

Oracle® Enterprise Manager

Policy Reference Manual

10g Release 2 (10.2)

B16231-01

December 2005

Copyright © 2005, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

| | |
|----------------------------------------------------------------------------------------------|------|
| Preface | ix |
| Audience | ix |
| Documentation Accessibility | ix |
| Related Documents | x |
| Conventions | x |
| | |
| How to Use This Manual | xi |
| Organization of Policy Text | xi |
| Background Information on Policies | xiii |
| | |
| 1 Automatic Storage Management (ASM) Policies | |
| 1.1 Disk Group Contains Disks of Significantly Different Sizes | 1-1 |
| 1.2 Disk Group Contains Disks with Different Redundancy Attributes | 1-2 |
| 1.3 Disk Group Depends on External Redundancy and Has Unprotected Disks | 1-2 |
| 1.4 Disk Group with NORMAL or HIGH Redundancy Has Mirrored or Parity Protected Disks..... | 1-3 |
| | |
| 2 BEA WebLogic Managed Server Policies | |
| 2.1 WebLogic Admin Port Enabled | 2-1 |
| 2.2 WebLogic Performance Pack Enabled | 2-2 |
| 2.3 WebLogic Production Mode Enabled | 2-2 |
| | |
| 3 Calendar Server Policy | |
| 3.1 High Log Level..... | 3-1 |
| | |
| 4 Cluster Database Policies | |
| 4.1 Configuration Policies | 4-1 |
| 4.1.1 Force Logging Disabled | 4-1 |
| 4.1.2 Installation of JAccelerator (NCOMP)..... | 4-2 |
| 4.1.3 Insufficient Number of Control Files | 4-3 |
| 4.1.4 Insufficient Number of Redo Logs | 4-3 |
| 4.1.5 Recovery Area Location Not Set..... | 4-4 |
| 4.2 Security Policies - UNIX..... | 4-5 |
| 4.2.1 Access to ALL_SOURCE View | 4-5 |

| | | |
|--------|----------------------------------------------------------------------------|------|
| 4.2.2 | Access to DBA Role Privileges View | 4-6 |
| 4.2.3 | Access to DBA Roles View | 4-6 |
| 4.2.4 | Access to DBA_SYS_PRIVS View | 4-7 |
| 4.2.5 | Access to DBA_TAB_PRIVS View | 4-8 |
| 4.2.6 | Access to DBA_USERS View | 4-8 |
| 4.2.7 | Access to ROLE_ROLE_PRIVS View | 4-9 |
| 4.2.8 | Access to STATS\$SQL Summary Table | 4-10 |
| 4.2.9 | Access to STATS\$SQL Text Table | 4-10 |
| 4.2.10 | Access to SYS.AUDIT\$ Table | 4-11 |
| 4.2.11 | Access to SYS.LINK\$ Table | 4-11 |
| 4.2.12 | Access to SYS.SOURCE\$ Table | 4-12 |
| 4.2.13 | Access to SYS.USER\$ Table | 4-13 |
| 4.2.14 | Access to SYS.USER_HISTORY\$ Table | 4-13 |
| 4.2.15 | Access to USER_ROLE_PRIVS View | 4-14 |
| 4.2.16 | Access to USER_TAB_PRIVS View | 4-14 |
| 4.2.17 | Control File Permission | 4-15 |
| 4.2.18 | Default Passwords | 4-16 |
| 4.2.19 | Excessive Allowed Failed Login Attempts | 4-16 |
| 4.2.20 | Excessive PUBLIC EXECUTE Privileges | 4-17 |
| 4.2.21 | Execute UTL_FILE Privileges to PUBLIC | 4-18 |
| 4.2.22 | Oracle Home Datafile Permission | 4-18 |
| 4.2.23 | Password Grace Time | 4-19 |
| 4.2.24 | Password Life Time | 4-20 |
| 4.2.25 | Password Locking Time | 4-20 |
| 4.2.26 | Password Reuse Maximum | 4-21 |
| 4.2.27 | Password Reuse Time | 4-22 |
| 4.2.28 | Profiles with Excessive Allowed Failed Login Attempts | 4-22 |
| 4.2.29 | PUBLIC EXECUTE Privileges to DBMS Job | 4-23 |
| 4.2.30 | PUBLIC EXECUTE Privileges to DBMS LOB | 4-24 |
| 4.2.31 | PUBLIC EXECUTE Privileges to DBMS SYS SQL | 4-24 |
| 4.2.32 | System Privileges to Public | 4-25 |
| 4.2.33 | Unlimited Tablespace Quota | 4-26 |
| 4.2.34 | Use of Database Links with Cleartext Password | 4-26 |
| 4.2.35 | Well Known Accounts | 4-27 |
| 4.2.36 | Well Known Accounts (Status) | 4-28 |
| 4.3 | Security Policies - Windows | 4-28 |
| 4.3.1 | Control File Permission (Windows) | 4-28 |
| 4.3.2 | Oracle Home Datafile Permission (Windows) | 4-29 |
| 4.4 | Storage Policies | 4-30 |
| 4.4.1 | Default Permanent Tablespace Set to a System Tablespace | 4-30 |
| 4.4.2 | Default Temporary Tablespace Set to a System Tablespace | 4-31 |
| 4.4.3 | Dictionary Managed Tablespaces | 4-32 |
| 4.4.4 | Insufficient Redo Log Size | 4-33 |
| 4.4.5 | Non-System Data Segments in a System Tablespace | 4-33 |
| 4.4.6 | Non-Uniform Default Extent Size for Dictionary Managed Tablespaces | 4-34 |
| 4.4.7 | Rollback in SYSTEM Tablespace | 4-35 |
| 4.4.8 | Segment in Dictionary Tablespace with Extent Growth Policy Violation | 4-36 |

| | | |
|--------|---------------------------------------------------------------|------|
| 4.4.9 | Tablespace Not Using Automatic Segment-Space Management | 4-37 |
| 4.4.10 | Tablespaces Containing Rollback and Data Segments..... | 4-38 |
| 4.4.11 | Users with a System Tablespace as Default Tablespace | 4-39 |
| 4.4.12 | Users with Permanent Tablespace as Temporary Tablespace | 4-40 |

5 Database Instance Policies

| | | |
|--------|-----------------------------------------------------|------|
| 5.1 | Configuration Policies | 5-1 |
| 5.1.1 | Disabled Automatic Statistics Collection | 5-1 |
| 5.1.2 | Force Logging Disabled | 5-2 |
| 5.1.3 | Installation of JAccelerator (NCOMP) | 5-3 |
| 5.1.4 | Insufficient Number of Control Files | 5-3 |
| 5.1.5 | Insufficient Number of Redo Logs | 5-4 |
| 5.1.6 | Not Using Automatic PGA Management | 5-5 |
| 5.1.7 | Not Using Automatic Shared Memory Management | 5-6 |
| 5.1.8 | Not Using Automatic Undo Management..... | 5-7 |
| 5.1.9 | Not Using Latest Version of Optimizer..... | 5-8 |
| 5.1.10 | Not Using Spfile | 5-9 |
| 5.1.11 | Recovery Area Location Not Set..... | 5-10 |
| 5.1.12 | Statistics Level Parameter Set to ALL | 5-10 |
| 5.1.13 | Use of Non-Standard Initialization Parameters | 5-11 |
| 5.2 | Security Policies - UNIX..... | 5-12 |
| 5.2.1 | Access to ALL_SOURCE View | 5-12 |
| 5.2.2 | Access to DBA Role Privileges View | 5-12 |
| 5.2.3 | Access to DBA Roles View | 5-13 |
| 5.2.4 | Access to DBA_SYS_PRIVS View..... | 5-14 |
| 5.2.5 | Access to DBA_TAB_PRIVS View | 5-14 |
| 5.2.6 | Access to DBA_USERS View | 5-15 |
| 5.2.7 | Access to ROLE_ROLE_PRIVS View..... | 5-16 |
| 5.2.8 | Access to STAT\$SQL Summary Table..... | 5-16 |
| 5.2.9 | Access to STAT\$SQL Text Table | 5-17 |
| 5.2.10 | Access to SYS.AUDIT\$ Table | 5-17 |
| 5.2.11 | Access to SYS.LINK\$ Table | 5-18 |
| 5.2.12 | Access to SYS.SOURCE\$ Table..... | 5-19 |
| 5.2.13 | Access to SYS.USER\$ Table | 5-19 |
| 5.2.14 | Access to SYS.USER_HISTORY\$ Table | 5-20 |
| 5.2.15 | Access to USER_ROLE_PRIVS View | 5-20 |
| 5.2.16 | Access to USER_TAB_PRIVS View..... | 5-21 |
| 5.2.17 | Audit File Destination..... | 5-22 |
| 5.2.18 | Background Dump Destination..... | 5-22 |
| 5.2.19 | Control File Permission..... | 5-23 |
| 5.2.20 | Core Dump Destination..... | 5-24 |
| 5.2.21 | Default Passwords | 5-25 |
| 5.2.22 | Default Table Space | 5-25 |
| 5.2.23 | Excessive Allowed Failed Login Attempts | 5-26 |
| 5.2.24 | Excessive PUBLIC EXECUTE Privileges..... | 5-27 |
| 5.2.25 | Execute UTL_FILE Privileges to PUBLIC | 5-27 |
| 5.2.26 | IFILE Referenced File Permission..... | 5-28 |

| | | |
|--------|---------------------------------------------------------------------------------------------------|------|
| 5.2.27 | Initialization Parameter File Permission | 5-29 |
| 5.2.28 | Log Archive Destination Owner | 5-29 |
| 5.2.29 | Log Archive Destination Permission | 5-30 |
| 5.2.30 | Log Archive Duplex Destination Owner | 5-31 |
| 5.2.31 | Log Archive Duplex Destination Permission | 5-32 |
| 5.2.32 | Naming Database Links..... | 5-32 |
| 5.2.33 | Oracle Home Datafile Permission | 5-33 |
| 5.2.34 | Oracle Home Executable Files Owner | 5-34 |
| 5.2.35 | Oracle Home Executable Files Permission..... | 5-34 |
| 5.2.36 | Oracle Home File Permission..... | 5-35 |
| 5.2.37 | Password Grace Time..... | 5-36 |
| 5.2.38 | Password Life Time | 5-36 |
| 5.2.39 | Password Locking Time..... | 5-37 |
| 5.2.40 | Password Reuse Maximum..... | 5-38 |
| 5.2.41 | Password Reuse Time | 5-38 |
| 5.2.42 | Profiles with Excessive Allowed Failed Login Attempts..... | 5-39 |
| 5.2.43 | PUBLIC EXECUTE Privileges to DBMS Job | 5-40 |
| 5.2.44 | PUBLIC EXECUTE Privileges to DBMS LOB..... | 5-40 |
| 5.2.45 | PUBLIC EXECUTE Privileges to DBMS SYS SQL | 5-41 |
| 5.2.46 | PUBLIC Trace Files..... | 5-42 |
| 5.2.47 | Remote OS Authentication | 5-42 |
| 5.2.48 | Remote OS Role..... | 5-43 |
| 5.2.49 | Remote Password File | 5-44 |
| 5.2.50 | Secure OS Audit Level | 5-44 |
| 5.2.51 | Server Parameter File Permission..... | 5-45 |
| 5.2.52 | System Privileges to Public | 5-46 |
| 5.2.53 | Unlimited Tablespace Quota..... | 5-46 |
| 5.2.54 | Use of Appropriate umask on UNIX Systems..... | 5-47 |
| 5.2.55 | Use of Automatic Log Archival Features | 5-48 |
| 5.2.56 | Use of Basic Audit Features | 5-48 |
| 5.2.57 | Use of Database Links with Cleartext Password | 5-49 |
| 5.2.58 | Use of Remote Listener Instances..... | 5-50 |
| 5.2.59 | Use of SQL92 Security Features..... | 5-50 |
| 5.2.60 | User Dump Destination | 5-51 |
| 5.2.61 | User Temporary Table Space | 5-52 |
| 5.2.62 | Using Externally Identified Accounts..... | 5-53 |
| 5.2.63 | Utility File Directory Initialization Parameter Setting | 5-53 |
| 5.2.64 | Utility File Directory Initialization Parameter Setting for Oracle9i Release 1 and Later | 5-54 |
| 5.2.65 | Well Known Accounts | 5-55 |
| 5.2.66 | Well Known Accounts (Status)..... | 5-55 |
| 5.3 | Security Policies - Windows | 5-56 |
| 5.3.1 | Audit File Destination (Windows) | 5-56 |
| 5.3.2 | Background Dump Destination (Windows)..... | 5-57 |
| 5.3.3 | Control File Permission (Windows)..... | 5-57 |
| 5.3.4 | Core Dump Destination (Windows) | 5-58 |
| 5.3.5 | IFILE Referenced File Permission (Windows)..... | 5-59 |
| 5.3.6 | Initialization Parameter File Permission (Windows) | 5-60 |

| | | |
|--------|---------------------------------------------------------------------------|------|
| 5.3.7 | Log Archive Destination Permission (Windows) | 5-61 |
| 5.3.8 | Log Archive Duplex Destination Permission (Windows) | 5-62 |
| 5.3.9 | Oracle Home Datafile Permission (Windows) | 5-62 |
| 5.3.10 | Oracle Home Executable Files Permission (Windows)..... | 5-63 |
| 5.3.11 | Oracle Home File Permission (Windows)..... | 5-64 |
| 5.3.12 | Server Parameter File Permission (Windows)..... | 5-64 |
| 5.3.13 | Use of Windows NT Domain Prefix (Windows)..... | 5-65 |
| 5.3.14 | User Dump Destination (Windows) | 5-66 |
| 5.4 | Storage Policies..... | 5-67 |
| 5.4.1 | Default Permanent Tablespace Set to a System Tablespace | 5-67 |
| 5.4.2 | Default Temporary Tablespace Set to a System Tablespace..... | 5-68 |
| 5.4.3 | Dictionary Managed Tablespaces..... | 5-69 |
| 5.4.4 | Insufficient Redo Log Size | 5-69 |
| 5.4.5 | Non-System Data Segments in a System Tablespace | 5-70 |
| 5.4.6 | Non-Uniform Default Extent Size for Dictionary Managed Tablespaces | 5-71 |
| 5.4.7 | Rollback in SYSTEM Tablespace | 5-72 |
| 5.4.8 | Segment in Dictionary Tablespace with Extent Growth Policy Violation..... | 5-73 |
| 5.4.9 | Tablespace Not Using Automatic Segment-Space Management | 5-73 |
| 5.4.10 | Tablespaces Containing Rollback and Data Segments..... | 5-74 |
| 5.4.11 | Users with a System Tablespace as Default Tablespace | 5-75 |
| 5.4.12 | Users with Permanent Tablespace as Temporary Tablespace | 5-76 |

6 Host Policies

| | | |
|-------|-------------------------------------------------|-----|
| 6.1 | Configuration Policies..... | 6-1 |
| 6.1.1 | Critical Patch Advisories for Oracle Homes..... | 6-1 |
| 6.2 | Security Policies..... | 6-2 |
| 6.2.1 | Execute Stack | 6-2 |
| 6.2.2 | Insecure Services | 6-3 |
| 6.2.3 | NTFS File System..... | 6-4 |
| 6.2.4 | Open Ports | 6-4 |

7 Listener Policies

| | | |
|--------|---------------------------------------------|-----|
| 7.1 | Security Policies - UNIX..... | 7-1 |
| 7.1.1 | Allowed Logon Version..... | 7-1 |
| 7.1.2 | Listener Default Name | 7-2 |
| 7.1.3 | Listener Direct Administration..... | 7-2 |
| 7.1.4 | Listener Log File Owner | 7-3 |
| 7.1.5 | Listener Log File Permission..... | 7-4 |
| 7.1.6 | Listener Logging Status | 7-4 |
| 7.1.7 | Listener Password..... | 7-5 |
| 7.1.8 | Listener Trace Directory Owner | 7-5 |
| 7.1.9 | Listener Trace Directory Permission..... | 7-6 |
| 7.1.10 | Listener Trace File Owner | 7-7 |
| 7.1.11 | Listener Trace File Permission | 7-7 |
| 7.1.12 | Listener.ora Permission | 7-8 |
| 7.1.13 | Oracle Net Client Log Directory Owner | 7-9 |

| | | |
|--------|--------------------------------------------------------------|------|
| 7.1.14 | Oracle Net Client Log Directory Permission | 7-9 |
| 7.1.15 | Oracle Net Client Trace Directory Owner..... | 7-10 |
| 7.1.16 | Oracle Net Client Trace Directory Permission | 7-11 |
| 7.1.17 | Oracle Net Server Log Directory Owner..... | 7-11 |
| 7.1.18 | Oracle Net Server Log Directory Permission | 7-12 |
| 7.1.19 | Oracle Net Server Trace Directory Owner..... | 7-13 |
| 7.1.20 | Oracle Net Server Trace Directory Permission..... | 7-13 |
| 7.1.21 | Restrict sqlnet.ora Permissions | 7-14 |
| 7.1.22 | Use of Hostname in Listener.ora | 7-15 |
| 7.2 | Security Policies - Windows | 7-15 |
| 7.2.1 | Listener Log File Permission (Windows)..... | 7-15 |
| 7.2.2 | Listener Trace Directory Permission (Windows)..... | 7-16 |
| 7.2.3 | Listener Trace File Permission (Windows) | 7-17 |
| 7.2.4 | Listener.ora Permission (Windows)..... | 7-17 |
| 7.2.5 | Oracle Net Client Log Directory Permission (Windows) | 7-18 |
| 7.2.6 | Oracle Net Client Trace Directory Permission (Windows) | 7-19 |
| 7.2.7 | Oracle Net Server Log Directory Permission (Windows)..... | 7-20 |
| 7.2.8 | Oracle Net Server Trace Directory Permission (Windows)..... | 7-20 |
| 7.2.9 | Restrict sqlnet.ora Permissions (Windows) | 7-21 |

8 OC4J Policy

| | | |
|-----|---------------------------------|-----|
| 8.1 | OC4J Password Indirection | 8-1 |
|-----|---------------------------------|-----|

9 Oracle HTTP Server Policies

| | | |
|-------|---------------------------------------|-----|
| 9.1 | Configuration Policies..... | 9-1 |
| 9.1.1 | HTTP Server HostNameLookups | 9-1 |
| 9.1.2 | HTTP Server MaxKeepAliveRequests..... | 9-2 |
| 9.2 | Security Policies..... | 9-3 |
| 9.2.1 | HTTP Server Access Logging..... | 9-3 |
| 9.2.2 | HTTP Server Directory Indexing..... | 9-4 |
| 9.2.3 | HTTP Server Dummy Wallet..... | 9-4 |
| 9.2.4 | HTTP Server Owner And Setuid Bit..... | 9-5 |
| 9.2.5 | HTTP Server SSL..... | 9-6 |
| 9.2.6 | HTTP Server Writable Files..... | 9-7 |

10 Web Cache Policies

| | | |
|------|--------------------------------------|------|
| 10.1 | Web Cache Access Logging..... | 10-1 |
| 10.2 | Web Cache Dummy Wallet | 10-2 |
| 10.3 | Web Cache Owner and Setuid Bit | 10-3 |
| 10.4 | Web Cache Writable Files | 10-3 |

Preface

This manual is a compilation of the policies provided in Oracle Enterprise Manager. Through the Grid Control Console, you can access all the policies mentioned in this manual.

For additional information about policies, see the Enterprise Manager online help and *Oracle Enterprise Manager Concepts*.

Audience

This manual is intended for Oracle Enterprise Manager users interested in policies.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following manuals in the Oracle Enterprise Manager 10g Release 2 documentation set:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Quick Installation Guide*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Metric Reference Manual*
- *Oracle Enterprise Manager Extensibility*
- *Oracle Enterprise Manager Command Line Interface*
- *Oracle Enterprise Manager SNMP Support Reference Guide*
- *Oracle Enterprise Manager Licensing Information*

Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| boldface | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| <i>italic</i> | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

How to Use This Manual

The *Oracle Enterprise Manager Policy Reference Manual* (hereafter referred to as the *Policy Reference Manual*) lists all the Oracle defined target policies that Enterprise Manager monitors. This manual compiles in one place all the target policy help available online, eliminating the need to have the Grid Control Console up and running.

Organization of Policy Text

This manual contains a chapter for each Enterprise Manager target for which there are policies defined by Oracle. The policies in each chapter are in alphabetical order according to category.

Policy Information

The information for each policy comprises a description, summary of the policy's main properties, default values, impact of the violation, and action to perform when the violation occurs. The following list provides greater detail:

- **Description**
Defines the policy.
- **Policy Summary**
Summarizes in table format the severity, category, target type, versions affected, policy rule evaluation, automatically enabled, and alert message statistics for the policy.
- **Defaults**
Lists the parameters with their default values and objects that are excluded by default.
- **Impact of Violation**
Describes the effect of the policy violation on Enterprise Manager.
- **Action**
Provides guidelines to follow once the policy rule is violated.

Definitions of Columns in Policy Summary Tables

The Policy Summary table is part of the overall policy information. The following is an example of a customary Policy Summary table.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------------------|------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 7 days. | Yes | Disk Group %DISK_GROUP_NAME% contains disks with different redundancy attributes. This may offer inconsistent levels of data protection. |

¹ The policy rule is evaluated each time its underlying *osm_diskGroup_Policies* metric is collected.

The following table provides descriptions of columns in the Policy Summary table.

| Column Header | Column Definition |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity | Seriousness of the policy. Options are: Critical, Warning, and Informational. |
| Category | Classification of the policy. Options are: Configuration, Security, and Storage. |
| Target Type | Components monitored by Enterprise Manager, The target options are: Automatic Storage Management (ASM), BEA WebLogic Managed Server, Calendar Server, Cluster Database, Database Instance, Host, Listener, OC4J, Oracle HTTP Server, and Web Cache. |
| Versions Affected | Version of the target, for example, BEA WebLogic Server 7.1 or later. |
| Policy Rule Evaluation | Lists the underlying metric and that metric's collection frequency. |
| Automatically Enabled? | States whether the policy is enabled upon installation of Enterprise Manager. The possible values are <i>yes</i> and <i>no</i> . |
| Alert Message | Message indicating why the policy was violated. Words that display between percent signs (%) denote variables. For example, Disk Group %DISK_GROUP_NAME% could translate to Disk Group /dev/hda. |

Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

| Abbreviation/Acronym | Name |
|----------------------|-----------------------------------------------|
| ASM | Automatic Storage Management |
| Database | Oracle Database |
| DBA | Database Administrator |
| IP | Internet Protocol |
| FAT | File Allocation Table |
| FTP | File Transfer Protocol |
| HTTP | HyperText Transfer Protocol |
| HTTPd | HyperText Transfer Protocol daemon |
| LGWR | Log Writer Process |
| Listener | Oracle Listener |
| OC4J | Oracle Application Server Containers for J2EE |
| NCOMP | Natively Compiled |
| NTFS | NT File System |
| PGA | Program Global Area |

| Abbreviation/Acronym | Name |
|-----------------------------|-------------------------------|
| RAC | Real Application Cluster |
| SGA | System Global Area |
| SSL | Secure Sockets Layer |
| SSO | Single Sign-On |
| SMTP | Simple Mail Transfer Protocol |
| SPFILE | Server Parameter File |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

Background Information on Policies

A policy defines the desired behavior of systems and is associated with one or more targets or groups.

While a metric alert monitors data that is very dynamic in nature and attempts to evaluate how the system is performing, a policy monitors data that changes much less frequently. Policies evaluate the existing state of the system against corporate standards and best practices.

Accessing Policy Rules Using the Grid Control Console

To access the Policy Rule Library page that contains all the policy rules provided by Oracle, perform the following steps:

1. From the Grid Control Console home page, click **Policies**.
2. On the Policy Violations page, click **Library**.
3. On the Policy Rule Library page, locate the policy of interest and click the Information icon (*i*) in the Description column. The help for the policy displays.

For additional information about policies, see the Enterprise Manager online help and *Oracle Enterprise Manager Concepts*.

Automatic Storage Management (ASM) Policies

This chapter provides the following information for each of the Automatic Storage Management (ASM) policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Automatic Storage Management target only has storage policies.

1.1 Disk Group Contains Disks of Significantly Different Sizes

This policy checks the disk group for disks with disk sizes which vary by more than 5%.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------------------|------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 7 days. | Yes | Disk Group %DISK_GROUP_NAME% contains disks of significantly different sizes. For balanced I/O and optimal performance, disks in a given disk group should have similar size and performance characteristics. |

¹ The policy rule is evaluated each time its underlying *osm_diskGroup_Policies* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Disks in a disk group should have sizes within 5% of each other, unless data migration is in progress. Automatic Storage Management distributes data uniformly proportional to the size of the disks. For balanced I/O and optimal performance, disks in a given disk group should have similar size and performance characteristics.

Action

Remove, replace, or resize disks in the disk group so the size difference between disks is less than 5%.

1.2 Disk Group Contains Disks with Different Redundancy Attributes

This policy checks the disk group for disks that have different redundancy attributes

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------------------|------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 7 days. | Yes | Disk Group %DISK_GROUP_NAME% contains disks with different redundancy attributes. This may offer inconsistent levels of data protection. |

¹ The policy rule is evaluated each time its underlying *osm_diskGroup_Policies* metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Disks in the same disk group with different redundancy attributes may offer inconsistent levels of data protection.

Action

Move disks with different redundancy attributes into separate disk groups.

1.3 Disk Group Depends on External Redundancy and Has Unprotected Disks

This policy checks the disk group, which depends on external redundancy, for disks that are not mirrored or parity protected.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------------------|------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 7 days. | Yes | Disk Group %DISK_GROUP_NAME% depends on external redundancy and has disks that are not mirrored or parity protected. |

¹ The policy rule is evaluated each time its underlying *osm_diskGroup_Policies* metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Data loss can occur if the disk group depends on external redundancy and disks are not mirrored or parity protected.

Action

Replace problem disks with mirrored or parity protected disks, or move unprotected disks into a disk group with NORMAL or HIGH redundancy.

1.4 Disk Group with NORMAL or HIGH Redundancy Has Mirrored or Parity Protected Disks

This policy has detected that a disk group with normal or high redundancy has mirrored or parity protected disks.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------------------|------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 7 days. | Yes | NORMAL or HIGH redundancy disk group %DISK_GROUP_NAME% has disks that are mirrored or parity protected. Disk resources are wasted, and performance may be unnecessarily affected when both a disk and its owning disk group are providing data redundancy. |

¹ The policy rule is evaluated each time its underlying *osm_diskGroup_Policies* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Disk resources are wasted, and performance may be unnecessarily affected when both a disk and its owning disk group are providing data redundancy.

Action

Replace disks in the NORMAL or HIGH redundancy disk group with unprotected disks.

BEA WebLogic Managed Server Policies

This chapter provides the following information for each of the BEA WebLogic Managed Server policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The BEA WebLogic Managed Server only has configuration policies.

2.1 WebLogic Admin Port Enabled

This policy verifies whether the BEA WebLogic Server Domain Administration Port is enabled or not. An Administration Port limits all administrative traffic between server instances in a WebLogic Server domain to a single port.

When used in conjunction with a connection filter, you can specify that a WebLogic Server instance accepts administrative requests only from a known set of machines or subnets and only on a single port.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-----------------------------|----------------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------|
| Critical | Configuration | BEA WebLogic Managed Server | BEA WebLogic Server 7.1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | BEA WebLogic Server Domain doesn't have its Administration Port Enabled. |

¹ The policy rule is evaluated each time its underlying *DomainPolicyMetrics* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

It enables you to separate administration traffic from application traffic in your domain. The administration port accepts only secure and SSL traffic, and all connections through the port require authentication by a server administrator.

Action

Enable Domain Wide Administration Port. For more information, refer to the BEA WebLogic documentation.

2.2 WebLogic Performance Pack Enabled

This policy verifies whether the BEA WebLogic Server Performance Pack is enabled or not.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-----------------------------|----------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------|
| Critical | Configuration | BEA WebLogic Managed Server | BEA WebLogic Server 7.1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | BEA WebLogic Server doesn't have its Performance Pack Enabled. |

¹ The policy rule is evaluated each time its underlying *ServerPolicyMetrics* metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

None

Impact of Violation

Benchmarks show major performance improvements in WebLogic Server when you use the performance pack for your platform. Performance packs use a platform-optimized (native) socket multiplexor to improve server performance.

Action

To use a performance pack, make sure the `NativeIOEnabled` attribute of the `Server` element is defined in your `config.xml` file. The default `config.xml` file that shipped with your distribution enables this attribute by default: `NativeIOEnabled=true`. For more information, refer to the BEA WebLogic documentation.

2.3 WebLogic Production Mode Enabled

This policy verifies whether the BEA WebLogic Server is running in Production Mode or not.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-----------------------------|----------------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------|
| Critical | Configuration | BEA WebLogic Managed Server | BEA WebLogic Server 7.1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | BEA WebLogic Server is not running under production mode. |

¹ The policy rule is evaluated each time its underlying *DomainPolicyMetrics* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

WebLogic Server uses different default values for various services depending on the type of environment you specify. You can indicate whether a domain is to be used in a development environment or a production environment.

Action

Start the BEA WebLogic servers by enabling Production Mode. For more information, refer to the BEA WebLogic documentation.

Calendar Server Policy

This chapter provides the following information for the Calendar Server policy:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

3.1 High Log Level

This policy detects when log level configuration is set too high.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|------------------------|-----------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------|
| Warning | Configuration | Oracle Calendar Server | Oracle Collaboration Suite 10.1.1 | The underlying metric has a collection frequency of once every 24 hours. | Yes | Log level is set too high. |

¹ The policy rule is evaluated each time its underlying *cal_conf_metrics* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

When the log level is set too high, all unnecessary messages are displayed in the log file. The volume of messages reduces the readability of the log file and increases the risk of missing important messages. Performance is affected because more messages are printed, and due to increase volume of log files, disk space is impacted.

Action

Set log level to FALSE.

Cluster Database Policies

This chapter provides the following information for each of the Cluster Database policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Cluster Database policies are categorized as follows

- [Section 4.1, "Configuration Policies"](#)
- [Section 4.2, "Security Policies - UNIX"](#)
- [Section 4.3, "Security Policies - Windows"](#)
- [Section 4.4, "Storage Policies"](#)

4.1 Configuration Policies

The configuration policies for the Cluster Database target are:

4.1.1 Force Logging Disabled

When Data Guard Broker is being used, this policy checks the primary database for disabled force logging.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|----------------------------------------|----------------------------------------|----------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | Oracle Server 9i Release 2 or later | The underlying metrics have a collection frequency of once every 24 hours. | Yes | The primary database is not in force logging mode. As a result, unlogged direct writes in the primary database cannot be propagated to the standby database. |

¹ The policy rule is evaluated each time its underlying *db_init_params* and *ha_info* metrics are collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The primary database is not in force logging mode. As a result, unlogged direct writes in the primary database cannot be propagated to the standby database.

Action

The primary database should be put in force logging mode using the ALTER DATABASE FORCE LOGGING parameter.

4.1.2 Installation of JAccelerator (NCOMP)

This policy checks for installation of JAccelerator (NCOMP) that improves Java Virtual Machine performance by running natively compiled (NCOMP) classes.

Policy Summary

The following table lists the policy’s main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | JAccelerator (NCOMP) is not installed. Without JAccelerator Java VM performance will be sub-optimal. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Java VM performance will be sub-optimal.

Action

For improved Java Virtual Machine performance, install JAccelerator (NCOMP) which typically contains Natively compiled (NCOMP) classes.

4.1.3 Insufficient Number of Control Files

This policy checks for use of a single control file.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has insufficient control files. If you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks. |

¹ The policy rule is evaluated each time its underlying *db_controlfiles* metric are collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The control file is one of the most important files in an Oracle database. It maintains many physical characteristics and important recovery information about the database. If you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

Action

Use at least two control files that are multiplexed on different disks.

4.1.4 Insufficient Number of Redo Logs

This policy checks for use of less than three redo logs.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has insufficient number of redo log files. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods. |

¹ The policy rule is evaluated each time its underlying `db_redoLogs` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The online redo log files are used to record changes in the database for the purposes of recoverability. When archiving is enabled, these online redo logs need to be archived before they can be reused. Every database requires at least two online redo log groups to be up and running. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods.

Action

Oracle recommends having at least three online redo log groups with at least two members in each group. For obvious reasons, members of the same group must be on different disk drives.

4.1.5 Recovery Area Location Not Set

This policy checks if the `DB_RECOVERY_FILE_DEST` initialization parameter is set.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|----------------------------------------|-------------------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | Oracle Server 10g Release1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The recovery area location is not set. Setting the recovery area location provides a unified storage location for all recovery components. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Not setting the recovery area location results in a divided storage location for all recovery components.

Action

Set the recovery area location to provide a unified storage location for all recovery components.

4.2 Security Policies - UNIX

The security policies for the Cluster Database target for UNIX are:

4.2.1 Access to ALL_SOURCE View

This policy ensures restricted access to ALL_SOURCE view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege to the ALL_SOURCE view. |

¹ The policy rule is evaluated each time its underlying *allSourceRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

ALL_SOURCE view contains the source of all the stored packages in the database.

Action

Revoke access to the ALL_SOURCE view from the non-SYS database users.

4.2.2 Access to DBA Role Privileges View

This policy ensures restricted access to DBA_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaRolePrivsRec* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBA_ROLE_PRIVS view lists the roles granted to users and other roles. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_ROLE_PRIVS view.

4.2.3 Access to DBA Roles View

This policy ensures restricted access to DBA_ROLES view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_ROLES view. |

¹ The policy rule is evaluated each time its underlying *dbaRoleRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

DBA_ROLES view contains details of all roles in the database. Knowledge of the structure of roles in the database can be exploited by a malicious user. For example, a public select privilege might increase the likelihood of Denial of Service attacks.

Action

Restrict access to DBA_ROLES view.

4.2.4 Access to DBA_SYS_PRIVS View

This policy ensures restricted access to DBA_SYS_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_SYS_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaSysPrivsRec* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

DBA_SYS_PRIVS view can be queried to find system privileges granted to roles and users. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_SYS_PRIVS view.

4.2.5 Access to DBA_TAB_PRIVS View

This policy ensures restricted access to DBA_TAB_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database may be insecure as user %grantee% has %privilege% privilege to the DBA_TAB_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaTabPrivsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists privileges granted to users or roles on objects in the database. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_TAB_PRIVS view.

4.2.6 Access to DBA_USERS View

This policy ensures restricted access to DBA_USERS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_USERS view. |

¹ The policy rule is evaluated each time its underlying *dbaUsersRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Contains user name and password hashes and other account information. Access to this information can be used to mount brute-force attacks against the database.

Action

Restrict access to DBA_USERS view.

4.2.7 Access to ROLE_ROLE_PRIVS View

This policy ensures restricted access to ROLE_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the ROLE_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *rolerolePrivsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists roles granted to other roles. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to ROLE_ROLE_PRIVS view.

4.2.8 Access to STAT\$SQL Summary Table

This policy ensures restricted access to the STAT\$SQL_SUMMARY table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure. User %grantee% has %privilege% privilege on the STAT\$SQL_SUMMARY table. |

¹ The policy rule is evaluated each time its underlying *sqlSummaryRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Contains first few lines of SQL text of the most resource intensive commands given to the server. SQL statements executed without bind variables can appear and expose privileged information.

Action

Restrict access to the STAT\$SQL_SUMMARY table.

4.2.9 Access to STAT\$SQL Text Table

This policy ensures restricted access to the STAT\$SQLTEXT table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on STAT\$SQLTEXT table. |

¹ The policy rule is evaluated each time its underlying *sqlTextRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The STAT\$SQLTEXT table provides the full text of the recently-executed SQL statements. The SQL statements can reveal sensitive information.

Action

Restrict access to the STAT\$SQLTEXT table.

4.2.10 Access to SYS.AUD\$ Table

This policy ensures restricted access to the SYS.AUD\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SYS.AUD\$ table. |

¹ The policy rule is evaluated each time its underlying *audTabRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The SYS.AUD\$ table is the system audit table. If you set the parameter AUDIT_TRAIL to DB, all audited activity will be written to the SYS.AUD\$ table. Thus a malicious user can gain access to the sensitive audit information.

Action

Revoke access to the SYS.AUD\$ table from the non-DBA/SYS database users.

4.2.11 Access to SYS.LINK\$ Table

This policy ensures restricted access to the SYS.LINK\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER\$ table. |

¹ The policy rule is evaluated each time its underlying *linkTabRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to user names and passwords from the SYS.LINK\$ table.

Action

Revoke access to SYS.LINK\$ table.

4.2.12 Access to SYS.SOURCE\$ Table

This policy ensures restricted access to the SYS.SOURCE\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SOURCE\$ table. |

¹ The policy rule is evaluated each time its underlying *sourceTabRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the source of all stored packages in the database.

Action

Revoke access to the SYS.SOURCE\$ table from the non-SYS/DBA database users.

4.2.13 Access to SYS.USER\$ Table

This policy ensures restricted access to the SYS.USER\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER\$ table. |

¹ The policy rule is evaluated each time its underlying *userTabRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

User name and password hash may be read from the SYS.USER\$ table, enabling a malicious user to launch a brute-force attack against the database.

Action

Restrict access to SYS.USER\$ table.

4.2.14 Access to SYS.USER_HISTORY\$ Table

This policy ensures restricted access to the SYS.USER_HISTORY\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SYS.USER_HISTORY\$ table. |

¹ The policy rule is evaluated each time its underlying *userHistRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

User name and password hash may be read from the SYS.USER_HISTORY\$ table, enabling a malicious user to launch a brute-force attack.

Action

Revoke access to SYS.USER_HISTORY\$ table from the non-DBA/SYS database users.

4.2.15 Access to USER_ROLE_PRIVS View

This policy ensures restricted to the USER_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *userRolePrivsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists the roles granted to the current user. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to the USER_ROLE_PRIVS view.

4.2.16 Access to USER_TAB_PRIVS View

This policy ensures restricted access to the USER_TAB_PRIVS table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER_TAB_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *userTabPrivsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists the grants on objects for which the user is the owner, grantor, or grantee. Knowledge of the grants in the database can be exploited by a malicious user.

Action

Restrict access to the USER_TAB_PRIVS view.

4.2.17 Control File Permission

This policy ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The control file (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *dbControlFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

Action

Restrict permission to the control files to:

- Owner of the Oracle software installation
- DBA group

Do not give read and write permissions to public

4.2.18 Default Passwords

This policy ensures there are no default passwords for known accounts.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Default password for the account %dbaccount% has not been changed. |

¹ The policy rule is evaluated each time its underlying *defaultAccountPasswordsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using default passwords.

Action

Change all default passwords.

4.2.19 Excessive Allowed Failed Login Attempts

This policy ensures that the number of allowed failed login attempts is no more than 10.

The FAILED_LOGIN_ATTEMPTS parameter defines the number of successive failed login attempts that can be performed before an account's status is changed to locked. This protects against malicious users attempting to guess a password for an account.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. FAILED_LOGIN_ATTEMPTS is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *loginserver_failed_logins* metric is collected.

Defaults

Parameters and Their Default Values

Maximum FAILED_LOGIN_ATTEMPTS: 10 failed attempts

Objects Excluded by Default

None

Impact of Violation

Permits manual and automated password guessing by a malicious user.

By setting the parameter to UNLIMITED, a malicious user can attempt an unlimited amount of guesses of the password for all accounts granted the specified profile.

However, setting the value too low may result in valid users locking their accounts when mistyping a password.

Action

In user profiles, set the value for the FAILED_LOGIN_ATTEMPTS setting to no more than 10.

4.2.20 Excessive PUBLIC EXECUTE Privileges

Checks for PUBLIC having execute privileges on powerful packages (UTL_HTTP, UTL_TCP and UTL_SMTP).

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in insecure state. EXECUTE privilege on the package %package% is granted to the PUBLIC role. |

¹ The policy rule is evaluated each time its underlying *executePrivilegesRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to e-mail, network, and http modules using the EXECUTE privilege.

Action

Revoke EXECUTE privileges on powerful packages.

4.2.21 Execute UTL_FILE Privileges to PUBLIC

This policy ensures the PUBLIC role does not have EXECUTE privilege on the UTL_FILE package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. EXECUTE privilege on UTL_FILE package is granted to PUBLIC. |

¹ The policy rule is evaluated each time its underlying *pubexecutePrivilegesRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can read and write arbitrary files in the system when granted the UTL_FILE privilege.

Action

Revoke EXECUTE privileges granted to UTL_FILE package from PUBLIC.

4.2.22 Oracle Home Datafile Permission

This policy ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The datafile (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *dbDataFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The datafiles contain all the database data. If datafiles are made readable to public, they can be read by a user who has no database privileges on the data.

Action

Restrict permissions to the datafiles to:

- Owner of the Oracle software set
- DBA group

Do not give read and write permissions to public.

4.2.23 Password Grace Time

This policy ensures that all profiles have `PASSWORD_GRACE_TIME` set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. <code>PASSWORD_GRACE_TIME</code> is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdGraceRep* metric is collected.

Defaults

Parameters and Their Default Values

`MAX_PASSWORD_GRACE_TIME` = 3

Objects Excluded by Default

Not Applicable

Impact of Violation

A high value for the PASSWORD_GRACE_TIME parameter may cause serious database security issues by allowing the user to keep the same password for a long time.

Action

Set the PASSWORD_GRACE_TIME parameter to no more than 3 days for all profiles.

4.2.24 Password Life Time

This policy ensures that all profiles have PASSWORD_LIFE_TIME set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_LIFE_TIME is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdLifeRep* metric is collected.

Defaults**Parameters and Their Default Values**

MAX_PASSWORD_LIFE_TIME = 90

Objects Excluded by Default

Not Applicable

Impact of Violation

A long password life time gives malicious users a long time to decipher the password. May cause serious database security issues.

Action

Set the PASSWORD_LIFE_TIME parameter to no more than 90 days for all profiles.

4.2.25 Password Locking Time

This policy ensures that PASSWORD_LOCK_TIME is set to a reasonable number of days for all profiles.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_LOCK_TIME is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdLockRep* metric is collected.

Defaults

Parameters and Their Default Values

MIN_PASSWORD_LOCK_TIME = 1

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_LOCK_TIME resource relates to the number of days an account is locked after a user tries unsuccessfully to login for more than FAILED_LOGIN_ATTEMPTS (another related resource) times. Having a low value for this resource increases the likelihood of Denial of Service attacks.

Action

Set the PASSWORD_LOCK_TIME parameter to no less than 1 for all the profiles.

4.2.26 Password Reuse Maximum

This policy ensures that all profiles have PASSWORD_REUSE_MAX set to a reasonable number of times.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_REUSE_MAX is set to %limit% times for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *reuseMaxRep* metric is collected.

Defaults

Parameters and Their Default Values

MAX_PASSWORD_REUSE_MAX = 20

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_REUSE_MAX parameter specifies the number of password changes required before the current password can be reused. Old passwords are usually the best guesses for the current password. A low value for the PASSWORD_REUSE_MAX parameter may cause serious database security issues by allowing users to reuse their old passwords more often. Ensuring a reasonable value for this resource will discourage users from reusing their passwords resulting in more secure password usage.

Action

Set the PASSWORD_REUSE_MAX parameter to no less than 20 times for all profiles.

4.2.27 Password Reuse Time

This policy ensures that all profiles have PASSWORD_REUSE_TIME set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_REUSE_TIME is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *passwdReuseTimeRep* metric is collected.

Defaults**Parameters and Their Default Values**

MAX_PASSWORD_REUSE_TIME = 2147483647

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_REUSE_TIME parameter defines the number of days before a password can be reused. A low value for the password reuse time can increase the danger of an already leaked password to cause serious database security issues.

Ensuring a reasonable value for this resource will discourage users from reusing their passwords resulting in more secure password usage.

Action

Set the PASSWORD_REUSE_TIME parameter to UNLIMITED for all profiles.

4.2.28 Profiles with Excessive Allowed Failed Login Attempts

This policy ensures that the number of allowed failed login attempts is no more than 10.

The FAILED_LOGIN_ATTEMPTS parameter defines the number of successive failed login attempts that can be performed before an account's status is changed to locked. This protects against malicious users attempting to guess a password for an account.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. FAILED_LOGIN_ATTEMPTS is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *loginserver_failed_logins* metric is collected.

Defaults

Parameters and Their Default Values

Maximum FAILED_LOGIN_ATTEMPTS: 10 failed attempts

Objects Excluded by Default

Not Applicable

Impact of Violation

Permits manual and automated password guessing by a malicious user.

By setting the parameter to UNLIMITED, a malicious user can attempt an unlimited amount of guesses of the password for all accounts granted the specified profile. However, setting the value too low may result in valid users locking their accounts when mistyping a password.

Action

In user profiles, set the value for the FAILED_LOGIN_ATTEMPTS setting to no more than 10.

4.2.29 PUBLIC EXECUTE Privileges to DBMS Job

This policy ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_JOB package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsjobPrivsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Granting EXECUTE privilege to PUBLIC on DBMS_JOB package allows all users to schedule jobs on the database.

Action

PUBLIC must not be granted EXECUTE privileges on DBMS_JOB package.

4.2.30 PUBLIC EXECUTE Privileges to DBMS LOB

This policy ensures PUBLIC group is not granted EXECUTE privileges to the DBMS_LOB package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_LOB package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsLobRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBMS_LOB package can be used to access any file on the system as the owner of the Oracle software installation.

Action

Revoke the EXECUTE privileges on DBMS_LOB package from the PUBLIC group.

4.2.31 PUBLIC EXECUTE Privileges to DBMS SYS SQL

This policy ensures PUBLIC is not granted EXECUTE privileges on DBMS_SYS_SQL package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_SYS_SQL package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsSysSqlRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBMS_SYS_SQL package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.

Action

Revoke the EXECUTE privileges on DBMS_SYS_SQL package from the PUBLIC group.

4.2.32 System Privileges to Public

This policy ensures system privileges are not granted to PUBLIC.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. System privilege %privilege% is assigned to the PUBLIC role. |

¹ The policy rule is evaluated each time its underlying *systemPrivilegesRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. There are security risks when granting SYSTEM privileges to all users.

Action

Revoke SYSTEM privileges from the PUBLIC role.

4.2.33 Unlimited Tablespace Quota

This policy ensures that database users are allocated a limited tablespace quota.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. User %dbuser% has an unlimited tablespace quota. |

¹ The policy rule is evaluated each time its underlying *tableSpaceQuotaRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Granting unlimited tablespace quotas can cause the filling up of the allocated disk space. This can lead to an unresponsive database.

Action

For users with an unlimited tablespace quota, reallocate their tablespace quotas to a specific limit.

4.2.34 Use of Database Links with Cleartext Password

Ensures database links with clear text passwords are not used, that is, the password is hashed or encrypted.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-----------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 9i and pre-9i | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Database link %link% has clear text password. |

¹ The policy rule is evaluated each time its underlying *dbLinkPwdRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The table SYS.LINK\$ contains the clear text password used by the database link. A malicious user can read clear text password from SYS.LINK\$ table that can lead to undesirable consequences.

Action

Avoid creating fixed user database links.

4.2.35 Well Known Accounts

This policy ensures well-known accounts are expired and locked.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Account %dbaccount% is not locked and terminated. |

¹ The policy rule is evaluated each time its underlying *installAndDemoAccountsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using a well-known account.

Action

Expire and lock well-known accounts.

4.2.36 Well Known Accounts (Status)

This policy ensures well-known accounts are expired and locked.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Account %dbaccount% is not locked and terminated. |

¹ The policy rule is evaluated each time its underlying *installAndDemoAccountsRepmetric* is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using a well-known account.

Action

Expire and lock well-known accounts.

4.3 Security Policies - Windows

The security policies for the Cluster Database target for Windows are:

4.3.1 Control File Permission (Windows)

This policy ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. The users %users% have critical permissions on the control file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *dbControlFilesPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

Action

Restrict permission to the control files to:

- Owner of the Oracle software installation
- DBA group

Do not give read and write permissions to public.

4.3.2 Oracle Home Datafile Permission (Windows)

This policy ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the datafile (%file_name%). |

¹ The policy rule is evaluated each time its underlying *dbDataFilesPermNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The datafiles contain all the database data. If datafiles are made readable to public, they can be read by a user who has no database privileges on the data.

Action

Restrict permissions to the datafiles to:

- Owner of the Oracle software set
- DBA group

Do not give read and write permissions to public.

4.4 Storage Policies

The storage policies for the Cluster Database target are:

4.4.1 Default Permanent Tablespace Set to a System Tablespace

This policy verifies that the DEFAULT_PERMANENT_TABLESPACE database property is set to a non-system tablespace. The default permanent tablespace for the database is used as the default permanent tablespace for any users who are not explicitly assigned a permanent tablespace. The default permanent tablespace is defaulted to the SYSTEM tablespace until it is changed by a DBA.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance; Cluster Database | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The default permanent tablespace is not set explicitly and defaults to SYSTEM tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults**Parameters and Their Default Values**

SYSTEM

Objects Excluded by Default

Not Applicable

Impact of Violation

If not specified explicitly, the `DEFAULT_PERMANENT_TABLESPACE` is defaulted to the `SYSTEM` tablespace. This is not the recommended setting. The default permanent tablespace for the database is used as the permanent tablespace for any non-`SYSTEM` users who are not explicitly assigned a permanent tablespace. If the database default permanent tablespace is set to a system tablespace, then any user who is not explicitly assigned a tablespace uses the system tablespace. Non-`SYSTEM` users should not be using a system tablespaces to store data. Doing so may result in performance degradation for the database.

Action

Set the `DEFAULT_PERMANENT_TABLESPACE` to a non-system tablespace. Create or edit a tablespace and set it to be the default permanent tablespace.

Clicking the `DEFAULT_PERMANENT_TABLESPACE` link will bring up the Tablespace Search page. From this page you can create or edit a tablespace and set it to be the default permanent tablespace.

On the Administration property page for the database instance, click **Tablespaces** under the Storage options. After providing your credentials, create or edit a permanent tablespace and set it to be the default permanent tablespace.

4.4.2 Default Temporary Tablespace Set to a System Tablespace

This policy verifies that the `DEFAULT_TEMP_TABLESPACE` database property is set to a non-system tablespace. The default temporary tablespace for the database is used as the temporary tablespace for any users that are not explicitly assigned a temporary tablespace. The temporary tablespace is defaulted to the `SYSTEM` tablespace until it is changed by a DBA.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|---------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance; Cluster Database | Oracle Server 9i or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The default temporary tablespace is not set explicitly and defaults to <code>SYSTEM</code> tablespace. |

¹ The policy rule is evaluated each time its underlying `db_recTablespaceSettings` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

If not specified explicitly, the `DEFAULT_TEMP_TABLESPACE` defaults to the `SYSTEM` tablespace. This is not the recommended setting. The default temporary tablespace is used as the temporary tablespace for any users who are not explicitly assigned a temporary tablespace. If the database default temporary tablespace is set to a system tablespace, then any user who is not explicitly assigned a temporary tablespace uses the system tablespace as their temporary tablespace. System tablespaces should not be used to store temporary data. Doing so can result in performance degradation for the database.

Action

Set the `DEFAULT_TEMP_TABLESPACE` to a non-system temporary tablespace. In Oracle Database 10g Release 1 or later, you can also set the `DEFAULT_TEMP_TABLESPACE` to a temporary tablespace group. Create or edit a temporary tablespace, or temporary tablespace group, and set it to be the default temporary tablespace.

Clicking the `DEFAULT_TEMP_TABLESPACE` link will bring up the `Tablespace Search` page. From this page the user can create or edit a temporary tablespace and set it to be the default temporary tablespace.

On the Administration property page for the database instance, click **Tablespaces** under the Storage options. After providing your credentials, create or edit a temporary tablespace and set it to be the default temporary tablespace.

4.4.3 Dictionary Managed Tablespaces

This policy determines whether dictionary managed tablespaces are being used. Use locally managed tablespaces.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% is dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management. |

¹ The policy rule is evaluated each time its underlying `db_recTablespaceSettings` metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

These tablespaces are dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management.

Action

Redefine these tablespaces to be locally managed.

4.4.4 Insufficient Redo Log Size

This policy, using the SMALL_REDO_LOGS parameter, checks for redo log files that are less than 1 MB.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------|
| Critical | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has redo log that has insufficient size. |

¹ The policy rule is evaluated each time its underlying *db_redo_logs* metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Small redo logs cause system checkpoints to continuously put a high load on the buffer cache and I/O system.

Action

Increase size of the redo logs to at least 1 MB.

4.4.5 Non-System Data Segments in a System Tablespace

Redefine the tablespaces containing the segments to be locally managed; or, reorganize these segments, specifying a Next Extent value that is a multiple of Initial Extent, and a Percent Increase value of 0.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Segment %OBJECT% belonging to non-system users are stored in system tablespace %TABLESPACE_NAME%. This makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recSegmentSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Cluster object types because the Reorganize Objects wizard does not support them.

All user accounts that are, by default, part of the Oracle Database or Enterprise Manager. For example: SYS, SYSTEM, SYSMAN, CTXSYS, SCOTT, ADAMS, and so on.

Impact of Violation

These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX. This violation makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. System users include users that are part of the DBMS such as SYS and SYSTEM, or that are part of facilities supplied by Oracle: for example, CTXSYS, SYSMAN, and OLAPSYS.

Action

Relocate the non-system segments to a non-system tablespace.

4.4.6 Non-Uniform Default Extent Size for Dictionary Managed Tablespaces

This policy checks for tablespaces with non-uniform default extent size.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% uses non-uniform extents. Using uniform extents ensures that any free extent in the tablespace can always be used for any segment in the tablespace. |

¹ The policy rule is evaluated each time its underlying *db_tablespace* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

SYSTEM tablespace. This policy is only applicable to PERMANENT DICTIONARY tablespaces.

Impact of Violation

Tablespaces using a non-uniform default extent size exist. Extents in a tablespace should be the same size. This ensures that any free extent in the tablespace can always be used for any segment in the tablespace.

Action

To ensure uniform extent sizes, set each tablespace's default storage clause so that the NEXT value should be equal to or a multiple of the INITIAL value, and the PCTINCREASE value is set to zero. Then never explicitly specify a storage clause at the segment level. Instead, let the storage values for the segments be inherited from the default storage clause of the tablespace.

4.4.7 Rollback in SYSTEM Tablespace

Rollback in SYSTEM Tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|-------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | See following table | Yes | Your SYSTEM tablespace contains rollback segment %RBS_NAME%. The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. |

¹ The policy rule is evaluated each time its underlying metric is collected.

The following table lists the policy's underlying metrics.

| Underlying Metric | Collection Frequency |
|-------------------------|----------------------|
| <i>db_init_params</i> | Every 24 hours |
| <i>db_rollback_segs</i> | Every 24 hours |

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. It should NOT be used to store any other types of objects such as user tables, user indexes, user views, rollback segments, undo segments, or temporary segments.

Action

Use a tablespace dedicated to undo instead of the SYSTEM tablespace.

4.4.8 Segment in Dictionary Tablespace with Extent Growth Policy Violation

This policy, using the SEG_EXT_GROWTH_VIO parameter, checks for segments in dictionary managed tablespaces having irregular extent sizes and/or non-zero Percent Increase settings.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Segment %OBJECT% in dictionary managed tablespace %TABLESPACE_NAME% has irregular extent sizes and/or non-zero Percent Increase settings. This can result in inefficient reuse of space and fragmentation problems. |

¹ The policy rule is evaluated each time its underlying *db_recSegmentSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

These segments have extents with sizes that are not multiples of the initial extent, and/or a non-zero Percent Increase setting. This can result in inefficient reuse of space and fragmentation problems.

Action

Redefine the tablespaces containing the segments to be locally managed; or, reorganize these segments, specifying a Next Extent value that is a multiple of Initial Extent, and a Percent Increase value of 0.

4.4.9 Tablespace Not Using Automatic Segment-Space Management

This policy checks for locally managed tablespaces that are using MANUAL segment space management.

There are two segment-space management settings: MANUAL and AUTO.

- MANUAL segment-space management uses free lists to manage free space within segments. Free lists are lists of data blocks that have space available for inserting rows. With this form of segment-space management, you must specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace.
- AUTO segment-space management uses bitmaps to manage the free space in segments. The bitmap describes the status of each data block within a segment with respect to the amount of space in the block available for inserting rows. These bitmaps allow the database to manage free space automatically.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|----------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | Oracle Server 9.2 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% is not using automatic segment-space management. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Automatic segment-space management is a simpler and more efficient way of managing space within a segment. It completely eliminates any need to specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace.

In a RAC environment, there is the additional benefit of avoiding the hard partitioning of space inherent with using free list groups.

Action

Change the segment-space management of all permanent locally managed tablespaces to AUTO.

Clicking the name of each tablespace listed will bring up the Reorganize Objects wizard with the tablespace automatically selected. This wizard allows you to change the segment-space management of the tablespace from MANUAL to AUTO.

4.4.10 Tablespaces Containing Rollback and Data Segments

This policy, using the TBSP_MIXED_SEGS parameter, checks for tablespaces containing both rollback and data segments.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% contains both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

SYSTEM tablespace

Impact of Violation

These tablespaces contain both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the

tablespace. Use of a dedicated tablespace for rollback segments enhances availability and performance.

Action

Use Automatic Undo Management (in Oracle Server Release 9.0.1 or later) and perform one of the following:

- Drop the rollback segments from this tablespace
- Create one or more tablespaces dedicated to rollback segments and drop the rollback segments from this tablespace
- Dedicate this tablespace to rollback segments and move the data segments to another tablespace

4.4.11 Users with a System Tablespace as Default Tablespace

This policy, using the `SYSTEM_AS_DEFAULT_TBSP` parameter, checks for any user having a System tablespace listed as their default tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | User %USER_NAME% uses SYSTEM tablespace as the default tablespace. This will result in non-system data segments being added to the SYSTEM tablespace and possible performance degradation in the SYSTEM tablespace. |

¹ The policy rule is evaluated each time its underlying `db_recUserSettings` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Cluster object types because the Reorganize Objects wizard does not support them.

All user accounts that are, by default, part of the Oracle Database or Enterprise Manager, for example: SYS, SYSTEM, SYSMAN, CTXSYS, SCOTT, ADAMS, and so on.

Impact of Violation

These users use a system tablespace as the default tablespace. This violation will result in non-system data segments being added to the system tablespace, making it more difficult to manage these data segments and possibly resulting in performance degradation in the system tablespace.

Action

Change the default tablespace for these users to specify a non-system tablespace.

4.4.12 Users with Permanent Tablespace as Temporary Tablespace

This policy checks the PERM_AS_TEMP_TBSP parameter to detect whether a permanent tablespace is being used as a temporary tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|----------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | Oracle Server 9.2 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | User %USER_NAME% uses permanent tablespace %TABLESPACE_NAME% as the temporary tablespace. Using a permanent tablespace as the temporary tablespace may result in performance degradation, especially for Real Application Clusters. |

¹ The policy rule is evaluated each time its underlying *Db_reclUserSettings* metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

These users use a permanent tablespace as the temporary tablespace. Using temporary tablespaces allows space management for sort operations to be more efficient. Using a permanent tablespace for these operations may result in performance degradation, especially for Real Application Clusters.

Action

Change the temporary tablespace for these users to specify a tablespace of type TEMPORARY.

Database Instance Policies

This chapter provides the following information for each of the Database Instance policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Database Instance policies are categorized as follows:

- [Section 5.1, "Configuration Policies"](#)
- [Section 5.2, "Security Policies - UNIX"](#)
- [Section 5.3, "Security Policies - Windows"](#)
- [Section 5.4, "Storage Policies"](#)

5.1 Configuration Policies

The configuration policies for the Database Instance target are:

5.1.1 Disabled Automatic Statistics Collection

This policy checks if the STATISTICS_LEVEL initialization parameter is set to BASIC.

The STATISTICS_LEVEL initialization parameter has three valid settings, TYPICAL, ALL, and BASIC.

- The default setting of TYPICAL ensures collection of all major statistics required for database self-management and functionality and provides best overall performance. The default value should be adequate for most environments.
- Setting the parameter to ALL collects all the same statistics that are collected with the TYPICAL setting, plus timed OS and plan execution statistics.
- Setting the parameter to BASIC disables the collection of many important statistics that are required by Oracle Database features and functionality.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------------|---------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | Database Instance | Oracle Server 10g Release | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is set to BASIC. Many important statistics required by Oracle database features and functionality are disabled. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

STATISTICS_LEVEL: TYPICAL

Objects Excluded by Default

Not Applicable

Impact of Violation

Automatic statistics collection allows the optimizer to generate accurate execution plans and is essential for identifying and correcting performance problems. By default, STATISTICS_LEVEL is set to TYPICAL. If the STATISTICS_LEVEL initialization parameter is set to BASIC, the collection of many important statistics, required by Oracle database features and functionality, are disabled.

Action

Set the STATISTICS_LEVEL initialization parameter to TYPICAL.

5.1.2 Force Logging Disabled

When Data Guard Broker is being used, this policy checks the primary database for disabled force logging.

Policy Summary

The following table lists the policy’s main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|-------------------------------------|-------------------------------------|----------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | Oracle Server 9i Release 2 or later | The underlying metrics have a collection frequency of once every 24 hours. | Yes | The primary database is not in force logging mode. As a result, unlogged direct writes in the primary database cannot be propagated to the standby database. |

¹ The policy rule is evaluated each time its underlying *db_init_params* and *ha_info* metrics are collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The primary database is not in force logging mode. As a result, unlogged direct writes in the primary database cannot be propagated to the standby database.

Action

The primary database should be put in force logging mode using the ALTER DATABASE FORCE LOGGING parameter.

5.1.3 Installation of JAccelerator (NCOMP)

This policy checks for installation of JAccelerator (NCOMP) that improves Java Virtual Machine performance by running natively compiled (NCOMP) classes.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | JAccelerator (NCOMP) is not installed. Without JAccelerator Java VM performance will be suboptimal. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Java VM performance will be sub-optimal.

Action

For improved Java Virtual Machine performance, install JAccelerator (NCOMP) which typically contains Natively compiled (NCOMP) classes.

5.1.4 Insufficient Number of Control Files

This policy checks for use of a single control file.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has insufficient control files. If you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks. |

¹ The policy rule is evaluated each time its underlying *db_controlfiles* metric are collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The control file is one of the most important files in an Oracle database. It maintains many physical characteristics and important recovery information about the database. If you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

Action

Use at least two control files that are multiplexed on different disks.

5.1.5 Insufficient Number of Redo Logs

This policy checks for use of less than three redo logs.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Configuration | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has insufficient number of redo log files. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods. |

¹ The policy rule is evaluated each time its underlying *db_redoLogs* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The online redo log files are used to record changes in the database for the purposes of recoverability. When archiving is enabled, these online redo logs need to be archived before they can be reused. Every database requires at least two online redo log groups to be up and running. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods.

Action

Oracle recommends having at least three online redo log groups with at least two members in each group. For obvious reasons, members of the same group must be on different disk drives.

5.1.6 Not Using Automatic PGA Management

This policy checks if the `PGA_AGGREGATE_TARGET` initialization parameter has a value of 0 or if `WORKAREA_SIZE_POLICY` has value of `MANUAL`.

This parameter automatically controls the amount of memory allocated for sorts and hash joins. Larger amounts of memory allocated for sorts or hash joins reduce the optimizer cost of these operations.

- For OLTP systems, the PGA memory typically accounts for a small fraction of the total memory available (for example, 20%), leaving 80% for the SGA.
- For DSS systems running large, memory-intensive queries, PGA memory can typically use up to 70% of that total (up to 2.2 GB in this example).

Good initial values for the parameter `PGA_AGGREGATE_TARGET` might be:

- For OLTP: $PGA_AGGREGATE_TARGET = (total_mem * 80\%) * 20\%$
- For DSS: $PGA_AGGREGATE_TARGET = (total_mem * 80\%) * 50\%$ where `total_mem` is the total amount of physical memory available on the system.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------------|---------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Warning | Configuration | Database Instance | Oracle Server 9i or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is not using Automatic PGA memory management. It simplifies and improves the way PGA memory is allocated. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

PGA_AGGREGATE_TARGET: 0

WORKAREA_SIZE_POLICY: MANUAL

Objects Excluded by Default

Not Applicable

Impact of Violation

Automatic PGA memory management simplifies and improves the way PGA memory is allocated. When enabled, Oracle can dynamically adjust the portion of the PGA memory dedicated to work areas while honoring the PGA_AGGREGATE_TARGET limit set by the DBA.

Action

Enable Automatic PGA Memory Management and set the PGA_AGGREGATE_TARGET initialization parameter to a non-zero number. Use Oracle PGA advice to help set PGA_AGGREGATE_TARGET to the best size.

5.1.7 Not Using Automatic Shared Memory Management

This policy checks if the SGA_TARGET initialization parameter has a value of zero.

By setting the SGA_TARGET to the desired size of the SGA, Oracle automatically manages the size of the shared pool (SHARED_POOL_SIZE), large pool (LARGE_POOL_SIZE), java pool (JAVA_POOL_SIZE), and buffer cache (DB_CACHE_SIZE). Therefore, instead of setting four initialization parameters, you only need to set one. The only exception to this is if some application has a minimum requirement on these pool sizes. In this case, the initialization parameter can be set, but it will be treated as a minimum.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|-------------------|--------------------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is not using automatic shared memory management that simplifies the configuration of the SGA. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The `SGA_TARGET` initialization parameter is set to zero. This means that all SGA memory management must be done manually. Specify a non-zero `SGA_TARGET` so that `SHARED_POOL_SIZE`, `LARGE_POOL_SIZE`, `JAVA_POOL_SIZE`, and `DB_CACHE_SIZE` can be managed automatically.

By setting `SGA_TARGET`, these parameters will be set to zero, allowing Oracle to use the entire `SGA_TARGET` size for dynamic adjustment. Before setting `SGA_TARGET`, determine if any pool sizes should be set to support application level minimum pool size requirements.

Action

Automatic Shared Memory Management simplifies the configuration of the SGA and is the recommended memory configuration. To use Automatic Shared Memory Management, set the `SGA_TARGET` initialization parameter to the amount of memory you want to dedicate to the SGA. The amount can be less than or equal to the value of the `SGA_MAX_SIZE` initialization parameter. Once you set the `SGA_TARGET` initialization parameter, verify that the `STATISTICS_LEVEL` initialization parameter is set to `TYPICAL`.

Clicking the statistics level link displays the Initialization Parameters page, `statistics_level` is automatically filled in to the search criteria. Clicking on the `sga_target` link displays the Memory Parameters SGA page from the Administration tab where you can enable automatic shared memory management.

5.1.8 Not Using Automatic Undo Management

This policy checks for automatic undo space management not being used.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------------|----------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | Database Instance | Oracle Server 9.2 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is not using automatic undo management. This can cause unnecessary contention and performance issues. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

None

Impact of Violation

Not using automatic undo management can cause unnecessary contention and performance issues in your database. This may include among other issues, contention for the rollback segment header blocks, in the form of buffer busy waits and increased probability of ORA-1555s (Snapshot Too Old).

Action

Use automatic undo space management instead of manual undo or rollback segments.

5.1.9 Not Using Latest Version of Optimizer

This policy checks if `OPTIMIZER_FEATURES_ENABLE` has a value that is lower than the latest optimizer version.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------------|-------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Configuration | Database Instance | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is not using the latest optimizer version. The new version of the optimizer has better information to help it determine the most efficient way to run a SQL Statement. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Using older versions of the optimizer can lead to execution plan or query performance issues. The Oracle optimizer does not make the same decisions from one version to the next. The new version of the optimizer has better information to help it determine the most efficient way to run a SQL Statement.

Action

Set the `OPTIMIZER_FEATURES_ENABLE` parameter to the latest version. This allows the optimizer to use the latest functionality. Any queries that were tuned for an older version of the optimizer, and are experiencing execution plan or query performance issues, should be fixed on a case-by-case basis.

Clicking the `OPTIMIZER_FEATURES_ENABLE` link displays the Initialization Parameters page with `OPTIMIZER_FEATURES_ENABLE` automatically filled in to the search criteria. From this page, you can change the setting of the `OPTIMIZER_FEATURES_ENABLE` to the latest version.

5.1.10 Not Using Spfile

This policy checks for SPFILE (server parameter file) not being used.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------------|---------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Critical | Configuration | Database Instance | Oracle Server 9i or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is not using spfile. The changes made using ALTER SYSTEM commands will not persist. |

¹ The policy rule is evaluated each time its underlying `db_init_params` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The SPFILE (server parameter file) enables you to persist any dynamic changes to the Oracle initialization parameters using ALTER SYSTEM commands. This persistence is

provided across database shutdowns. When a database has an SPFILE configured, you do not have to remember to make the corresponding changes to the Oracle initialization file. In addition, any changes that are made using the ALTER SYSTEM commands are not lost after a shutdown and restart.

Action

Use the server side parameter file to update changes dynamically.

5.1.11 Recovery Area Location Not Set

This policy checks if the DB_RECOVERY_FILE_DEST initialization parameter is set.

Policy Summary

The following table lists the policy’s main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|----------------------------------------|-------------------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance; Cluster Database | Oracle Server 10g Release1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The recovery area location is not set. Setting the recovery area location provides a unified storage location for all recovery components. |

¹ The policy rule is evaluated each time its underlying *db_init_params* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Not setting the recovery area location results in a divided storage location for all recovery components.

Action

Set the recovery area location to provide a unified storage location for all recovery components.

5.1.12 Statistics Level Parameter Set to ALL

This policy checks if the STATISTICS_LEVEL initialization parameter is set to ALL.

Policy Summary

The following table lists the policy’s main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|-------------------|--------------------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Unnecessary timed OS and plan execution statistics are being collected. This creates additional overhead on the system. |

¹ The policy rule is evaluated each time its underlying `db_init_params` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

When the database collects more statistics than are actually needed, this creates additional overhead on the system.

Action

Collect only those statistics that are needed.

5.1.13 Use of Non-Standard Initialization Parameters

This policy checks for use of non-standard initialization parameters.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|---------------|-------------------|-------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Configuration | Database Instance | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database is using non-standard initialization parameter <code>%INIT_PARAM_NAME%</code> . Using these parameters may cause problems that can require considerable investigation. |

¹ The policy rule is evaluated each time its underlying `db_init_params` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Parameters starting with two underscore characters (__). These parameters are special and are reserved for the Oracle Database.

Impact of Violation

Non-standard initialization parameters are being used. These may have been implemented based on poor advice or incorrect assumptions. In particular, parameters associated with SPIN_COUNT on latches and undocumented optimizer features can cause a great deal of problems that can require considerable investigation.

Action

Avoid use of non-standard initialization parameters.

5.2 Security Policies - UNIX

The security policies for the Database Instance target on UNIX are:

5.2.1 Access to ALL_SOURCE View

This policy ensures restricted access to ALL_SOURCE view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege to the ALL_SOURCE view. |

¹ The policy rule is evaluated each time its underlying *allSourceRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

ALL_SOURCE view contains the source of all the stored packages in the database.

Action

Revoke access to the ALL_SOURCE view from the non-SYS database users.

5.2.2 Access to DBA Role Privileges View

This policy ensures restricted access to DBA_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaRolePrivsRec* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBA_ROLE_PRIVS view lists the roles granted to users and other roles. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_ROLE_PRIVS view.

5.2.3 Access to DBA Roles View

This policy ensures restricted access to DBA_ROLES view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_ROLES view. |

¹ The policy rule is evaluated each time its underlying *dbaRoleRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

DBA_ROLES view contains details of all roles in the database. Knowledge of the structure of roles in the database can be exploited by a malicious user. For example, a public select privilege might increase the likelihood of Denial of Service attacks.

Action

Restrict access to DBA_ROLES view.

5.2.4 Access to DBA_SYS_PRIVS View

This policy ensures restricted access to DBA_SYS_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_SYS_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaSysPrivsRec* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

DBA_SYS_PRIVS view can be queried to find system privileges granted to roles and users. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_SYS_PRIVS view.

5.2.5 Access to DBA_TAB_PRIVS View

This policy ensures restricted access to DBA_TAB_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database may be insecure as user %grantee% has %privilege% privilege to the DBA_TAB_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *dbaTabPrivsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists privileges granted to users or roles on objects in the database. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to DBA_TAB_PRIVS view.

5.2.6 Access to DBA_USERS View

This policy ensures restricted access to DBA_USERS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the DBA_USERS view. |

¹ The policy rule is evaluated each time its underlying *dbaUsersRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Contains user name and password hashes and other account information. Access to this information can be used to mount brute-force attacks against the database.

Action

Restrict access to DBA_USERS view.

5.2.7 Access to ROLE_ROLE_PRIVS View

This policy ensures restricted access to ROLE_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the ROLE_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *rolerolePrivsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists roles granted to other roles. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to ROLE_ROLE_PRIVS view.

5.2.8 Access to STAT\$SQL Summary Table

This policy ensures restricted access to the STAT\$SQL_SUMMARY table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure. User %grantee% has %privilege% privilege on the STAT\$SQL_SUMMARY table. |

¹ The policy rule is evaluated each time its underlying *sqlSummaryRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Contains first few lines of SQL text of the most resource intensive commands given to the server. SQL statements executed without bind variables can appear and expose privileged information.

Action

Restrict access to the STAT\$SQL_SUMMARY table.

5.2.9 Access to STAT\$SQL Text Table

This policy ensures restricted access to the STAT\$SQLTEXT table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on STAT\$SQLTEXT table. |

¹ The policy rule is evaluated each time its underlying *sqlTextRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The STAT\$SQLTEXT table provides the full text of the recently-executed SQL statements. The SQL statements can reveal sensitive information.

Action

Restrict access to the STAT\$SQLTEXT table.

5.2.10 Access to SYS.AUD\$ Table

This policy ensures restricted access to the SYS.AUD\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SYS.AUD\$ table. |

¹ The policy rule is evaluated each time its underlying *audTabRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The SYS.AUD\$ table is the system audit table. If you set the parameter AUDIT_TRAIL to DB, all audited activity will be written to the SYS.AUD\$ table. Thus a malicious user can gain access to the sensitive audit information.

Action

Revoke access to the SYS.AUD\$ table from the non-DBA/SYS database users.

5.2.11 Access to SYS.LINK\$ Table

This policy ensures restricted access to the SYS.LINK\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER\$ table. |

¹ The policy rule is evaluated each time its underlying *linkTabRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to user names and passwords from the SYS.LINK\$ table.

Action

Revoke access to SYS.LINK\$ table.

5.2.12 Access to SYS.SOURCE\$ Table

This policy ensures restricted access to the SYS.SOURCE\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SOURCE\$ table. |

¹ The policy rule is evaluated each time its underlying *sourceTabRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the source of all stored packages in the database.

Action

Revoke access to the SYS.SOURCE\$ table from the non-SYS/DBA database users.

5.2.13 Access to SYS.USER\$ Table

This policy ensures restricted access to the SYS.USER\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER\$ table. |

¹ The policy rule is evaluated each time its underlying *userTabRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

User name and password hash may be read from the SYS.USER\$ table, enabling a malicious user to launch a brute-force attack against the database.

Action

Restrict access to SYS.USER\$ table.

5.2.14 Access to SYS.USER_HISTORY\$ Table

This policy ensures restricted access to the SYS.USER_HISTORY\$ table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the SYS.USER_HISTORY\$ table. |

¹ The policy rule is evaluated each time its underlying *userHistRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

User name and password hash may be read from the SYS.USER_HISTORY\$ table, enabling a malicious user to launch a brute-force attack.

Action

Revoke access to SYS.USER_HISTORY\$ table from the non-DBA/SYS database users.

5.2.15 Access to USER_ROLE_PRIVS View

This policy ensures restricted to the USER_ROLE_PRIVS view.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER_ROLE_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *userRolePrivsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists the roles granted to the current user. Knowledge of the structure of roles in the database can be exploited by a malicious user.

Action

Restrict access to the USER_ROLE_PRIVS view.

5.2.16 Access to USER_TAB_PRIVS View

This policy ensures restricted access to the USER_TAB_PRIVS table.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | No | Database is in an insecure state. User %grantee% has %privilege% privilege on the USER_TAB_PRIVS view. |

¹ The policy rule is evaluated each time its underlying *userTabPrivsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Lists the grants on objects for which the user is the owner, grantor, or grantee. Knowledge of the grants in the database can be exploited by a malicious user.

Action

Restrict access to the USER_TAB_PRIVS view.

5.2.17 Audit File Destination

This policy ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The audit file directory has insecure permissions. The audit file directory (%dir_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *auditFileDestRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

Action

Restrict permissions to the Audit File directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.2.18 Background Dump Destination

This policy ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The background dump directory has insecure permissions. The background dump directory (%dir_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *backgrdDumpDestRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

Action

Restrict permissions to the Background Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.2.19 Control File Permission

This policy ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The control file (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *dbControlFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

Action

Restrict permission to the control files to:

- Owner of the Oracle software installation
- DBA group

Do not give read and write permissions to public.

5.2.20 Core Dump Destination

This policy ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The core dump directory has insecure permissions. The core dump directory (%dir_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *coreDumpDestRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

Action

Restrict permissions to the Core Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.2.21 Default Passwords

This policy ensures there are no default passwords for known accounts.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Default password for the account %dbaccount% has not been changed. |

¹ The policy rule is evaluated each time its underlying *defaultAccountPasswordsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using default passwords.

Action

Change all default passwords.

5.2.22 Default Table Space

This policy ensures that users are not assigned SYSTEM or SYSAUX as their default tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The tablespace %tablespace% is the default tablespace for user %dbuser%. |

¹ The policy rule is evaluated each time its underlying *dfltTableSpaceRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Users objects are created in the default tablespaces. An incorrectly set default tablespace (SYSTEM or SYSAUX) for a user can consume all available space thus causing the database to stop working.

A user assigned the default tablespace as SYSTEM can potentially fill up the space and cause the database to stop responding. This can also cause denial of service exploits. The SYSTEM tablespace always contains the data dictionary tables for the entire database.

All data stored on behalf of stored PL/SQL program units (procedures, functions, packages, and triggers) resides in the SYSTEM tablespace.

Action

Reassign the tablespace of users having SYSTEM or SYSAUX defined as their default tablespace.

5.2.23 Excessive Allowed Failed Login Attempts

This policy ensures that the number of allowed failed login attempts is no more than 10.

The FAILED_LOGIN_ATTEMPTS parameter defines the number of successive failed login attempts that can be performed before an account's status is changed to locked. This protects against malicious users attempting to guess a password for an account.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. FAILED_LOGIN_ATTEMPTS is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *loginserver_failed_logins* metric is collected.

Defaults

Parameters and Their Default Values

Maximum FAILED_LOGIN_ATTEMPTS: 10 failed attempts

Objects Excluded by Default

None

Impact of Violation

Permits manual and automated password guessing by a malicious user.

By setting the parameter to UNLIMITED, a malicious user can attempt an unlimited amount of guesses of the password for all accounts granted the specified profile. However, setting the value too low may result in valid users locking their accounts when mistyping a password.

Action

In user profiles, set the value for the FAILED_LOGIN_ATTEMPTS setting to no more than 10.

5.2.24 Excessive PUBLIC EXECUTE Privileges

Checks for PUBLIC having execute privileges on powerful packages (UTL_HTTP, UTL_TCP and UTL_SMTP).

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in insecure state. EXECUTE privilege on the package %package% is granted to the PUBLIC role. |

¹ The policy rule is evaluated each time its underlying *executePrivilegesRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to e-mail, network, and http modules using the EXECUTE privilege.

Action

Revoke EXECUTE privileges on powerful packages.

5.2.25 Execute UTL_FILE Privileges to PUBLIC

This policy ensures the PUBLIC role does not have EXECUTE privilege on the UTL_FILE package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. EXECUTE privilege on UTL_FILE package is granted to PUBLIC. |

¹ The policy rule is evaluated each time its underlying *pubexecutePrivilegesRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can read and write arbitrary files in the system when granted the UTL_FILE privilege.

Action

Revoke EXECUTE privileges granted to UTL_FILE package from PUBLIC.

5.2.26 IFILE Referenced File Permission

This policy ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The IFILE parameter referenced file (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *iFileRefFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict access to the files referenced by the IFILE initialization parameter to:

- Owner of Oracle software installation
- DBA group

Do not give read, write, and execute permissions to public.

5.2.27 Initialization Parameter File Permission

This policy ensures that access to the initialization parameter file is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The text initialization parameter file (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *initoraPermRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Oracle traditionally stored initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict access to the initialization parameter file to:

- Owner of Oracle software installation
- DBA group

Do not give read and write permissions to public.

5.2.28 Log Archive Destination Owner

This policy ensures that the server's archive logs directory is a valid directory owned by the Oracle software owner and that there are no permissions to public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state as the directory (%dir_name%) specified by the LOG_ARCHIVE_DEST parameter is owned by %owner%. |

¹ The policy rule is evaluated each time its underlying *logArchiveDestRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in the init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

In other words, if the path or device name specified by the LOG_ARCHIVE_DEST initialization parameter is not owned by the owner of the Oracle software installation, anyone can use LogMiner to extract database information from the archive logs.

Action

Directory specified by LOG_ARCHIVE_DEST parameter should be owned by the Oracle software set.

Do not grant public read permission to the LOG_ARCHIVE_DEST initialization parameter. Restrict access to the path or device name referenced by the LOG_ARCHIVE_DEST initialization parameter to the owner of the Oracle software installation.

5.2.29 Log Archive Destination Permission

This policy ensures that the server's archive logs are not accessible to public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The directory (%dir_name%) specified by the LOG_ARCHIVE_DEST parameter has an inappropriate permission: %permission%. |

¹ The policy rule is evaluated each time its underlying *logArchiveDestRep* metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

None

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in the init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

Action

Permissions of the directory specified by LOG_ARCHIVE_DEST parameter should be restricted to the owner of the Oracle software set and DBA group with no permissions to public.

5.2.30 Log Archive Duplex Destination Owner

This policy ensures that the server's archive logs directory is a valid directory owned by the Oracle software owner and that there are no permissions to public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state as the directory (%dir_name%) specified by the LOG_ARCHIVE_DUPLEX_DEST parameter is owned by %owner%. |

¹ The policy rule is evaluated each time its underlying *logArchiveDupDestRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

In other words, if the path or device name specified by the LOG_ARCHIVE_DUPLEX_DEST initialization parameter is not owned by the owner of the Oracle software installation, anyone can use LogMiner to extract database information from the archive logs.

Action

Directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter should be owned by the Oracle software set.

5.2.31 Log Archive Duplex Destination Permission

This policy ensures that the server's archive logs are not accessible to public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The directory(%dir_name%) specified by the LOG_ARCHIVE_DUPLEX_DEST parameter has an inappropriate permission: %permission%. |

¹ The policy rule is evaluated each time its underlying *logArchiveDupDestRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

Action

Permissions of the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter should be restricted to the owner of the Oracle software set and DBA group with no permissions to public.

5.2.32 Naming Database Links

This policy ensures that the name of a database link is the same as that of the remote database.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The GLOBAL_NAMES parameter is set to %:value%. |

¹ The policy rule is evaluated each time its underlying *dbLinkGBLNameRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Database link names that do not match the global names of the databases to which they are connecting can cause an administrator to inadvertently give access to a production server from a test or development server. Knowledge of this can be used by a malicious user to gain access to the target database.

Action

If you use or plan to use distributed processing, Oracle recommends that you set the GLOBAL_NAMES initialization parameter to TRUE to ensure the use of consistent naming conventions for databases and links in a networked environment.

5.2.33 Oracle Home Datafile Permission

This policy ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The datafile (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *dbDataFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The datafiles contain all the database data. If datafiles are made readable to public, they can be read by a user who has no database privileges on the data.

Action

Restrict permissions to the datafiles to:

- Owner of the Oracle software set
- DBA group

Do not give read and write permissions to public.

5.2.34 Oracle Home Executable Files Owner

This policy ensures that the ownership of all files and directories in the ORACLE_HOME/bin folder is the same as the Oracle software installation owner.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Owner of (%file_name%) is %owner% who is not the owner of the Oracle software installation. |

¹ The policy rule is evaluated each time its underlying *ohBinFilesOwnerRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Incorrect file permissions on some of the Oracle files can cause major security issues. For example, SQL*Plus could be replaced with a malicious script which the user might run inadvertently.

Action

For files and directories in the ORACLE_HOME/bin folder that do not have the same owner as the Oracle software installation, change their owner to the installation owner.

5.2.35 Oracle Home Executable Files Permission

This policy ensures that all files in the ORACLE_HOME/bin folder have permissions set to 0751 or less.

For Oracle9i Release 2, permissions should be set to 0755. This means that Group and Others have only read and execute permissions; no write permission.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. File (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *ohExeBinFilesPermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Incorrect file permissions on some of the Oracle files can cause major security issues.

Action

For files in the ORACLE_HOME/bin folder that do not have permissions set to 0751 or less, change their file permissions to 0751 or less.

For Oracle9i Release 2, set permissions to 0755.

5.2.36 Oracle Home File Permission

This policy ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) have permission set to 0750 or less.

Normally, only the owner and DBA group members must be allowed to work with non-executable files in the Oracle Home.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. File (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *ohFilesPermissionRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Incorrect file permissions on some of the Oracle files can cause major security issues.

Action

All files in \$ORACLE_HOME directories (except for \$ORACLE_HOME/bin) must have permission set to 0750 or less.

5.2.37 Password Grace Time

This policy ensures that all profiles have PASSWORD_GRACE_TIME set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_GRACE_TIME is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdGraceRep* metric is collected.

Defaults

Parameters and Their Default Values

MAX_PASSWORD_GRACE_TIME = 3

Objects Excluded by Default

Not Applicable

Impact of Violation

A high value for the PASSWORD_GRACE_TIME parameter may cause serious database security issues by allowing the user to keep the same password for a long time.

Action

Set the PASSWORD_GRACE_TIME parameter to no more than 3 days for all profiles.

5.2.38 Password Life Time

This policy ensures that all profiles have PASSWORD_LIFE_TIME set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_LIFE_TIME is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdLifeRep* metric is collected.

Defaults

Parameters and Their Default Values

MAX_PASSWORD_LIFE_TIME = 90

Objects Excluded by Default

Not Applicable

Impact of Violation

A long password life time gives malicious users a long time to decipher the password. May cause serious database security issues.

Action

Set the PASSWORD_LIFE_TIME parameter to no more than 90 days for all profiles.

5.2.39 Password Locking Time

This policy ensures that PASSWORD_LOCK_TIME is set to a reasonable number of days for all profiles.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_LOCK_TIME is set to %limit% days for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *pwdLockRep* metric is collected.

Defaults

Parameters and Their Default Values

MIN_PASSWORD_LOCK_TIME = 1

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_LOCK_TIME resource relates to the number of days an account is locked after a user tries unsuccessfully to login for more than FAILED_LOGIN_

ATTEMPTS (another related resource) times. Having a low value for this resource increases the likelihood of Denial of Service attacks.

Action

Set the PASSWORD_LOCK_TIME parameter to no less than 1 for all the profiles.

5.2.40 Password Reuse Maximum

This policy ensures that all profiles have PASSWORD_REUSE_MAX set to a reasonable number of times.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_REUSE_MAX is set to %limit% times for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *reuseMaxRep* metric is collected.

Defaults

Parameters and Their Default Values

MAX_PASSWORD_REUSE_MAX = 20

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_REUSE_MAX parameter specifies the number of password changes required before the current password can be reused. Old passwords are usually the best guesses for the current password. A low value for the PASSWORD_REUSE_MAX parameter may cause serious database security issues by allowing users to reuse their old passwords more often. Ensuring a reasonable value for this resource will discourage users from reusing their passwords resulting in more secure password usage.

Action

Set the PASSWORD_REUSE_MAX parameter to no less than 20 times for all profiles.

5.2.41 Password Reuse Time

This policy ensures that all profiles have PASSWORD_REUSE_TIME set to a reasonable number of days.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. PASSWORD_REUSE_TIME is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *passwdReuseTimeRep* metric is collected.

Defaults

Parameters and Their Default Values

MAX_PASSWORD_REUSE_TIME = 2147483647

Objects Excluded by Default

Not Applicable

Impact of Violation

The PASSWORD_REUSE_TIME parameter defines the number of days before a password can be reused. A low value for the password reuse time can increase the danger of an already leaked password to cause serious database security issues.

Ensuring a reasonable value for this resource will discourage users from reusing their passwords resulting in more secure password usage.

Action

Set the PASSWORD_REUSE_TIME parameter to UNLIMITED for all profiles.

5.2.42 Profiles with Excessive Allowed Failed Login Attempts

This policy ensures that the number of allowed failed login attempts is no more than 10.

The FAILED_LOGIN_ATTEMPTS parameter defines the number of successive failed login attempts that can be performed before an account's status is changed to locked. This protects against malicious users attempting to guess a password for an account.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. FAILED_LOGIN_ATTEMPTS is set to %limit% for the profile %profile%. |

¹ The policy rule is evaluated each time its underlying *loginserver_failed_logins* metric is collected.

Defaults

Parameters and Their Default Values

Maximum FAILED_LOGIN_ATTEMPTS: 10 failed attempts

Objects Excluded by Default

Not Applicable

Impact of Violation

Permits manual and automated password guessing by a malicious user.

By setting the parameter to UNLIMITED, a malicious user can attempt an unlimited amount of guesses of the password for all accounts granted the specified profile. However, setting the value too low may result in valid users locking their accounts when mistyping a password.

Action

In user profiles, set the value for the FAILED_LOGIN_ATTEMPTS setting to no more than 10.

5.2.43 PUBLIC EXECUTE Privileges to DBMS Job

This policy ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_JOB package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsJobPrivsRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Granting EXECUTE privilege to PUBLIC on DBMS_JOB package allows all users to schedule jobs on the database.

Action

PUBLIC must not be granted EXECUTE privileges on DBMS_JOB package.

5.2.44 PUBLIC EXECUTE Privileges to DBMS LOB

This policy ensures PUBLIC group is not granted EXECUTE privileges to the DBMS_LOB package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_LOB package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsLobRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBMS_LOB package can be used to access any file on the system as the owner of the Oracle software installation.

Action

Revoke the EXECUTE privileges on DBMS_LOB package from the PUBLIC group.

5.2.45 PUBLIC EXECUTE Privileges to DBMS SYS SQL

This policy ensures PUBLIC is not granted EXECUTE privileges on DBMS_SYS_SQL package.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. DBMS_SYS_SQL package has PUBLIC EXECUTE privileges. |

¹ The policy rule is evaluated each time its underlying *dbmsSysSqlRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The DBMS_SYS_SQL package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.

Action

Revoke the EXECUTE privileges on DBMS_SYS_SQL package from the PUBLIC group.

5.2.46 PUBLIC Trace Files

This policy ensures database trace files are not public readable.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. _TRACE_FILES_PUBLIC initialization parameter is set to :%value%. |

¹ The policy rule is evaluated each time its underlying *trcFilePublicRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If trace files are readable by the PUBLIC group, a malicious user may attempt to read the trace files. This could lead to sensitive information being exposed, for example, creation or deletion of tablespace information.

Action

Set the initialization parameter _TRACE_FILES_PUBLIC to FALSE.

5.2.47 Remote OS Authentication

This policy ensures REMOTE_OS_AUTHENT initialization parameter is set to FALSE.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. REMOTE_OS_AUTHENT initialization parameter is set to %remote_os_auth%. |

¹ The policy rule is evaluated each time its underlying *remoteAuthenticationRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database if remote OS authentication is allowed. This feature allows external users (authenticated by the remote OS) to connect to the database without having password authentication done by the database.

Action

Disable this feature by setting the REMOTE_OS_AUTHENT initialization parameter to FALSE.

5.2.48 Remote OS Role

This policy ensures REMOTE_OS_ROLES initialization parameter is set to FALSE.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. REMOTE_OS_ROLES initialization parameter is set to %value%. |

¹ The policy rule is evaluated each time its underlying *remoteRolesRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database if remote users can be granted privileged roles.

Action

Disable this feature by setting the REMOTE_OS_ROLES initialization parameter to FALSE.

5.2.49 Remote Password File

This policy ensures that the REMOTE_LOGIN_PASSWORDFILE initialization parameter is set to EXCLUSIVE.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. REMOTE_LOGIN_PASSWORDFILE initialization parameter is set to %value%. |

¹ The policy rule is evaluated each time its underlying *remoteLoginPasswordFileRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database if remote password files are allowed.

Action

For non-RAC configurations, set the REMOTE_LOGIN_PASSWORDFILE setting to EXCLUSIVE mode, thereby assigning specific users the SYSDBA/SYSOPER privilege to manage the database.

5.2.50 Secure OS Audit Level

This policy ensures that AUDIT_SYSLOG_LEVEL is set to a non-default value when OS-level auditing is enabled, on UNIX systems.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The AUDIT_SYSLOG_LEVEL initialization parameter is set to %logLevel%. |

¹ The policy rule is evaluated each time its underlying *secureOSAuditLevelRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Setting the AUDIT_SYSLOG_LEVEL initialization parameter to the default value (NONE) will result in DBAs gaining access to the OS audit records.

Action

When operating system auditing is enabled, set the AUDIT_SYSLOG_LEVEL initialization parameter to a valid value and configure `/etc/syslog.conf` so that Oracle OS audit records are written to a separate file.

5.2.51 Server Parameter File Permission

This policy ensures that access to the server parameter file (SPFILE) is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The server parameter file (%file_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *spfilePermRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict permission to the server parameter file (SPFILE) to:

- Oracle software owner
- Oracle group

Do not give read and write permissions to public.

5.2.52 System Privileges to Public

This policy ensures system privileges are not granted to PUBLIC.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. System privilege %privilege% is assigned to the PUBLIC role. |

¹ The policy rule is evaluated each time its underlying *systemPrivilegesRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Privileges granted to the PUBLIC role automatically apply to all users. There are security risks when granting SYSTEM privileges to all users.

Action

Revoke SYSTEM privileges from the PUBLIC role.

5.2.53 Unlimited Tablespace Quota

This policy ensures that database users are allocated a limited tablespace quota.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. User %dbuser% has an unlimited tablespace quota. |

¹ The policy rule is evaluated each time its underlying *tableSpaceQuotaRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Granting unlimited tablespace quotas can cause the filling up of the allocated disk space. This can lead to an unresponsive database.

Action

For users with an unlimited tablespace quota, reallocate their tablespace quotas to a specific limit.

5.2.54 Use of Appropriate umask on UNIX Systems

On UNIX systems, this policy ensures that log and trace files do not become accessible to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The umask value for the Oracle software owner is set to %umask%. |

¹ The policy rule is evaluated each time its underlying *umaskSettingRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If umask is not set to an appropriate value (such as 022), log or trace files might become accessible to the public, thus exposing sensitive information.

Action

Set umask to 022 for the owner of Oracle software.

5.2.55 Use of Automatic Log Archival Features

This policy ensures that archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. Only applicable if database is in archivelog mode.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. LOG_ARCHIVE_START initialization parameter is set to %value%. |

¹ The policy rule is evaluated each time its underlying *logArchiveStartRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Setting the LOG_ARCHIVE_START initialization parameter to TRUE ensures that the archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. This feature is only applicable if the database is in archivelog mode.

If the LOG_ARCHIVE_START initialization parameter is set to FALSE, redo log files are not automatically archived and instance operations are suspended when the redo logs are full.

Action

Set the value of the LOG_ARCHIVE_START initialization parameter to TRUE.

5.2.56 Use of Basic Audit Features

This policy ensures that basic auditing features are enabled.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------|
| Informational | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. AUDIT_TRAIL initialization parameter is set to %value%. |

¹ The policy rule is evaluated each time its underlying *auditTrailRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Not enabling basic audit features might increase the likelihood of a denial of service attack going unnoticed.

Action

Enable auditing by setting the AUDIT_TRAIL initialization parameter to a value other than NONE or FALSE. A value of OS is the most secure setting.

5.2.57 Use of Database Links with Cleartext Password

Ensures database links with clear text passwords are not used, that is, the password is hashed or encrypted.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|---------------------------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 9 <i>i</i> and pre-9 <i>i</i> | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Database link %link% has clear text password. |

¹ The policy rule is evaluated each time its underlying *dbLinkPwdRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The table SYS.LINK\$ contains the clear text password used by the database link. A malicious user can read clear text password from SYS.LINK\$ table that can lead to undesirable consequences.

Action

Avoid creating fixed user database links.

5.2.58 Use of Remote Listener Instances

This policy ensures listener instances on a remote machine separate from the database instance are not used.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database may be in an insecure state as REMOTE_LISTENER initialization parameter is set to %value%. |

¹ The policy rule is evaluated each time its underlying *rmtLsnrRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The REMOTE_LISTENER initialization parameter can be used to allow a listener on a remote machine to access the database. This parameter is not applicable in a multi-master replication or RAC environment where this setting provides a load balancing mechanism for the listener.

Action

REMOTE_LISTENER should be set to the null string (""). This parameter is not applicable in a multi-master replication or RAC environment where this setting provides a load balancing mechanism for the listener.

5.2.59 Use of SQL92 Security Features

This policy ensures the use of the SQL92 security features.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-----------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 9i and pre-9i | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. SQL92 security features are not enabled. |

¹ The policy rule is evaluated each time its underlying *sql92Rep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If SQL92 security features are not enabled, a user might be able to execute an UPDATE or DELETE statement using a WHERE clause without having select privilege on a table.

Action

Enable SQL92 security features by setting the initialization parameter SQL92_SECURITY to TRUE.

5.2.60 User Dump Destination

This policy ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The user dump directory has insecure permissions. The user dump directory (%dir_name%) permission is %permission%. |

¹ The policy rule is evaluated each time its underlying *userDumpDestRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

Action

Restrict permissions to the User Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.2.61 User Temporary Table Space

This policy ensures that users are not assigned SYSTEM or SYSAUX as their temporary tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The tablespace %tablespace% is the default temporary tablespace for user %dbuser%. |

¹ The policy rule is evaluated each time its underlying *tempTableSpaceRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The user's temporary objects are created in the temporary tablespace. An incorrectly set temporary tablespace (SYSTEM or SYSAUX) for a user can consume all available space thus causing the database to stop working.

A user assigned the default tablespace as SYSTEM can potentially fill up the space and cause the database to stop responding. This can also cause denial of service exploits. The SYSTEM tablespace always contains the data dictionary tables for the entire database.

All data stored on behalf of stored PL/SQL program units (procedures, functions, packages, and triggers) resides in the SYSTEM tablespace.

Action

Reassign the tablespace of users having SYSTEM or SYSAUX defined as their default temporary tablespace.

5.2.62 Using Externally Identified Accounts

This policy ensures that the OS_AUTHENT_PREFIX is set to a value other than OPS\$ or null string ("").

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Operating System authentication prefix is set to %value%. |

¹ The policy rule is evaluated each time its underlying *osAuthRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Setting this parameter ensures that the only way an account can be used externally is by specifying IDENTIFIED EXTERNALLY when creating a user.

Action

The identified externally approach should only be used on development and test databases. On a production system, ensure that the user cannot access the operating system level.

5.2.63 Utility File Directory Initialization Parameter Setting

This policy ensures that the Utility File Directory (UTL_FILE_DIR) initialization parameter is not set to one of the following: asterisk (*), period (.), or core dump trace file locations.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|-------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. UTL_FILE_DIR parameter is set to %dir_name%. |

¹ The policy rule is evaluated each time its underlying *utilFileDirSettingRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Specifies the directories which the UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories, could expose them to all users having execute privilege on the UTL_FILE package.

Action

Change the UTL_FILE_DIR initialization parameter to a value other than asterisk (*), period (.), or to core dump trace locations.

5.2.64 Utility File Directory Initialization Parameter Setting for Oracle9i Release 1 and Later

This policy ensures that the UTL_FILE_DIR initialization parameter is not used in Oracle9i Release 1 and later.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|---------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 9i or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. UTL_FILE_DIR parameter (set to %dir_name%) is used in a 9i+ server. |

¹ The policy rule is evaluated each time its underlying *utlSetting9IplusRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Specifies the directories which UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories could expose them to all users having execute privilege on UTL_FILE package.

Using the UTL_FILE package it is possible to write programs to access the directories set by utl_file_dir (assuming the user has execute privilege on this package). There is a possibility that the program is used to read files and data that should not be otherwise possible.

Action

For Oracle 9i Release 1 and later, remove the UTL_FILE_DIR initialization parameter. Instead, use the CREATE DIRECTORY feature.

5.2.65 Well Known Accounts

This policy ensures well-known accounts are expired and locked.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Account %dbaccount% is not locked and terminated. |

¹ The policy rule is evaluated each time its underlying *installAndDemoAccountsRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using a well-known account.

Action

Expire and lock well-known accounts.

5.2.66 Well Known Accounts (Status)

This policy ensures well-known accounts are expired and locked.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------|
| Warning | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. Account %dbaccount% is not locked and terminated. |

¹ The policy rule is evaluated each time its underlying *installAndDemoAccountsRepmetric* is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user can gain access to the database using a well-known account.

Action

Expire and lock well-known accounts.

5.3 Security Policies - Windows

The security policies for the Database Instance on Windows target are:

5.3.1 Audit File Destination (Windows)

This policy ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The audit file directory has insecure permissions. The users %users% have critical permissions on audit file directory %dir_name% |

¹ The policy rule is evaluated each time its underlying *auditFileDestNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

Action

Restrict permissions to the Audit File directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.3.2 Background Dump Destination (Windows)

This policy ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The background dump directory has insecure permissions. The users %users% have critical permissions on background dump directory (%dir_name%). |

¹ The policy rule is evaluated each time its underlying *backgrdDumpDestNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

Action

Restrict permissions to the Background Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.3.3 Control File Permission (Windows)

This policy ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the control file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *dbControlFilesPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

Action

Restrict permission to the control files to:

- Owner of the Oracle software installation
- DBA group

Do not give read and write permissions to public.

5.3.4 Core Dump Destination (Windows)

This policy ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The core dump directory has insecure permissions. The users %users% have critical permissions on core dump directory (%dir_name%). |

¹ The policy rule is evaluated each time its underlying *coreDumpDestNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Core dump files are stored in the directory specified by the *CORE_DUMP_DEST* initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

Action

Restrict permissions to the Core Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.3.5 IFILE Referenced File Permission (Windows)

This policy ensures that access to the files referenced by the *IFILE* parameter is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: *DELETE*, *WRITE_DAC*, *WRITE_OWNER*, *CHANGE*, *ADD*, and *FULL*. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the <i>IFILE</i> parameter referenced file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *iFileRefFilesPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict access to the files referenced by the IFILE initialization parameter to:

- Owner of Oracle software installation
- DBA group

Do not give read, write, and execute permissions to public.

5.3.6 Initialization Parameter File Permission (Windows)

This policy ensures that access to the initialization parameter file is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the text initialization parameter file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *initoraPermNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Oracle traditionally stored initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict access to the initialization parameter file to:

- Owner of Oracle software installation
- DBA group

Do not give read and write permissions to public.

5.3.7 Log Archive Destination Permission (Windows)

This policy ensures that the server's archive logs are not accessible to public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the directory (%dir_name%) specified by the LOG_ARCHIVE_DEST parameter. |

¹ The policy rule is evaluated each time its underlying *logArchiveDestNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Database may be in insecure state as the directory (%file_name%) specified by the LOG_ARCHIVE_DEST parameter has an inappropriate permission or owner: %permission%.

Objects Excluded by Default

Database may be in insecure state as the directory (%file_name%) specified by the LOG_ARCHIVE_DEST parameter has an inappropriate permission or owner: %permission%.

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in the init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

Action

Permissions of the directory specified by LOG_ARCHIVE_DEST parameter should be restricted to the owner of the Oracle software set and DBA group with no permissions to public.

5.3.8 Log Archive Duplex Destination Permission (Windows)

This policy ensures that the server's archive logs are not accessible to public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the directory (%dir_name%) specified by the LOG_ARCHIVE_DUPLEX_DEST parameter. |

¹ The policy rule is evaluated each time its underlying *logArchiveDupDestNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

Action

Permissions of the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter should be restricted to the owner of the Oracle software set and DBA group with no permissions to public.

5.3.9 Oracle Home Datafile Permission (Windows)

This policy ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------------------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance; Cluster Database | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the datafile (%file_name%). |

¹ The policy rule is evaluated each time its underlying *dbDataFilesPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The datafiles contain all the database data. If datafiles are made readable to public, they can be read by a user who has no database privileges on the data.

Action

Restrict permissions to the datafiles to:

- Owner of the Oracle software set
- DBA group

Do not give read and write permissions to public.

5.3.10 Oracle Home Executable Files Permission (Windows)

This policy ensures that all files in the ORACLE_HOME/bin folder have appropriate permissions. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *ohExeBinFilesPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Incorrect file permissions on some of the Oracle files can cause major security issues.

Action

For files in the ORACLE_HOME/bin folder, revoke unnecessary right given to users or user groups.

5.3.11 Oracle Home File Permission (Windows)

This policy ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) have permission set appropriately. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Normally, only the owner and DBA group members must be allowed to work with non-executable files in the Oracle Home.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------|
| Warning | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *ohFilesPermissionNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Incorrect file permissions on some of the Oracle files can cause major security issues.

Action

All files in \$ORACLE_HOME directories must have permission set appropriately.

5.3.12 Server Parameter File Permission (Windows)

This policy ensures that access to the server parameter file (SPFILE) is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_

OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. The users %users% have critical permissions on the server parameter file (%file_name%). |

¹ The policy rule is evaluated each time its underlying *spfilePermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

Action

Restrict permission to the server parameter file (SPFILE) to:

- Oracle software owner
- Oracle group

Do not give read and write permissions to public.

5.3.13 Use of Windows NT Domain Prefix (Windows)

This policy ensures externally identified users specify the domain while connecting.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in an insecure state. OSAUTH_PREFIX_DOMAIN is not set to TRUE. |

¹ The policy rule is evaluated each time its underlying *osauthPrefixDomainRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If externally identified accounts are required, setting OSAUTH_PREFIX_DOMAIN to TRUE in the registry forces the account to specify the domain. This prevents spoofing of user access from an alternate domain or local system.

Action

For externally identified users from Windows systems, set the OSAUTH_PREFIX_DOMAIN initialization parameter to TRUE.

5.3.14 User Dump Destination (Windows)

This policy ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Database Instance | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The user dump directory has insecure permissions. The users %users% have critical permissions on user dump directory (%dir_name%). |

¹ The policy rule is evaluated each time its underlying *userDumpDestNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

Action

Restrict permissions to the User Dump directory to:

- Owner of the Oracle software set
- DBA group

Do not give read, write, and execute permissions to public.

5.4 Storage Policies

The storage policies for the Database Instance target are:

5.4.1 Default Permanent Tablespace Set to a System Tablespace

This policy verifies that the DEFAULT_PERMANENT_TABLESPACE database property is set to a non-system tablespace. The default permanent tablespace for the database is used as the default permanent tablespace for any users who are not explicitly assigned a permanent tablespace. The default permanent tablespace is defaulted to the SYSTEM tablespace until it is changed by a DBA.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|--------------------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance; Cluster Database | Oracle Server 10g Release 1 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The default permanent tablespace is not set explicitly and defaults to SYSTEM tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults

Parameters and Their Default Values

SYSTEM

Objects Excluded by Default

Not Applicable

Impact of Violation

If not specified explicitly, the DEFAULT_PERMANENT_TABLESPACE is defaulted to the SYSTEM tablespace. This is not the recommended setting. The default permanent tablespace for the database is used as the permanent tablespace for any non-SYSTEM users who are not explicitly assigned a permanent tablespace. If the database default permanent tablespace is set to a system tablespace, then any user who is not explicitly assigned a tablespace uses the system tablespace. Non-SYSTEM users should not be using a system tablespaces to store data. Doing so may result in performance degradation for the database.

Action

Set the DEFAULT_PERMANENT_TABLESPACE to a non-system tablespace. Create or edit a tablespace and set it to be the default permanent tablespace.

Clicking the `DEFAULT_PERMANENT_TABLESPACE` link will bring up the Tablespace Search page. From this page you can create or edit a tablespace and set it to be the default permanent tablespace.

On the Administration property page for the database instance, click **Tablespaces** under the Storage options. After providing your credentials, create or edit a permanent tablespace and set it to be the default permanent tablespace.

5.4.2 Default Temporary Tablespace Set to a System Tablespace

This policy verifies that the `DEFAULT_TEMP_TABLESPACE` database property is set to a non-system tablespace. The default temporary tablespace for the database is used as the temporary tablespace for any users that are not explicitly assigned a temporary tablespace. The temporary tablespace is defaulted to the `SYSTEM` tablespace until it is changed by a DBA.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|---------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------|
| Warning | Storage | Database Instance; Cluster Database | Oracle Server 9i or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The default temporary tablespace is not set explicitly and defaults to <code>SYSTEM</code> tablespace. |

¹ The policy rule is evaluated each time its underlying `db_recTablespaceSettings` metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

If not specified explicitly, the `DEFAULT_TEMP_TABLESPACE` defaults to the `SYSTEM` tablespace. This is not the recommended setting. The default temporary tablespace is used as the temporary tablespace for any users who are not explicitly assigned a temporary tablespace. If the database default temporary tablespace is set to a system tablespace, then any user who is not explicitly assigned a temporary tablespace uses the system tablespace as their temporary tablespace. System tablespaces should not be used to store temporary data. Doing so can result in performance degradation for the database.

Action

Set the `DEFAULT_TEMP_TABLESPACE` to a non-system temporary tablespace. In Oracle Database 10g Release 1 or later, you can also set the `DEFAULT_TEMP_TABLESPACE` to a temporary tablespace group. Create or edit a temporary tablespace, or temporary tablespace group, and set it to be the default temporary tablespace.

Clicking the `DEFAULT_TEMP_TABLESPACE` link will bring up the Tablespace Search page. From this page the user can create or edit a temporary tablespace and set it to be the default temporary tablespace.

On the Administration property page for the database instance, click **Tablespaces** under the Storage options. After providing your credentials, create or edit a temporary tablespace and set it to be the default temporary tablespace.

5.4.3 Dictionary Managed Tablespaces

This policy determines whether dictionary managed tablespaces are being used. Use locally managed tablespaces.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% is dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management. |

¹ The policy rule is evaluated each time its underlying `db_recTablespaceSettings` metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

These tablespaces are dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management.

Action

Redefine these tablespaces to be locally managed.

5.4.4 Insufficient Redo Log Size

This policy, using the `SMALL_REDO_LOGS` parameter, checks for redo log files that are less than 1 MB.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------|
| Critical | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Your database has redo log that has insufficient size. |

¹ The policy rule is evaluated each time its underlying *db_redo_logs* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Small redo logs cause system checkpoints to continuously put a high load on the buffer cache and I/O system.

Action

Increase size of the redo logs to at least 1 MB.

5.4.5 Non-System Data Segments in a System Tablespace

Redefine the tablespaces containing the segments to be locally managed; or, reorganize these segments, specifying a Next Extent value that is a multiple of Initial Extent, and a Percent Increase value of 0.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Segment %OBJECT% belonging to non-system users are stored in system tablespace %TABLESPACE_NAME%. This makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recSegmentSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Cluster object types because the Reorganize Objects wizard does not support them.

All user accounts that are, by default, part of the Oracle Database or Enterprise Manager. For example: SYS, SYSTEM, SYSMAN, CTXSYS, SCOTT, ADAMS, and so on.

Impact of Violation

These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX. This violation makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. System users include users that are part of the DBMS such as SYS and SYSTEM, or that are part of Oracle-supplied facilities: for example, CTXSYS, SYSMAN, and OLAPSYS.

Action

Relocate the non-system segments to a non-system tablespace.

5.4.6 Non-Uniform Default Extent Size for Dictionary Managed Tablespaces

This policy checks for tablespaces with non-uniform default extent size.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% uses non-uniform extents. Using uniform extents ensures that any free extent in the tablespace can always be used for any segment in the tablespace. |

¹ The policy rule is evaluated each time its underlying *db_tablespaces* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

SYSTEM tablespace. This policy is only applicable to PERMANENT DICTIONARY tablespaces.

Impact of Violation

Tablespaces using a non-uniform default extent size exist. Extents in a tablespace should be the same size. This ensures that any free extent in the tablespace can always be used for any segment in the tablespace.

Action

To ensure uniform extent sizes, set each tablespace's default storage clause so that the NEXT value should be equal to or a multiple of the INITIAL value, and the PCTINCREASE value is set to zero. Then never explicitly specify a storage clause at the segment level. Instead, let the storage values for the segments be inherited from the default storage clause of the tablespace.

5.4.7 Rollback in SYSTEM Tablespace

Rollback in SYSTEM Tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|-------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | See following table | Yes | Your SYSTEM tablespace contains rollback segment %RBS_NAME%. The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. |

¹ The policy rule is evaluated each time its underlying metric is collected.

The following table lists the policy's underlying metrics.

| Underlying Metric | Collection Frequency |
|-------------------------|----------------------|
| <i>db_init_params</i> | Every 24 hours |
| <i>db_rollback_segs</i> | Every 24 hours |

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. It should NOT be used to store any other types of objects such as user tables, user indexes, user views, rollback segments, undo segments, or temporary segments.

Action

Use a tablespace dedicated to undo instead of the SYSTEM tablespace.

5.4.8 Segment in Dictionary Tablespace with Extent Growth Policy Violation

This policy, using the SEG_EXT_GROWTH_VIO parameter, checks for segments in dictionary managed tablespaces having irregular extent sizes and/or non-zero Percent Increase settings.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Segment %OBJECT% in dictionary managed tablespace %TABLESPACE_NAME% has irregular extent sizes and/or non-zero Percent Increase settings. This can result in inefficient reuse of space and fragmentation problems. |

¹ The policy rule is evaluated each time its underlying *db_recSegmentSettings* metric is collected.

Defaults**Parameters and Their Default Values**

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

These segments have extents with sizes that are not multiples of the initial extent, and/or a non-zero Percent Increase setting. This can result in inefficient reuse of space and fragmentation problems.

Action

Redefine the tablespaces containing the segments to be locally managed; or, reorganize these segments, specifying a Next Extent value that is a multiple of Initial Extent, and a Percent Increase value of 0.

5.4.9 Tablespace Not Using Automatic Segment-Space Management

This policy checks for locally managed tablespaces that are using MANUAL segment space management.

There are two segment-space management settings, MANUAL and AUTO.

- MANUAL segment-space management uses free lists to manage free space within segments. Free lists are lists of data blocks that have space available for inserting rows. With this form of segment-space management, you must specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace.
- AUTO segment-space management uses bitmaps to manage the free space in segments. The bitmap describes the status of each data block within a segment with respect to the amount of space in the block available for inserting rows. These bitmaps allow the database to manage free space automatically.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------------------------------|----------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | Oracle Server 9.2 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% is not using automatic segment-space management. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

Automatic segment-space management is a simpler and more efficient way of managing space within a segment. It completely eliminates any need to specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace.

In a RAC environment, there is the additional benefit of avoiding the hard partitioning of space inherent with using free list groups.

Action

Change the segment-space management of all permanent locally managed tablespaces to AUTO.

Clicking the name of each tablespace listed will bring up the Reorganize Objects wizard with the tablespace automatically selected. This wizard allows you to change the segment-space management of the tablespace from MANUAL to AUTO.

5.4.10 Tablespaces Containing Rollback and Data Segments

This policy, using the TBSP_MIXED_SEGS parameter, checks for tablespaces containing both rollback and data segments.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | Tablespace %TABLESPACE_NAME% contains both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recTablespaceSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

SYSTEM tablespace

Impact of Violation

These tablespaces contain both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the tablespace. Use of a dedicated tablespace for rollback segments enhances availability and performance.

Action

Use Automatic Undo Management (in Oracle Server Release 9.0.1 or later) and perform one of the following:

- Drop the rollback segments from this tablespace.
- Create one or more tablespaces dedicated to rollback segments and drop the rollback segments from this tablespace.
- Dedicate this tablespace to rollback segments and move the data segments to another tablespace.

5.4.11 Users with a System Tablespace as Default Tablespace

This policy, using the `SYSTEM_AS_DEFAULT_TBSP` parameter, checks for any user having a System tablespace listed as their default tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|-------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | All | The underlying metric has a collection frequency of once every 24 hours. | Yes | User %USER_NAME% uses SYSTEM tablespace as the default tablespace. This will result in non-system data segments being added to the SYSTEM tablespace and possible performance degradation in the SYSTEM tablespace. |

¹ The policy rule is evaluated each time its underlying *db_recUserSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Cluster object types because the Reorganize Objects wizard does not support them.

All user accounts that are, by default, part of the Oracle Database or Enterprise Manager. For example: SYS, SYSTEM, SYSMAN, CTXSYS, SCOTT, ADAMS, and so on.

Impact of Violation

These users use a system tablespace as the default tablespace. This violation will result in non-system data segments being added to the system tablespace, making it more difficult to manage these data segments and possibly resulting in performance degradation in the system tablespace.

Action

Change the default tablespace for these users to specify a non-system tablespace.

5.4.12 Users with Permanent Tablespace as Temporary Tablespace

This policy checks the PERM_AS_TEMP_TBSP parameter to detect whether a permanent tablespace is being used as a temporary tablespace.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|----------------------------------------|----------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informational | Storage | Database Instance; Cluster Database | Oracle Server 9.2 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | User %USER_NAME% uses permanent tablespace %TABLESPACE_NAME% as the temporary tablespace. Using a permanent tablespace as the temporary tablespace may result in performance degradation, especially for Real Application Clusters. |

¹ The policy rule is evaluated each time its underlying *Db_recUserSettings* metric is collected.

Defaults

Parameters and Their Default Values

Parameter default values are dependent on the version of the Oracle Database target. Refer to the Oracle Database documentation for that version of the database target to learn about the parameters and their default values.

Objects Excluded by Default

Not Applicable

Impact of Violation

These users use a permanent tablespace as the temporary tablespace. Using temporary tablespaces allows space management for sort operations to be more efficient. Using a permanent tablespace for these operations may result in performance degradation, especially for Real Application Clusters.

Action

Change the temporary tablespace for these users to specify a tablespace of type TEMPORARY.

Host Policies

This chapter provides the following information for each of the Host policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Host policies are categorized as follows:

- [Section 6.1, "Configuration Policies"](#)
- [Section 6.2, "Security Policies"](#)

6.1 Configuration Policies

The configuration policies for the Host target are:

6.1.1 Critical Patch Advisories for Oracle Homes

This policy evaluates and informs the Enterprise Manager administrators of patch advisories that are applicable to various Oracle Homes in the enterprise.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | Host | Any version of Oracle products in the Oracle Homes could be affected by the patch advisories. | The underlying metric is <i>critical_patch_advisories_metric</i> . Whenever the RefreshFromMetalink job is run or any HostConfigurationCollect ion happens, the metric is evaluated. The RefreshFromMetalink job is scheduled to run once every 24 hours but the user can run the job anytime. | Yes | To help ensure a secure and reliable configuration, all relevant and current critical patches should be applied. Vulnerabilities have been identified for the following critical patch advisories. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Vulnerabilities have been identified for the current critical patch advisories.

Action

The user is advised to apply the critical patches and resolve the vulnerabilities.

6.2 Security Policies

The security policies for the Host target are:

6.2.1 Execute Stack

This policy ensures that the Operating System configuration parameter, which enables execution of code on the user stack, is not enabled.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|----------------------------------|----------------------------------------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------|
| Warning | Security | Host | All UNIX-Based Operating Systems | The underlying metric is <i>executeStackRep</i> which has a collection frequency of once every 24 hours. | Yes | The host is in an insecure state. Executable code on the user stack is enabled. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Enabling code execution on the user stack may allow a malicious user to exploit stack buffer overflows. Overflows can cause portions of a system to fail, or even execute arbitrary code.

Action

Disable code execution on the user stack.

6.2.2 Insecure Services

This policy ensures that there are no insecure services (for example, telnet and FTP) running on the server. When installed, most operating systems run services that are not always necessary, for example Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP). These services might pose security risks. This policy ensures that such services are shut down.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|-------------------|--------------------------------------------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------|
| Warning | Security | Host | All Systems | The underlying metric is <i>insecureServicesRep</i> which has a collection frequency of once every 24 hours. | Yes | The host is in an insecure state. The insecure service %service% is running on the host. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Insecure services may allow a malicious user to take over the host.

Action

Do not run insecure services.

6.2.3 NTFS File System

This policy ensures that the file system on a Windows operating system uses is NT File System (NTFS).

NTFS is far more secure than File Allocation Table (FAT) because it is tightly integrated with the operating system security. NTFS also allows users to set file-level security and permissions on folders. Local or domain accounts can be used to provide different levels of access to files and folders. Windows 2000 also supports encryption on NTFS partitions, making the partitions more secure.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|---------------------------|------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------|
| Critical | Security | Host | Windows Operating Systems | The underlying metric is <i>fileSystemTypeRep</i> which has a collection frequency of once every 24 hours. | Yes | The host is in an insecure state. NTFS is not configured on the Windows operating system. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Other than NTFS, file systems on Windows platforms may have serious security risks.

Action

On Windows operating systems, it is strongly recommended to use NTFS as the file system.

6.2.4 Open Ports

This policy ensures that no unintended ports are left open.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|-----------------------|-------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------|
| Critical | Security | Host | All Operating Systems | The underlying metric is <i>openPortsRep</i> which has a collection frequency of once every 24 hours. | Yes | The host is in an insecure state. Port %port% is open. |

¹ The policy rule is evaluated each time its underlying metric is collected.

Defaults**Parameters and Their Default Values**

Parameter name: DFLT_PORT

Default value: 32767

Objects Excluded by Default

Not Applicable

Impact of Violation

Open ports may allow a malicious user to take over the host.

Action

Do not open insecure ports. Be sure to close both the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) ports to ensure security.

Listener Policies

This chapter provides the following information for each of the Listener policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Listener policies are categorized as follows:

- [Section 7.1, "Security Policies - UNIX"](#)
- [Section 7.2, "Security Policies - Windows"](#)

7.1 Security Policies - UNIX

The security policies for the Listener target on UNIX are:

7.1.1 Allowed Logon Version

This policy ensures that the server allows logon from clients with a matching version or higher only.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The SQLNET.ALLOWED_LOGON_VERSION parameter is set to %version%. |

¹ The policy rule is evaluated each time its underlying *sqlnetAllowedLogonVersionRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Setting the parameter `SQLNET.ALLOWED_LOGON_VERSION` in `sqlnet.ora` to a version lower than the server version will force the server to use a less secure authentication protocol.

Action

Set the parameter `SQLNET.ALLOWED_LOGON_VERSION` in `sqlnet.ora` to the server's major version. Setting this value to older versions could expose vulnerabilities that may have existed in the authentication protocols.

7.1.2 Listener Default Name

This policy ensures that the default name of the listener is not used.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener is addressed by the default name. |

¹ The policy rule is evaluated each time its underlying `lsnrDefaultNameMetricRep` metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Having a listener with the default name increases the risk of unauthorized access and denial of service attacks.

Action

Avoid having a listener with the default name (LISTENER).

7.1.3 Listener Direct Administration

This policy ensures that no runtime modifications to the listener configuration is allowed.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. Direct administration is enabled. |

¹ The policy rule is evaluated each time its underlying *IsnrDirectAdminMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

Not Applicable

Impact of Violation

A malicious user who has access to a running listener can perform runtime modifications (for example, SET operations) using the `lsnrctl` program.

Action

All listeners must have direct administration disabled. Set `ADMIN_RESTRICTIONS_<listener_name>` to ON in `listener.ora`.

7.1.4 Listener Log File Owner

This policy ensures that the listener log file is owned by the Oracle software owner.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener log file <code>%file_name%</code> is owned by <code>%file_owner%</code> . |

¹ The policy rule is evaluated each time its underlying *IsnrLogFileOwnerMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The information in the log file can reveal important network and database connection details. Having a log file not owned by the Oracle software owner can expose them to public scrutiny with possible security implications.

Action

The listener log file must be owned by Oracle software owner.

7.1.5 Listener Log File Permission

This policy ensures that the listener log file cannot be read by or written to by public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener log file %file_name% has permission %file_permission%. |

¹ The policy rule is evaluated each time its underlying *IsnrLogFilePermMetricRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The information in the log file can reveal important network and database connection details. Allowing access to the log file can expose them to public scrutiny with possible security implications.

Action

The listener log file must not allow public to read or write to it. Restrict the file permission to Oracle software owner and DBA group.

7.1.6 Listener Logging Status

This policy ensures that listener logging is enabled.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. Logging is not enabled. |

¹ The policy rule is evaluated each time its underlying *IsnrLogStatusMetricRep* metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Without listener logging attacks on the listener can go unnoticed.

Action

Enable listener logging by setting the LOG_STATUS parameter to ON.

7.1.7 Listener Password

This policy ensures that access to listener is password protected.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. Listener %listener% is running without password protection. |

¹ The policy rule is evaluated each time its underlying *IsnrPasswdMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

Not Applicable

Impact of Violation

Without password protection, a user can gain access to the listener. Once someone has access to the listener, he or she can stop the listener. He or she can also set a password and prevent others from managing the listener.

Action

All listeners should be protected by a non-trivial password using the CHANGE_PASSWORD command.

7.1.8 Listener Trace Directory Owner

This policy ensures that the listener trace directory is a valid directory owned by Oracle software owner.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener trace directory %dir_name% is owned by %dir_owner%. |

¹ The policy rule is evaluated each time its underlying *IsnrTraceDirOwnMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Having a trace directory not owned by the Oracle software owner can expose the trace files to public scrutiny with possible security implications.

Action

The listener trace directory must be owned by the Oracle software owner.

7.1.9 Listener Trace Directory Permission

This policy ensures that the listener trace directory does not have public read or write permissions.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener trace directory %dir_name% has permission %dir_permission%. |

¹ The policy rule is evaluated each time its underlying *IsnrTraceDirPermMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Allowing access to the trace directory can expose them to public scrutiny with possible security implications.

Action

The listener trace directory must not allow public to read or write to it. Restrict the directory permission to Oracle software owner and DBA group.

7.1.10 Listener Trace File Owner

This policy ensures that the listener trace file owner is the same as the Oracle software owner.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener trace file %file_name% is owned by %file_owner%. |

¹ The policy rule is evaluated each time its underlying *IsnrTraceFileOwnMetricRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Having trace files not owned by the Oracle software owner can expose them to public scrutiny with possible security implications.

Action

The listener trace file must be owned by Oracle software owner.

7.1.11 Listener Trace File Permission

This policy ensures that the listener trace file is not accessible to public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The listener trace file %file_name% has permission %file_permission%. |

¹ The policy rule is evaluated each time its underlying *IsnrTraceFilePermMetricRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Allowing access to the trace files can expose them to public scrutiny with possible security implications.

Action

The listener trace file must not allow public to read or write to it. Restrict the file permission to Oracle software owner and DBA group.

7.1.12 Listener.ora Permission

This policy ensures that the file permissions for listener.ora are restricted to the owner of Oracle software.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. Permissions of listener.ora are not restricted to the Oracle set. |

¹ The policy rule is evaluated each time its underlying *lsnrOraPermRep* metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

Not Applicable

Impact of Violation

If the listener.ora file is public readable, passwords may be extracted from this file. This can also lead to exposure of detailed information on the Listener, database, and application configuration. Also, if public has write permissions, a malicious user can remove any password that has been set on the listener.

Action

Listener.ora permissions should be restricted to the owner of Oracle software installation and DBA group.

7.1.13 Oracle Net Client Log Directory Owner

This policy ensures that the client log directory is a valid directory owned by Oracle set with no permissions to the PUBLIC role.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The client log directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *clientLogDirRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.14 Oracle Net Client Log Directory Permission

This policy ensures that the client log directory is a valid directory owned by Oracle set with no permissions to the PUBLIC role.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The client log directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *clientLogDirRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.15 Oracle Net Client Trace Directory Owner

This policy ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The client trace directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *clientTrcDirRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.16 Oracle Net Client Trace Directory Permission

This policy ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The client trace directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *clientTrcDirRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.17 Oracle Net Server Log Directory Owner

This policy ensures that the server log directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The server log directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *svrLogDirRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.18 Oracle Net Server Log Directory Permission

This policy ensures that the server log directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The server log directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *svrLogDirRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.19 Oracle Net Server Trace Directory Owner

This policy ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The server trace directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *svrTrcDirRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.20 Oracle Net Server Trace Directory Permission

This policy ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The server trace directory %dir_name% has permission %permissions%. |

¹ The policy rule is evaluated each time its underlying *svrTrcDirRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.1.21 Restrict sqlnet.ora Permissions

This policy ensures that the sqlnet.ora file is not accessible to the public.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The sqlnet.ora file has permission %permission%. |

¹ The policy rule is evaluated each time its underlying *sqlnetOraPermRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If the sqlnet.ora file is public readable, a malicious user may attempt to read this file which could lead to sensitive information being exposed. For example, log and trace destination information of the client and server could be exposed.

Action

Public should not be given any permissions on the sqlnet.ora file.

7.1.22 Use of Hostname in Listener.ora

This policy ensures that the listener host is specified as IP address and not hostname in the listener.ora file.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Host is not specified as IP address in listener.ora. |

¹ The policy rule is evaluated each time its underlying *lsnrHostNameMetricRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

Not Applicable

Impact of Violation

An insecure Domain Name System (DNS) Server can be taken advantage of for mounting a spoofing attack. Name server failure can result in the listener unable to resolved the host.

Action

Host should be specified as IP address in listener.ora.

7.2 Security Policies - Windows

The security policies for the Listener target on Windows are:

7.2.1 Listener Log File Permission (Windows)

This policy ensures that the listener log file cannot be read by or written to by public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state.The users %users% have critical permissions on the listener log file %file_name%. |

¹ The policy rule is evaluated each time its underlying *lsnrLogFilePermMetricNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

The information in the log file can reveal important network and database connection details. Allowing access to the log file can expose them to public scrutiny with possible security implications.

Action

The listener log file must not allow public to read or write to it. Restrict the file permission to Oracle software owner and DBA group.

7.2.2 Listener Trace Directory Permission (Windows)

This policy ensures that the listener trace directory does not have public read or write permissions. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The users %users% have critical permissions on the listener trace directory %dir_name%. |

¹ The policy rule is evaluated each time its underlying *lsnrTraceDirPermMetricNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Allowing access to the trace directory can expose them to public scrutiny with possible security implications.

Action

The listener trace directory must not allow public to read or write to it. Restrict the directory permission to Oracle software owner and DBA group.

7.2.3 Listener Trace File Permission (Windows)

This policy ensures that the listener trace file is not accessible to public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|---------------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Informational | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. The users %users% have critical permissions on the listener trace file %file_name%. |

¹ The policy rule is evaluated each time its underlying *lsnrTraceFilePermMetricNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Allowing access to the trace files can expose them to public scrutiny with possible security implications.

Action

The listener trace file must not allow public to read or write to it. Restrict the file permission to Oracle software owner and DBA group.

7.2.4 Listener.ora Permission (Windows)

This policy ensures that the file permissions for listener.ora are restricted to the owner of Oracle software. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------|
| Warning | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Listener is in an insecure state. Permissions of listener.ora are not restricted to the Oracle set. |

¹ The policy rule is evaluated each time its underlying *lsnrOraPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

Not Applicable

Impact of Violation

If the listener.ora file is public readable, passwords may be extracted from this file. This can also lead to exposure of detailed information on the Listener, database, and application configuration. Also, if public has write permissions, a malicious user can remove any password that has been set on the listener.

Action

Listener.ora permissions should be restricted to the owner of Oracle software installation and DBA group.

7.2.5 Oracle Net Client Log Directory Permission (Windows)

This policy ensures that the client log directory is a valid directory owned by Oracle set with no permissions to the PUBLIC role. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The users %users% have critical permissions on the client log directory %dir_name%. |

¹ The policy rule is evaluated each time its underlying *clientLogDirNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.2.6 Oracle Net Client Trace Directory Permission (Windows)

This policy ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to the public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The users %users% have critical permissions on the client trace directory %dir_name%. |

¹ The policy rule is evaluated each time its underlying *clientTrcDirNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The client trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.2.7 Oracle Net Server Log Directory Permission (Windows)

This policy ensures that the server log directory is a valid directory owned by Oracle set with no permissions to the public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The users %users% have critical permissions on the server log directory %dir_name%. |

¹ The policy rule is evaluated each time its underlying *svrLogDirNTRep* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server log directory must be a valid directory owned by the Oracle set with no permissions to public.

7.2.8 Oracle Net Server Trace Directory Permission (Windows)

This policy ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to the public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | The database is in an insecure state. The users %users% have critical permissions on the server trace directory %dir_name%. |

¹ The policy rule is evaluated each time its underlying *svrTrcDirNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

Action

The server trace directory must be a valid directory owned by the Oracle set with no permissions to public.

7.2.9 Restrict sqlnet.ora Permissions (Windows)

This policy ensures that the sqlnet.ora file is not accessible to the public. The following permissions on Windows NT based platforms are considered critical: DELETE, WRITE_DAC, WRITE_OWNER, CHANGE, ADD, and FULL. The policy gives the number of users or user groups which have been granted such permissions, and lists the users and user groups in parentheses.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------|
| Critical | Security | Listener | Oracle Server 8 or later | The underlying metric has a collection frequency of once every 24 hours. | Yes | Database is in insecure state. The users %users% have critical permissions on the sqlnet.ora file. |

¹ The policy rule is evaluated each time its underlying *sqlnetOraPermNTRep* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If the sqlnet.ora file is public readable, a malicious user may attempt to read this file which could lead to sensitive information being exposed. For example, log and trace destination information of the client and server could be exposed.

Action

Public should not be given any permissions on the sqlnet.ora file.

OC4J Policy

This chapter provides the following information for the Oracle Application Server Containers for J2EE (OC4J) policy:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

8.1 OC4J Password Indirection

This policy verifies that password indirection is used in OC4J XML configuration and deployment files.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------|
| Critical | Security | OC4J | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Password indirection is not used in configuration file %FILE_NAME%. |

¹ The policy rule is evaluated each time its underlying *Password_Indirection* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Embedding these passwords into deployment and configuration files poses a security risk, especially if the permissions on the files allow them to be read by any user.

Action

To avoid this problem, OC4J provides password indirection and password obfuscation.

Oracle HTTP Server Policies

This chapter provides the following information for each of the Oracle HyperText Transfer Protocol (HTTP) Server policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

The Oracle HTTP Server policies are categorized as follows:

- [Section 9.1, "Configuration Policies"](#)
- [Section 9.2, "Security Policies"](#)

9.1 Configuration Policies

The configuration policies for the HTTP target are:

9.1.1 HTTP Server HostNameLookups

This policy verifies that the HostNameLookups directive is set to *off* on this HTTP Server.

Any DNS lookup can affect Apache performance. The HostNameLookups directive in Apache informs Apache whether it should log information based on the IP address (if the directive is set to *off*), or look up the hostname associated with the IP address of each request in the DNS system on the Internet (if the directive is set to *on*).

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------|
| Critical | Configuration | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | HostNameLookups directive is set to <i>on</i> for HTTP Server. |

¹ The policy rule is evaluated each time its underlying *PerfRelated* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If HostNameLookups directive is set to *on* or *double*, then extra DNS lookups will be performed. Any DNS lookup can affect HTTP Server performance.

Oracle has found that performance degraded by a minimum of about 3% in our tests with HostNameLookups set to *on*.

Action

In the configuration file (`httpd.conf`), set the HostNameLookups directive to *off*.

9.1.2 HTTP Server MaxKeepAliveRequests

This policy verifies that the MaxKeepAliveRequests directive is set to a non-zero value on this HTTP Server.

A value of zero in the MaxKeepAliveRequests directive means there is no limit on the number of connections, which are kept alive expecting subsequent client requests. But Httpd server process cannot be used to service other requests until either the client disconnects, or the connection times out.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|---------------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------|
| Critical | Configuration | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | MaxKeepAliveRequests directive is set to zero in the HTTP Server configuration file (<code>httpd.conf</code>). |

¹ The policy rule is evaluated each time its underlying *PerfRelated* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If the `MaxKeepAliveRequests` directive is set to zero (an unlimited number of connections), the `Httpd` server process cannot be used to service other requests until either the client disconnects, or the connection times out.

Action

Do not set the `MaxKeepAliveRequests` directive to zero.

9.2 Security Policies

The security policies for the HTTP target are:

9.2.1 HTTP Server Access Logging

To effectively manage an HTTP server, it is necessary to get feedback about the activity and performance of the server, as well as any problems that may be occurring. The server access log records all requests processed by the server. The location and content of the access log is controlled by the `CustomLog` directive. The `LogFormat` directive can be used to simplify the selection of the contents of the logs.

Access Logging can be configured in such a way that it contains vital information about requests and users who access HTTP Server. This policy verifies that Access Logging is enabled.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Access logging is not enabled for HTTP Server. |

¹ The policy rule is evaluated each time its underlying `httpdSecurityViolations` metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Absence of an access log can severely cripple administrators' ability to monitor malicious attacks.

Action

Enable the access logging for HTTP Server.

9.2.2 HTTP Server Directory Indexing

The HTTP Server can automatically generate the index of a directory. The IndexOptions directive can be used to configure this.

This policy verifies that Directory Indexing is disabled.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|-----------------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | HTTP Server Directory Indexing is <i>on</i> . |

¹ The policy rule is evaluated each time its underlying *httpdSecurityViolations* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If indexing is *on*, a malicious user may be able to view restricted files and directories in the Document Root directory.

Action

Turn off Directory Indexing.

9.2.3 HTTP Server Dummy Wallet

The HTTP Server comes with a preconfigured wallet that is used for SSL authentication. The *ssl.conf* file has already been configured to use this wallet. The wallet location is specified in this file with the SSLWallet parameter. By default, this parameter points to the *ewallet.p12* file which is located in your `$ORACLE_HOME/Apache/Apache/conf/ssl.wlt/default` directory.

This policy checks whether a Dummy Wallet is being used on HTTP Server.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Dummy Wallet is used by HTTP Server. |

¹ The policy rule is evaluated each time its underlying *httpdSecurityViolations* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Use of a Dummy Wallet provided by Oracle can severely compromise the security of the site.

Action

Do not use a Dummy Wallet for production SSL load.

9.2.4 HTTP Server Owner And Setuid Bit

This policy verifies that the HTTPd binary is not owned by a super user and the suid bit is not set.

Binaries with suid privilege can be exploited to get extra privilege on the host. If a super user owns the HTTPd binary and the suid bit is set; a malicious user can exploit it to gain super user privileges on the host.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|---------------------------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | HTTP Server is owned by root and the setuid bit is set. |

¹ The policy rule is evaluated each time its underlying *httpdSecurityViolations* metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If HTTPd is owned by root and the setuid bit is set, malicious users may be able to gain access to the system as a super user.

Action

A user other than root should own the HTTPd binary.

9.2.5 HTTP Server SSL

The `ias-component` element in `opmn.xml` file is used to enable or disable the use of Secure Socket Layer (SSL). This file is located in `ORACLE_HOME/opmn/conf/opmn.xml`.

This policy checks whether Secure Socket Layer (SSL) is enabled for Single Sign-On (SSO) on HTTP Server.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|--------------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | SSL is not enabled for SSO on HTTP Server. |

¹ The policy rule is evaluated each time its underlying `httpdSecurityViolations` metric is collected.

Defaults**Parameters and Their Default Values**

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

If SSL is not enabled on HTTP Server, malicious users may detect the user name and password entered by a user.

Action

For secure transmission of user name and password, enable SSL on HTTP Server.

9.2.6 HTTP Server Writable Files

This policy checks whether users other than the owner have write permission in the DocumentRoot folder.

The DocumentRoot directive sets the directory from which HTTP Server will serve files. Unless matched by a directive like Alias, the server appends the path from the requested URL to the document root to make the path to the document.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------|
| Critical | Security | HTTP Server | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | There are writable files in the Document Root folder on HTTP Server. |

¹ The policy rule is evaluated each time its underlying *httpdSecurityViolations* metric is collected.

Defaults

Parameters and Their Default Values

Not Applicable

Objects Excluded by Default

Not Applicable

Impact of Violation

Malicious users may be able to overwrite a writable file in the Document Root directory.

Action

Do not include any group or world writable files in the Document Root folder.

Web Cache Policies

This chapter provides the following information for each of the Oracle Application Server Web Cache policies:

- Brief description of the policy
- Summary of the policy's main properties
- Default values for the policy: parameters with their default values and objects excluded by default
- Impact of the policy violation
- Action to perform when the violation occurs

10.1 Web Cache Access Logging

This policy checks whether access logging is enabled on Web Cache. To effectively manage Web Cache, it is necessary to get feedback about the activity and performance of the server, as well as any problems that may be occurring.

The server access log records all requests processed by the server. The ACCESSLOG element in `$ORACLE_HOME/webcache/webcache.xml` is used to configure this.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------|
| Critical | Security | Web Cache | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Access logging is not enabled for Web Cache. |

¹ The policy rule is evaluated each time its underlying `webcacheSecurityViolations` metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Absence of an access log can severely cripple administrators' ability to monitor malicious attacks.

Action

Enable access logging for Web Cache.

10.2 Web Cache Dummy Wallet

This policy checks whether a Dummy Wallet is being used on Web Cache.

A dummy wallet is located in `$ORACLE_HOME/webcache/wallets/default` on UNIX and `ORACLE_HOME\webcache\wallets\default` on Windows. This wallet is intended for testing purposes for OracleAS Web Cache HTTPS communication to origin servers.

For a production environment, use the procedures described in the documentation to create a new wallet with Oracle Wallet Manager. By default, Oracle Wallet Manager stores wallets in directory `/etc/ORACLE/WALLETS/user_name` on UNIX and `%USERPROFILE%\ORACLE\WALLETS` on Windows.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|------------------------------------|
| Critical | Security | Web Cache | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Dummy Wallet is used by Web Cache. |

¹ The policy rule is evaluated each time its underlying `webcacheSecurityViolations` metric is collected.

Defaults**Parameters and Their Default Values**

None

Objects Excluded by Default

None

Impact of Violation

Use of a Dummy Wallet provided by Oracle could severely compromise the security of the site.

Action

Do not use a Dummy Wallet for production SSL load.

10.3 Web Cache Owner and Setuid Bit

This policy verifies that the webcached binary is not owned by a super user.

Binaries with suid privilege can be exploited to get extra privileges on the host. If a super user owns the webcached binary and the suid bit is set, a malicious user can exploit it to gain super user privileges on the host.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------|
| Critical | Security | Web Cache | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | Web Cache is owned by root and the setuid bit is set. |

¹ The policy rule is evaluated each time its underlying *webcacheSecurityViolations* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

If Web Cache is owned by root and the setuid bit is set, malicious users may be able to gain access to the system as a super user.

Action

A user other than super user (root) should own the webcached binary.

10.4 Web Cache Writable Files

This policy checks whether users other than the owner have write permission in the directory from which Web Cache will serve files.

Policy Summary

The following table lists the policy's main properties.

| Severity | Category | Target Type | Versions Affected | Policy Rule Evaluation ¹ | Automatically Enabled? | Alert Message |
|----------|----------|-------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------|----------------------------------------------------------|
| Warning | Security | Web Cache | Oracle Application Server 9.0.4.x and Oracle Application Server 10.1.2.x | The underlying metric has a collection frequency of once every 24 hours. | Yes | There are writable files in the docs folder of Webcache. |

¹ The policy rule is evaluated each time its underlying *webcacheSecurityViolations* metric is collected.

Defaults

Parameters and Their Default Values

None

Objects Excluded by Default

None

Impact of Violation

Malicious users may be able to overwrite a writable file in the Document Root directory.

Action

Do not include any group or world writable files in the Document Root directory.