In addition, the Oracle Database Appliance architecture provides security capabilities to the core components. The capabilities are grouped into the following categories:

- Using Isolation Policies
- Controlling Access to Data
- Using Cryptographic Services
- Monitoring and Auditing of Oracle Database Appliance
- Using Oracle ILOM for Secure Management

The preceding security capabilities are most often applied by organizations seeking to deploy a layered security strategy.

2.1 Using Isolation Policies

Organizations wanting to consolidate IT infrastructure, implement shared service architectures, and deliver secure multitenant services 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. The following are the secure isolation levels of Oracle Database Appliance:

- Isolating Network Traffic
- Isolating Databases

2.1.1 Isolating Network Traffic

At the physical network level, client access is isolated from device management and inter-device communication. Client and management network traffic are isolated on separate networks. Client access is provided over a redundant 10 Gbps Ethernet

network that ensures reliable, high-speed access to services running on the system. Management access is provided over a physically separate 1 Gbps Ethernet network. This provides a separation between operational and management networks.

Organizations may choose to further segregate network traffic over the client access Ethernet network by configuring virtual LANs (VLANs). VLANs segregate network traffic based on their requirements. Oracle recommends the use of encrypted protocols over VLANs to assure the confidentiality and integrity of communications.

2.1.2 Isolating Databases

Physical separation by dedicating an entire environment to a single application or database is one of the best isolation methods. However, it is expensive. A more cost-effective isolation strategy uses multiple databases within the same operating system image. Multiple database isolation is achieved through a combination of database and operating system-level controls, such as dedicated credentials for users, groups, and resource controls.

All Oracle Database security options are available for Oracle Database Appliance. Organizations wanting finer-grained database isolation can use software such as Oracle Database Vault, Oracle Virtual Private Database, and Oracle Label Security.

Oracle Database Vault includes a mandatory access control model to enforce isolation 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 is used to classify data, and mediate access to that data based upon its classification. Organizations 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.

2.2 Controlling Access to Data

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.

2.2.1 Controlling Network Access

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.

2.2.2 Controlling Database Access

Separation of duties is critical at every layer of the architecture to reduce the risk of collusive behavior, and prevent inadvertent errors. For example, use different operating system accounts to ensure role separation for database and storage administrators, including administrators supporting Oracle ASM. Within Oracle Database, users can be assigned 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 option 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.

Oracle Database Vault can be used 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.

2.2.3 Using SUDO

In environments where the system administration is handled by a different group than the database administration or where security is a large concern, you may want to limit access to the `root` user account and password. SUDO allows a system administrator to give certain users (or groups of users) the ability to run commands as `root` while logging all commands and arguments.

A SUDO security policy is configured via the file `/etc/sudoers`. Within the sudoers file, you can configure groups of users and sets of commands to simplify SUDO administration. You can also group hosts to allow similarly configured systems to share a single sudoers file.

Allowing Root User Access in SUDO

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.

To configure SUDO to allow a user to perform any operation as `root`, add lines to the commands section in the `/etc/sudoers` file as follows:

```
## The commands section may have other options added to it.
##
```

```
## Allow root to run any commands anywhere

root    ALL=(ALL)       ALL
jdoe  ALL=(ALL)      NOPASSWD: ALL
```

In this example, *jdoe* is the username. `ALL=(ALL)` grants the *jdoe* user permission to run commands as `root` on any host this sudoers file is on. NOPASSWD allows *jdoe* permissions without a password. The sudoers file is designed so that one sudoers file can be copied to multiple hosts with different rules on each host. `ALL` indicates that the *jdoe* user can run any command.

Example

After you configure the sudoer file with the user, the oakcli commands can be run by *jdoe* as the following. The root, oracle, and grid passwords will not be prompted.

```
$ sudo oakcli create database -db newdb

INFO: 2015-08-05 14:40:55: Look at the logfile
'/opt/oracle/oak/log/scaoda1011/tools/12.1.2.4.0/createdb_newdb_91715.log' for
more details

INFO: 2015-08-05 14:40:59: Database parameter file is not provided. Will be using
default parameters for DB creation
Please enter the 'SYSASM'  password : (During deployment we set the SYSASM
password to 'welcome1'):
Please re-enter the 'SYSASM' password:

INFO: 2015-08-05 14:41:10: Installing a new home: OraDb12102_home3 at
/u01/app/oracle/product/12.1.0.2/dbhome_3
s
Please select one of the following for Database type  [1 .. 3]:
1    => OLTP
2    => DSS
3    => In-Memory
```

See Also

For more information about configuring and using SUDO, refer to the SUDO man pages at `http://www.sudo.ws/sudo.html`

2.3 Using Cryptographic Services

The requirement to protect and validate information at rest, in transit, and in use often employs cryptographic services. 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 hardware-based cryptographic engines on processor chips provided by Intel AES-NI and Oracle SPARC. Using hardware for cryptographic operations provides significant performance improvement over performing the operations in software. Both engines provide the ability to perform cryptographic operations in hardware, and both are leveraged by Oracle software on the database and storage servers.

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 Integrated Lights Out Managers (ILOMs). SSL/TLS can enable secure communications between applications and other services.

Databases 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. For organizations concerned about the confidentiality of stored database content, database encryption, either at the table space level or column-level, Oracle Advanced Security should be considered.

In addition, Oracle Advanced Security can encrypt Oracle Net Services and JDBC traffic using either native encryption or SSL 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 SSL implementation supports the standard set of authentication methods including anonymous (Diffie-Hellman), server-only authentication using X.509 certificates, and mutual (client-server) authentication with X.509.

2.4 Monitoring and Auditing of Oracle Database Appliance

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 support of fine-grained auditing allows organizations to establish policies that selectively determine when audit records are generated. This helps organizations focus on other database activities, and 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.

2.5 Using Oracle ILOM for Secure Management

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. It is used to perform out-of-band management activities, such as the following:

- Provide secure access to perform secure lights-out management of the database and storage servers. Access includes web-based access protected by SSL, command-line access using Secure Shell, and IPMI v2.0 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.
- Provide 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

Security practices should be in place before the arrival of Oracle Database Appliance. After arrival, the security practices should be periodically reviewed and adjusted to stay current with the security requirements of your organization. This chapter contains the following sections:

3.1 Considerations for a Secure Environment

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.

3.2 Understanding User Accounts

The following table lists the default users and passwords for the Oracle Database Appliance components. All default passwords should be changed after deployment of Oracle Database Appliance.

Component	User Name and Password
Oracle Database Appliance servers	■ root/welcome1 ■ oracle/welcome1 ■ grid/welcome1
Oracle Databases	■ sys/welcome1 ■ system/welcome1 ■ dbsnmp/welcome1

3.3 Understanding the Default Security Settings

Oracle Database Appliance software is installed with many default security settings. Whenever possible and practical, secure default settings should be chosen and configured. The following default settings are used in Oracle Database Appliance:

- 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 listen 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

This chapter describes policies and procedures to keep Oracle Database Appliance secure. It includes the following topics:

- Securing the Hardware
- Securing the Software
- Maintaining a Secure Environment

4.1 Securing the Hardware

After installation of Oracle Database Appliance, the hardware should be secured. Hardware can be secured by restricting access to the hardware and recording the serial numbers. Oracle recommends the following practices to restrict access:

- 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.
- Use SSH protocol 2 (SSH-2) and FIPS 140-2 approved ciphers.
- Limit SSH allowed authentication mechanisms. Inherently insecure 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.

4.2 Securing the Software

Frequently, hardware security is implemented through software measures. Implement the following guidelines to protect hardware and software:

- 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 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.

See Also: "Understanding User Accounts" on page 3-3

- Create and use Oracle Integrated Lights Out Manager (ILOM) user accounts for individual users to ensure a positive identification in audit trails, and 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.
- Refer to the documentation to enable available security features.

See Also: *Oracle Database Security Guide*

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
- Oracle Audit Vault
- Data Masking
- Oracle Database Firewall
- Oracle Database Vault
- Oracle Label Security
- Oracle Secure Backup
- Oracle Total Recall

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.

4.3 Maintaining a Secure Environment

After security measures are implemented, they must be maintained to keep the system secure. Software, hardware and user access need to be updated and reviewed periodically. For example, organizations should review the users and administrators with access to Oracle Database Appliance, and its deployed services to verify if the levels of access and privilege are appropriate. Without review, the level of access granted to individuals may increase unintentionally due to role changes or changes to default settings. It is recommended that access rights for operational and administrative tasks be reviewed to ensure that each user's level of access is aligned to their roles and responsibilities.

4.3.1 Maintaining Network Security

After the networks are configured based on the security guidelines, regular review and maintenance is needed 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.

4.3.2 Updating Software and Firmware

Security enhancements are introduced through new releases and patch sets. Effective proactive patch management is a critical part of system security. Oracle recommends installing the latest release of the software, and all necessary security patches on the equipment. The application of Oracle recommended and security patches is a best practice for the establishment of baseline security.

4.3.3 Ensuring Data Security Outside of Oracle Database Appliance

Data located outside of Oracle Database Appliance can be secured by backing up important data. The data should then be stored in an off-site, secure location. Retain the backups according to organizational policies and requirements.

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

Index

R

S

T

V

X