
E81009-02

Copyright © 2008, 2017, Oracle and/or its affiliates. All rights reserved.

Primary Author: Janet Stern

Contributing Authors: Arturo Ceron, Caroline Johnston, Lypp-Tek Khoo-Ellis, Dan Norris, Kevin Simmons

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Preface

Audience v
Documentation Accessibility v
Related Documents v
Conventions v

1 Overview of Oracle Exadata Database Machine Security

1.1 Survivability of Mission-Critical Workloads 1-1
1.2 Defense in Depth to Secure the Operating Environment 1-2
1.3 Least Privilege for Services and Users 1-2
1.4 Accountability of Events and Actions 1-3

2 Security Features of Oracle Exadata Database Machine

2.1 Using Isolation Policies 2-1
  2.1.1 Isolating Network Traffic 2-1
  2.1.2 Isolating Databases 2-2
  2.1.3 Isolating Storage 2-2
2.2 Controlling Access to Data 2-3
  2.2.1 Controlling Network Access 2-3
  2.2.2 Controlling Database Access 2-3
  2.2.3 Controlling Storage Access 2-3
2.3 Using Cryptographic Services 2-4
2.4 Monitoring and Auditing of Oracle Exadata Database Machine 2-5
  2.4.1 Monitoring and Auditing Database Activity 2-5
2.5 Maintaining Quality Service 2-5
2.6 Using Oracle ILOM for Secure Management 2-6

3 Planning a Secure Environment

3.1 Considerations for a Secure Environment 3-1
3.2 Understanding User Accounts 3-5
Preface

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

Audience

This document is intended for database administrators and network administrators responsible for securing Oracle Exadata Database Machine.

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 Exadata Database Machine System Overview
• Oracle Exadata Database Machine Installation and Configuration Guide
• Oracle Exadata Storage Server Software User's Guide
• Oracle Database Security Guide
• Sun Datacenter InfiniBand Switch 36 Hardware Security Guide
• Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2
• The Security Guide for your platform, for example Oracle Server X6-2 Security Guide

Conventions

The following text conventions are used in this document:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, emphasis, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><strong>italic</strong></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
<tr>
<td><code>$</code> prompt</td>
<td>The dollar sign ($) prompt indicates a command run as the oracle user.</td>
</tr>
<tr>
<td><code>#</code> prompt</td>
<td>The pound (#) prompt indicates a command that is run as the root user.</td>
</tr>
</tbody>
</table>
Overview of Oracle Exadata Database Machine Security

Oracle Exadata Database Machine is an engineered system that combines the optimized database performance of Oracle Database integrated with Exadata Storage Servers. These core components are connected over a redundant InfiniBand fabric that enables low latency, and high throughput network communication. The redundant 10 Gbps Ethernet network is used for client access to services running on Oracle Exadata Database Machine. The 1 Gbps Ethernet network is used to manage the Oracle Exadata Database Machine components.

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 Exadata Database Machine 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 Exadata Database Machine 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 Exadata Database Machine 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 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 Exadata Database Machine addresses survivability, defense in depth, least privilege, and accountability. Oracle Exadata Database Machine delivers a well-integrated set of security capabilities that help organizations address their most-pressing security requirements and concerns.

1.1 Survivability of Mission-Critical Workloads

Organizations selecting hardware and software platforms for their mission-critical workloads can be assured that Oracle Exadata Database Machine can prevent or minimize the damage caused from accidental and malicious actions taken by internal personnel.
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 Exadata Database Machine 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 Exadata Database Machine 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 Exadata Database Machine employs multiple, independent, and mutually-reinforcing security controls to help organizations create a secure operating environment for their workloads and data. Oracle Exadata Database Machine 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 Exadata Database Machine 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 Exadata Storage Server Software release.

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 Exadata Database Machine 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
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 Exadata Database Machine supports the principle of accountability as follows:

- Ensuring each of the components used in Oracle Exadata Database Machine 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.
Security Features of Oracle Exadata Database Machine

Oracle Exadata Database Machine hardware and software are hardened. The following steps have been done to harden Oracle Exadata Database Machine:

- Trimmed the list of installed packages so that unnecessary packages are not installed on the servers.
- Turned on only essential services on the Exadata Storage Servers.
- Enabled firewalls (iptables) on the storage servers.
- Enabled auditing of the operating system user.
- Enforced hardened password policies.

Oracle also provides recommended secure configurations for services such as NTP and SSH. In addition, the Oracle Exadata Database Machine architecture provides the following security capabilities to the core components. These 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 Exadata Database Machine provides organizations the flexibility to implement the isolation policies and strategies based on their needs. The following are the secure isolation levels of Oracle Exadata Database Machine:

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.

Inter-device communication is provided by a redundant InfiniBand network. The InfiniBand network is a high-performance, low-latency backplane for communication between Exadata Storage Servers and database servers. By default, Exadata Storage Servers include a configured software firewall. The database servers can also be configured with a software firewall.
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 Exadata Database Machine. 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.

2.1.3 Isolating Storage

Oracle Exadata Database Machine storage is isolated from the rest of the architecture through the use of a private InfiniBand network. The storage managed by Exadata Storage Servers can be subdivided using Oracle Automatic Storage Management (Oracle ASM) to create individual disk groups. Each disk group can have its own security policies.
2.2 Controlling Access to Data

To protect application data, workloads, and the underlying infrastructure on which it runs, Oracle Exadata Database Machine offers comprehensive yet flexible access control capabilities for both users and administrators. The control capabilities include network access, database access, and storage 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 Exadata Database Machine 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 password-based authentication, Oracle Database also supports public key credentials, RADIUS, and Kerberos. 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 Controlling Storage Access

Oracle Exadata Storage Server Software supports the access control modes of open security, Oracle ASM-scoped security, and database-scoped security.

Open security allows any database to access any of the grid disks.

Oracle ASM-scoped security allows multiple databases assigned to one or more Oracle ASM clusters to share specific grid disks.

Note the following:
• The /etc/oracle/cell/network-config/cellkey.ora file needs to be readable only by the owner of the Grid Infrastructure with its specific unique group, such as asmadmin.

• Use the kfod utility in the Grid Infrastructure home to troubleshoot or verify which disks are accessible for your cluster.

• You should only set up database-scoped security after configuring and testing Oracle ASM-scoped security.

Database-scoped security, the most fine-grained level of access control, ensures that only specific databases are able to access specific grid disks. Database-scoped security works on a container level. This means that grid disks must be made available to the DB_UNIQUE_NAME of the CDB or non-CDB. Because of this, it is not possible to have database-scoped security per PDB.

In addition to its overall access control mode, Oracle ASM supports access controls at the disk group and file level to ensure that access to content stored on disk is only available to authorized users.

See Also:
Oracle Exadata Storage Server Software User's Guide for additional information about the access control modes

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. Oracle Exadata Database Machine includes network cryptographic services.

Whenever possible, Oracle Exadata Database Machine 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 Exadata Database Machine

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 Exadata Database Machine 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.

2.4.1 Monitoring and Auditing Database Activity

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 Maintaining Quality Service

There are many ways that applications can be attacked besides breaching a boundary or subverting an access control policy. Oracle Exadata Database Machine provides a number of capabilities to help detect and prevent resource exhaustion attacks, denial
of service attacks, and accidental or intentional faults that can impact the availability of services and data.

Oracle Exadata Storage Server Software includes I/O Resource Manager (IORM) to manage interdatabase and intradatabase I/O resources. IORM allows different databases with different performance requirements to share a common Exadata Storage Server pool. Multiple workloads within the same database can have their own resource policies. This flexible architecture allows organizations to ensure that critical workloads and databases share I/O resources when operating on a consolidated architecture.

Oracle Database includes tools to enable multiple databases to operate under the same operating system. Oracle Database Resource Manager (Resource Manager), and instance caging support the ability to dynamically control access to CPU resources using fine-grained methods. Resource Manager can control the degree of parallelism, the number of active sessions, and other shared resources to protect one database from monopolizing resources needed in shared database architectures.

Oracle Database Quality of Service Management (Oracle Database QoS Management) is an automated, policy-based solution that monitors the workload requests of an entire system. Oracle Database QoS Management correlates accurate run-time performance and resource metrics, analyzes the data to identify bottlenecks, and produces recommended resource adjustments to maintain performance objectives under dynamic load conditions.

### 2.6 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 Exadata Database Machine uses the security management capabilities of Oracle ILOM.

Oracle ILOM is a service processor embedded in many Oracle Exadata Database Machine 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.
Planning a Secure Environment

Security practices should be in place before the arrival of Oracle Exadata Database Machine. After arrival, the security practices should be periodically reviewed and adjusted to stay current with the security requirements of your organization.

3.1 Considerations for a Secure Environment

Oracle Exadata Database Machine 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 Exadata Database Machine.

A unified approach to identity and access management should be used when integrating Oracle Exadata Database Machine 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 Exadata Database Machine may be compromised.

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

- The ability to directly log in to common operating system accounts such as root, grid, and oracle should be disabled. Individual user accounts should be created for each administrator. After logging in with their individual account, the administrator can use sudo to run privileged commands, when required.
- The use of intrusion prevention systems on database servers to monitor network traffic flowing to and from Oracle Exadata Database Machine. 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 Exadata Database Machine. 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 Exadata Database Machine. 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 Exadata Database Machine. Exadata Storage Servers
include a configured software firewall by default. The database servers 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.

- The use of centralized audit and log repositories to aggregate the security-relevant information for improved correlation, analysis, and reporting. Exadata Storage Servers support this through the cell attribute `syslogConf`. The database servers support centralized logging using the typical system configuration methods.

While many of the features integrated into Oracle Exadata Database Machine 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 Exadata Database Machine 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.

**Note:**

To minimize the attack surface, Exadata Storage Servers do not support customization outside of their management interfaces. No custom users are permitted on the storage servers. The servers have been optimized and hardened for their specific purpose.

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 of administrative and operational services to use encryption protocols and key lengths that align with current policies. Cryptographic services provided by Oracle Exadata Database Machine benefit from hardware acceleration, which improves security without impacting performance.

- Create separate software owner accounts for Oracle Grid Infrastructure and Oracle Database software installations. These accounts should be used when deploying Oracle Exadata Database Machine.

- Manage and separate switches in Oracle Exadata Database Machine from data traffic on the network. This separation is also referred to as “out-of-band.”

- Separate sensitive clusters of 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.

Figure 3-1 (page 3-3) shows the default network for Oracle Exadata Database Machine X6-2, X5-2, X4-2, X3-2, and X2-2. Each Oracle Exadata Database Machine requires a minimum of two Ethernet networks and one InfiniBand network.

Figure 3-1  Network for Oracle Exadata Database Machine X6-2, X5-2, X4-2, X3-2, and X2-2 with Bonded Client Access

Figure 3-2 (page 3-4) shows the default network for Oracle Exadata Database Machine X6-8, X5-8, and X4-8 Full Rack. Each Oracle Exadata Database Machine requires a minimum of two Ethernet networks and one InfiniBand network.
Figure 3-2  Network for Oracle Exadata Database Machine X6-8, X5-8, and X4-8 Full Rack with Bonded Client Access

Figure 3-3 (page 3-5) shows the default network for Oracle Exadata Database Machine X3-8 Full Rack, and Oracle Exadata Database Machine X2-8 Full Rack. Each Oracle Exadata Database Machine requires a minimum of two Ethernet networks and one InfiniBand network.
See Also:

Oracle Exadata Database Machine Installation and Configuration Guide

3.2 Understanding User Accounts

In addition to the root user, Exadata Storage Servers have two users, celladmin and cellmonitor. The celladmin user is used to run all services on the cell. The cellmonitor user is used for monitoring purposes. The cellmonitor user cannot run services on the cell. Other Oracle Exadata Database Machine components have users for the management of the component.

The following table lists the default users and passwords for the Oracle Exadata Database Machine components. All default passwords should be changed after installation of Oracle Exadata Database Machine. Refer to My Oracle Support note 1291766.1 for information about changing the default user accounts passwords.
Table 3-1  Default Users and Passwords

<table>
<thead>
<tr>
<th>Component</th>
<th>User Name and Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database servers</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>root/welcome</td>
</tr>
<tr>
<td>•</td>
<td>oracle/Welcome$</td>
</tr>
<tr>
<td>•</td>
<td>grid/Welcome$</td>
</tr>
<tr>
<td>(this user exists only if</td>
<td>role separation is</td>
</tr>
<tr>
<td>role separation is chosen</td>
<td>chosen during deployment)</td>
</tr>
<tr>
<td>•</td>
<td>dbadmin/welcome</td>
</tr>
<tr>
<td>•</td>
<td>dbmonitor/welcome</td>
</tr>
<tr>
<td>•</td>
<td>SYS/Welcome$</td>
</tr>
<tr>
<td>(SYS is a database user)</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>SYSTEM/Welcome$</td>
</tr>
<tr>
<td>(SYSTEM is a database user)</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>Password for the grub boot loader: sos1Exadata</td>
</tr>
<tr>
<td>Exadata Storage Servers</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>root/welcome</td>
</tr>
<tr>
<td>•</td>
<td>celladmin/welcome</td>
</tr>
<tr>
<td>•</td>
<td>cellmonitor/welcome</td>
</tr>
<tr>
<td>•</td>
<td>CELLDIAG</td>
</tr>
<tr>
<td>CELLDIAG is an Exadata</td>
<td>Storage software user,</td>
</tr>
<tr>
<td>user, not an operating</td>
<td>system user.</td>
</tr>
<tr>
<td>Password of the CELLDIAG</td>
<td>user is reset to a random password</td>
</tr>
<tr>
<td>user is reset to a random</td>
<td>during the &quot;Apply Security Fixes&quot; step of Oracle Exadata Deployment Assistant. If this step is not run, then the default password is Welcome12345.</td>
</tr>
<tr>
<td>Password for the grub boot</td>
<td>loader: sos1Exadata</td>
</tr>
<tr>
<td>Exadata Storage Servers</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>root/welcome</td>
</tr>
<tr>
<td>•</td>
<td>celladmin/welcome</td>
</tr>
<tr>
<td>•</td>
<td>cellmonitor/welcome</td>
</tr>
<tr>
<td>•</td>
<td>CELLDIAG</td>
</tr>
<tr>
<td>CELLDIAG is an Exadata</td>
<td>Storage software user,</td>
</tr>
<tr>
<td>user, not an operating</td>
<td>system user.</td>
</tr>
<tr>
<td>Password of the CELLDIAG</td>
<td>user is reset to a random password</td>
</tr>
<tr>
<td>user is reset to a random</td>
<td>during the &quot;Apply Security Fixes&quot; step of Oracle Exadata Deployment Assistant. If this step is not run, then the default password is Welcome12345.</td>
</tr>
<tr>
<td>Password for the grub boot</td>
<td>loader: sos1Exadata</td>
</tr>
<tr>
<td>InfiniBand switches</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>root/welcome</td>
</tr>
<tr>
<td>•</td>
<td>nm2user/changeme</td>
</tr>
<tr>
<td>•</td>
<td>ilom-admin/ilom-admin</td>
</tr>
<tr>
<td>•</td>
<td>ilom-operator/ilom-operator</td>
</tr>
<tr>
<td>Ethernet switches</td>
<td>admin/welcome</td>
</tr>
<tr>
<td>Note: Secure the enable mode password and secret values for the admin user.</td>
<td></td>
</tr>
<tr>
<td>Power distribution units</td>
<td>admin/welcome</td>
</tr>
<tr>
<td>(PDUs)</td>
<td></td>
</tr>
<tr>
<td>The password for the admin</td>
<td>user is admin if you reset the PDU to factory default settings.</td>
</tr>
<tr>
<td>Database server ILOMs</td>
<td>root/welcome</td>
</tr>
<tr>
<td>•</td>
<td>MSUser</td>
</tr>
<tr>
<td>Management Server (MS) uses</td>
<td>this account to manage ILOM and reset it if it detects a hang.</td>
</tr>
<tr>
<td>this account to manage ILOM and reset it if it detects a hang.</td>
<td></td>
</tr>
<tr>
<td>Do not modify this account. This account is to be used by MS only.</td>
<td></td>
</tr>
<tr>
<td>Each time MS starts up, it deletes the previous MSUser account and re-creates the account with a randomly generated password.</td>
<td></td>
</tr>
<tr>
<td>MS communicates with ILOM using MSUser through the lanplus interface. It uses the IPMI v2.0 RMCP+ protocol for authentication. RMCP+ (remote management control protocol) is a UDP-based protocol with stronger authentication than RMCP.</td>
<td></td>
</tr>
<tr>
<td>The MSUser password is not persisted anywhere. If you need to change account passwords regularly, you can restart MS to change the password of the MSUser account.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-1  (Cont.) Default Users and Passwords

<table>
<thead>
<tr>
<th>Component</th>
<th>User Name and Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exadata Storage Server ILOMs</td>
<td>• root/welcome1</td>
</tr>
<tr>
<td></td>
<td>• MSUser</td>
</tr>
<tr>
<td></td>
<td>See the description above for details about this user.</td>
</tr>
<tr>
<td>InfiniBand ILOMs</td>
<td>• ilom-admin/ilom-admin</td>
</tr>
<tr>
<td></td>
<td>• ilom-operator/ilom-operator</td>
</tr>
<tr>
<td></td>
<td>• root/welcome1</td>
</tr>
<tr>
<td>Keyboard, video, mouse (KVM)</td>
<td>admin/welcome1</td>
</tr>
</tbody>
</table>

**Note:**

After Oracle Exadata Database Machine has been deployed, the installation process disables all root SSH keys and expires all user passwords as a security measure for your system. If you do not want the SSH keys disabled or the passwords expired, advise the installation engineer before the deployment.

**Related Topics:**

- CREATE DIAGPACK
- How to change OS user password for Cell Node, Database Node, ILOM, KVM, Infiniband Switch, GigaBit Ethernet Switch and PDU on Exadata Database Machine (My Oracle Support Doc ID 1291766.1)

### 3.3 Understanding the Default Security Settings

Oracle Exadata Storage Server 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 Exadata Database Machine:

- 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.
- Limited ability to use the `su` command.
- Password-protected boot loader installation.
- All unnecessary system services are disabled, including the Internet service daemon (inetd/xinetd).
• Software firewall configured on the storage cells.
• 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.

3.4 Using Oracle Exadata Deployment Assistant for Greater Security

Oracle Exadata Deployment Assistant includes a step to increase hardware security on Oracle Exadata Database Machine. The last step of Oracle Exadata Deployment Assistant, "Secure Oracle Exadata Database Machine" implements the following security policies:

• For the root user, and all users with their home directory in the /home directory, on the database servers and Exadata Storage Servers, the following password-aging values are set:
  – The maximum number of days for a password is 90 days.
  – The minimum amount of time between password changes is 24 hours.
  – The number of days of alerts before a password change is seven days.
  – All non-root users must change their password at their next log in.

• For all users, the following password qualifications are set:
  – Password using one character class is not allowed.
  – Password using two character classes is not allowed.
  – A minimum of 16 characters are required for a passphrase.
  – A minimum length of 12 characters for a password when using three character classes.
  – A minimum length of eight characters for a password when using four character classes.
  – Character classes for passwords are uppercase letters, lowercase letters, digits, and other characters.
  – Uppercase letters at the beginning of the password, and digits at the end of the password are not counted when calculating the number of character classes.
  – The maximum length for a password is 40 characters.
  – A new password cannot be similar to old passwords.

• For the root user, SSH equivalency is removed for all database servers and Exadata Storage Servers.
• The following permissions are set by Oracle Exadata Deployment Assistant:
  – The Automatic Diagnostic Repository (ADR) base directory, $ADR_BASE, has SUID ((Set owner User ID) on the diag directory and its sub-directories.
  – The celladmin user group has read and write permissions.
4

Keeping Oracle Exadata Database Machine Secure

This chapter describes policies and procedures to keep Oracle Exadata Database Machine secure.

4.1 Securing the Hardware

After installation of Oracle Exadata Database Machine, 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 Exadata Database Machine and related equipment in a locked, restricted-access room.
- Lock the rack door unless service is required on components within the rack.
- Restrict access to hot-pluggable or hot-swappable devices because the components can be easily removed by design.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- 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.
- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system managers in the case of a system emergency.
- Record the serial numbers of the components in Oracle Exadata Database Machine, and keep a record in a secure place. All components in Oracle Exadata Database Machine have a serial number.

Related Topics:

- How To Obtain The Serial Number Associated With The System Board, Motherboard, Disk Controller, Disks, Infiniband HCA And More Contained In A Cell Or Compute Box (Exadata-Sun V2 or X2 / 11.2)? (My Oracle Support Doc ID 949614.1)
- How to Determine the Serial Number of a Datacenter InfiniBand Switch 36 or QDR InfiniBand Gateway InfiniBand Switch (My Oracle Support Doc ID 1299791.1)

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 Exadata Database Machine 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.

- Limit use of the root super user account. 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.

- Ensure Oracle Exadata Database Machine is deployed with separate software owner accounts for Oracle Grid Infrastructure and Oracle Database software installations.

- Disable unnecessary protocols and modules in the operating system.

- 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.

Oracle Exadata Database Machine 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.

Related Topics:

- Understanding User Accounts (page 3-5)
- Oracle Database Security Guide

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 Exadata Database Machine, 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.

Organizations are encouraged to utilize tools to detect unauthorized changes,
configuration drift, and prepare for security patch application. Oracle Enterprise
Manager Grid Control provides an integrated solution for managing operational issues
for hardware, deployed applications, and services.

Related Topics:
• Responses to common Exadata security scan findings(My Oracle Support Doc ID
  1405320.1)
• Oracle Exadata Database Machine Maintenance Guide

4.3.1 Maintaining Network Security

After the networks are configured based on the security guidelines, regular review and
maintenance is needed. The management network switch configuration file should be
managed offline, and access to the configuration file should be limited to authorized
administrators. The configuration file should contain descriptive comments for each
setting. Consider keeping a static copy of the configuration file in a source code control
system. Periodic reviews of the client access network are required to ensure that
secure host and ILOM settings remain intact and in effect. In addition, periodic reviews
of the settings ensure that they remain intact and in effect.

Follow these guidelines to ensure the security of local and remote access to the
system:
• Create a login banner to state that unauthorized access is prohibited.
• 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 Exadata Database
  Machine.
• 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.
Standard 140 of FIPS (Federal Information Processing Standards) relates to security and cryptography. FIPS 140 is a collection of standards published by NIST (National Institute of Standards and Technology), an agency of the United States federal government. FIPS 140 protects data during transit as well as at rest. It specifies security standards for cryptographic components within a computing environment. FIPS 140 is useful for organizations that need to document that their computing environment meets a published level of security. Many government agencies and financial institutions use FIPS 140 qualified systems.

Configuring FIPS 140 at the Oracle Database level enables the use of FIPS 140 cryptographic modules in the Secure Sockets Layer (SSL), Transparent Data Encryption (TDE), DBMS_CRYPTO PL/SQL package, and Exadata Smart Scan. This protects data while processing Exadata Smart Scan offload operations.

See Also:

- Oracle Database Security Guide
- Oracle Database Advanced Security Guide
- Oracle Exadata Database Machine System Overview

4.3.2 Updating Software and Firmware

Effective proactive patch management is a critical part of system security. Security enhancements are introduced through new releases and patch sets. 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.

Exadata Storage Server operating system and kernel updates are delivered with Oracle Exadata Storage Server Software updates. Oracle Exadata Database Machine database servers are updated using yum facilities. Power distribution unit (PDU) firmware updates are handled separately from the software and other firmware updates. Ensure that the PDU is running the latest approved firmware for Oracle Exadata Database Machine. As PDU firmware updates are not issued frequently, it is usually sufficient to check the PDU firmware release when upgrading Oracle Exadata Storage Server Software.

Note:

Devices such as network switches that contain firmware may require patches and firmware updates.

Related Topics:

- Oracle Exadata Database Machine Maintenance Guide
4.3.3 Ensuring Data Security Outside of Oracle Exadata Database Machine

Data located outside of Oracle Exadata Database Machine 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 Exadata Database Machine disk retention support option allows the retention of all replaced hard drives and flash drives, instead of returning them to Oracle.

The CellCLI DROP CELLDISK command includes an option to securely erase data by overwriting the data. If Exadata Storage Server drives contain sensitive data that needs to be erased for redeployment or another purpose, then the secure erase feature should be used on the storage cell. The ERASE option ensures that all data is overwritten with random data, and erased up to seven times. This ensures that the data cannot be recovered, and that the data is permanently erased.
5

Securely Erasing Oracle Exadata Database Machine

This section contains the following topics:

• Overview of Secure Eraser (page 5-1)
• Securely Erasing Database Servers and Storage Servers (page 5-4)
• Automatic Secure Erasure through PXE Boot (page 5-5)
• Interactive Secure Erasure through PXE Boot (page 5-9)
• Interactive Secure Erasure through External USB (page 5-12)
• Secure Eraser Syntax (page 5-14)
• Resetting InfiniBand Switches, Ethernet Switch, and Power Distribution Units to Factory Default (page 5-15)

5.1 Overview of Secure Eraser

Oracle Exadata software release 12.2.1.1.0 or later provides a secure erasure solution, called Secure Eraser, for every component within Oracle Exadata Database Machine.

Oracle Exadata Database Machine consists of the following components:

• Database servers
• Storage servers
• InfiniBand switches
• Ethernet switches
• Power distribution units

Secure Eraser is a comprehensive solution that covers all Exadata Database Machines V2 or higher, including both 2-socket and 8-socket servers. The solution securely erases all data on both database servers and storage servers, and resets InfiniBand switches, Ethernet switches, and power distribution units back to factory default.

To achieve the best possible performance, secure erasure is performed in parallel at every layer on an Oracle Exadata Database Machine. Database servers and storage servers are securely erased in parallel. Within a server, all device types (such as hard drives, flash devices, and internal USBs) are securely erased in parallel. For each device type, all devices are further securely erased in parallel.

Secure Eraser automatically detects the hardware capability of a storage device and picks the best erasure method supported by the device. Crypto erase is used whenever possible to provide better security and faster speed.

Secure Eraser comes with flexible options. You can choose to initiate a secure erasure either through PXE or through an external USB. The entire process can be completely
automated without any user intervention. Or, you can choose to do it interactively and choose to erase specific types of storage devices.

Secure Eraser periodically generates a progress report every 10 seconds so that you can easily monitor the progress.

When the secure erasure is completed, a certificate is generated for each server with a list of devices that have been securely erased. The following figure shows a sample certificate from Secure Eraser.
**Figure 5-1  Sample Certificate from Secure Eraser**

![Certificate Image]

---

**Data Erasure Certificate**

- **Start Time:** 2016-07-06 21:27:05
- **End Time:** 2016-07-06 21:28:11
- **Chassis Number:** 1523NM705C

This is to certify that the components identified below have been securely erased in accordance with the applicable guidelines of NIST SP-800-88r1 standard.

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Model</th>
<th>Serial</th>
<th>Size</th>
<th>Erasure Level</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A096H</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>2</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A0A4Y</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>3</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A07D4</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>4</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A08G8</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>5</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F008KSE</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>6</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F008KS3</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>7</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F008KL7</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>8</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F008KQR</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>9</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F008A12</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>10</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A79G</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>11</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A80C</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>12</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A79F</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>13</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A5WD</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>14</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A5XS</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>15</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A7N1</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>16</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>F00A62G</td>
<td>200.00GB</td>
<td>Crypto Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>17</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E68HXX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>18</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E650SYX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>19</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E6004X</td>
<td>4.00TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>20</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5UPAX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>21</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5X3X</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>22</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5M7X</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>23</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5P8PX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>24</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E507UX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>25</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5LYDX</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>26</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5024X</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>27</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5LY9X</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>28</td>
<td>Disk</td>
<td>H7240AS60SUN4.0T</td>
<td>1552E5VX4X</td>
<td>3.99TB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>29</td>
<td>USB</td>
<td>SSM</td>
<td>190063B8AFB749</td>
<td>8.01GB</td>
<td>3-Pass Erase</td>
<td>Succeeded</td>
</tr>
<tr>
<td>30</td>
<td>ILOM</td>
<td>ILOM</td>
<td>1516NM705E</td>
<td>1.00GB</td>
<td>Factory Reset</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

**ERASURE PERFORMED BY:**

Name: Jane Doe

Signature: ___________________________  Date: ______________

**ERASURE WITNESSSED BY:**

Name: John Smith

Signature: ___________________________  Date: ______________
5.2 Securely Erasing Database Servers and Storage Servers

Oracle Exadata software 12.2.1.1.0 or later comes with a utility called Secure Eraser which securely erases data on hard drives, flash devices, and internal USBs, and resets ILOM to factory default.

In earlier versions of Exadata, you can securely erase user data through CellCLI commands such as `DROP CELL ERASE`, `DROP CELLDISK ERASE`, or `DROP GRIDDISK ERASE`. These DROP commands only cover user data on hard drives and flash devices. Secure Eraser, on the other hand, sanitizes all content, not only user data but also operating system, Exadata software, and user configurations. In addition, it covers a wider range of hardware components including hard drives, flash devices, internal USBs, and ILOMs.

⚠️ **Caution:**

The server will become unbootable after the system devices are securely erased, and ILOM will no longer be remotely accessible after being reset to factory default. ILOM will remain accessible through serial console.

The Secure Eraser utility works on both database servers and storage servers and covers all Oracle Exadata Database Machines V2 or higher.

Based on hardware capabilities, different secure erasure methods are applied. In general, Secure Eraser has two types of erasure methods: 3-pass erase and crypto erase. The 3-pass erase method overwrites all addressable locations with a character, its complement, then a random character, and finally verifies the results. The crypto erase method erases all user data present on instant secure erase (ISE) devices by deleting the encryption keys with which the user data was previously encrypted.

The following table gives a summary of the secure erasure methods used and their approximate time. Note that the time for 3-pass erase varies from drives to drives based on their size and speed. It is approximately equal to the time required to overwrite the entire device three times and read it one more time. Hard drives, flash devices, and internal USBs are securely erased in parallel: the time required to erase one device is the same as that required for erasing multiple devices of the same kind.

<table>
<thead>
<tr>
<th>Component</th>
<th>Make Model</th>
<th>Erasure Method</th>
<th>Approximate Time</th>
</tr>
</thead>
</table>
| Hard drive | • 8 TB hard drives on X5   
                      • All hard drives on X6 or later | Crypto erase | 1 minute |

Table 5-1   Time Required to Securely Erase Various Devices
<table>
<thead>
<tr>
<th>Component</th>
<th>Make Model</th>
<th>Erasure Method</th>
<th>Approximate Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard drive</td>
<td>All other hard drives</td>
<td>3-pass erase</td>
<td>600 GB: 7 hours 1.2 TB: 12 hours 2 TB: 35 hours 3 TB: 49 hours 4 TB: 56 hours</td>
</tr>
<tr>
<td>Flash device</td>
<td>Flash devices on X3 or later</td>
<td>Crypto erase</td>
<td>1 minute</td>
</tr>
<tr>
<td>Flash device</td>
<td>All other flash devices</td>
<td>3-pass erase</td>
<td>22.875 GB: 20 minutes</td>
</tr>
<tr>
<td>Internal USB</td>
<td>All platforms</td>
<td>3-pass erase</td>
<td>4 GB: 30 minutes 8 GB: 1 hour</td>
</tr>
<tr>
<td>ILOM</td>
<td>All platforms</td>
<td>Factory reset</td>
<td>1 minute</td>
</tr>
</tbody>
</table>

### 5.3 Automatic Secure Erasure through PXE Boot

In this procedure, you configure Secure Eraser to run automatically when you reboot the nodes.

**Before you begin:**

- Review My Oracle Support note 2180963.1 for the latest Secure Eraser information and to download the Secure Eraser package.
- Make sure you have access to a PXE server where the nodes to be erased can boot from.
- Make sure you have access to a NFS server that is accessible from all the nodes to be erased.
- Make sure you have access to one of the nodes to be erased.

1. Copy the PXE image files `initrd` (`initrd-<version>`) and `kernel` (`vmlinux-<version>`) from the Secure Eraser package to the `/tftpboot` directory on the PXE server.

2. Create a file containing the names of the database servers and storage servers you want to erase.

   To generate this file, you can run the following command from one of the nodes to be erased, and verify the nodes in the files are the ones to be erased.

   ```
   # ibhosts | awk '/S [0-9.\,\,]\*\||,|C [0-9.\,\,]\*\| (print $6)\| sed s/\*//g' > nodes_to_be_erased
   ```

3. Copy the `dcli` utility from the Secure Eraser package and the `nodes_to_be_erased` file generated in step 2 to the PXE server.

4. Create a PXE configuration template called `pxe_cfg.template` to contain the following lines:

   ```
   default linux
   label linux
   ```
kernel vmlinux-nfs-12.2.1.1.0-161015-cell
append initrd=initrd-nfs-12.2.1.1.0-161015-cell.img dhcp pxe quiet loglevel=0
secureeraser bootarea=diagnostics console=tty1 console=ttyS0,115200n8
logpath=10.133.42.221:/export/exadata_secure_eraser_certificate_dir

• The first line (default) indicates that the default label to use is called linux.
• The second line (label) defines the linux label.
• The third line (kernel) identifies the kernel file to load. In this case it is the file copied over in step 1.
• The fourth line (append) adds more options to the kernel command line. The append statement must be on a single line in the configuration file.
  – The initrd option specifies the initrd file to load. In this case it is the initrd file copied over in step 1.
  – The dhcp option specifies to use DHCP to discover the eth0 interface.
  – The pxe option suppresses search for the image on virtual CD and USB devices.
  – The quiet option suppresses excessive kernel log messages.
  – The loglevel=0 option suppresses non-critical kernel messages.
  – The bootarea option indicates that the boot mode is diagnostic and not imaging install or rescue.
  – The console options indicate standard output and standard error messages are printed to both ILOM web console and serial console.
  – The secureeraser option indicates PXE boot will automatically trigger the Secure Eraser utility to sanitize all media including hard drives, flash devices, internal USBs, and ILOM on the node.
  – The logpath option specifies the NFS share directory where Secure Eraser will save the certificate.

By default, the append line shown above causes Secure Eraser to erase all components. You can use secureeraser-options to specify command-line options for Secure Eraser to change the default behavior and securely erase certain components only. For example, to erase hard drives and USBs only during the PXE boot, the template would look like this:

default linux
label linux
kernel vmlinux-nfs-12.2.1.1.0-161015-cell
append initrd=initrd-nfs-12.2.1.1.0-161015-cell.img dhcp pxe quiet loglevel=0
secureeraser secureeraser-options="--hdd --usb" bootarea=diagnostics
console=tty1 console=ttyS0,115200n8 logpath=10.133.42.221:/export/exadata_secure_eraser_certificate_dir

5. On the PXE server, use the template file to generate a PXE configuration file in the /tftpboot/pxelinux.cfg/ directory for each of the nodes to be erased.

The PXE configuration file name is the dash-separated MAC address of the node with the prefix 01-.

If the nodes to be erased are accessible, use the following steps to automatically generate a PXE configuration file for each node based on the template.

a. Set up SSH equivalence with the nodes to be erased from the PXE server.
   The command will prompt for the root password of each node.
pxe_server# dcli -g nodes_to_be_erased -l root

b. Create PXE configuration files, one for each node to be erased based on the configuration template.

pxe_server# dcli -g nodes_to_be_erased -l root "ip addr show eth0" | awk '/link/ether/ {print "01:"$3}="/ | sed "s/:-/:-/g" | xargs -I {} cp pxe_cfg.template {}

If the nodes are not accessible, use the following step to generate a PXE configuration file for each node to be erased:

a. Manually collect the MAC address of the eth0 interface from each node and write them into a text file called \texttt{mac_addresses}. Write one MAC address per line. For example:

00:10:e0:62:c4:fa
00:10:e0:62:c2:8a
00:10:e0:62:b8:7c
00:10:e0:62:b8:3a
00:10:e0:62:c6:bc

b. Use the following command to create a list of PXE configuration files, one for each node to be erased based on the configuration template.

pxe_server# cat mac_addresses | sed "s/:/-/g;s/^/01-/g" | xargs -I {} cp pxe_cfg.template {}

In both cases, you should get a list of PXE configuration files, one for each node to be erased. For example, if the MAC addresses of the nodes in a quarter rack are 00:10:e0:62:c4:fa, 00:10:e0:62:c2:8a, 00:10:e0:62:b8:7c, 00:10:e0:62:b8:3a, and 00:10:e0:62:c6:bc, you should get the following files:

01-00-10-00-62-c4-fa
01-00-10-00-62-c2-8a
01-00-10-00-62-b8-7c
01-00-10-00-62-b8-3a
01-00-10-00-62-c6-bc

The files have the same content as the configuration template.

Check your specific PXE server requirements. Your PXE server may need slightly different names or settings.

6. Configure the nodes to boot from PXE and reboot the nodes.

If the nodes to be erased are accessible, run the following commands:

pxe_server# dcli -g nodes_to_be_erased -l root "ipmitool chassis bootdev pxe"
pxe_server# dcli -g nodes_to_be_erased -l root "reboot"

If the nodes to be erased are not remotely accessible but the ILOMs are, use the following steps

a. Create a file called \texttt{iloms_to_be_reset} containing the names of ILOMs. For example:

db1-ilom
db2-ilom
cell1-ilom
cell2-ilom
cell3-ilom
b. Configure the nodes to boot from PXE through ILOMs. The command will prompt for ILOM root password.

```
pxe_server# cat iloms_to_be_reset | xargs -I {} ipmitool -I lanplus -H {} -U root chassis bootdev pxe
```

c. Reboot the nodes from ILOMs. The command will prompt for ILOM root password.

```
pxe_server# cat iloms_to_be_reset | xargs -I {} ipmitool -I lanplus -H {} -U root chassis power cycle
```

If neither host nor ILOM is remotely accessible, log into ILOM using a serial console and run the following commands

```
ILOM> set /HOST/boot_device=pxe
```

```
ILOM> reset /SYS
```

7. The Secure Eraser utility will be automatically called to sanitize all storage media including hard drives, flash devices, and internal USBs, and to reset ILOM to factory default for all nodes in parallel.

Secure Eraser creates a file called `secureeraser_node_chassis_number_date_time.certificate` in the specified logpath location. `node_chassis_number` is the ID attribute of the storage server or database server in CellCLI or DBMCLI.

The file contains a progress report that is updated every 10 seconds. The progress report is also output to the console on each node. The following is an example of the progress report:

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A96H</td>
<td>200.00GB</td>
<td>Being (6%)</td>
</tr>
<tr>
<td>2</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A84Y</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>3</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A7D4</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>4</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A6WG</td>
<td>200.00GB</td>
<td>Being (6%)</td>
</tr>
<tr>
<td>5</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL008KSE</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>6</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL008KS3</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>7</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL008KL7</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>8</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL008KQR</td>
<td>200.00GB</td>
<td>Being (6%)</td>
</tr>
<tr>
<td>9</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A812</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>10</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A79G</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>11</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A80C</td>
<td>200.00GB</td>
<td>Being (6%)</td>
</tr>
<tr>
<td>12</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A79F</td>
<td>200.00GB</td>
<td>Being (6%)</td>
</tr>
<tr>
<td>13</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A5WD</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>14</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A5XS</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
<tr>
<td>15</td>
<td>Flash</td>
<td>Flash Accelerator F80 PCIe Card</td>
<td>FL00A7N1</td>
<td>200.00GB</td>
<td>Being (5%)</td>
</tr>
</tbody>
</table>
As the sample progress report shows, Secure Eraser erases all storage devices in parallel. After the storage devices are securely erased, Secure Eraser will reset the ILOM to the factory default. This is to ensure that in the case that secure erasure fails on some storage device, the web console is still accessible for remote debugging, and ILOM is still accessible to control the host.

Once secure erasure is complete, a certificate called
secureeraser_node_chassis_number_date_time.certificate.pdf is generated at the NFS share location specified by the logpath option in step 4. If secure erasure is successful, the nodes will be shut down automatically. If Secure Eraser does not succeed on some components, then the node will be left in diagnostic shell for further debugging. Assuming all previous steps are successful, and you have resolved the issue, you can go back to step 6 and rerun Secure Eraser.

Related Topics:

- Secure Eraser Syntax (page 5-14)
  The Secure Eraser utility has several option.
- Securely Erasing Oracle Exadata Database Machine Servers (My Oracle Support Doc ID 2180963.1)

5.4 Interactive Secure Erasure through PXE Boot

Before you begin:

- Review My Oracle Support note 2180963.1 for the latest information and to download the Secure Eraser package
• Make sure you have access to a PXE server where the nodes to be erased can boot from.
• Make sure you have access to a NFS server that is accessible from all the nodes to be erased.
• Make sure you have access to one of the nodes to be erased.

1. Copy the cell PXE image files initrd (initrd-version) and kernel (vmlinux-version) from the Secure Eraser package to the /tftpboot directory on the PXE server.

2. Create a file containing the names of the database servers and storage servers to be erased.

To generate this file, you can run the following command from one of the nodes to be erased, and verify the nodes in the files are the ones to be erased.

```
# ibhosts | awk '/S [0-9.\.]/ || /C [0-9.\.]/ {print $6}' | sed "s/"//g"
> nodes_to_be_erased
```

3. Copy the dcli utility from the Secure Eraser package along with the file generated in step 2 to the PXE server.

4. Create a PXE configuration template called pxe_cfg.template to contain the following lines:

```plaintext
default linux
label linux
kernel vmlinux-nfs-12.2.1.1.0-161015-cell
append initrd=initrd-nfs-12.2.1.1.0-161015-cell.img dhcp pxe quiet loglevel=0
bootarea=diagnostics console=tty1 console=ttyS0,115200n8
```

This configuration file differs from the one in Automatic Secure Erasure through PXE Boot (page 5-5) in that the secureeraser option is left out to indicate that no secure erasure shall be triggered automatically. The rest of the file is the same.

5. On the PXE server, use the template file to generate a PXE configuration file in the /tftpboot/pxelinux.cfg/ directory for each of the nodes to be erased.

The PXE configuration file name is the dash-separated MAC address of the node with the prefix 01-.

If the nodes to be erased are accessible, perform the following steps to automatically generate a PXE configuration file for each node based on the template:

a. Set up SSH equivalence with the nodes to be erased from the PXE server. The command will prompt for the root password of each node.

```
pxe_server# dcli -g nodes_to_be_erased -k -l root
```

b. Create a list of PXE configuration files, one for each node to be erased based on the configuration template.

```
pxe_server# dcli -g nodes_to_be_erased -l root "ip addr show eth0" | awk '/link/ether/ {print "01:"$3} | sed "s/:-/:-/g" | xargs -I {} cp pxe_cfg.template {}'
```

If the nodes are not accessible, perform the following steps to generate a PXE configuration file for each node:

a. Manually collect the MAC address of the eth0 interface from each node and write them into a text file called mac_addresses. Write one MAC address per line. For example:
b. Use the following command to create a list of PXE configuration file, one for each node to be erased based on the configuration template.

```
pxe_server# cat mac_addresses | sed "s/:/-/g;s/^/01-/g" | xargs -I {} cp pxe_cfg.template {}
```

In both cases, you should have a list of PXE configuration files, one for each node to be erased. For example, if the MAC addresses of the nodes in a quarter rack are 00:10:e0:62:c4:fa, 00:10:e0:62:c2:8a, 00:10:e0:62:b8:7c, 00:10:e0:62:b8:3a, and 00:10:e0:62:c6:bc, then you should get the following files:

- 01-00-10-e0-62-c4-fa
- 01-00-10-e0-62-c2-8a
- 01-00-10-e0-62-b8-7c
- 01-00-10-e0-62-b8-3a
- 01-00-10-e0-62-c6-bc

The files have the same content as the configuration template.

Check your specific PXE server requirements. Your PXE server may need slightly different names or settings.

6. Configure the nodes to boot from PXE and reboot the nodes.

If the nodes to be erased are accessible, run the following commands:

```
pxe_server# dcli -g nodes_to_be_erased -l root "ipmitool chassis bootdev pxe"

pxe_server# dcli -g nodes_to_be_erased -l root "reboot"
```

If the nodes are not accessible, then perform the following steps:

a. Create a file called `iloms_to_be_reset` containing the names of ILOMs. For example:

```
db1-ilom
db2-ilom
cell1-ilom
cell2-ilom
cell3-ilom
```

b. Configure the nodes to boot from PXE through ILOMs. The command will prompt for ILOM root password.

```
pxe_server# cat iloms_to_be_reset | xargs -I {} ipmitool -I lanplus -H {} -U root chassis bootdev pxe
```

C. Reboot the nodes from ILOMs. The command will prompt for ILOM root password.

```
pxe_server# cat iloms_to_be_reset | xargs -I {} ipmitool -I lanplus -H {} -U root chassis power cycle
```

7. If you get the following prompt on the remote or serial console, enter "e" at the prompt to enter the diagnostic shell:

Choose from following by typing letter in '()':

(e)nter interactive diagnostics shell. Must use credentials from Oracle
support to login (reboot or power cycle to exit the shell).

Select:

8. Log in to the system as the root user.

You will be prompted for the password for the root user of diagnostic shell. The password can be retrieved from Oracle Support.

localhost login: root
Password: *********

9. Run the Secure Eraser utility to sanitize all devices or one type of device.

- /usr/sbin/secureeraser --erase --all --output=REMOTE_NFS_LOCATION

REMOTE_NFS_LOCATION is the remote NFS location in the format of IP:FILE_PATH. The Secure Eraser utility will automatically mount the remote NFS location and save the certificate there.

For example, to erase all devices including hard drives, flash devices, internal USBs, and ILOM, and save the certificate at this NFS location:

10.133.42.221:/export/exadata_secure_eraser_certificate_dir:

- /usr/sbin/secureeraser --erase --all --output=10.133.42.221:/export/exadata_secure_eraser_certificate_dir

To erase just the hard drives:

- /usr/sbin/secureeraser --erase --hdd --output=10.133.42.221:/export/exadata_secure_eraser_certificate_dir

Note that it is important to point the output option to an NFS location so that the certificate can be saved properly.

You will be prompted with a list of devices to be erased and to confirm that you want to proceed with the secure erasure.

A progress report, as shown in step 7 of the Automatic Secure Erasure through PXE Boot (page 5-5), will be printed to the console every 10 seconds.

In interactive mode, the server will be left on after the specified devices are securely erased. You can power off the node from the diagnostic shell.

The web console will no longer be accessible if ILOM is reset. You can power off the server from the serial console or with the power button.

Related Topics:

- Secure Eraser Syntax (page 5-14)
  The Secure Eraser utility has several option.
- Securely Erasing Oracle Exadata Database Machine Servers (My Oracle Support Doc ID 2180963.1)

5.5 Interactive Secure Erasure through External USB

You can securely erase a node using an external USB drive.

Before you begin:

- Review My Oracle Support note 2180963.1 for the latest information and to download the Secure Eraser package.
• Make sure you have an external USB.
• Make sure you have physical access to the nodes to be erased.

1. Copy the diagnostic image from the Secure Eraser package to an external USB.

   `# dd if=PATH_TO_DIAGNOSTIC_IMAGE of=USB_DEVICE`

   For example:
   
   `# dd if=image_diagnostics_12.2.1.1.0_LINUX.X64_161015-1.x86_64.usb of=/dev/sdm`

2. Insert the external USB to the node to be securely erased.

   External USB slots are located at both the front panel and the back panel of 2-
   socket database servers and storage servers. On 8-socket database servers, external USB slots are located at the back panel.

3. Reboot the node from the external USB by pressing **CTRL+P** after BIOS initialization splash screens and selecting the inserted external USB device.

4. Login to the server.
   
   a. If you are erasing a storage server, then login to the diagnostic shell.

      Enter `e` to enter the diagnostic shell as follows:

      Choose from following by typing letter in '()':
      (e)nter interactive diagnostics shell. Must use credentials from Oracle support to login (reboot or power cycle to exit the shell),
      Select:e

   b. If you are erasing database servers, then log in as the **root** user.

      You will be prompted for the password for the **root** user of diagnostic shell. The password can be retrieved from Oracle Support.

      localhost login: root
      Password: *********
      -sh-3.1#

5. Run the Secure Eraser utility to sanitize all devices or one type of device.

   For example, to erase all devices:

   `-sh-3.1# /usr/sbin/secureeraser -- erase --all --output=/mnt/iso`

   To erase just the hard drives:

   `-sh-3.1# /usr/sbin/secureeraser -- erase --hdd --output=/mnt/iso`

   By default, `/mnt/iso` is the mount point for the external USB when system is booted from the diagnostic ISO on the external USB. It is important to point the output option to the external USB mount point `/mnt/iso` so that the certificate can be saved properly.

6. Secure Eraser prompts you with a list of devices to be erased. Confirm that you want to proceed with the secure erasure.

   A progress report, as shown in step 7 of Automatic Secure Erasure through PXE Boot (page 5-5), is printed to the console every 10 seconds.

   In interactive mode, the server will be left on after the specified devices are securely erased. You can power off the node from the diagnostic shell.
The web console will no longer be accessible if ILOM is reset. You need to power off the server from the serial console or with the power button.

Related Topics:
- Secure Eraser Syntax (page 5-14)
- Securely Erasing Oracle Exadata Database Machine Servers (My Oracle Support Doc ID 2180963.1)

5.6 Secure Eraser Syntax

The Secure Eraser utility has several options.

Usage:
secureeraser [options]

Table 5-2 Command-Line Options for Secure Eraser

<table>
<thead>
<tr>
<th>Command-Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--list</td>
<td>List devices (hard drives, flash devices, USB devices, and ILOM) on the system.</td>
</tr>
<tr>
<td>--erase</td>
<td>Perform secure erasure of data.</td>
</tr>
<tr>
<td>-q, --quiet</td>
<td>Quietly skip prompts.</td>
</tr>
<tr>
<td>--all</td>
<td>Perform the action (--list or --erase) on all devices on the system. Devices include hard drives, flash devices, USB devices, and ILOM.</td>
</tr>
<tr>
<td>--hdd</td>
<td>Erase all hard drives.</td>
</tr>
<tr>
<td>--hdd_erasure_method=HDD_ERASURE_METHOD</td>
<td>Erase all hard drives using the specified method. The following values are supported:</td>
</tr>
<tr>
<td></td>
<td>• 3pass</td>
</tr>
<tr>
<td></td>
<td>• 7pass</td>
</tr>
<tr>
<td>--flash</td>
<td>Erase all flash devices.</td>
</tr>
<tr>
<td>--flash_erasure_method=FLASH_ERASURE_METHOD</td>
<td>Erase all flash devices using the specified method. The following values are supported:</td>
</tr>
<tr>
<td></td>
<td>• 3pass</td>
</tr>
<tr>
<td></td>
<td>• 7pass</td>
</tr>
<tr>
<td>--usb</td>
<td>Erase all internal USB devices.</td>
</tr>
<tr>
<td>--usb_erasure_method=USB_ERASURE_METHOD</td>
<td>Erase all internal USB devices using the specified method. The following values are supported:</td>
</tr>
<tr>
<td></td>
<td>• 3pass</td>
</tr>
<tr>
<td></td>
<td>• 7pass</td>
</tr>
<tr>
<td>--ilom</td>
<td>Reset ILOM to factory default.</td>
</tr>
</tbody>
</table>
Table 5-2  (Cont.) Command-Line Options for Secure Eraser

<table>
<thead>
<tr>
<th>Command-Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t TECHNICIAN_NAME, --technician=TECHNICIAN_NAME</td>
<td>Specify the name of the technician performing the erasure. This name will be recorded in the certificate.</td>
</tr>
<tr>
<td>-w WITNESS_NAME, --witness=WITNESS_NAME</td>
<td>Specify the name of the person witnessing the erasure. This name will be recorded in the certificate.</td>
</tr>
<tr>
<td>-o, --output=CERTIFICATE_DIRECTORY</td>
<td>Specify a full path to the directory for the certificate output location. The default is /var/log/cellos.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Show this help message and exit.</td>
</tr>
</tbody>
</table>

Examples

List all devices (hard drives, flash devices, USB devices, and ILOM) on the system.
secureeraser --list --all

List all hard drives.
secureeraser --list --hdd

Securely erase all devices, and enter the names of the technician and witness in the certificate.
secureeraser --erase --all --technician="jdoe" --witness="jsmith"

Reset ILOM to factory default.
secureeraser --erase --ilom

Securely erase all hard drives.
secureeraser --erase --hdd

Securely erase all hard drives, all flash devices, and all internal USB devices. Force "3-pass" method on flash devices.
secureeraser --erase --hdd --flash --usb --flash_erasure_method 3pass

5.7 Resetting InfiniBand Switches, Ethernet Switch, and Power Distribution Units to Factory Default

Before you begin:

- Review My Oracle Support note 2180963.1 for the latest information and to download the Secure Eraser package
• Print out the Exadata Factory Reset Certificate template in the Secure Eraser package.

The following figure shows the Factory Reset certificate:

**Figure 5-2  Factory Reset Certificate**

![Factory Reset Certificate](image)

This is to certify the following components have been reset to factory default.

<table>
<thead>
<tr>
<th>Component</th>
<th>Serial Number</th>
<th>Technician's Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Datacenter InfiniBand Switch 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sun Datacenter InfiniBand Switch 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sun Datacenter InfiniBand Switch 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sun Datacenter InfiniBand Switch 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 4948 Ethernet Switch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Distribution Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Distribution Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics:**

• Securely Erasing Oracle Exadata Database Machine Servers (My Oracle Support Doc ID 2180963.1)

5.7.1 Resetting InfiniBand Switches to Factory Default

To reset Sun Datacenter InfiniBand Switch 36 to factory default, refer to My Oracle Support note 2180877.1.

Record the serial numbers of the switches that have been reset to factory default in the Exadata Factory Reset certificate template. Sign and date the entries.

You can identify the serial number of an InfiniBand switch by running the following command on the switch:

```
[root@switch1 ~]# version | grep "Serial Number"
```

**Related Topics:**

• Sun Datacenter InfiniBand Switch Reset to Factory Default Setting (My Oracle Support Doc ID 2180877.1)
5.7.2 Resetting Ethernet Switch to Factory Default

To reset Ethernet switch to factory default, refer to the Sun Rack II Power Distribution Units User's Guide.

Record the serial number of the Ethernet switch that has been reset to factory default in the Exadata Factory Reset certificate template. Sign and date the entry.

The serial number of an Ethernet switch can be identified by the “Processor board ID” field in the “show version” command output.

Switch# show version

See Also:


5.7.3 Resetting Power Distribution Units to Factory Default

There are two types of power distribution units (PDUs): original PDUs and enhanced PDUs. Enhanced PDUs have SER MGT port that can be connected to a host using an RS-232 cable, whereas the original PDUs do not have SER MGT port. Typically, Exadata V2 to X3 racks have the original PDUs, and X4 and later have the enhanced PDUs.

You can reset both the original power distribution units and the enhanced power distribution units, as described in the Sun Rack II Power Distribution Units User's Guide.

Record the serial numbers of the power distribution units that have been reset to factory default in the Exadata Factory Reset certificate template. Sign and date the entries.

The serial number can be found on the “Module Information” page of the PDU web interface, as described in the Sun Rack II Power Distribution Units User's Guide.

For enhanced PDUs, the serial number can also be retrieved through the following CLI command:

pducli -> get pdu_serial_number
See Also:

- "Restore the PDU to Factory Default Settings (Original PDU)" in Sun Rack II Power Distribution Units User’s Guide
- "Restore the PDU to Factory Default Settings (Enhanced PDU)" in Sun Rack II Power Distribution Units User’s Guide
- "View Module Information (Original PDU)" in Sun Rack II Power Distribution Units User’s Guide
- "View Module Information (Enhanced PDU)" in Sun Rack II Power Distribution Units User’s Guide
Index

Symbols
1 Gbps Ethernet, 1-1
10 Gbps Ethernet, 1-1

A
access policies, 2-2
accessing ILOMs, 2-6
accountability, 1-3
accounting, 1-1
auditing, 1-1
authentication, 1-1
authorization, 1-1

ciphers, 4-1
classification strategies, 2-2
classifying data, 2-2
client access
isolating, 2-1
client access network, 1-1
cryptographic services, 2-4

database-scoped security, 2-4
default passwords, 3-5
denial of service attacks, 2-5
Diffie-Hellman, 2-4
disposing old hard drives, 4-5

E
enabling multiple databases, 2-6
encrypting
backups, 3-1
JDBC traffic, 2-4
Oracle Net Services, 2-4
traffic, 3-1
erasing data on drives, 5-4
Ethernet security guidelines, 3-1
event accountability, 1-3

F
FIPS 140-2, 4-1

H
hardening, 2-1

I
ILOM (Integrated Lights Out Manager), 2-4, 2-6
inetd, 3-7
instant secure erase (ISE), 5-4
Intel AES-NI, 2-4
IORM, 2-6
IORM (I/O Resource Manager), 2-6
IPMI v2.0, 2-6
isolating
client access, 2-1
management access, 2-1
multiple databases, 2-2

K
Kerberos, 2-3

L
LDAP repositories, 2-3
logical realms, 2-2

M
MAC (Media Access Control), 3-1
management access
isolating, 2-1
management network, 1-1
Media Access Control
See MAC
monitoring user logins, 1-1

N
networks
networks (continued)
  client access, 1-1
  management, 1-1

O
  open security, 2-3
  Oracle Advanced Security
    cryptographic services, 2-4
    encrypting traffic, 3-1
  Oracle ASM-scoped security, 2-3
  Oracle Audit Vault
    enabling proactive detection, 2-5
    managing database audits, 2-5
  Oracle Data Guard, 3-1
  Oracle Database Firewall Remote Monitor, 2-5
  Oracle Database Quality of Service Management
    monitoring workload requests, 2-6
  Oracle Database Resource Manager
    See Resource Manager
  Oracle Database security products, 4-1
  Oracle Database Vault
    managing access, 2-3
    mandatory access control, 2-2
  Oracle Enterprise User Security, 2-3
  Oracle Exadata Deployment Assistant, 3-8
  Oracle Label Security, 2-2
  Oracle Recovery Manager, 2-1
  Oracle Virtual Private Database, 2-2
  out-of-band, 3-1

P
  password policies, 3-8
  preventing resource exhaustion attacks, 2-5
  public key credentials, 2-3

R
  RADIUS, 2-3

Resource Manager (Oracle Database Resource Manager), 2-6
  RMAN (Oracle Recovery Manager)
    encrypting backups, 3-1
    row level isolation, 2-2

S
  secure erase, 5-4
  secure isolation levels, 2-1
  secure lights-out management, 2-6
  Secure Shell
    See SSH
  securing communications, 2-4
  security considerations, 3-1
  separation of duties, 2-3
  serial numbers, 1-1
  SNMPv3, 2-6
  SSH (Secure Shell), 2-4, 2-6, 4-1
  SSH protocol 2 (SSH2), 4-1
  SSL/TLS, 2-4

T
  TDE (Transparent Data Encryption), 2-4, 3-1
  tracking hardware assets, 1-1
  Transparent Data Encryption
    See TDE

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

X
  X.509 certificates, 2-4