Oracle® Argus Mart

Minimum Security Configuration Guide

Release 8.2.1
F28464-02
June 2020

Oracle Argus Mart Minimum Security Configuration Guide, Release 8.2.1

F28464-02

Copyright © 2019, 2020, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

Preface

Documentation accessibility iv
Related resources iv
Access to Oracle Support iv

1 Minimum Security Configuration Guide

Establish SQLPLUS Connection 1-1
Configure Strong Password on the Database and WLS 1-1
Close All Open Ports not in Use 1-2
Disable the Telnet Service 1-2
Disable Other Unused Services 1-2
(Optional) Encrypt Tablespaces using the Oracle Advanced Security TDE 1-2

Preface

This preface contains the following sections:

- Documentation accessibility
- Related resources
- Access to Oracle Support
  To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

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.

Related resources

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

Cloud customers receive support assistance through Support Cloud

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

On-premises customers receive support assistance through My 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.

1

Minimum Security Configuration Guide

This guide describes essential security management guidelines and recommendations for the Oracle Argus Mart application. It contains the following topics:

- Establish SQLPLUS Connection
- Configure Strong Password on the Database and WLS
- Close All Open Ports not in Use
- Disable the Telnet Service
- Disable Other Unused Services
- (Optional) Encrypt Tablespaces using the Oracle Advanced Security TDE

Establish SQLPLUS Connection

To connect to SQLPLUS, execute the following steps:

1. Open a command prompt in Windows.

   Alternatively, in Unix, type at the shell prompt.
2. Enter the *sqlplus <dbuser>@<tnsnames_entry>* command, and press **Enter**.
3. Enter the password when prompted by the SQLPLUS program.

   You must not enter the password in the same command line that is used while calling the SQLPLUS program.

Configure Strong Password on the Database and WLS

Although the importance of passwords is well-known, the following basic rule of security management is worth repeating:

Make sure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the Oracle Database Security Guide specific to the database release you are using.You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the weblogic server default accounts, such as weblogic.
- Password for the database listener. If you do not configure the database listener to require an authorization password, you unnecessarily expose the underlying database service names to unauthorized individuals.

Close All Open Ports not in Use

Keep only a minimum number of ports open. You should close all ports that are not in use.

Disable the Telnet Service

The Oracle Argus Mart application does not use the Telnet service. Telnet listens on port 23 by default. If the Telnet service is available on the Oracle Argus Mart host machine, Oracle recommends that you disable Telnet in favor of Secure Shell (ssh). Telnet, which sends clear-text passwords and user names through a login, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

Disable Other Unused Services

In addition to not using Telnet, the Oracle Argus Mart application does not use the following services or information for any functionality:

- **Simple Mail Transfer Protocol (SMTP)—**This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- **Identification Protocol (identd)—**This protocol is generally used to identify the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP)—**This protocol is one method for managing and reporting information about different systems.

Therefore, restricting these services or information will not affect the Oracle Argus Mart application. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure.

If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

(Optional) Encrypt Tablespaces using the Oracle Advanced Security TDE

Oracle Database Transparent Data Encryption (TDE) feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 12c (https://docs.oracle.com/database/121/ASOAG, or

http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html

TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications.

Oracle Argus Mart product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature.