

Oracle Exadata Storage Server

Security Configuration Supplement for the
United States Department of Defense





Table of Contents

| | |
|--|----|
| Overview | 4 |
| Product Description | 4 |
| Product Security Guide | 4 |
| Version and Update Information | 5 |
| Security Configuration Information | 5 |
| Default Accounts and Passwords | 5 |
| Default Exposed Network Services | 6 |
| Security Configuration Hardening | 6 |
| Implement Oracle ILOM Security Configuration Hardening | 6 |
| Configure a System Boot Loader Password | 7 |
| Disable Oracle ILOM System Console Access | 7 |
| Restrict Remote Root Access Using Secure Shell | 7 |
| Configure System Account Lockout | 7 |
| Configure Password Complexity Rules | 8 |
| Configure Password History Policy | 9 |
| Configure Failed Authentication Lock Delay | 9 |
| Password Aging Control Policies | 9 |
| Configure Administrative Interface Inactivity Timeout (Login Shell) | 10 |
| Configure Administrative Interface Inactivity Timeout (Secure Shell) | 10 |
| Configure Login Warning Banner | 10 |
| Limiting Remote Network Access | 11 |
| Management Network Recommendations | 11 |



| | |
|---|----|
| Commonly Reported Security Findings and Recommendations | 12 |
| Additional Information | 12 |

Overview

United States Department of Defense (DoD) Instruction 8500.01 (effective March 2014) instructs DoD Component Heads to "ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs with any exceptions documented and approved by the responsible authorizing official (AO)." Within the DoD, Security Technical Implementation Guides (STIGs) help to define the security configuration baselines for IA and IA-enabled devices. Specifically, STIGs contain prescriptive steps that can be used to both assess and improve the security configuration of systems and devices deployed on DoD networks. For more information on DoD STIGs, see: <http://iase.disa.mil/stigs/Pages/index.aspx>.

As of this white paper's publication, STIGs can only be developed when they align to one of the published DoD Security Requirements Guides (SRGs) per the STIG development vendor process, documented at: <http://iase.disa.mil/stigs/Pages/vendor-process.aspx>. Unfortunately, while the published SRGs map to common technology areas, there is no suitable SRG for IT appliances. As a result, there is no published STIG for the Oracle Exadata Storage Server product as it is a dedicated, fixed-function appliance.

To mitigate this shortcoming, this technical white paper will provide prescriptive security configuration hardening guidance that will allow DoD customers to improve upon the default security configuration of the Oracle Exadata Storage Server in a manner suitable to what would otherwise have been published as a DoD STIG.

Product Description

The Oracle Exadata Storage Server is the storage building block of the Oracle Exadata Database Machine, Oracle SuperCluster and Oracle Exadata Storage Expansion Rack. Each Oracle Exadata Storage Server is delivered to customers pre-installed and integrated with all of its necessary compute, storage, and software components. Customers are only permitted to make changes to the configuration through the application of approved methods, patches or updates. The Oracle Exadata Storage Server software may not be altered in any other manner.

Product Security Guide

This white paper is intended to provide common information and procedures necessary to improve the "out of the box" security configuration of this product. The security guide for the Oracle Exadata Storage Server, available as a standard part of the Oracle product documentation, has additional information on the product's security features, capabilities and configuration options. It is strongly recommended that customers review the product security guide before implementing the recommendations contained within this technical white paper.

» Oracle Exadata Storage Server Software User's Guide 12c Release 1 (Part Number: E50471-05)

The Oracle Exadata Storage Server documentation is not currently publicly available. Rather, it is included with each physical Exadata Storage Server. Always review the correct version of the product security guide as the security features, capabilities and configuration options will often vary based upon product version.

In addition, customers are encouraged to also review the product security guides associated with any relevant Oracle Engineered Systems that incorporate Oracle Exadata Storage Servers, such as:

- » Oracle Exadata Database Machine Security Guide 12c Release 1 (Part Number: E50469-02)
- » Oracle SuperCluster System Security Guide (Part Number: E26202-02)

Version and Update Information

To leverage the most recent features, capabilities and security enhancements, customers are encouraged to update their Oracle Exadata Storage Servers to the latest, supported version for their respective platform. To determine the version of the Oracle Exadata Storage Server software that is being used on the platform, execute the following command after first logging into the Oracle Exadata Storage Server.

```
# imageinfo | grep "Active image version:"  
Active image version: 12.1.1.1.1.140712
```

In the above example, the Oracle Exadata Storage Server is version 12.1.1.1.1.140712. For more information on updating Oracle Exadata Storage Servers, see the "Maintaining Exadata Storage Servers" section in the Oracle Exadata Database Machine Maintenance Guide 12c Release 1 (Part Number: E51951-03).

Security Configuration Information

Default Accounts and Passwords

This section describes the default accounts and passwords associated with this device:

ORACLE EXADATA STORAGE SERVER DEFAULT ACCOUNTS AND PASSWORDS

| Account Name | Account Type | Default Password | Account Description |
|--------------|--------------------|------------------|---|
| root | Administrator | welcome1 | The <code>root</code> account is used to access the Oracle Exadata Storage Server operating system. This account is used to perform general administrative actions as well as to update the Oracle Exadata Storage Server software. |
| celladmin | Cell Administrator | welcome1 | This account is used for to perform Oracle Exadata Storage Server set up and configuration. In addition, all storage services on the platform operate using this account. |
| cellmonitor | Monitoring | welcome1 | This account is used for monitoring purposes only. This account leverages a restricted shell to ensure that the configuration and objects residing on the Oracle Exadata Storage Server cannot be modified from this account. |

To change a default password, use the `passwd` command at the operating system prompt:

```
# passwd <account name>
```

Most customer environments will employ multiple Oracle Exadata Storage Servers. To change a user's password across all of the servers, the DCLI utility can be used:

```
dcli -g cell_group -l root "echo <new_password> | passwd --stdin <account_name>"
```

In the above example, `cell_group` is a simple text file listing the host names of all of the Oracle Exadata Storage Servers (one per line). The value `new_password` is the value that will be used as the new password. This value should be changed to something that is appropriate for the environment and compliant with site policy. Finally, the `account_name` value should be replaced with the name of the Oracle Linux account whose password is to be changed.

Default Exposed Network Services

This section describes the default network services that are exposed by this device:

ORACLE EXADATA STORAGE SERVER DEFAULT EXPOSED NETWORK SERVICES

| Service Name | Protocol | Port | Service Description |
|--------------|----------|------|--|
| SSH | TCP | 22 | <p>This port is used by the Secure Shell service integrated into the Oracle Exadata Storage Server software to provide administrative access to the system using a command-line interface.</p> <p>By default, the Secure Shell server is configured to respond to connection requests only on the management (NET0) and InfiniBand (BONDIB0) networks.</p> |

The Oracle Exadata Storage Server also communicates with Oracle Database Servers using the Reliable Datagram Sockets (RDSv3) protocol over remote direct memory access (RDMA) interfaces. This point-to-point communication does not use TCP/IP and is limited to the internal InfiniBand network partition onto which both the Oracle Database Servers and Oracle Exadata Storage Servers reside.

Security Configuration Hardening

The `host_access_control` command, available as of Exadata software version 11.2.3.3.0, is utilized to implement a limited set of access and security configuration settings, including: restricting remote root access, restricting network access to certain accounts, implementing password aging and complexity policies, implementing login warning banners, defining account lockout and session timeout policies, etc. For more information, use the command:

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

The `host_access_control` utility, although officially undocumented, is the only permitted and supported method to implement security configuration changes on the Oracle Exadata Storage Servers. Customers are not permitted to make manual changes to the configuration of these devices per Oracle Support notice 1068804.1. Further, before using this tool, customers must first obtain explicit approval from Oracle Product Development to change the security configuration of their Oracle Exadata Storage Servers. To request this approval, customers must open a service request with Oracle Support.

Implement Oracle ILOM Security Configuration Hardening

The Oracle Exadata Storage Server includes an embedded Oracle Integrated Lights Out Manager as part of the product. As with other Oracle ILOM implementations, there are security relevant configuration changes that can be implemented to improve upon the default security configuration of the device. For more information, see the Oracle Integrated Lights Out Manager Security Configuration Supplement for the U.S. Department of Defense.

Configure a System Boot Loader Password

The Oracle Exadata Storage Servers can be configured to require a system boot loader password whenever an administrator attempts to access the boot loader (GRUB) editor or command interface.

To configure a system boot loader password, use the command:

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: <password>
Retype new GRUB password: <password>
[ ... ]
```

To determine the current status of this setting, use the command:

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoizETJwmNQsFnH9oFy.
```

If this command returns a value similar to the example above, then a boot loader password has been installed.

Disable Oracle ILOM System Console Access

Each of the Oracle Exadata Storage Servers includes an embedded Oracle Integrated Lights Out Manager (Oracle ILOM) to enable remote monitoring and management. The Oracle ILOM can also be used to provide remote access to the Oracle Exadata Storage Server system console.

To disable system console access from the Oracle ILOM, use the command:

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

Restrict Remote Root Access Using Secure Shell

By default, the `root` user is permitted to remotely access each of the Oracle Exadata Storage Servers.

To disable remote `root` access using Secure Shell, use the command:

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

To determine the current status of this setting, use the command:


```
# /opt/oracle.cellos/host_access_control rootssh --status
```

Configure System Account Lockout

By default, the Oracle Exadata Storage Servers are configured to lock system accounts after five consecutive failed authentication attempts.

To change this threshold, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```



To comply with U.S. Department of Defense security requirements, in the above example, the value of 3 is used as the actual limit. If necessary, replace that value with one that is compliant with local site policy.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

Configure Password Complexity Rules

By default, the Oracle Exadata Storage Servers do not implement any significant restrictions governing the complexity of system account passwords. To define a password complexity policy, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc <comma-separated-values>
```

The value `<comma-separated-values>` should be replaced with a comma-separated set of five values. These five values will collectively be used to set the actual system password complexity policy. The values, per the `passwdqc.conf(5)` manual page are as follows:

- » N0. This parameter is used for passwords consisting of only one character class (digits, lower case characters, upper case characters, and special characters). In general, this parameter is set to `disabled` as simple passwords such as these should be avoided.
- » N1. This parameter is used for passwords consisting of two characters classes that do not meet the requirements for a passphrase. For this rule to apply, the password must be at least `N1` characters in length.
- » N2. This parameter is used for passwords consisting of a passphrase. For this rule to apply, the password must be at least `N2` characters in length and must meet the passphrase requirement.
- » N3. This parameter is used for passwords consisting of at least three character classes. For this rule to apply, the password must be at least `N3` characters in length.
- » N4. This parameter is used for passwords consisting of at least four character classes. For this rule to apply, the password must be at least `N4` characters in length.

To comply with U.S. Department of Defense security requirements, it is recommended that the `<comma-separated-values>` parameter be set to `"disabled,disabled,disabled,disabled,15"`. This will ensure that the only passwords that will be accepted will consist of at least four characters classes (upper case, lower case, numeric, and special) and be at least 15 characters in length.

Note: 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.

To install this password complexity policy, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth \  
    --passwdqc disabled,disabled,disabled,disabled,15
```

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```


Configure Password History Policy

By default, the Oracle Exadata Storage Servers define a password history policy that prevents users from reusing their last ten (10) passwords.

To change the password history policy, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

To comply with U.S. Department of Defense security requirements, in the above example, the password history policy is set to 5. This will ensure that a system account will not reuse one of the last five passwords assigned to the account. If necessary, replace that value with one that is compliant with local site policy.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

Configure Failed Authentication Lock Delay

By default, the Oracle Exadata Storage Servers implement a policy where a system account will be locked for ten (10) minutes after any single failed authentication attempt.

To change this threshold, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

To comply with U.S. Department of Defense security requirements, in the above example, the value of 4 (seconds) is used as the actual limit. If necessary, replace that value with one that is compliant with local site policy.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

Password Aging Control Policies


The Oracle Exadata Storage Servers support a variety of password aging controls including parameters to control the maximum number of days a password is used, the minimum number of days between passwords changes, and the number of days in advance of password expiration that a user should be warned.

To comply with U.S. Department of Defense security requirements, the following parameters are recommended:

- » Maximum Password Lifetime: 60 days (Oracle Default: 90 days)
- » Minimum Password Lifetime: 1 day (Oracle Default: 1 day)
- » Minimum Password Length: 15 characters (Oracle Default: 8 characters)
- » Password Expiration Warning: 7 days (Oracle Default: 7 days)

To configure this recommended password aging policy, use the commands:

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```



To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

Configure Administrative Interface Inactivity Timeout (Login Shell)

The Oracle Exadata Storage Server supports the ability to terminate administrative sessions that have been inactive for more than some pre-defined number of seconds.

To define the administrative interface inactivity timeout for a system account login shell, use the command:

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

To comply with U.S. Department of Defense security requirements, in the above example, the value of 900 (seconds) is used as the actual limit. If necessary, replace that value with one that is compliant with local site policy.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

Configure Administrative Interface Inactivity Timeout (Secure Shell)

The Oracle Exadata Storage Server supports the ability to terminate administrative sessions that have been inactive for more than some pre-defined number of seconds.

To define the administrative interface inactivity timeout for a Secure Shell session, use the command:

```
# /opt/oracle.cellos/host_access_control idle-timeout --client 900
```

To comply with U.S. Department of Defense security requirements, in the above example, the value of 900 (seconds) is used as the actual limit. If necessary, replace that value with one that is compliant with local site policy.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

Configure Login Warning Banner

The Oracle Exadata Storage Server supports the ability to display customer-specific messages before a user has successfully authenticated to the system.

To define a pre-authentication login warning banner, use the command:

```
# /opt/oracle.cellos/host_access_control banner --file <filename>
```

To comply with U.S. Department of Defense security requirements, in the above example, the value of <filename> should be replaced with the path and name of an actual file that contains the approved login warning banner message.

To determine the current status of this setting, use the command:

```
# /opt/oracle.cellos/host_access_control banner --status
```

Limiting Remote Network Access

Inbound network access to the Oracle Exadata Storage Server may be restricted by the implementation of a top-down filtering rule set that defines access by user account and origin. A custom rule set may also be created and managed to allow or deny access according to U.S. Department of Defense security requirements. Configurable parameters for this command include allowing and denying access based on:

- » Username. Valid values include either the keyword "all" or one or more valid, local account user names.
- » Origin. Valid values include either the keyword "all" or individual entries that describe the source of system access including from the console, virtual console, ILOM, IP address, network address, host name, or DNS domain.

The recommended method to create and implement a rule set is to first export the existing access control rules, save as a backup copy, make edits using a text editor or command line edit utility, and finally import and implement the modified rules.

To examine the active rule set, use the command:

```
# /opt/oracle.cellos/host_access_control access --status
```

To implement an open rule set that removes inbound network restrictions, use the command:

```
# /opt/oracle.cellos/host_access_control access-open
```

To implement a closed rule set that will only permit inbound access using Secure Shell, use the command:

```
# /opt/oracle.cellos/host_access_control access-close
```

To export the current rule set to an ASCII text file, use the command:

```
# /opt/oracle.cellos/host_access_control access-export --file <filename>
```

To import a custom rule set and override the existing rule set, use the command:

```
# /opt/oracle.cellos/host_access_control access-import --file <filename>
```

To add specific rules individually, use the command:

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \  
--origins trustedhost.example.org,.trusted.domain.com
```

In this last example, access to the Oracle Exadata Storage Server is granted to the "celladmin" user when the connection is initiated from the host, `trusted.example.org`, or any host within the domain, `.trusted.domain.com`.

Note: Use caution when implementing non-default policies to ensure that access to the system is not interrupted. Further, when adding new individual rules, be aware that these changes will take effect immediately.

Management Network Recommendations

In addition to the above security hardening procedures, the Oracle Exadata Storage server is intended to be deployed on a dedicated, isolated management network. This will help to shield the Oracle Exadata Storage server from unauthorized or unintended network traffic. Access to this management network should be strictly controlled with access granted only to those administrators requiring this level of access.



Commonly Reported Security Findings and Recommendations

The following issues may be reported by some commercial and/or open-source vulnerability scanners when configured to assess the security posture of the Oracle Exadata Storage Server. This section is intended to provide information on commonly reported findings as well as specific technical recommendations to respond to these findings.

There were no security findings reported as of the time this white paper was written.

Additional Information

For more information describing the features and capabilities of the Exadata Storage Server as well as detailed technical instructions for the installation, configuration and management of this product, refer to the Oracle product documentation. The Oracle Exadata Storage Server documentation is not currently publicly available. Rather, it is included with each Oracle Exadata Storage Server.



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US



Hardware and Software, Engineered to Work Together

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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. 0215

Oracle Exadata Storage Server Security Configuration Supplement for the United States Department of Defense
February 2015
Author: Richard Qualls
Contributing Authors: Glenn Brunette



Oracle is committed to developing practices and products that help protect the environment